BC1103/BL1103/FD1103

3 MP Intelligent IP cameras

User Manual

TKH GROUP SECURITY SOLUTIONS

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

BC1103/BL1103/FD1103
User Manual v3 (162303-3)
AIT55

Brand names

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

Liability

Siqura 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 via t.writing@tkhsecurity.com. 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:

Siqura B.V.
Zuidelijk Halfrond 4
2801 DD Gouda
The Netherlands

General : +31 182 592 333
Fax : +31 182 592 123
E-mail : sales.nl@tkhsecurity.com
WWW : http://www.tkhsecurity.com

Contents

1 About this manual

What's in this manual

This is version 3 of the user assistance which is embedded in the web interface of the BC1103/BL1103/FD1103 camera. The Help topics give you all the information you need to use this product efficiently. They tell you:

- How to get access to the camera
- How to communicate with the camera
- How to operate the camera
- How to configure the settings of the camera

Where to find more information

Find additional manuals, the datasheet, the EU Declaration of Conformity, and the latest firmware for this product at www.tkhsecurity.com/support-files. 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 configure and operate BC1103/BL1103/FD1103 cameras.

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

At TKH Security, 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.

We like to hear from you!

Customer satisfaction is our first priority. We welcome and value your opinion about our products and services. Should you detect errors or inaccuracies in this manual, we would be grateful if you would inform us. We invite you to offer your suggestions and comments via t.writing@tkhsecurity.com. Your feedback helps us to further improve our documentation.

2 Safety and compliance

This section provides safety instructions and compliance information.

In This Chapter

2.1 Safety instructions

These instructions are intended to make sure that the user can use the product correctly and avoid danger or property loss.

The precaution measure is divided into 'Warnings' and 'Cautions':

- **Warnings**: Serious injury or death may be caused if any of these warnings are neglected.
- **Cautions**: Injury or equipment damage may be caused if any of these cautions are neglected.

			
Warnings	Follow these safeguards to prevent serious injury or death.	**Cautions**	Follow these precautions to prevent potential injury or material damage.

Warnings

	• Use a power adapter which can meet the safety extra low voltage (SELV) standard and source it with 12 Vdc or 24 Vac (depending on the model) according to the IEC60950-1 and Limited Power Source standard.
	• To reduce the risk of fire or electrical shock, do not expose this product to rain or moisture.
	• This installation should be made by a qualified service person and should conform to all the local codes.
	• Install blackout equipment into the power supply circuit for convenient supply interruption.
	• Make sure that the ceiling can support more than 50 (N) Newton if the camera is fixed to the ceiling.
	• If the product does not work properly, contact your dealer or the nearest service centre. Never attempt to disassemble the camera yourself. We shall not assume any responsibility for problems caused by unauthorised repair or maintenance.

Cautions

- Make sure the power supply voltage is correct before using the camera.
- Do not drop the camera or subject it to physical shock.
- Do not touch the sensor modules with your fingers. If cleaning is necessary, use a cleaning cloth with a bit of ethanol and wipe it gently. If the camera will not be used for an extended period of time, put on the lens cap to protect the sensor from dirt.
- Do not aim the camera lens at strong light such as the sun or an incandescent lamp. The strong light can cause fatal damage to the camera.
- The sensor may be burned out by a laser beam, so if any laser equipment is used, make sure that the surface of the sensor is not exposed to the laser beam.
- Use the unit under conditions where the temperature remains within the range given in the Technical Specifications of this product. You can download the datasheet of the camera at www.tkhsecurity.com/support-files.
- Do not install the camera in a dusty or damp environment, and do not expose it to high electromagnetic radiation.
- To avoid heat accumulation, good ventilation is required to ensure a proper operating environment.
- Keep the camera away from water and any liquid.
- While shipping, the camera should be packed into its original packing.
- Improper use or replacement of the battery may result in the hazard of explosion. Use the battery type recommended by the manufacturer.

Cautions

The following cautions apply to cameras with IR functionality. Be sure to follow them to prevent IR reflection.

- Dust or grease on the dome cover will cause IR reflection. Do not remove the dome cover film until the installation is finished. If there is dust or grease on the dome cover, clean the dome cover with a clean soft cloth and isopropyl alcohol.
- Make sure that the installation location does not have any reflective surfaces of objects that are too close to the camera. The IR light from the camera may reflect back into the lens causing a reflection in the video image.
- The foam ring around the lens must be seated flush against the inner surface of the bubble to isolate the lens from the IR LEDS. Fasten the dome cover to the camera body so that the foam ring and the dome cover are attached seamlessly.

2.2 Compliance information

FCC compliance

This equipment has been tested and found to comply with the limits for a digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Conditions

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

1 This device may not cause harmful interference.

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

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.

EU Conformity Statement

CE	This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonised European standards listed under the EMC Directive 2004/108/EC, the RoHS Directive 2011/65/EU.
	2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info.
	2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info.

3 Connect to network

This section gives instructions for connecting the camera to the network.

In This Chapter

3.1 System requirements

To open communication with the camera, you need:

- A computer with a web browser installed.
- An IP connection between the computer and the camera.

Computer

The browsing computer should meet the following minimum system requirements:

Item	Description
Operating System	Microsoft Windows 7 / Server 2008 32 bits
CPU	Intel Pentium IV 3.0 GHz or higher
RAM	1 GB or higher
Display	1024×768 resolution or higher
Web browser	Internet Explorer 7.0 and higher, Apple Safari 5.02 and higher, Mozilla Firefox 5 and higher, and Google Chrome 8 and higher

IP connection

You can connect the network camera to:

- A local area network (LAN)
- A wide area network (WAN)

Note: Be aware that using this product with Internet access may pose serious threats to your network security. To avoid network attacks and information leakage, strengthen your security against intrusions. To ensure the network security of the network camera, we advise you to inspect and maintain the network camera at specific intervals. If the product does not work properly, contact your sales representative.

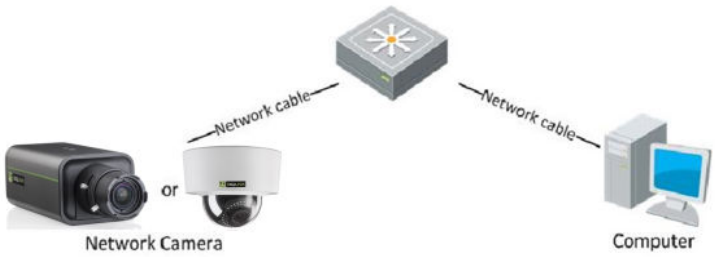
3.2 Connect the camera to a LAN

To view (live) video from the camera and configure its settings, there must be an IP connection between the camera and a computer.

Important: The network settings of the camera and the computer should be such that they are on the same subnet.

Connection via switch or router

Generally, the network camera and the computer are connected via a switch or a router.



Direct connection

To bring the network camera into the same subnet as the computer (or to test the camera), connect the two devices directly with a network cable.

Bring the camera and computer into the same subnet

Take the following steps to connect to the network camera from the computer:

1 Set the network adapter of the computer to the factory-set subnet of the camera.
(Control Panel > Network and Sharing Center > Change adapter settings ... > Properties ...)
For the default network settings of the camera, see *Default settings* (below) .

2 Connect the two devices with a network cable.

3 Open the web interface of the camera from a web browser on the computer.
For details, see *Get access via web browser*.
For information about Device Manager, see *Get access via Device Manager*.

Default settings

Out of the box, the camera has these settings:

- IP address: 192.168.1.64
- DHCP: enabled
- UPnP: enabled

Note: If no DHCP server is found on the network, the camera is initially assigned the IP address 0.0.0.0. After 30 seconds, the IP address 192.168.1.64 is adopted.

Add the camera to the intended subnet

Via the web interface of the camera, you can change its network settings to add it to the subnet it will be used in.

1 On the **Network** page, click the **TCP/IP** tab.

2 Set the IP address of the camera to the desired subnet.

3 Click **Save**.

4 Reboot the camera.

5 (Optional) Configure the network settings of the computer to assign it to the subnet set in step 2.

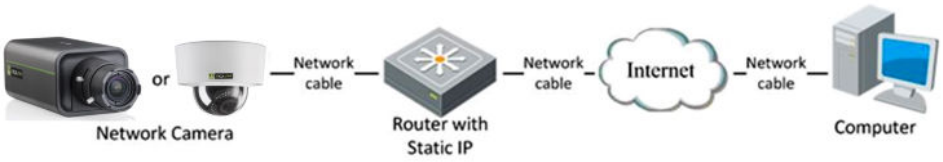
With both devices on the same subnet, you can reopen communication between the computer and the camera.

3.3 Connect the camera to a WAN

This section explains how to connect the network camera to the WAN with a static or dynamic IP address.

Static IP connection

Before you start, obtain a static IP address from an Internet Service Provider (ISP). With the static IP address, you can connect the network camera via a router.



To connect the network camera via a router

1 Establish a connection between the network camera and the router.

2 Assign a LAN IP address, subnet mask and gateway address.

For more information about the IP address configuration of the camera, see *Connect the camera to a LAN*.

3 Save the static IP in the router.

4 Set the port mapping.

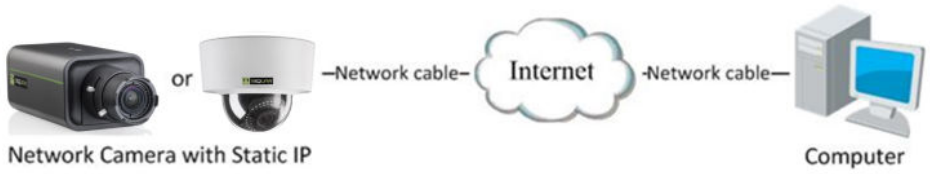
Use 80, 8000, and 554 as ports, for example.

The steps for port mapping vary according to the different routers. If necessary, contact the router manufacturer for assistance with port mapping

5 Visit the network camera through a web browser or client software over the internet.

Directly connect the network camera with a static IP address

You can also save the static IP on the camera and directly connect it to the internet without using a router.



Dynamic IP connection

Before you start, obtain a dynamic IP address from an Internet Service Provider (ISP). With the dynamic IP address, you can connect the network camera via a modem or a router.

To connect the network camera via a router

1 Establish a connection between the network camera and the router.

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

For more information about the IP address configuration of the camera, see *Connect the camera to a LAN*.

3 In the router, set the PPPoE user name, password and confirm the password.

4 Set the port mapping.

Use 80, 8000, and 554 as ports, for example.

The steps for port mapping vary according to the different routers. If necessary, contact the router manufacturer for assistance with port mapping.

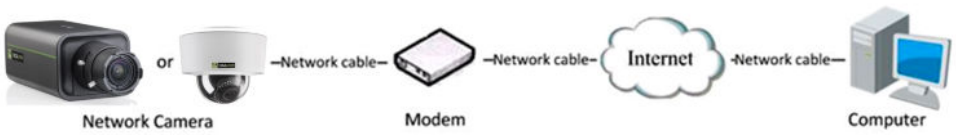
5 Apply a domain name from a domain name provider.

6 Configure the DDNS settings in the setting interface of the router.

7 Visit the camera via the applied domain name.

Connect the network camera via a modem

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



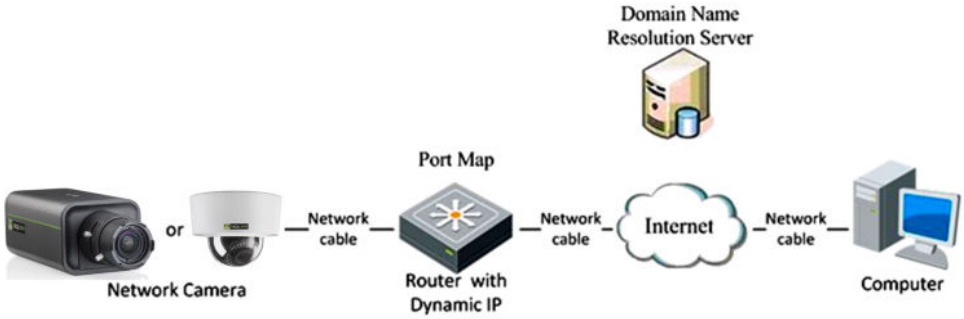
The obtained IP address is dynamically assigned via PPPoE, so the IP address always changes after rebooting the camera. To solve the inconvenience of the dynamic IP, you need to get a domain name from the DDNS provider (for example, DynDys.com). Follow the steps below to set a normal domain name resolution and a private domain name resolution to solve the problem.

To set normal domain name resolution

1 Apply a domain name from a domain name provider.

2 On the *DDNS* tab of the Network page in the camera, configure the DDNS settings.

3 Visit the camera via the applied domain name.



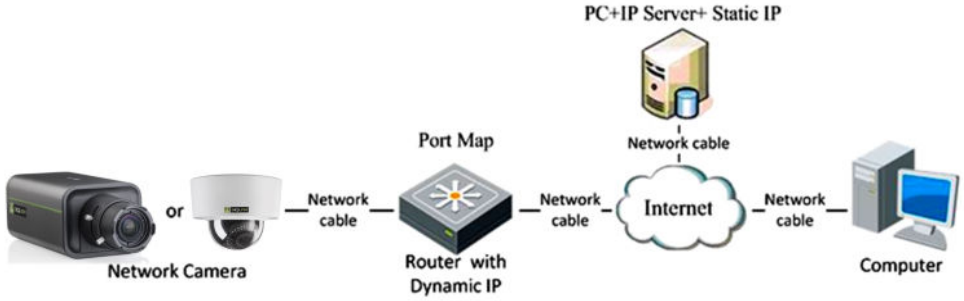
To set private domain name resolution

1 Install and run the IP Server software on a computer with a static IP.

2 Access the network camera through the LAN through a web browser.

3 On the *DDNS* tab of the Network page in the camera, select **Enable DDNS.**

4 In the *DDNS Type* list, select **IPServer**.



4 Get access to the camera

The webpages of the camera offer a user-friendly interface for configuring its settings and viewing live video over the network. This section explains how to log on to the built-in web server.

In This Chapter

4.1 Get access via web browser

Default settings

Out of the box, the camera has these settings:

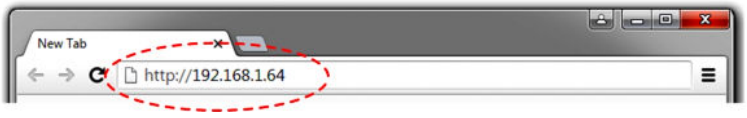
- DHCP: enabled
- UPnP: enabled

If a DHCP server exists on the network, the camera acquires an IP address from the DHCP address range. If necessary, refer to your system administrator for assistance.

If no DHCP server is found on the network, the camera is initially assigned the IP address 0.0.0.0. After 30 seconds, an IP address in the range of 192.168.1.2~192.168.1.253 is adopted.

To connect to the camera via your web browser

1 Open your web browser.
2 Type the IP address of the camera in the address bar.
3 Press ENTER.
You are directed to the login page (see *Log on to the camera*).



Note: If you do not know the IP address of the camera you can use Device Manager or UPnP, both described in the following sections, to detect the camera on the network.

4.2 Get access via Device Manager

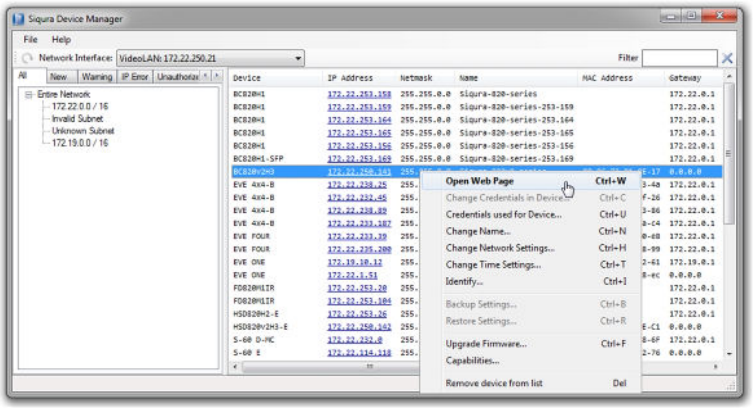
Device Manager is a Windows-based software tool that you can use to manage and configure TKH Security IP cameras and video encoders. The tool automatically locates TKH Security devices on the network and offers you an intuitive interface to set and manage network settings, configure devices, show device status, and perform firmware upgrade.

To install Device Manager

1 Download the latest version of Device Manager at www.tkhsecurity.com/support-files.
2 Double-click the setup file.
3 Follow the installation steps to install the software.

To connect to the camera via Device Manager

1 Start Device Manager
The network is scanned.
Detected devices appear in the List View pane.
2 If multiple network adapters exist, select the appropriate adapter to scan the network that you wish to connect to.
3 To perform a manual search, click the **Rescan** button.
4 Use the tabs in the *Tree View* pane to define the scope of your search.
5 Click the column headings in the *List View* pane to sort devices by type, IP address, or name.
6 To connect to the webpages of the camera, double-click its entry in the device list,
You are directed to the login page. (see *Log on to the camera*).



Change the network settings with Device Manager

With Device Manager, you can directly change the network settings of the camera.

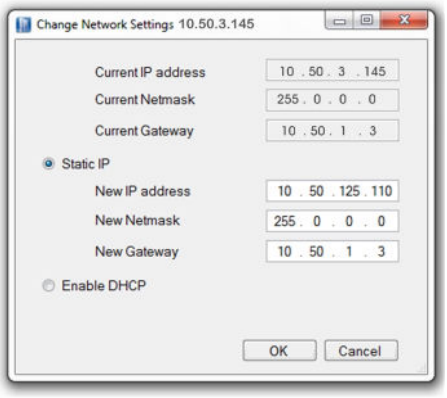
To assign a static IP address

1 Go to the list of detected devices, and then right-click the entry for the camera.
2 Click **Change Network Settings**.
3 In *Change Network Settings*, click **Static IP**.
4 Provide the camera with an appropriate IP address, netmask, and gateway address for the desired network configuration, and then click **OK**.

5 In the pop-up window indicating that you have successfully changed the settings, click **OK**.

6 Wait one minute, and then rescan the network.

7 To access the webpages of the camera, double-click its entry in the list of found devices.



To assign a DHCP server

1 Record the MAC address of the camera (see the *Serial no.* column in Device Manager) for future identification

2 In the list of detected devices, right-click the device with the network property that you would like to change.

3 Click **Change Network Settings**.

4 In *Change Network Settings*, click **Enable DHCP**, and then click **OK**.

5 In the pop-up window indicating that you have successfully changed the settings, click **OK**.

6 Wait one minute, and then rescan the network.

You can identify the camera by its MAC address.

7 To access the webpages of the camera, double-click its entry in the list of found devices.

Note: A DHCP server must be installed on the network in order to provide DHCP network support. If no DHCP server is found on the network, the camera is initially assigned the IP address 0.0.0.0. After 30 seconds, an IP address in the range of 192.168.1.2~192.168.1.253 is adopted.

4.3 Get access via UPnP

Universal Plug and Play (UPnP) support is enabled by default on the camera. With the UPnP service enabled in Windows, you can get access to the camera from Windows Explorer.

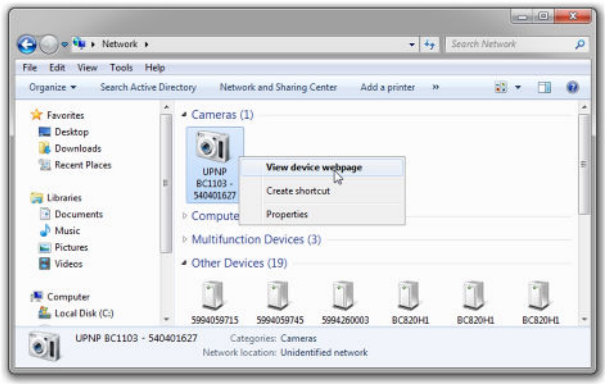
To connect to the camera via UPnP

1 In Windows Explorer, open the **Network** folder.

Detected devices in the same subnet as the computer are displayed, including codecs and cameras with UPnP support.

2 Double-click the camera that you want to connect to.

You are directed to the login page (see *Log on to the camera*).



4.4 Log on to the camera

Admin account

When you connect to the web interface of the camera for the first time, you are prompted to set a password. By supplying a password, you create an account with Administrator level that you can use to add "Operator" and "User" accounts for other users of the camera.

CAUTION: TO KEEP THE ACCOUNT SAFE, SET A STRONG, COMPLEX PASSWORD. THIS HELPS TO PREVENT UNAUTHORISED ACCESS.

To create a strong password

- Use at least eight characters
- Do not include your real name, user name, company name, or other personal information
- Do not use complete words that can be found in a dictionary
- Use a random combination of at least two of the following categories: upper case letters, lower case letters, numbers and special characters

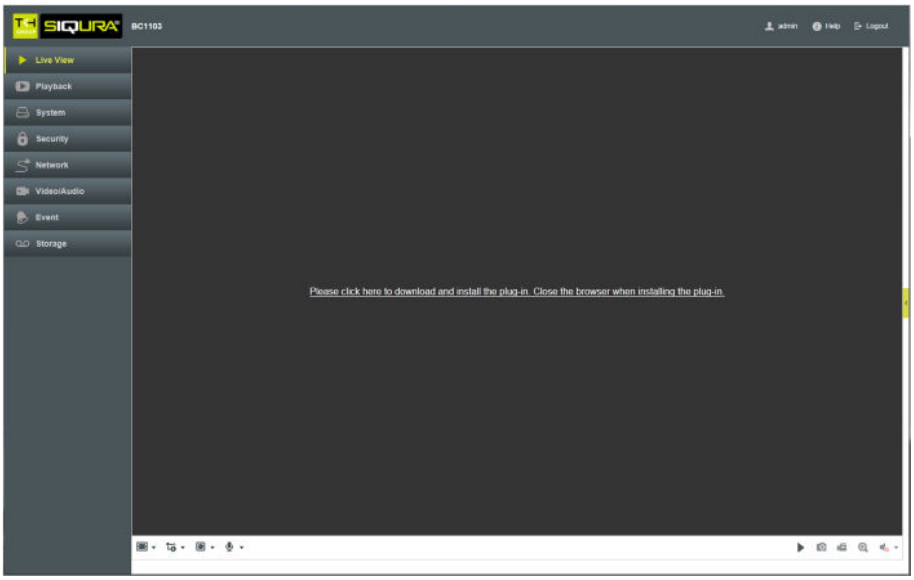
Note: For better protection, especially in high-security systems, we advise you to change the password at regular intervals.

Login box

Once the Admin account has been created, you will encounter a login box when you connect. Only users with a valid account can log on.

Note: The IP address of the camera gets locked after seven failed passwords attempts for the Admin and five attempts for the user/operator.

4.5 Install the videoplayer plug-in



For (live) video viewing and operating the camera, a videoplayer plug-in is needed. If the plug-in is not detected you are prompted to download and install it.

To install the plug-in

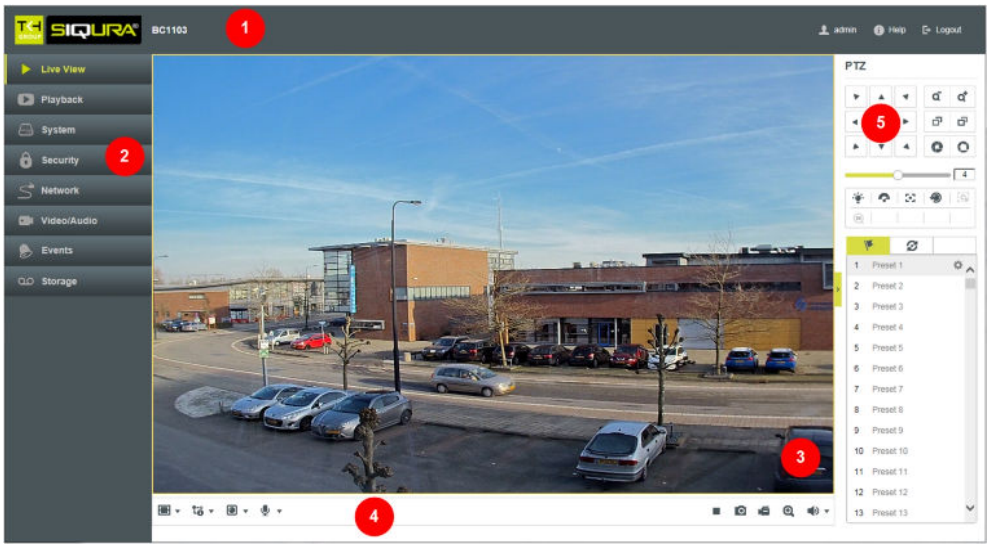
1 Click the hyperlink in the webpage of the camera.
2 Save the WebComponents.exe file to your Downloads folder.
3 Close your web browser.
4 Go to your Downloads folder.
5 Double-click **WebComponents.exe**.
The executable file does not give rise to any security risks. You can install it safely.
6 Follow the installation steps.
7 Open your web browser.
8 Reconnect to the camera.

5 Live View

The Live View page is the home page of the web interface. It is shown when you successfully connect to the camera.

What this page is for

On the Live View page, you can view real-time video, capture images and configure various video settings. Cameras with PTZ functionality can be controlled from the PTZ panel.



1. Title bar 2. Menu 3. Live View window 4. Toolbar 5. PTZ panel

To show/hide the PTZ panel

- Click the arrow on the right side of of the Live View window.

Title bar

The horizontal bar at the top of the window has the following items.

Item	Description
SIQURA	Shows the brand of the camera you are connected to
BC1103	Shows the camera model name
admin	Shows the user currently logged on to the camera
Help	Opens the Online Help information
Logout	Logs out the current user

Menu

The vertical menu on the left gives access to the pages of the web interface.

Live View window

This area is used to display live video from the connected camera.

Toolbar

The horizontal bar at the bottom of the page contains two groups of buttons.

Buttons (left side)	Description
	Opens the Aspect Ratio list. Use the options to set the relation between the width and height of the video display.
	Sets the video aspect ratio to 4:3
	Sets the video aspect ratio to 16:9
	Sets the original video aspect ratio
	Sets the video aspect ratio to Auto mode (self-adaptive resizing)
	Opens the Stream Type list. Use the options to select a video stream for display in the Live View window.
	Selects Stream 1
	Selects Stream 2
	Selects Stream 3
	Opens the video player plug-in list. Use the options to select a plug-in or live video display.
	Selects the Webcomponents plug-in
	Selects the QuickTime plug-in
	Opens the Two-way Audio list
	Turns the microphone on/off

Buttons (right side)	Description
	Stops Live View (screen goes blank)
	Starts Live View
	Captures the image
	Starts a recording
	Stops a recording
	Enables digital zoom (e-PTZ)
	Disables digital zoom (e-PTZ)
	Opens Audio Volume control
	Enables you to control audio volume by dragging the slider

Manual recordings and snapshots

Clicking **Start Recording** starts a manual recording. The recording is saved to the location set via the Local Configuration tab of the System page. There, you can also set the storage path for captured snapshots.

Important: To use this function, run your web browser as Administrator.

PTZ Operation

On the Live View page, you can use the PTZ control buttons for pan/tilt/zoom control of the camera.

Important: To realise PTZ control, the camera connected to the network must support the PTZ function or a pan/tilt unit must be installed to the camera. Before you realise PTZ control, make sure that the PTZ parameters (*System* > *RS-485*) are correctly configured.

Direction buttons

To pan/tilt the camera

- Click the direction buttons shown above.

Note: The direction buttons are not available if your camera model supports lens movement only.

PTZ Speed slider

Use the PTZ Speed slider to adjust the speed of pan/tilt movements. Drag to the right to increase speed and to the left to decrease speed.

Zoom/Focus/Iris buttons

	Zoom out/in
	Focus far/near
	Iris close/open

Additional buttons

Availability of the following buttons varies per camera model.

	Light
	Wiper
	Auxiliary Focus
	Lens Initialisation

Presets

By setting a preset, you can save a camera position to which you want the camera to return when you call the preset or when an event occurs.

Preset buttons

The following buttons are available for preset management.

	Set preset
	Call preset
	Delete preset

To set a preset

1 In the *PTZ* control panel, select a preset number from the preset list.
2 Use the PTZ control buttons to move the lens to the desired position.
- Pan the camera to the right or left.
- Tilt the camera up or down.
- Zoom in or out.
- Refocus the lens.
3 Click **Set**.

To call a preset

1 In the *PTZ* control panel, select the preset you need.
2 Click **Call**.
The camera moves to the position stored for this preset.

To delete a preset

1 In the *PTZ* control panel, select the preset you wish to delete.
2 Click **Delete**.

Patrols

A patrol is a recorded sequence of presets to be adopted consecutively by the camera when the patrol is started. A patrol can be configured with 32 presets. Before you create a patrol, make sure that the presets you want to add to the patrol have been defined.

Patrol buttons

The following buttons are available for patrol management.

	Set patrol			Add preset
	Start patrol			Delete preset
	Stop patrol			Move preset down
	Delete patrol			Move preset up

To create a patrol

1 In the *PTZ* panel, click the **Patrol** tab.
2 Select a Patrol Path number.
3 Click **Set**.
4 Click **Add**.
5 In the *Preset* list, select a preset number.
6 In the *Speed* box, type a value for the patrol speed.
This is the speed of moving from one preset to the next.
7 In the *Time* box, type a value for the patrol duration.
This defines the time span for the camera to stay at one patrol point. The camera moves to the next patrol point after the patrol time.
8 Repeat steps 4 ~ 7 to add more presets.
9 (Optional) Use the arrow buttons to adjust the order of the presets.
10 Click **OK**.

To start a patrol

1 In the *PTZ* pane, click the **Patrol** tab.
2 Select the Patrol Path to be started.
3 Click **Start**.

To stop a patrol

1 In the *PTZ* pane, click the **Patrol** tab.
2 Select the Patrol Path to be stopped.
3 Click **Stop**.

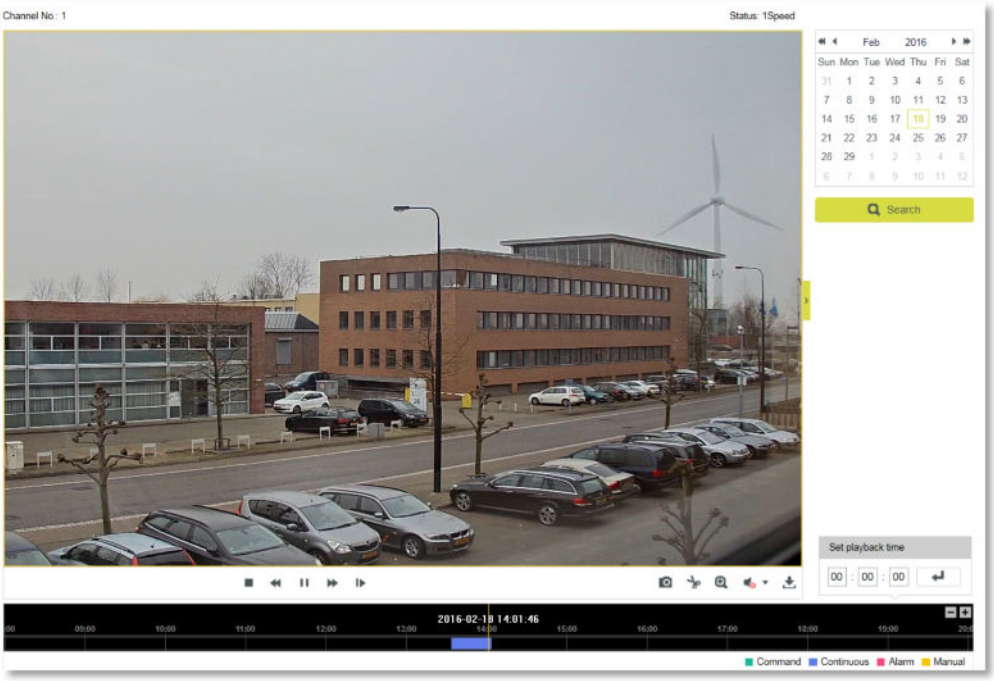
To delete a patrol

1 In the *PTZ* pane, click the **Patrol** tab.
2 Select the Patrol Path to be deleted.
3 Click **Delete**.

Full-screen mode

You can double-click on the live video to go from the current live view mode to full-screen or return to normal mode from full-screen.

6 Playback



What this page is for

On the Playback page, you can view recorded video stored on a network disk or on the SD card.

To search for recorded video

1 On the *Playback* page, go to the calender on the right.

2 Select the date you need.

3 Click **Search**.

Video recordings for this date - if any - appear in the Time line at the bottom of the page.

Recording types - *Command*, *Continuous*, *Alarm*, and *Manual* - can be distinguished by their colour.

The progress pointer is positioned at the start of the first recording.

To locate a specific playback point

- In **Set playback time**, type the exact time, and then click **Enter**.

  - or -

- Drag the Time line to the left or right, relative to the pointer.

  You can click the "-" and "+" button to zoom the Time line.

Video playback

For video playback, use the following buttons in the Playback toolbar.

Task	Action	Button
To start playback	Click **Start**	
To pause playback	Click **Pause**	
To stop playback	Click **Stop**	
To accelerate playback speed	Click **Fast forward**	
To reduce playback speed	Click **Slow forward**	
To advance one frame	Click **Single frame**	

Additional functions

The buttons below are located on the right side of the toolbar.

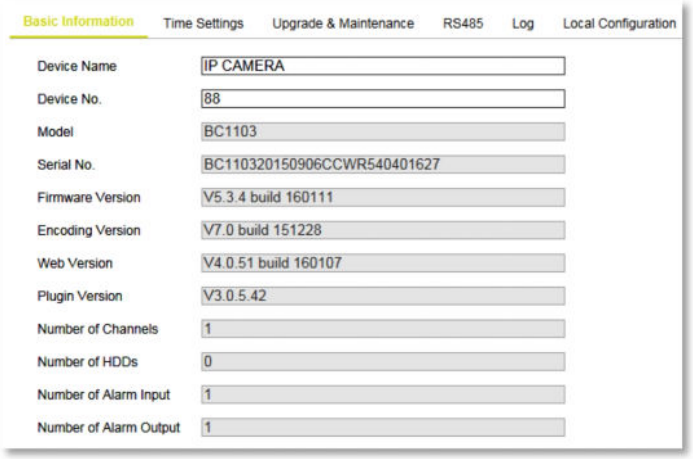
Task	Action	Button
To capture a snapshot	Click **Capture**	*1,* 
To create a video clip	Click **Start/Stop clipping**	
To use digital zoom (e-PTZ)	Click **Enable/Disable e-PTZ**	
To control audio volume	Click **Audio On / Mute**	
To download a file	Click **Download**	

7 System

The System page is the central place for viewing and configuring device and firmware related information and settings. On the various tabs, you can adjust the time settings, reboot the camera, restore the default settings, upgrade the firmware, view logs, and configure RS-485 and local settings.

In This Chapter

7.1 Basic Information



System > Basic Information

What this tab is for

The Basic Information tab gives general information about the camera. It is made up of editable and non-editable content.

Identification

For easier identification of the camera on the network, assign a device name and device number to the camera.

To assign a device name and device number

1 In *Device Name*, type a (user-friendly) name for the camera.

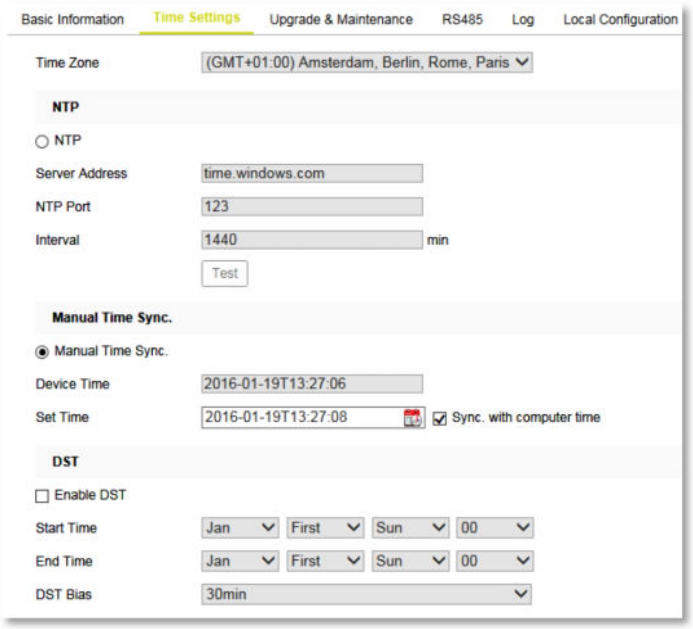
2 In *Device No.*, type the camera number.

3 Click **Save**.

Reference information

The non-editable content on this tab serves as reference information for maintenance or future configuration of the camera. Note that this information varies per model.

7.2 Time Settings



System > Time Settings

What this tab is for

On the Time Settings tab, you can set the device date and time manually or use an NTP server. You can also configure the Daylight Saving Time (DST) settings here.

To set the time zone

1 Click to open the **Time Zone** list.

2 Select the location of the camera.

3 Click **Save**.

Note: The Time Zone list is not available if *Sync. with computer time* is selected.

To synchronise the system time with a Network Time Protocol (NTP) server

1 In the *NTP* section,click **NTP**.

2 In *Server Address*, type the IP address of the NTP server.

3 In *NTP Port*, type the port number of the NTP server.

4 In *Interval*, type the time interval (in minutes) between the consecutive time service queries.

The interval between two synchronising actions by an NTP server can be set from 1 to 10080 minutes.

5 Click **Test**.

The connection to the time server is tested.

6 If your settings are correct, click **Save**.

Note: If the camera is connected to a public network, use an NTP server that has a time synchronisation function. If the camera is set up in a customised network, NTP software can be used to establish an NTP server for time synchronisation.

To set the system time manually

1 In the *Manual Time Sync* section, select **Manual Time Sync**.

2 In *Set Time*, click the **Calender/Clock** icon.

3 Use the calender and the *Time* list to set the system date and time.

4 Click **OK** to confirm your settings.

5 (Optional) As an alternative to steps 2-4, you can select **Sync. with computer time**.

This synchronises the camera system time with the time of your computer.

6 Click **Save**.

To enable DST

1 In the *DST* section, select **Enable DST**.

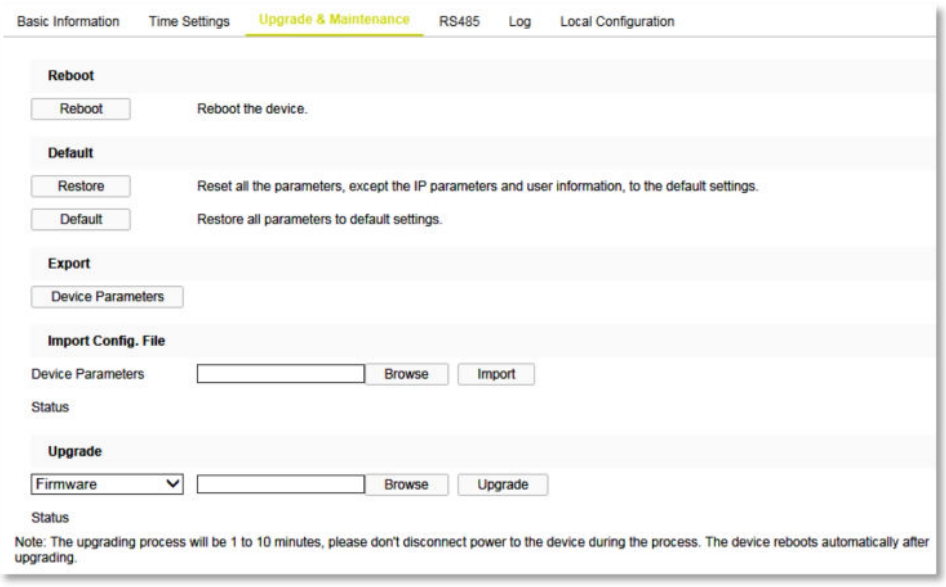
2 In the **Start Time** and **End Time** lists, select the appropriate start and end details.

3 In the **DST Bias** list, select the offset.

This is the amount of time you need to subtract from or add to Coordinated Universal time (UTC) to get the current time for the location of the camera.

4 Click **Save**.

7.3 Upgrade & Maintenance



System > Upgrade & Maintenance

What this tab is for

Use the Upgrade & Maintenance tab for the following tasks:

- Reboot the camera
- Restore the factory-default camera settings,
- Export/Import a camera configuration file
- Upgrade the camera firmware

Reboot the camera

If there are connectivity problems or if an error occurs, reboot the camera. A reboot does not affect the settings of the camera.

To reboot the camera

1 Click **Reboot**.

2 Click **OK** to confirm.

The webpage is unresponsive while the camera is rebooting.

Restore default settings

With the options in the *Default* section, you can restore the camera settings to their original factory-default values. Depending on the option you select, the reset includes or excludes the current network settings and user information.

To restore the default settings

- Click **Restore** to reset all settings with the exception of the network settings and the user information.

  - or -

- Click **Default** to perform a complete reset including the network settings and user information.

  Use this button with caution.

Warning: Clicking **Default** can make the camera unreachable for in-band communications. In that case you can only get access to the web interface by (temporarily) moving a PC to the factory-default subnet of the camera.

Use a configuration file

If you want to apply the same settings to a batch of cameras, use a configuration file to simplify the process. You configure a camera with the required settings, export the settings in a configuration file and import this file on the other cameras.

To export a configuration file

1 Click **Device Parameters**.

2 Browse to the folder where you want to store the file.

3 Specify a file name.

4 Click **Save**.

To import a configuration file

1 In the *Import Config. File* section, click **Browse**.

2 Browse to the folder where the file is stored.

3 Select the file.

4 Click **Open**.

5 Click **Import**.

6 Reboot the camera when the import has completed.

Upgrade the system

We advise you to visit www.tkhsecurity.com/support-files and check if new firmware for your camera is available. To upgrade the system, download the latest firmware file to your computer and complete the steps below.

To upgrade the system

1 In the *Upgrade* section, click **Firmware**.

2 Click **Browse**.

3 Locate and select the firmware file.

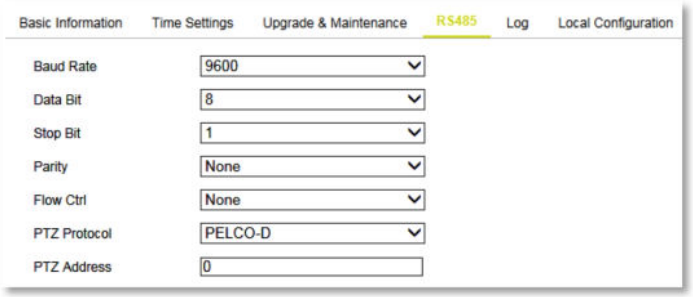
It is essential that the selected file is compatible with the camera.

4 Click **Upgrade**.

The upgrade process takes 1~10 minutes. Do not disconnect the power of the camera during the process. The camera reboots automatically after the upgrade.

Note: It is also possible to select *Firmware Directory* in step 1. In that case, you need to find the directory where the firmware is stored. The device can find the firmware in the directory automatically.

7.4 RS-485



System > RS-485

What this tab is for

On camera models which support PTZ, use this tab to configure the RS-485 settings.

PTZ

The RS-485 serial port is used to control the PTZ of the camera. Configure the PTZ parameters before you control the PTZ unit.

To configure the RS-485 settings

1 Use the RS-485 parameter lists to select the desired values.

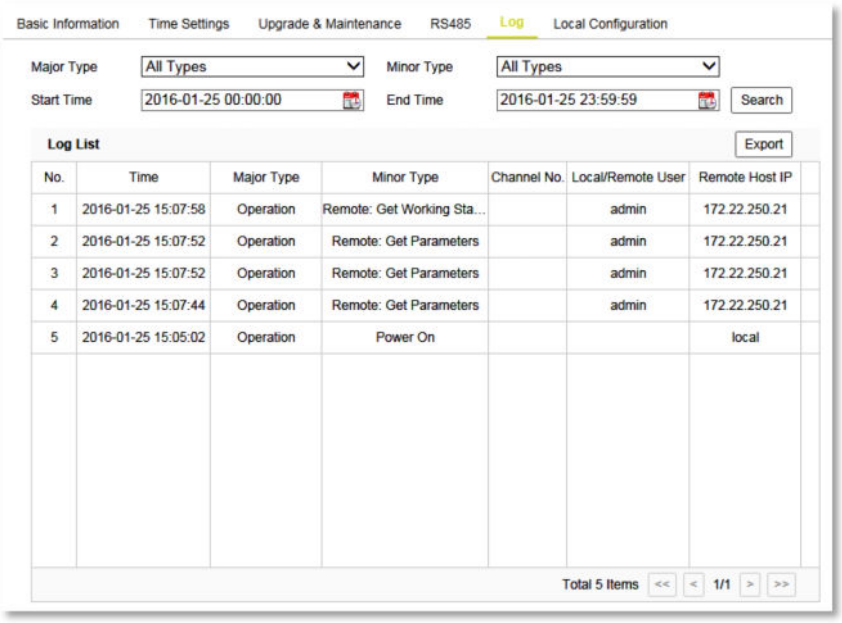
By default, the Baud Rate is set to 9600 bps, the Data Bit is 8, the Stop bit is 1 and the Parity and Flow Control are None.

2 In *PTZ Address*, type the address to be used.

3 Click **Save**.

Note: Make sure that the Baud Rate, PTZ Protocol and PTZ Address parameters of the camera are exactly the same as those of the control device.

7.5 Log



System > Log

What this tab is for

On the Log tab, you can view and export information kept in the Alarm, Exception, Operation, and Information logs of the camera. This information is often useful when you are troubleshooting occurred issues.

Before you start

Configure network storage for the camera or insert an SD card into the camera.

To perform a search

1 In the *Major Type* and *Minor Type* lists, select the filter type to be applied.

2 Use *Start Time* and *End Time* lists to set the date/time range.

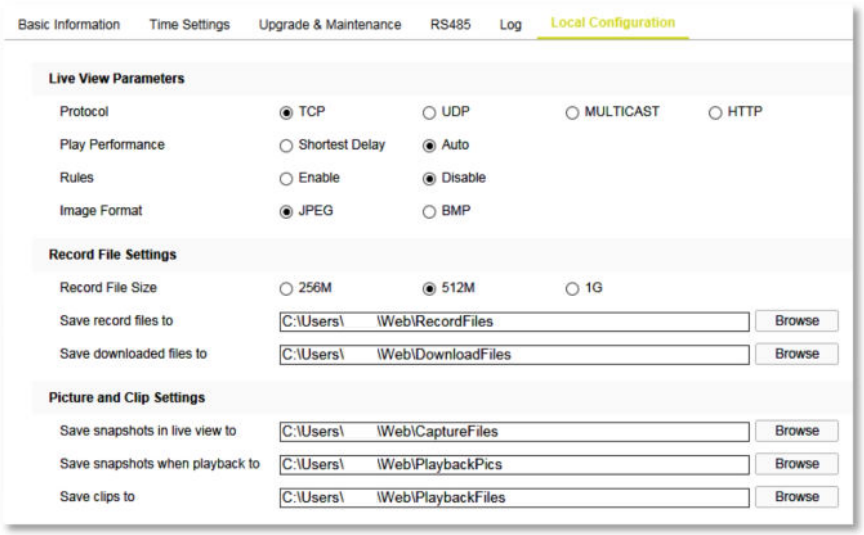
3 Click **Search**.

The results of your search are shown in the Log List.

4 To export the search results, click **Export**.

Exports can be saved as Text files or Excel files.

7.6 Local Configuration



System > Local Configuration

What this tab is for

On the Local Configuration tab, you can configure Live View settings and set the paths to the storage folders for snapshots, clips and downloads.

Live View Parameters

Use this section to set the protocol type and live view performance.

To configure the Live View parameters

1 Select the protocol to be used.

TCP: Ensures complete delivery of streaming data and better video quality. Real-time transmission will be affected, though.

UDP: Provides real-time audio and video streams.

Multicast: For information about multicast, see the description of the TCP/IP tab of the Network page.

HTTP: Provides the same quality as the TCP option without setting specific ports for streaming under some network environments.

2 Set *Play Performance* to **Shortest Delay** or **Auto**.

3 Set *Rules* to **Enable** or **Disable**.

This setting determines the behaviour of your local browser. To have the coloured overlays shown or hidden when motion detection, face detection, or intrusion detection is triggered, select *Enable* or *Disable*, respectively. With *Rules* and face detection both enabled, faces are marked with a green rectangle in Live View once they are detected.

4 Select the image format to be used for captured pictures.

Record File Settings

Use this section to set the file size and the paths to the storage folders for video you recorded with your web browser.

To set the file size and the paths to your storage

1 Set the packed size of manually recorded and downloaded video files to **256M**, **512M** or **1G**.

This sets the maximum file size for recordings to the selected value.

2 In **Save record file to**, type the storage path for manually recorded files or use the **Browse** button.

3 In **Save downloaded files to**, type the storage path for video files downloaded in playback mode or use the **Browse** button.

Picture and Clip Settings

Use this section to set the paths to the storage folders for snapshots and video clips you captured with your web browser.

To set the paths to your storage

1 To set the storage path for pictures manually captured in Live View mode, type the path in the **Save snapshots in live view to** box or use the **Browse** button.

2 In **Save snapshots when playback to**, type the storage path for pictures captured in Playback mode or use the **Browse** button.

3 In **Save clips to**, type the storage path for video clipped in Playback mode or use the **Browse** button.

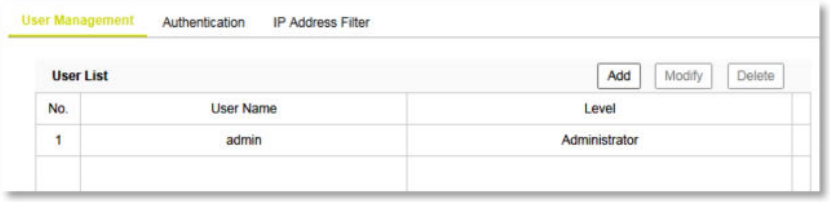
4 Click **Save**.

8 Security

On the Security page, you can manage user accounts, configure authentication settings and enable an IP address filter.

In This Chapter

8.1 User Management



Security > User Management (Administrator account created)

What this tab is for

The User Management tab is the place where the admin user adds, modifies and deletes user accounts.

Admin account

When you connect to the web interface of the camera for the first time, you are prompted to set a password. By supplying a password, you create an account with Administrator level that you can use to add "Operator" and "User" accounts for other users of the camera.

CAUTION: TO KEEP THE ACCOUNT SAFE, SET A STRONG, COMPLEX PASSWORD. THIS HELPS TO PREVENT UNAUTHORISED ACCESS.

To create a strong password

- Use at least eight characters
- Do not include your real name, user name, company name, or other personal information
- Do not use complete words that can be found in a dictionary
- Use a random combination of at least two of the following categories: upper case letters, lower case letters, numbers and special characters

Note: For better protection, especially in high-security systems, we advise you to change the password at regular intervals.

User management

Up to 31 user accounts can be created. Two user levels are available: Operator and User. Per user, different permissions can be assigned.

To add a user account

1 Click **Add**.
2 Type the user name.
3 In the *Level* list, select **Operator** or **User**.
4 Type the password.
For information about strong passwords, see above.
5 Select and/or clear the permissions for the new user, as required.
6 Click **OK**.

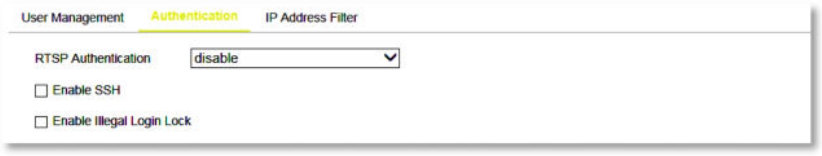
To modify a user account

1 Select the user in the *User List*.
2 Click **Modify**.
3 Change the user name, level or password as needed.
4 Select or clear permissions as needed.
5 Click **OK**.

To delete a user account

1 Select the user in the *User List*.
2 Click **Delete**.
3 Click **OK**.

8.2 Authentication



Security > Authentication

What this tab is for

On the Authentication tab, you can enable/disable the following functions:

- Authentication for users who want to extract an RTSP video stream from the camera
- Access for users who do not have a user account for the camera
- Data communication security
- Illegal login lock

RTSP Authentication

From a security perspective, it may be undesirable that users can freely connect to the camera over RTSP to view a video stream. With RTSP Authentication, it is possible to restrict access to users with a valid account. On attempting to start an RTSP stream, users are prompted to provide a user name and password.

To configure RTSP Authentication

1 In the *RTSP Authentication* list, select **basic** or **disable** as required.
2 Click **Save**.

Important: If you disable RTSP Authentication, anyone can use a connection over RTSP to start a video stream via the IP address of the camera.

Security service

With SSH enabled, the data communication is encrypted and compressed to improve security and reduce the transmission time.

To turn on the security service

1 Select **Enable SSH**.
2 Click **Save**.

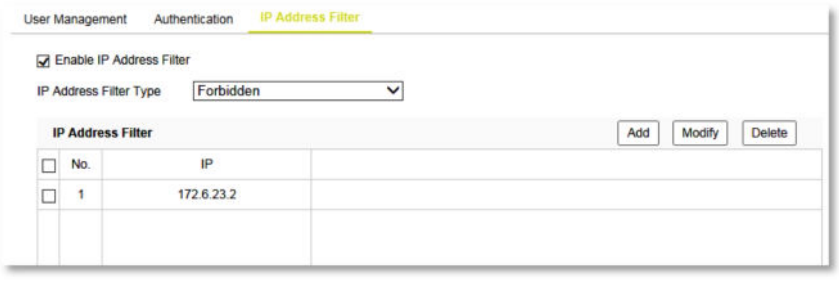
Illegal login prevention

It is possible to have the camera locked if an operator/user user enters an incorrect user name or password for five consecutive times. The admin is locked out after seven failed logon attempts. If the camera is locked, you can try to log on again after 30 minutes.

To turn on the illegal login lock

1 Select **Enable Illegal Login Lock**.
2 Click **Save**.

8.3 IP Address Filter



Security > IP Address Filter

What this tab is for

On the IP Address Filter tab, you can deny/allow access to the camera from specific IP addresses.

To turn on the IP address filter

1 Select **Enable IP Address Filter**.
2 In the *IP Address Filter Type* list, select **Forbidden** or **Allowed**, as required.
Forbidden: Forbid the IP addresses added in the IP Address Filter list to log in.
Allowed: Allow only the IP addresses added in the IP Address Filter list to log in.
3 Set up the *IP Address Filter* list (see below).
4 Click **Save**.

To add an IP address

1 Click **Add**.
2 Type the IP address.
3 Click **OK**.
4 Click **Save**.

To modify an IP address

1 Select the IP address in the list.
2 Click **Modify**.
3 Type the new IP address.
4 Click **OK**.
5 Click **Save**.

To delete an IP address

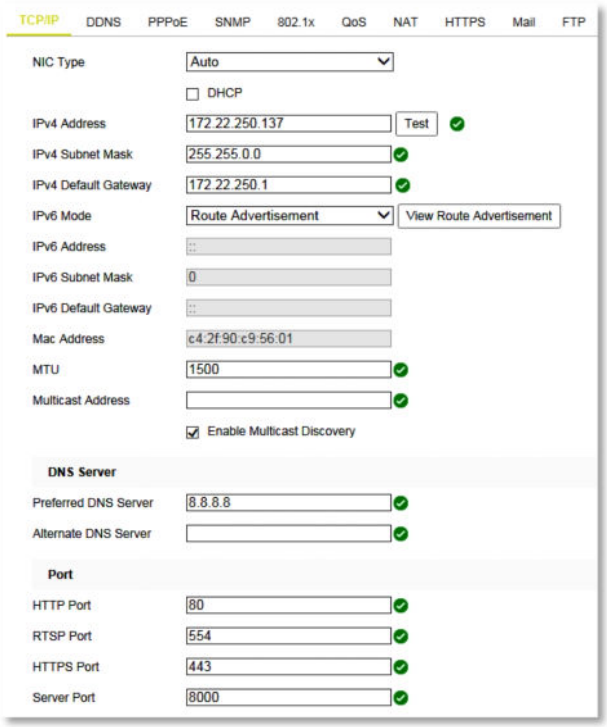
1 Select the check box of the IP address in the list.
To select all IP addresses, click the header row check box.
2 Click **Delete**.
3 Click **Save**.

9 Network

On the Network page, you can configure the TCP/IP, DDNS, SNMP, 802.1X, QoS, NAT, HTTPS, Mail, and FTP settings of the camera.

In This Chapter

9.1 TCP/IP



Network > TCP/IP

What this tab is for

On the TCP/IP tab, you can configure the basic network settings, the DNS server settings and the port settings.

Basic settings

The TCP/IP settings must be properly configured before you operate the camera over the network. The camera supports the IPv4 and IPv6 protocols. Both versions may be configured simultaneously without conflicting each other. At least one IP version should be configured.

To configure the basic network settings

1 In the *NIC Type* list, select the appropriate network adapter type.

2 If the IP address will be assigned via a DHCP server, select **DHCP**.

This makes the IPv4 and DNS Server boxes unavailable.

3 In *IPv4 Address*, type the IP address.

This is the fixed IP address that will be used for the camera.

4 In *IPv4 Subnet Mask*, type the subnet mask.

This is used to determine to what subnet the camera belongs.

5 In *IPv4 Default Gateway*, type the IP address of the default gateway.

This is the device that passes traffic from the local subnet to other subnets and networks.

6 Click **Test**.

This is to determine if the chosen IP address is available on the network.

7 If you use IPv6, select the required mode in the *IPv6 Mode* list.

With Manual mode selected, you need to specify the IP address, subnet mask and default gateway.

If you select Route Advertisement, the router must support this function.

8 In *MTU*, type the Maximum Transmission Unit (MTU) size.

This is the maximum size of an IP packet that can be sent over the network without dividing it into pieces. The valid MTU size range is 1280 ~ 1500. The default value is 1500 (Ethernet). The value you type here must be supported on the other side of the connection.

9 In *Multicast Address*, type the multicast IP address to be used.

Multicast can be used to send a media stream from the camera to a group of interested receivers in a single transmission. The stream is sent to the multicast group address and multiple clients can acquire the stream at the same time by requesting a copy from the multicast group address. The switches and other network devices must be carefully configured for, and capable of handling multicasting and its protocols (most notably IGMP).

10 (Optional) Select **Enable Multicast Discovery**.

If selected, the online network camera can be automatically detected by client software via the private multicast protocol in the Local Area Network (LAN).

11 Click **Save**.

A reboot is required for the settings to take effect.

DNS Server

The Preferred DNS Server is the primary domain name server that translates domain names and host names into the corresponding IP addresses. The Alternate DNS Server is a second domain name server that is used if the Preferred DNS Server is unavailable. Configure the DNS server settings if they are required for specific applications, such as sending email.

To configure the DNS Server settings

1 In *Preferred DNS Server* and *Alternate DNS Server*, type the IP addresses of the two DNS servers.
2 Click **Save**.

Port numbers

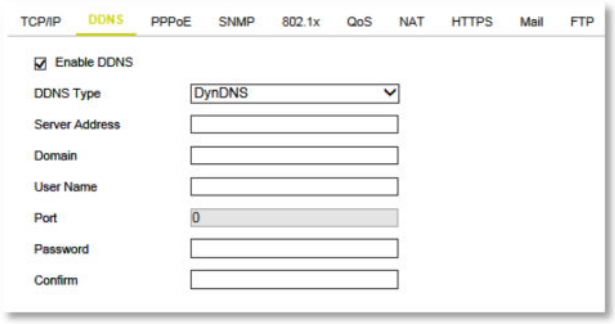
Refer to the following table to change a default port number of the camera.

Port	Default value	Range
HTTP Port	80	Any unoccupied number
RTSP Port	554	1024~65535
HTTPS Port	443	Any unoccupied number
Server Port	8000	2000~65535

To change a port number

1 Replace the current port number with a value from the corresponding range in the table above.
2 Click **Save**.
A reboot is required for the settings to take effect.

9.2 DDNS



Network > DDNS

What this tab is for

If your camera is set to use PPPoE as its default network connection, you can use the DDNS tab to configure the Dynamic DNS (DDNS) for network access.

Note: Registration on the DDNS server is required before you configure the DDNS settings of the camera.

To turn on DDNS

1 Select **Enable DDNS**.
2 In the *DDNS Type* list, select the DDNS type you will be using.
3 Configure the DDNS settings for the selected type as described below .
4 Click **Save**.
A reboot is required for the settings to take effect.

To implement DynDNS

1 In *Server Address*, type the server address of DynDNS (for example, members.dyndns.org).
2 In *Domain*, type the domain name obtained from the DynDNS website.
3 In *User Name*, type the user name registered on the DynDNS website.
4 In *Port*, type the port number of the DynDNS server.
5 In *Password*, type the password registered on the DynDNS website.
6 In *Confirm*, type the same password once more.

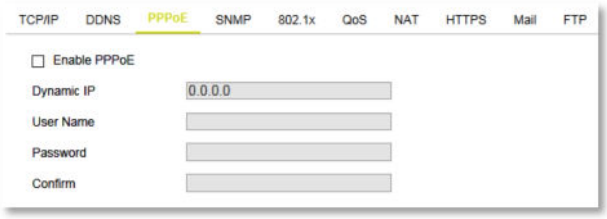
To implement IPServer

- In *Server Address*, type the server address of the IP Server.
To use the IP Server, you have to apply a static IP address, subnet mask, gateway and preferred DNS from the ISP. Under "Server Address" should be entered the static IP address of the computer that runs the IP Server software.

To implement NO-IP

1 In *Server Address*, type the server address as www.noip.com.
2 In *Domain*, type the domain name you registered.
3 In *User Name*, type the user name.
4 In *Port*, type the port number, if needed.
5 In *Password*, type the password.
6 In *Confirm*, type the same password once more.
After clicking *Save*, you can view the camera with the domain name.

9.3 PPPoE



Network > PPPoE

What this tab is for

If you have no router but only a modem, you can use the Point-to-Point Protocol over Ethernet (PPPoE) function. PPPoE enables users to transfer data securely.

To configure PPPoE

1 Select **Enable PPPoE**.

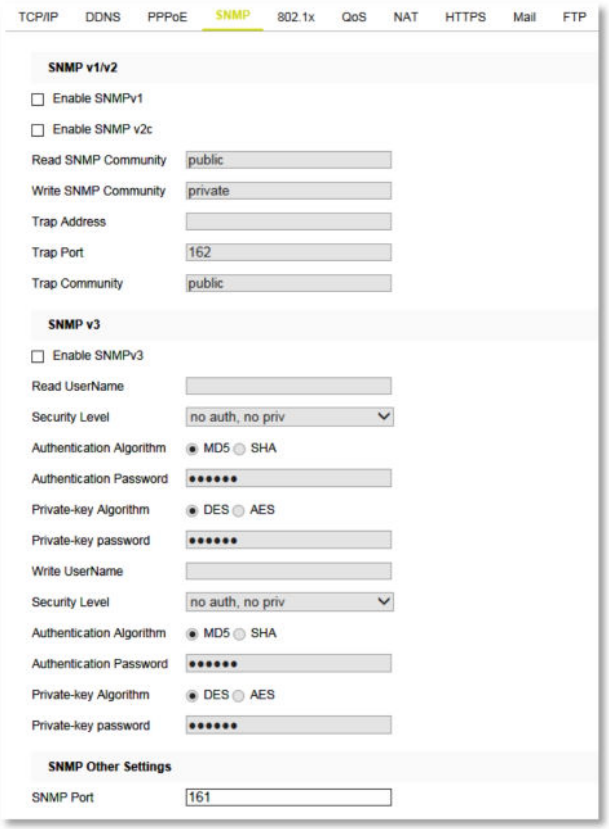
2 For PPPoE access, type the user name and password (2x).

The user name and password should be assigned by your Internet Service Provider (ISP).

3 Click **Save**.

A reboot is required for the settings to take effect.

9.4 SNMP



Network > SNMP

What this tab is for

On the SNMP tab, you can turn on SNMP and configure its settings to get the camera status, parameters and alarm related information and manage the camera remotely when it is connected to the network.

Before you continue

Before you set up SNMP, download and install the SNMP software and configure it to receive the camera information via the SNMP port. By setting the Trap Address, the camera can send the alarm event and exception messages to the surveillance centre.

Note: The SNMP version you select on the SNMP tab should be the same as that of the SNMP software. The SNMP version that you select must meet the security level you require. SNMP v1 provides no security. SNMP v2 requires a password for access. SNMP v3 provides encryption and if you use v3, an HTTPS protocol must be enabled.

To turn on SNMP

1 Select the check box of the required SNMP version.

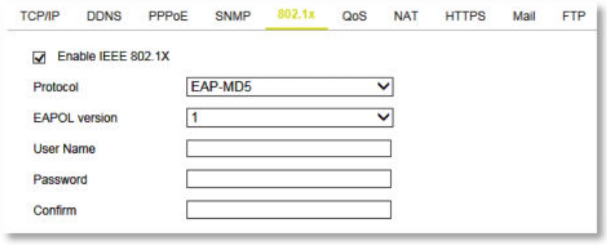
2 Configure the SNMP settings.

The settings you configure here should correspond with the settings of the SNMP software.

3 Click **Save**.

A reboot is required for the settings to take effect.

9.5 802.1X



Network > 802.1X

What this tab is for

The camera supports the IEEE 802.1X standard. IEEE 802.1X is a port-based network access control. It enhances the security level of the LAN. When devices connect to this network with IEEE 802.1X standard, authentication is needed. If the authentication fails, the devices do not connect to the network. On this tab, you can turn on this feature so that the camera data is secured and user authentication is needed when connecting the camera to the network.

Authentication steps

The authentication server must be configured. Apply for and register a user name and password for 802.1X in the server.

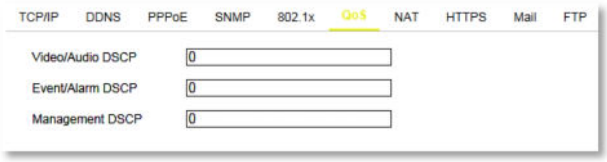
- Before connecting the camera to the protected LAN, request a digital certificate from a Certificate Authority.
- The camera requests access to the protected LAN via the authenticator (a switch).
- The switch forwards the identity and password to the authentication server (RADIUS server).
- The switch forwards the certificate of authentication server to the camera.

- If all the information is validated, the switch allows network access to the protected network.

To turn on IEEE 802.1X

1 Connect the network camera directly to your PC with a network cable.
2 Log on to the camera.
3 Go to the 802.1X tab of the Network page.
4 Select **Enable IEEE 802.1X**.
5 In the *EAPOL version* list, select the version which corresponds with the version of the router or switch.
6 Type the user name and password (issued by the Certificate authority) (2x) to access the server.
7 Click **Save**.
The camera reboots when you save the settings.
8 After the configuration, connect the camera to the protected network.

9.6 QoS



Network > QoS

What this tab is for

On this tab, you can turn on the Quality of Service (QoS) feature which can help solve network delay and network congestion by configuring the priority of data sending.

Differentiated Services Code Point (DSCP)

Differentiated Services (DiffServ, or DS) is a method for adding QoS to IP networks. In routed networks, critical network traffic such as video and audio streams, which require a relatively uninterrupted flow of data, can get blocked due to other traffic. DiffServ can be used to classify network traffic and give precedence - that is, low-latency, guaranteed service, to high-priority traffic.

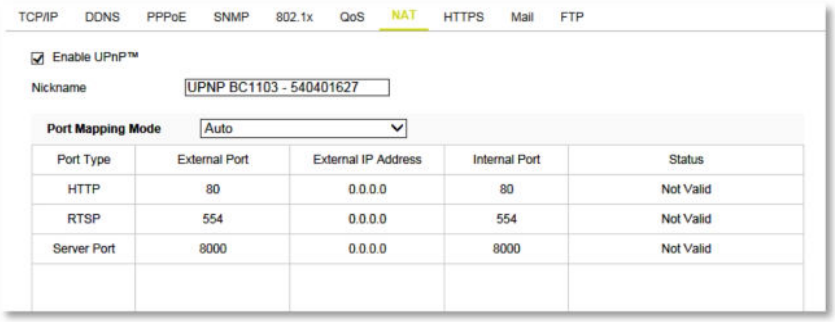
Each stream has a DSCP (Differentiated Services Code Point) field in the IP header. Routers will identify the network service type in the DSCP field and provide the appropriate level of service.

To turn on QoS

1 In *Video/Audio DSCP*, *Event/Alarm DSCP* and *Management DSCP,* type the DSCP value.
The valid range of the DSCP value is 0~63. The higher the DSCP value, the higher the priority.
2 Click **Save**.
A reboot is required for the settings to take effect.

Note: Make sure that you enable the QoS function of your network device (such as a router).

9.7 NAT



Network > NAT

What this tab is for

On this tab, you can turn on UPnP and configure the Network Address Translation (NAT) settings.

Note: With Universal Plug and Play (UPnP™) enabled, you do not need to configure the port mapping for each port. The camera will be connected to the Wide Area Network via the router.

NAT

To add an extra level of security, NAT can translate the IP addresses of computers on the local network to a single IP address. This address is used by the router that connects the computers to the internet. Should computers on the internet try to connect to computers on the local network, they will only "see" the IP address of the router. The router may include firewall functionality which only allows authorised systems to connect to computers on the local network.

UPnP

UPnP is a networking architecture that provides compatibility among networking equipment, software and other hardware devices. The UPnP protocol allows devices to connect seamlessly and to simplify the implementation of the networks in the home and corporate environments.

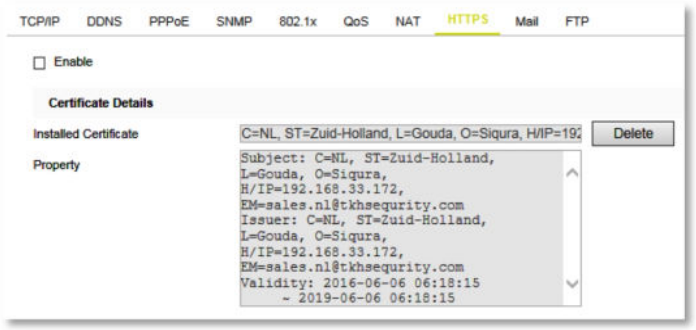
To turn on UPnP

1. Select **Enable UPnP™**.
2. In *Nickname*, type a (user-friendly) name for online detection.
3. Click **Save**.

To configure the NAT settings

1. In the Port Mapping Mode list, select **Auto** or **Manual**.
2. With Manual mode selected, click the table cells you wish to edit and customise the port number values.
3. Click **Save**.

9.8 HTTPS



Network > HTTPS

What this tab is for

On this tab, you can install security certificates to enable secure connections between the camera and web browsers. If, for example, the HTTPS port number is set to 443 and the IP address is 192.168.1.64, you can establish a secure connection to the camera by typing "https://192.168.1.64:443" in the address bar of the web browser.

Secure connections

With HTTPS implemented and used on the camera, a safe exchange of data between the camera and a web browser is ensured. Information transported over the network, such as device settings and credentials, is encrypted to protect it against eavesdropping.

Certificates

To implement HTTPS on the camera, you need to install an HTTPS certificate. You can use a self-signed certificate or one created by a Certificate Authority (CA). CA-issued certificates provide a higher level of security and inspire more trust than self-signed certificates. Self-signed certificates are often installed for test purposes or as a temporary solution until a CA-issued certificate has been obtained.

To create a self-signed certificate

1. To turn on HTTPS, select **Enable**.
2. Select **Create Self-signed Certificate**.
   If you already have a certificate installed, the *Install Certificate* section is hidden. You can display it by deleting the current certificate.
3. Click **Create**.
4. Refer the table below and type the required information in the text boxes.
5. Click **OK**.
   The certificate information is shown in the HTTPS tab after you successfully created the certificate.
6. Click **Save**.

Item	Description
Country	Two-letter country code (where the certificate is to be used)
Hostname/IP	Host name or IP address of the device to be certified
Validity	Valid period (in days) of the certificate
Password	(Strong) Password
State or province	Administrative region in which the organisation is located
Locality	City/Location where the organisation is based
Organization	Name of the organisation which owns the device
Organizational Unit	Name of the organisational unit which owns the device
Email	Contact email address

To create an authorised certificate request

1 To turn on HTTPS, select **Enable**.

2 Select **Create the certificate request first ...**.

If you already have a certificate installed, the *Install Certificate* section is hidden. You can display it by deleting the current certificate.

3 Click **Create**.

4 Refer the table below and type the required information in the text boxes.

5 Click **OK** to save the information.

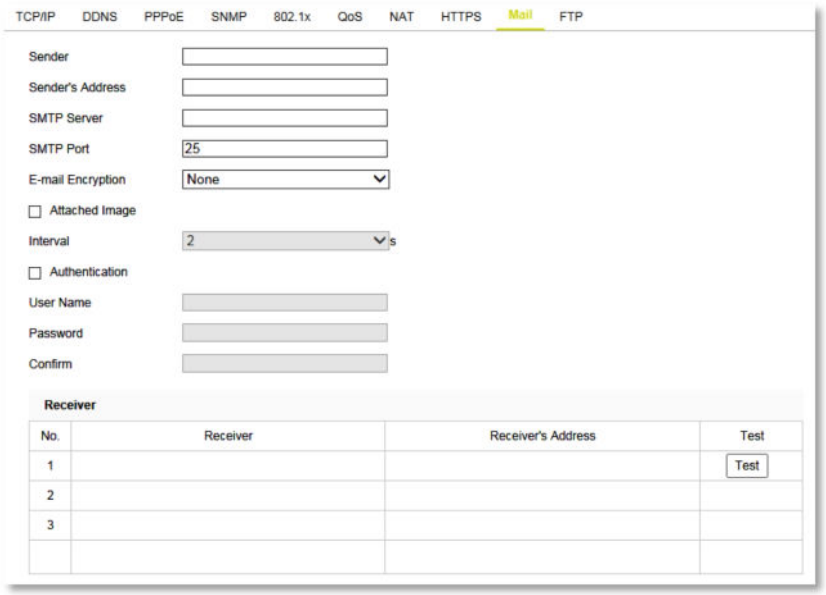
6 Click **Download**.

7 Save the certificate request.

8 Send the request to a certificate authority.

Item	Description
Country	Two-letter country code (where the certificate is to be used)
Hostname/IP	Host name or IP address of the device to be certified
Password	(Strong) Password
State or province	Administrative region in which the organisation is located
Locality	City/Location where the organisation is based
Organization	Name of the organisation which owns the device
Organizational Unit	Name of the organisational unit which owns the device
Email	Contact email address

9.9 Mail



Network > Mail

What this tab is for

The system can be configured to send an email notification to all designated receivers if an alarm event, such as a motion detection, video loss or video tampering event, is detected.

Before you continue

Go to the TCP/IP tab of the Network page and make sure that the IPv4 address, the IPv4 subnet mask, the IPv4 default gateway and the preferred DNS server are set correctly.

To configure the email settings

1 In *Sender*, type the name of the email sender.

2 In *Sender's Address*, type the email address of the sender.

3 In *SMTP Server*, type the IP address or host name of the SMTP server (for example, smtp.263xmail.com)

4 In *SMTP Port*, type the port number of the SMTP port.

The default TCP/IP port for SMTP is 25 (not secured). The SSL SMTP port is 465.

5 In the *E-mail Encryption* list, select **SSL**, if this is required by the SMTP server.

6 Select **Attached Image**, if you want to send emails with attached alarm images.

7 In the *Interval* list, select the required interval (in seconds).

The interval refers to the time between two actions of sending attached pictures.

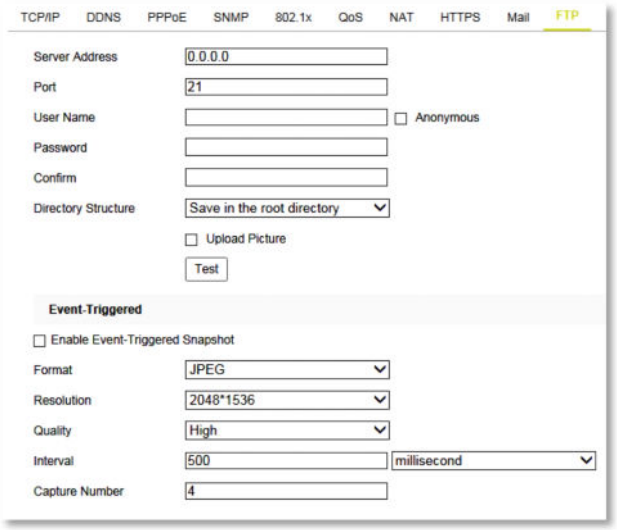
8 If your email server requires authentication, select **Authentication**.

Users will be prompted for the logon user name and password to log on to the server.

9 In the *Receiver* table, type the details of up to three receivers who are to be notified of the alarm.

10 Click **Save**.

9.10 FTP



Network > FTP

What this tab is for

On the FTP tab, you can configure the FTP server related information to enable the uploading of captured pictures to the FTP server. Captures can be triggered by events or a timing snapshot task.

To configure the FTP server settings

1 In *Server Address*, type the IP address of the FTP server.

2 In *Port*, type the port number used on the FTP server.

The FTP protocol typically uses port 21 on the FTP server to listen for clients initiating a connection. Port 21 is also where the server is listening for commands issued to it.

3 In *User Name*, *Password* and *Confirm*, type the authorisation needed to get access to the FTP server.

The target FTP server must hold a user account associated with the camera.

If the FTP server supports anonymous access, you can select **Anonymous**. Authorisation details are not required then.

4 In the *Directory Structure* list, select the **root**, **parent** or **child** directory.

This sets the folder on the FTP server assigned to the FTP client.

Root: The files are saved to the root folder of the server.

Parent: The files are saved to a folder on the FTP server. To define the folder name, use the Device Name, Device Number, Device IP or a custom name.

Child: The files are saved to a subfolder of the parent directory on the FTP server. To define the folder name, use the Camera Name, Camera Number or a custom name.

5 To enable the uploading of picture captures to the FTP server, select **Upload Picture**.

6 To test your settings. click **Test**.

7 Click **Save**.

To configure event-triggered snapshots

1 Select **Enable Event-Triggered Snapshot**.

2 In the *Quality* list, select the picture quality to be used.

3 In *Interval*, type the interval (in seconds or milliseconds) to be applied between uploads.

4 In *Capture Number*, type the number of captures to be uploaded per event.
Range: 1~120.

5 Click **Save**.

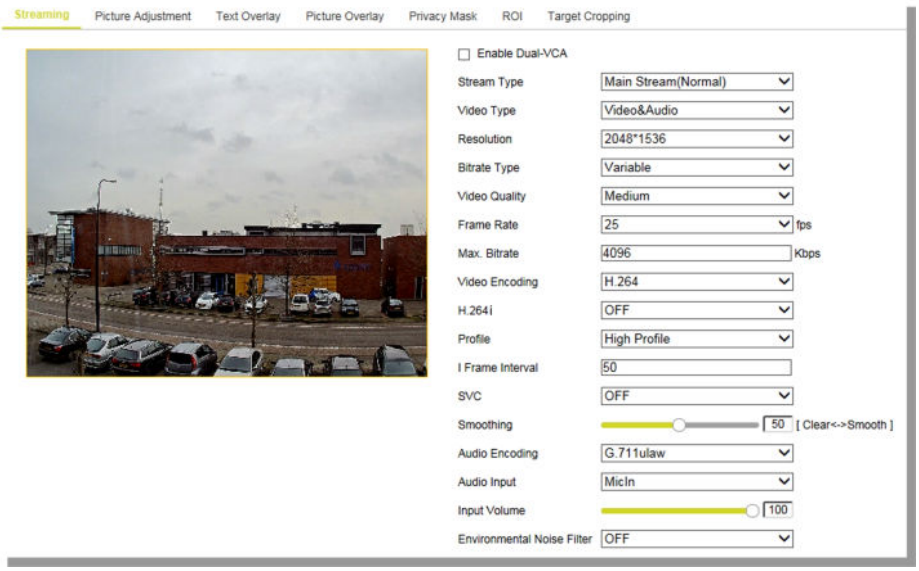
Note: If you want to upload captured pictures to the FTP server, you have to enable the timing snapshot on the Capture tab of the Storage page or event-triggered snapshot on the page of the specific event.

10 Video/Audio

On the Video/Audio page, you can configure the settings for video and audio streaming, picture adjustment, text and picture overlays, privacy masks, the region of interest (ROI), and target cropping.

In This Chapter

10.1 Streaming



Video/Audio > Streaming

What this tab is for

On the Streaming tab, you can select a stream type and configure the associated video and audio streaming settings.

To configure video streaming

1 Select **Enable Dual-VCA** if you want information of objects (for example, human, vehicle, etc.) highlighted in the video stream.

2 In the *Stream Type* list, select **Main Stream**, **Sub stream** or **Third Stream**.

The main stream is usually for recording and live viewing with good bandwidth, whereas the sub stream and third stream can be used for live viewing when the bandwidth is limited.

3 In the *Video Type* list, select **Video&Audio** or **Video stream**.

The audio signal is recorded only if Video&Audio is selected.

4 In the *Resolution* list, select the required resolution for the video output.

5 In the *Bitrate Type* list, select **Variable** or **Constant**.

Constant bit rate mode (CBR) is generally safest. Although the image quality may vary, the network load generated will remain fairly constant.

If constant picture quality is required and a varying network load will pose no problems, choose Variable bit rate mode (VBR). Video streaming is generally smoother under VBR.

6 In the *Video Quality* list, select a video quality level.

The Video Quality list is available if the bit rate type is set to Variable.

Note that higher video quality levels require more bandwidth.

7 In the *Frame Rate* list, select a frame rate for the stream.

The frame rate determines the frequency at which the video stream is updated. It is expressed in frames per second (fps). A higher frame rate is advantageous when there is movement in the video stream, as it maintains the image quality throughout.

8 In the *Max. Bitrate* list, enter a value for the maximum bit rate to be allowed.

Higher values will give a higher video quality, but more bandwidth is required.

Note that the available values in this list can vary per camera model.

9 In the *Video Encoding* list, select the encoding mode - that is, the method used to compress the video input signal.

Note that the available encoding modes (for example H.264, MPEG-4 and MJPEG) vary per camera model and per stream type.

10 In the *H.264i* list, select **ON** or **OFF**.

If you set the stream type to *Main Stream* and if you select *H.264* for the video coding, you will see that the H.264i setting is available. H.264i is an advanced compression coding technology. By enabling H.264i, the user can calculate the HDD consumption by its average bit rate, and save storage by lowering the bit rate. You need to reboot the camera if you want to turn on or turn off H.264i.

If H.264i is enabled and the Bitrate Type is set to *Variable*, you can configure the average bit rate and you can calculate the HDD consumption according to the average bit rate, or you can set the average bit rate manually, which should be smaller than the Max. Bitrate.

Note that the Max. Bitrate setting is unavailable if Bitrate Type is set to *Variable*. The Video Quality, Profile, I Frame Interval and SVC are unavailable if you set Bitrate Type to *Constant*.

If H.264i is enabled, some functions, including ROI, Clipping, Third Stream, Smart Event, Display Info. On Stream, Counting, and Rotation are not supported.

11 In the *Profile* list, select **Basic Profile**, **Main Profile** or **High Profile**.

These profiles are available in H.264 encoding mode.

12 In *I Frame Interval*, type the required value.

Range: 1~400. This setting determines the distance in frames between two I-frames.

13 In the *SVC* list, select **ON**, **Auto** or **OFF**.

Scalable Video Coding (SVC) is an extension of the H.264/AVC standard.

ON: Turns on the SVC function.

OFF: Turns off the SVC function.

Auto: The camera automatically extracts frames from the original video if the network bandwidth is insufficient.

14 Drag the **Smoothing** slider to control the smoothness of the stream.

The higher the smoothing value, the better the fluency of the stream will be. The video quality may not be satisfactory, though.

The lower the smoothing value, the higher the quality of the stream will be. It may not appear as fluent, though.

15 Click **Save**.

To configure audio streaming

1 In the *Audio Encoding* list, select the mode to be used.

G.722.1, G.711 ulaw, G.711alaw, G.726, MP2L2 and PCM are selectable. For MP2L2, the sampling rate and audio stream bitrate are configurable. For PCM, the sampling rate can be set.

2 In the *Audio Input* list, select the required input.

MicIn and LineIn are selectable for a connected microphone and intercom, respectively.

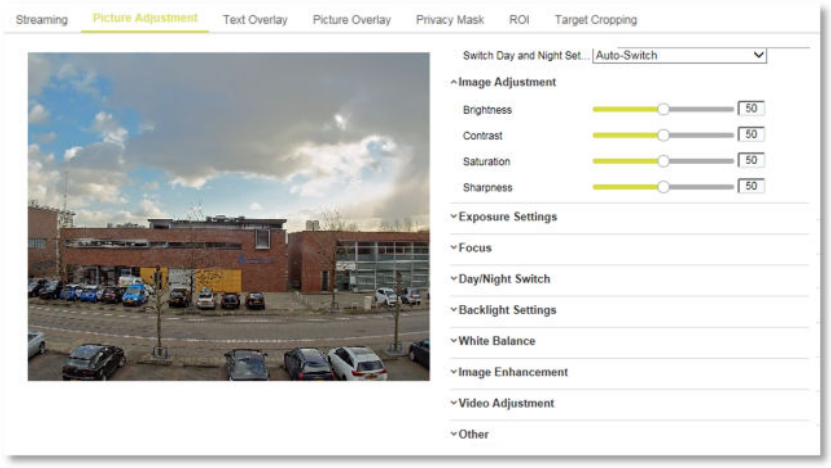
3 Drag the **Input Volume** slider to control the volume of the audio input.

4 In the *Environmental Noise Filter* list, select **ON** or **OFF**.

With this function turned on, the noise in the environment can be filtered to some extent.

5 Click **Save**.

10.2 Picture Adjustment



Video/Audio > Picture Adjustment

What this tab is for

On this tab, you can set the image quality of the camera, including brightness, contrast, saturation, hue, sharpness, etc. You can double-click the live view to enter fullscreen mode. Double-click again to exit.

Note: The display parameters vary per camera model. Refer to the actual interface for details.

Day/Night switching

To guarantee the image quality in different illuminations, the camera provides two sets of parameters for the user to configure.

- Day/Night Auto-Switch settings
- Day/Night Scheduled Switch settings

Day/Night Auto-Switch settings

The settings described in the following paragraphs are available if you select Auto-Switch.

Image Adjustment

Use the Image Adjustment sliders to adjust the image quality. Range: 1~100. Default value: 50.

- **Brightness**: Controls the brightness level of the image.
- **Contrast**: Controls the contrast level of the image - that is, the difference in brightness between the light and dark areas of an image.
- **Saturation**: Controls the intensity (purity) of the colours in the image.
- **Sharpness**: Controls the clarity of detail perceived in an image.

Exposure Settings

If the camera is equipped with a fixed lens, only *Manual* is selectable and *Iris Mode* is not configurable.

If *Auto* is selected, you can set the auto iris level from 0~100.

For the camera which supports P-Iris lens, if P-Iris lens is adopted, then the P-Iris lens type is selectable, e.g.: Tamron 2.8-8 mm F1.2 (M13VP288-IR), or if a DC lens is adopted, then *Manual* and *Auto* are selectable.

The exposure time refers to the electronic shutter time, which ranges from 1~1/100,000 s. Adjust it according to the actual luminance condition.

Focus Settings

If the camera supports an electronic lens, you can set the focus mode to *Auto*, *Manual* or *Semi-auto*.

- **Auto**: The focus is adjusted automatically according to the actual monitoring scenario.
- **Manual**: You can control the lens by adjusting the zoom, focus, lens initialisation, and auxiliary focus via the PTZ control interface.
- **Semi-auto**: The camera focuses automatically when you adjust the zoom parameters.

Day/Night Switch

Use this section to select the Day/Night switch mode and to configure the smart IR settings.

- **Day**: The camera stays in day mode.
- **Night**: The camera stays in night mode.
- **Auto**: The camera switches automatically between day mode and night mode according to the illumination. The sensitivity ranges from 0~7. The higher the value, the easier the mode switches. The filtering time refers to the interval time between the day/night switch. You can set it from 5 s to 120 s.
- **Schedule**: Set the start time and the end time to define the duration for day/night mode.

- **Triggered by alarm input**: This switch is triggered by alarm input, and you can set the trigger mode to day or night.
- **Smart Supplement Light**: On cameras with IR LEDs, the Smart Supplement Light function gives users an option to adjust the power of the IR LED to provide a clear image that is not overexposed or too dark. Select *ON* to enable the smart IR. This makes *Auto* is selectable for the IR mode.

  In *AUTO* mode, the power of the IR LED changes automatically according to the actual luminance. For example, if the current scene is bright enough, the IR LED adjusts itself to lower power. If the scene is not bright enough, the IR LED adjusts itself to higher power.

  In *Manual* mode, you can manually set the value of the distance between the IR camera and the object, to adjust the power of the IR LED. A small distance value indicates that the object is near the IR camera, and the device adjusts the IR LED to lower power to avoid overexposure. A large distance value indicates that the object is far away, and the device adjusts the IR LED to higher power to avoid a too dark image.

Backlight Settings

If you focus on an object against strong backlight, the object will be too dark to be seen clearly. Backlight Compensation (BLC) compensates the light to the object in the front to make it clear.

- **BLC Area**: Select an area from the list. As an alternative, you can select **Custom**, click **Draw Area**, and then drag your mouse pointer across the camera view to create a custom area. With OFF selected, the WDR setting is available.
- **WDR**: The wide dynamic range (WDR) function helps the camera provide clear images when there are both very bright and very dark areas simultaneously in the field of view. WDR balances the brightness level of the whole image to provide clear images with details. Use the slider to set the WDR level.
- **HLC**: Highlight compensation (HLC) makes the camera identify and suppress strong light sources in a scene. This makes it possible to see image detail that would normally be hidden.

White Balance

The White Balance is the white rendition function of the camera used to adjust the colour temperature according to the environment.

Image Enhancement

This section includes the Digital Noise Reduction, Defog and Gray Scale settings.

- **Digital Noise Reduction**: Reduces the noise in the video stream. Options: *OFF*, *Normal* and *Expert*. Noise reduction level range: 0~100. Default value: 50 in Normal Mode. In Expert mode, you can set the Space DNR Level [0~100] and the Time DNR Level [0~100].
- **Defog Mode**: Enhances the subtle details so that the image appears clearer. You can turn on the defog function when the environment is foggy and the image is misty.
- **Gray Scale**: Controls the gray scale of the image. Range: [0~235] or [16~235].

Video Adjustment

This section offers the following functionality:

- **Mirror**: Mirrors the image so you can see it inversed. Options: *Left/Right*, *Up/Down*, *Center*, and *OFF*.
- **Rotate**: To make a complete use of the 16:9 aspect ratio, you can turn on the *Rotate* function when you use the camera in a narrow view scene. When installing the camera, turn it to 90 degrees or rotate the 3-axis lens to 90 degrees and set the Rotate Mode to *ON*. You will get a normal view of the scene with a 9:16 aspect ratio to ignore the needless information such as the wall and get more meaningful information of the scene.
- **Scene Modes**: Select *Indoor* or *Outdoor* according to the actual environment.

- **Video Standard**: Options: PAL(50HZ) and NTSC(60HZ). Select the applicable video standard according to the video system in your country.
- **Capture Mode**: Is the selectable video input mode to meet the different demands of the field of view and the resolution.
- **Lens Distortion Correction**: (On cameras which support this function) Can correct the distorted image caused by a wide-angle lens, if turned on.

Other

Video output may vary per camera model. Some of the cameras support CVBS, SDI, or HDMI output. Refer to the actual camera model for details.

- **Local Output**: Select ON to enable analogue video output via the BNC connector on the back panel of the camera.

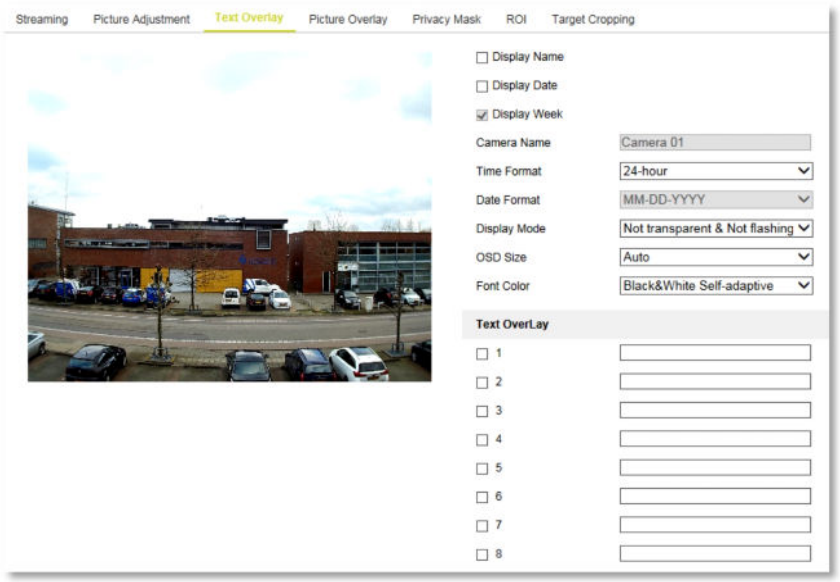
Day/Night Scheduled-Switch

The Day/Night scheduled-switch configuration interface enables you to set separate camera parameters for day and night to guarantee the image quality in different illuminations.

To configure the Scheduled-Switch settings

1 In *Start Time* and *End Time*, enter the start and end time of the switch.
2 Click **Common**.
3 Configure the common settings applicable to the day mode and the night mode.
For information about each setting, see the description of the Day/Night Auto-Switch mode.
4 Click **Day**.
5 Configure the settings applicable to the day mode.
6 Click **Night**.
7 Configure the settings applicable to the night mode.
The settings are saved automatically as you make changes.

10.3 Text Overlay



Video/Audio > Text Overlay

What this tab is for

On the Text Overlay tab, you can add and edit information for On-Screen Display (OSD).

OSD Items

The camera name, date and time information and custom text overlays can be superimposed onto the video images.

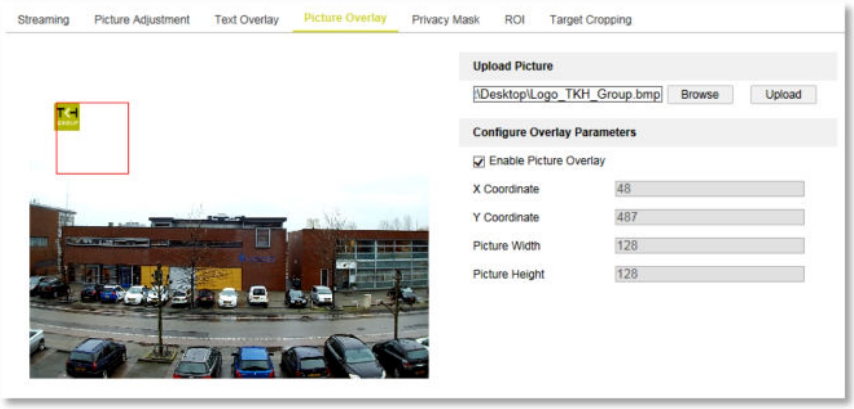
To add the camera name and date/time information

1 Select **Display Name**, **Display Date** and **Display Week** as needed.
2 In *Camera Name*, type the camera name.
3 In the *Time Format*, *Date Format*, *Display Mode*, *OSD Size* and *Font Color* lists, select the required formatting.
4 In the *Live View* window, drag the OSD frame to position it as needed.
5 Click **Save**.

To add a text overlay

1 Select the overlay you wish to add.
2 In the overlay text box, type the text to be displayed.
3 In the *Live View* window, drag the OSD frame to position it as needed.
4 Click **Save**.

10.4 Picture Overlay



Video/Audio > Picture Overlay

What this tab is for

On the Picture Overlay tab, you can superimpose a picture onto the video images. This enables you to add a company logo to the images, for example.

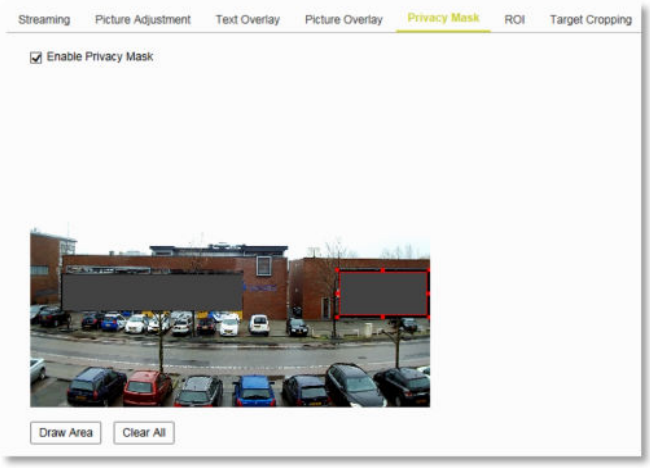
Picture requirements

The picture must be in RGB24 bmp format and the maximum size of the picture is 128*128 pixels.

To add a picture

1 To select a picture, click **Browse**.
2 Locate the picture and select it.
3 Click **Upload**.
4 Select **Enable Picture Overlay**.
5 In the *Live View* window, drag the OSD frame to position it as needed.
6 Click **Save**.
The X Coordinate and Y Coordinate values indicate the location of the picture in the image. The Picture Width and Height show the size of the picture.

10.5 Privacy Mask



Video/Audio > Privacy Mask

What this tab is for

On the Privacy Mask tab, you can superimpose privacy masks onto the video images. This makes it possible to cover certain areas on the live video to prevent certain spots in the surveillance area from being live viewed and recorded.

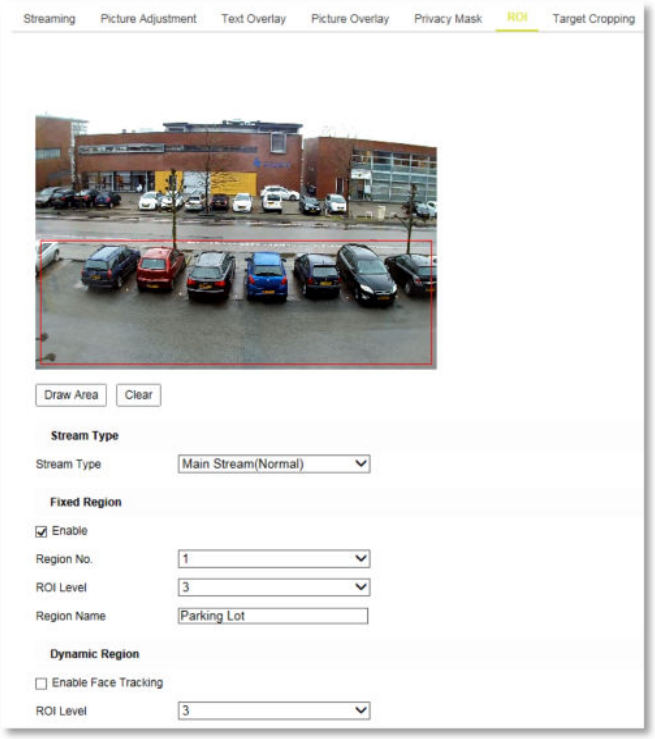
To add a privacy mask

1 Select **Enable Privacy Masks**.
2 Click **Draw Area**.
3 Drag your mouse pointer across the *Live View* window to draw the mask area.
You can drag the sizing handles to resize the area. If necessary, drag the area to position it correctly.
4 Click **Stop Drawing**.
- or -
Click **Clear All** to remove all of the areas you set without saving them.
5 Click **Add**.
The privacy mask is saved and added to the Privacy Mask List.
6 (Optional) In the **Name** box, type a name for the mask.
7 Click **Save**.

To delete a privacy mask

1 In the *Privacy Mask List*, select the mask.
2 Click **Delete**.

10.6 ROI



Video/Audio > ROI

What this tab is for

On the ROI tab, you can draw a Region of Interest (ROI). ROI encoding helps to discriminate the ROI and background information in video compression, which means, the technology assigns more encoding resources to the region of interest. This increases the quality of the ROI, whereas the background information is less focused. Note that the ROI function varies per camera model.

Region types

You can configure Fixed Region settings and Dynamic Region settings.

- Fixed Region: Using fixed region encoding you can configure an area manually. You can select an image quality enhancing level and also name the ROI area.
- Dynamic Region: The region with motion is automatically calculated.

To configure a fixed region for ROI

1 In the *Stream Type* list, select the stream for ROI encoding.
2 In the *Region No.* list, select a region number.
3 Under *Fixed Region*, select **Enable**.
4 Click **Draw Area**.
5 Drag your mouse pointer across the *Live View* window to draw the region.
6 (Optional) Drag the region to position it correctly.
7 Click **Stop Drawing**.
8 In the *ROI Level* list, select the image quality level.
The higher the value, the better the image quality.

9 In *Region Name*, type a name for the region.

10 Click **Save**.

To remove a fixed region

1 In the *Region No.* list, select the region.

2 Click **Clear**.

3 To confirm, click **OK**.

To configure a dynamic region for ROI

1 In the *Stream Type* list, select the stream for ROI encoding.

2 (Optional) **Select Face Tracking**.

The captured face picture is set as a region of interest. When the face detection is triggered, the image quality of the face will be increased.

Note that the face detection function must be supported and turned on, to enable the face tracking function.

3 (Optional) Select **Enable License Plate Tracking**.

The captured license plate picture is set as a region of interest. When the license plate tracking is triggered, the image quality of the license plate will be increased.

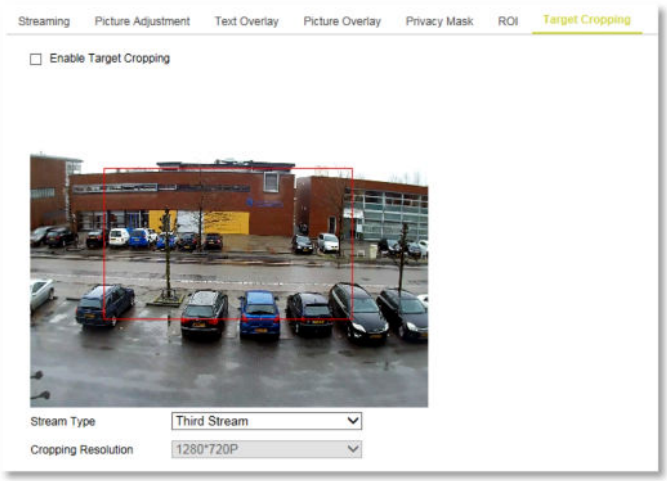
Note that the vehicle detection function must be supported and turned on, to enable the license plate tracking function.

4 In the *ROI Level* list, select the image quality level.

The higher the value, the better the image quality.

5 Click **Save**.

10.7 Target Cropping



Video/Audio > Target Cropping

What this tab is for

On the *Target Cropping* tab, you can specify a target area on the live video. The area can then be displayed via the third stream in a specific resolution, providing more details of the target area if needed. Note that the Target Cropping function can vary per camera model.

To configure target cropping

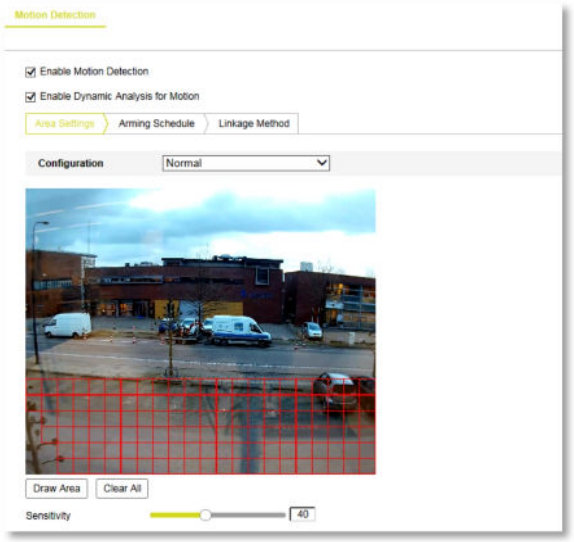
1 Select **Enable Target Cropping**.
2 In the *Stream Type* list, select **Third Stream**.
3 In the *Cropping Resolution* list, select the cropping resolution for the video display of the target area.
A red rectangle is displayed on the live video to mark the target area.
4 Drag the rectangle to position the target area as desired.
5 Click **Save**.
6 On the **Live View** page, click the **Stream Type** list in the *Toolbar*.
7 Click **Third Stream**.
The Live View window displays the video within the target area.

11 Events

This section explains how to configure the network camera to respond to events, such as motion detection, video tampering, alarm input, alarm output, and exception. These events can trigger the linkage methods, such as Notify Surveillance Center, Send Email, Upload to FTP, Trigger Alarm Output, and Trigger Cannel.

In This Chapter

11.1 Motion Detection



Events > Motion Detection

What this tab is for

Motion Detection detects moving objects in the configured surveillance area. A series of actions can be taken when an alarm is triggered. On the Motion Detection tab, you can turn on Motion Detection and configure the settings of this function.

Modes

To detect moving objects accurately and reduce the false alarm rate, the following configuration modes are available for different motion detection environments:

- Normal configuration
- Expert configuration

Normal mode

The Normal configuration mode adopts the same set of motion detection parameters in the daytime and at night. It involves the following steps:

1 On the *Area Settings* tab, you define the area to be monitored.
2 On the *Arming Schedule* tab, you define when you want the function to be active.
3 On the *Linkage Method* tab, you define the action(s) to be taken when an event occurs.

To set the motion detection area

1 Select **Enable Motion Detection**.
2 If you want to have detected objects marked by green rectangles, select **Enable Dynamic Analysis for Motion**.
Note: If you do not want the detected objected marked by the rectangles, go to *System > Local Configuration > Live View Parameters > Rules*, and then select **Disable**.
3 On the *Area Settings* tab, click **Draw Area**.
4 Drag your mouse pointer across the *Live View* window to draw a detection area.
5 Click **Stop Drawing** to finish the drawing of one area.
6 (Optional) Click **Clear All** to delete all areas.

7 (Optional) Drag the slider to set the sensitivity of the detection.
The higher the value, the more easily the alarm will be triggered.

8 Click **Save**.

To set the arming schedule

1 On the *Arming Schedule* tab, drag your mouse pointer across the required day(s) to set the arming schedule.
A Copy button appears as you move your pointer across the schedule. You can click it to copy the settings of a specific day to another day.
You can click a time section to edit, save or delete it.

2 Click **Save**.

To set the alarm actions

1 On the *Linkage Method* tab, select the required actions (see descriptions below).
Options: *Send Email*, *Notify Surveillance Center*, *Upload to FTP*, *Trigger Alarm Output*, *Trigger Channel*.

2 Click **Save**.

Send Email

Send an email with alarm information to a user or users when an event occurs. Before emails can be sent, the related settings on the Mail tab of the Network page must be correctly and completely configured.

Notify Surveillance Center

Send an exception or alarm signal to remote management software when an event occurs.

Upload to FTP

Capture the image when an alarm is triggered and upload the picture to an FTP server. Before images can be uploaded, the related settings on the FTP tab of the Network page and on the Capture tab of the Storage page must be correctly and completely configured. The captured image can also be uploaded to the available SD card or network disk.

Trigger Alarm Output

Trigger one or more external alarm outputs when an event occurs. Before the output can be triggered, the related settings on the Alarm Output tab of the Events page must be correctly and completely configured.

Trigger Channel

Video is recorded when an event occurs. Before recording can start, the recording schedule on the Record Schedule tab of the Storage page must be set.

Expert mode

Expert mode is mainly used to configure the sensitivity and proportion of the object in relation to the area, per available Day/Night Settings switch.

To configure settings in Expert mode

1 Select the Switch Day and Night Setting.
OFF: disables the day and night switch.
Auto-Switch: automatically switches the day and night mode according to the illumination.
Scheduled-Switch: enables you to set a start and end time.

2 In the *Area* list, select the area number.

3 Draw the detection area as described for the normal configuration mode.

Up to eight areas are supported.

4 Drag the **Sensitivity and Percentage** sliders to adjust the sensitivity and proportion of the object in relation to the area.

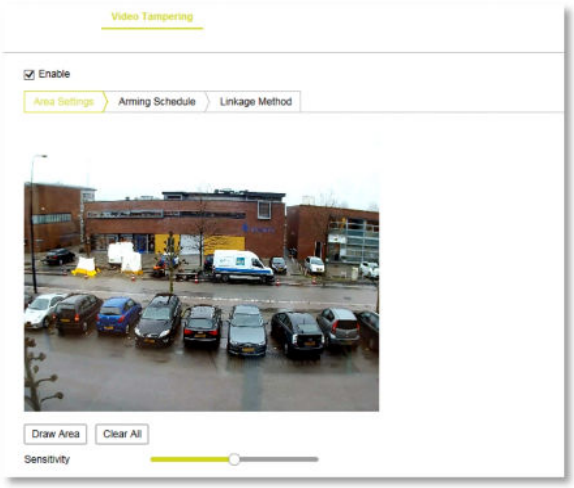
Sensitivity: The higher the value, the more easily the alarm will be triggered.

Percentage: When the size proportion of the moving object exceeds the predefined value, the alarm is triggered. The lower the value, the more easily the alarm will be triggered.

5 Set the arming schedule and linkage method as in the normal configuration mode.

6 Click **Save**.

11.2 Video Tampering



Events > Video Tampering

What this tab is for

On the Video Tampering tab, you can configure the camera to raise an alarm when the lens is covered and to link specific response actions to such an event.

Steps

Video Tampering configuration involves the following steps:

1 On the *Area Settings* tab, you define the area to be monitored.

2 On the *Arming Schedule* tab, you define the period(s) when you want the function to be active.

3 On the *Linkage Method* tab, you define the action(s) to be taken when an event occurs.

To set the video tampering detection area

1 Select **Enable**.

2 On the *Area Settings* tab, click **Draw Area**.

3 Drag your mouse pointer across the *Live View* window to draw a detection area.

4 (Optional) Drag the sizing handles to resize the area.

5 (Optional) Drag the area to position it correctly.
6 Click **Stop Drawing** to finish the drawing of one area.
7 (Optional) Click **Clear All** to delete all areas.
8 (Optional) Drag the slider to set the sensitivity of the detection.
9 Click **Save**.

To set the arming schedule

1 On the *Arming Schedule* tab, drag your mouse pointer across the required day(s) to set the arming schedule.

A Copy button appears as you move your pointer across the schedule. You can click it to copy the settings of a specific day to another day.

You can click a time section to edit, save or delete it.

2 Click **Save**.

To set the alarm actions

1 On the *Linkage Method* tab, select the required actions (see descriptions below).

Options: *Send Email*, *Notify Surveillance Center*, *Trigger Alarm Output*.

2 Click **Save**.

Send Email

Send an email with alarm information to a user or users when an event occurs. Before emails can be sent, the related settings on the Mail tab of the Network page must be correctly and completely configured.

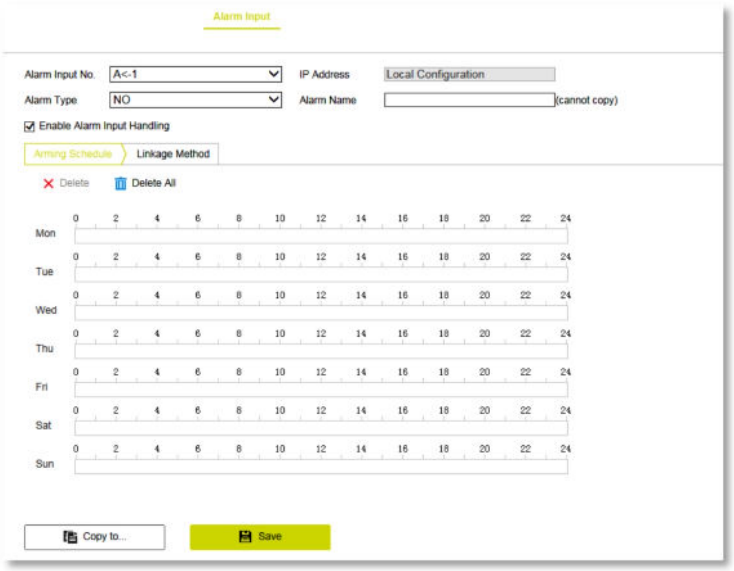
Notify Surveillance Center

Send an exception or alarm signal to remote management software when an event occurs.

Trigger Alarm Output

Trigger one or more external alarm outputs when an event occurs. Before the output can be triggered, the related settings on the Alarm Output tab of the Events page must be correctly and completely configured.

11.3 Alarm Input



Events > Alarm Input

What this tab is for

The camera has alarm input functionality for alarm application. On the Alarm Input tab, you can enable alarm input handling and configure the related settings.

Steps

Alarm Input configuration involves the following steps:

1 On the *Alarm Input* tab, you enable alarm input handling.

2 On the *Arming Schedule* tab, you define the period(s) when you want the function to be active.

3 On the *Linkage Method* tab, you define the action(s) to be taken when an event occurs.

To enable alarm input handling

1 In the *Alarm Input No.* list, select the input number.

2 In the *Alarm Type* list, select **NO** (Normally Open) or **NC** (Normally Closed).

3 (Optional) In *Alarm Name*, type a name for the alarm input.

4 Select **Enable Alarm Input Handling**.

To set the arming schedule

1 On the *Arming Schedule* tab, drag your mouse pointer across the required day(s) to set the arming schedule.

A Copy button appears as you move your pointer across the schedule. You can click it to copy the settings of a specific day to another day.

You can click a time section to edit, save or delete it.

2 Click **Save**.

To set the alarm actions

1 On the *Linkage Method* tab, select the required actions (see descriptions below).

Options: *Send Email*, *Notify Surveillance Center*, *Upload to FTP*, *Trigger Alarm Output*, *Trigger Channel*.

2 Click **Save**.

Send Email

Send an email with alarm information to a user or users when an event occurs. Before emails can be sent, the related settings on the Mail tab of the Network page must be correctly and completely configured.

Notify Surveillance Center

Send an exception or alarm signal to remote management software when an event occurs.

Upload to FTP

Capture the image when an alarm is triggered and upload the picture to an FTP server. Before images can be uploaded, the related settings on the FTP tab of the Network page and on the Capture tab of the Storage page must be correctly and completely configured. The captured image can also be uploaded to the available SD card or network disk.

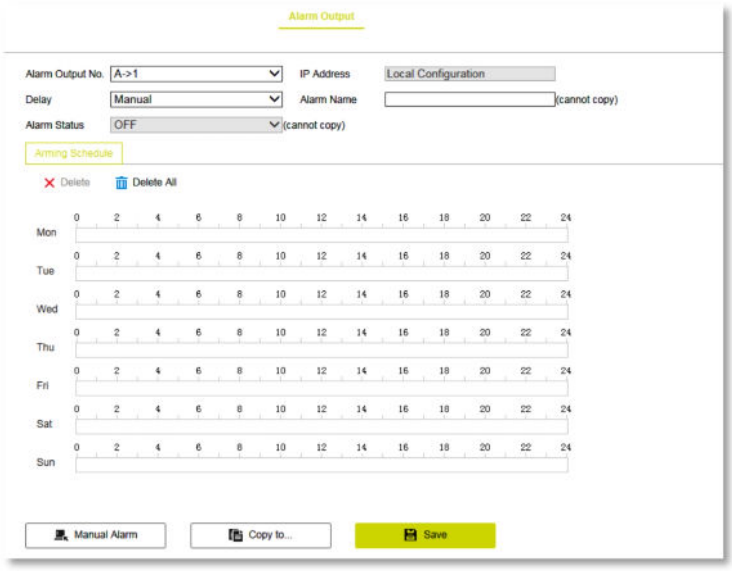
Trigger Alarm Output

Trigger one or more external alarm outputs when an event occurs. Before the output can be triggered, the related settings on the Alarm Output tab of the Events page must be correctly and completely configured.

Trigger Channel

Video is recorded when an event occurs. Before recording can start, the recording schedule on the Record Schedule tab of the Storage page must be set.

11.4 Alarm Output



Events > Alarm Output

What this tab is for

The camera has alarm output functionality for alarm application. On the Alarm Output tab, you can configure the related settings and activate/deactivate a manual alarm.

To configure the Alarm Output settings

1 In the *Alarm Output No.* list, select the alarm output channel.

2 (Optional) In *Alarm Name*, type a name for the output.

3 In the *Delay* list, select a delay time.

The delay time indicates the time span during which the alarm output remains active after the alarm occurs.

4 On the *Arming Schedule* tab, drag your mouse pointer across the required day(s) to set the arming schedule.

A Copy button appears as you move your pointer across the schedule. You can click it to copy the settings of a specific day to another day.

You can click a time section to edit, save or delete it.

5 (Optional) You can copy your settings to other alarm outputs.

6 Click **Save**.

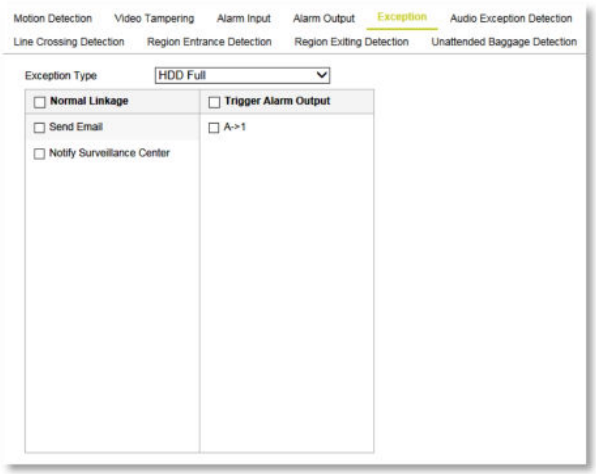
To activate a manual alarm

- Click **Manual Alarm**.

  The Alarm Status changes to ON.

  The alarm remains active until you click Clear Alarm.

11.5 Exception



Events > Exception

What this tab is for

On the Exception tab, you can link actions to the occurrence of an Exception Alarm. The exception type can be HDD Full, HDD Error, Network Disconnected, IP address Conflicted and Illegal Login to the camera.

To set the actions for exception alarms

1 In the *Exception Type* list, select the exception you need to configure.

2 Select the required actions (see descriptions below).
Options: *Send Email*, *Notify Surveillance Center*, *Trigger alarm Output*.

3 Click **Save**.

4 Repeat steps 1-3 for other exception types you need to configure.

Send Email

Send an email with alarm information to a user or users when an event occurs. Before emails can be sent, the related settings on the Mail tab of the Network page must be correctly and completely configured.

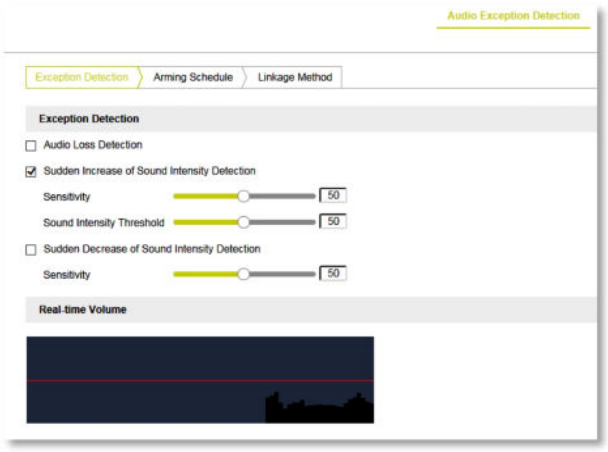
Notify Surveillance Center

Send an exception or alarm signal to remote management software when an event occurs.

Trigger Alarm Output

Trigger one or more external alarm outputs when an event occurs. Before the output can be triggered, the related settings on the Alarm Output tab of the Events page must be correctly and completely configured.

11.6 Audio Exception Detection



Events > Audio Exception Detection

What this tab is for

The Audio Exception Detection function detects abnormal sounds in the surveillance scene, such as the sudden increase or decrease of the sound intensity. Specific actions can be taken when the alarm is triggered. Note that the Audio Exception Detection function varies per camera model.

Steps

Audio Exception Detection configuration involves the following steps:

1 On the *Exception Detection* tab, you activate and configure the detection of sudden changes in sound.

2 On the *Arming Schedule* tab, you define the period(s) when you want the function to be active.

3 On the *Linkage Method* tab, you define the action(s) to be taken when an event occurs.

To set up audio exception detection

- (Optional) On the *Audio Exception Detection* tab, select **Audio Loss Detection** to enable the audio loss detection function.
- (Optional) Select **Sudden Increase of Sound Intensity Detection** to detect a steep rise in sound in the surveillance scene.

  Drag the sliders to set the detection sensitivity and threshold (see also below) for the steep rise in sound.
- (Optional) Select **Sudden Decrease of Sound Intensity Detection** to detect a steep drop in sound in the surveillance scene.

  Drag the slider to set the detection sensitivity (see also below) for the steep drop in sound.
- Click **Save**.

  The real-time sound volume is shown in the graph.

Sensitivity

Sensitivity range: [1-100]. The smaller the value, the more severe the change should be to trigger the detection.

Sound Intensity Threshold

Sound Intensity Threshold range: [1-100]. It can filter the sound in the environment. The louder the environmental sound, the higher the value should be. You can adapt the threshold to the actual environment.

To set the arming schedule

1 On the *Arming Schedule* tab, drag your mouse pointer across the required day(s) to set the arming schedule.

A Copy button appears as you move your pointer across the schedule. You can click it to copy the settings of a specific day to another day.

You can click a time section to edit, save or delete it.

2 Click **Save**.

To set the alarm actions

1 On the *Linkage Method* tab, select the required actions (see descriptions below).

Options: *Send Email*, *Notify Surveillance Center*, *Trigger Alarm Output*, *Trigger Channel*.

2 Click **Save**.

Send Email

Send an email with alarm information to a user or users when an event occurs. Before emails can be sent, the related settings on the Mail tab of the Network page must be correctly and completely configured.

Notify Surveillance Center

Send an exception or alarm signal to remote management software when an event occurs.

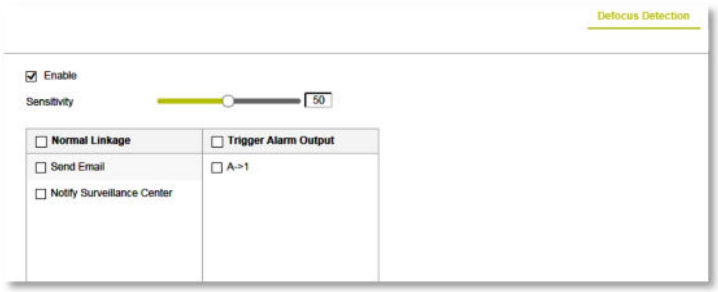
Trigger Alarm Output

Trigger one or more external alarm outputs when an event occurs. Before the output can be triggered, the related settings on the Alarm Output tab of the Events page must be correctly and completely configured.

Trigger Channel

Video is recorded when an event occurs. Before recording can start, the recording schedule on the Record Schedule tab of the Storage page must be set.

11.7 Defocus Detection



Events > Defocus Detection

What this tab is for

The image blur caused by the defocusing of the lens can be detected. On the Defocus Detection tab, you can turn on the detection and define actions to be taken when the the event occurs.

To set up defocus detection

1 Select **Enable**.

2 Drag the slider to set the detection sensitivity.

The sensitivity value ranges from 1 to 100. The higher the value, the more easily the defocus image can trigger the alarm.

3 Select the required actions (see descriptions below).

Options: *Send Email*, *Notify Surveillance Center*, *Focus*, *Trigger alarm Output*.

4 Click **Save**.

Send Email

Send an email with alarm information to a user or users when an event occurs. Before emails can be sent, the related settings on the Mail tab of the Network page must be correctly and completely configured.

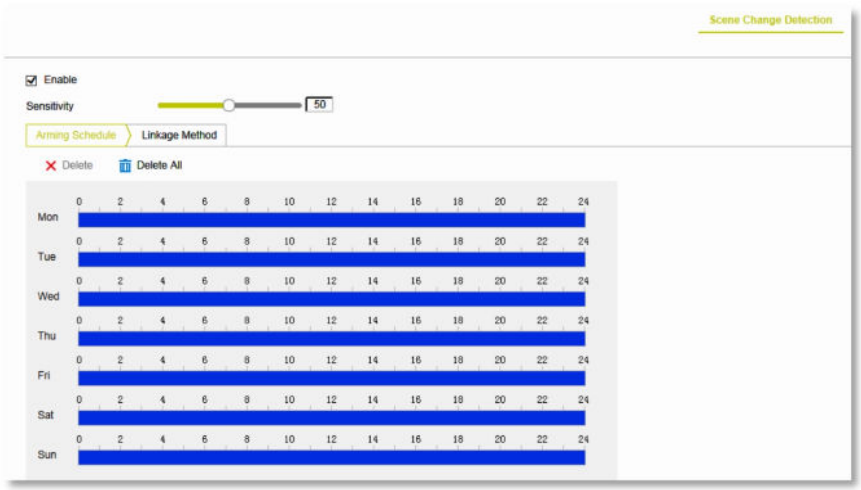
Notify Surveillance Center

Send an exception or alarm signal to remote management software when an event occurs.

Trigger Alarm Output

Trigger one or more external alarm outputs when an event occurs. Before the output can be triggered, the related settings on the Alarm Output tab of the Events page must be correctly and completely configured.

11.8 Scene Change Detection



Events > Scene Change Detection

What this tab is for

Scene Change Detection detects changes of the surveillance environment caused by external factors, such as the intentional rotation of the camera. On the Scene Change Detection tab, you can turn on the detection and define actions to be taken when the event occurs. Note that Scene Change Detection varies per camera model.

Steps

1 On the *Scene Change Detection* tab, you enable the function and set the sensitivity.
2 On the *Arming Schedule* tab, you define the period(s) when you want the function to be active.
3 On the *Linkage Method* tab, you define the action(s) to be taken when an event occurs.

To enable scene change detection

1 Select **Enable** to enable the function.
2 Drag the slider to set the sensitivity.

The sensitivity value ranges from 1 to 100. The higher the value, the more easily the change of scene can trigger the alarm.

To set the arming schedule

1 On the *Arming Schedule* tab, drag your mouse pointer across the required day(s) to set the arming schedule.

A Copy button appears as you move your pointer across the schedule. You can click it to copy the settings of a specific day to another day.

You can click a time section to edit, save or delete it.

2 Click **Save**.

To set the alarm actions

1 On the *Linkage Method* tab, select the required actions (see descriptions below).

Options: *Send Email*, *Notify Surveillance Center*, *Upload to FTP*, *Trigger Alarm Output*, *Trigger Channel*.

2 Click **Save**.

Send Email

Send an email with alarm information to a user or users when an event occurs. Before emails can be sent, the related settings on the Mail tab of the Network page must be correctly and completely configured.

Notify Surveillance Center

Send an exception or alarm signal to remote management software when an event occurs.

Upload to FTP

Capture the image when an alarm is triggered and upload the picture to an FTP server. Before images can be uploaded, the related settings on the FTP tab of the Network page and on the Capture tab of the Storage page must be correctly and completely configured. The captured image can also be uploaded to the available SD card or network disk.

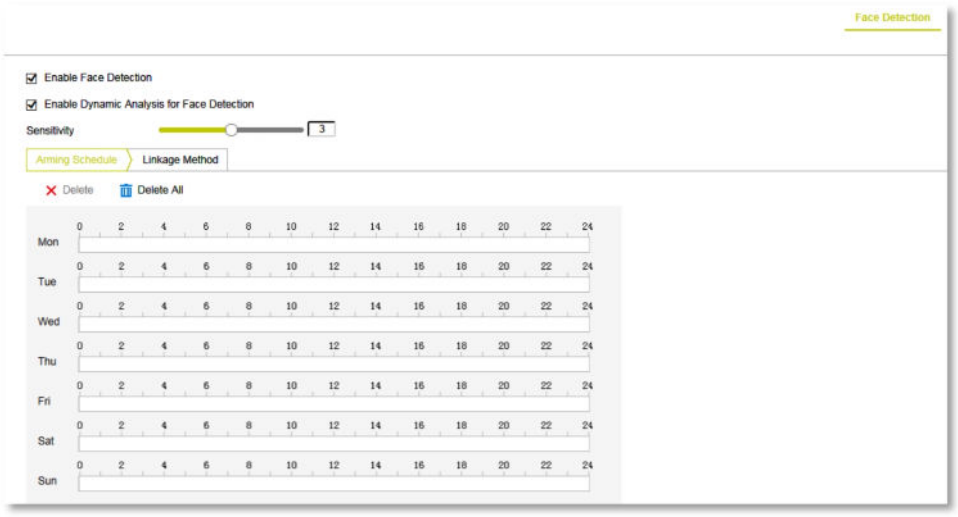
Trigger Alarm Output

Trigger one or more external alarm outputs when an event occurs. Before the output can be triggered, the related settings on the Alarm Output tab of the Events page must be correctly and completely configured.

Trigger Channel

Video is recorded when an event occurs. Before recording can start, the recording schedule on the Record Schedule tab of the Storage page must be set.

11.9 Face Detection



Events > Face Detection

What this tab is for

The Face Detection function detects a face appearing in the surveillance scene. On the Face Detection tab, you can turn on the detection and define actions to be taken when the event occurs. Note that Face Detection varies per camera model.

Steps

1 On the *Face Detection* tab, you enable the function and set the sensitivity.

2 On the *Arming Schedule* tab, you define the period(s) when you want the function to be active.

3 On the *Linkage Method* tab, you define the action(s) to be taken when an event occurs.

To enable face detection

1 Select **Enable Face Detection** to enable the function.

2 If you want to have detected objects marked by green rectangles, select **Enable Dynamic Analysis for Face Detection**.

Note: If you do not want the detected objected marked by the rectangles, go to *System > Local Configuration > Live View Parameters > Rules*, and then select **Disable**.

3 Drag the slider to set the sensitivity.

The sensitivity value ranges from 1 to 5. The higher the value, the more easily the face can be detected.

To set the arming schedule

1 On the *Arming Schedule* tab, drag your mouse pointer across the required day(s) to set the arming schedule.

A Copy button appears as you move your pointer across the schedule. You can click it to copy the settings of a specific day to another day.

You can click a time section to edit, save or delete it.

2 Click **Save**.

To set the alarm actions

1 On the *Linkage Method* tab, select the required actions (see descriptions below).

Options: *Send Email*, *Notify Surveillance Center*, *Upload to FTP*, *Trigger Alarm Output*, *Trigger Channel*.

2 Click **Save**.

Send Email

Send an email with alarm information to a user or users when an event occurs. Before emails can be sent, the related settings on the Mail tab of the Network page must be correctly and completely configured.

Notify Surveillance Center

Send an exception or alarm signal to remote management software when an event occurs.

Upload to FTP

Capture the image when an alarm is triggered and upload the picture to an FTP server. Before images can be uploaded, the related settings on the FTP tab of the Network page and on the Capture tab of the Storage page must be correctly and completely configured. The captured image can also be uploaded to the available SD card or network disk.

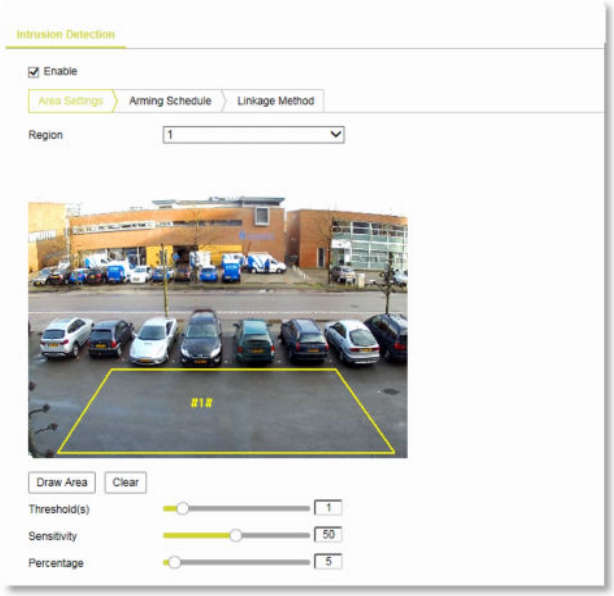
Trigger Alarm Output

Trigger one or more external alarm outputs when an event occurs. Before the output can be triggered, the related settings on the Alarm Output tab of the Events page must be correctly and completely configured.

Trigger Channel

Video is recorded when an event occurs. Before recording can start, the recording schedule on the Record Schedule tab of the Storage page must be set.

11.10 Intrusion Detection



Events > Intrusion Detection

What this tab is for

The Intrusion detection function detects people, vehicles or other objects which enter and loiter in a predefined virtual region longer than the set duration. On the Intrusion Detection tab, you can enable and set up the function, and define the actions to be taken when the alarm is triggered.

Steps

Intrusion Detection configuration involves the following steps:

1 On the *Area Settings* tab, you define the area to be monitored.
2 On the *Arming Schedule* tab, you define the period(s) when you want the function to be active.
3 On the *Linkage Method* tab, you define the action(s) to be taken when an event occurs.

To set the intrusion detection area(s)

1 Select **Enable**.
2 On the *Area Settings* tab, click to open the **Region** list.
3 Select the region you want to create.
4 Click **Draw Area**.
5 Left-click in the Live Video window to set the first of the four vertexes of the detection area.
6 Move the mouse pointer to the next vertex.
7 Left-click to set the second vertex.
8 In the same way, set vertexes three and four.
9 Right-click to complete your drawing.
10 Click **Stop Drawing**.
11 Drag the **Threshold(s)** slider to set the time threshold.

Range: [0 s ~ 10 s]. This is the threshold for the duration of the object loitering in the region. If you set the value to 0, the alarm is triggered immediately after the object has entered the region.

12 Drag the **Sensitivity** slider to set the sensitivity of the detection.

Range: [1~100]. The value of the sensitivity defines the size of the object which can trigger the alarm. If the sensitivity is high, a very small object can trigger the alarm.

13 Drag the **Percentage** slider to set the ratio of the in-region part of the object which can trigger the alarm.

For example, if the percentage is set as 50%, when the object enters the region and occupies half of the whole region, the alarm is triggered.

14 Repeat steps 3-13 to configure other regions.

Up to 4 regions can be set. You can click Clear to delete all existing regions.

15 Click **Save**.

To set the arming schedule

1 On the *Arming Schedule* tab, drag your mouse pointer across the required day(s) to set the arming schedule.

A Copy button appears as you move your pointer across the schedule. You can click it to copy the settings of a specific day to another day.

You can click a time section to edit, save or delete it.

2 Click **Save**.

To set the alarm actions

1 On the *Linkage Method* tab, select the required actions (see descriptions below).

Options: *Send Email*, *Notify Surveillance Center*, *Upload to FTP*, *Trigger Alarm Output*, *Trigger Channel*.

2 Click **Save**.

Send Email

Send an email with alarm information to a user or users when an event occurs. Before emails can be sent, the related settings on the Mail tab of the Network page must be correctly and completely configured.

Notify Surveillance Center

Send an exception or alarm signal to remote management software when an event occurs.

Upload to FTP

Capture the image when an alarm is triggered and upload the picture to an FTP server. Before images can be uploaded, the related settings on the FTP tab of the Network page and on the Capture tab of the Storage page must be correctly and completely configured. The captured image can also be uploaded to the available SD card or network disk.

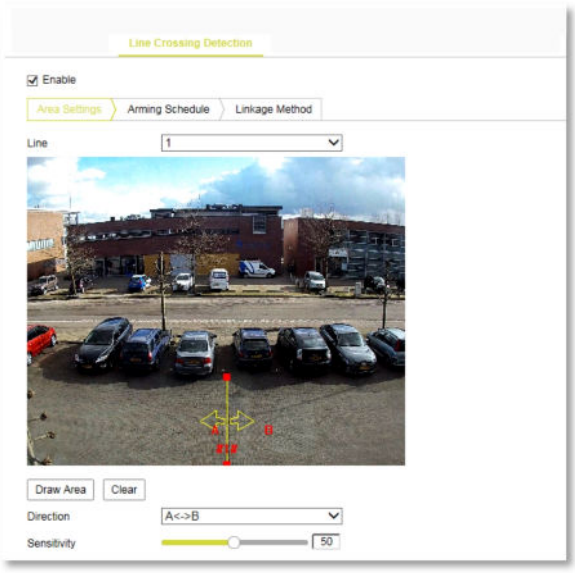
Trigger Alarm Output

Trigger one or more external alarm outputs when an event occurs. Before the output can be triggered, the related settings on the Alarm Output tab of the Events page must be correctly and completely configured.

Trigger Channel

Video is recorded when an event occurs. Before recording can start, the recording schedule on the Record Schedule tab of the Storage page must be set.

11.11 Line Crossing Detection



Events > Line Crossing Detection

What this tab is for

The Line Crossing Detection function detects people, vehicles or other objects which cross a predefined virtual line. On the Line Crossing Detection tab, you can enable and set up the function, and define the actions to be taken when the alarm is triggered. Note that this function varies per camera model.

Steps

Line Crossing Detection configuration involves the following steps:

1 On the *Area Settings* tab, you draw and configure the virtual line to be monitored.

2 On the *Arming Schedule* tab, you define the period(s) when you want the function to be active.

3 On the *Linkage Method* tab, you define the action(s) to be taken when an event occurs.

To draw the virtual line(s)

1 Select **Enable**.

2 On the *Area Settings* tab, click to open the **Line** list.

3 Select the line you want to create.

4 Click **Draw Area**.

A virtual line is displayed in the centre of the Live View window.

5 Drag the line to move it to the required position.

6 Drag the sizing handles to resize the line.

7 In the *Direction* list, select a direction for the line crossing detection.

A<->B: Objects crossing the line from A to B, and objects crossing from B to A can be detected.

A->B: Objects crossing from A to B can be detected.

B->A: Objects crossing from B to A can be detected.

8 Drag the **Sensitivity** slider to set the sensitivity of the detection.

Range: [1-100]. The higher the value, the more easily the line crossing action can be detected.

9 Repeat the steps above to configure other lines.

Up to 4 lines can be set. You can click Clear to delete all existing lines.

10 Click **Save**.

To set the arming schedule

1 On the *Arming Schedule* tab, drag your mouse pointer across the required day(s) to set the arming schedule.

A Copy button appears as you move your pointer across the schedule. You can click it to copy the settings of a specific day to another day.

You can click a time section to edit, save or delete it.

2 Click **Save**.

To set the alarm actions

1 On the *Linkage Method* tab, select the required actions (see descriptions below).

Options: *Send Email*, *Notify Surveillance Center*, *Upload to FTP*, *Trigger Alarm Output*, *Trigger Channel*.

2 Click **Save**.

Send Email

Send an email with alarm information to a user or users when an event occurs. Before emails can be sent, the related settings on the Mail tab of the Network page must be correctly and completely configured.

Notify Surveillance Center

Send an exception or alarm signal to remote management software when an event occurs.

Upload to FTP

Capture the image when an alarm is triggered and upload the picture to an FTP server. Before images can be uploaded, the related settings on the FTP tab of the Network page and on the Capture tab of the Storage page must be correctly and completely configured. The captured image can also be uploaded to the available SD card or network disk.

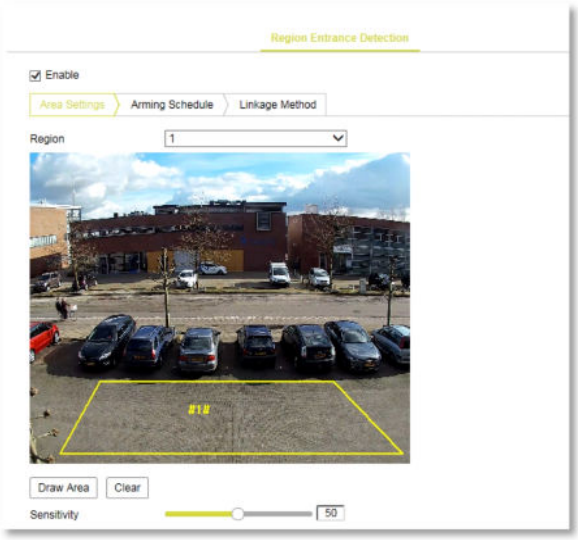
Trigger Alarm Output

Trigger one or more external alarm outputs when an event occurs. Before the output can be triggered, the related settings on the Alarm Output tab of the Events page must be correctly and completely configured.

Trigger Channel

Video is recorded when an event occurs. Before recording can start, the recording schedule on the Record Schedule tab of the Storage page must be set.

11.12 Region Entrance Detection



Events > Region Entrance Detection

What this tab is for

The Region Entrance Detection function detects people, vehicles or other objects that enter a predefined virtual region from outside this region. On the Region Entrance Detection tab, you can enable and set up the function, and define the actions to be taken when the alarm is triggered. Note that this function varies per camera model.

Steps

Region Entrance Detection configuration involves the following steps:

1 On the *Area Settings* tab, you define the area to be monitored.
2 On the *Arming Schedule* tab, you define the period(s) when you want the function to be active.
3 On the *Linkage Method* tab, you define the action(s) to be taken when an event occurs.

To set the region entrance detection area(s)

1 Select **Enable**.
2 On the *Area Settings* tab, click to open the **Region** list.
3 Select the region you want to create.
4 Click **Draw Area**.
5 Left-click in the Live Video window to set the first of the four vertexes of the detection area.
6 Move the mouse pointer to the next vertex.
7 Left-click to set the second vertex.
8 In the same way, set vertexes three and four.
9 Right-click to complete your drawing.
10 Click **Stop Drawing**.
11 Drag the **Sensitivity** slider to set the sensitivity of the detection.
Range: [1-100]. The value of the sensitivity defines the size of the object which can trigger the alarm. If the sensitivity is high, a very small object can trigger the alarm.

12 Repeat the steps above to configure other regions.

Up to 4 regions can be set. You can click Clear to delete all existing regions.

13 Click **Save**.

To set the arming schedule

1 On the *Arming Schedule* tab, drag your mouse pointer across the required day(s) to set the arming schedule.

A Copy button appears as you move your pointer across the schedule. You can click it to copy the settings of a specific day to another day.

You can click a time section to edit, save or delete it.

2 Click **Save**.

To set the alarm actions

1 On the *Linkage Method* tab, select the required actions (see descriptions below).

Options: *Send Email*, *Notify Surveillance Center*, *Upload to FTP*, *Trigger Alarm Output*, *Trigger Channel*.

2 Click **Save**.

Send Email

Send an email with alarm information to a user or users when an event occurs. Before emails can be sent, the related settings on the Mail tab of the Network page must be correctly and completely configured.

Notify Surveillance Center

Send an exception or alarm signal to remote management software when an event occurs.

Upload to FTP

Capture the image when an alarm is triggered and upload the picture to an FTP server. Before images can be uploaded, the related settings on the FTP tab of the Network page and on the Capture tab of the Storage page must be correctly and completely configured. The captured image can also be uploaded to the available SD card or network disk.

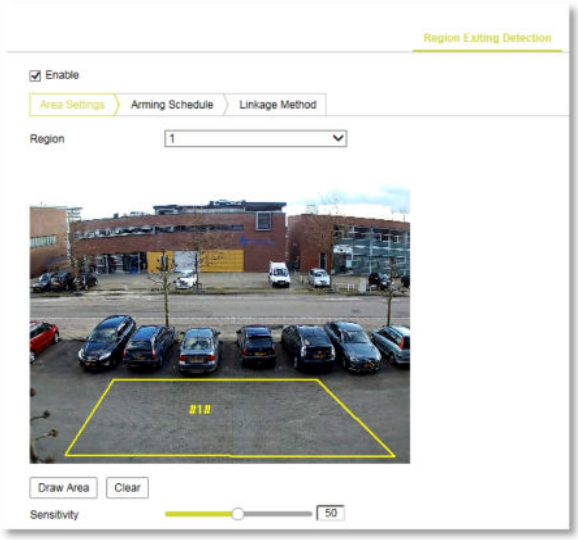
Trigger Alarm Output

Trigger one or more external alarm outputs when an event occurs. Before the output can be triggered, the related settings on the Alarm Output tab of the Events page must be correctly and completely configured.

Trigger Channel

Video is recorded when an event occurs. Before recording can start, the recording schedule on the Record Schedule tab of the Storage page must be set.

11.13 Region Exiting Detection



Events > Region Exiting Detection

What this tab is for

The Region Exiting Detection function detects people, vehicles or other objects that exit a predefined virtual region. On the Region Exiting Detection tab, you can enable and set up the function, and define the actions to be taken when the alarm is triggered. Note that this function varies per camera model.

Steps

Region Exiting Detection configuration involves the following steps:

1 On the *Area Settings* tab, you define the area to be monitored.
2 On the *Arming Schedule* tab, you define the period(s) when you want the function to be active.
3 On the *Linkage Method* tab, you define the action(s) to be taken when an event occurs.

To set the region exiting detection area(s)

1 Select **Enable**.
2 On the *Area Settings* tab, click to open the **Region** list.
3 Select the region you want to create.
4 Click **Draw Area**.
5 Left-click in the Live Video window to set the first of the four vertexes of the detection area.
6 Move the mouse pointer to the next vertex.
7 Left-click to set the second vertex.
8 In the same way, set vertexes three and four.
9 Right-click to complete your drawing.
10 Click **Stop Drawing**.
11 Drag the **Sensitivity** slider to set the sensitivity of the detection.
Range: [1-100]. The value of the sensitivity defines the size of the object which can trigger the alarm. If the sensitivity is high, a very small object can trigger the alarm.

12 Repeat the steps above to configure other regions.

Up to 4 regions can be set. You can click Clear to delete all existing regions.

13 Click **Save**.

To set the arming schedule

1 On the *Arming Schedule* tab, drag your mouse pointer across the required day(s) to set the arming schedule.

A Copy button appears as you move your pointer across the schedule. You can click it to copy the settings of a specific day to another day.

You can click a time section to edit, save or delete it.

2 Click **Save**.

To set the alarm actions

1 On the *Linkage Method* tab, select the required actions (see descriptions below).

Options: *Send Email*, *Notify Surveillance Center*, *Upload to FTP*, *Trigger Alarm Output*, *Trigger Channel*.

2 Click **Save**.

Send Email

Send an email with alarm information to a user or users when an event occurs. Before emails can be sent, the related settings on the Mail tab of the Network page must be correctly and completely configured.

Notify Surveillance Center

Send an exception or alarm signal to remote management software when an event occurs.

Upload to FTP

Capture the image when an alarm is triggered and upload the picture to an FTP server. Before images can be uploaded, the related settings on the FTP tab of the Network page and on the Capture tab of the Storage page must be correctly and completely configured. The captured image can also be uploaded to the available SD card or network disk.

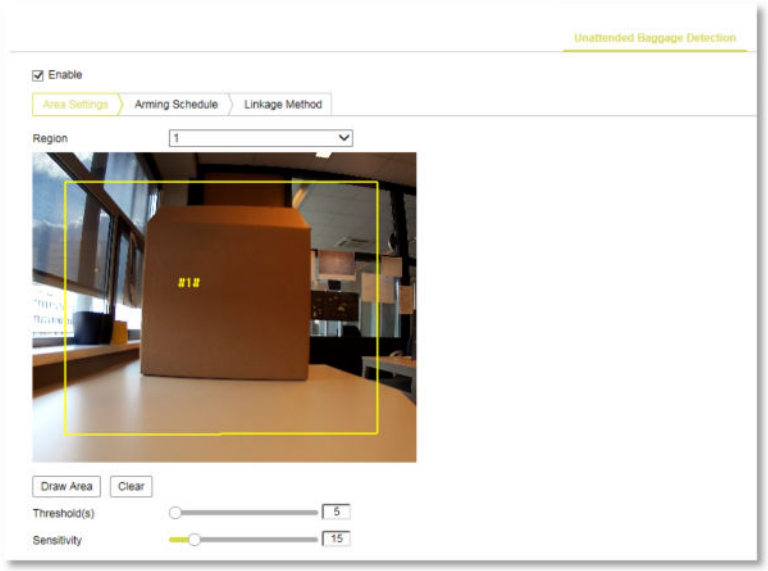
Trigger Alarm Output

Trigger one or more external alarm outputs when an event occurs. Before the output can be triggered, the related settings on the Alarm Output tab of the Events page must be correctly and completely configured.

Trigger Channel

Video is recorded when an event occurs. Before recording can start, the recording schedule on the Record Schedule tab of the Storage page must be set.

11.14 Unattended Baggage Detection



Events > Unattended Baggage Detection

What this tab is for

The Unattended Baggage Detection function detects objects left in the predefined region such as baggage, purses, dangerous materials, etc.. On the Unattended Baggage Detection tab, you can enable and set up the function, and define the actions to be taken when the alarm is triggered. Note that this function varies per camera model.

Steps

Region Exiting Detection configuration involves the following steps:

1 On the *Area Settings* tab, you define the area to be monitored.
2 On the *Arming Schedule* tab, you define the period(s) when you want the function to be active.
3 On the *Linkage Method* tab, you define the action(s) to be taken when an event occurs.

To set the region exiting detection area(s)

1 Select **Enable**.
2 On the *Area Settings* tab, click to open the **Region** list.
3 Select the region you want to create.
4 Click **Draw Area**.
5 Left-click in the Live Video window to set the first of the four vertexes of the detection area.
6 Move the mouse pointer to the next vertex.
7 Left-click to set the second vertex.
8 In the same way, set vertexes three and four.
9 Right-click to complete your drawing.
10 Click **Stop Drawing**.
11 Drag the **Threshold(s)** slider to set the time threshold.

Range: [5 s ~ 3600 s]. This is the threshold for the duration that objects are left behind in the region. If you set the value to 10, the alarm is triggered after the object was left and has been in the region for ten seconds.

12 Drag the **Sensitivity** slider to set the sensitivity of the detection.

Range: [1~100]. The value of the sensitivity defines the similarity degree of the background image. Usually, when the sensitivity is high, a very small object left in the region can trigger the alarm.

13 Repeat the steps above to configure other regions.

Up to 4 regions can be set. You can click Clear to delete all existing regions.

14 Click **Save**.

To set the arming schedule

1 On the *Arming Schedule* tab, drag your mouse pointer across the required day(s) to set the arming schedule.

A Copy button appears as you move your pointer across the schedule. You can click it to copy the settings of a specific day to another day.

You can click a time section to edit, save or delete it.

2 Click **Save**.

To set the alarm actions

1 On the *Linkage Method* tab, select the required actions (see descriptions below).

Options: *Send Email*, *Notify Surveillance Center*, *Upload to FTP*, *Trigger Alarm Output*, *Trigger Channel*.

2 Click **Save**.

Send Email

Send an email with alarm information to a user or users when an event occurs. Before emails can be sent, the related settings on the Mail tab of the Network page must be correctly and completely configured.

Notify Surveillance Center

Send an exception or alarm signal to remote management software when an event occurs.

Upload to FTP

Capture the image when an alarm is triggered and upload the picture to an FTP server. Before images can be uploaded, the related settings on the FTP tab of the Network page and on the Capture tab of the Storage page must be correctly and completely configured. The captured image can also be uploaded to the available SD card or network disk.

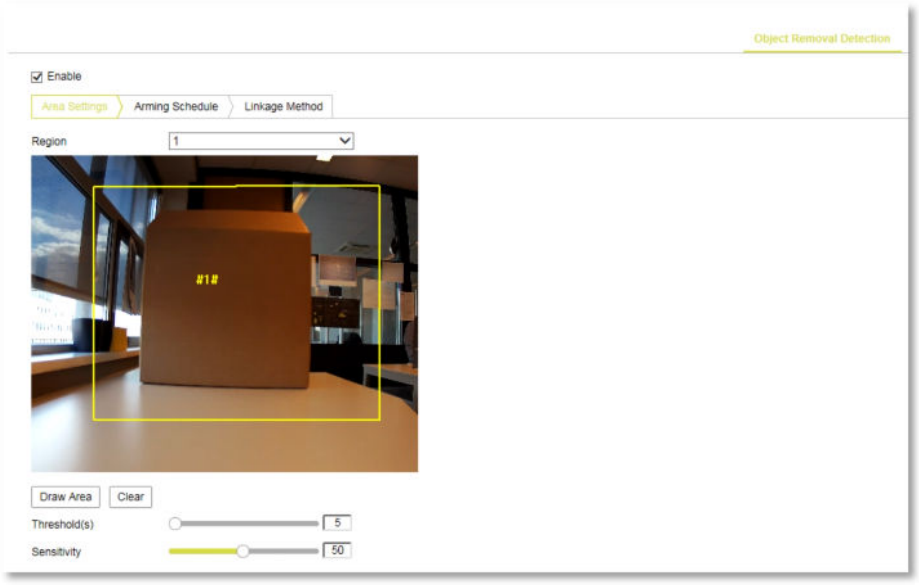
Trigger Alarm Output

Trigger one or more external alarm outputs when an event occurs. Before the output can be triggered, the related settings on the Alarm Output tab of the Events page must be correctly and completely configured.

Trigger Channel

Video is recorded when an event occurs. Before recording can start, the recording schedule on the Record Schedule tab of the Storage page must be set.

11.15 Object Removal Detection



Events > Objects Removal Detection

What this tab is for

The Object Removal Detection function detects if objects have been removed from a predefined region, such as exhibits on display. On the Object Removal Detection tab, you can enable and set up the function, and define the actions to be taken when the alarm is triggered. Note that this function varies per camera model.

Steps

Object Removal Detection configuration involves the following steps:

1 On the *Area Settings* tab, you define the area to be monitored.
2 On the *Arming Schedule* tab, you define the period(s) when you want the function to be active.
3 On the *Linkage Method* tab, you define the action(s) to be taken when an event occurs.

To set the object removal detection area(s)

1 Select **Enable**.
2 On the *Area Settings* tab, click to open the **Region** list.
3 Select the region you want to create.
4 Click **Draw Area**.
5 Left-click in the Live Video window to set the first of the four vertexes of the detection area.
6 Move the mouse pointer to the next vertex.
7 Left-click to set the second vertex.
8 In the same way, set vertexes three and four.
9 Right-click to complete your drawing.
10 Click **Stop Drawing**.
11 Drag the **Threshold(s)** slider to set the time threshold.

Range: [5 s ~ 3600 s]. This is the threshold for the duration that objects have been removed from the region. If you set the value to 10, the alarm is triggered ten seconds after the object was removed from the region.

12 Drag the **Sensitivity** slider to set the sensitivity of the detection.

Range: [1~100]. The value of the sensitivity defines the similarity degree of the background image. Usually, when the sensitivity is high, a very small object taken from the region can trigger the alarm.

13 Repeat the steps above to configure other regions.

Up to 4 regions can be set. You can click Clear to delete all existing regions.

14 Click **Save**.

To set the arming schedule

1 On the *Arming Schedule* tab, drag your mouse pointer across the required day(s) to set the arming schedule.

A Copy button appears as you move your pointer across the schedule. You can click it to copy the settings of a specific day to another day.

You can click a time section to edit, save or delete it.

2 Click **Save**.

To set the alarm actions

1 On the *Linkage Method* tab, select the required actions (see descriptions below).

Options: *Send Email*, *Notify Surveillance Center*, *Upload to FTP*, *Trigger Alarm Output*, *Trigger Channel*.

2 Click **Save**.

Send Email

Send an email with alarm information to a user or users when an event occurs. Before emails can be sent, the related settings on the Mail tab of the Network page must be correctly and completely configured.

Notify Surveillance Center

Send an exception or alarm signal to remote management software when an event occurs.

Upload to FTP

Capture the image when an alarm is triggered and upload the picture to an FTP server. Before images can be uploaded, the related settings on the FTP tab of the Network page and on the Capture tab of the Storage page must be correctly and completely configured. The captured image can also be uploaded to the available SD card or network disk.

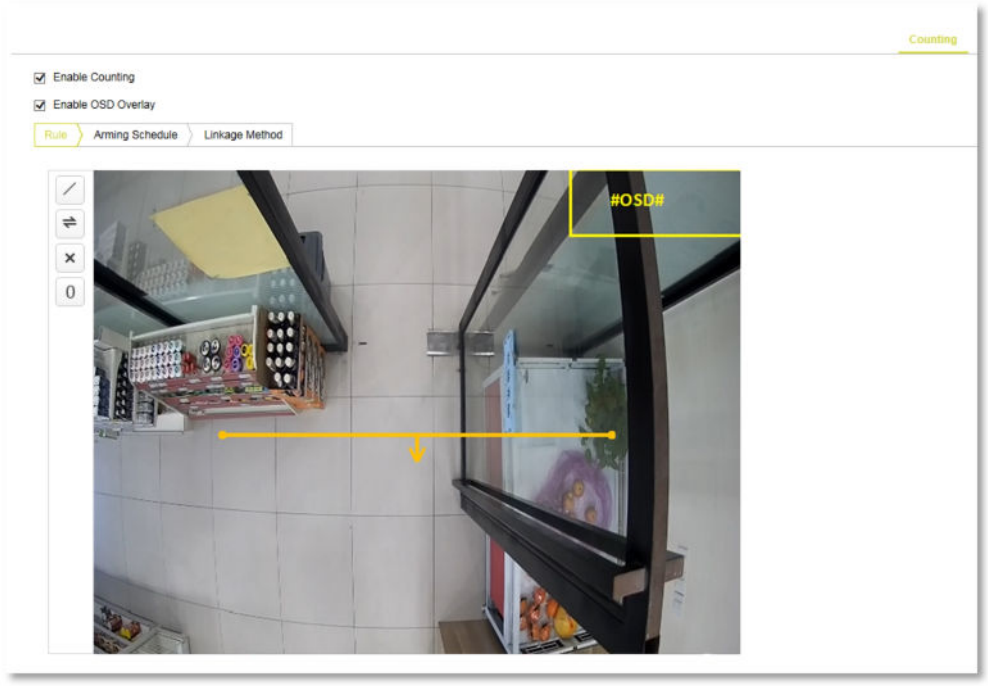
Trigger Alarm Output

Trigger one or more external alarm outputs when an event occurs. Before the output can be triggered, the related settings on the Alarm Output tab of the Events page must be correctly and completely configured.

Trigger Channel

Video is recorded when an event occurs. Before recording can start, the recording schedule on the Record Schedule tab of the Storage page must be set.

11.16 Counting



Events > Counting

What this tab is for

The Counting function is used to calculate the number of objects entering or exiting a certain configured area and is widely applied to roads, entrances or exits.

Counting accuracy

For better counting accuracy:

- Install the camera directly above the entrance/exit to be monitored.
- Make sure the camera is horizontal.

Steps

Counting configuration involves the following steps:

1 On the *Rule* tab, you define the area to be monitored.

2 On the *Arming Schedule* tab, you define the period(s) when you want the function to be active.

3 On the *Linkage Method* tab, you define the action(s) to be taken when an event occurs.

Buttons

The following buttons are available on the Rule tab:

	Draw Line
	Change Direction
	Delete
	Reset Counter

To set the detection line

1 Select **Enable Counting**.

2 (Optional) Select **Enable OSD Overlay**.

The real-time number of objects entering and exiting is displayed as an overlay over the live video. You can adjust the position of the OSD according to your needs.

3 Click **Draw Line**.

A detection line appears in the centre of the image.

4 Drag the line to adjust its position.

5 Drag the sizing handles to resize/rotate the line.

The detection line should cover the entire entrance/exit.

With the line selected, an arrow indicates the direction of people entering.

6 (Optional) To change the direction, click **Change Direction**.

7 (Optional) To reset the the counters in the OSD, click **Reset Counter**.

To set the arming schedule

1 On the *Arming Schedule* tab, drag your mouse pointer across the required day(s) to set the arming schedule.

A Copy button appears as you move your pointer across the schedule. You can click it to copy the settings of a specific day to another day.

You can click a time section to edit, save or delete it.

2 Click **Save**.

To set the alarm actions

1 On the *Linkage Method* tab, select the required action (see description below).

Option: *Notify Surveillance Center*.

2 Click **Save**.

Notify Surveillance Center

Send an exception or alarm signal to remote management software when an event occurs.

To view people counting statistics

1 Click **People Counting Statistics**.

2 In the **Report Type** list, select the report type to be shown.

Options: Daily, Weekly, Monthly, Annual.

3 Select **People Entered** or **People Exited**.

4 Select the Statistics Time.

5 Click **Counting** to calculate the data.

6 Select the export format.

Options: Table, Bar Chart, Line Chart.

If you select *Table*, there is an Export button to export the data in an Excel file.

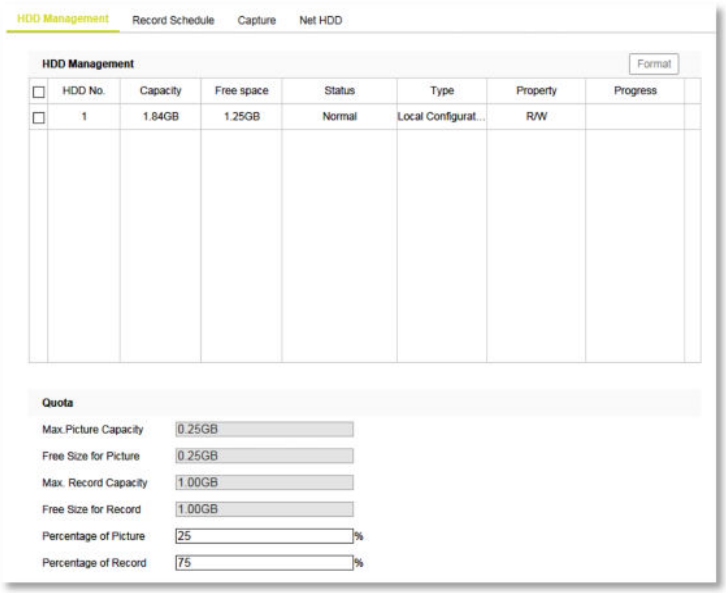
Note: To avoid compromising the accuracy of the data, we advise you not to adjust the camera lens after completing the installation.

12 Storage

Before you configure recording and storage settings, make sure that a network storage device is available within the network or that an SD card is inserted in your camera.

In This Chapter

12.1 HDD Management



Storage > HDD Management

What this tab is for

On the HDD Management tab, you can perform the following tasks:

- Initialise a network disk or an SD card that you have inserted into the camera.
- Define the quota for recordings and snapshots.

Available storage

Network disks added via the Net HDD tab or an SD card inserted into the camera will be available in the HDD Management table. You can see the capacity, free space, status type and property of each item. Up to eight NAS disks can be connected to the camera. If the status is *Uninitialised* you need to format the disk or card before you can use it.

To initialise a network disk or SD card

1 In the *HDD Management* table, click the check box to select the disk or card.

2 Click **Format**.

Note that all existing data (if any) on the storage medium will be erased and irretrievably lost!

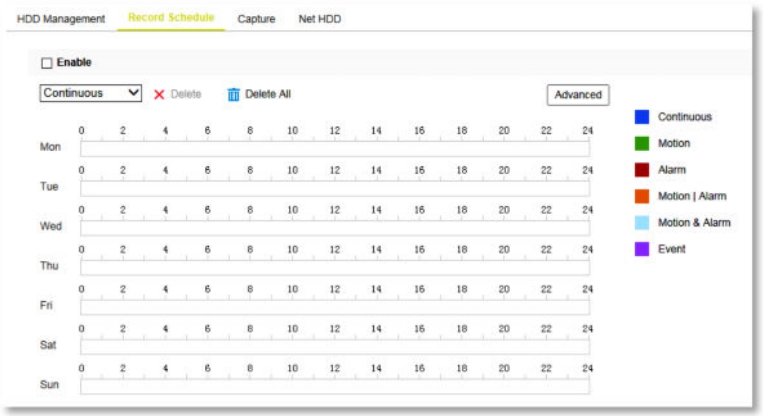
When the formatting has completed, the status of disk changes to "Normal".

To define the quota for recordings and snapshots

1 In *Percentage of Picture* and *Percentage of Record*, type the quota percentages you want to assign.

2 To activate the settings, click **Save** and refresh the browser page.

12.2 Record Schedule



Storage > Record Schedule

What this tab is for

There are two kinds of recording for the camera:

- Manual Recording
- Scheduled Recording

This section gives instructions for configuring scheduled recording. For instructions on manual recording, see the description of the *Live View* page.

Storage medium

By default, the files of recordings and snapshots are stored on the SD card (if supported) or on a network disk. Network disks can be added via the *Net HDD* tab. On the *HDD Management* tab, you can initialise connected disks and the SD card.

To set up scheduled recording

1 Select **Enable**.
2 Under *Enable*, click to open the *Recording type* list.
3 Select a recording type.
Available options: *Continuous*, *Motion*, *Alarm*, *Motion | Alarm*, *Motion & Alarm*, *Event*.
See below for a description of each type.
4 Drag your mouse pointer across the required day(s) to set up the recording schedule for this type of recording.
5 Repeat steps 3 and 4 for other recording types, if necessary.
A Copy button appears as you move your pointer across the schedule. You can click it to copy the settings of a specific day to another day.
You can click a time section to edit, save or delete it.
6 Click **Advanced**.
7 Select or clear **Overwrite**, as needed.
If you enable this function and the HDD is full, the new record files overwrite the oldest record files automatically.
8 In the *Pre-record* list, select a time span.
The recording is started at the number of seconds set here, before the scheduled time or the event. For example, if an alarm triggers the recording at 10:00, and the pre-record time is set as 5 seconds, the camera starts recording at 9:59:55.
9 In the *Post-record* list, select a time span.
The recording is stopped at the time set here, after the scheduled time or the event. For example, if an alarm triggered recording ends at 11:00, and the post-record time is set as 5 seconds, the camera records until 11:00:05.
10 Select the **Stream Type**.
Main Stream, Sub Stream and Third Stream are selectable. The streaming settings per stream type determine the time span you can record with the same storage capacity. Note that the record parameter configuration varies per camera model.
11 Click **OK**.
12 Click **Save**.

Continuous recording

Video is recorded automatically according to the time of the schedule.

Recording triggered by Motion Detection

Video is recorded when motion is detected. Besides configuring the recording schedule, you have to set the motion detection area and select the *Trigger Channel* check box in the *Linkage Method* of the Motion Detection settings interface. For more information, see the description of the Motion Detection tab (Event page).

Recording triggered by Alarm

Video is recorded when an alarm is triggered via the external alarm input channels. Besides configuring the recording schedule, you have to set the *Alarm Type* and select the *Trigger Channel* check box in the *Linkage Method* of the Alarm Input settings interface. For more information, see the description of the Alarm Input tab (Event page).

Recording triggered by Motion | Alarm

Video is recorded when the external alarm is triggered or motion is detected. Besides configuring the recording schedule, you have to configure the settings on the *Motion Detection* and the *Alarm Input* settings interfaces. For more information, see the descriptions of the *Motion Detection* and *Alarm Input* tabs (Event page).

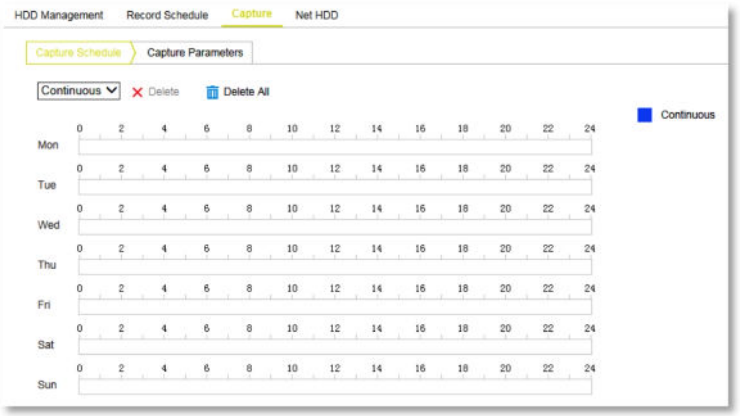
Recording triggered by Motion & Alarm

Video is recorded when motion detection and alarm input are triggered at the same time. Besides configuring the recording schedule, you have to configure the settings on the *Motion Detection* and the *Alarm Input* settings interfaces. For more information, see the descriptions of the *Motion Detection* and *Alarm Input* tabs (Event page).

Recording triggered by Event

Video is recorded on the occurrence of so-called smart events such as Face Detection, Audio Exception Detection, Intrusion Detection, and others found on the Events page. Besides configuring the recording schedule, make sure that the settings of the specific event are correctly configured. For more information, see the description of the Event page.

12.3 Capture



Storage > Capture

What this tab is for

On the Capture tab, you can configure the settings for snapshot captures.

Storage medium

By default, the files of recordings and snapshots are stored on the SD card (if supported) or on a network disk. Network disks can be added via the *Net HDD* tab. On the *HDD Management* tab, you can initialise connected disks and the SD card.

To set up the capture schedule

1 On the *Capture Schedule* tab, drag your mouse pointer across the required day(s) to set up the recording schedule for this type of recording.

A Copy button appears as you move your pointer across the schedule. You can click it to copy the settings of a specific day to another day.

You can click a time section to edit, save or delete it.

2 Click **Save**.

To enable timing snapshots

1 On the *Capture Parameters* tab, select **Enable Timing Snapshot**.

2 In the *Quality* list, select the required quality.

3 In the *Interval* unit list, select a unit.

Options: millisecond, s, min, Hour, Day(s).

4 Type a value in *Interval*.

This sets the time interval between two snapshots.

5 Click **Save**.

To upload continuous snapshots to an FTP server

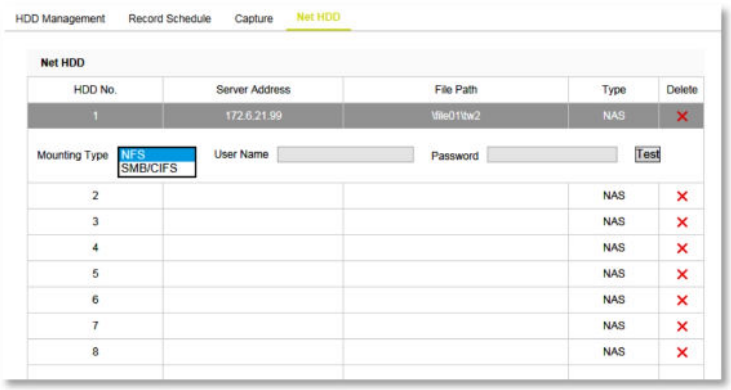
1 Go to the **FTP** tab of the **Network** page.

2 Configure the FTP settings.

3 Select **Upload Picture**.

4 Click **Save**.

12.4 Net HDD



Storage > Net HDD

What this tab is for

On the Net HDD tab, you can configure and test the settings for Network Attached Storage (NAS).

Before you continue

The network disk should be available within the network and properly configured to store the recorded files, log files, etc.

To add a network disk

1 In the *Net HDD* table, click to select a **HDD No**.

2 In the *Server Address* column, type the IP address of the server which houses the network disk.

3 In the *File Path* column, type the path to the server.

For information about the file path, contact your system administrator or refer to the user manual of your NAS.

4 In the *Mounting Type* list, select **NFS** or **SMB/CIFS**.

5 If you selected *NFS*, type the user name and password.

6 To test your settings, click **Test**.

7 Click **Save**.

Note: You can initialise the network disk on the HDD Management tab of the Storage page.

Use strong passwords

For your privacy and to better protect your system against security risks, we strongly advise the use of strong passwords for all functions and network devices. Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user of the camera.

To create a strong password

- Use at least eight characters
- Do not include your real name, user name, company name, or other personal information
- Do not use complete words that can be found in a dictionary
- Use a random combination of at least two of the following categories: upper case letters, lower case letters, numbers and special characters

Number of network disks

You can connect up to eight network disks to the camera.

To delete a network disk

1 In *Delete* column of the *Net HDD* table, click the red **Delete** icon.

2 Click **Save**.

Index

T

U

V