

# PD1103 Series

3 MP Intelligent IP PTZ Dome Cameras

## User Manual



SECURITY  
SOLUTIONS

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

## **Copyright © 2017 Siqua B.V.**

All rights reserved.

PD1103

User Manual v3 (160805-3)

AIT55

Nothing from this publication may be copied, translated, reproduced, and/or published by means of printing, photocopying, or by any other means without the prior written permission of Siqua.

Siqua reserves the right to modify specifications stated in this manual.

## **Brand names**

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

## **Liability**

Siqua 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](mailto: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:

Siqua B.V.  
Zuidelijk Halfroond 4  
2801 DD Gouda  
The Netherlands

General : +31 182 592 333  
Fax : +31 182 592 123  
E-mail : [sales.nl@tkhsecurity.com](mailto:sales.nl@tkhsecurity.com)  
WWW : <http://www.tkhsecurity.com>

# Contents

<b>1</b>	<b>About this manual .....</b>	<b>5</b>
<b>2</b>	<b>Safety and compliance .....</b>	<b>6</b>
2.1	Safety instructions .....	6
2.2	Compliance information .....	7
<b>3</b>	<b>Functions overview .....</b>	<b>9</b>
<b>4</b>	<b>Connect to network .....</b>	<b>12</b>
4.1	System requirements .....	12
4.2	Connect the camera to a LAN .....	12
4.3	Connect the camera to a WAN .....	14
<b>5</b>	<b>Get access to the camera .....</b>	<b>17</b>
5.1	Get access via web browser .....	17
5.2	Get access via Device Manager .....	18
5.3	Get access via UPnP .....	19
5.4	Log on to the camera .....	20
5.5	Install the videoplayer plug-in .....	21
5.6	Power-up action .....	21
<b>6</b>	<b>Live View .....</b>	<b>23</b>
<b>7</b>	<b>Playback .....</b>	<b>32</b>
<b>8</b>	<b>System .....</b>	<b>34</b>
8.1	Basic Information .....	34
8.2	Time Settings .....	35
8.3	Upgrade & Maintenance .....	36
8.4	RS-485 .....	38
8.5	Log .....	39
8.6	Local Configuration .....	40
<b>9</b>	<b>Security .....</b>	<b>42</b>
9.1	User Management .....	42
9.2	Authentication .....	43
9.3	IP Address Filter .....	44
<b>10</b>	<b>Network .....</b>	<b>46</b>
10.1	TCP/IP .....	46
10.2	DDNS .....	48
10.3	PPPoE .....	49
10.4	SNMP .....	50
10.5	802.1X .....	51
10.6	QoS .....	52
10.7	NAT .....	53
10.8	HTTPS .....	54
10.9	Mail .....	56
10.10	FTP .....	57
<b>11</b>	<b>Video/Audio .....</b>	<b>59</b>

11.1	Streaming .....	59
11.2	Picture Adjustment .....	61
11.3	Text Overlay .....	64
11.4	Privacy Mask .....	65
11.5	ROI .....	66
<b>12</b>	<b>Events .....</b>	<b>68</b>
12.1	Motion Detection .....	68
12.2	Video Tampering .....	71
12.3	Alarm Input .....	72
12.4	Alarm Output .....	74
12.5	Exception .....	75
12.6	Audio Exception Detection .....	76
12.7	Face Detection .....	78
12.8	Intrusion Detection .....	80
12.9	Line Crossing Detection .....	82
12.10	Region Entrance Detection .....	84
12.11	Region Exiting Detection .....	86
<b>13</b>	<b>Storage .....</b>	<b>88</b>
13.1	HDD Management .....	88
13.2	Record Schedule .....	89
13.3	Capture .....	91
13.4	Net HDD .....	92
<b>14</b>	<b>PTZ .....</b>	<b>94</b>
14.1	Settings .....	94
14.2	Zero Position .....	96
14.3	Home Action .....	97
14.4	Limit .....	98
14.5	Auto Tracking .....	99
14.6	Clear Config .....	100
	<b>Appendix: NTCIP Configuration .....</b>	<b>101</b>
	Supported conformance groups .....	101
	<i>Configuration</i> .....	101
	<i>CCTV configuration</i> .....	102
	<i>Motion control</i> .....	102
	SNMP MIB .....	103
	<b>Index .....</b>	<b>104</b>

# 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 PD1103 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](http://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 PD1103 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](mailto: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.....	6
2.2 Compliance information.....	7

## 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.

			
<b>Warnings</b>	Follow these safeguards to prevent serious injury or death.	<b>Cautions</b>	Follow these precautions to prevent potential injury or material damage.

### Warnings

	<ul style="list-style-type: none"> <li>• Use a power adapter which can meet the safety extra low voltage (SELV) standard.The power consumption cannot be less than the required value.</li> </ul>
	<ul style="list-style-type: none"> <li>• Do not connect several devices to one power adapter as an adapter overload may cause overheating and can be a fire hazard.</li> </ul>
	<ul style="list-style-type: none"> <li>• When the product is installed on a wall or ceiling, the device should be firmly fixed.</li> </ul>
	<ul style="list-style-type: none"> <li>• To reduce the risk of fire or electrical shock, do not expose this product to rain or moisture.</li> </ul>
	<ul style="list-style-type: none"> <li>• This installation should be made by a qualified service person and should conform to all the local codes.</li> </ul>
	<ul style="list-style-type: none"> <li>• Install blackout equipment into the power supply circuit for convenient supply interruption.</li> </ul>
	<ul style="list-style-type: none"> <li>• 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.</li> </ul>

## Cautions

	<ul style="list-style-type: none"> <li>• Make sure the power supply voltage is correct before using the camera.</li> </ul>
	<ul style="list-style-type: none"> <li>• Do not drop the camera or subject it to physical shock. Do not install the product on vibratory surfaces or places.</li> </ul>
	<ul style="list-style-type: none"> <li>• Do not expose the camera to a high electromagnetic radiating environment.</li> </ul>
	<ul style="list-style-type: none"> <li>• 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.</li> </ul>
	<ul style="list-style-type: none"> <li>• 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.</li> </ul>
	<ul style="list-style-type: none"> <li>• 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 <a href="http://www.tkhsecurity.com/support-files">www.tkhsecurity.com/support-files</a>.</li> </ul>
	<ul style="list-style-type: none"> <li>• To avoid heat accumulation, good ventilation is required to ensure a proper operating environment.</li> </ul>
	<ul style="list-style-type: none"> <li>• While shipping, the camera should be packed into its original packing.</li> </ul>
	<ul style="list-style-type: none"> <li>• Use the provided glove when you open the product cover. Do not touch the product cover directly with your fingers. The acidic sweat of the fingers may erode the surface coating of the product cover.</li> </ul>
	<ul style="list-style-type: none"> <li>• Use a soft and dry cloth when you clean the inside and outside surfaces of the product cover. Do not use alkaline detergents.</li> </ul>
	<ul style="list-style-type: none"> <li>• Improper use or replacement of the battery may result in the hazard of explosion. Use the battery type recommended by the manufacturer.</li> </ul>

## 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.

## EU Conformity Statement

	<p>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 Low Voltage Directive 2006/95/EC, the EMC Directive 2004/108/EC, the RoHS Directive 2011/65/EU.</p>
	<p>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: <a href="http://www.recyclethis.info">www.recyclethis.info</a>.</p>
	<p>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: <a href="http://www.recyclethis.info">www.recyclethis.info</a>.</p>



## 3 Functions overview

---

This section gives an overview of the functions offered by the speed dome camera.

**Note:** The availability of the functions may vary depending on the model of the camera.

### Limit stops

The dome can be programmed to move within limit stops (left/right, up/down).

### Scan modes

The dome provides five scan modes: auto scan, tilt scan, frame scan, random scan and panorama scan.

### Presets

A preset is a predefined image position. When the preset is called, the dome automatically moves to the defined position. Presets can be added, modified, deleted and called.

### Preset freezing

This feature freezes the scene on the monitor when the dome is moving to a preset. This allows for smooth transition from one preset scene to another. It also guarantees that a masked area is not revealed when the dome is moving to a preset.

### Patrol

A patrol is a memorised series of predefined preset function. The scanning speed between two presets and the dwell time at the preset are programmable.

### Pattern

A pattern is a memorised series of pan, tilt, zoom, and preset functions. By default, the focus and iris are in autostatus when the pattern is being memorised.

### Label display

The on-screen label of the preset title, azimuth/elevation, zoom, time and dome name can be displayed on the monitor. The displays of time and speed dome name can be programmed.

### Autoflips

In manual tracking mode, when a target object goes directly beneath the dome, the video will automatically flips 180 degrees in horizontal direction to maintain continuity of tracking. This function can also be realised by auto mirror image, depending on different camera models.

### Privacy mask

This function allows you to block or mask certain areas of a scene to prevent the personal privacy from being violated by recording or live viewing. A masked area will move with pan and tilt functions and will automatically adjust in size as the lens goes to telephoto and wide angle.

### 3D Positioning

In the client software, use the left mouse button to click on the desired position in the video image and drag a rectangle area in the lower right direction. The dome system will move the position to the centre and allow the rectangle area to zoom in. Use the left mouse button to drag a rectangle area in the upper left direction to move the position to the centre and allow the rectangle area to zoom out.

### **Proportional pan/tilt**

Proportional pan/tilt automatically reduces or increases the pan and tilt speeds according to the amount of zoom. In telephoto zoom mode, the pan and tilt speeds are slower than in wide angle zoom mode. This keeps the image from moving too fast on the live view image when there is a large amount of zoom.

### **Autofocus**

The autofocus function enables the camera to focus automatically to maintain clear video images.

### **Day/Night autoswitch**

The speed domes deliver colour images during the day. As light diminishes at night, the speed domes switch to night mode and deliver black and white images with high quality.

### **Slow shutter**

In slow shutter mode, the shutter speed is automatically reduced in low illumination conditions to maintain clear video images by extending the exposure time. The feature can be enabled or disabled.

### **Backlight compensation (BLC)**

If you focus on an object against strong backlight, the object will be too dark to be seen clearly. The backlight compensation (BLC) function can compensate the light in front of the object to make it clear, but this causes overexposure of the background where the light is strong.

### **Wide dynamic range (WDR)**

The wide dynamic range (WDR) function helps the camera provide clear images even under difficult light circumstances. 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 and provide clear images with details.

<b>Note:</b> This feature varies depending on the speed dome model.
---

### **White balance (WB)**

White balance can remove unrealistic colour casts. White balance is the white rendition function of the camera to automatically adjust the colour temperature according to the environment.

### **Power off memory**

The dome supports the power off memory capability with the predefined resume time. It allows the dome to resume its previous position after power is restored.

### **Time task**

A time task is a preconfigured action that can be performed automatically at a specific date and time. The programmable actions include: auto scan, random scan, patrol 1-8 ,pattern 1-4, preset 1-8, frame scan, panorama scan, tilt scan, day, night, reboot, PT adjust, Aux Output, and other actions.

### **Park action**

This feature allows the dome to start a predefined action automatically after a period of inactivity.

### **User management**

The user logged in as admin can edit users with different levels of permission. Multiple users are allowed to simultaneously access and control the same network speed dome via the network.

### **3D Digital noise reduction**

Compared to general 2D digital noise reduction, 3D digital noise reduction processes the noise between two frames besides processing the noise in one frame. The noise will be much less and the video will be clearer.

## 4 Connect to network

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

### In This Chapter

4.1 System requirements.....	12
4.2 Connect the camera to a LAN.....	12
4.3 Connect the camera to a WAN.....	14

### 4.1 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.

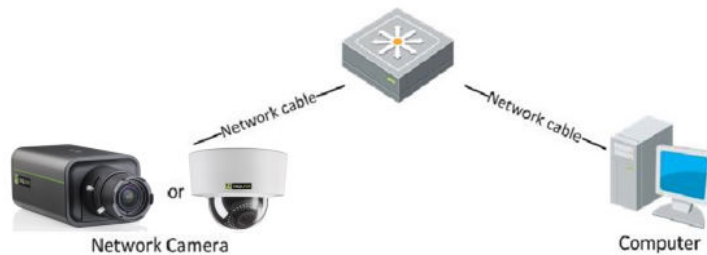
### 4.2 Connect the camera to a LAN

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.

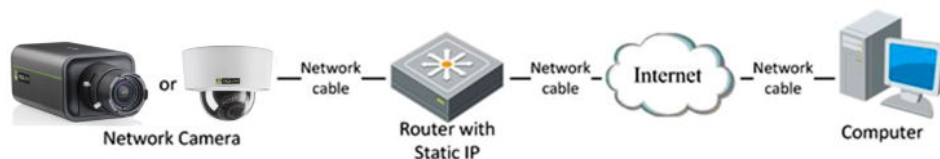
With both devices on the same subnet, you can reopen communication between the computer and the camera.

## 4.3 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.

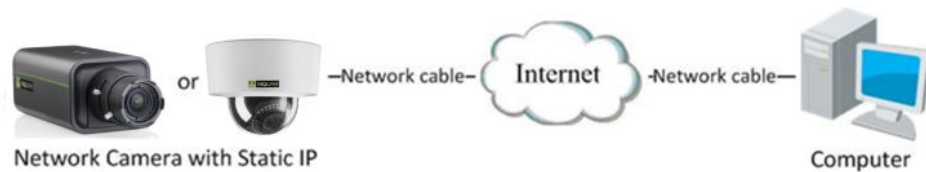


#### » To connect the network camera via a router

- 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

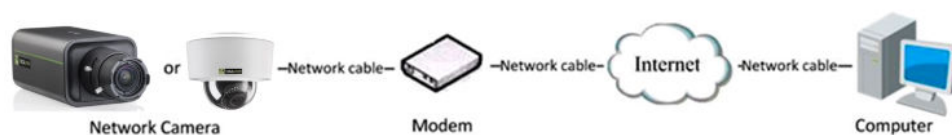
Before you start, obtain a dynamic IP address from an Internet Service Provider (ISP). With the dynamic IP address, you can connect the network camera via a modem or a router.

### » 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

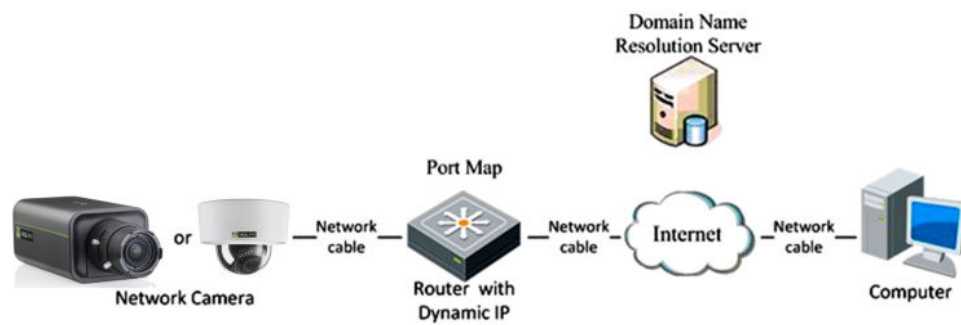
This camera supports the PPPoE auto dial-up function. The camera gets a public IP address by ADSL dial-up after the camera is connected to a modem. You need to configure the PPPoE parameters of the network camera.



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.

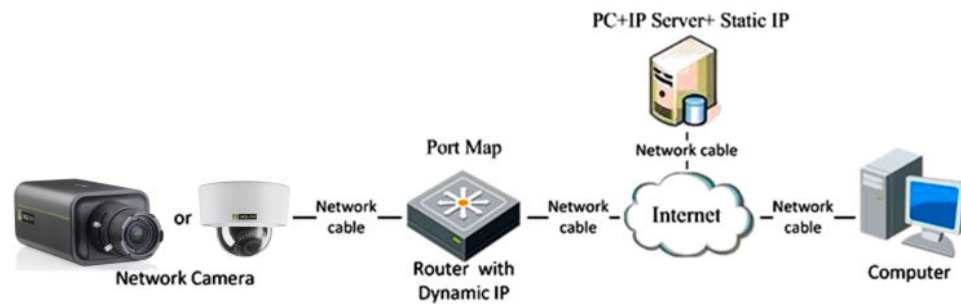
### » To set normal domain name resolution

- 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**.





# 5 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

5.1 Get access via web browser.....	17
5.2 Get access via Device Manager.....	18
5.3 Get access via UPnP.....	19
5.4 Log on to the camera.....	20
5.5 Install the videoplayer plug-in.....	21
5.6 Power-up action.....	21

## 5.1 Get access via web browser

### Default settings

Out of the box, the camera has these settings:

- DHCP: enabled
- UPnP: enabled

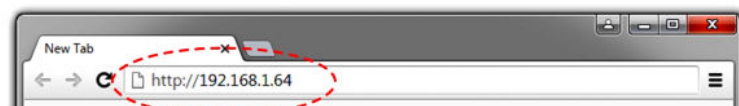
If a DHCP server exists on the network, the camera acquires an IP address from the DHCP address range. If necessary, refer to your system administrator for assistance.

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.

## 5.2 Get access via Device Manager

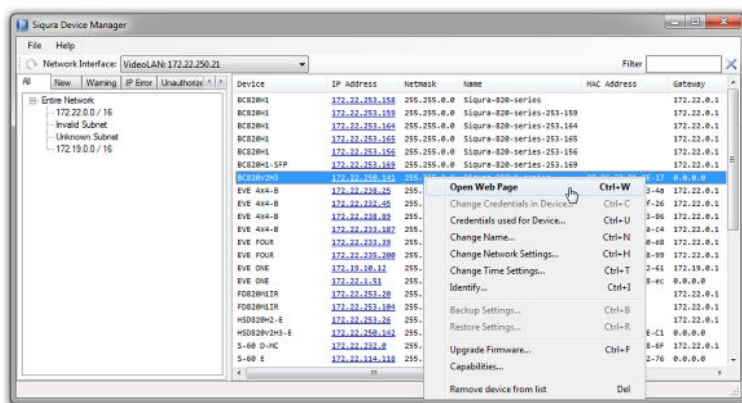
Device Manager is a Windows-based software tool that you can use to manage and configure TKH Security IP cameras and video encoders. The tool automatically locates TKH Security devices on the network and offers you an intuitive interface to set and manage network settings, configure devices, show device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

### » To install Device Manager

- 1 Download the latest version of Device Manager at [www.tkhsecurity.com/support-files](http://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*).



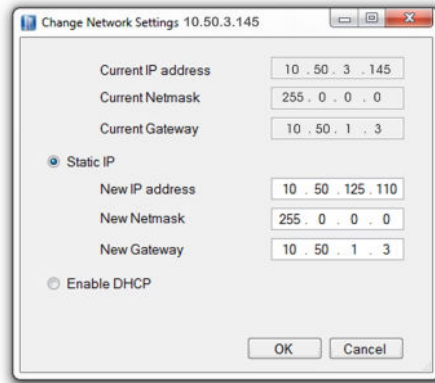
## Change the network settings with Device Manager

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.

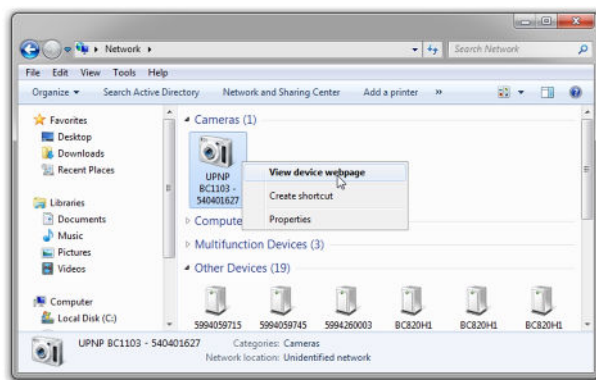
**Note:** A DHCP server must be installed on the network in order to provide DHCP network support. If no DHCP server is found on the network, the camera is initially assigned the IP address 0.0.0.0. After 30 seconds, an IP address in the range of 192.168.1.2~192.168.1.253 is adopted.

## 5.3 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*).



## 5.4 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.

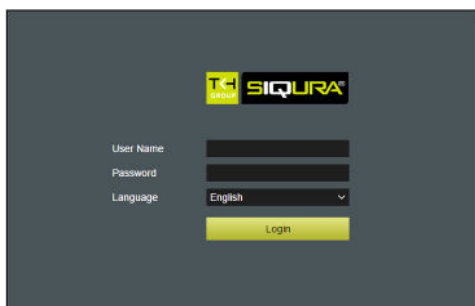
#### » To create a strong password

- 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.

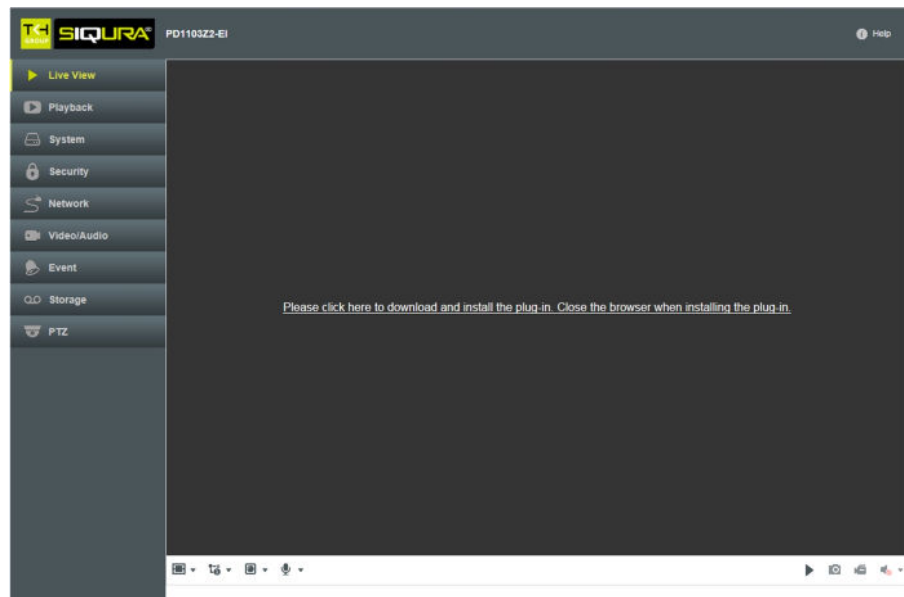
### Login box

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.

## 5.5 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 safely install it.
- 6 Follow the installation steps.
- 7 Open your web browser.
- 8 Reconnect to the camera.

## 5.6 Power-up action

After the power is applied, the speed dome performs self-test actions. It starts with lens actions and then proceeds with pan and tilt movement. After the power-up self-test actions, system information is displayed on screen for 40 seconds.

The information includes details about the dome model, address, protocol, version and other information. The Communication item gives the baud, parity, data bit and stop bit settings of the dome. For example, "2400, N, 8, 1" indicates that the dome is configured with 2400 baud, no parity, 8 data bits and 1 stop bit.

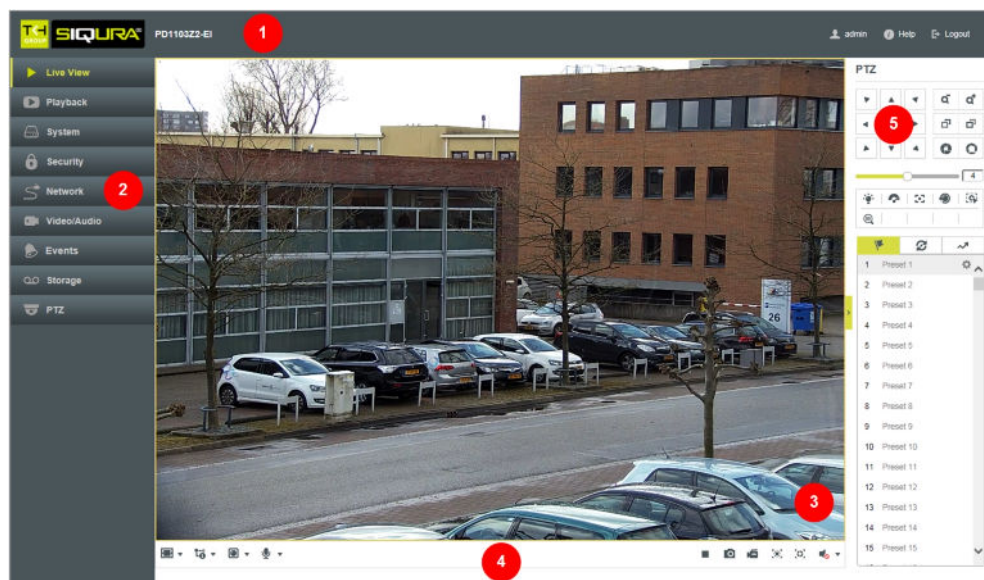


## 6 Live View

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
	Shows the brand of the camera you are connected to
	Shows the camera model name
	Shows the user currently logged on to the camera
	Opens the Online Help information
	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 regional exposure
	Enables regional focus
	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
	Start Manual Tracking
	Start 3D Zoom

## Use presets, patrols and patterns

The area under the PTZ buttons is where you manage presets, patrols and patterns. You can set 300 presets, eight patrols and four patterns.

	Preset management
	Patrol management
	Pattern management

## 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**.

## Predefined presets

The Preset list contains 300 presets. Some of them are predefined with special commands. You can call them but not configure them. For example, preset 99 is "Start auto scan". If you call this preset, the speed dome starts the auto scan function.

Preset	Function	Preset	Function
33	Auto flip	93	Set limit stops manually
34	Back to initial position	94	Remote reboot
35	Call patrol 1	95	Call OSD menu
36	Call patrol 2	96	Stop a scan
37	Call patrol 3	97	Start random scan
38	Call patrol 4	98	Start frame scan
39	IR cut filter in	99	Start auto scan
40	IR cut filter out	100	Start tilt scan
41	Call pattern 1	101	Start panorama scan
42	Call pattern 2	102	Call patrol 5
43	Call pattern 3	103	Call patrol 6
44	Call pattern 4	104	Call patrol 7
45	Automatically Create Patrol	105	Call patrol 8
92	Start to set limit stops		


You may need to use the OSD (On Screen Display) menu when controlling the speed dome remotely. To display the OSD menu on the live view screen, you can call preset number 95.

## 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**.

## Patterns






A pattern is a memorised series of pan, tilt, zoom, and preset functions. It can be called on the pattern settings tab. There are up to four patterns for customising. The patterns can be operated separately and with no priority level. When configuring and calling a pattern:

- Proportional pan is valid.

- The limit stops and auto flip will be invalid.
- The 3D positioning operation is not supported.

## Pattern buttons

The following buttons are available for pattern management.

	Start recording			Stop pattern
	Stop recording			Delete pattern
	Start pattern			

### » To create a pattern

- 1 In the *PTZ* panel, click the **Pattern** tab.
- 2 Select a Pattern number.
- 3 Click **Start recording**.
- 4 Use the PTZ control buttons to move the lens to the desired position(s), as needed.
  - Pan the speed dome to the right or left.
  - Tilt the speed dome up or down.
  - Zoom in or out.
  - Refocus the lens.

Information of Program Pattern Remaining Memory (%) is displayed on the screen.
- 5 Click **Stop recording**.

### » To start a pattern

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

### » To stop a pattern

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

### » To delete a pattern

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

## Manual tracking

Clicking **Start Manual Tracking** in the toolbar of the PTZ panel opens the manual tracking mode. In this mode, you can click a moving object in the video which will then automatically be tracked by the camera.

**Important:** Before you can use this function, you need to go to the PTZ page and enable Auto Tracking.

## 3D Positioning

Clicking **Start 3D Zoom** in the toolbar of the PTZ panel opens the 3D positioning mode. In this mode, you can:

- Left click a position on the live video.  
The corresponding position will be moved to the centre of the live video.
- Hold down the left mouse button and drag the mouse to the lower right on the live video.  
The corresponding position will be moved to the centre of the live video and zoomed in.
- Hold down the left mouse button and drag the mouse to the upper left on the live video.  
The corresponding position will be moved to the center of the live video and zoomed out.

## 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.

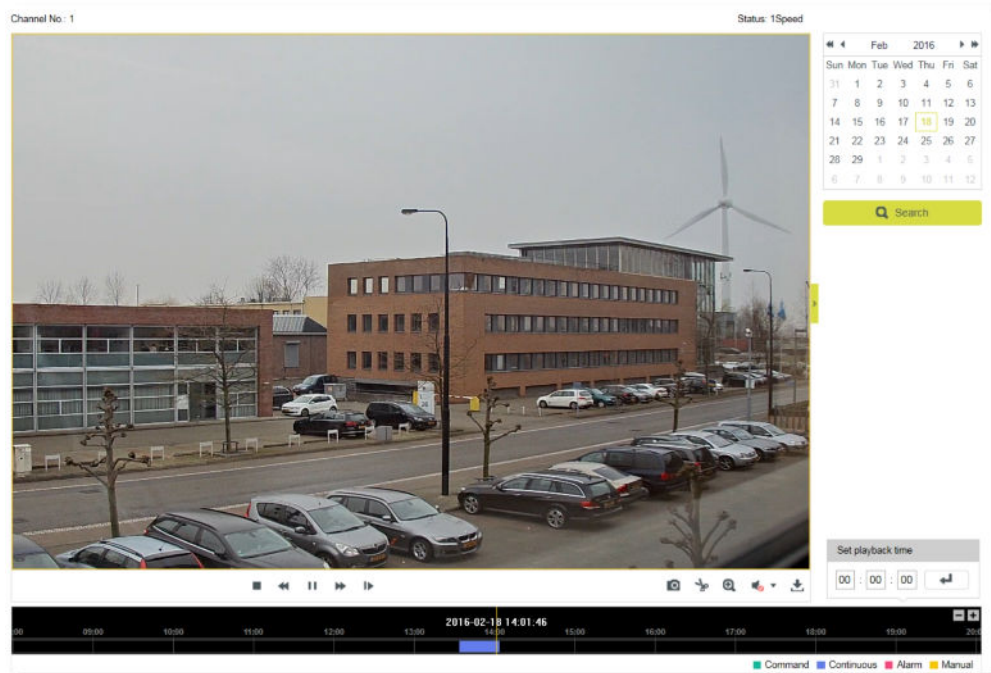
## Regional focus

Clicking the Regional Focus button in the toolbar opens the regional focus operation mode. In this mode, you can draw a rectangle (by dragging the mouse pointer) across the video in the camera view to define the desired focus region.

## Regional exposure

Clicking the Regional Exposure button in the toolbar opens the regional exposure operation mode. In this mode, you can draw a rectangle (by dragging the mouse pointer) across the video in the camera view to define the desired exposure region.

# 7 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 calendar 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 <b>Start</b>	
To pause playback	Click <b>Pause</b>	
To stop playback	Click <b>Stop</b>	
To accelerate playback speed	Click <b>Fast forward</b>	
To reduce playback speed	Click <b>Slow forward</b>	
To advance one frame	Click <b>Single frame</b>	

## Additional functions

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

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

## 8 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

8.1 Basic Information.....	34
8.2 Time Settings.....	35
8.3 Upgrade & Maintenance.....	36
8.4 RS-485.....	38
8.5 Log.....	39
8.6 Local Configuration.....	40

## 8.1 Basic Information

Basic Information

Time Settings

Upgrade & Maintenance

RS485

Log

Local Configuration

Device Name

IP CAMERA

Device No.

88

Model

BC1103

Serial No.

BC110320150906CCWR540401627

Firmware Version

V5.3.4 build 160111

Encoding Version

V7.0 build 151228

Web Version

V4.0.51 build 160107

Plugin Version

V3.0.5.42

Number of Channels

1

Number of HDDs

0

Number of Alarm Input

1

Number of Alarm Output

1

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.

## 8.2 Time Settings

The screenshot shows the 'Time Settings' tab with the following configuration:

- Time Zone:** (GMT+01:00) Amsterdam, Berlin, Rome, Paris
- NTP:**
  - ☐ NTP
  - Server Address: time.windows.com
  - NTP Port: 123
  - Interval: 1440 min
  - Test button
- Manual Time Sync:**
  - ☒ Manual Time Sync.
  - Device Time: 2016-01-19T13:27:06
  - Set Time: 2016-01-19T13:27:08
  - ☒ Sync. with computer time
- DST:**
  - ☐ Enable DST
  - Start Time: Jan, First, Sun, 00
  - End Time: Jan, First, Sun, 00
  - DST Bias: 30min

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.

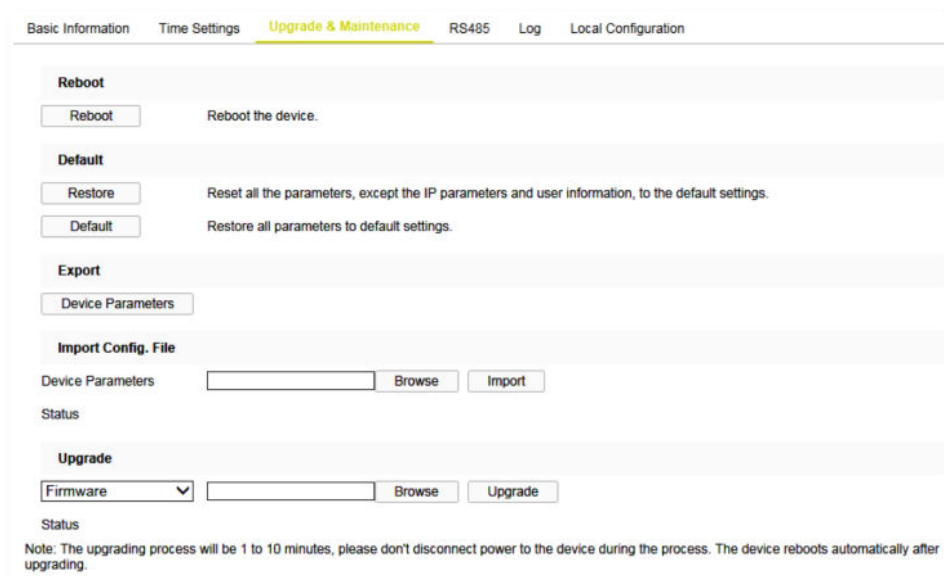
#### » To set the system time manually

- 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**.

## 8.3 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](http://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.

## 8.4

## RS-485

Basic Information		Time Settings		Upgrade & Maintenance		RS485		Log		Local Configuration	
Baud Rate	9600										
Data Bit	8										
Stop Bit	1										
Parity	None										
Flow Ctrl	None										
PTZ Protocol	PELCO-D										
PTZ Address	0										

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.

## 8.5 Log

Basic Information Time Settings Upgrade & Maintenance RS485 **Log** Local Configuration

Major Type: All Types Minor Type: All Types

Start Time: 2016-01-25 00:00:00 End Time: 2016-01-25 23:59:59 Search

**Log List** Export

No.	Time	Major Type	Minor Type	Channel No.	Local/Remote User	Remote Host IP
1	2016-01-25 15:07:58	Operation	Remote: Get Working Sta...		admin	172.22.250.21
2	2016-01-25 15:07:52	Operation	Remote: Get Parameters		admin	172.22.250.21
3	2016-01-25 15:07:52	Operation	Remote: Get Parameters		admin	172.22.250.21
4	2016-01-25 15:07:44	Operation	Remote: Get Parameters		admin	172.22.250.21
5	2016-01-25 15:05:02	Operation	Power On			local

Total 5 Items << < 1/1 > >>

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.

## 8.6 Local Configuration

Basic Information Time Settings Upgrade & Maintenance RS485 Log **Local Configuration**

**Live View Parameters**

Protocol ☒ TCP ☐ UDP ☐ MULTICAST ☐ HTTP

Play Performance ☐ Shortest Delay ☒ Auto

Rules ☐ Enable ☒ Disable

Image Format ☒ JPEG ☐ BMP

**Record File Settings**

Record File Size ☐ 256M ☒ 512M ☐ 1G

Save record files to C:\Users\ \Web\RecordFiles

Save downloaded files to C:\Users\ \Web\DownloadFiles

**Picture and Clip Settings**

Save snapshots in live view to C:\Users\ \Web\CaptureFiles

Save snapshots when playback to C:\Users\ \Web\PlaybackPics

Save clips to C:\Users\ \Web\PlaybackFiles

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**.

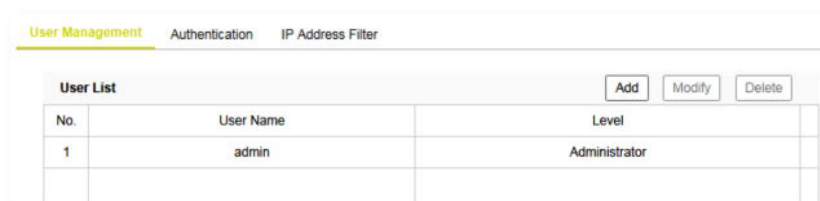
# 9 Security

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

## In This Chapter

9.1 User Management.....	42
9.2 Authentication.....	43
9.3 IP Address Filter.....	44

## 9.1 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**.

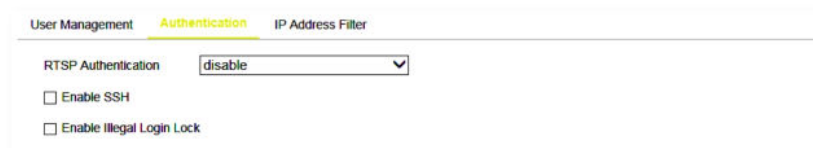
### » To modify a user account

- 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**.

## 9.2 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 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**.

## 9.3 IP Address Filter

User Management Authentication **IP Address Filter**

☒ Enable IP Address Filter

IP Address Filter Type: Forbidden

IP Address Filter	
No.	IP
1	172.6.23.2

Add Modify Delete

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**.

# 10 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

10.1 TCP/IP.....	46
10.2 DDNS.....	48
10.3 PPPoE.....	49
10.4 SNMP.....	50
10.5 802.1X.....	51
10.6 QoS.....	52
10.7 NAT.....	53
10.8 HTTPS.....	54
10.9 Mail.....	56
10.10 FTP.....	57

## 10.1 TCP/IP

TCP/IP

DDNS

PPPoE

SNMP

802.1x

QoS

NAT

HTTPS

Mail

FTP

NIC Type

Auto

☐ DHCP

IPv4 Address

172.22.250.137

Test

✓

IPv4 Subnet Mask

255.255.0.0

✓

IPv4 Default Gateway

172.22.250.1

✓

IPv6 Mode

Route Advertisement

View Route Advertisement

IPv6 Address

::

IPv6 Subnet Mask

0

IPv6 Default Gateway

::

Mac Address

c4:2f:90:c9:56:01

MTU

1500

✓

Multicast Address

✓

☒ Enable Multicast Discovery

DNS Server

Preferred DNS Server

8.8.8.8

✓

Alternate DNS Server

✓

Port

HTTP Port

80

✓

RTSP Port

554

✓

HTTPS Port

443

✓

Server Port

8000

✓

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.

## 10.2 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 IP Server

- 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](http://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.

## 10.3 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.

## 10.4 SNMP

TCP/IP DDNS PPPoE **SNMP** 802.1x QoS NAT HTTPS Mail FTP

**SNMP v1/v2**

☐ Enable SNMPv1

☐ Enable SNMP v2c

Read SNMP Community public

Write SNMP Community private

Trap Address

Trap Port 162

Trap Community public

**SNMP v3**

☐ Enable SNMPv3

Read UserName

Security Level no auth, no priv

Authentication Algorithm MD5 SHA

Authentication Password

Private-key Algorithm DES AES

Private-key password

Write UserName

Security Level no auth, no priv

Authentication Algorithm MD5 SHA

Authentication Password

Private-key Algorithm DES AES

Private-key password

**SNMP Other Settings**

SNMP Port 161

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.

## 10.5 802.1X

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.

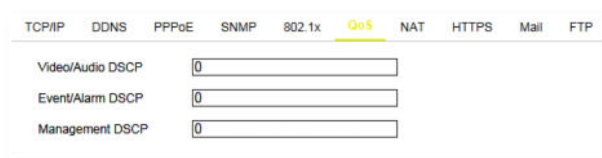
- Before connecting the camera to the protected LAN, request a digital certificate from a Certificate Authority.
- The camera requests access to the protected LAN via the authenticator (a switch).
- The switch forwards the identity and password to the authentication server (RADIUS server).
- The switch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

## 10.6 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).

## 10.7 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**.

## 10.8 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

## 10.9 Mail

TCP/IP DDNS PPPoE SNMP 802.1x QoS NAT HTTPS **Mail** FTP

Sender

Sender's Address

SMTP Server

SMTP Port

E-mail Encryption

☐ Attached Image

Interval  s

☐ Authentication

User Name

Password

Confirm

**Receiver**

No.	Receiver	Receiver's Address	Test
1			<input type="button" value="Test"/>
2			
3			

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 login 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**.



## 10.10 FTP

The screenshot shows the 'FTP' configuration tab. At the top, there are tabs for TCP/IP, DDNS, PPPoE, SNMP, 802.1x, QoS, NAT, HTTPS, Mail, and FTP (which is active). The main configuration area includes:

- Server Address:** 0.0.0.0
- Port:** 21
- User Name:** (empty field)
- Password:** (empty field)
- Confirm:** (empty field)
- Directory Structure:** Save in the root directory (dropdown menu)
- Upload Picture:** (checkbox, currently unchecked)
- Test:** (button)
- Event-Triggered:**
  - Enable Event-Triggered Snapshot:** (checkbox, currently unchecked)
  - Format:** JPEG (dropdown menu)
  - Resolution:** 2048\*1536 (dropdown menu)
  - Quality:** High (dropdown menu)
  - Interval:** 500 (text field) milliseconds (dropdown menu)
  - Capture Number:** 4 (text field)

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.

# 11 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, and the region of interest (ROI).

## In This Chapter

11.1 Streaming.....

59

11.2 Picture Adjustment.....

61

11.3 Text Overlay.....

64

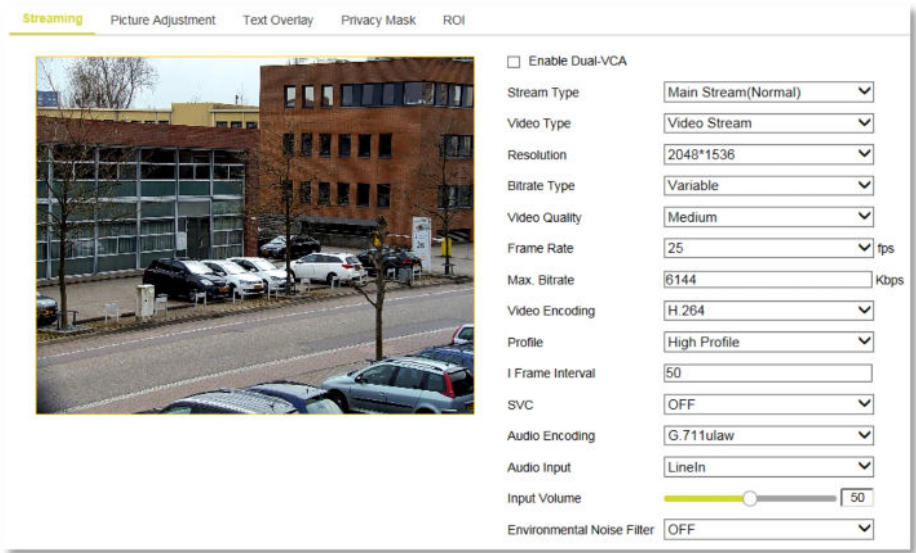
11.4 Privacy Mask.....

65

11.5 ROI.....

66

## 11.1 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 *Profile* list, select **Basic Profile**, **Main Profile** or **High Profile**.

These profiles are available in H.264 encoding mode.
- 11 In *I Frame Interval*, type the required value.

Range: 1~400. This setting determines the distance in frames between two I-frames.
- 12 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.

SVC is a video encoding technology. It extracts frames from the original video and sends these frames to a video recorder (which also supports the SVC function) when the network bandwidth is insufficient.
- 13 Click **Save**.

## » To configure audio streaming

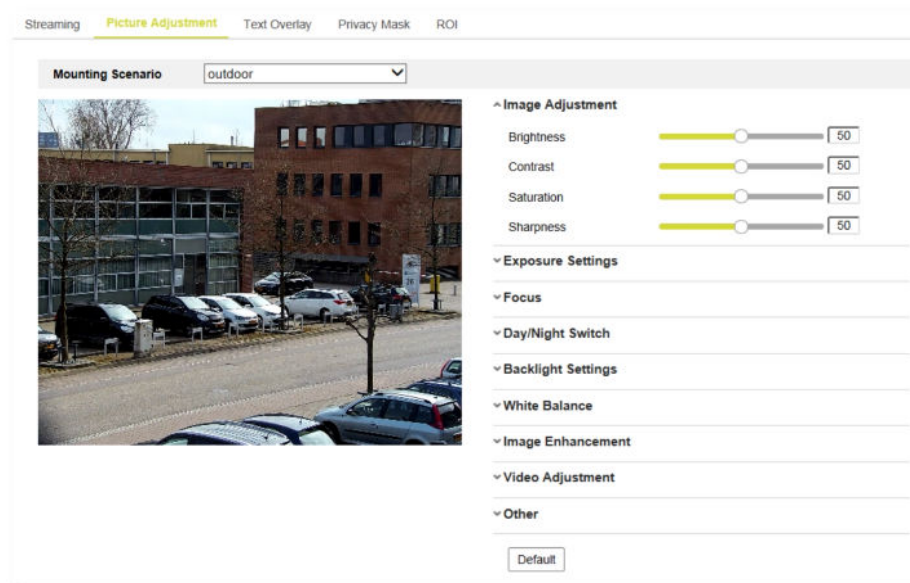
- 1 In the *Audio Encoding* list, select the mode to be used.

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**.

## 11.2 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.

### Mounting Scenario

Depending on where the camera is mounted, select *indoor* or *outdoor*. The two options have different predefined image settings.

### 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

This is where you select the exposure mode of the camera with the associated iris and shutter settings.

- **Exposure Mode** can be set to *Auto*, *Iris Priority*, *Shutter Priority*, and *Manual*. Note that this function varies per camera model.

*Auto:* The iris, shutter and gain values will be adjusted automatically according to the brightness of the environment.

*Iris Priority:* The value of iris needs to be adjusted manually. The shutter and gain values will be adjusted automatically according to the brightness of the environment.

*Shutter Priority:* The value of shutter needs to be adjusted manually. The iris and gain values will be adjusted automatically according to the brightness of the environment.

*Manual:* In Manual mode, you can adjust the values of Gain, Shutter, and Iris manually.

- **Limit Gain** is used to adjust the gain of the image. The value ranges from 0~100.
- **Slow Shutter** can be used in underexposure conditions. It lengthens the shutter time to ensure full exposure. If Slow Shutter is set to ON, the value can be set to *Slow Shutter*\*2, \*4, \*6, and \*8.

## Focus

- The **Focus Mode** can be set to *Auto*, *Manual*, and *Semi-auto*.  
*Auto:* The speed dome focuses automatically at any time according to objects in the scene.  
*Semi-auto:* The speed dome focuses automatically only once after panning, tilting and zooming.  
*Manual:* Use the "Focus -" and "Focus +" buttons on the PTZ control panel to focus manually.
- **Min. Focus distance** is used to limit the minimum focus distance.  
The minimum focus value varies depending on the model of the camera.

## Day/Night Switch

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

- The **Day/Night Switch** mode can be set to *Auto*, *Day*, *Night*, and *Scheduled-Switch*.  
In *Auto* mode, the day mode and night mode can switch automatically according to the light condition of the environment. The switching sensitivity can be set from 1 to 3.  
In *Day* mode, the speed dome displays colour images. This mode is used for normal lighting conditions.  
In *Night* mode, the image is black and white. Night mode can increase the sensitivity in low light conditions.  
In *Scheduled-Switch* mode, you can set the time schedule by defining the start time and end time for day mode. The camera will be in night mode for the remaining time in the schedule.
- **Smart Supplement Light:** If the IR light is on and the image centre is overexposed, you can enable this function.
- **IRLightMode:** In Auto mode, the brightness of the infrared light is adjusted automatically.
- **Brightness Limit:** Move the slider to set a limit to the brightness of the infrared light.

## Backlight Settings

If there's a bright backlight, the subject in front of the backlight appears silhouetted or dark. Backlight compensation (BLC) can correct the exposure of the subject. The backlight environment will be washed out to white, however.

- **BLC:** Select an area from the list or set BLC to Auto.
- **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. This function varies per camera model.
- **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. The White Balance mode can be set to *Auto*, *MWB*, *Outdoor*, *Indoor*, *Fluorescent Lamp*, *Sodium Lamp* and *Auto-Tracking*. This function varies per camera model.

- In **Auto** mode, the camera retains the colour balance automatically according to the current colour temperature.
- In **MWB** (Manual White Balance) mode, you can adjust the colour temperature manually to meet your requirements.
- Select **Outdoor** when the camera is installed in an outdoor environment.
- Select **Indoor** when the camera is installed in an indoor environment.
- Select **Fluorescent Lamp** when there are fluorescent lamps installed near the camera.
- Select **Sodium Lamp** when there are sodium lamps installed near the camera.
- In **Auto-Tracking** mode, the white balance is continuously adjusted in real-time according to the colour temperature of the scene illumination.

## Image Enhancement

This section includes the Digital Noise Reduction and Defog 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]. This function varies per camera model.
- **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.

## Video Adjustment

The options for video adjustment vary per camera model.

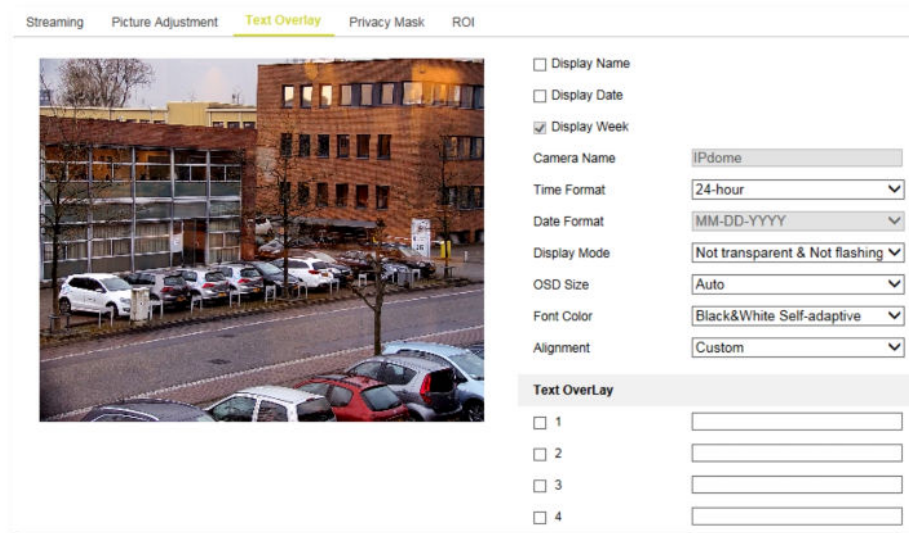
- **Mirror**: Mirrors the image so you can see it inversed. Options: *Center* and *OFF*.
- **Video Standard**: Options: PAL(50HZ) and NTSC(60HZ). Select the applicable video standard according to the video system in your country..
- **Capture Mode** is the selectable video input mode to meet the different demands of the field of view and the resolution.

## Other

This section offers the following functionality:

- Select **Lens Initialisation** to have the camera operate the movements for lens initialisation.
- You can set a **Zoom Limit** value to limit the maximum value of zooming.
- **Local Output**: You can enable or disable the video output through the CVBS interface as required.

## 11.3 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

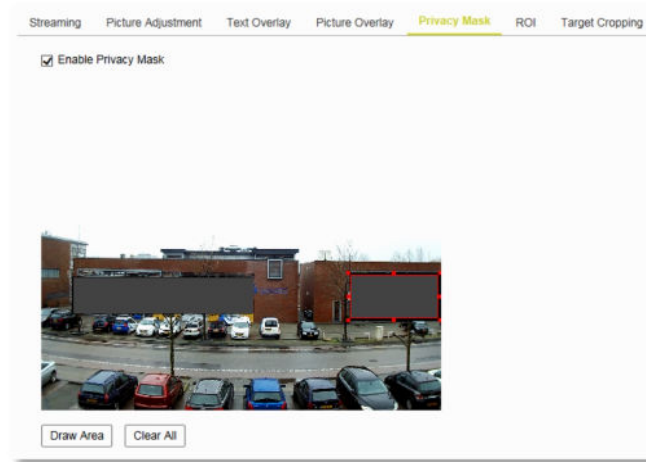
- 1 Select **Display Name**, **Display Date** and **Display Week** as needed.
- 2 In *Camera Name*, type the camera name.
- 3 In the *Time Format*, *Date Format*, *Display Mode*, *OSD Size*, *Font Color* and *Alignment* lists, select the required formatting.
- 4 In the *Live View* window, drag the OSD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



## 11.4 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.

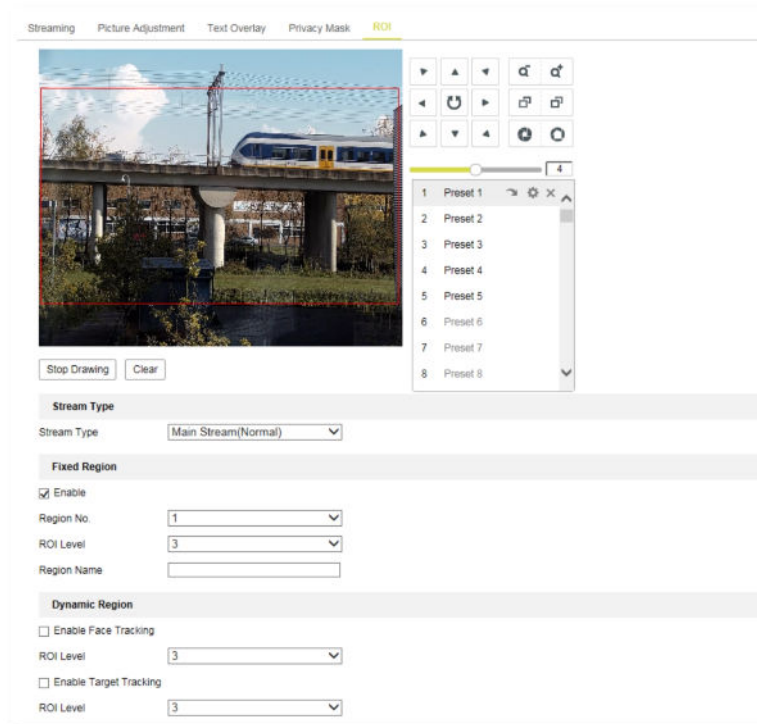
#### » To add a privacy mask

- 1 Select **Enable Privacy Masks**.
- 2 Click the PTZ buttons to define the area where you want to set the privacy mask.
- 3 Click **Draw Area**.
- 4 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.
- 5 Click **Stop Drawing**.  
- or -  
Click **Clear All** to remove all of the areas you set without saving them.
- 6 Click **Add**.  
The privacy mask is saved and added to the Privacy Mask List.
- 7 (Optional) In the **Name** box, type a name for the mask.
- 8 (Optional) In the Active Zoom Ratio box, type an appropriate value.  
The mask will only appear if the zoom ratio is greater than the value defined by you.
- 9 Click **Save**.

#### » To delete a privacy mask

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

## 11.5 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 Click the PTZ buttons to define the area where you want to set the ROI.
- 3 In the *Region No.* list, select a region number.
- 4 Under *Fixed Region*, select **Enable**.
- 5 Click **Draw Area**.
- 6 Drag your mouse pointer across the *Live View* window to draw the region.
- 7 (Optional) Drag the region to position it correctly.
- 8 Click **Stop Drawing**.
- 9 In the *ROI Level* list, select the image quality level.  
The higher the value, the better the image quality.

- 10 In *Region Name*, type a name for the region.
- 11 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 Target Tracking.**  
When a smart event, such as line crossing, is detected, the object which triggered the predefined rule is automatically tracked and the image quality of the tracked target will be increased. Note that at least one smart event should be enabled to enable the target 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**.

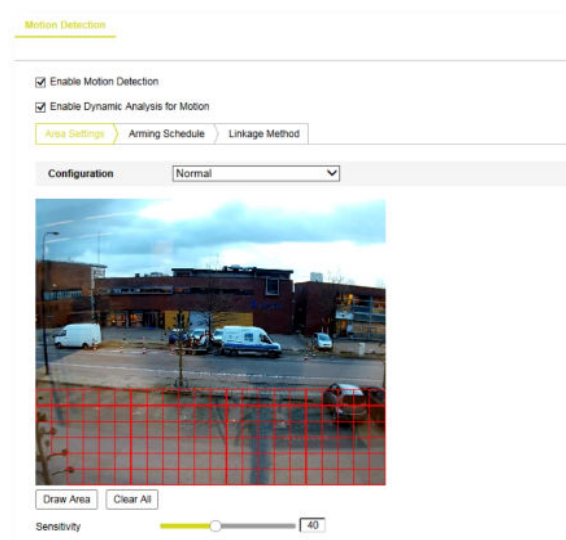
# 12 Events

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

12.1 Motion Detection.....	68
12.2 Video Tampering.....	71
12.3 Alarm Input.....	72
12.4 Alarm Output.....	74
12.5 Exception.....	75
12.6 Audio Exception Detection.....	76
12.7 Face Detection.....	78
12.8 Intrusion Detection.....	80
12.9 Line Crossing Detection.....	82
12.10 Region Entrance Detection.....	84
12.11 Region Exiting Detection.....	86

## 12.1 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 object 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.

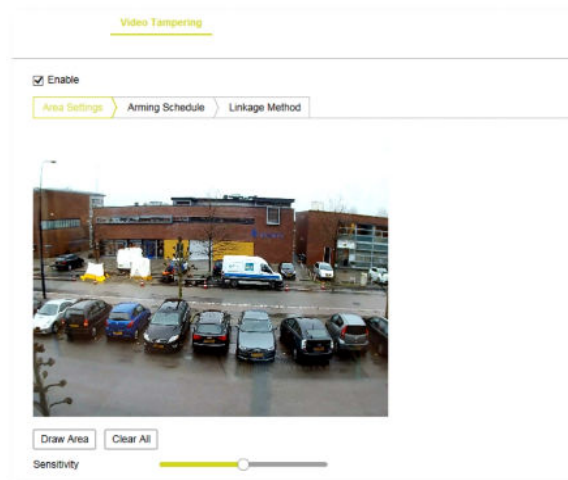
## Expert mode

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**.

## 12.2 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.

## 12.3 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*, *PTZ Linking*.
- 2 (Optional) You can copy your settings to other alarm inputs.
- 3 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.

## PTZ Linking

Select a preset, a patrol or a pattern to be executed by the camera when the alarm input occurs. When you select an option, the other options become unavailable. If necessary, go to the Live View page first, to create the preset, patrol or pattern.

## 12.4 Alarm Output

The screenshot shows the 'Alarm Output' configuration page. At the top, there's a title 'Alarm Output'. Below it, there are several configuration fields: 'Alarm Output No.' with a dropdown menu showing 'A->1', 'IP Address' with a dropdown showing 'Local Configuration', 'Delay' with a dropdown showing 'Manual', 'Alarm Name' with a text field containing '(cannot copy)', and 'Alarm Status' with a dropdown showing 'OFF'. Below these fields is a section titled 'Arming Schedule'. This section contains a grid for the days of the week (Mon, Tue, Wed, Thu, Fri, Sat, Sun) and time slots (0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24). Above the grid are buttons for 'Delete' and 'Delete All'. At the bottom of the page are three buttons: 'Manual Alarm', 'Copy to...', and 'Save'.

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.

## 12.5 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.

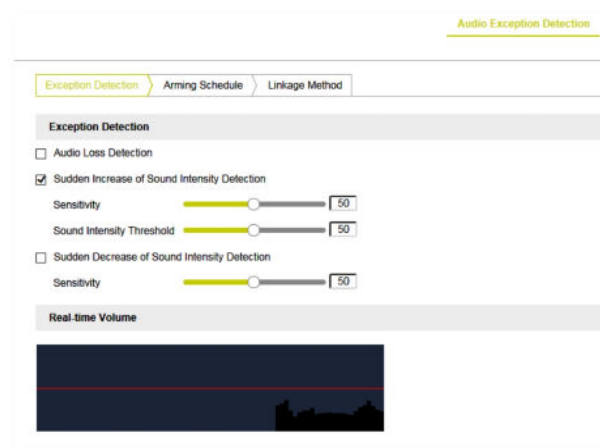
#### Notify Surveillance Center

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.

## 12.6 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.

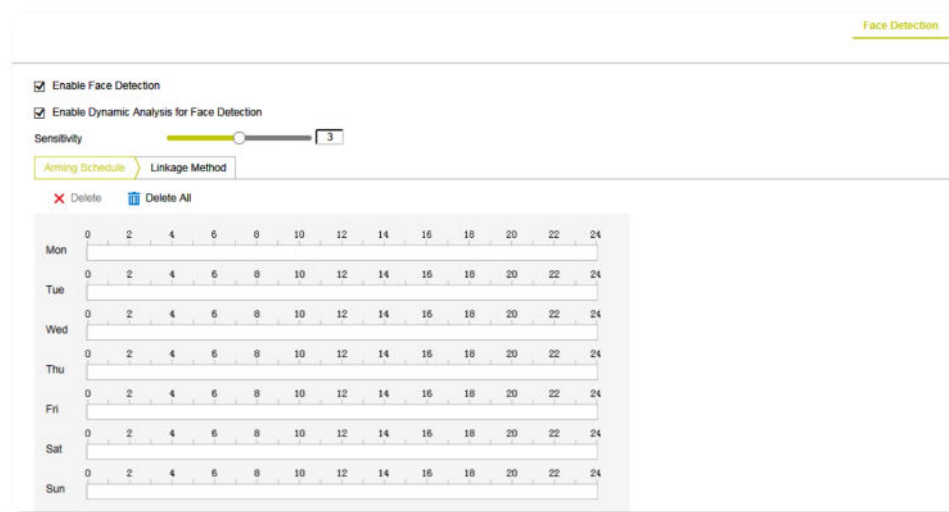
## Trigger Alarm Output

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.

## 12.7 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 object 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.

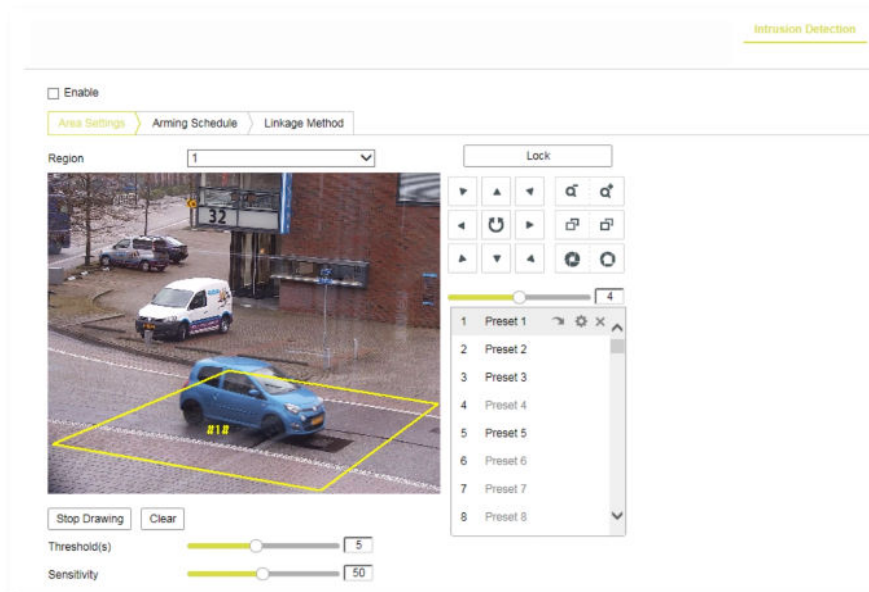
#### **Trigger Alarm Output**

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.

## 12.8 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 Use the PTZ panel to position the camera as required.
- 5 Click **Draw Area**.
- 6 Left-click in the Live Video window to set the first of the four vertexes of the detection area.
- 7 Move the mouse pointer to the next vertex.
- 8 Left-click to set the second vertex.
- 9 In the same way, set vertexes three and four.
- 10 Right-click to complete your drawing.
- 11 Click **Stop Drawing**.



- 12 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.
- 13 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.
- 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, Smart Tracking, 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.

#### Smart Tracking

If enabled, the camera automatically tracks moving objects when the alarm is triggered. Smart tracking settings, such as the tracking duration and zoom ratio can be configured on the Auto Tracking tab of the PTZ page.

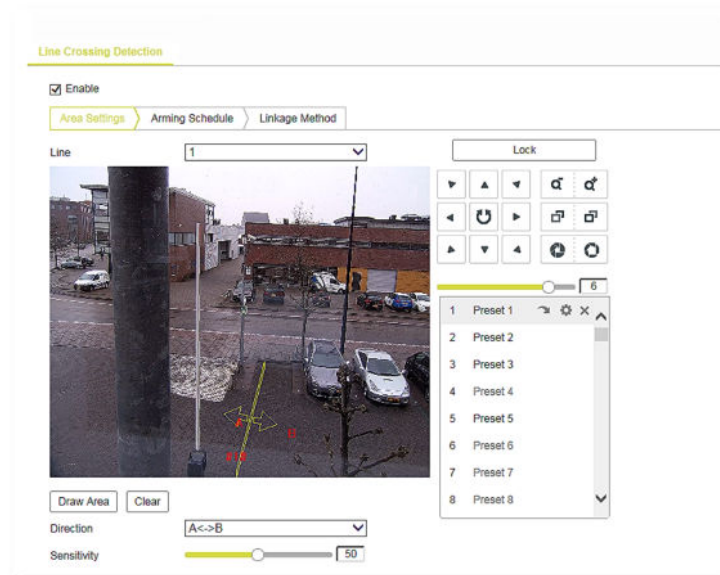
#### Trigger Alarm Output

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.

## 12.9 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 Use the PTZ panel to position the camera as required.
- 5 Click **Draw Area**.  
A virtual line is displayed in the centre of the Live View window.
- 6 Drag the line to move it to the required position.
- 7 Drag the sizing handles to resize the line.
- 8 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.

- 9 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.
- 10 Repeat the steps above to configure other lines.  
Up to 4 lines can be set. You can click Clear to delete all existing lines.
- 11 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, Smart Tracking, 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.

#### Smart Tracking

If enabled, the camera automatically tracks moving objects when the alarm is triggered. Smart tracking settings, such as the tracking duration and zoom ratio can be configured on the Auto Tracking tab of the PTZ page.

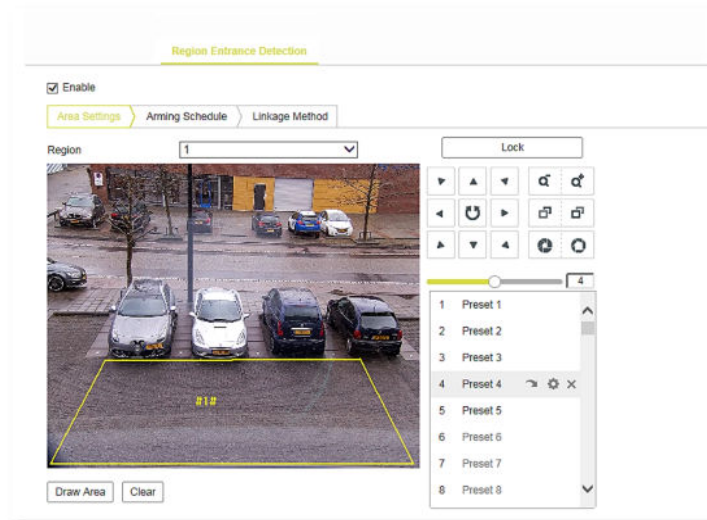
#### Trigger Alarm Output

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.

## 12.10 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 Use the PTZ panel to position the camera as required.
- 5 Click **Draw Area**.
- 6 Left-click in the Live Video window to set the first of the four vertexes of the detection area.
- 7 Move the mouse pointer to the next vertex.
- 8 Left-click to set the second vertex.
- 9 In the same way, set vertexes three and four.
- 10 Right-click to complete your drawing.
- 11 Click **Stop Drawing**.
- 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*, *Smart Tracking*, *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.

#### Smart Tracking

If enabled, the camera automatically tracks moving objects when the alarm is triggered. Smart tracking settings, such as the tracking duration and zoom ratio can be configured on the Auto Tracking tab of the PTZ page.

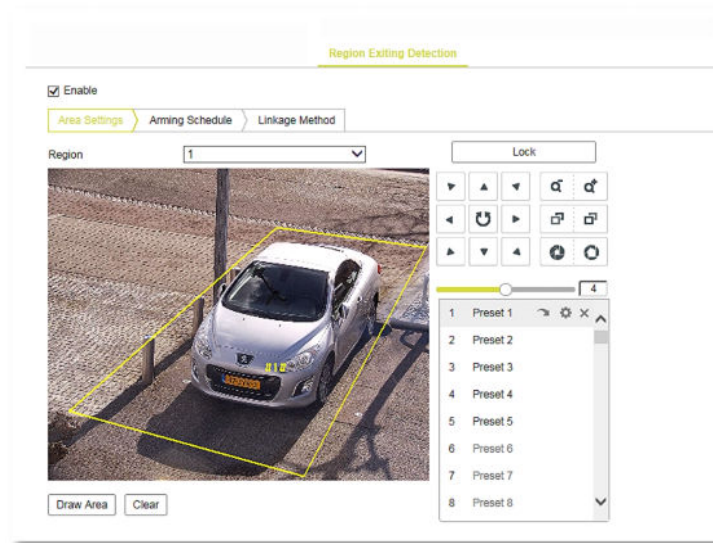
#### Trigger Alarm Output

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.

## 12.11 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 Use the PTZ panel to position the camera as required.
- 5 Click **Draw Area**.
- 6 Left-click in the Live Video window to set the first of the four vertexes of the detection area.
- 7 Move the mouse pointer to the next vertex.
- 8 Left-click to set the second vertex.
- 9 In the same way, set vertexes three and four.
- 10 Right-click to complete your drawing.
- 11 Click **Stop Drawing**.
- 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*, *Smart Tracking*, *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.

#### Smart Tracking

If enabled, the camera automatically tracks moving objects when the alarm is triggered. Smart tracking settings, such as the tracking duration and zoom ratio can be configured on the Auto Tracking tab of the PTZ page.

#### 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.

13

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

13.1 HDD Management.....

13.2 Record Schedule.....

13.3 Capture.....

13.4 Net HDD.....

88

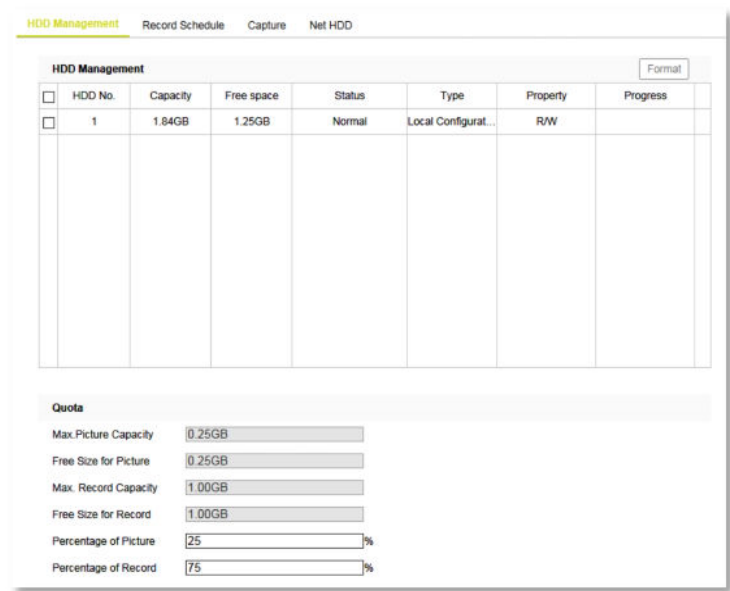
89

91

92

13.1

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**.

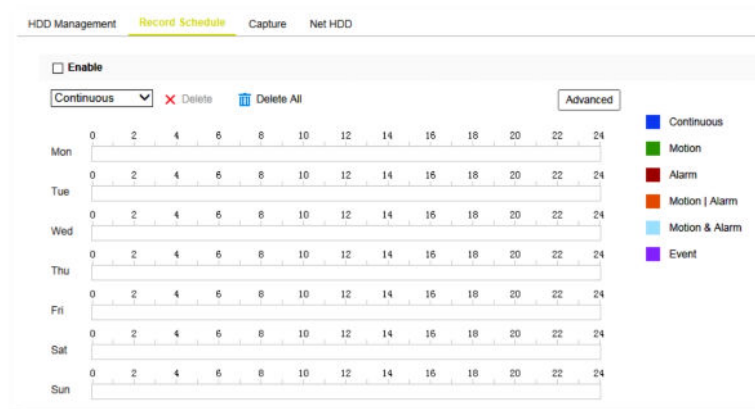
Note that all existing data (if any) on the storage medium will be erased and irretrievably lost!

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.

## 13.2 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).

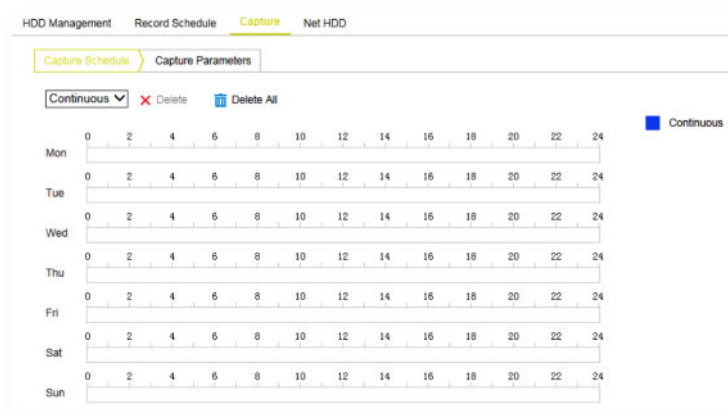
### Recording triggered by Motion & Alarm

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.

## 13.3 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**.

## 13.4 Net HDD

HDD No.	Server Address	File Path	Type	Delete
1	172.6.21.99	\\file01\\fw2	NAS	X
2			NAS	X
3			NAS	X
4			NAS	X
5			NAS	X
6			NAS	X
7			NAS	X
8			NAS	X

Mounting Type: NAS SMB/CIFS User Name:  Password:

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**.

14

PTZ

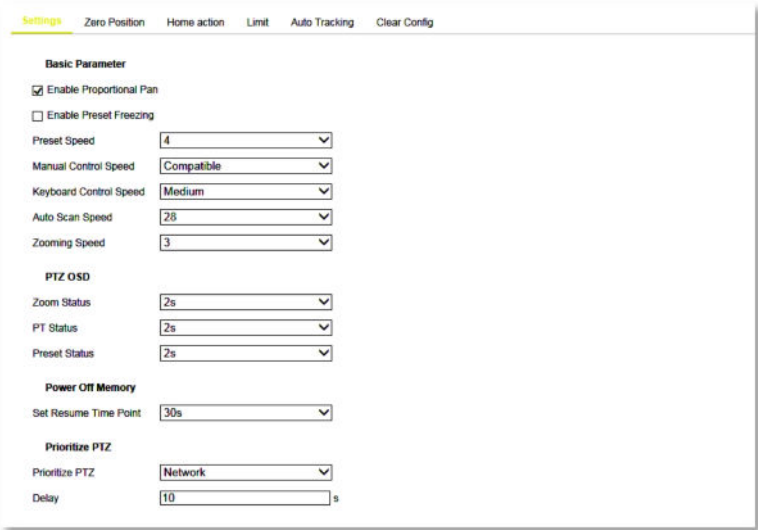
On the PTZ page, you can configure the PTZ parameters of the camera.

In This Chapter

14.1 Settings.....	94
14.2 Zero Position.....	96
14.3 Home Action.....	97
14.4 Limit.....	98
14.5 Auto Tracking.....	99
14.6 Clear Config.....	100

14.1

Settings



PTZ > Settings

What this tab is for

This is where you can configure the basic PTZ parameters, including proportional pan, preset freezing, preset speed, etc.

Basic parameters

Here you can configure the following settings:

- Proportional Pan:** If you enable this function, the pan/tilt speeds change according to the amount of zoom. When there is a large amount of zoom, the pan/tilt speed will be lower to prevent the image from moving too fast in the live view window.
- Preset Freezing:** This function enables the live view to switch directly from one scene saved as a preset to another, without showing the intermediate areas between the two, to ensure the surveillance efficiency. It can also reduce the use of bandwidth in a digital network system. Note that the Preset freezing function is invalid when you call a pattern.

- **Preset Speed:** You can set the speed of a defined preset from 1 to 8.
- **Manual Control Speed:** The camera provides five manual control modes: *Compatible*, *Pedestrian*, *Non-motor Vehicle*, *Motor Vehicle*, and *Auto*.
- **Keyboard Control Speed:** Define the speed of PTZ control by a keyboard as *Low*, *Medium* or *High*.
- **Auto Scan Speed:** The auto scan speed can be set from level 1 to 40.
- **Zooming speed:** The zoom speed is adjustable from level 1 to 3.

## PTZ OSD

This is where you set the on-screen display duration of the PTZ status.

- **Zoom Status:** Set the OSD duration of the zooming status as *2 seconds*, *5 seconds*, *10 seconds*, *Normal Close* or *Normal Open*.
- **PT Status:** Set the azimuth angle display duration while panning and tilting as *2 seconds*, *5 seconds*, *10 seconds*, *Normal Close* or *Normal Open*.
- **Preset Status:** Set the preset name display duration while calling the preset as *2 seconds*, *5 seconds*, *10 seconds*, *Normal Close* or *Normal Open*.

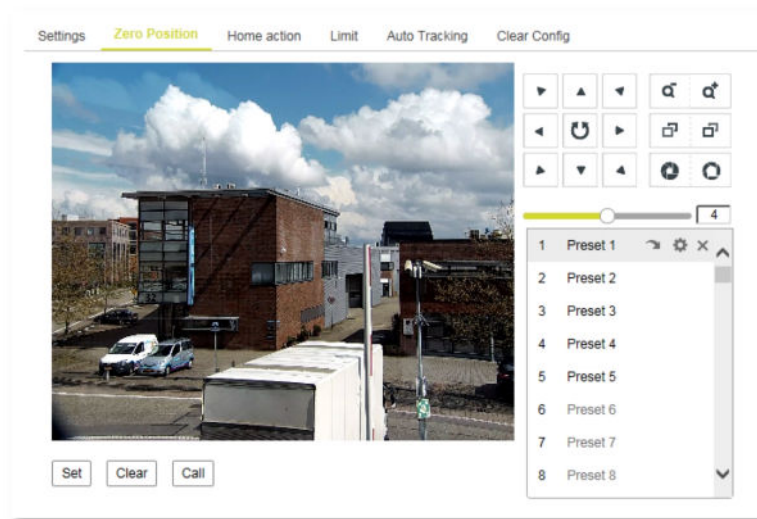
## Power-off Memory

The dome can resume its previous PTZ status or actions after it restarted from a power-off. You can set the point in time for which the dome resumes its PTZ status. You can set it to resume the status of 30 seconds, 60 seconds, 300 seconds or 600 seconds prior to power-off.

## Prioritize PTZ

The speed dome can be controlled by network and RS-485 signals. You can set the control priority of these two signals. An Operator action has priority over that of a User. When the Operator is controlling the speed dome, the User cannot control it. When the Operator finishes, the User can control the speed dome after the Delay time. The Delay time can be set from 2 to 200 seconds.

## 14.2 Zero Position



PTZ > Zero Position

### What this tab is for

The zero position is the origin of the PTZ coordinates. It can be the factory default zero position but you can also customise the zero position to your needs.

#### » To set the zero position

- 1 Click the PTZ control buttons to define a position as the zero position of the camera. You can also call a defined preset and set it as the zero position.
- 2 Click **Set** to save the position.

#### » To call the zero position

- Click **Call**.

#### » To delete the zero position

- Click **Clear**.  
The zero position set by the user is deleted.  
The factory default zero position is restored.



## 14.3 Home Action

PTZ > Home action

### What this tab is for

You can configure the camera to perform a specific action automatically in a user-defined time period.

#### » To configure a park action

This feature allows the camera to start a predefined park action (scan, preset, pattern, etc.) automatically after a period of inactivity (park time).

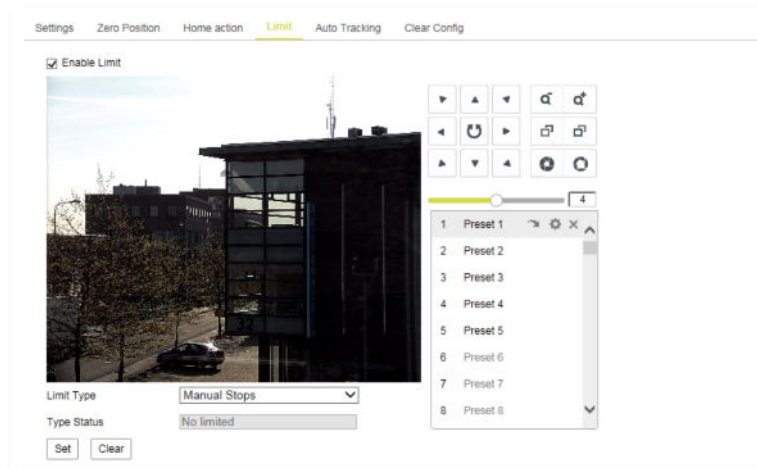
- 1 Select **Enable Park Action**.
- 2 In **Park Time**, type a value.  
Range: 5~720 s.  
This is the inactivity time of the camera before it starts the park action.
- 3 In the **Action Type** list, select the action to be performed.

**Note:** The Scheduled Tasks function has priority over the Park Action function. When these two functions are set at the same time, only the Scheduled Tasks function takes effect.

#### » To schedule a task

- 1 Select **Enable Scheduled Task**.
- 2 Set the **Park Time**.  
You can set the park time (a period of inactivity) before the dome starts the scheduled tasks.
- 3 Choose the day for which you want to schedule the task.
- 4 Drag the mouse pointer across the time line to set the start time and end time for the task.
- 5 In the task list, select the type of task to be performed.  
The time of each task cannot be overlapped. Up to 10 tasks can be configured for each day.
- 6 (Optional) After you set the scheduled task, you can copy the task to other days.

## 14.4 Limit



PTZ > Limit

### What this tab is for

On this tab, you can program the camera to move within configurable limit stops (left/right, up/down).

#### » To set limit stops

- 1 Use the PTZ panel to position the camera as required.
- 2 Select **Enable Limit**.
- 3 Click to open the **Limit Type** list.
- 4 Select **Manual Stops** or **Scan Stops**.

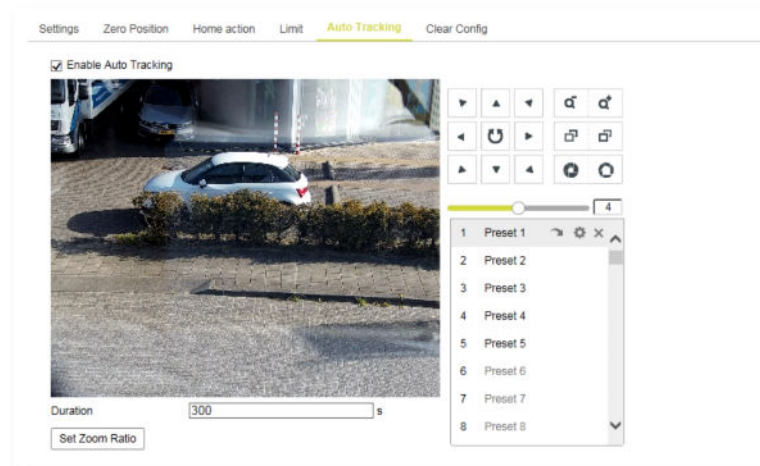
*Manual Stops:* You can operate the PTZ control panel manually only in the limited surveillance area.

*Scan Stops:* The random scan, frame scan, auto scan, tilt scan, panorama scan is performed only in the limited surveillance area.

Note that Manual Stops has priority over Scan Stops. When you set the two limit types at the same time, Manual Stops is valid and Scan Stops is invalid.

- 5 Click the PTZ control buttons to find the left/right/up/down limit stops.  
You can also call the defined presets and set them as the limits of the camera.
- 6 Click **Set** to save the limits.
- 7 (Optional) Click **Clear** to clear the limits.

## 14.5 Auto Tracking



PTZ > Auto Tracking

### What this tab is for

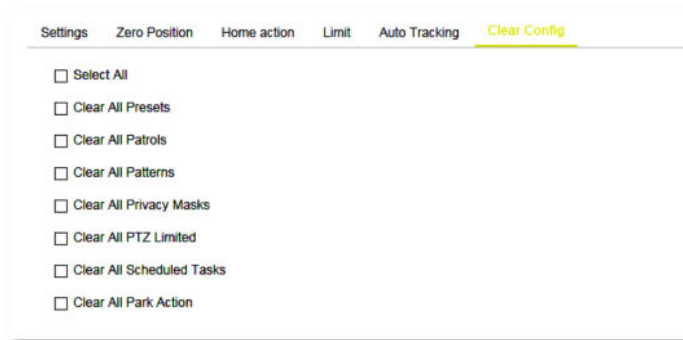
If Auto Tracking is enabled, the camera automatically tracks moving objects.

#### » To configure Auto Tracking

- 1 Select **Enable Auto Tracking**.
- 2 Click the PTZ buttons to select an object.
- 3 Click **Set Zoom Ratio**.  
This sets the current zoom ratio as the tracking zoom ratio.
- 4 Set the tracking duration.  
Range: 03~00 s. The speed dome stops tracking when the duration time is up.  
Setting the duration to 0 means that there's no duration when the speed dome tracks.

**Note:** Not all speed dome models support this function. Please take the browser interface of the actual product as standard.

## 14.6 Clear Config



*PTZ > Clear Config*

### What this tab is for

On this tab, you can clear PTZ configurations, including all presets, patrols, patterns, privacy masks, PTZ limits, scheduled tasks, and park actions.

#### » To clear PTZ configurations

- 1 Select the items that you want to clear.
- 2 Click **Save**.

# Appendix: NTCIP Configuration

The National Transportation Communications for ITS Protocol (NTCIP) provides a communications standard that ensures the interoperability and interchangeability of traffic control and Intelligent Transportation Systems (ITS) devices. This appendix provides information about the conformance groups which are supported by the PD1103.

## In This Chapter

Supported conformance groups.....	101
SNMP MIB.....	103

## Supported conformance groups

The PD1103 firmware supports all the mandatory parts and some of the optional parts (see table below) of the NTCIP CCTV specification as laid down in the NTCIP 1205:2001 v01.08 document. This means that - in terms of section 4 of this document - the following conformance groups are supported.

Conformance group	Reference	Conformance requirement
Configuration	NTCIP 1201:1996	mandatory
CCTV Configuration	NTCIP 1205	mandatory
Motion Control	NTCIP 1205	optional

*Conformance statement table*

## Configuration

Most of the Configuration conformance group objects listed below contain static device information.

- Global Set ID parameter
- Maximum modules parameter
- Module table
- Module number
- Module device node
- Module make
- Module model
- Model version
- Module type
- Base standards parameter

## CCTV configuration

The CCTV Configuration conformance group consist of objects that specify the configuration parameters of a CCTV. For details, refer to NTCIP 1205. Conformance requirement within the group is mandatory.

- rangeMaximumPreset
- rangePanLeftLimit
- rangePanRightLimit
- rangePanHomePosition
- trueNorthOffset
- rangeTiltUpLimit
- rangeTiltDownLimit
- rangeZoomLimit
- rangeFocusLimit
- rangeIrisLimit
- rangeMinimumPanStepAngle
- rangeMinimumTiltStepAngle
- timeoutPan
- timeoutTilt
- timeoutZoom
- timeoutFocus
- timeoutIris
- labelTable
  - labelEntry
  - labelIndex
  - labelText
  - labelFontType
  - labelHeight
  - labelColor
  - labelStartRow
  - labelStartColumn
  - labelStatus
  - labelLocationLabel
  - labelEnableTextDisplay

## Motion control

The Motion Control group defines the variables that provide PTZ control. For details, refer to NTCIP 1205. Conformance requirement within the group is mandatory.

- presetGotoPosition
- presetStorePosition
- positionPan
- positionTilt
- positionZoomLens
- positionFocusLens
- positionIrisLens

**Note:** Camera control through NTCIP on TKH Security multichannel products is limited to video channel 1.

## SNMP MIB

NTCIP has its own SNMP MIB. This database is used to store information, which is used to control cameras and other devices in the transportation management system. An electronic version of the MIB is available from a NEMA FTP site. To get access to the FTP site, send your name, organisation name, and email address to [ntcip@nema.org](mailto:ntcip@nema.org), and request access.

# Index

## 8

802.1X..... 51

## A

About this manual..... 5  
Alarm Input..... 72  
Alarm Output..... 74  
Appendix: NTCIP Configuration..... 101  
Audio Exception Detection..... 76  
Authentication..... 43  
Auto Tracking..... 99

## B

Basic Information..... 34

## C

Capture..... 91  
CCTV configuration..... 102  
Clear Config..... 100  
Compliance information..... 7  
Configuration..... 101  
Connect the camera to a LAN..... 12  
Connect the camera to a WAN..... 14  
Connect to network..... 12

## D

DDNS..... 48

## E

Events..... 68  
Exception..... 75

## F

Face Detection..... 78  
FTP..... 57  
Functions overview..... 9

## G

Get access to the camera..... 17  
Get access via Device Manager..... 18  
Get access via UPnP..... 19  
Get access via web browser..... 17

## H

HDD Management..... 88  
Home Action..... 97  
HTTPS..... 54

## I

Install the videoplayer plug-in..... 21  
Intrusion Detection..... 80  
IP Address Filter..... 44

## L

Limit..... 98  
Line Crossing Detection..... 82  
Live View..... 23  
Local Configuration..... 40  
Log..... 39  
Log on to the camera..... 20

## M

Mail..... 56  
Motion control..... 102  
Motion Detection..... 68

## N

NAT..... 53  
Net HDD..... 92  
Network..... 46

## P

Picture Adjustment..... 61  
Playback..... 32  
Power-up action..... 21  
PPPoE..... 49  
Privacy Mask..... 65  
PTZ..... 94

## Q

QoS..... 52

## R

Record Schedule..... 89  
Region Entrance Detection..... 84  
Region Exiting Detection..... 86  
ROI..... 66  
RS-485..... 38

## S

Safety and compliance..... 6  
Safety instructions..... 6  
Security..... 42  
Settings..... 94  
SNMP..... 50  
SNMP MIB..... 103



Storage.....	88
Streaming.....	59
Supported conformance groups.....	101
System.....	34
System requirements.....	12

## **T**

TCP/IP.....	46
Text Overlay.....	64
Time Settings.....	35

## **U**

Upgrade & Maintenance.....	36
User Management.....	42

## **V**

Video Tampering.....	71
Video/Audio.....	59

## **Z**

Zero Position.....	96
--------------------	----