Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

FE5012

User Manual

Status:	v1.0 draft	26-mei-2025
Author:	Onno Verkerk	

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Revision history

Nr	Date	Remarks
1	26-mei-2025	Version 1.0 initial version (draft)

Note: To ensure proper operation, please read this manual thoroughly before using the product and retain the information for future reference.

Copyright © 2025 TKH Security B.V.

FE5012 User Manual v1.0 draft

Brand names

Any brand names mentioned in this manual are registered trademarks of their respective owners.

Liability

TKH Security accepts no liability for claims from third parties arising from improper use other than that stated in this manual.

Although considerable care has been taken to ensure a correct and suitably comprehensive description of all relevant product components, this manual may nonetheless contain errors and inaccuracies. We invite you to offer your suggestions and comments by email. Your feedback will help us to further improve our documentation.

How to contact us

If you have any comments or queries concerning any aspect related to the product, do not hesitate to contact:

TKH Security B.V.
Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

General : +31 79 363 8111
E-mail : support@tkhsecurity.com
WWW : https://tkhsecurity.com

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Legal Information

About this Manual

This Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in this Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the company website.
Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

Trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

To the maximum extent permitted by applicable law, this manual and the product described, with its hardware, software and firmware, are provided "as is" and "with all faults and errors". Our company makes no warranties, express or implied, including without limitation, merchantability, satisfactory quality, or fitness for a particular purpose. The use of the product by you is at your own risk. In no event will our company be liable to you for any special, consequential, incidental, or indirect damages, including, among others, damages for loss of business profits, business interruption, or loss of data, corruption of systems, or loss of documentation, whether based on breach of contract, tort (including negligence), product liability, or otherwise, in connection with the use of the product, even if our company has been advised of the possibility of such damages or loss.
You acknowledge that the nature of the internet provides for inherent security risks, and our company shall not take any responsibilities for abnormal operation, privacy leakage or other damages resulting from cyber-attack, hacker attack, virus infection, or other internet security risks; however, our company will provide timely technical support if required.
You agree to use this product in compliance with all applicable laws, and you are solely responsible for ensuring that your use conforms to the applicable law. Especially, you are responsible, for using this product in a manner that does not infringe on the rights of third parties, including without limitation, rights of publicity, intellectual property rights, or data protection and other privacy rights. You shall not use this product for any prohibited end-uses, including the development or production of weapons of mass destruction, the development or production of chemical or biological weapons, any activities in the context related to any nuclear explosive or unsafe nuclear fuel-cycle, or in support of human rights abuses.
In the event of any conflicts between this manual and the applicable law, the latter prevails.

Regulatory Information

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

FCC Information

1. FCC compliance

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

2. FCC conditions:

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

CE Information

CE The products have been manufactured to comply with the following directives:

EMC Directive 2014/30/EU

RoHS

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

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

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

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

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

Privacy Protection

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

Cybersecurity Recommendations

- Use a strong password. At least 8 characters or a combination of characters, numbers, and upper and lower case letters should be used in your password.
- Regularly change the passwords of your devices to ensure that only authorized users can access the system (for instance every 90 days).
- It is recommended to change the service default ports (like HTTP-80, HTTPS-443, etc.) to reduce the risk of outsiders being able to access.
- It is recommended to set
- the firewall of your router. But note that some important ports cannot be closed (like HTTP port, HTTPS port, Data Port).
- It is not recommended to expose the device to the public network. When it is necessary to be exposed to the public network, please set the external hardware firewall and the corresponding firewall policy.
- It is not recommended to use the v1 and v2 functions of SNMP.
- In order to enhance the security of WEB client access, please create a TLS certificate to enable HTTPS.
- Use black and white list to filter the IP address. This will prevent everyone, except those specified IP addresses from accessing the system.
- If you add multiple users, please limit functions of guest accounts.
- If you enable UPnP, it will automatically try to forward ports in your router or modem. It is really very convenient for users, but this will increase the risk of data leakage when the system automatically forwards ports. Disabling UPnP is recommended when the function is not used in real applications.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

- Check the log. If you want to know whether your device has been accessed by unauthorized users or not, you can check the log. The system log will show you which IP addresses were used to log in your system and what was accessed.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Table of Contents

1 About this manual 11

2 Introduction 12

3 Network Connection 13

3.1 LAN 13

3.1.1 Access through SDM2 Device Manager software 13

4 Live View 16

5 Network Camera Configuration 20

5.1 System Configuration 20

5.1.1 Basic Information 20

5.1.2 Date and Time 20

5.1.3 Local Config 21

5.1.4 Storage 21

5.1.5 Serial Port Settings 25

5.1.6 Configuring Fisheye Parameters 25

5.2 Image Configuration 25

5.2.1 Display Configuration 25

5.2.2 Video / Audio Configuration 28

5.2.3 OSD Configuration 29

5.2.4 Video Mask 31

5.2.5 ROI Configuration 31

5.3 Alarm Configuration 32

5.3.1 Motion Detection 32

5.3.2 Exception Alarm 35

5.3.3 Alarm In 36

5.3.4 Alarm Out 37

5.3.5 Alarm Server 38

5.3.6 Audio Alarm 38

5.3.7 Audio Exception 40

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

5.3.8 Disarming 41
5.4 Event Configuration 42
5.4.1 Line Crossing 42
5.4.2 Region Intrusion 45
5.4.3 Region Entrance 47
5.4.4 Region Exiting 47
5.4.5 Target Counting by Line 47
5.4.6 Heat Map 50
5.5 Network Configuration 51
5.5.1 TCP/IP 51
5.5.2 Port 53
5.5.3 Server Configuration 53
5.5.4 Onvif 54
5.5.5 DDNS 54
5.5.6 SNMP 55
5.5.7 802.1x 56
5.5.8 RTSP 57
5.5.9 RTMP 58
5.5.10 UPNP 59
5.5.11 Email 59
5.5.12 FTP 60
5.5.13 HTTP POST 61
5.5.14 HTTPS 62
5.5.15 Cloud Service 64
5.5.16 QoS 64
5.6 Security Configuration 65
5.6.1 User Configuration 65
5.6.2 Online User 66
5.6.3 Block and Allow Lists 67
5.6.4 Security Management 67
5.7 Maintenance Configuration 68
5.7.1 Backup and Restore 68

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

5.7.2 Reboot 69
5.7.3 Upgrade 70
5.7.4 Operation Log 71
5.7.5 Serial Output 71
5.7.6 Maintenance Information 71

6 Search 72

6.1 Image Search 72
6.2 Video Search 73

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

1 About this manual

What's in this manual

This is version 1 of the installation assistance provided for the FE5012. The manual gives you all the information you need to install the product. It tells you:

- How to connect cables
- How to get access to the camera
- How to set up video resolution
- How to export and import configuration files
- How to delete previously-installed Viewer software and to enable Siqura Viewer installation

Where to find more information

Find additional manuals, and the latest firmware for this product at https://tkhsecurity.com. We advise you to make sure that you have the latest version of this manual.

Who this manual is for

These instructions are for all professionals who will install FE5012.

What you need to know

You will have a better understanding of how the camera works if you are familiar with:

- Camera technologies
- CCTV systems and components
- Ethernet network technologies and Internet Protocol (IP)
- Windows environments
- Video, audio, data, and contact closure transmissions
- Video compression methods

Before you continue

Before you continue, read and obey all instructions and warnings in this manual. Keep this manual with the original bill of sale for future reference and, if necessary, warranty service. When you unpack your product, make sure there are no missing or damaged items. If any item is missing, or if you find damage, do not install or operate this product. Ask your supplier for assistance.

Why specifications may change

We are committed to delivering high-quality products and services. The information given in this manual was current when published. As we continuously seek to improve our products and user experience, all features and specifications are subject to change without notice.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

2 Introduction

The fisheye network camera which adopts high-definition fisheye lens and high performance image sensor can meet 360° high definition surveillance requirements. With the advanced H.265/H.264 video compression technology, high compression rate, accuracy and stable stream control, the camera ensures higher quality image and less occupancy of storage space.
This product can be widely used in banks, telecommunication systems, electricity power departments, law systems, factories, storehouses, uptowns, etc. In addition, it is also an ideal choice for surveillance sites with middle or high risks.

Surveillance Application

DORI Distance

Level	Resolution	Detect	Observe	Recognize	Identify
Object Distance	6MP	33m	13m	6m	3m
	12MP	35m	14m	7m	3.5m
Recommended Installation Height	2.5m				

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

3 Network Connection

System Requirement

For proper operating the product, the following requirements are suggested for your computer.

Operating System: Windows 10 professional version or higher

CPU: i7-117000 2.5GHz or higher

GPU: AMD770+intel UHD Graphics 750

RAM: 8G or higher (6MP fisheye camera); 16G or higher (12MP fisheye camera)

Display: 1920*1080 resolution or higher

Web browser: Chrome89.0+/Edge89.0+/Firefox87.0+/Safari 14.0+

It is recommended to use the latest version of these web browsers.

The menu display and operation of the camera may be slightly different by using the browser with plug-in or without plug-in. Installing the plug-in will display more functions of the camera.

Connect IP camera via LAN or WAN. Here only take the plug-in required browser for example. The details are as follows:

3.1 LAN

In LAN, there are two ways to access the device: 1. access through SDM2 Device Manager software; 2. direct access through IE browser.

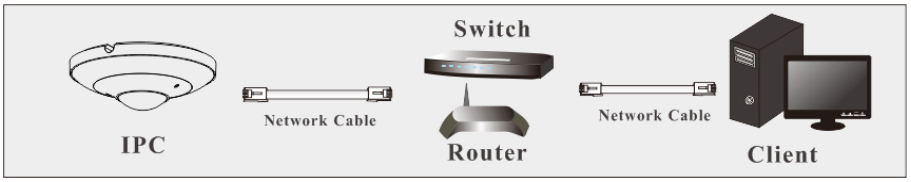
3.1.1 Access through SDM2 Device Manager software

SDM2 Device Manager is a tool to detect, activate and modify the IP address of the device over the LAN.

Before You Start

- Get the SDM2 Device Manager software from the TKH Security website (tkhsecurity.com> Products> Services> Knowledge Base> Support software> SDM2 Device Manager), and install the SDM2 Device Manager according to the prompts.
- The device and the PC that runs the SDM2 Device Manager tool should belong to the same subnet.

Network connection:



Note

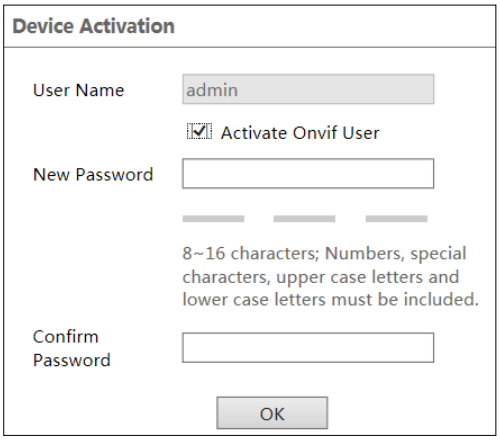
Make sure the PC and device are connected to the LAN and the SDM2 is installed on the PC.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

By default, the camera has DHCP enabled, which means that it will obtain its IP address automatically from your network. In case your network does not support the DHCP function, i.e. no DHCP server is active on your network, then after some time the camera will fall back to the factory default static IP address 10.x.y.z / 255.0.0.0, where x.y.z are the last three bytes from the camera's MAC address. If you do not know the camera's MAC address, you can check the product label and find the camera's serial number. The camera's serial number consists of the model name, then the last three bytes in the MAC address. Converting those three bytes from hexadecimal into decimal will result in the last three numbers in the factory static IP address. If you are in difficulty making these calculations, then find the helper dialog in the SDM2 Device Manager's Tools menu, which will make the calculations for you.

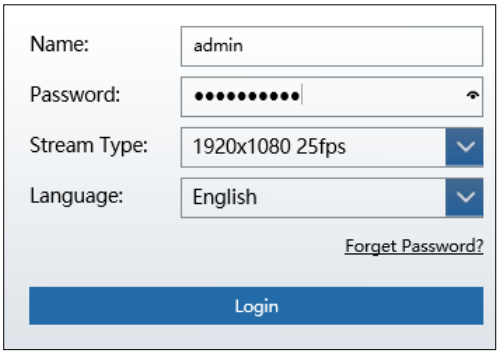
If SDM2 does not automatically detect the camera, then you can also manually add it with the static IP address.

You will need to first Activate the camera. To do this, go to the camera' web page. Double click the IP address and then the system will pop up the IE browser to connect the device. Activate the device.



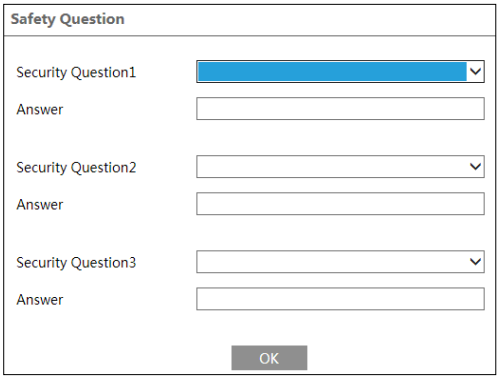
Please self-define the password of admin according to the tip.
If "Activate Onvif User" is enabled, the ONVIF user can be activated simultaneously. When you connect the camera through the ONVIF protocol in the third-party platform, you can use the default username and the password set above to connect.
After that, follow directions to download, install and run the Active X control if prompted.
Re-connect your camera via IE browser and then a login box will appear.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands



Please enter the user name (admin) and password. Then select the stream type and language as needed.
Stream Type: The plug-in free live view only supports1080P or lower resolution.

The security questions should be set after you click “Login” button. It is very important for you to reset your password. Please remember these answers.

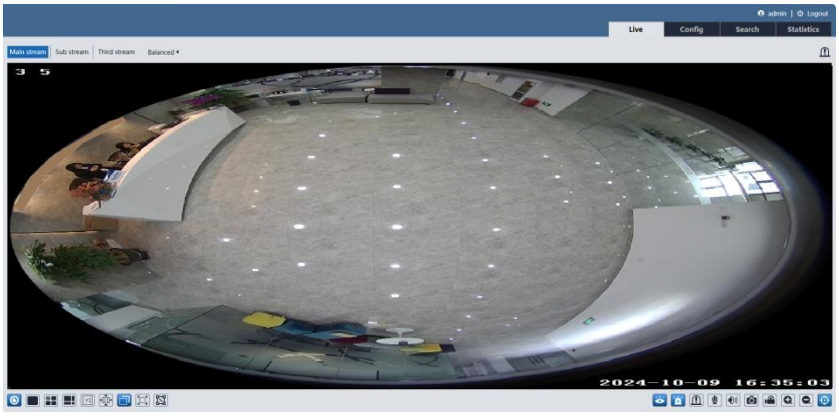


If you forget the admin password, you can reset the password by clicking Forget Password on the login page. Then you can reset the password by the security questions and answers you set.
You can set the account security question during the activation, or you can go to Config> Security> User, click Safety Question, select the security questions and input your answers.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

4 Live View

After logging in, the following window will be shown. Before you view the live image, please set the stream mode and installation method as needed (see Configuring Fisheye Parameters for details).



In the live mode, the different streams and live view modes can be switched as needed. Different stream types will be shown for different view modes.
The following table is the instructions of the icons on the live view interface.

Icon	Description	Icon	Description
	Select live preview mode		Zoom in
	Fisheye view mode		Zoom out
	Panoramic view mode		PTZ control
	Fisheye+ 3PTZ view mode		Rule information display
	4PTZ/4PTZ Fusion view mode		Sensor alarm indicator icon
	Original size		Alarm output indicator icon
	Appropriate size		Audio exception indicator icon (sudden increase)
	Auto		Audio exception indicator icon (sudden decrease)
	Full screen		Audio alarm indicator
	Measure Tool		Motion alarm indicator icon
	Start/stop live view		SD card recording indicator
	Enable/disable alarm status display		Line crossing indicator
	Enable/disable alarm output		Region intrusion indicator
	Start/stop two-way audio		Region entrance indicator
	Enable/disable audio		Region exiting indicator
	Snap		Target counting (by line) indicator

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Icon	Description	Icon	Description
	Start/stop recording		Heat map indicator

*Measure Tool: get the height and width pixel of the selected region in the live view interface. (This function is only available for main stream under fisheye/panoramic view mode). Click  and drag the mouse on the image to draw a desired box. The width and height pixel will directly display in the box.
*Those smart alarm indicators will flash only when the camera supports those functions and the corresponding events are enabled.
*After clicking the audio alarm icon, the sound warning will be triggered according to the set warning times (you can set the warning times by clicking ***Config→Alarm→Audio Alarm***). Click this icon again. After the current warning voice is completely sounded, it will stop.
*Plug-in free live view: the local recording is not supported and the preview mode switch (real-time/balanced/fluent mode) is not available too.
In full screen mode, double click on the mouse to exit or press the ESC key on the keyboard.

Fisheye view mode: See the picture as shown above.
Panoramic view mode

Fisheye+ 3PTZ view mode

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Panoramic + 3PTZ view mode

4PTZ view mode (you need to switch the stream mode in the fisheye parameter interface)

4PTZ fusion view mode: you can view an entire picture formed by 4 small windows. Each small window cannot be controlled by PTZ panel.
In panoramic + 3PTZ view mode or fisheye + 3PTZ view mode or 4PTZ view mode, select a PTZ window and view the image from every direction by controlling PTZ panel.

Click  to display the control panel. The descriptions of the control panel are as follows:

Icon	Description	Icon	Description
	Move upper left direction		Move upper right direction
	Move up		Stop movement
	Move left		Move right
	Move lower left direction		Move lower right direction
	Move down		Speed adjustment

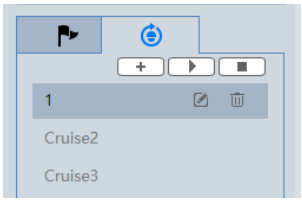
Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

	Zoom out		Zoom in
	Automatic cruise		Preset
	Create and call cruise		

Select and set the preset and then click to save the preset. After position of the set, select it the preset is and click to call the preset. Select the set preset and click to delete it.

To create a cruise:

1. Click as shown below.



2. Click to create a cruise. In the cruise creation window, enter the cruise name and then click “Add preset”.
3. In the preset adding window, select the preset name and time. Click “OK” to add this preset. After the presets are added to the cruise, click “OK” to save the settings.

Select the cruise and then click to start cruise. Click to stop cruise.

The added cruise also can be modified and deleted by clicking or .

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

5 Network Camera Configuration

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

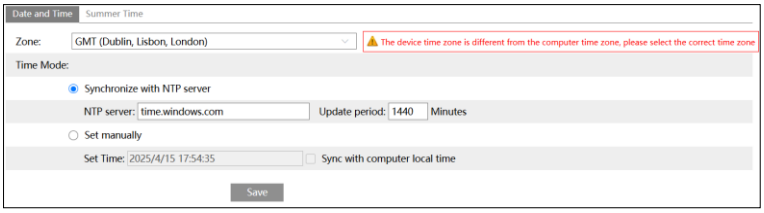
5.1 System Configuration

5.1.1 Basic Information

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

5.1.2 Date and Time

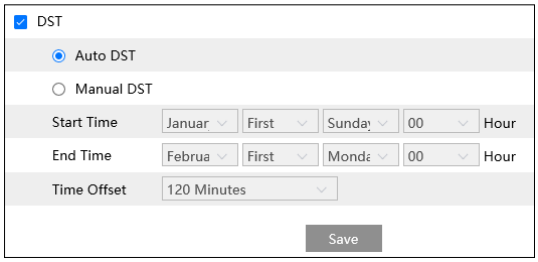
Go to ***Config→System→Date and Time***. Please refer to the following interface.



Select the time zone and time mode as needed.
Note: The time zone of the camera and the computer must be the same. It is recommended to modify the time zone of the camera according to the time zone of the computer. If the time zone of the computer is modified, the current web client needs to be closed. Then re-open it and log in again.

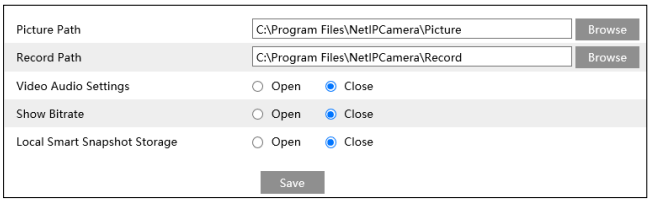
Time Mode:
NTP: Specify an NTP server to synchronize the time.
Manual: Set the system time manually or you can synchronize the time with the time of the local computer.
Click the “Summer Time” tab to set DST (Daylight Saving Time) as needed.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands



5.1.3 Local Config

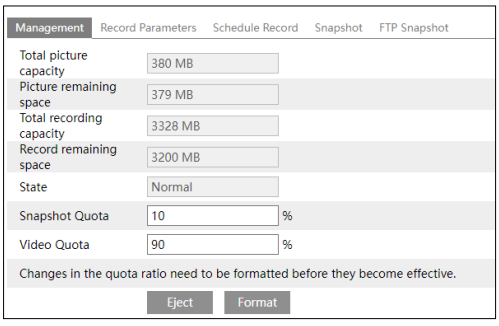
Go to ***Config→System→Local Config*** to set up the storage path of captured pictures and recorded videos on the local PC. There is also an option to enable or disable audio in the recorded files.



Show Bitrate: enable or disable bitrate display on the live video.
Additionally, “Local smart snapshot storage” can be enabled or disabled here. If enabled, the captured pictures triggered by smart events will be saved to the local PC.
Note: when you access your camera by the web browser without the plug-in, only Show Bitrate can be set in the above interface.

5.1.4 Storage

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



- **SD Card Management**

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

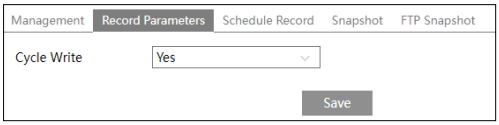
Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Click the “Eject” button to stop writing data to the SD card. Then the SD card can be ejected safely.
Snapshot Quota: Set the capacity proportion of captured pictures on the SD card.
Video Quota: Set the capacity proportion of record files on the SD card.

Note: This series of products support ANR (Automatic Network Replenishment) function.
The offline video recorded files can be searched in the search interface.
1. When the network of the camera is disconnected (for example, the network cable is unplugged), the camera will automatically trigger record and store the recorded files to the SD card.
2. After the IPC is added to the NVR supporting ANR function and the ANR function of the IPC is enabled in the NVR, the IPC will automatically trigger record and store the recorded files to the SD card when the network between the NVR and the IPC is disconnected. After resuming connection, the IPC will automatically upload the recorded files during the offline period to the NVR.

- **Configuring Record Parameters**

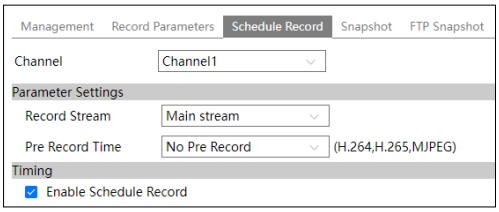
Go to ***Config→System→Storage→Record Parameters***.



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

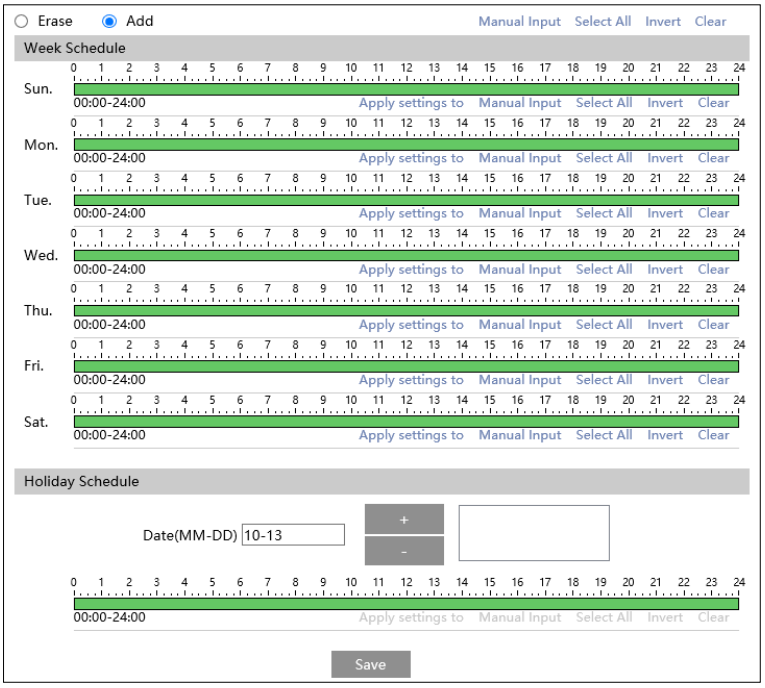
- **Schedule Recording Settings**

Go to ***Config→System→Storage→Schedule Record*** to go to the interface as shown below.
You can set the record stream, pre-record time, and schedule recording for different channels.



Pre-Record Time: Set the time to record before the actual recording begins.
Schedule Record: Check “Enable Schedule Record” and set the schedule.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands



Weekly schedule

Set the alarm time from Monday to Sunday for a single week. Each day is divided into one-hour increments. Green means scheduled. Blank means unscheduled.
“Add”: Add the schedule for a special day. Drag the mouse to set the time on the timeline.
“Erase”: Delete the schedule. Drag the mouse to erase the time on the timeline.
Manual Input: Click it for a specific day to enter specific start and end times. This adds more granularities (minutes).

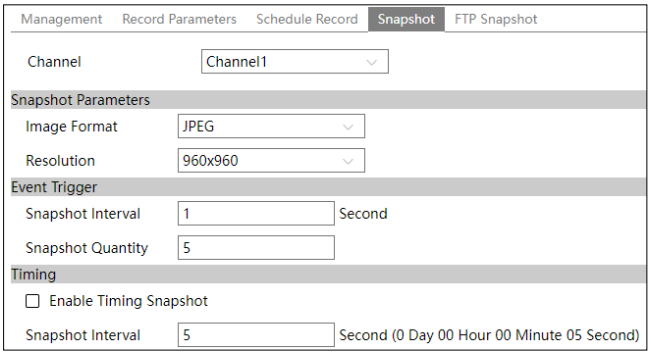
Day schedule

Set the alarm time for a special day, such as a holiday.
Note: Holiday schedule takes priority over weekly schedule.

- **Snapshot Settings**

Go to ***Config→System→Storage→Snapshot*** to go to the interface as shown below.
Set the format, resolution and quality of the image saved on the SD card and the snapshot interval and quantity and the timing snapshot for different channels.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

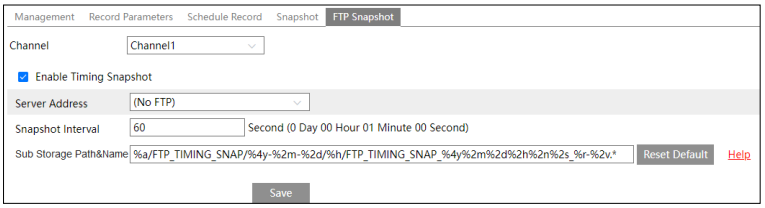


Snapshot Quantity: The number you set here is the maximum quantity of snapshots. The actual quantity of snapshots may be less than this number. Supposing the occurrence time of an alarm event is less than the time of capturing pictures, the actual quantity of snapshots is less than the set quantity of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

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

- **FTP Snapshot**

You can set the FTP snapshot for different channels. Select the desired channel and enable timing snapshot. If enabled, the system will upload snapshots to the FTP server according to the set snapshot interval.



Server Address: select the set FTP server. See FTP section for the FTP server setting.
Sub Storage Path& Name: Click “Help” to view the rule and then set it as needed.
Meanings of the default Path & Name Settings:
“%a/FTP_TIMING_SNAP/%4y-%2m-%2d/%h” stands for sub storage path
“FTP_TIMING_SNAP_%4y%2m%2d%2h%2n%2s_%r-%2v.* ” stands for file name
The entire default value means that a jpg file named “FTP_TIMING SNAP _Year Month Day Hour Minute Second_Random number_Channel number” will be generated under FTP root directory> MAC address>FTP_TIMING SNAP>Year-Month-Day>Hour
“FTP_TIMING SNAP” refers to the event type. You can modify the event name as needed (for example: FTP Snapshot).
If the sub storage path and name box is empty, the snapshot will be uploaded and named according to the default settings.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

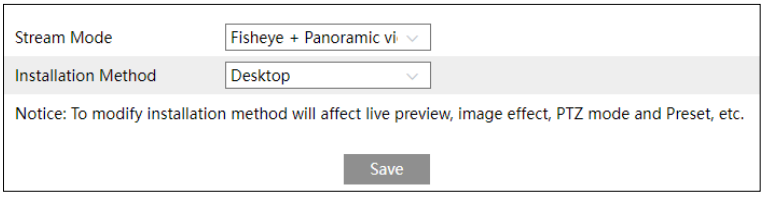
If you only enter the file name rule, the snapshot will be uploaded to the root directory of the FTP server.

5.1.5 Serial Port Settings

You can use RS485 to transmit the data between the camera and the computer or terminal. Before using this function, please connect the camera and computer or terminal with RS485 cable. Please set the parameters of RS485 as needed. Note that you should keep the parameters of the camera and the computer or terminal all the same.

5.1.6 Configuring Fisheye Parameters

Before viewing the live image, please go to ***Config→System→Fisheye Parameters*** to set the stream mode and installation method.



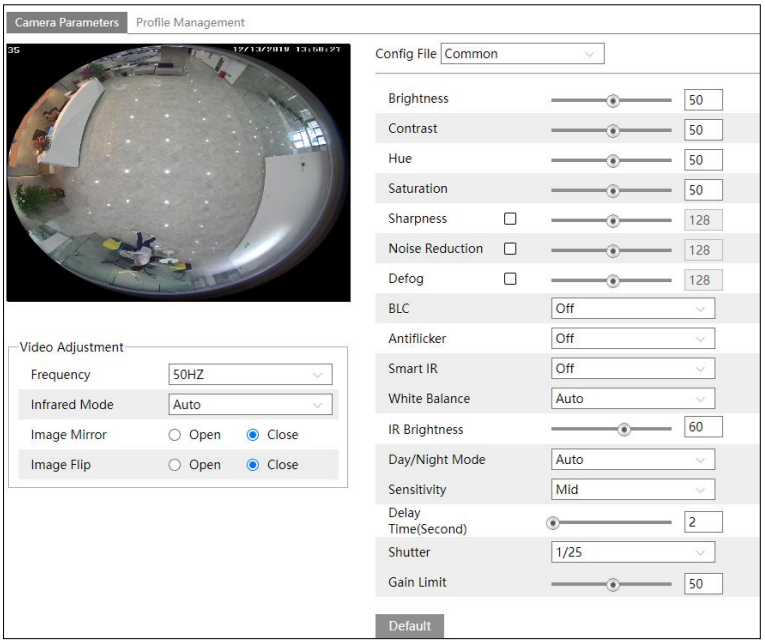
Stream mode: “Fisheye”, “Panoramic View”, “Fisheye + Panoramic view + 3PTZ”, “Fisheye + 4PTZ” or “Fisheye + 4PTZ Fusion” mode are optional.
Installation method: wall, ceiling and desktop are optional. Please select the installation mode according to the actual way of installation.

5.2 Image Configuration

5.2.1 Display Configuration

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

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands



Brightness: Set the brightness level of the camera's image.
Contrast: Set the color difference between the brightest and darkest parts.
Hue: Set the total color degree of the image.
Saturation: Set the degree of color purity. The purer the color, the brighter the image is.
Sharpness: Set the resolution level of the image plane and the sharpness level of the image edge.
Noise Reduction: Decrease the noise and make the image more thorough. Increasing the value will make the noise reduction effect better but it will reduce the image resolution.
Defog: Activating this function and setting an appropriate value as needed in foggy, dusty, smoggy, or rainy environments to get clear images.
Backlight Compensation (BLC):

- Off: disables the backlight compensation function. It is the default mode.
- HWDR: WDR can adjust the camera to provide a better image when there are both very bright and very dark areas simultaneously in the field of view by lowering the brightness of the bright area and increasing the brightness of the dark area.

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

- HLC: lowers the brightness of the entire image by suppressing the brightness of the image's bright area and reducing the size of the halo area.
- BLC: If enabled, the auto exposure will activate according to the scene so that the object of the image in the darkest area will be seen clearly.

Antiflicker:

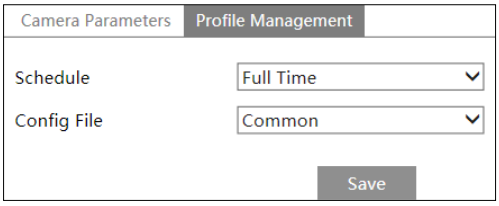
- Off: disables the anti-flicker function. This is used mostly in outdoor installations.
- 50Hz: reduces flicker in 50Hz lighting conditions.
- 60Hz: reduces flicker in 60Hz lighting conditions.

Smart IR: Choose "ON" or "OFF". This function can effectively avoid image overexposure to make the image more realistic. The higher the level is, the more overexposure compensation will be given.

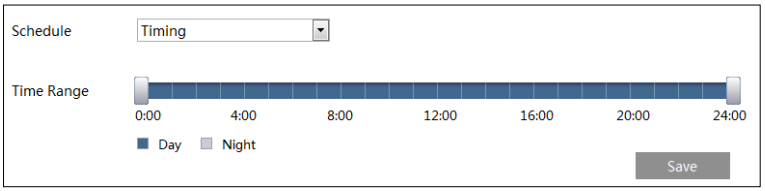
Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

White Balance: Adjust the color temperature according to the environment automatically.
IR Brightness: The value ranges from 1 to 100. Please set it as needed.
Day/Night Mode: Choose “Auto”, “Day”, “Night”, “Alarm input linkage”, or “Timing”.
If “Timing” is selected, you need to set daytime and night time. For example: if “Daytime” is set to “7:00”, the camera will switch to Day mode at 7:00 o’clock; if “Night time” is set to “17:00”, the camera will switch from Day mode to Night mode at 17:00 o’clock.
If “Alarm input linkage” is selected, the system will switch to day or night mode (according to your choice) upon the occurrence of the sensor alarm.
Shutter: Set the upper limit of the effective exposure time. The exposure time will be automatically adjusted (within the set shutter limit value) according to the actual situation.
Gain Limit: Set the upper limit of the gain. The gain value will be automatically adjusted (within the set gain limit value) according to the actual situation.
Frequency: 50Hz and 60Hz can be optional.
Note: If the frequency is switched, the camera will reboot automatically.
Infrared Mode: Choose “Auto”, “ON” or “OFF”.
Image Mirror: Turn the current video image horizontally.
Image Flip: Turn the current video image vertically.

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



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

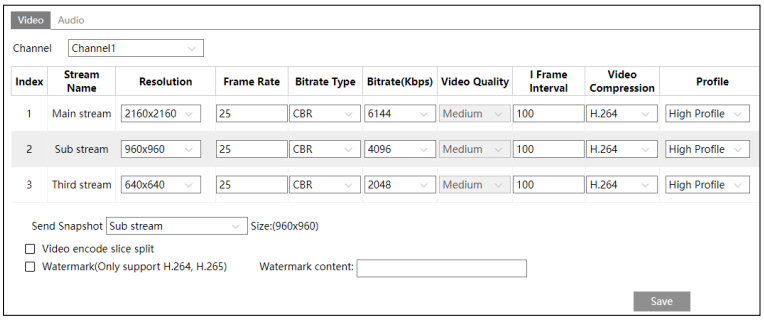


Drag “ ” icons to set the time of day and night. Blue means day time and blank means night time. If the current mode of camera parameters is set to schedule, the image configuration mode will automatically switch between day and night according to the schedule.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

5.2.2 Video / Audio Configuration

Go to ***Image→Video / Audio*** as shown below. In this interface, set the resolution, frame rate, bitrate type, video quality, and so on subject to the actual network condition.
Note: the video stream parameters of different camera series may be different. The following pictures and descriptions are for reference only. The real camera interface shall prevail.

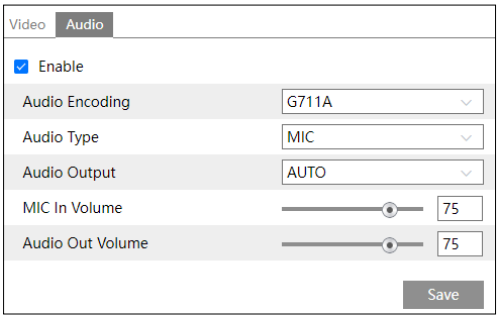


You can select streams for different channels.
For instance, “Fisheye + Panoramic View +3PTZ” mode:
IP Channel 1: Fisheye view channel, 3 streams can be set. Please set them according to the actual network condition.
IP Channel 2: Panoramic view channel, 3 streams can be set. Please set them according to the actual network condition.
IP Channel 3/4/5: PTZ view channel, main stream can be set for each channel. Please set them according to the actual network condition.
Resolution: The size of the image.
Frame rate: The higher the frame rate, the video is smoother.
Bitrate type: CBR and VBR are optional. Bitrate is related to image quality. CBR means that no matter how much change is seen in the video scene, the compression bitrate will be kept constant. VBR means that the compression bitrate will be adjusted according to scene changes. For example, for scenes that do not have much movement, the bitrate will be kept at a lower value. This can help optimize the network bandwidth usage.
Bitrate: it can be adjusted when the mode is set to CBR. The higher the bitrate, the better the image quality will be.
Video Quality: It can be adjusted when the mode is set to VBR. The higher the image quality, the more bitrate will be required.
I Frame interval: It determines how many frames are allowed between “a group of pictures”. When a new scene begins in a video, until that scene ends, the entire group of frames (or pictures) can be considered as a group of pictures. If there is not much movement in the scene, setting the value higher than the frame rate is fine, potentially resulting in less bandwidth usage. However, if the value is set too high, and there is a high frequency of movement in the video, there is a risk of frame skipping.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Video Compression: MJPEG, H264+, H264, H265 or H265+ can be optional. If H.265/H.265+is chosen, make sure the client system is able to decode H.265/H.265+. Compared to H.265, H.265+ saves more storage space with the same maximum bitrate in most scenes. Compared to H.264, H.265 reduces the transmission bitrate under the same resolution, frame rate and image quality.
Profile: For H.264. Baseline, main and high profiles are selectable.
Send Snapshot: Set the snapshot stream.
Video encode slice split: If this function is enabled, a smooth image can be obtained even though using the low-performance PC.
Watermark: When playing back the local recorded video in the search interface, the watermark can be displayed. To enable it, check the watermark box and enter the watermark text.

Click the “Audio” tab to go to the interface as shown below.
Only the models with the built-in MIC support this function.

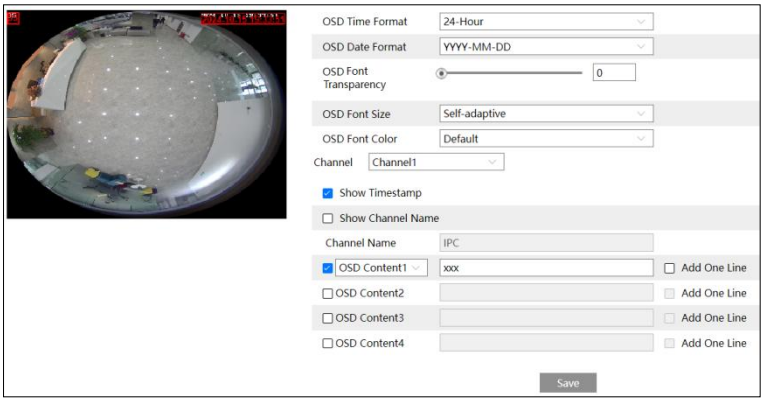


Audio Encoding: G711A and G711U are selectable.
Audio Type: MIC or LIN. (If the internal MIC is used, choose “MIC”. If you want to use an external line-level audio input device, choose “LIN”.)
Audio Output: Talkback, warning or auto can be optional. If “Talkback” is selected, the audio output will be used for two-way audio. If “Warning” is selected, the audio output will be used to play the pre-defined audio alarm. If “Auto” is selected, the system will output sound for two-way audio or warning voice as needed. But when it is warning and two-way audio is being enabled simultaneously, two-way audio will be output first.
LIN IN/MIC IN/Audio Out Volume: Set it as needed.

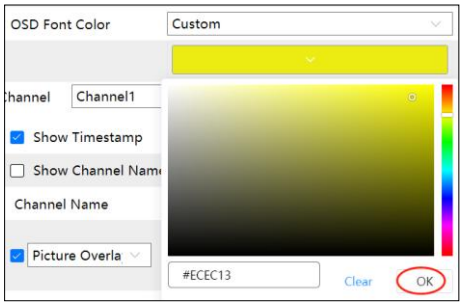
5.2.3 OSD Configuration

Go to ***Image→OSD***.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands



Set time format, date format, OSD content and OSD font transparency/size/color here. After enabling the corresponding display and entering the content, drag them to change their position. Then click the “Save” button to save the settings.
OSD Font Size: When the image resolution is less than 720P, the OSD font size will be automatically changed to 16*16, and will not follow the change of the font size you have set.
OSD Font Color: You can use the default OSD font color (white) or customize the OSD font color as needed.
To customize the font size color:
1. Select “Custom” and then click on the blank box under it.
2. Select a color on the colorful bar (right).
3. Click on the left color box to choose the desired color. Or you can directly enter the hexadecimal color code to set the color.
4. Click “OK” to save the OSD font color settings.



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

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

5.2.4 Video Mask

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

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

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

5.2.5 ROI Configuration

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

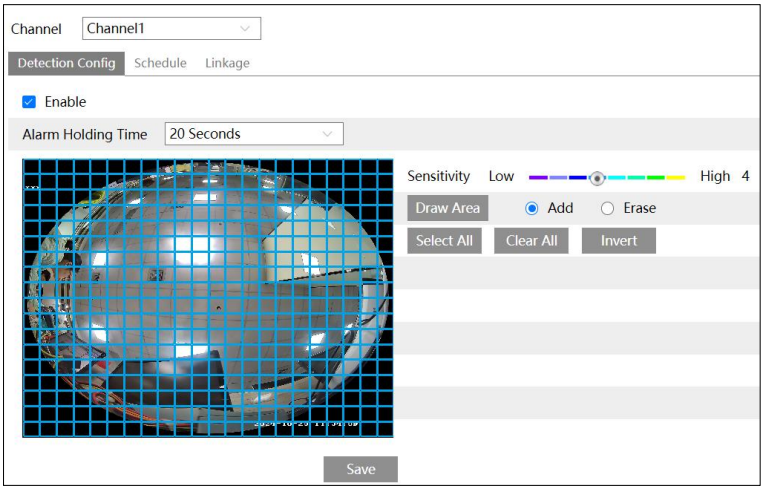
Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

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

5.3 Alarm Configuration

5.3.1 Motion Detection

Motion Detection: when a moving object appears in the detection area and the percentage of the moving area exceeds the configured sensitivity level, an alarm will be triggered.
Go to ***Alarm→Motion Detection*** to set the motion detection alarm.
Note: The default channel varies by different stream modes and installation methods



Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

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

Alarm Holding Time: it refers to the time that the alarm extends after an alarm ends. For instance, if the alarm holding time is set to 20 seconds, once the camera detects a motion, it will go to alarm and would not detect any other motion in 20 seconds. If there is another motion detected during this period, it will be considered as continuous movement; otherwise it will be considered as a single motion.

2. Set motion detection area and sensitivity.

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

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

You can set different sensitivity levels for different areas.

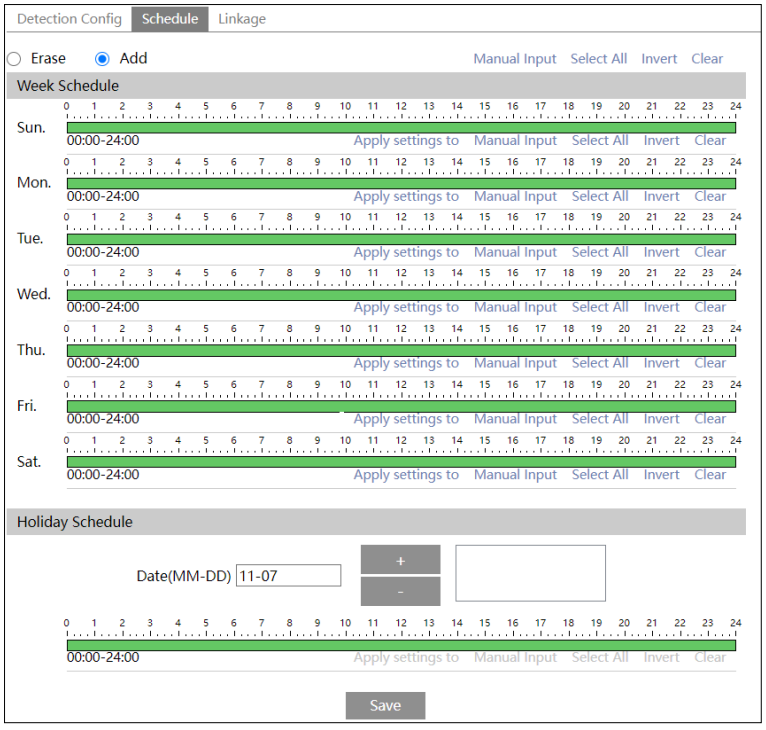
After that, click the “Save” to save the settings.

Note:

a) The area without colored grids means the sensitivity value is 0, which will be considered as a blocked area.

b) After detecting a moving object in the area covered with grid lines, an alarm will be triggered when the number of the red grid lines exceeds the threshold of the sensitivity level.

3. Set the schedule for motion detection.



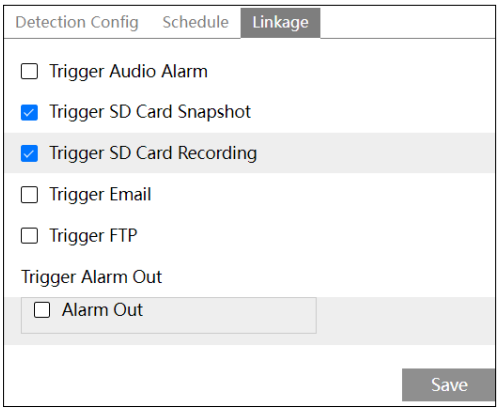
Weekly schedule

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Set the alarm time from Monday to Sunday for a single week. Each day is divided into one -hour increments. Green means scheduled. Blank means unscheduled.
“Add”: Add the schedule for a special day. Drag the mouse to set the time on the timeline.
“Erase”: Delete the schedule. Drag the mouse to erase the time on the timeline.
Manual Input: Click it for a specific day to enter specific start and end times. This adds more granularities (minutes).

Day schedule
Set the alarm time for a special day, such as a holiday.
Note: Holiday schedule takes priority over weekly schedule.

4. Click “Linkage” to configure the alarm linkage items.



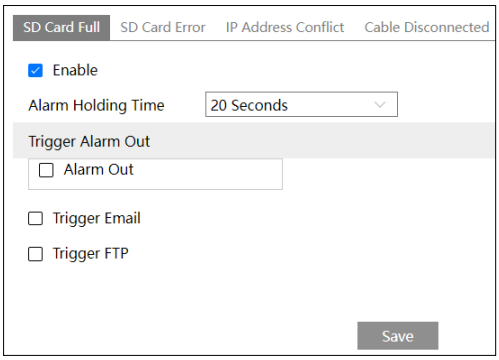
Trigger Audio Alarm: If selected, the warning voice will be played on detecting a motion based alarm. After checking it, you need to select the voice file as needed. If “Default” is selected, the voice file is the voice set in the audio alarm interface (see Audio Alarm for details). If “Specified” is selected, you can specify the warning voice and language for the motion alarm.
Trigger SD Card Snapshot: If selected, the system will capture images on motion detection and save the images on an SD card.
Trigger SD Card Recording: If selected, the video will be recorded on an SD card on motion detection.
Trigger Email: If “Trigger Email” and “Attach Picture” are checked (email address must be set first in the Email configuration interface), the captured pictures and triggered event will be those addresses.
Trigger FTP: If “Trigger FTP” and “Attach Picture” are checked, the captured pictures will be sent to the FTP server address. You can set the sub storage path and name as needed. Please refer to the FTP configuration for more details.
Alarm Out: If selected, this would trigger an external relay output that is connected to the camera on detecting a motion based alarm.
After that, click “Save” to save the settings.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

5.3.2 Exception Alarm

- **SD Card Full**

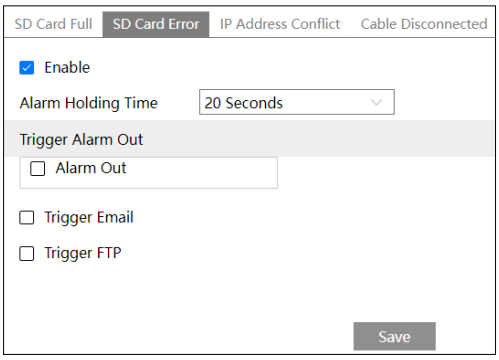
1. Go to ***Config→Alarm→Exception Alarm→SD Card Full***.



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

- **SD Card Error**

When there are some errors in writing to the SD card, the corresponding alarms will be triggered.
1. Go to ***Config→Alarm→ Exception Alarm →SD Card Error*** as shown below.

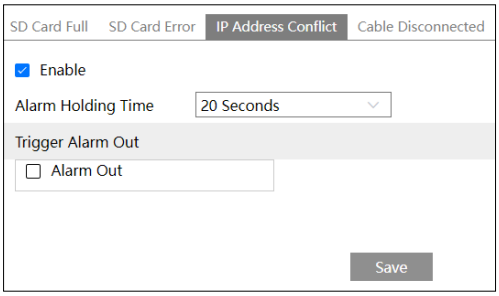


2. Click “Enable”.
3. Set the alarm holding time and alarm trigger options. Trigger alarm out, Email and FTP. The setup steps are the same as motion detection. Please refer to motion detection for details.

- **IP Address Conflict**

This function is only available for the models with Alarm Out interface.
1. Go to ***Config→Alarm→ Exception Alarm →IP Address Conflict*** as shown below.

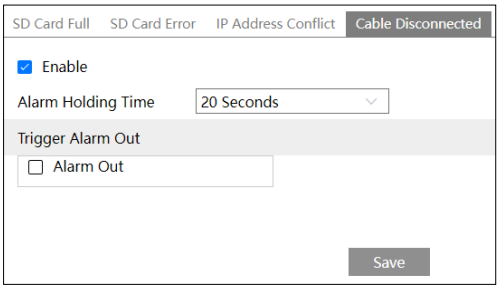
Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands



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

- **Cable Disconnection**

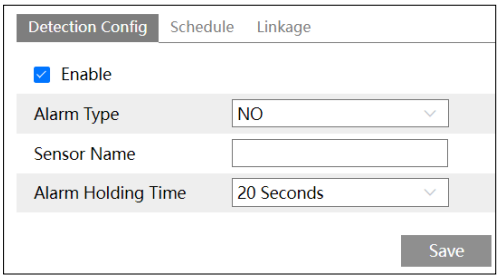
This function is only available for the models with Alarm Out interface.
1. Go to ***Config→Alarm→ Exception Alarm →Cable Disconnected*** as shown below.



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

5.3.3 Alarm In

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

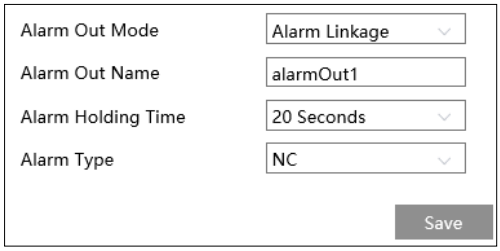


Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

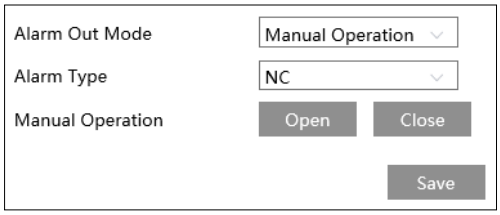
1. Click “Enable” and set the alarm type, alarm holding time and sensor name.
2. Set the schedule of the sensor alarm. The setup steps of the schedule are the same as the schedule recording setup. (See Schedule Recording).
3. Set alarm trigger options. The setup steps are the same as motion detection.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

5.3.4 Alarm Out

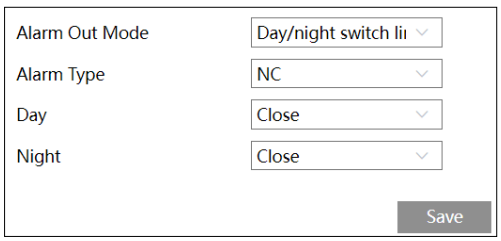
Go to ***Config→Alarm→Alarm Out***.



Alarm Out Mode: Alarm linkage, manual operation, day/night switch linkage and timing are optional.
Alarm Linkage: Having selected this mode, select alarm out name, alarm holding time at the “Alarm Holding Time” pull down list box and alarm type.
Manual Operation: Having selected this mode, select the alarm type and click “Open” to trigger the alarm out immediately; click “Close” to stop alarm.

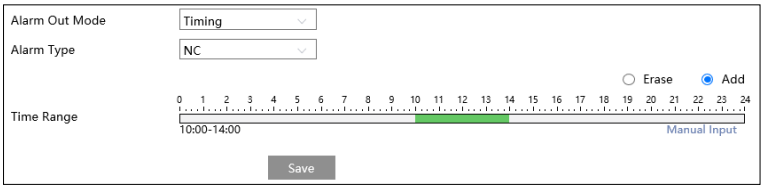


Day/Night Switch Linkage: Having selected this mode, select the alarm type and then choose to open or close alarm out when the camera switches to day mode or night mode.



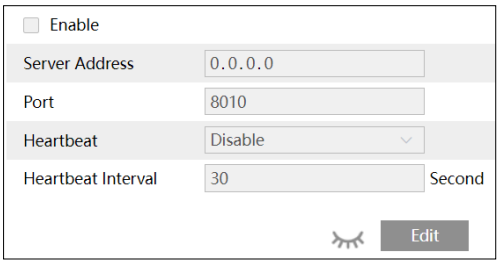
Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

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



5.3.5 Alarm Server

Go to ***Alarm→Alarm Server*** as shown below.



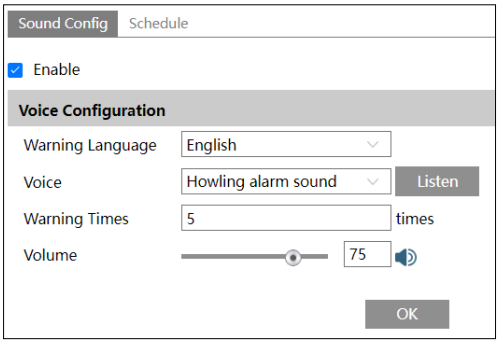
Click “Edit” and check “Enable” to set the alarm server.
Set the server address, port, heartbeat and heartbeat interval. When an alarm occurs, the camera will transfer the alarm event to the alarm server. If an alarm server is not needed, there is no need to configure this section.

Click to view the entire server address; click to hide a part of sensitive data.

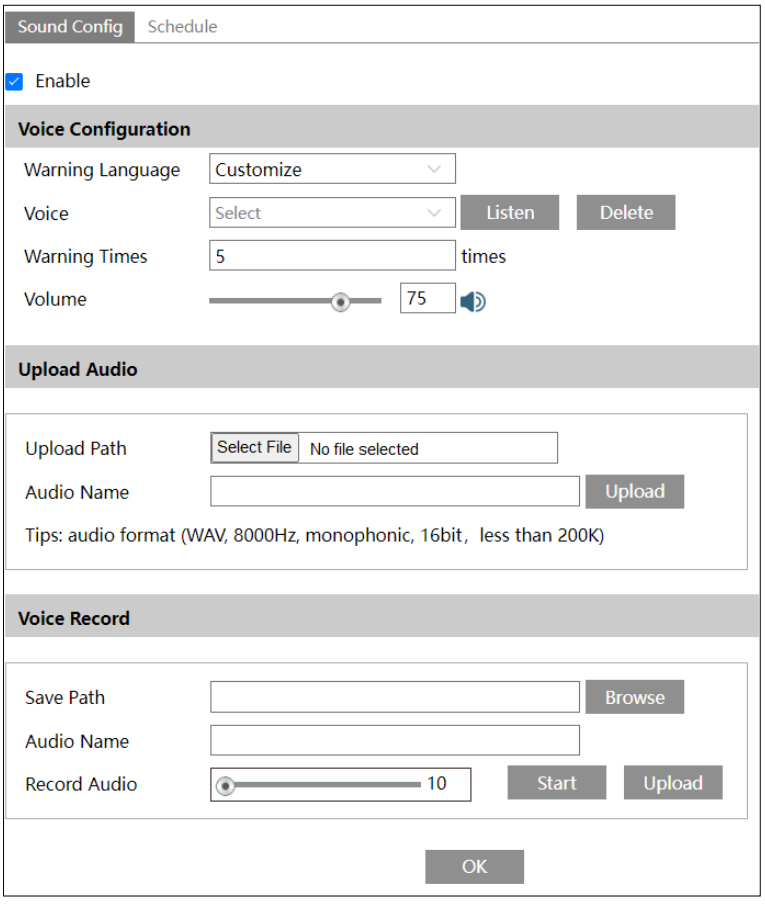
5.3.6 Audio Alarm

Go to ***Alarm→Audio Alarm*** as shown below.
Enable audio alarm. If disabled, the camera will not play the desired warning voice even if an event triggers audio alarm. Additionally, you need to enable audio in the audio configuration interface and the audio output type should be “Warning” or “Auto”, or the warning voice cannot play too.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands



① Select the warning voice. If you want to customize the voice, you can choose “Customize”. Click “Select File” or “Browse” to choose the audio file you want to upload and then enter the audio name. Finally, click “Upload” to upload the audio file. Note that the format of the audio file must meet the requirement (see Tips), or it will not be uploaded. After you upload the audio file, you can select the audio name from the audio list and click “Listen” to listen to it. Click “Delete” to delete the audio.



You can also record your own voice in the above interface and then upload.

- Insert the microphone into your PC.
- Click “Browse” to choose the save path of the audio you want to record.

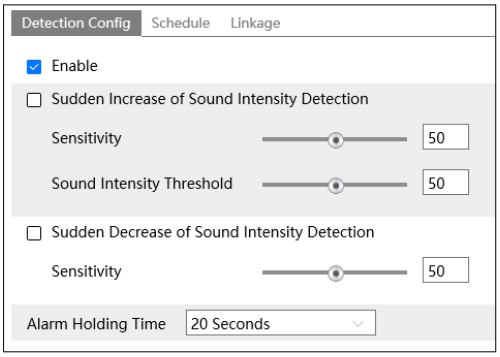
- Set the record audio volume and then click “Start” to start recording your voice.
- Click “Upload” to upload your customized voice.

Note: when you access your camera by the web browser without the plug-in, “video record” is not available in the above interface.

② Select the voice and then set the warning times and volume as needed.
Warning times: it ranges from 1 to 50.
③ Set the schedule of audio alarm. The setup steps of the schedule are the same as the schedule recording setup. (See Schedule Recording).
④ Click “OK” to save the settings.

5.3.7 Audio Exception

Alarms will be triggered when the abnormal sound is detected in the surveillance scene, such as the sudden increase/decrease of the sound intensity.
To set audio exception detection:
1. Go to ***Alarm→Audio Exception*** as shown below.

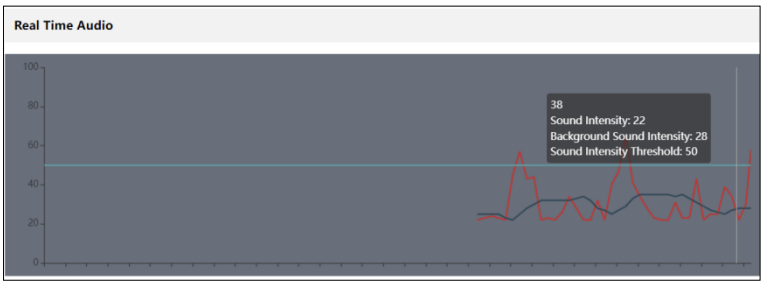


2. Enable audio exception.
3. Select the audio exception detection types.

Sudden Increase of Sound Intensity Detection: Detect sudden increase of sound intensity. If enabled, sensitivity and sound intensity threshold are configurable. Alarms will be triggered when the detected sound intensity exceeds the sound threshold.
Sensitivity: The higher the value is, the easier the alarm will be triggered.
Sound Intensity Threshold: It is the sound intensity reference for the detection. The lower the value is, the easier the alarm will be triggered. It is recommended to set the average sound intensity in the environment. The louder the environment sounds, the higher the value should be. Please adjust it according to the actual environmental condition.
Sudden Decrease of Sound Intensity Detection: Detect sudden decrease of sound intensity. Please set the sensitivity as needed. The higher the value is, the easier the alarm will be triggered.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Real-time audio graphic:
Red wavy line stands for the current detected sound intensity.
Navy blue line stands for the environment (background) sound intensity.
Green line stands for the sound intensity threshold.
In order to reduce false alarms, it is recommended to set the sensitivity and sound intensity threshold according to the real-time audio graphic.

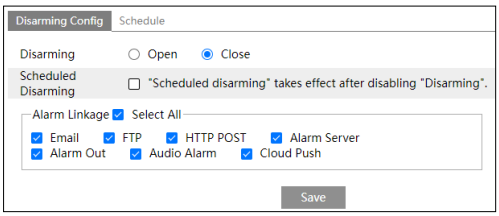


4. Set the alarm holding time and click “Save” to save the settings.
5. Set the schedule of audio exception detection. The setup steps of the schedule are the same as the schedule recording (See Schedule Recording).
6. Click “Linkage” to configure the alarm linkage items. The setup steps are the same as motion detection. Please refer to Motion Detection for details.

Note: The alarm recording type triggered by an audio exception event is “Common”. In the search interface, you can search the recorded files of audio exception by selecting the “Common” event.

5.3.8 Disarming

You can disarm alarm linkage actions quickly in this interface.



Disarming: The system stops triggering alarm linkage actions immediately.
Scheduled Disarming: The system stops triggering alarm linkage actions in the selected period. Click “Schedule” to set the schedule. The setup steps of the schedule are the same as the motion detection schedule settings (See Motion Detection for details).

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Note: After “Disarming” or “Scheduled Disarming” is enabled, the reported general alarms (the alarm start time and end time of alarm out and audio alarm) will probably not match the actual situation. You need to handle it manually.

5.4 Event Configuration

For more accuracy, here are some recommendations for installation.

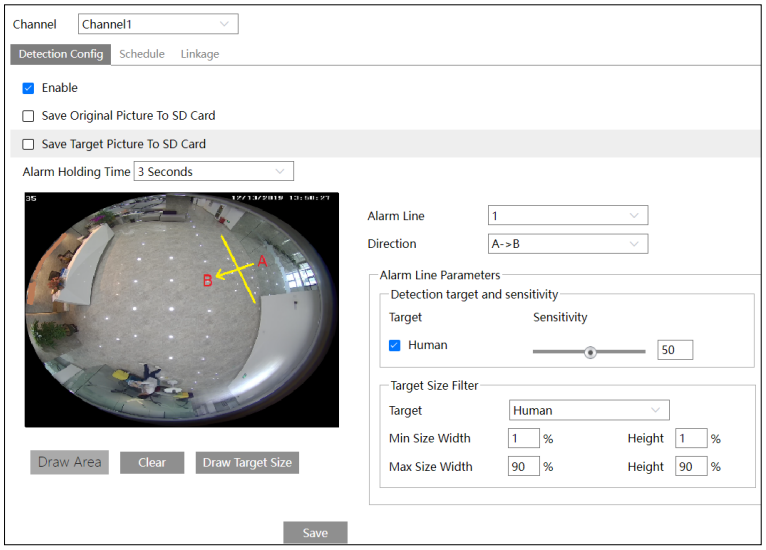
- Cameras should be installed on stable surfaces, as vibrations can affect the accuracy of detection.
- Avoid pointing the camera at the reflective surfaces (like shiny floors, mirrors, glass, lake surfaces and so on).
- Avoid places that are narrow or have too much shadowing.
- Avoid scenario where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

Note: Events may vary by different installation methods and stream modes. Go to ***Config→System→Fisheye Parameters*** to set the stream mode and installation method.
* When the installation method is set to “Wall” or “Desktop” and the stream mode is set to “Panoramic View” or “Fisheye + Panoramic view +3 PTZ”, line crossing, region intrusion, region entrance, region exiting and target counting by line (human/motor vehicle/ non-motor vehicle classification) are supported.
* When the installation method is set to “Ceiling” and the stream mode is set to any one of the stream modes except “Panoramic view”, line crossing, region intrusion, region entrance, region exiting, target counting by line and heat map (only human) are supported.
*You can enable multiple smart detection events (such as line crossing detection, region intrusion detection, region exiting detection, etc.) simultaneously, but detecting multiple smart events in the same time will cause the reduction in performance and affect the detection results. Please enable smart events according to the actual performance of your camera.

5.4.1 Line Crossing

Line Crossing: Alarms will be triggered if the target crosses the pre-defined alarm lines.
Go to ***Config→Event→Line Crossing*** as shown below.
Note: The default channel and image display vary by different stream modes and installation methods. The following picture is for reference only.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands



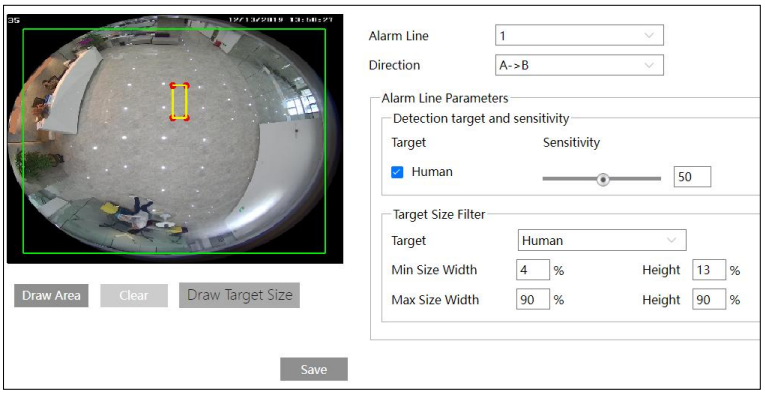
1. Enable line crossing detection and select the snapshot type.
Save Original Picture to SD Card: If it is enabled, the detected original pictures will be captured and saved to the SD card when the targets cross the alarm line.
Save Target Picture to SD Card: If it is enabled, the detected target cutout pictures will be captured and saved to the SD card when the targets cross the alarm line.
Note: To save snapshots to the local PC, please enable “Local Smart Snapshot Storage” in the local config interface first. To save snapshots to the SD card, please install an SD card first.
2. Set the alarm holding time.
3. Set alarm lines, detection target, and target size filter for line crossing detection.
Set the alarm line number and direction. Four lines can be added. Multiple lines cannot be added simultaneously.
Direction: A<->B, A->B and A<-B optional. This indicates the direction of the intruder who crosses over the alarm line that would trigger the alarm.
A<->B: The alarm will be triggered when the intruder crosses over the alarm line from B to A or from A to B.
A->B: The alarm will be triggered when the intruder crosses over the alarm line from A to B.
A<-B: The alarm will be triggered when the intruder crosses over the alarm line from B to A.
Click the “Draw Area” button and then drag the mouse to draw a line in the image. Click the “Stop Draw” button to stop drawing. Click the “Clear” button to delete the lines. Click the “Save” button to save the settings.
Note: If the set rule line is very close to the edge of the screen, it may be difficult for the target to trigger the alarm. Please make sure that there is at least one full target-sized space between the rule line and the edge of the screen.

Detection Target:
Note: When the installation method is set to “Ceiling”, only “Human” can be selected.
Human: Select it and then alarms will be triggered if someone crosses the pre-defined alarm lines.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Motor Vehicle: Select it and then alarms will be triggered if a vehicle with four or more wheels (eg. a car, bus or truck) crosses the pre-defined alarm lines.
Non-motor Vehicle: Select it and then alarms will be triggered if a vehicle with two wheels (eg. a motorcycle or bicycle) crosses the pre-defined alarm lines.
All of the three types of objects can be selected simultaneously. Please select the detection objects as needed. If no object/target is selected, alarms will not be triggered even if line crossing detection is enabled.
Sensitivity: The higher the value is, the easier the alarm will be triggered.

To set target size filter:
Click “Draw Target Size” to draw the maximum and minimum size of a specific target as shown below.



Target: choose “Human”, “Motor Vehicle” or “Motorcycle/Bicycle” as needed.
Green box is the maximum target detection box; yellow box is the minimum target detection box. Click the green box to edit the maximum target detection box; click the yellow box to edit the minimum target detection box.
Drag one of four corners of the green or yellow box to change the box size. The corresponding size value on the right will be changed too. You can also enter the digital number to directly change the box size.
Click and drag the green or yellow box to move its position.
Finally, click “Save” to save the settings.
After the target size range is set, only the target whose size is between the minimum value and the maximum value can be detected.

4. Set the schedule of the line crossing alarm. The setup steps of the schedule are the same as the motion detection schedule settings (See Motion Detection for details).
5. Click “Linkage” to configure the alarm linkage items. The setup steps are the same as motion detection. Please refer to Motion Detection for details.
6. In the live view interface, click “Panoramic view” (desktop or wall mounting mode) or “Fisheye” (ceiling mounting mode) to view line crossing detection.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

※ Configuration requirements of the camera and surrounding area

1. Avoid the scenes with many trees or the scenes with various light changes (like many flashing headlights). The ambient brightness of the scenes shouldn't be too low.
example).
2. The recommended target recognition size:

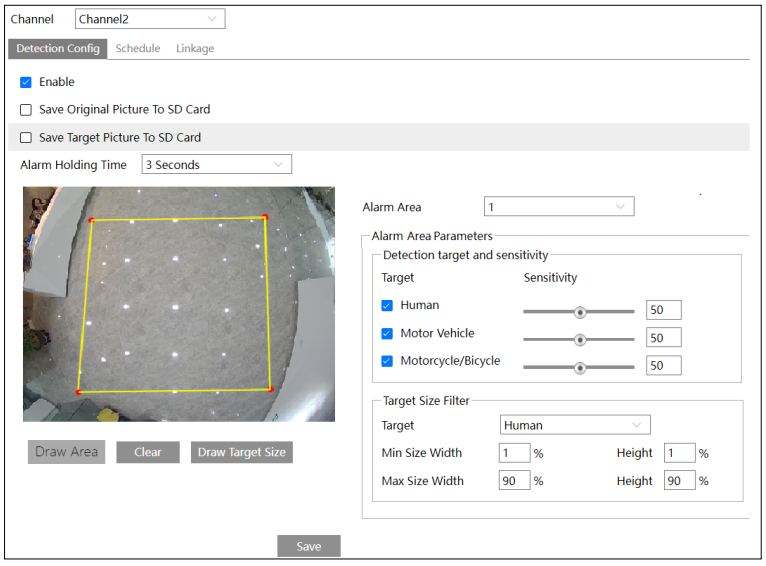
Percentage	Human	Motor Vehicle	Motorcycle/Bicycle
Minimum (Width × Height)	4% × 8%	8% × 8%	4% × 4%
Maximum (Width × Height)	50%× 50%	50%× 50%	50%× 50%

Note: The percentage means that a target occupies the percentage of the entire image. For example: In a 1080P(1920×1080) video image, the minimum resolution of human is 80×160 (w =1920x4%=80, h=1920x8%=160)

3. Make sure cameras can view objects for at least 2 seconds in the detected area for accurate detection.
4. Adequate light and clear scenery are crucial for line crossing detection.
6. Please adjust the installation position or focus to meet the requirements of the target recognition size.

5.4.2 Region Intrusion

Region Intrusion: Alarms will be triggered if the target intrudes into the pre-defined areas. This function can be applicable to important supervision places, danger areas and prohibited areas, like military administrative zones, high danger areas, no man's areas, etc.
Go to ***Config→Event→Region Intrusion***.
Note: The image display may be different due to different installation modes. The following picture is for reference only.



Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

1. Enable region intrusion detection and select the snapshot type.
Save Original Picture to SD Card: If it is enabled, the detected original pictures will be captured and saved to the SD card when the target intrudes into the pre-defined areas.
Save Target Picture to SD Card: If it is enabled, the detected target cutout pictures will be captured and saved to the SD card when the target intrudes into the pre-defined areas.
Note: To save snapshots to the local PC, please enable “Local Smart Snapshot Storage” in the local config interface first. To save snapshots to the SD card, please install an SD card first.
2. Set the alarm holding time.
3. Set alarm areas, detection target, and target size filter for region intrusion detection.
Set the alarm area number. Four alarm areas can be added.
Click the “Draw Area” button and then click around the area where you want to set as the alarm area in the image (the alarm area should be a closed area). Click the “Stop Draw” button to stop drawing. Click the “Clear” button to delete the alarm area. Click the “Save” button to save the settings.
Note: If the set rule line is very close to the edge of the screen, it may be difficult for the target to trigger the alarm. Please make sure that there is at least one full target-sized space between the rule line and the edge of the screen.

Detection Target:
Note: When the installation method is set to “Ceiling”, only “Human” can be selected.
Human: Select it and then alarms will be triggered if someone intrudes into the pre-defined area.
Motor Vehicle: Select it and then alarms will be triggered if a vehicle with four or more wheels (eg. a car, bus, or truck) intrudes into the pre-defined area.
Motorcycle/Bicycle: Select it and then alarms will be triggered if a vehicle with two wheels (eg. a motorcycle or bicycle) intrudes into the pre-defined area.
All of the three types of objects can be selected simultaneously. Please select the detection objects as needed. If no object/target is selected, alarms will not be triggered even if intrusion detection is enabled.

Target size filter setup: The setup steps of the target size filter are the same as the line crossing target size filter setup (See Line Crossing for details).
4. Click the “Save” button to save the settings.
5. Set the schedule of the region intrusion detection. The setup steps of the schedule are the same as the motion detection schedule settings (See Motion Detection for details).
6. Click “Linkage” to configure the alarm linkage items. The setup steps are the same as motion detection. Please refer to Motion Detection for details.
7. In the live view interface, click “Panoramic view” (desktop or wall mounting mode) or “Fisheye” (ceiling mounting mode) to view region intrusion detection.

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

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

5.4.3 Region Entrance

Region Entrance: Alarms will be triggered if the target enters the pre-defined areas.
Go to ***Config→Event→Region Entrance*** interface.
1. Enable region entrance detection and select the snapshot type and the detection target.
2. Set the alarm holding time.
3. Set alarm areas and target size filter for region entrance detection.
4. Set the schedule of region entrance detection.
5. Set the alarm linkage items.

The setup steps of the region entrance detection are the same as the region intrusion detection setup (See Region Intrusion for details).

5.4.4 Region Exiting

Region Exiting: Alarms will be triggered if the target exits from the pre-defined areas.
Go to ***Config→Event→Region Exiting*** interface.
1. Enable region exiting detection and select the snapshot type and the detection target.
2. Set the alarm holding time.
3. Set alarm areas and target size filter for region exiting detection.
4. Set the schedule of region exiting detection.
5. Set the alarm linkage items.

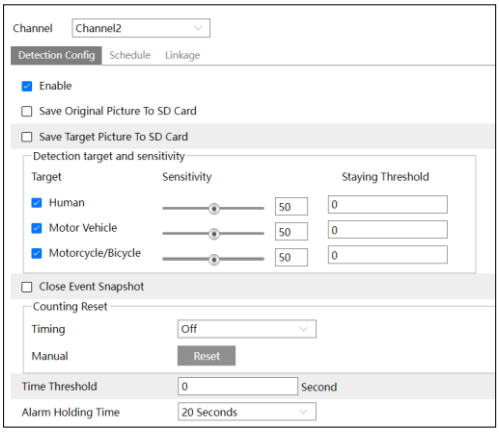
The setup steps of the region exiting detection are the same as the region intrusion detection setup (See Region Intrusion for details).

5.4.5 Target Counting by Line

This function is used to detect, track and count the number of people or vehicles crossing the set alarm line.

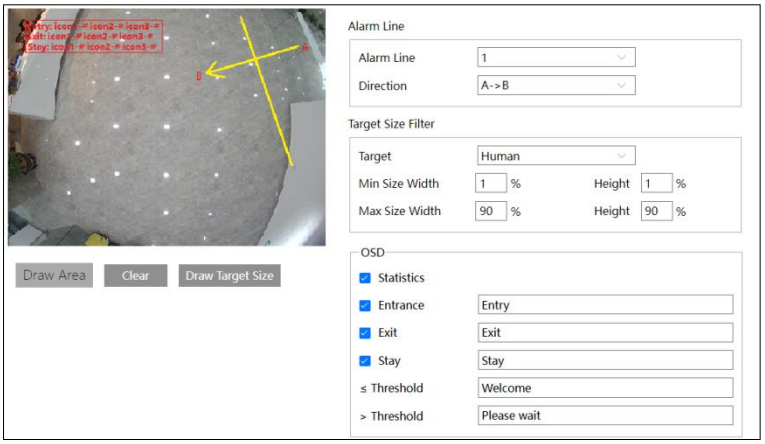
1. Go to ***Config→Event→Target Counting by Line*** as shown below.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands



2. Enable target counting by line and select the snapshot type and the detection target.
Detection Target: Select the target to calculate. Human, motor vehicle and motorcycle/bicycle can be selected.
Note: When the installation method is set to “Ceiling”, only “Human” can be selected.
Staying Threshold: When the targets (human/vehicle) staying in the specified area exceed the threshold, alarms will be triggered.
Close Event Snapshot: if enabled, the captured pictures based on target counting by line will be neither saved to an SD card/local PC nor pushed to the NVR/APP/platform/….
Counting Reset: The current number of the target counting can be reset. You can choose to reset the counting daily, weekly or monthly. Click “Reset” to manually reset the current number of crossing line people/motor vehicle/non-motor vehicle counting.
Time Threshold: The duration time that the number of targets exceeds the staying threshold. Alarms will not be triggered even if the targets staying in the specified area exceed the threshold within the set delay alarm duration. But if you set it to “0”, alarms will be triggered immediately when the targets staying in the specified area exceed the threshold.
3. Set the alarm holding time.
Alarm Holding Time: it is the time that the alarm extends after an alarm ends.
4. Set alarm lines and target size filter.
Note: The image display may be different due to different installation modes. The following picture is for reference only.

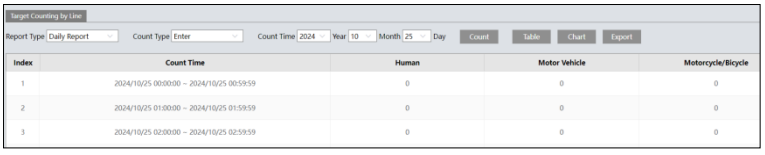
Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands



Set the alarm line number and direction. Only one alarm line can be added.
Direction：A->B and A<-B can be optional. The direction of the arrow is entrance.
Click the “Draw Area” button and then drag the mouse to draw a line in the image. Click the “Clear” button to delete the lines.
Note: If the set rule line is very close to the edge of the screen, it may be difficult for the target to trigger the alarm. Please make sure that there is at least one full target-sized space between the rule line and the edge of the screen.

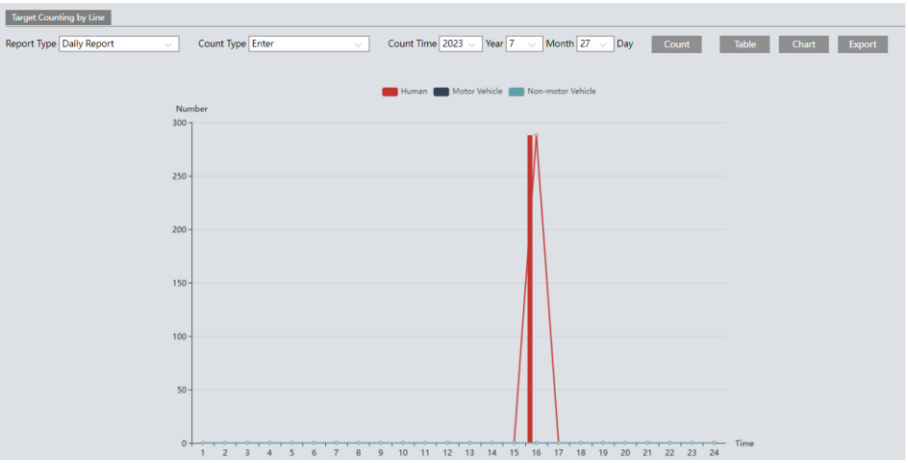
Target size filter setup: The setup steps of the target size filter are the same as the line crossing target size filter setup (See Line Crossing for details).
Statistics: If enabled, you can see the statistical information in the live view interface. If disabled, the statistical information will not be displayed in the live view interface.
Check “Statistics” and then move the red box to change the position of the statistical information displayed on the screen.
The statistical OSD information can be customized as needed.
Click the “Save” button to save the settings.

5. Set the schedule of the target counting by line. The setup steps of the schedule are the same as the motion detection schedule settings (See Motion Detection for details).
6. Click “Linkage” to configure the alarm linkage items. The setup steps are the same as motion detection. Please refer to Motion Detection for details.
7. View the statistical information in the live view interface by clicking “Panoramic view” (desktop or wall mounting mode) or “Fisheye” (ceiling mounting mode).
8. View the statistical information of target counting by line. Click “Statistics” to enter the following interface.



Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Select the report type. Daily report, weekly report, monthly report and annual report are selectable.
Select the count type. Enter or leave can be optional.
Select the start time and then click “Count”. Then the counting result will be displayed in the statistic result area. Click Table or Chart to display the result in different way.



※ Configuration requirements of the camera and surrounding area

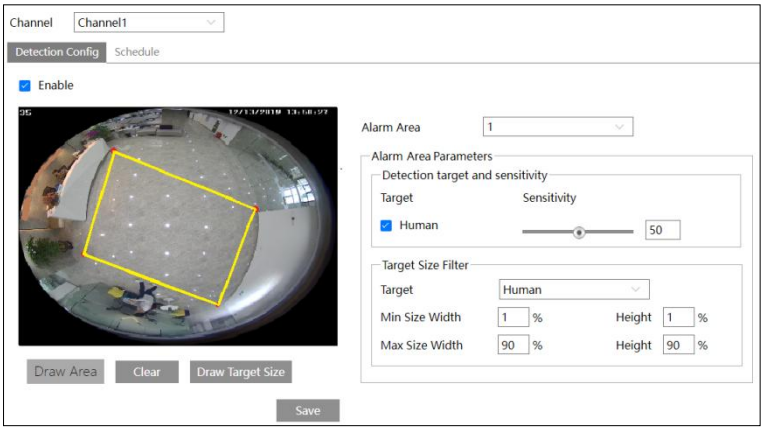
The requirements are similar to line crossing detection. Please refer to Configuration requirements of the camera and surrounding area of line crossing detection for details.

5.4.6 Heat Map

Heat Map is to display the flow distribution of people in pre-defined areas by different colors.
Note: Heat Map is only available when the following three conditions are met: a. the installation method is set to “Ceiling”; b. the stream mode is set to the mode that has the “Fisheye” view (“Fisheye”, “Fisheye + Panoramic view + 3 PTZ”, “Fisheye + 4 PTZ”, or “Fisheye + 4 PTZ Fusion”); c. an SD card is installed.

1. Enable heat map, set snapshot type and detection target type as needed.
2. Set heat map display area and target size filter. Up to 4 areas can be set.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

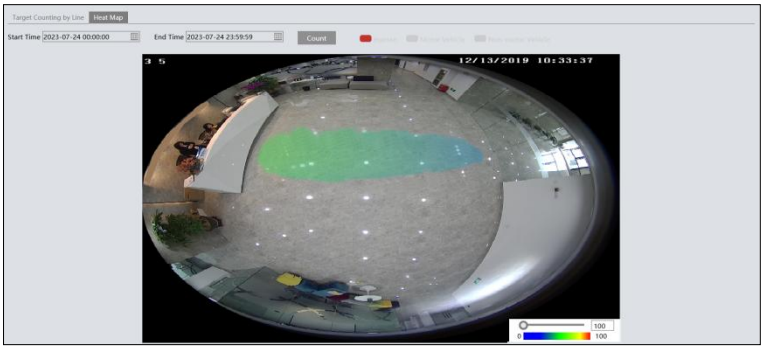


Click the “Draw Area” button and then click around the area where you want to set as the alarm area in the image (the alarm area should be a closed area). Click the “Clear” button to delete the alarm area. Click the “Save” button to save the settings.

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

3. Set the schedule of heat map. The setup steps of the schedule are the same as the motion detection schedule settings (See Motion Detection for details).

4. View the heat map data (click ***Statistics→Heat Map***). Set the start time and the end time. Click “Count” to view the heat map as shown below. The default heat map is people flow data display.

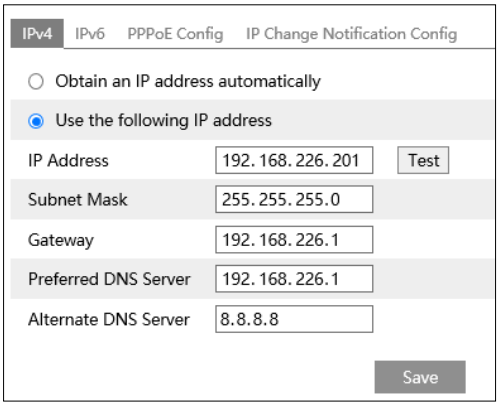


5.5 Network Configuration

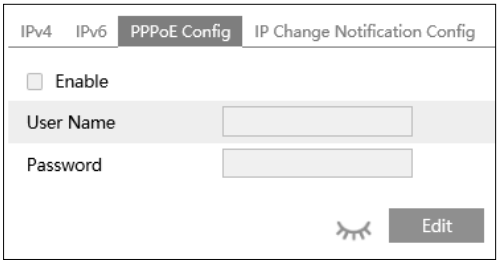
5.5.1 TCP/IP

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

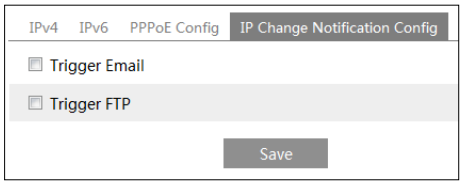
Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands



Use IP address (take IPv4 for example)-There are two options for IP setup: obtain an IP address automatically by DHCP and use the following IP address. Please choose one of the options as needed.
Test: Test the effectiveness of the IP address by clicking this button.
Use PPPoE-Click the “PPPoE Config” tab to go to the interface as shown below. Click “Edit”, enable PPPoE and then enter the user name and password from your ISP.



Either of these two network connection methods can be used. If PPPoE is used to connect internet, the camera will get a dynamic WAN IP address. This IP address will change frequently. To be notified, the IP change notification function can be used.
Click “IP Change Notification Config” to go to the interface as shown below.

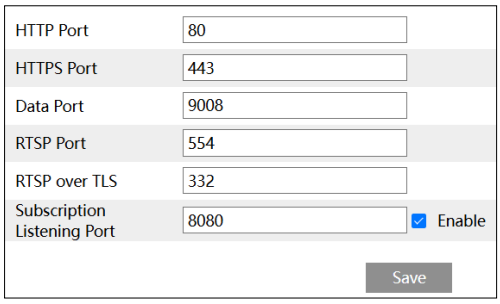


Trigger Email: when the IP address of the device is changed, the new IP address will be sent to the email address that has been set up.
Trigger FTP: when the IP address of the device is changed, the new IP address will be sent to FTP server that has been set up.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

5.5.2 Port

Go to ***Config→Network→Port*** as shown below.



HTTP Port: The default HTTP port is 80. It can be changed to any port which is not occupied.
HTTPS Port: The default HTTPs port is 443. It can be changed to any port which is not occupied.
Data Port: The default data port is 9008. Please change it as necessary.
RTSP Port: The default port is 554. Please change it as necessary.
RTSP over TLS: Supports media stream transmission based on TLS channel encryption protection.
Subscription Listening Port: The port is used for a persistent connection of the third-party platform to push smart data.

5.5.3 Server Configuration

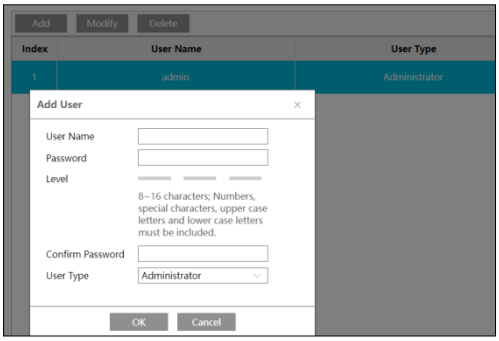
This function is mainly used for connecting network video management system.

1. Click “Edit” and then check “Enable”.
2. Check the IP address and port of the transfer media server in the NVMS. Then enable the auto report in the NVMS when adding a new device. Next, enter the remaining information of the device in the NVMS. After that, the system will automatically allot a device ID. Please check it in the NVMS.
3. Enter the above-mentioned server address, server port and device ID in the corresponding boxes. Click the “Save” button to save the settings. You can show or hide the sensitive data as needed.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

5.5.4 Onvif

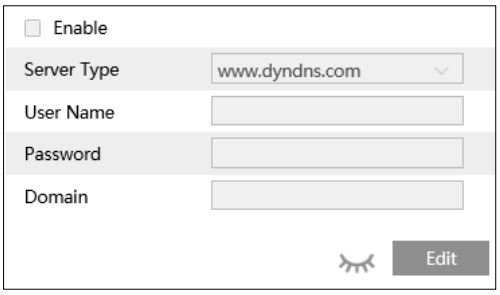
The camera can be searched and connected to the third-party platform via ONVIF/RTSP protocol. If “Match Onvif Password” is enabled in the device activation interface, the password of ONVIF admin user can be modified simultanously. When you connect the camera through the ONVIF protocol in the third-party platform, you can use this onvif user to connect.
You can also modify the password of admin sperately in the following interface and add new users in the Onvif interface.



Note: when adding the device to the third-party platform with ONVIF/RTSP protocol, please use the onvif user in the above interface.

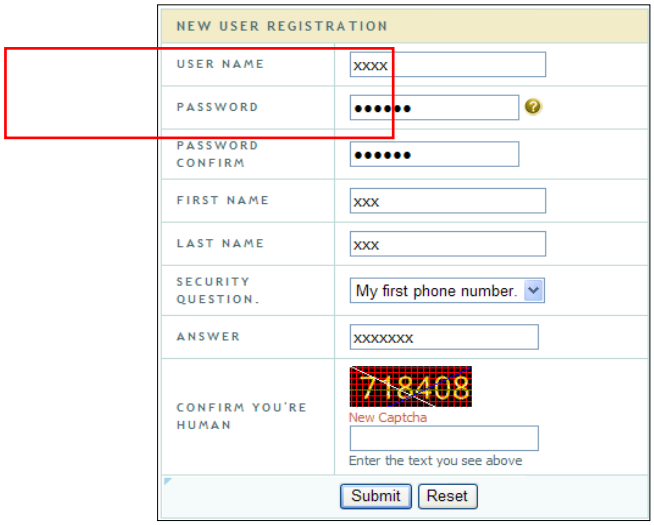
5.5.5 DDNS

If the camera is set up with a DHCP connection, DDNS should be set for the internet.
1. Go to ***Config→Network→ DDNS***.

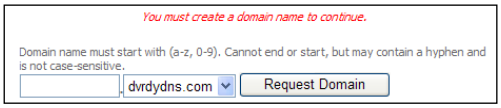


2. Apply for a domain name. Take www.dvrdyndns.com for example.
Enter www.dvrdydns.com in the address bar of a web browser to visit its website. Then Click the “Registration” button.

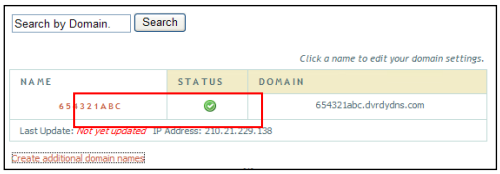
Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands



Create domain name.



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

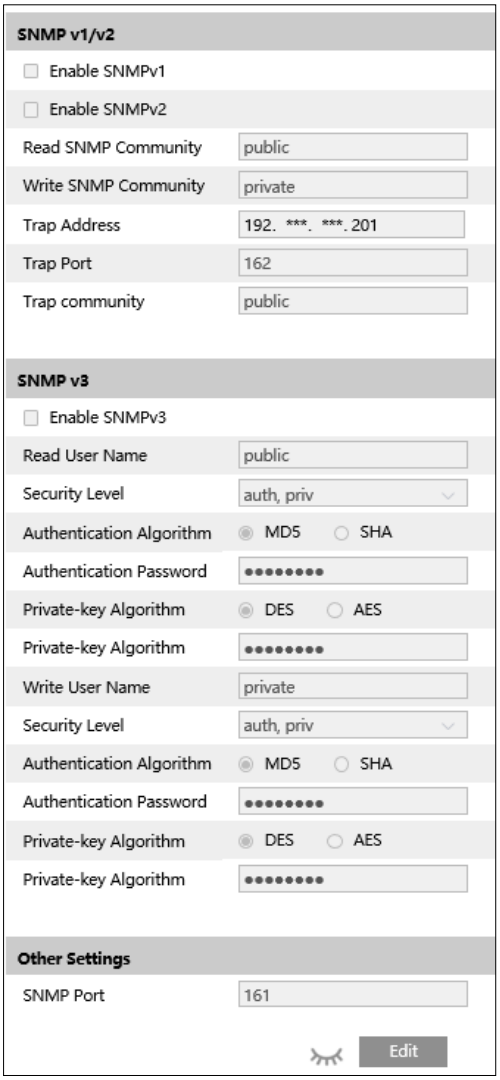


3. Click “Edit” and then enter the username, password, domain you apply for in the DDNS configuration interface.
4. Click the “Save” button to save the settings.

5.5.6 SNMP

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

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

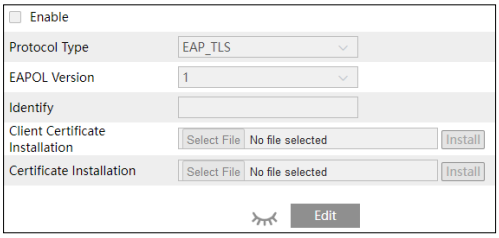


2. Click “Edit” and then check the corresponding version checkbox (Enable SNMPv1, Enable SNMPv2, Enable SNMPv3) according to the version of the SNMP software that will be used.
3. Set the values for “Read SNMP Community”, “Write SNMP Community”, “Trap Address”, “Trap Port” and so on. Please make sure the settings are the same as that of the SNMP software.
Note: Please use the different version in accordance with the security level you required. The higher the version is, the higher the level of the security is.

5.5.7 802.1x

If it is enabled, the camera’s data can be protected. When the camera is connected to the network protected by the IEE802.1x, user authentication is needed.

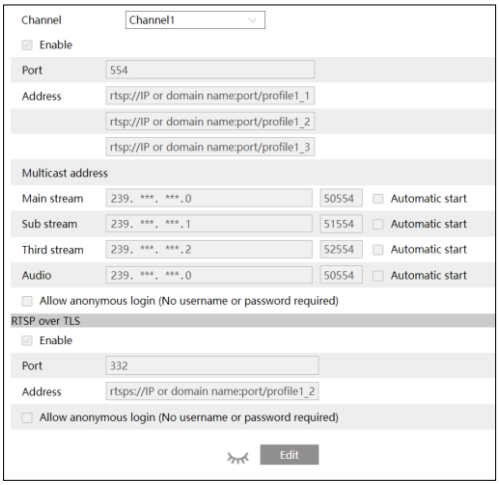
Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands



To use this function, the camera shall be connected to a switch supporting 802.1x protocol. The switch can be regarded as an authentication system to identify the device in a local network. If the camera connected to the network interface of the switch has passed the authentication of the switch, it can be accessed via the local network.
Click “Edit” to start the setup.
Protocol type: Choose “EAP_MD5” or “EAP_TLS” as needed.
Select EAP-TLS as the EAP method. Enter your ID issued by the CA, and then upload related certificate(s). Before connecting the camera to the protected network with 802.1x, apply a digital certificate from a Certificate Authority (i.e., your network administrator) which can be validated by a RADIUS server.
Select EAP_MD5 as the EAP method. You need to enter the username and password.
User name and password: The user name and password must be the same as the user name and password applied for and registered in the authentication server.

5.5.8 RTSP

Go to ***Config→Network→RTSP***.
Select the channel you want set the parameters of RTSP.



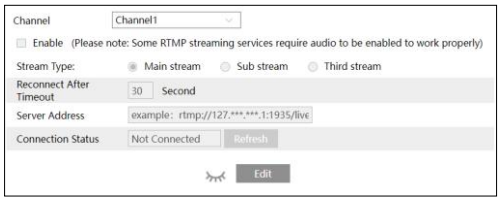
Click “Edit” and then select “Enable” to enable the RTSP function.
Port: Access port of the streaming media. The default number is 554.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

RTSP Address: The RTSP address (unicast) format that can be used to play the stream in a media player.
Multicast Address
Main stream: The address format of Channel 1 is
"rtsp://IP address: rtsp port/profile1_1?transportmode=mcast".
Sub stream: The address format of Channel 1 is
"rtsp://IP address: rtsp port/profile1_2?transportmode=mcast".
Third stream: The address format of Channel 1 is
"rtsp://IP address: rtsp port/profile1_3?transportmode=mcast".
Note: The number of streams varies by different channels.
Audio: Having entered the main/sub stream in a VLC player, the video and audio will play automatically.
If "Allow anonymous login…" is checked, there is no need to enter the username and password to view the video.
If "auto start" is enabled, the multicast received data should be added into a VLC player to play the video.
RTSP over TLS: Enable RTSP stream encryption by using TLS.
Note: 1. The IP address mentioned above cannot be the address of IPv6.
2. Avoid the use of the same multicast address in the same local network.
3. When playing the video through the multicast streams in a VLC player, please pay attention to the mode of the VLC player. If it is set to TCP mode, the video cannot be played.

5.5.9 RTMP

You can access the third-party (like YouTube) to realize video live view through RTMP protocol.
Go to ***Config→Network→RTMP***.

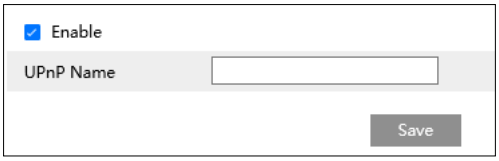


Select the channel, click "Edit" and then check "Enable". Select stream type and set the reconnection time after timeout and server address as needed.
Server address: Enter the server address allocated by the third party server. For example: rtmp://127.0.0.1:1935/live/livestream/0.
After that, click "Save" to save the settings. Then click "Refresh" to view the connection status.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

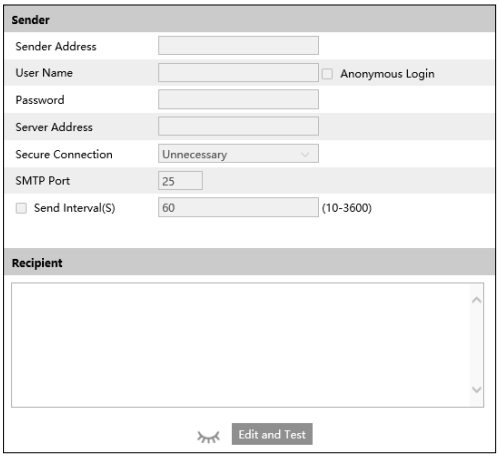
5.5.10 UPNP

If this function is enabled, the camera can be quickly accessed through the LAN.
Go to ***Config→Network→UPnP***. Enable UPNP and then enter UPnP name.



5.5.11 Email

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



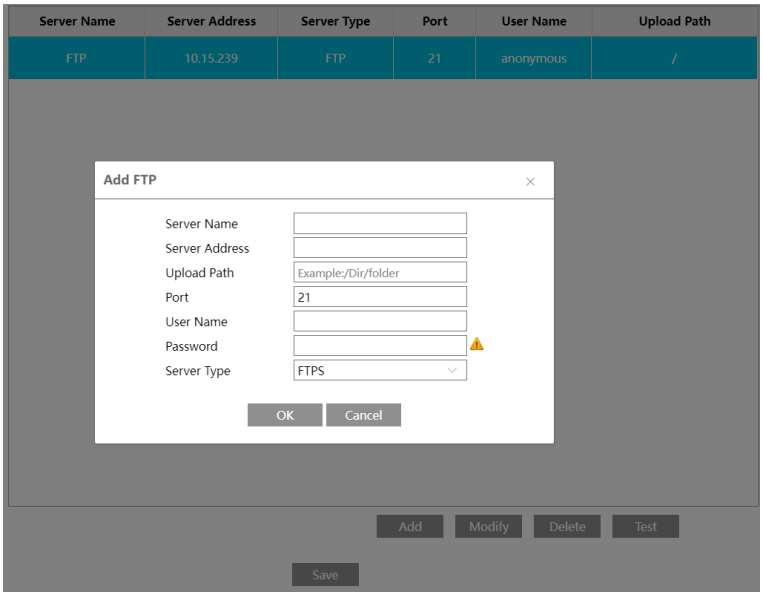
Click “Edit and Test” to set the sender and the recipient.
Sender Address: sender’s e-mail address.
User name and password: sender’s user name and password (you don’t have to enter the username and password if “Anonymous Login” is enabled).
Server Address: The SMTP IP address or host name.
Select the secure connection type at the “Secure Connection” pull-down list according to what’s required.
SMTP Port: The SMTP port.
Send Interval(S): The time interval of sending an email. For example, if it is set to 60 seconds and multiple motion detection alarms are triggered within 60 seconds, they will be considered as only one alarm event and only one email will be sent. If one motion alarm event is triggered and then another motion detection alarm event is triggered after 60 seconds, two emails will be sent. When different alarms are triggered at the same time, multiple emails will be sent separately.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Click the “Test” button to test the connection of the account.
Recipient Address: receiver’s e-mail address.

5.5.12 FTP

After an FTP server is set up, captured pictures from events will be uploaded to the FTP server.
1. Go to ***Config→Network →FTP***.



2. Click “Edit and Test” and then click “Add” to add the information of the FTP. After that, click “Save” to save the settings.
Server Name: The name of the FTP server.
Server Address: The IP address or domain name of the FTP.
Upload Path: The directory where files will be uploaded to.
Port: The port of the FTP server.
User Name and Password: The username and password that are used to login to the FTP server.
Server Type: FTP or FTPS
3. In the event setting interface (like motion detection, region intrusion, line crossing, etc.), trigger FTP as shown below.

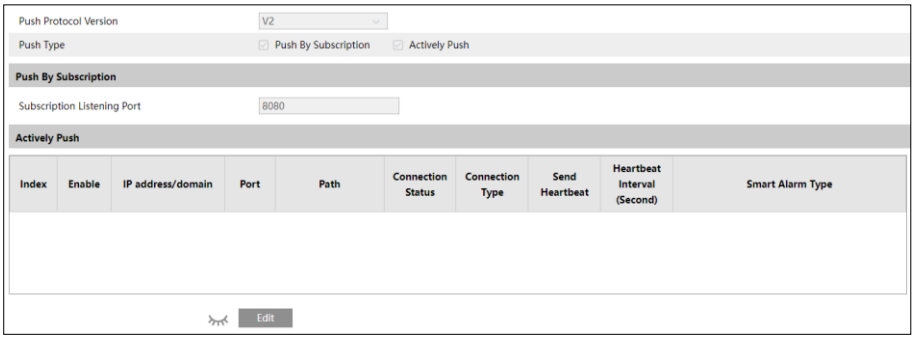
If “Trigger FTP” and “Attach Picture” are checked, the captured pictures will be sent to the FTP server address.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Sub Storage Path& Name: Click “Help” to view the rule and then set it as needed.
Meanings of the default Path & Name Settings (taking motion detection as an example):
“%a/MOTION/%4y-%2m-%2d/%h” stands for sub storage path
“MOTION_%4y-%2m-%2d-%2h-%2n-%2s-%3u-%3i-%2v.* ” stands for file name
When an motion alarm is triggered and “Trigger FTP” and “Attach Picture” are checked, a jpg file named “MOTION_Year Month Day Hour Minute Second_Event number_Channel number” and a txt file named “MOTION_Year Month Day Hour Minute Second_Event number_Channel number” will be generated under FTP root directory> MAC address>MOTION>Year-Month-Day>Hour
“MOTION” refers to the event type. You can modify the event name as needed (for example: Motion). You can also change the display order and contents of the sub storage path and file name.
If the sub storage path and name box is empty, the snapshot will be uploaded and named according to the default settings.
If you only enter the file name rule, the snapshot will be uploaded to the root directory of the FTP server.

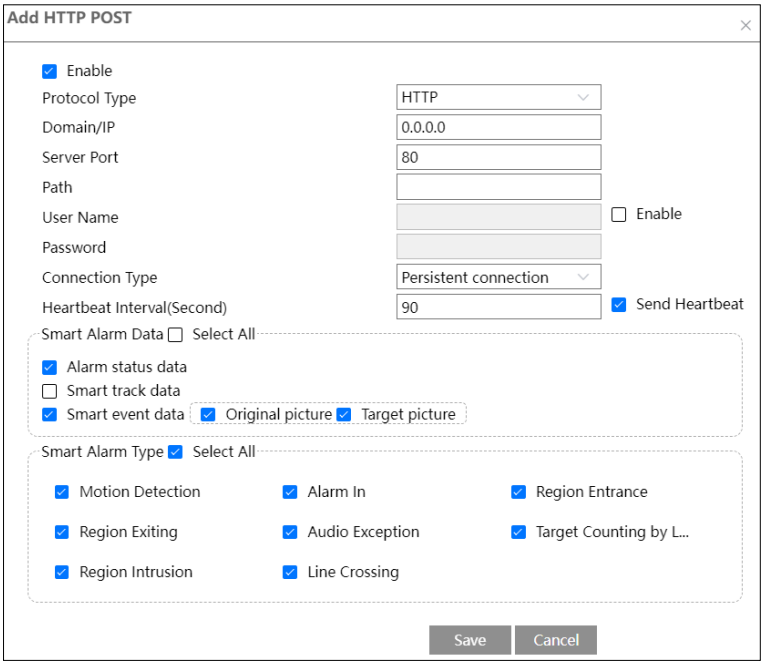
5.5.13 HTTP POST

Go to ***Config→Network →HTTP POST***.



Click “Edit” and then check “Enable”.
Push Protocol Version: Choose “V1” or “V2” as needed. It is recommended to use V2.
Push Type: “Push by Subscription” and/or “Actively Push” can be selected.
Push by Subscription: Push target trajectory (moving coordinate) to API test tool with a persistent connection. If enabled, the system will push the target trajectory upon detecting a target. If disabled, the system will push the target trajectory only when triggering a smart event (such as line crossing detection, region intrusion detection, etc.)
If the subscription listening port is occupied, you can modify it.
Actively Push: Click “Add” to add HTTP POST.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

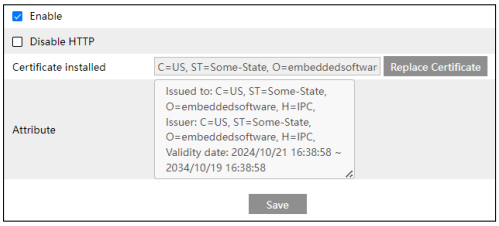


Protocol type: HTTP
Domain/IP: the IP address/domain name of the third-party platform.
Server port: the server port of the third-party platform.
Path: enter the subdomain of the above server, for example, the URL of alarm information push: “/SendAlarmStatus”.
Username and password: Please enable and enter as needed.
Connection Type: Choose persistent connection or short connection as needed.
Enable “Send heartbeat” and set heartbeat interval as needed. Check smart alarm data and type. After the above parameters are set, click “Save” to save the settings. Select one URL and click “Test” to test the connection of the URL. Then the camera will automatically connect to the third-party platform. The online state can be viewed in the above interface. After the camera is successfully connected, it will send the selected alarm data to the third-party platform once the selected smart alarm is triggered.

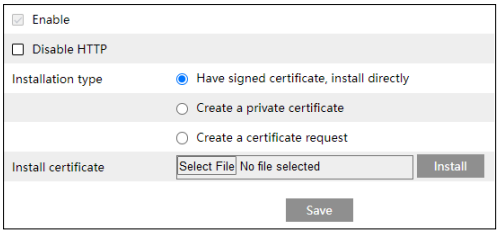
5.5.14 HTTPS

HTTPS provides authentication of the web site and protects user privacy.
Go to ***Config →Network→HTTPS*** as shown below.

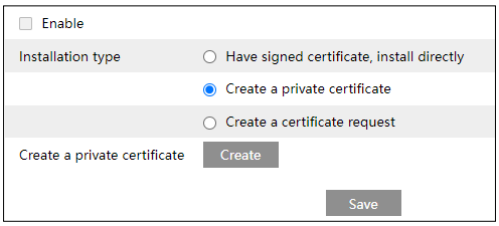
Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands



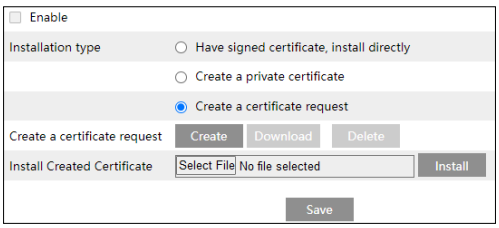
There is a certificate installed by default as shown above. Enable this function and save it. Then the camera can be accessed by entering https://IP: https port via a web browser (eg. https://192.168.226.201:443).
A private certificate can be created if users don't want to use the default one. Click "Replace Certificate" to change a certificate. Then the following interface will be displayed.



* If there is a signed certificate, click "Select File" to select it and then click "Install" to install it.
* Click "Create a private certificate" to enter the following creation interface.



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

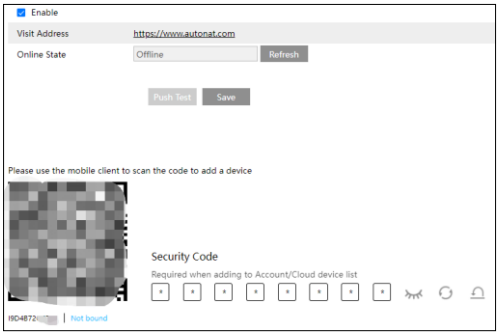


Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

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

5.5.15 Cloud Service

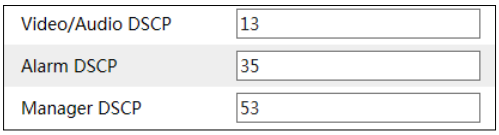
If this function is enabled, the network camera can be quickly accessed by scanning the QR Code and entering the security code in mobile APP via WAN. In addition, you can also enter the visit address in the address bar of a web browser to log in the camera via WAN. Enable this function by going to ***Config→Network→Cloud Service***.



After the device is successfully bound, you can unbind it via APP (go to the server list of the APP and delete the device).
Note that after you bind the camera to your APP account, a verification code will be required when logging onto the web client by using the above-mentioned visit address.

5.5.16 QoS

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



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

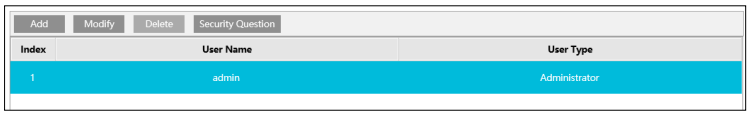
Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

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

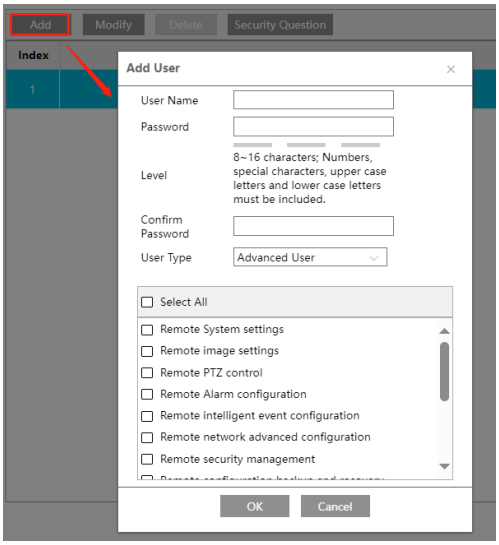
5.6 Security Configuration

5.6.1 User Configuration

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



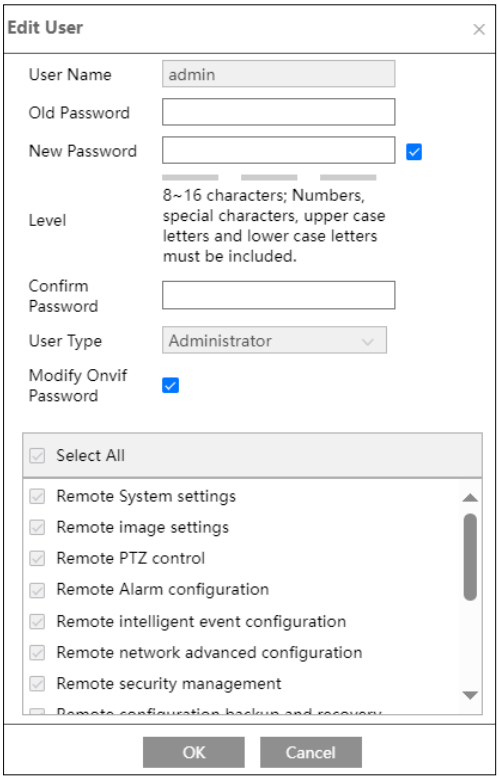
Add user:
1. Click the “Add” button to display the following textbox.



2. Enter user name in the “User Name” textbox.
3. Enter the password in the “Password” and “Confirm Password” textbox. Please set the password according to the requirement of the password security level (Go to ***Config→Security→Security Management→Password Security*** to set the security level).
4. Choose the user type and select the desired user permissions.
5. Click the “OK” button and then the newly added user will be displayed in the user list.

Modify user:
1. Select a user to modify password if necessary in the user configuration list box.
2. The “Edit user” dialog box pops up by clicking the “Modify” button.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands



3. Enter the old password of the user in the “Old Password” text box.
4. Enter the new password in the “New password” and “Confirm Password” text box.
5. Select the user permissions for advanced or normal user.
6. Click the “OK” button to save the settings.

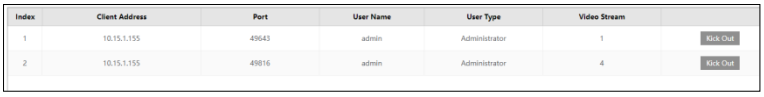
Delete user:
1. Select the user to be deleted in the user configuration list box.
2. Click the “Delete” button to delete the user.

Note: The default administrator account cannot be deleted.

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

5.6.2 Online User

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



In addition, you can also view the number of video streams, IP address, user type, etc.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

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

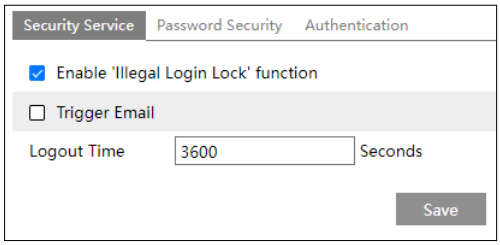
5.6.3 Block and Allow Lists

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

The setup steps are as follows:
Check the “Enable address filtering” check box.
Select “Block/Allow the following address”, IPv4/IPv6 and then enter IP address in the address box and click the “Add” button.

5.6.4 Security Management

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



In order to prevent against malicious password unlocking, “Illegal Login Lock” function can be enabled here. If this function is enabled, login failure after trying five times will make the login interface locked. The camera can be logged in again after a half hour or after the camera reboots. Trigger Email: if enabled, e-mail will be sent when logging in/out or illegal login lock occurs.

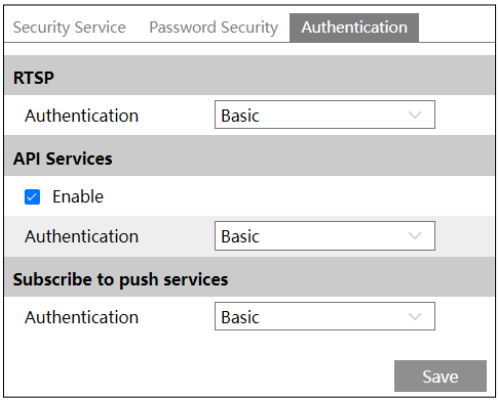
- **Password Security**

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Please set the password level and expiration time as needed.
Password Level: Weak, Medium or Strong.
Weak level: Numbers, special characters, upper or lower case letters can be used. You can choose one of them or any combination of them when setting the password.
Medium Level: 8~16 characters, including at least two of the following categories: numbers, special characters, upper case letters and lower case letters.
Strong Level: 8~16 characters. Numbers, special characters, upper case letters and lower case letters must be included.
For your account security, it is recommended to set a strong password and change your password regularly.

- **Authentication**

You can improve the network access security by setting RTSP and API service authentication.



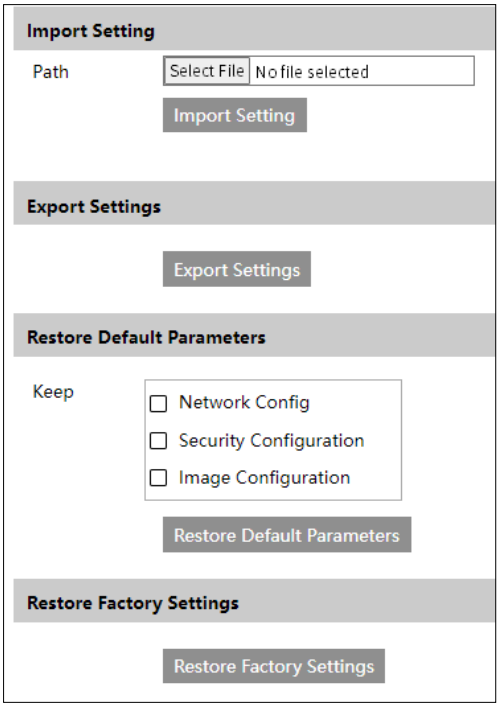
RTSP Authentication: Digest or basic can be selected.
API Service Authentication: Digest or basic can be selected.
Push Subscription Authentication: Digest or basic can be selected.

5.7 Maintenance Configuration

5.7.1 Backup and Restore

Go to ***Config→Maintenance→Backup and Restore***.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands



- **Import & Export Settings**

Configuration settings of the camera can be exported form a camera into another camera.
1. Click “Select File” to select the save path for import or export information on the PC.
2. Click the “Import Setting” or “Export Setting” button.

Note: * The login password needs to be entered after clicking the “Import Setting” button.
* The customized audio files are not supported to export or import.

- **Restore Default Parameters**

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

- **Restore Factory Settings**

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

5.7.2 Reboot

Go to ***Config→Maintenance→Reboot***.
Click the “Reboot” button and then enter the password to reboot the device.

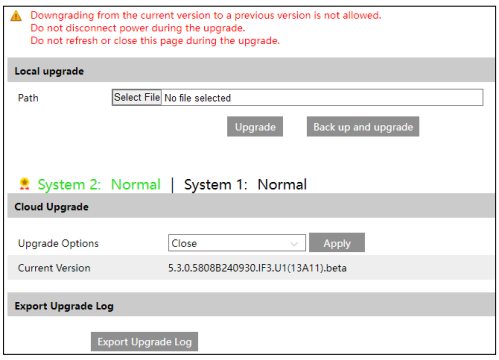
Timed Reboot Setting:

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

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

5.7.3 Upgrade

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



- **Local Upgrade**

1. Click the “Select File” button to select the save path of the upgrade file.
2. Click the “Upgrade” or “Back up and upgrade” button to start upgrading the firmware.
3. Enter the correct password and then the device will restart automatically.

Note: If “Back up and upgrade” is selected, the configuration file will be exported to your local PC before starting upgrading.

- **Cloud Upgrade**

Note: Before you use cloud upgrade, please make sure the cloud service is enabled successfully. After the cloud server pushes the latest version, you can upgrade the camera by itself or NVR.

1. Go to ***Config→Maintenance→Upgrade***.
2. Select “Notify Only” in the cloud upgrade options or click “Manual Check” to check whether the current version is the latest. If your software version is not the latest, click “Upgrade” to download and upgrade from the cloud server.

Caution:

1. You cannot downgrade to a lower version.
2. Do not refresh/close the browser or disconnect the camera from the network during the upgrade, or it will cause system failure. After the device is successfully upgraded, there are ten minutes of observation. During this observation period, do not upgrade the device again.

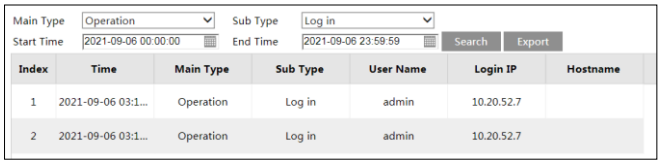
Note: To decrease the upgrade risk, this series of cameras adopts two systems. After one system is successfully upgraded, the other system will be synchronized. If one system fails caused by power failure or other reasons during the upgrade, the other system will not be affected and the camera still can work normally. You can also upgrade your camera through the normal system.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

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

5.7.4 Operation Log

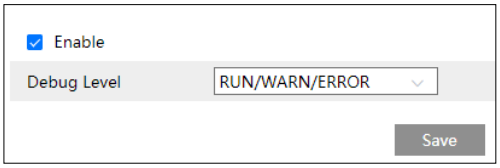
To query and export log:
1. Go to ***Config→Maintenance→Operation Log***.



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

5.7.5 Serial Output

Serial output mode is used to record and collect the required system data, so that the technician can quickly find out and analyze the problem, and help us to improve service.
Before enabling the mode, you are advised to consult our technical support.



5.7.6 Maintenance Information

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

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

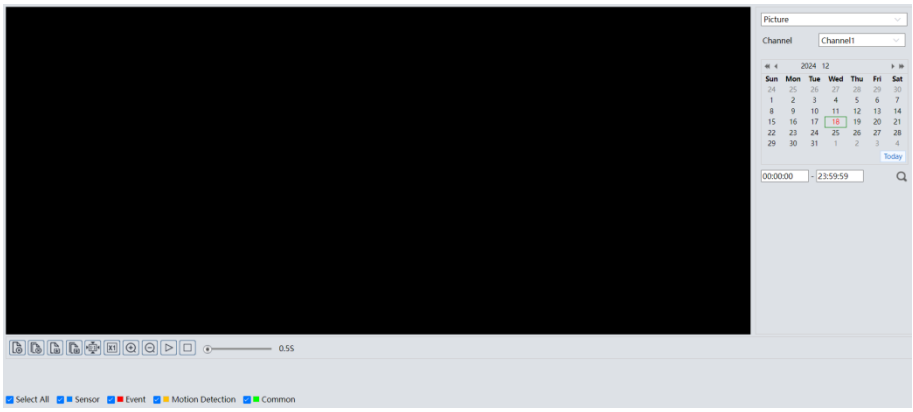
6 Search

6.1 Image Search

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

- **SD Card Image Search**

1. Choose “Picture” and the desired channel.



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

The descriptions of the buttons are shown as follows.

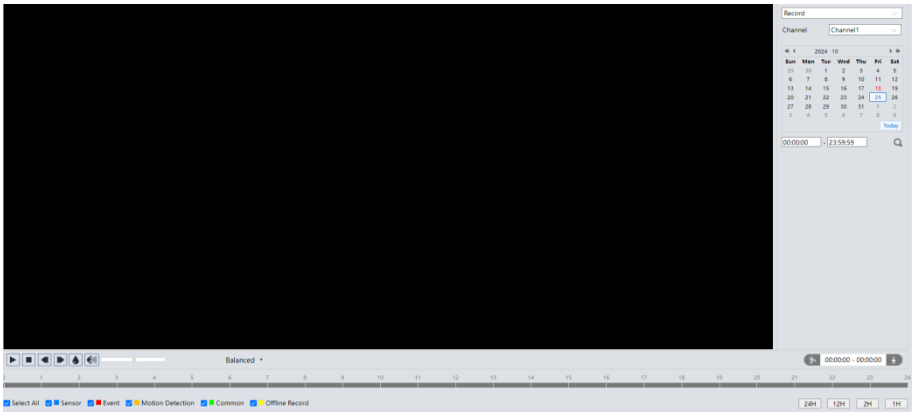
Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Icon	Description	Icon	Description
	Close: Select an image and click this button to close the image.		Close all: Click this button to close all images.
	Save: Click this button to select the path for saving the image on the PC.		Save all: Click this button to select the path for saving all pictures on the PC.
	Fit size: Click to fit the image on the screen.		Actual size: Click this button to display the actual size of the image.
	Zoom in: Click this button to digitally zoom in.		Zoom out: Click this button to digitally zoom out.
	Slide show play: Click this button to start the slide show mode.		Stop: Click this button to stop the slide show.
5.5S	Play speed: Play speed of the slide show.		

6.2 Video Search

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

1. Choose “Record”.
2. Select the channel you want to search.
3. Set search time: Select the date and choose the start and end time.
4. Select the alarm events at the bottom of the interface.
5. Click to search the images.



6. Double click on a file name in the list to start playback.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

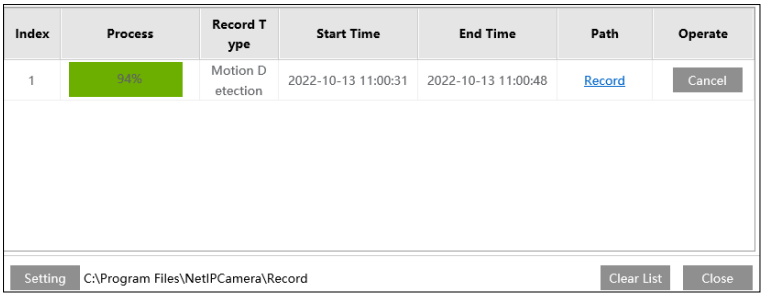
Icon	Description	Icon	Description
	Play button. After pausing the video, click this button to continue playing.		Pause button
	Stop button		Speed down
	Speed up		Watermark display
	Enable / disable audio; drag the slider to adjust the volume after enabling audio.		

Note:  and  cannot be displayed in the above interface via the plug-in free browser. Additionally, for plug-in free playback, playback mode switch (balanced/real-time/fluent mode) and downloading functions are not supported too.

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

Video clip and downloading

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



Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Click “Setting” to set the storage directory of the video files.
Click “Open” to play the video.
Click “Clear List” to clear the downloading list.
Click “Close” to close the downloading window.