Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

360/950/980-series Cameras

User Manual

Status:	v20251015	13-okt-2025
Author:	Onno Verkerk	

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Revision history

Nr	Date	Remarks
1	24-jun-2022	Version 1.0 initial version
2	20-okt-2022	Version 1.1 reworked into new format, with minor modifications
3	17-mei-2024	Version 1.2 minor modifications
4	04-dec-2024	Version 1.3 OSD text length 54, not 16
5	05-dec-2024	Version 1.4 OSD subtitle count not 5 but 3
6	20-dec-2024	Version 1.5 Corrected documentation on privacy mask configuration
7	12-jun-2025	Version v20250612 added chapter 4 on Cyber Security
8	13-okt-2025	Version v20251013 rewritten to reflect new camera web app; this manual now applies to full 360/950/980-series IPC and PTZ cameras.
9	15-okt-2025	Version v20251015 removed references to non-existent documentation.

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

Copyright © 2023-2025 TKH Security B.V.

360/950/980-series Cameras User Manual v20251015

TKH Security reserves the right to modify specifications stated in this manual without prior notice.

Brand names

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

Liability

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

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

How to contact us

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

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

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

TKH Security LLC
5340 Spectrum Drive, Suite C
Frederick, Maryland 21703
United States of America

General : +1 301 444 2200
Email : sales.us@tkhsecurity.com

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Table of Contents

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

1 About this manual

What's in this manual

This manual provides the installation assistance for the 360/950/980-series Cameras. The manual gives you all the information you need to install the product. It tells you:

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

Where to find more information

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

Who this manual is for

These instructions are for all professionals who will install 360/950/980-series 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

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

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

2 Overview

The DNN Network IP Camera features newest Deep Neural Network technology. With new hardware accelerated engine which benefits from SoC Structure, it provides professional-level Video Analytics (VA) functions (e.g., object recognition, facial detection, facial recognition, license plate recognition).

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

3 Menu Tree

For cameras with RS-485, there are six main tabs including <System>, <Streaming>, <Recording>, <Analytics>, <Camera>, <Pan Tilt> on the Home Page.

For PTZ Cameras, there are six main tabs including <System>, <Streaming>, <Recording>, <Analytics>, <Camera>, <PTZ> on the Home Page.

For other cameras, there are five main tabs including <System>, <Streaming>, <Recording>, <Analytics>, <Camera> on the Home Page.

NETWORK CAMERA / FISHEYE CAMERA / NETWORK PTZ

Users can monitor the live video of the targeted area. If on another page, click NETWORK CAMERA / FISHEYE CAMERA / NETWORK PTZ to return to the homepage.

System Setting

The administrator can set host name, system time, root password, network related settings, etc.

Streaming Setting

The administrator can configure Video Configuration, Video Rotation, Video Text Overlay, Privacy Mask, Video ROI, Video ROI Encoding, Streaming Protocol and Audio in this page.

Recording Setting

The administrator can set Video Playback, Recording Device and Storage Management.

Analytics Setting

The administrator can set video analytics including Video Analytics-AI, Motion Detection, Audio Detection, etc.

Camera Setting

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

This setting page is only available for the administrator and user accounts that have been granted the privilege of camera control. The administrator and users can adjust various camera parameters including Exposure, White Balance, Picture Adjustment, Noise Reduction, Digital Zoom, HDR, etc.

Pan Tilt Setting

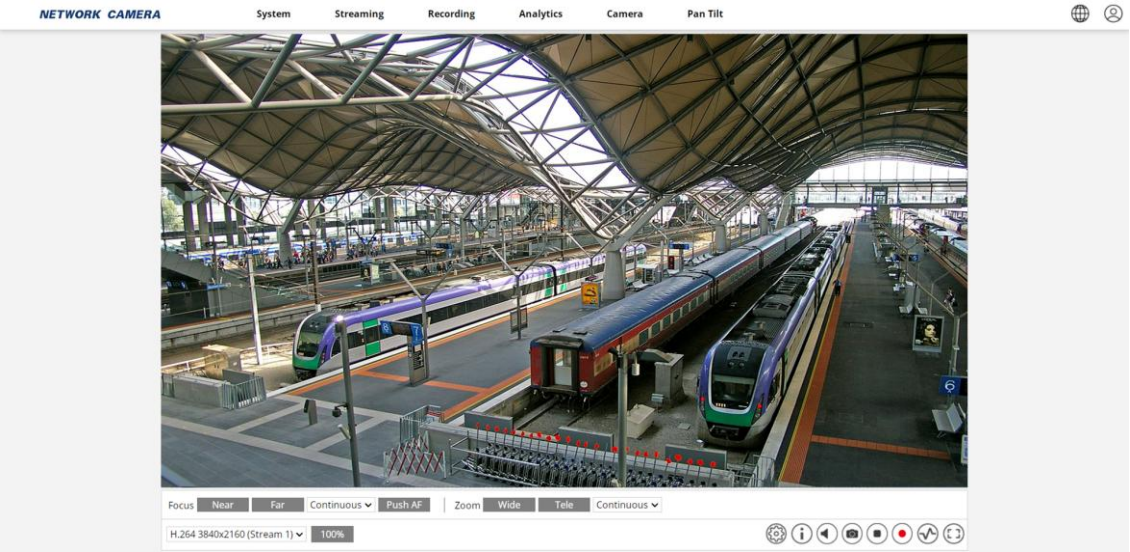
This setting page is only available for the administrator and user accounts that have been granted the privilege of camera control. The administrator and users can set preset point and sequence line in this page. However, only the administrator can access the <Pan/Tilt Control> setting to activate the pan/tilt functions and select the RS-485 protocol. Pan Tilt function is only available for camera models with RS-485.

PTZ Setting

This setting page is only available for the administrator and user accounts that have been granted the privilege of camera control. The administrator and users can program Preset Point(s), Cruise Line(s), Auto Pan Path(s) and Sequence Line(s), as well as adjust PTZ settings including Home Function, Tilt Range, etc. PTZ Setting function is only available for PTZ Cameras.

3.1 Home Page

There are several function buttons on this page. Detailed information of each item is as described in the following section.



Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

NOTE: The function buttons on the Home page will vary according to different camera models.

3.1.1 Function Items on Home Page

Multiple Languages Support

Multiple languages are supported, including German, English, Spanish, French, Italian, Japanese, Portuguese, Russian, Simplified Chinese and Traditional Chinese for the viewer window interface.

Log Out

Click on <> to logout the system. Click <Login> to re-login the camera with another username and password.

Display Stream Selection

According to the streaming setting, users can choose the one stream to display from the drop-down menu.

Full Resolution

Click the <100%> button to show the live view at full resolution. If the full resolution is larger than the user screen size, use the smaller image to navigate in the image.

Pan/Tilt Control

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Users can implement pan/tilt control by moving the cursor to the live video pane, then left click and drag the yellow pointer in any direction. Pan/Tilt Control function is only available for PTZ Cameras.

Setting 

Click to turn on/turn off the camera setting of whether to keep the aspect ratio at full screen. The function enables maintaining the aspect ratio of the image according to the selected resolution when in full screen mode.

Information 

Click to show/hide the camera information. Users can instantaneously check the basic information of the camera, such as video format, video codec, video bitrate, video framerate and video drop.

Listen  (On / Off)

Click on <Listen> to mute / activate the audio. Users must select the suitable transmission mode under Streaming> Audio to enable this function.

NOTE: Both Talk and Listen functions are only available for user accounts that have been granted this privilege by the administrator. Please refer to section System> Users> Accounts for further details.

Snap Shot 

Click on the button and the JPEG snapshots will automatically be saved in the appointed place. The default place of saving snapshots is determined by the browser's settings.

Stop Video / Live View  (Pause / Restart)

Click on <Pause> to disable video streaming, the live video will be displayed as <>. Click on <Restart> to show the live video again.

Recording  (On / Off)

Click on <Record> and the Live View through the web browser will be directly recorded to the specific location on the local hard drive. The default storage location for the web recording is determined by the browser's settings.

Trigger 

Click on <Trigger> to activate the manual trigger. Please refer to section Manual Trigger of chapter Analytics> General for further details.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Max Window

Image display size can be adjusted to full screen. To exit full screen mode, users can tap <Esc> on the keyboard.

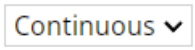
Wiper

Click to command wiper to clean the cover of the PTZ. Wiper function is only available for PTZ Cameras.

Manual Focus Adjustment

- **Near / Far** 

Hold the <Near / Far> button, and implement continuous focus adjustment.

- **Near / Far Steps** 

Select a step value from the drop-down menu and click <Near / Far> button to shift the focus lens according to the defined value. Select Continuous, then click and hold to adjust the focus continuously. This function is only for ABF Box and Motorized Lens Models.

- **Push AF** 

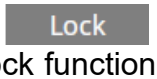
The Push AF function is for setting the focus automatically with one click. This function is only for ABF Box and Motorized Lens Models.

- **Manual** 

In <Manual> mode, click near / far to manually adjust the focus. This function is only for Zoom Lens and PTZ Cameras.

- **Auto** 

In <Auto> mode, the camera will keep in focus automatically and continuously regardless of zoom changes or any view changes. This function is only for Zoom Lens and PTZ Cameras.

- **Lock** 

The Lock function is to lock the ABF function of the Box camera after the auto focus is adjusted to the best position. Click on this button to lock the ABF function of the camera. Click again to disable this function and adjust the focus of the camera. This function is only for ABF Box.

Lock ABF Function Instruction (ABF Box IP Cameras Only)

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

This function is to prevent the camera from being out of focus when the camera is moved afterwards or is accidentally adjusted locally or remotely via NVR/VMS. Follow the instruction steps below for the best focus adjustment.

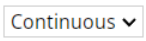
Step 1: Once the camera is powered on, manually adjust the lens to the approximate zoom and focus position.
Step 2: Click <Push AF>.
Step 3: Click <Lock> to lock the current focus position of the camera.

Zoom Adjustment

- **Wide / Tele** 

Click the <Wide / Tele> button, and implement zoom adjustment or drag the zoom bar to adjust the zoom ratio. This function is only for Zoom Lens and Motorized Lens Models.

  For zoom lens models, optical zoom in/out functions can also be implemented by moving the cursor to the live video pane and scrolling the mouse wheel in Normal View display mode.

- **Wide / Tele Steps** 

Select a Wide /Tele step value from the drop-down menu to zoom out / zoom in according to the define value. Select Continuous, then click and hold to zoom out / zoom in continuously. This function is only for Motorized Lens Models.

Go Preset / Run Sequence / Run Cruise

Go to <PTZ> → <Preset>/<Cruise>/<Sequence> to setup the relevant settings beforehand. Select a Preset / Cruise / Sequence line from the drop-down list and the camera will start running. **This function is only for PTZ Cameras.**

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

3.1.2 Function Differences among Models

The table below shows the available function items seen on the home page for different IP camera models. The first table below lists the applicable lens for different IP camera models. According to the applied lens, the supported functions will vary; refer to the tables below for details. In each table, the applicable lens and the supported function items are marked by “v”.

Applicable Lens for Different IP Camera Models

Lens / Model	Motorized	Zoom	CS Mount	Fisheye
Fixed Dome Camera	v	v	-	-
Bullet Camera	v	v	-	-
Board Camera		v		-
Box Camera	-	-	v	-
Fisheye Camera (8)	-	-	-	v
PTZ Camera	-	v	-	-

Supported Functions for the Applied Lens

Function / Lens		Motorized	Zoom	CS Mount	Fisheye**		PTZ
					Wall Mount	Ceiling Mount	
Multiple Language		v	v	v	v	v	v
Log Out		v	v	v	v	v	v
Full Resolution		v	v	v	v	v	v
Setting		v	v	v	v	v	v
Information		v	v	v	v	v	v
Listen		v	v	v	v	v	v
Snap Shot		v	v	v	v	v	v
Stop Video/Live View Pause/Restart		v	v	v	v	v	v
Recording (On / Off)		v	v	v	v	v	v
Trigger		v	v	v	v	v	v
Max Window		v	v	v	v	v	v
Wiper		-	-	-	-	-	v
Manual Focus Adjust.	Near/Far	v	v	v	-	-	v
	Near/Far Steps	v	-	v	-	-	-
	Push AF	v	v	v	-	-	-
	Manual						
	Auto	-	v	-	-	-	v
	Lock	-	-	v	-	-	-

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Function \ Lens		Motorized	Zoom	CS Mount	Fisheye**		PTZ
					Wall Mount	Ceiling Mount	
Zoom Adjust.	Wide/Tele	V	V	-	-	-	V
	Wide/Tele Steps	V	-	-	-	-	-
	Zoom Bar	-	V	-	-	-	V
Go Preset / Run Sequence / Run Cruise		-	-	-	-	-	V

**The function items for fisheye IP camera models will vary according to different installation methods. Two installation methods are provided: wall mount and ceiling mount installation.

Function \ Lens	Fisheye**	
	Ceiling Mount	Wall Mount
1 View No Dewarp	V	V
1 View ePTZ Dewarp	V	V
2 Views 180 Dewarp	V	-
4 Views ePTZ Dewarp	V	-
1 View 180 Dewarp	-	V
1 View 180 and 2 Views ePTZ	-	V

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

3.2 System

Under the tab <**System**>, there are categories including: <Information>, <Date and Time>, <Users>, <Network Basic>, <Network Advanced>, <Security>, <Event Management>, <Schedule Profile>, <Iris Adjustment>, <Log Management> and <Maintenance>.

NOTE: Only Administrator can access the <System> configuration page.

3.2.1 Information

The Information setting can be found under the path: **System> Information**.

The current device information and software version is displayed on the software version page.

3.2.2 Date and Time

The Date and Time setting can be found under the path: **System> Date and Time**.

Time Zone and Format

- **Date Format**
  Choose a time format (yyyy/mm/dd or dd/mm/yyyy) from the drop-down menu. The format of the date will be changed according to the selected format.

- **Time Format**
  The time format is hh:mm:ss.

- **Time Zone**
  Select the time zone from the drop-down menu according to the location of the camera.

Time Synchronization

- **Sync with PC**
  Select <Sync with PC>, video date and time display will synchronize with the PC's.

- **Manual**
  The administrator can set video date and time manually.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

- **Sync with NTP Server**
  Network Time Protocol (NTP) is an alternate way to synchronize the camera's clock with a NTP server. Please specify the server that is wished to synchronize in the entry field. Then select an update interval from the drop-down menu. For further information about NTP, please see the web site: www.ntp.org.

  NOTE: The synchronization will be done every time the camera boots up.

Daylight Saving

To enable DST (Daylight Saving Time), please check the item and then specify the time offset and the DST duration. The format for time offset is [hh:mm:ss]; for instance, if the amount of time offset is one hour, please enter "01:00:00" into the field.

Click on <Save> to confirm the setting.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

3.2.3 Users

The Users setting can be found under this path: **System> Users**.

Admin Password

This item is for the administrator to reset password. Enter the current password in <Old Admin Password> and enter the new password in <New Admin Password> and <Confirm Admin Password>. The maximum length is 14 characters. The input characters / numbers will be displayed as dots for security purposes. Click on <Save> to confirm the changes. After the changes are confirmed, the web browser will ask the administrator to re-login to the camera with the new password.

NOTE: The following characters are valid: A-Z, a-z, 0-9, !#$%&'-.@^_~.

Accounts

This item allows the administrator to add / edit / delete users. Select "Add User" from the <Manage User> drop-down menu. Enter the new user's name in <User Name> and the password in <User Password>. Username can be up to 16 characters, and the maximum length of the password is 14 characters. Tick the boxes below to give privileges for functions, including "Camera control", "Talk" and "Listen". Click on <Save> to add the new user. The name of the new added user will be displayed when under "Edit User" in the drop-down menu. There is a maximum of twenty user accounts.

Select "Edit User" to edit user password or permissions, or delete the user. Click on <Save> to confirm the changes, or click on <Delete> to remove the selected name.

- **I/O access**
  This item supports fundamental functions that enable users to view the live video when accessing to the camera.

- **Camera Control**
  This item allows the appointed user to change camera parameters on the <Camera> and <Pan Tilt> setting page.

- **Talk/Listen**
  This item allows the appointed user in the local site (camera site) to communicate with, for instance, the administrator in the remote site.

Authentication Setting

- **HTTP Authentication Type**
  This setting allows secured connections between the IP camera and web browser by enforcing access controls to web resources. When users approach to the web browser, it'll ask for username and password, which protects the camera settings or live streaming information from snooping. There are two security models available: Basic and Digest. Refer to the descriptions below for more details.

  - Basic
    This mode can only provide basic protection for the connection security. There will still be risks for the password being intercepted.

  - Digest
    Digest mode is a safer option for protection. The password is sent in an encrypted format to prevent it from being stolen.

- **Streaming Authentication Type**
  This setting provides security against unauthorized users from getting streaming via Real Time Streaming Protocol (RTSP). If the setting is enabled, users will be requested to enter user name and password before viewing the live streams. There are three security modes available: Disable, Basic and Digest. Refer to the descriptions below for more details.

  - Disable
    If disable mode is selected, there will be no security provided to against unauthorized access. Users will not be asked to input user name and password for authentication.

  - Basic
    This mode can only provide basic protection for the live streams. There will still be risks for the password being intercepted.

  - Digest
    Digest mode is a safer option for protection. The password is sent in an encrypted format to prevent it from being stolen.

Account Lockout Function

The Account Lockout Function is to lock out an account when someone tries to log on unsuccessfully several times in a row. To protect user's account, "Account

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Lockout Function'' is activated when multiple login failures occur. Enable the <Account Lockout Function> and enter the number of threshold and duration.

- **Threshold**
  Threshold is a maximum number of login attempts, ranging from 5-20 times. The default value is 5 (attempts).

- **Duration**
  Duration is the length of time that the account remains locked once the account lockout function is triggered, ranging from 1-60 minute(s). The default value is 10 (mins).

Click on <Save> to confirm the setting.

3.2.4 Network Basic

The Network Basic setting can be found under this path: **System> Network Basic**.

This setting page is for setting a new IP address for the camera, configuring other network-related parameters and activating IPv6 address (if the network supports it).

Host Name
Administrator can set the host name of the camera.

IP Address
This setting menu is for configuring a new IP address for the camera. To setup an IP address, please find out the network type first. Contact the network provider for it. Then refer to the network type and follow the instructions to setup the IP address.

NOTE: If the network type is Point-to-Point Protocol over Ethernet (PPPoE), please obtain the PPPoE username and password from the network provider.

- **Get IP Address Automatically**
  Select the item and click <Save> to confirm the new setting. A note for camera system reboot will appear. Click <OK> and the camera system will restart. The camera will be assigned with a new IP address. Close the web browser and search the camera through the installer program: DeviceDiscovery.exe. Please refer to DeviceDiscovery User's Manual for more details.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

NOTE: Please contact the sales representatives for DeviceDiscovery User's Manual documents.

NOTE: Before searching the camera through DeviceDiscovery.exe, please record the camera's MAC address, which can be found on the label or on the package container of the camera, for later use and identification in the future.

- **Use Fixed IP Address**
  Select the item and insert the new IP address, e.g. 192.168.7.123. Note that the inserted IP address should be in the same LAN as the PC's IP address. Then go to the Default gateway (explained later) blank and change the setting, e.g. 192.168.7.254. Click on <Save> to confirm the new setting. A note for system restart will appear, click <OK> and the camera system will restart. Wait for 15 seconds. The camera's IP address in the URL bar will be changed, and users have to login again.

  When using a static IP address to connect the camera, users can access the camera by inputting the IP address in the URL bar and hit <Enter> on the keyboard. Alternatively, users can access the camera by the installer program: DeviceDiscovery.exe. Please refer to DeviceDiscovery User's Manual for more details.

  NOTE: Please contact the sales representatives for DeviceDiscovery User's Manual documents.

  - IP Address
    This is necessary for network identification.

  - Subnet Mask
    It is used to determine if the destination is in the same subnet. The default value is "255.255.255.0".

  - Default Gateway
    This is the gateway used to forward frames to destinations in different subnet. Invalid gateway setting will fail the transmission to destinations in different subnet.

  - Primary DNS
    Primary DNS is the primary domain name server that translates hostnames into IP addresses.

  - Secondary DNS

Secondary DNS is a secondary domain name server that backs up the primary DNS.

- **Use PPPoE**
  For the PPPoE users, enter the PPPoE username and password into the enter fields, and click on <Save> to complete the setting.

Network Service Port

The following introduces the camera's Web Server port, RTSP port, MJPEG over HTTP port, HTTPS port and RTSP URL.

- **Web Server Port**
  The default web server port is 80. With the default web server port '80', users can simply input the IP address of the camera in the URL bar of a web browser to connect the camera. When the web server port is changed to any number other than 80, users have to enter the camera's IP address followed by a colon and the port number. For instance, a camera whose IP address is set as 192.168.0.100 and web server port as 8080 can be connected by entering "http://192.168.0.100:8080" in the URL bar.

- **RTSP Port**
  The default setting of RTSP Port is 554; the RTSP Port should be set as 554 or from the range 1024 to 65535.

- **RTSPS Port**
  The default setting of RTSPS Port is 322; the RTSPS Port should be set as 322 or from the range 1024 to 65535.

- **MJPEG over HTTP Port**
  The default setting of MJPEG over HTTP Port is 8008; the MJPEG over HTTP Port should be set as 8008 or from the range1024 to 65535.

- **HTTPS Port**
  The default setting of HTTPS Port is 443; the HTTPS Port should be set as 443 or from the range 1024 to 65535.

NOTE: Please make sure the port numbers set above are not the same with each other; otherwise, network conflict may occur.

- **RTSP URL**
  When users use RTSP players to view the live streaming, the camera provides the flexibility to configure the streaming access name for

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

stream 1 to stream 4. The streaming format is **rtsp://<ip address>:<rtsp port>/<access name>**. Take a camera whose IP address is set as 192.168.0.100 for example, if users enter "liveview.1" in the blank of stream 1 access name, the streaming address of stream 1 will be rtsp://192.168.0.100:554/liveview.1.

NOTE: The maximum length of the access name is 32 characters, and the valid characters are A-Z, a-z, 0-9 and !#$%&'-.@^_~.

Network Interface Card

- **Link Speed**
  Select <Auto (Max 1 Gbps)> or <Auto (Max 100 Mbps)> from the drop-down menu to automatically detect the supported link speed of the customer's device. Select <1000BaseTX (Full Duplex)>, <100BaseTX (Full Duplex)>, <100BaseTX (Half Duplex)>, <10BaseT (Full Duplex)>, or <10BaseT (Half Duplex)> from the drop-down menu to manually set the appropriate specification.

- **MTU Size**
  MTU is the largest size of a single data packet that the Network Interface Card can send. Proper MTU size helps avoid fragmentation and ensures efficient data transmission. The value range is from 500 to 1500.

IPv6 Address Configuration
If the network supports IPv6, users can check the box beside <Enable IPv6>. An IPv6 address will appear beside <IPv6 Address>, and users can use it to connect to the camera.

Click on <Save> to confirm the setting.

3.2.5 Network Advanced

The Network Advanced setting can be found under this path: **System> Network Advanced**.

3.2.5.1 SNMP

The SNMP (Simple Network Management Protocol) setting can be found under this path: **System> Network Advanced> SNMP**.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

With Simple Network Management Protocol (SNMP) support, the camera can be monitored and managed remotely by the network management system.

SNMP V1 / V2

- **Enable SNMP V1 / V2**
  Select the version of SNMP to use by checking the box.

- **Read Community**
  Specify the community name that has read-only access to all supported SNMP objects. The default value is “public”.

- **Write Community**
  Specify the community name that has read / write access to all supported SNMP objects (except read-only objects). The default value is “private”.

SNMP V3

SNMP V3 supports an enhanced security system that provides protection against unauthorized users and ensures the privacy of the messages. Users will be requested to enter security name, authentication type, authentication password, encryption type, and encryption password while setting the camera connections in the network management system. With SNMP V3, the messages sent between the cameras and the network management system will be encrypted to ensure privacy.

- **Enable SNMP V3**
  Enable SNMP V3 by checking the box.

- **Security Name**
  The maximum length of the security name is 32 characters.

  NOTE: The valid characters are A-Z, a-z, 0-9 and !#$%&’-.@^_~.

- **Authentication Type**
  There are two authentication types available: MD5 and SHA. Select <SHA> for a higher security level.

- **Authentication Password**
  The authentication password must be 8 characters and the maximum length is 32 characters. The input characters / numbers will be displayed as dots for security purposes.

  NOTE: The valid characters are A-Z, a-z, 0-9 and !#$%&’-.@^_~.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

- **Encryption Type**
  There are two encryption types available: DES and AES. Select <AES> for a higher security level.

- **Encryption Password**
  The minimum length of the encryption password is 8 characters and the maximum length is 512 characters. The input characters / numbers will be displayed as dots for security purposes. The encryption password can also be left blank. However, the messages will not be encrypted to protect privacy.

NOTE: The valid characters are A-Z, a-z, 0-9 and !#$%&'-.@^_~.

Traps For SNMP V1 / V2 / V3

Traps are used by the camera to send messages to a management system for important events or status changes.

- **Enable Traps**
  Check the box to activate trap reporting.

- **Trap Address**
  Enter the IP address of the management server.

- **Trap Community**
  Enter the community to use when sending a trap message to the management system.

- **Trap Option**
  - Warm Start
    A Warm Start SNMP trap signifies that the SNMP device, i.e. IP camera, performs software reload.

Click on <Save> when completed.

3.2.5.2 UPnP

The UPnP setting can be found under this path: **System> Network Advanced> UPnP**.

UPnP Setting

- **Enable UPnP**
  When the UPnP is enabled, whenever the camera is presented to the LAN, the icon of the connected cameras will appear in My Network Places to allow for direct access.

NOTE: To enable this function, please make sure the UPnP component is installed on the computer. Please refer to Appendix A: Install UPnP Components for UPnP component installation procedure.

- **Enable UPnP Port Forwarding**
  When the UPnP port forwarding is enabled, the camera is allowed to open the web server port on the router automatically.

  NOTE: To enable this function, please make sure that the router supports UPnP and it is activated.

- **Friendly name**
  Set a name for the camera for identity.

Click on <Save> when finished.

3.2.5.3 DDNS

The DDNS setting can be found under this path: **System> Network Advanced> DDNS**.

Dynamic Domain Name System (DDNS) allows a host name to be constantly synchronized with a dynamic IP address. In other words, it allows those using a dynamic IP address to be associated to a static domain name so others can connect to it by name.

DDNS Enable
Enable the DDNS function.

Provider
Select one DDNS host from the provider list.

Host Name
Enter the registered domain name in the field.

Username/E-Mail
Enter the username or E-mail required by the DDNS provider for authentication.

Password/Key
Enter the password or key required by the DDNS provider for authentication.

Click on <Save> when finished.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

3.2.5.4 VLAN

The VLAN setting can be found under this path: **System> Network Advanced> VLAN**.

VLAN Enable
Enable the VLAN function.

- **VLAN ID**
  Enter the VLAN ID. The allowed range of VLAN ID is from 1 to 4095. The default value is 20.

CoS
CoS stands for Class of Service. The higher the value of CoS is, the better transmission performance will be. The value also determines the transmission priority among the following three classes: Live Video, Live Audio and Management.

- **Live Video**
  The value range is from 0 to 7.
- **Live Audio**
  The value range is from 0 to 7.
- **Management**
  The value range is from 0 to 7.

Click on <Save> when finished.

3.2.5.5 QoS

The QoS (Quality of Service) setting can be found under this path: **System> Network Advanced> QoS**.

QoS allows providing differentiated service levels for different types of traffic packets, which guarantees delivery of priority services especially when network congestion occurs. Adapting the Differentiated Services (DiffServ) model, traffic flows are classified and marked with DSCP (DiffServ Codepoint) values, and thus receive the corresponding forwarding treatment from DiffServ capable routers.

DSCP (Differentiated Service Code Point)

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

The DSCP value range is from 0 to 63. The default DSCP value is 0, which means DSCP is disabled. The camera uses the following QoS Classes: Management, Video and Audio.

- **Management DSCP**
  The class consists of HTTP traffic: Web browsing.

- **Stream 1~4 DSCP**
  Users can set the Audio/Video DSCP of each stream.

  - Video DSCP
    The class consists of applications such as MJPEG over HTTP, RTP/RTSP and RTSP/HTTP.

  - Audio DSCP
    This setting is only available for the cameras that support audio.

Click on <Save> when finished.

NOTE: To enable this function, please make sure the switches / routers in the network support QoS.

3.2.5.6 LLDP

The LLDP (Link Layer Discovery Protocol) setting can be found under this path: **System> Network Advanced> LLDP**.

LLDP is a network protocol used by devices to advertise their identity, capabilities, and network interfaces to directly connected devices. Enable LLDP by turning on button.

3.2.5.7 RTMP

The RTMP (Real Time Messaging Protocol) setting can be found under this path: **System> Network Advanced> RTMP**.

RTMP (Real-Time Messaging Protocol) is designed for streaming audio, video, and data over the internet, with a focus on low latency and real-time delivery. This function enables live streaming of content to external platforms.

RTMP
Enable RTMP by turning on button.

Selected stream
Select the specific stream1~4.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Server URL
Enter the URL of the server.

Stream key
Enter the key.

Click on <Save> to save the setting.

3.2.6 Security

The Security setting can be found under this path: **System> Security**.

3.2.6.1 HTTPS

The HTTPS setting can be found under this path: **System> Security> HTTPS**.

HTTPS
<HTTPS> allows secure connections between the camera and the web browser using <Secure Socket Layer (SSL)> or <Transport Layer Security (TLS)>, which ensure camera settings or Username / Password info from snooping. It is required to install a self-signed certificate or a CA-signed certificate for implementing HTTPS.

To use HTTPS on the camera, an HTTPS certificate must be installed. The HTTPS certificate can be obtained by either creating and sending a certificate request to a Certificate Authority (CA) or creating a self-signed HTTPS certificate, as described below.

- **Disable HTTPS**
  The default setting of HTTPS is disabled.

- **Enable HTTPS**
  Check the box to enable HTTPS secure connection. Once enabled, choose one from the following two secure modes.

  - Enable HTTPS only
    Under this mode, the secure connection is ensured by HTTPS only.

  - Enable HTTP & HTTPS
    Under this mode, HTTP & HTTPS secure connections are enabled.

Click on <Save> to save the setting.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Installed Certificate

Click on <Properties> to see further details of the certificate, or click on <Remove> to remove it.

Install New Certificate

Before a CA-issued certificate is obtained, users can create and install a certificate first from the drop-down menu.

- **Generate Self-signed Certificate**

  Select <Generate Self-signed Certificate> from the drop-down menu. Click on <Create> under "Create self-signed certificate" and provide the requested information to install a self-signed certificate for the camera. Please refer to the last part of this section Provide the Certificate Information for more details.

  NOTE: Generate self-signed certificate does not provide the same high level of security as when using a CA-issued certificate.

- **Generate Certificate Request**

  Select <Generate Certificate Request>from the drop-down menu. Click on <Create Certificate Request> to create and submit a certificate request in order to obtain a signed certificate from CA.

  Provide the request information in the create dialog. Please refer to the following section Provide the Certificate Information for more details.

  When the request is complete, the subject of the Created Request will be shown in the field. Click on <Properties> below the Subject field, copy the PEM-formatted request and send it to the selected CA.

  When the signed certificate is returned, install it by uploading the signed certificate.

  Click on <Remove> to remove the certificate.

- **Upload Certificate**

  Select a file to upload certificate for Private Key and Certificate.

Provide the Certificate Information

To create a Self-signed Certificate or a Certificate Request to CA, please enter the information as requested.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

	• Generate Self-signed Certificate	Generate Certificate Request
Country	V	V
State or province	V	V
Locality	V	V
Organization	V	V
Organizational Unit	V	V
Common Name	V	V
Valid days	V	-

- **Country**
  Enter a two-letter combination code to indicate the country the certificate will be used in. For instance, type in “US” to indicate United States.

- **State or province**
  Enter the local administrative region.

- **Locality**
  Enter other geographical information.

- **Organization**
  Enter the name of the organization to which the entity identified in “Common Name” belongs.

- **Organization Unit**
  Enter the name of the organizational unit to which the entity identified in “Common Name” belongs.

- **Common Name**
  Indicate the name of the person or other entity that the certificate identifies (often used to identify the website).

- **Valid days**
  Enter the period in days (1 to 9999) to indicate the valid period of certificate.

  Click on <OK> to save the Certificate Information after completing the setting.

3.2.6.2 IP Filter

The IP Filter setting can be found under this path: **System> Security> IP Filter**.

With IP Filter, users can allow or deny specific IP addresses from accessing the camera.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

IP Filter

Enable the IP Filter function, the listed IP addresses in the <Filtered IP Addresses> list box will be allowed / denied to access the camera.

- **Deny / Allow the IP address listed below to access this camera**
  Select <Deny the IP address listed below to access this camera> or <Allow the IP address listed below to access this camera> to deny/ allow the IP addresses in the <Filtered IP Addresses> list box to access the camera.

- **Filtered IP Addresses**
  Once enabled, the listed IP addresses in the <Filtered IP Addresses> list box will be allowed / denied to access the camera. To remove an IP address from the <Filtered IP Address> list, please select the address and click on <Delete>.

- **Add New IP Address to Filter Table**
  Input IP address at the blank space beside the <New IP Address> and click <Add>. The newly-added address will be shown in the <Filtered IP Addresses> list. Up to 256 IP address entries can be specified.

  In addition, to filter a group of IP addresses, enter an address at the blank space followed with a slash and a number ranging from 1 to 31, e.g. 192.168.2.81/30. The number after the slash can define how many IP addresses will be filtered. For details, please refer to the following example.

  - Example: Filtering a group of consecutive IP addresses
    The steps below show what will be filtered when 192.168.2.81/30 is entered.

    Step 1: Convert 192.168.2.81 to binary numbers. The binary numbers are 11000000.10101000.00000010.01010001. Users can refer to Appendix B: IP Addresses from Decimal to Binary for converting the IP addresses to binary numbers. The number “30” after the slash is referring to the first 30 digits of the binary numbers.

    Step 2: Convert a few IP addresses before and after 192.168.2.81 to binary numbers. Then compare their first 30 digits with the binary numbers of 192.168.2.81.

    a. Convert 192.168.2.80 to binary numbers. The binary numbers are 11000000.10101000.00000010.01010000. The first 30

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

digits are the same with the binary numbers of 192.168.2.81, thus 192.168.2.80 will be filtered.

b. Convert 192.168.2.79 to binary numbers. The binary numbers are 11000000.10101000.00000010.01001111. The first 30 digits are different with the binary numbers of 192.168.2.81, thus 192.168.2.79 will not be filtered. This also means the IP addresses before 192.168.2.79 will not be filtered. Therefore, users can stop converting the IP addresses before 192.168.2.79 to binary numbers.

c. Repeat the same procedure in “a” with the IP addresses after 192.168.2.81. Stop when the situation occurs in “b” happened. Namely, the 30th digit of the binary numbers of IP address 192.168.2.84 is different, and will not be filtered.

As a result, the IP addresses 192.168.2.80 to 192.168.2.83 will be filtered when entering 192.168.2.81/30. The following table clearly shows the 30th digit of the binary numbers of IP addresses 192.168.79 and 192.168.84 are different from the others. Therefore, these two IP addresses will not be filtered.

IP Addresses	Binary Numbers
192.168.2.79	**11000000.10101000.00000010.01001**111
192.168.2.80	**11000000.10101000.00000010.01010**000
192.168.2.81	**11000000.10101000.00000010.01010**001
192.168.2.82	**11000000.10101000.00000010.01010**010
192.168.2.83	**11000000.10101000.00000010.01010**011
192.168.2.84	**11000000.10101000.00000010.01010**100

Click on <Save> to save the setting.

3.2.6.3 IEEE 802.1X

The IEEE 802.1X setting can be found under this path: **System> Security> IEEE 802.1X**.

The camera is allowed to access a network protected by 802.1X/EAPOL (Extensible Authentication Protocol over LAN).

Disable IEEE 802.1X
The default setting of IEEE 802.1X is disabled.

Enable IEEE 802.1X
Choose < Enable IEEE 802.1X > to enable the IEEE 802.1X function.

Select one among the four protocol types: <EAP-MD5>, <EAP-TLS>, <EAP-TTLS> and <EAP-PEAP>.

Users need to contact with the network administrator for gaining certificates, usernames and passwords.

Username
Enter the username.

Password
Enter the password.

CA Certificate
The CA certificate is created by the Certification Authority for the purpose of validating itself. Upload the certificate for checking the server's identity.

Client Certificate / Private Key
Upload the Client Certificate and Private Key for authenticating the camera itself.

Private Key
Enter the password (maximum 16 characters) for user identity.

Anonymous ID
Enter the user identity associated with the certificate. Up to 16 characters can be used.

Inner Auth
Select one among the six inner auth: <CHAP>, <EAP-MSCHAPV2>, <EAP-MD5>, <MSCHAP>, < MSCHAPV2>, and < PAP>. The default setting is <EAP-MD5>.

Click on <Save> to save the setting.

3.2.7 Event Management

The Events Management setting can be found under this path: **System> Event Management**.

Click on <Event Management>, there will be a drop-down menu with tabs including <Mail>, <FTP>, and <HTTP>.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

3.2.7.1 Mail

The Mail setting can be found under this path: **System> Event Management> Mail**.

The administrator can send an E-mail via Simple Mail Transfer Protocol (SMTP) when an event is triggered. SMTP is a protocol for sending E-mail messages between servers. SMTP is a relatively simple, text-based protocol, where one or more recipients of a message are specified and the message text is transferred.

Two sets of SMTP can be configured. Each set includes SMTP Server, SMTP Server Port, Account Name, Password and SMTP SSL. For SMTP server, contact the network service provider for more specific information.

Click on <Save> when finished. Then, please click on <Test> to check the connection between the camera and the specified SMTP (mail) server.

3.2.7.2 FTP

The FTP setting can be found under this path: **System> Event Management> FTP**.

The administrator can set the camera to send the alarm messages to a specific File Transfer Protocol (FTP) site when an event is triggered. Users can assign alarm message to up to two FTP sites. Each set includes server, server port, username, password, remote folder and Passive Mode.

Click on <Save> when finished. Then, please click on <Test> to check the connection between the camera and the specified FTP server.

3.2.7.3 HTTP

The HTTP setting can be found under this path: **System> Event Management> HTTP**.

An HTTP Notification server can listen for the notification messages from the cameras by triggered events. Enter the HTTP details, which include server name (for instance, http://192.168.0.100/admin.php), username, and password in the fields.

Click on <Save> when finished.

3.2.8 Schedule Profile

The Schedule Profile setting can be found under this path: **System> Schedule Profile**.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

This function allows users to setup schedules for Analytics or Camera> User Setting Profile. It supports up to 10 sets of time frames in the time frame list.

Schedules Setup

Step 1: Select specific weekdays from the edit item below.

Step 2: Specify the start time (hour:minute) and the time duration (hour:minute) to activate the schedule triggered features. The setting range for the time duration is from 00:00 to 168:59.

Step 3: Click on <Save> to save the setup. Alternatively, click on <Delete> to delete a chosen time frame.

3.2.9 Iris Adjustment

The Iris Adjustment setting can be found under this path: **System> Iris Adjustment**.

For users utilizing a CS mount lens with auto-iris, if iris adjustment is required, please refer to the iris adjustment procedure on the settings page. The adjustment process typically takes 30 to 120 seconds.

3.2.10 Log Management

The Log Management setting can be found under this path: **System> Log Management**.

3.2.10.1 System Log

The System Log setting can be found under this path: **System> Log Management> System Log**.

The camera keeps a record of the system's behavior and information related to the camera. These log data can be exported for future use. Click <Download> to download all system log files from camera, it will take around 3 seconds to generate log files and download them to local PC.

3.2.10.2 User Information

The User Information setting can be found under this path: **System> Log Management > User Information**.

The administrator can view the privileges of each added user (refer to section Users) shown as below.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Admin: 1:1:1:1:1
1:1:1:1:1= I/O access: Camera control: Talk: Listen: Administrator (refer to section Users)

The fifth digit indicates whether it is a User or an Administrator. “0” represents “User”, and “1” represents Administrator.

For other digits, “1” denotes this user is allowed to access the function; whereas “0” suggests no access for this user is allowed.

3.2.10.3 Parameters

The Parameters setting can be found under this path: **System> Log Management> Parameters**.

Click on this item to view the parameter settings of the entire system, such as Camera Settings, Mask Information and Network Information.

3.2.11 Maintenance

The Maintenance setting can be found under this path: **System> Maintenance**.

3.2.11.1 Software Upgrade

The Software Upgrade setting can be found under this path: **System> Maintenance> Software Upgrade**.

NOTE: Make sure the upgrade software file is available before carrying out software upgrade.

The procedure of software upgrade is as below.

Step 1: Select firmware files, such as <OS System Files>, <App: Video Analytics (AI)> or <MCU Firmwares>, to upgrade.

NOTE: Do not change the name of the upgrade file, or the system will fail to find the file.

Step 2: Click on <Upgrade>. Then the system will prepare to start the software upgrade. Subsequently, an upgrade status bar will be displayed on the page to show the current upgrade process. After the upgrade process is finished, it will return to the <Home> page.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

3.2.11.2 Factory Default

The Factory Default setting can be found under this path: **System> Maintenance> Factory Default**.

Users can follow the instructions on this page to reset the camera to factory default settings if needed.

Full System Restore

Click on <Full Restore> to recall the factory default settings. The camera system will restart in 30 seconds. The IP address will be restored to default. After the camera system is restarted, reconnect the camera using the default IP address. The default IP address is **10.x.y.z**, where x.y.z are the last octets of the device MAC address.

Restore Factory Settings Only (Keep Network Setting)

Click on <Partial Restore> to recall the factory default settings (excluding network settings). The camera system will restart in 30 seconds. Refresh the browser page after the camera system is restarted.

NOTE: The IP address will not be restored to default.

Reboot System

Click on <Reboot> and the camera system will restart without changing the current settings. Refresh the browser page after the camera system is restarted.

3.2.11.3 Configuration Files

The Configuration Files setting can be found under this path: **System> Maintenance> Configuration Files**.

Users can export configuration files to a specified location and retrieve data by uploading the configuration file to the camera.

Export SW Configuration Files

Users can save the system settings by exporting a configuration file (.bin) to a specified location for future use. Click on <Export>, and the popup File Download window will come out. Click on <Save> and specify a desired location for saving the configuration file.

Upload SW Configuration Files

To upload a configuration file to the camera, select a SW configuration file and then click on <Upload> for uploading.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Upload HW Configuration Files (FAE Only)

This feature is restricted to FAE use only.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

3.3 Streaming

Under the tab <**Streaming**>, there are categories including: <Video Configuration>, <Video Rotation>, <Video Text Overlay>, <Privacy Mask>, <Video ROI>, <Video ROI Encoding>, <Streaming Protocol>, and <Audio>.

In the Streaming submenu, the administrator can configure specific video resolution, video compression mode, video protocol, audio transmission mode, etc. Further details of these settings will be specified in the following sections.

NOTE: Only Administrator can access the <Streaming> configuration page.

3.3.1 Video Configuration

The Video Configuration setting can be found under this path: **Streaming> Video Configuration**.

NOTE: Fisheye Setting is only available for Fisheye IP Camera. For other cameras, please proceed to the Encoding section.

Fisheye Setting (Fisheye IP Camera Only)

Users can choose a dewarping type for correcting the fisheye source images, and select the camera's installation method to view the dewarped images with the correct viewing modes.

Dewarping

This item is for users to choose a method to dewarp the fisheye source images. The options are <Edge Dewarping> and <No Dewarping>. Please see below for more details.

- **Edge Dewarping**

  Edge Dewarping is a dewarping method that corrects fisheye source images only by the camera. Dewarping images by the camera can reduce network usage and image processing load of the backend device. It also allows the camera to record or take snapshots of the dewarped images.

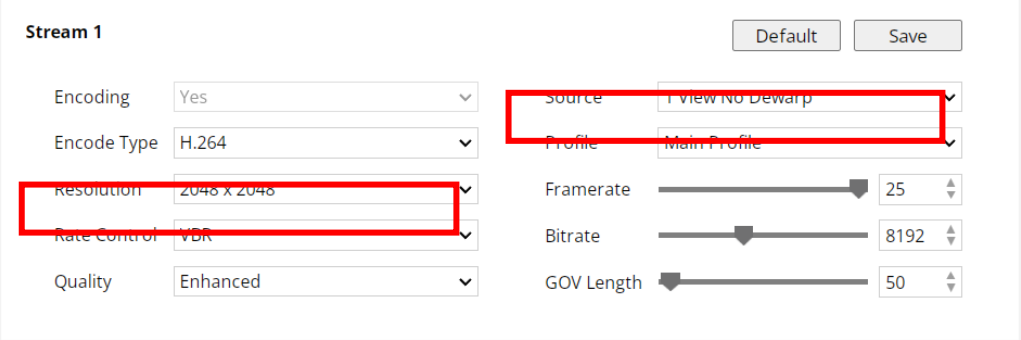
  With this method, when viewing the dewarped images from the camera's homepage, the video format of stream needs to be set. Refer to the following instructions to view the dewarped images.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Step 1: Select the camera's installation method at <Installation>. For more details, please refer to sub-section Installation below.

Step 2: Set the video format of the stream from the below <Stream>.

Step 3: Select one of the viewing modes from [Source] drop-down list. Then, select a desired resolution for the stream and click <Save>.



NOTE: The resolution options will vary according to the viewing mode selected from [Source] drop-down list.

NOTE: When selecting 2 Views 180 Dewarp / 1 View 180 Dewarp, there will be no resolution option with the video's aspect ratio of 1:1(e.g., 2048 x 2048, 1408 x 1408, 960 x 960).

- **No Dewarping**

  No Dewarping is a dewarping method that corrects the fisheye source images by a backend device or a backend software with dewarping function. This method can correct high resolution images and deliver clear dewarped images.

  With this approach, users can only record video or take snapshots of the fisheye source images delivered from the camera.

Installation

This item is for users to select the camera's installation method, so the dewarped images can be viewed with the correct viewing modes. Select a method from the drop-down list according to the location that the camera is installed. Choose <Ceiling Mount> if the camera is mounted to the ceiling, or select <Wall Mount> if the camera is mounted to the wall.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Dewarping Frame Rate

This item is for users to adjust the speed of the ePTZ. The refresh speed options are 5, 10, 15, and 20. The larger the value, the faster the pan tilt movement is.

Encoding

Select <Yes> from the drop-down menu to enable Stream 2~Stream 4 encoding. Or select <No> to disable the streaming encoding.

Encode Type

The available video resolution formats include H.265, H.264, and MJPEG. Users can select the preferred encode type from the drop-down menu.

Resolution

Video resolution combination will vary according to different camera models.

Rate Control

There are three kinds of H.265/H.264 bit rate modes provided: CBR (Constant Bit Rate), VBR (Variable Bit Rate) and LBR (Low Bit Rate).

- **CBR**
  The sent-out video bitrate will be fixed and consistent to maintain the bandwidth.

- **VBR**
  Video bitrate varies according to the activity of the monitoring environment to achieve better image quality.

  - Quality
    Users can set <Normal> or <Enhanced> to change the quality. The default setting is <Enhanced>.

    Set <Normal>, Video bitrate varies according to the activity of the monitoring environment, with the maximum being approximately the set bitrate.

    Set <Enhanced>, Video bitrate varies according to the activity in the monitoring environment and ensures superior image quality. If there is high activity in the scene, the bitrate can exceed approximately three times the set bitrate value. If there is small or zero activity in the scene, the bitrate can be lower compared to <Normal>.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

- **LBR**
  LBR keeps low bitrate and ensures superior image quality. To implement LBR control, setup the compression level and dynamic GOV for each streaming accordingly beforehand.

  - Compression
    Based on the current application area and streaming bitrate, select the most suitable compression level, high/mid/low/quality.

    Set <High>, and bitrate will vastly be reduced; however, image quality may be degraded at the same time.

    Set <Low>, and bitrate will stably keep low while image quality remains high.

    Set <Quality>, and bitrate will achieve the best compression while maintaining image quality. The bitrate may be higher than set value when there is high motion or noise in the scene.

  - Dynamic GOV
    According to the amount of motion in the application area, the GOV length of the video will be adjusted dynamically to reduce more bitrate, especially for scenes with minor changes. The length of Dynamic GOV is from <GOV Length> to <Max. GOV> (4094).

    Select <Enabled> and set <Max. GOV>. Then, click on <Save> to activate the setting.

    If there is small or zero activity in the scene, set <Max GOV> larger, the GOV length will be longer, resulting in lower bitrate and bandwidth.

    If there are constant dynamic changes in the scene, it is suggested just adjust <GOV Length> and disable <Dynamic GOV>.

Profile

Users can set H.265/H.264 Profile to <High Profile> or <Main Profile> according to its compression needs. With the same bit rate, the higher the compression ratio, the better the image quality is. The default setting is <Main Profile>.

NOTE: Please make sure the higher compression ratio is supported by the system before setup.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Framerate

Video framerate is for setting the frames per second (fps) if necessary. The maximum frame rate range of each stream will change according to the selected video resolution.

NOTE: Low framerate will decrease video smoothness.

Bitrate

- **8M Models**

  The default setting of the H.265/H.264 bitrate for Stream 1 is 12288 kbit/s; for Stream 2 is 4096 kbit/s; for Stream 3/ Stream 4 is 2048 kbit/s. The setting range is from 64 to 20480 kbps, and the total bit rate should not exceed 51200 kbps.

- **Fisheye Model**

  The default setting of the H.265/H.264 bitrate for Stream 1 is 8192 kbit/s; Stream 2/ Stream 3 is 4096 kbit/s. The setting range is from 64 to 20480 kbps, and the total bit rate should not exceed 40960 kbps.

GOV Length

Users can set the GOV length to determine the frame structure (I-frames and P-frames) in a video stream to save bandwidth. Less bandwidth is needed if the GOV length is set to a high value. However, the shorter the GOV length, the better the video quality is.

- **8M Models**

  The default setting for Stream 1 ~ Stream 4 is 25. The setting range of the GOV length is from 1 to 4094.

- **Fisheye Model**

  The default setting for Stream 1/ Stream 2 is 50. The setting range of the GOV length is from 1 to 4094.

- **PTZ Cameras**

  The default setting for Stream 1~4 is 30. The setting range of the GOV length is from 1 to 4094.

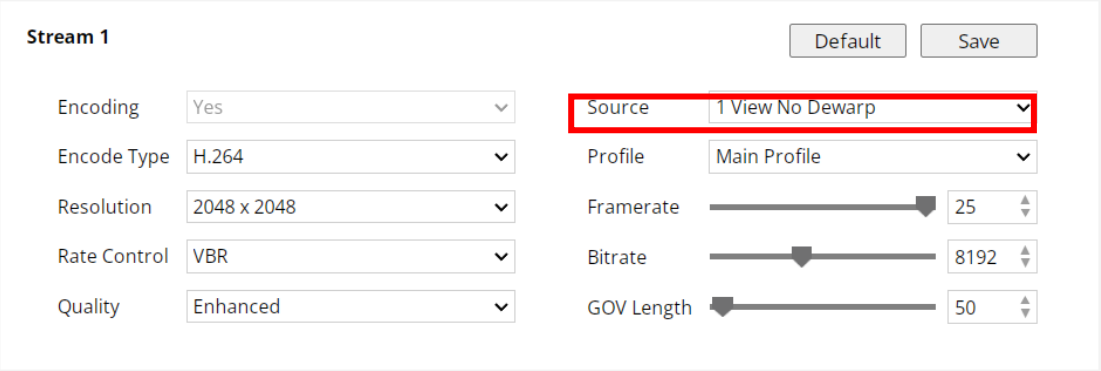
Q (Quality) Factor (MJPEG Only)

The default setting of MJPEG Q factor is 35; the setting range is from 1 to 70. A higher Q factor means less compression, resulting in better image quality but larger file sizes. Conversely, a lower Q factor means more compression, resulting in reduced image quality but smaller file sizes.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Source (Fisheye Camera Only)

Users can set the viewing mode of Fisheye Camera here. The resolution options will vary according to the viewing mode selected from [Source] drop-down list.



NOTE: This item is only available when Fisheye Dewarping Type is set as <Edge Dewarping>.

- **1 View No Dewarp**
  Select <1 View No Dewarp> to view the live videos without dewarping.

- **1 View ePTZ Dewarp**
  Select <1 View ePTZ Dewarp> to view the dewarped live images and virtually pan / tilt / zoom the camera according to users' needs. Users can implement virtual PTZ by rotating the mouse wheel (for zoom in / out), and drag the mouse into any direction.

- **2 Views 180 Dewarp**
  For Ceiling Mount Installed Camera, select <2 Views 180 Dewarp> to view the dewarped live images as two 180° views.

- **4 Views ePTZ Dewarp**
  For Ceiling Mount Installed Camera, select <4 Views ePTZ Dewarp> to view the dewarped live images as four ePTZ views.

- **1 View 180 Dewarp**
  For Wall Mount Installed Camera, select <1 View 180 Dewarp> to view the dewarped live video as a single 180° view.

- **1 View 180 and 2 Views ePTZ**
  For Wall Mount Installed Camera, select <1 View 180 and 2 Views ePTZ> to view the dewarped live video as a single 180° view with two ePTZ views. Users can implement virtual PTZ by rotating the mouse wheel (for zoom in / out), and drag the mouse into any direction in the

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

ePTZ live video panes.

The following table shows the available viewing modes in different installation methods of Edge Dewarping. The supported viewing modes are represented by "v".

Dewarping Type/ Installation Method / Source	Edge Dewarping	
	Ceiling Mount	Wall Mount
1 View No Dewarp	v	v
1 View ePTZ Dewarp	v	v
2 Views 180 Dewarp	V	-
4 Views ePTZ Dewarp	v	-
1 View 180 Dewarp	-	V
1 View 180 and 2 Views ePTZ	-	v

Click on <Save> to confirm the setting or click on <Default> to return to the previous settings.

BNC
The BNC is supported when only Stream 1 is active. The function will vary according to different camera models.

3.3.2 Video Rotation

The Video Rotation setting can be found under this path: **Streaming> Video Rotation**.

Rotate Type
Users can choose 0, 90, 180, or 270 degree from the drop-down menu to rotate the image. For Fisheye and PTZ Cameras, users can choose 0 or 180 degree from the drop-down menu to rotate the image.

3.3.3 Video Text Overlay

The Video Text Overlay setting can be found under this path: **Streaming> Video Text Overlay**.

Users can select the items to display data including font size and color / text overlay setting / image overlay setting on the live video pane.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Font Size and Color

Users can choose the Font Color (black, white, yellow, red, green, blue, cyan, or magenta) and Font Size (small, medium, or large) of the display date & time / text contents / azimuth / zoom ratio.

Text Overlay Setting

Users can select the following items to display on the live video pane.

- **Date & Time**
  Check the box to enable date & time display on the Live Video Pane and a Video Text Overlay Window will show up. Move the mouse cursor to the center of the window then click and drag the window to preferred display position. Users can choose to display date, time, or date & time from the drop-down menu.

- **Azimuth**
  Check the box to enable azimuth display on the Live Video Pane and move the mouse cursor to the center of the window then click and drag the window to preferred display position. Azimuth shows the pan/tilt degree and the shooting position of the camera, such as NE 050/00 (“NE”: the shooting position of the camera; “050”: pan degree, “00”: tilt degree.) Users can choose both or compass only from the drop-down menu. This function is only for PTZ Camera.

- **Zoom Ratio**
  Check the box to enable Zoom Ratio display on the Live Video Pane. Move the mouse cursor to the center of the window then click and drag the window to preferred display position. This function is only for PTZ Camera.

- **Text Contents**
  Check the box to enable text contents display on the Live Video Pane and a Video Text Overlay Window will show up. Move the mouse cursor to the center of the window then click and drag the window to preferred display position. Type the text to display in the entry field. The maximum length of the text string is 210 characters.

Image Overlay Setting

Users can upload an image and set its transparency to display on the live video pane. Enable the function, the setting range of image transparency is from 0 to 255; the lower the value, the more transparent it is. Users must save the image as a 8-bit BMP file; the length should be the multiple of 32, and the width should

be the multiple of 4. The maximum resolution of the image should not exceed 32768 pixels. Select the file and click on <Upload> to confirm the setting.

3.3.4 Privacy Mask

The Privacy Mask setting can be found under this path: **Streaming> Privacy Mask**.

On/Off
Enable the mask by turning on or off button.

Mask Color
The selections of color include black, white, red, green, blue, cyan, yellow and magenta.

Mask Setting
Select a masking number, the drop-down list will show “Empty” if it is not configured and “Already Set” if it is configured. Click on <Set> to set up the mask and click <Clear> to delete.

3.3.5 Video ROI

The Video ROI setting can be found under this path: **Streaming> Video ROI**.

ROI stands for Region of Interest. This function allows users to select specific monitoring region for Stream 1~Stream 4, instead of showing the full image.

NOTE: To use ROI function, dual streaming or above must be enabled, and the resolution of each streaming must be different. ROI function cannot be enabled if the resolution of the stream is 1920x1080. In any enabled stream, ROI function cannot be enabled for the highest resolution; and when 4 streams are enabled, ROI function cannot be enabled for the smallest resolution.

Enable Stream 1~ Stream 4 ROI Setting
Check the boxes and Stream 1~ Stream 4 ROI Window will be displayed. To adjust the ROI Window, click and drag the edge of the window outward/inward. To shift the window to the intended location, click the center of the ROI Window and drag the mouse cursor. Then, click <Save> to apply the setting. This function is **NOT** available for Fisheye and PTZ Cameras.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

3.3.6 Video ROI Encoding

The Video ROI Encoding setting can be found under this path: **Streaming> Video ROI Encoding**.

Video ROI Encoding is to set the compression of the selected zone within ROI for better performances; at most three zones can be set in the interested region. However, this function does **NOT** support MJPEG video format. This function is **NOT** available for PTZ Cameras.

The following shows how to setup Video ROI Encoding. To implement this function, Video ROI must be setup beforehand.

- Select a video stream from <Video Stream>.
- Select <Enable> from <ROI Encoding> to implement ROI Encoding.
- Click on <Add>, click and drag the center of the window to move it to the interested location; click and drag the edge of the window outward / inward to resize the window.
- Click on <Delete> to delete video stream.

Note that the total size of the three windows **CANNOT** be larger than the half size of the ROI. When exceeds, a warning window will pop up.

- Choose the quality of the setting zone from <Quality>.
  The higher the value, the better the image quality (higher bitrate) of the setting zone will be. On the contrary, the lower the value, the lower the image quality (lower bitrate) of the selected area will be.

Click on <Save All Settings> to apply the setting.

3.3.7 Streaming Protocol

The Streaming Protocol setting can be found under this path: **Streaming> Streaming Protocol**.

In the <Streaming Protocol> setting page, the administrator can select Unicast Mode or Multicast mode.

Unicast Mode
Live stream on the web interface use RTP over RTSP over WebSocket. The camera supports RTP over UDP and RTSP over TCP / RTP over RTSP (TCP) / RTSP and RTSP over HTTP / MJPEG over HTTP, user can stream video through backend integration or other application(e.g VLC) by these protocols.

Multicast Mode

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Enable multicast by selecting “Enable” from the drop-down menu. Enter all required data, including <Video Stream Address / Audio Stream Address / Metadata Stream Address>, < Port> and < TTL> into each blank. Only the multicast settings for stream 1 and stream 2 are shown on this page.

Click on <Save> to confirm the setting.

3.3.8 Audio

The Audio setting can be found under this path: **Streaming> Audio**.

In this page, the administrator can adjust the sound transmission mode, the audio gain levels and the audio bit rate. Setting for enabling sound recording to the microSD/SD card is also available.

Transmission Mode

- **Full-duplex (Talk and Listen Simultaneously)**
  In the Full-duplex mode, the local and remote sites can communicate with each other simultaneously, i.e. both sites can speak and listen to the other side at the same time.

- **Half-duplex (Talk or Listen, Not at the Same Time)**
  In the Half-duplex mode, the local / remote site can only talk or listen to the other site at a time.

- **Simplex (Talk Only)**
  In the Talk Only Simplex mode, the local / remote site can only talk to the other site.

- **Simplex (Listen Only)**
  In the Listen Only Simplex mode, the local / remote site can only listen to the other site.

- **Disable**
  Select the item to turn off the audio transmission function.

Audio Gain Setting

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Set the audio input / output gain levels for the sound amplification. The audio input gain value is adjustable from 1 to 10. The audio output gain value is adjustable from 1 to 6. The sound will be turned off if the audio gain is set to “Mute”.

General

- **Audio Codec**
  Selectable audio transmission bit rate include G726(40 kbps), G726(32 kbps), G726(24 kbps),G726(16 kbps), G711(uLAW), G711(ALAW), AAC, PCM (128 kbps), PCM (256 kbps), PCM (384 kbps), and PCM (768 kbps). Higher bit rate will let higher audio quality and require bigger bandwidth.

- **Audio Input**
  Selectable input types are <Line in>, <External Mic> or <Built-in Mic>, the function will vary according to different camera models. If the audio input is from the audio device connected via the Audio In connecters, users should select “Line in”. If the audio input is from the microphone connected via the Audio In connecters, users should select “External Mic” for better sound quality. If the audio input is from the microphone in the camera, users should select “Built-in Mic”. Click on <Save> to confirm the setting.

- **Recording to Storage**
  Select <Enable> from the drop-down menu to enable audio recording with videos into the microSD/SD card or the Network Storage.

NOTE: If the chosen audio codec is not compatible with the player, there will only be noise instead of audio during playback.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

3.4 Recording

Under the tab <**Recording**>, there are submenus including: <Playback>, <Recording Settings> and <Storage Management>.

3.4.1 Playback

The Playback setting can be found under this path: **Recording> Playback**.

Search From/End
Users can select the specific date and time to playback the record video.

Storage
Select SD Card or Network Storage to search the storage record video.

Format
Select Video or JPEG to present the format.

Click on <Search> to confirm the setting. The files will appear at the right side.

Select File to Download
To open / download a video clip / image, select the file from the Recording list field, and then click on <download>. The selected file window will pop up. Click on the file to directly open the file or download it to a specified location.

Select File to Delete
Select the file from the Recording list field, click on <Delete> to delete the file.

Delete All Files (0/0)
Click on <Delete> to delete all files.

Founded File Listing
Click on <Sort>, and the files in the Recording list will be listed in name and date order.

The capital letter A / M / N / T / S / R / V / U / W / VA# in the very beginning of name denotes the sort of the recording as below.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Initial	Recording Type	Initial	Recording Type
A	Alarm	**S**	Periodical Event
M	Motion	**R**	Regular Recording
N	Network Failure	**V**	Manual Trigger
T	Tampering	**U**	Audio Detection
W	Shock Detection	**VA#**	Video Analytics-AI

3.4.2 Recording Settings

The Recording Settings setting can be found under this path: **Recording> Recording Setting**.

Recording ON/OFF

Users can specify the recording schedule that fits the present surveillance requirement.

- **OFF**
  Select < OFF> to terminate the recording function.

- **ON**
  Users can select <ON> to activate microSD/SD card or Network Storage Recording all the time.

- **Recording base on following schedule table**
  Select a set of schedule from the time frame blank, check specific weekdays and setup the start time (hour:minute) and duration (hour:minute) to activate the recording at certain time frames. The setting range for the duration time is from 00:00 to 168:59. Please click on <Save> to save the setup.

  To delete a schedule, select one from the schedule list, and click <Delete>.

Recording Video Format

- **Capture Source**
  Select a video stream to set as the capture source. The default format of the video stream is <Stream 1>. Select a preferred stream from the drop-down list.

- **Video File Format**

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

The default video file format is <MP4>. MP4 can only support H.264/H.265 video and AAC audio codec.

- **File Name Options**
  Select a format as the recording filename format. The default recording file name options is <Start time only>. Select <Start time only> or <Start time + End Time> format from the drop-down list.

Recording Device
Select a recording storage type, <SD Card> or <Network Storage>.

3.4.3 Storage Management

The Storage Management setting can be found under this path: **Recording> Storage Management**.

3.4.3.1 SD Card

The SD Card setting can be found under this path: **Recording> Storage Management> SD Card**.

Users can implement local recording to the microSD/SDHC/SDXC card. This page shows the capacity information of the microSD/SD card. Please refer to Recording> Playback for recording list with all the recording files saved on the memory card. Users can also format the microSD/SD card and implement automatic recording cleanup through the setting page.

NOTE: Please format the microSD/SDHC/SDXC card when using it for the first time. Formatting will also be required when a memory card is being used on one camera and later transferred to another camera with different software platform.

NOTE: It is not recommended to record with the microSD/SD card for 24/7 continuously, as it may not be able to support long term continuous data read/write. Please contact the manufacturer of the microSD/SD card for information regarding the reliability and the life expectancy.

Device Information
After the microSD/SD card is inserted into the camera, the card information such as device type, available capacity and status will be shown at <Device Information>.

Format Device

Click on <Format> to format the memory card. Two filesystems are provided, <vfat (Default)> and <ext4 (Recommended)>. It is recommended to select <ext4> as the filesystem for steady and better performances.

Automatic Disk Cleanup

Enable the function and specify the time <1~999 day(s) or 1~142 week(s)> and storage limits <1~99% full> to configure disk cleanup settings. Disk cleanup will be triggered when the specified day(s)/week(s) or the storage limit threshold is reached. When the day(s)/week(s) condition is reached, data from the specified number of day(s)/week(s) prior will be deleted. When the storage limit threshold is reached, one-third of the files will be deleted. Click on <Save> to confirm the settings.

3.4.3.2 Network Storage

The Network Storage setting can be found under this path: **Recording> Storage Management> Network Storage**.

Users can store the recording videos to a network share folder, or Network Storage (Network-Attached Storage). A Network Storage device is used for data storage and data sharing via network. This page displays the capacity information of the network device and a recording list with all the recording files saved on the network device. Users can also format the Network Storage and implement automatic recording cleanup through the setting page.

Device Information

When a Network Storage is successfully installed, the device information such as device type, available capacity and status will be shown at <Device Information>.

Storage Settings

The administrator can set the camera to send the alarm messages to a specific Network Storage site when an alarm is triggered. Enter the network device details, which include protocol (SAMBA), host (the IP of the Network Storage), share (the folder name of the Network Storage), user name, and password, in the fields.

Click on <Save> when finished.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Format Device

Click on <Format> to format the Network Storage.

Automatic Disk Cleanup

Enable the function and specify the time <1~999 day(s) or 1~142 week(s)> and storage limits <1~99% full> to configure disk cleanup settings. Disk cleanup will be triggered when the specified day(s)/week(s) or the storage limit threshold is reached. When the day(s)/week(s) condition is reached, data from the specified number of day(s)/week(s) prior will be deleted. When the storage limit threshold is reached, one-third of the files will be deleted. Click on <Save> to confirm the settings.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

3.5 Analytics

Under the tab <**Analytics**>, there are submenus including: <System Overview>, <Common Setting>, <Video Analytics - AI>, <Video Analytics - Legacy>, <Audio Analytics>, <Alarm Input>, <General> and <License Management>.

3.5.1 System Overview

The System Overview setting can be found under this path: **Analytics> System Overview**.

Users can browse all Video Analytics features on this page and perform basic edits to Video Analytics functions. <Video Analytics-AI> includes multiple behavior analytics related to Human/Vehicle/Object Detection or Recognition. <System: Other Analytics> includes Motion Detection, Tampering, Audio Detection, Alarm Input, Network Failure Detection, Periodical Event, and Manual Trigger, etc.

NOTE: For PTZ Cameras, select a specified preset position to configure or view the <Video Analytics - AI> features set at that preset position. Please refer to PTZ> Preset to setup the relevant settings beforehand. Alternatively, select “Free Position” to configure or view the <Video Analytics - AI> features. This options allows the PTZ camera to activate the configured <Video Analytics - AI> features even in non-static scenes.

Analytics
Displays the video analytics functions supported by the camera.

Category
All Video Analytics in <Video Analytics-AI> are organized into categories, the same number corresponds to the same category. Information about how many different categories of video analytics can be executed simultaneously will be displayed in the “Video Analytics-AI Status (Total System Capability).” Please refer to section Video Analytics - AI Status (Total System Capability) below.

Enable
Enable or disable the function.

Show Zone

Enable the function by turning <On>, the virtual zones and lines data, object trajectory path data, object confidence level data or triggered analytics data will be shown on the live video pane. If the <Show Zone> function is enabled, the default setting is <Draw on PC Client Viewer>. Please refer to Analytics> Common Setting> Video Analytics - AI Data Overlay Options for more settings related to video analytics AI data overlay.

Scheduling

Users can specify the schedule on each functionality page. Once the schedule time is set, the configured Schedule Profile will appear in the Scheduling section. Please refer to System> Schedule Profile for schedule settings.

Edit

Click <Edit> will lead the administrator to the relevant Analytics functionality page.

Video Analytics - AI Status (Total System Capability)

This section specifies the number of categories that can be executed simultaneously and shows the features enabled for each category. Multiple video analytics within the same category ID can be run concurrently.

3.5.2 Common Setting

The Common setting can be found under this path: **Analytics> Common Setting**.

Video Analytics AI Data Overlay Options

This feature allows users to select the data overlay options, such as virtual zones and lines data, object trajectory path data, object confidence level data or triggered analytics data, to be displayed on either the PC client or the camera source video for Video Analytics – AI function.

Select <Draw on PC Client Viewer>, <Draw on Camera Source Video> or <Turn off> from the drop-down menu to choose the specific overlay method.

- **Draw on PC Client Viewer**
  Select <Draw on PC Client Viewer> to display the configured data overlays options on the screen when <Show Zone> function from

<System Overview> is enabled. However, if a screenshot or recording is taken, the data overlays options will not be included.

- **Draw on Camera Source Video**
  Select <Draw on Camera Source Video> and enable the <Show Zone> function from <System Overview> to display the configured data overlays options on the screen. Additionally, if a screenshot or recording is taken, the data overlays options will be included.

- **Turn off**
  Select <Turn off> will disable the <Show Zone> function.

Select the options below for data overlay type.

- **Metadata, Bounding Box Data (Always On Now)**
  Enabled by default, this function displays a rectangle around detected objects.

- **Virtual Zones and Lines Data**
  The area or line in the scenario where the object was detected.

- **Object Trajectory Path Data**
  This function displays the movement paths of objects.

- **Object Confidence Level Data**
  This function displays the reliability of detected objects.

- **Triggered Analytics Data Only**
  The live view pane only displays red bounding boxes that indicate when the analytics have been triggered.

  Click on <Set > to confirm the setting.

Video Analytics AI Data Location

- **Set Face/License Plate Database Location**
  Select <Internal> or <SD Card> for the database location. The default setting is <Internal>, the database will be stored on the flash memory of the camera. For this setting, the status will display “OK” if the storage is applicable or “Not OK” if it is not applicable. If the setting is <SD Card>, the status will display “OK” if it the storage is applicable or “No SD Card” if no SD Card is detected in the camera.

- **Set Heat Map Database Location**

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

The default setting is <SD Card>. The status will display “OK” if it the storage is applicable or “No SD Card” if no SD Card is detected in the camera.

NOTE: Please be advised that modifying the setting of the database location will delete ALL saved historical video analytics data.

3.5.3 Video Analytics - AI

The Video Analytics - AI setting can be found under this path: **Analytics> Video Analytics - AI**. For camera installation recommendations and scene requirements, please refer to Appendix C: Installation, for behavior settings related to Video Analytics, please refer to Appendix D: Standard Setting.

3.5.3.1 Help

The Help setting can be found under this path: **Analytics> Video Analytics - AI> Help**.

This function provides users with guidance on how to set up Analytics functions and offers detailed explanations for each feature.

3.5.3.2 Common Threshold

The Common Setting can be found under this path: **Analytics> Video Analytics - AI > Common Threshold**.

Video Analytics AI Confidence Level Threshold

Predictions with a confidence score lower than the threshold value are ignored. If the value of the detected object is higher than the threshold, it will be considered as human / bicycle / car / motorcycle / bus / truck / human head (valid objects). Each threshold ranges from 1-100%, and the default value is 50%.

Click on <Set > to confirm the setting.

3.5.3.3 Intrusion

The Intrusion setting can be found under this path: **Analytics> Video Analytics - AI> Intrusion**.

3.5.3.4 Line Crossing

The Line Crossing setting can be found under this path: **Analytics> Video Analytics - AI> Intrusion> Line Crossing**.

Line crossing function detects objects that cross a line. Users can configure a virtual line, set the trigger direction, and define trigger actions, etc., by following these steps.

Step 1: Select the detection objects from <Detection>. The available options are “Human”, “Human Head”, “All Vehicles”, or a specific vehicle type by selecting “Bicycle”, “Car”, “Motorcycle”, “Bus”, or “Truck”.

Step 2: Select <Zone> to setup virtual lines. Click on <New> in the Detect Zone, and a new zone will appear in the live video pane. Left-clicking the circle on the zone allows users to drag and reshape the virtual line. Left-clicking the square allows users to add an anchor point, splitting the line into two for further adjustments. Right-clicking the circle on the zone to remove an anchor point.

Click on <Reset> to reset the zone’s settings, and click on <Delete> to delete the zone. The maximum amount of virtual lines is 4.

Step 3: Select the specific zone and set up the direction in which objects should move to be detected from <Trigger Conditions for Detect Zone>. Click on <Change> to change the direction. The white arrows next to the line show the direction. Actions are triggered when objects cross the line in the direction of the arrows.

Step 4: Use Exclude Zone to create an area where users don’t want detected objects to trigger actions. Click on <New> in the exclude zone and a new ex-zone will appear in the live video pane. Left-clicking the circle on the zone allows users to drag and reshape the virtual zone. Left-clicking the square allows users to add an anchor point, splitting the line into two for further adjustments. Right-clicking the circle on the zone to remove an anchor point.

Click on <Reset> to reset the ex-zone’s settings, and click on <Delete> to delete the ex-zone. The maximum amount of detection zones is 4.

Step 5: Select <Object> to set up the object size and trigger condition. Click <Edit> to set the minimum and maximum size of the detected objects. Users can adjust the blue or pink frame or enter the width (FOV) and height (FOV) in the input fields. Click <Close> to finish the setting.

NOTE: All analytics share the same object size setting.

Step 6: Select <Object> and choose either “Bottom Center Overlay” or “Center Overlay” from the trigger condition drop-down menu. Please refer to Appendix E: Trigger Type for further details.

Step 7: Select <Alarm> and set up “Keep Alarm Time (1~1000s)”. This feature allows the alarm to continue for a specified time after the trigger condition ends.

Step 8: Select <Schedule> to specify schedule time. Please refer to section System> Schedule Profile for further details.

Step 9: Set up the actions to take when an event occurs, and specify the filename if required, under the <Triggered Action> and <File> sections. Please refer to Appendix D: Standard Setting for further details.

Step 10: This step is only available for PTZ Cameras. Proceed to next step if the camera is not a PTZ camera.

Select <Preset Position> and select a specific preset position from the drop-down menu. Click <Copy> to copy current analytics settings to this specific preset position, allowing the analytics to execute when the camera is at that preset position. Please refer to PTZ> Preset to setup the preset point before using this function.

Step 11: Click <Save All Settings> to apply the settings, or click <Restore Default> to revert to the default settings.

3.5.3.5 Object in Zone

The Object in Zone setting can be found under this path: **Analytics> Video Analytics - AI> Intrusion> Object in Zone**.

Object in Zone function detects objects that move inside a zone. Users can configure detection zones, zone positions, and set trigger actions, etc., by following these steps.

Step 1: Select the detection objects from <Detection>. The available options are “Human”, “Human Head”, “All Vehicles”, or a specific vehicle type by selecting “Bicycle”, “Car”, “Motorcycle”, “Bus”, or “Truck”.

Step 2: Select <Zone> to setup virtual zones. Click on <New> in the Detect Zone, and a new zone will appear in the live video pane. Left-clicking the circle on the zone allows users to drag and reshape the virtual zones. Left-clicking the square allows users to add an anchor point, splitting the line into two for further adjustments. Right-clicking the circle on the zone to remove an anchor point.

Click on <Reset> to reset the zone’s settings, and click on <Delete> to delete the zone. The maximum amount of detection zones is 4.

Step 3: Use Exclude Zone to create an area where users don’t want detected objects to trigger actions. Click on <New> in the exclude zone and a new ex-zone will appear in the live video pane. Left-clicking the circle on the zone allows users to drag and reshape the virtual zone. Left-clicking the square allows users to add an anchor point, splitting the line into two for further adjustments. Right-clicking the circle on the zone to remove an anchor point.

Click on <Reset> to reset the ex-zone's settings, and click on <Delete> to delete the ex-zone. The maximum amount of detection zones is 4.

Step 4: Select <Object> to set up the object size and trigger condition. Click <Edit> to set the minimum and maximum size of the detected objects. Users can adjust the blue or pink frame or enter the width (FOV) and height (FOV) in the input fields. Click <Close> to finish the setting.

NOTE: All analytics share the same object size setting.

Step 5: Select <Object> and choose either "Bottom Center Overlay" or "Center Overlay" from the trigger condition drop-down menu. Please refer to Appendix E: Trigger Type for further details.

Step 6: Select <Alarm> and set up "Keep Alarm Time (1~1000s)". This feature allows the alarm to continue for a specified time after the trigger condition ends.

Step 7: Select <Schedule> to specify schedule time. Please refer to section System> Schedule Profile for further details.

Step 8: Set up the actions to take when an event occurs, and specify the filename if required, under the <Triggered Action> and <File> sections. Please refer to Appendix D: Standard Setting for further details.

Step 9: This step is only available for PTZ Cameras. Proceed to next step if the camera is not a PTZ camera.

Select <Preset Position> and select a specific preset position from the drop-down menu. Click <Copy> to copy current analytics settings to this specific preset position, allowing the analytics to execute when the camera is at that preset position. Please refer to PTZ> Preset to setup the preset point before using this function.

Step 10: Click <Save All Settings> to apply the settings, or click <Restore Default> to revert to the default settings.

3.5.3.6 Object Counting

The Object Counting setting can be found under this path: **Analytics> Video Analytics - AI> Object Counting**.

3.5.3.7 Crossline Counting

The Crossline Counting setting can be found under this path: **Analytics> Video Analytics - AI> Object Counting> Crossline Counting**.

Crossline Counting function counts objects that cross a line. Users can configure virtual line, set the trigger direction, and define trigger actions, etc., by following these steps.

Step 1: Select the detection objects from <Detection>. The available options are “Human”, “Human Head”, “All Vehicles”, or a specific vehicle type by selecting “Bicycle”, “Car”, “Motorcycle”, “Bus”, or “Truck”.

Step 2: Select <Zone> to setup virtual lines. Click on <New> in the Detect Zone, and a new zone will appear in the live video pane. Left-clicking the circle on the zone allows users to drag and reshape the virtual line, while the square allows users to add an anchor point, splitting the line into two for further adjustments. Right-clicking the circle on the zone to remove an anchor point.

Click on <Reset> to reset the zone’s settings, and click on <Delete> to delete the zone. The maximum amount of virtual lines is 4.

Step 3: Select the specific zone and set up the direction in which objects should move to be detected from <Trigger Conditions for Detect Zone>. Click on <Change> to change the direction. The white arrows next to the line show the direction.

Step 4: Enter a value for “Number of Objects” to specify the number of objects that must be detected. The setting range of the number of objects is from 1 to 1000.

Select “Yes” from the drop-down menu of “Reset Counters on Triggers” to reset the counter to 0 when a trigger occurs. Select “No” to allow the counter to continue counting.

Step 5: Use Exclude Zone to create an area where users don’t want detected objects to trigger actions. Click on <New> in the exclude zone and a new ex-zone will appear in the live video pane. Left-clicking the circle on the zone allows users to drag and reshape the virtual zone, while the square allows users to add an anchor point, splitting the line into two for further adjustments. Right-clicking the circle on the zone to remove an anchor point.

Click on <Reset> to reset the ex-zone’s settings, and click on <Delete> to delete the ex-zone. The maximum amount of detection zones is 4.

Step 6: Select <Object> to set up the object size and trigger condition. Click <Edit> to set the minimum and maximum size of the detected objects. Users can adjust the blue or pink frame or enter the width (FOV) and height (FOV) in the input fields. Click <Close> to finish the setting.

NOTE: All analytics share the same object size setting.

Step 7: Select <Object> and choose either “Bottom Center Overlay”, “Center Overlay” or “Edge Overlay” from the trigger condition drop-down menu. Please refer to Appendix E: Trigger Type for further details.

Step 8: Select <Alarm> and set up “Keep Alarm Time (1~1000s)”. This feature allows the alarm to continue for a specified time after the trigger condition ends.

Step 9: Select <Schedule> to specify schedule time. Please refer to section System> Schedule Profile for further details.

Step 10: Set up the actions to take when an event occurs, and specify the filename if required, under the <Triggered Action> and <File> sections. Please refer to Appendix D: Standard Setting for further details.

Step 11: This step is only for PTZ Cameras. Proceed to next step if the camera is not a PTZ camera.

Select <Preset Position> and select a specific preset position from the drop-down menu. Click <Copy> to copy current analytics settings to this specific preset position, allowing the analytics to execute when the camera is at that preset position. Please refer to PTZ> Preset to setup the preset point before using this function.

Step 12: Click <Save All Settings> to apply the settings, or click <Restore Default> to revert to the default settings.

3.5.3.8 Occupancy in Zone

The Occupancy in Zone can be found under this path: **Analytics> Video Analytics - AI> Object Counting> Occupancy in Zone**.

Occupancy in Zone function counts objects present inside a zone. Users can configure detection zones, zone positions, and set trigger actions, etc., by following these steps.

Step 1: Select the detection objects from <Detection>. The available options are “Human”, “Human Head”, “All Vehicles”, or a specific vehicle type by selecting “Bicycle”, “Car”, “Motorcycle”, “Bus”, or “Truck”.

Step 2: Select <Zone> to setup virtual zones. Click on <New> in the Detect Zone, and a new zone will appear in the live video pane. Left-clicking the circle on the zone allows users to drag and reshape the virtual zones, while the square allows users to add an anchor point, splitting the line into two for further adjustments. Right-clicking the circle on the zone to remove an anchor point.

Click on <Reset> to reset the zone’s settings, and click on <Delete> to delete the zone. The maximum amount of detection zones is 4.

Step 3: Select the specific zone and configure its trigger condition from <Trigger Conditions for Detect Zone>. Enter a value for “Number of Objects” to specify the number of objects that must be detected. The setting range of the number of objects is from 1 to 1000.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Select “Yes” from the drop-down menu of “Reset Counters on Triggers” to reset the counter to 0 when a trigger occurs. Select “No” to allow the counter to continue counting.

Step 4: Use Exclude Zone to create an area where users don’t want detected objects to trigger actions. Click on <New> in the exclude zone and a new ex-zone will appear in the live video pane. Left-clicking the circle on the zone allows users to drag and reshape the virtual zone, while the square allows users to add an anchor point, splitting the line into two for further adjustments. Right-clicking the circle on the zone to remove an anchor point.

Click on <Reset> to reset the ex-zone’s settings, and click on <Delete> to delete the ex-zone. The maximum amount of detection zones is 4.

Step 5: Select <Object> to set up the object size and trigger condition. Click <Edit> to set the minimum and maximum size of the detected objects. Users can adjust the blue or pink frame or enter the width (FOV) and height (FOV) in the input fields. Click <Close> to finish the setting.

NOTE: All analytics share the same object size setting.

Step 6: Select <Object> and choose either “Bottom Center Overlay” or “Center Overlay” from the trigger condition drop-down menu. Please refer to Appendix E: Trigger Type for further details.

Step 7: Select <Alarm> and set up “Keep Alarm Time (1~1000s)”. This feature allows the alarm to continue for a specified time after the trigger condition ends.

Step 8: Select <Schedule> to specify schedule time. Please refer to section System> Schedule Profile for further details.

Step 9: Set up the actions to take when an event occurs, and specify the filename if required, under the <Triggered Action> and <File> sections. Please refer to Appendix D: Standard Setting for further details.

Step 10: This step is only for PTZ Cameras. Proceed to next step if the camera is not a PTZ camera.

Select <Preset Position> and select a specific preset position from the drop-down menu. Click <Copy> to copy current analytics settings to this specific preset position, allowing the analytics to execute when the camera is at that preset position. Please refer to PTZ> Preset to setup the preset point before using this function.

Step 11: Click <Save All Settings> to apply the settings, or click <Restore Default> to revert to the default settings.

3.5.3.9 Time in Zone

The Time in Zone setting can be found under this path: **Analytics> Video Analytics - AI> Time in Zone**.

3.5.3.10 Loitering

The Loitering setting can be found under this path: **Analytics> Video Analytics - AI> Time in Zone> Loitering**.

Loitering function detects humans who stay in a zone for longer than a specified time. Users can configure detection zones, zone positions, and set trigger actions, etc., by following these steps.

Step 1: Select the detection objects from <Detection>. The available options are “Human” and “Human Head”.

Step 2: Select <Zone> to setup virtual zones. Click on <New> in the Detect Zone, and a new zone will appear in the live video pane. Left-clicking the circle on the zone allows users to drag and reshape the virtual zones, while the square allows users to add an anchor point, splitting the line into two for further adjustments. Right-clicking the circle on the zone to remove an anchor point.

Click on <Reset> to reset the zone’s settings, and click on <Delete> to delete the zone. The maximum amount of virtual lines is 4.

Step 3: Select the specific zone and configure its trigger condition from <Trigger Conditions for Detect Zone>. Enter a value for “Object Allowed Time” to specify the amount of time allowed for an object to move within this zone. Actions will be triggered if an object exceeds this time. The available time ranges from 1 to 1800 seconds.

Step 4: Use Exclude Zone to create an area where users don’t want detected objects to trigger actions. Click on <New> in the exclude zone and a new ex-zone will appear in the live video pane. Left-clicking the circle on the zone allows users to drag and reshape the virtual zone, while the square allows users to add an anchor point, splitting the line into two for further adjustments. Right-clicking the circle on the zone to remove an anchor point.

Click on <Reset> to reset the ex-zone’s settings, and click on <Delete> to delete the ex-zone. The maximum amount of detection zones is 4.

Step 5: Select <Object> to set up the object size and trigger condition. Click <Edit> to set the minimum and maximum size of the detected objects. Users can adjust the blue or pink frame or enter the width (FOV) and height (FOV) in the input fields. Click <Close> to finish the setting.

NOTE: All analytics share the same object size setting.

Step 6: Select <Object> and choose either “Bottom Center Overlay”, “Center Overlay”, “Edge Overlay” or “Fully Inside Overlay” from the trigger condition drop-down menu. Please refer to Appendix E: Trigger Type for further details.

Step 7: Select <Alarm> and set up “Keep Alarm Time (1~1000 seconds)”. This feature allows the alarm to continue for a specified time after the trigger condition ends.

Step 8: Select <Schedule> to specify schedule time. Please refer to section System> Schedule Profile for further details.

Step 9: Set up the actions to take when an event occurs, and specify the filename if required, under the <Triggered Action> and <File> sections. Please refer to Appendix D: Standard Setting for further details.

Step 10: This step is only for PTZ Cameras. Proceed to next step if the camera is not a PTZ camera.

Select <Preset Position> and select a specific preset position from the drop-down menu. Click <Copy> to copy current analytics settings to this specific preset position, allowing the analytics to execute when the camera is at that preset position. Please refer to PTZ> Preset to setup the preset point before using this function.

Step 11: Click <Save All Settings> to apply the settings, or click <Restore Default> to revert to the default settings.

3.5.3.11 Parking Violation

The Parking Violation setting can be found under this path: **Analytics> Video Analytics - AI> Time in Zone> Parking Violation**.

Parking Violation function detects vehicles that stay in a zone for longer than a specified time. Users can configure detection zones, zone positions, and set trigger actions, etc., by following these steps.

Step 1: Select the detection objects from <Detection>. The available options are “All Vehicles”, or a specific vehicle type by selecting “Bicycle”, “Car”, “Motorcycle”, “Bus”, or “Truck”.

Step 2: Select <Zone> to setup virtual zones. Click on <New> in the Detect Zone, and a new zone will appear in the live video pane. Left-clicking the circle on the zone allows users to drag and reshape the virtual zones, while the square allows users to add an anchor point, splitting the line into two for further adjustments. Right-clicking the circle on the zone to remove an anchor point.

Click on <Reset> to reset the zone’s settings, and click on <Delete> to delete the zone. The maximum amount of detection zones is 4.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Step 3: Select the specific zone and configure its trigger condition from <Trigger Conditions for Detect Zone>. Enter a value for "Object Allowed Time" to specify the amount of time allowed for an object to move within this zone. Actions will be triggered if an object exceeds this time. The available time ranges from 1 to 1800 seconds.

Step 4: Use Exclude Zone to create an area where users don't want detected objects to trigger actions. Click on <New> in the exclude zone and a new ex-zone will appear in the live video pane. Left-clicking the circle on the zone allows users to drag and reshape the virtual zone, while the square allows users to add an anchor point, splitting the line into two for further adjustments. Right-clicking the circle on the zone to remove an anchor point.

Click on <Reset> to reset the ex-zone's settings, and click on <Delete> to delete the ex-zone. The maximum amount of detection zones is 4.

Step 5: Select <Object> to set up the object size and trigger condition. Click <Edit> to set the minimum and maximum size of the detected objects. Users can adjust the blue or pink frame or enter the width (FOV) and height (FOV) in the input fields. Click <Close> to finish the setting.

NOTE: All analytics share the same object size setting.

Step 6: Select <Object> and choose either "Bottom Center Overlay", "Center Overlay", "Edge Overlay", "Fully Inside Overlay" or "Fully Cover Overlay" from the trigger condition drop-down menu. Please refer to Appendix E: Trigger Type for further details.

Step 7: Select <Alarm> and set up "Keep Alarm Time (1~1000 seconds)". This feature allows the alarm to continue for a specified time after the trigger condition ends.

Step 8: Select <Schedule> to specify schedule time. Please refer to section System> Schedule Profile for further details.

Step 9: Set up the actions to take when an event occurs, and specify the filename if required, under the <Triggered Action> and <File> sections. Please refer to Appendix D: Standard Setting for further details.

Step 10: This step is only for PTZ Cameras. Proceed to next step if the camera is not a PTZ camera.

Select <Preset Position> and select a specific preset position from the drop-down menu. Click <Copy> to copy current analytics settings to this specific preset position, allowing the analytics to execute when the camera is at that preset position. Please refer to PTZ> Preset to setup the preset point before using this function.

Step 11: Click <Save All Settings> to apply the settings, or click <Restore Default> to revert to the default settings.

3.5.3.12 Others

The Others setting can be found under this path: **Analytics> Video Analytics - AI> Others**.

3.5.3.13 Wrong Way

The Wrong Way setting can be found under this path: **Analytics> Video Analytics - AI> Others> Wrong Way**.

Wrong Way function detects objects moving in the restricted direction. Users can configure a virtual line, set the trigger direction, and define trigger actions, etc., by following these steps.

Step 1: Select the detection objects from <Detection>. The available options are “Human”, “Human Head”, “All Vehicles”, or a specific vehicle type by selecting “Bicycle”, “Car”, “Motorcycle”, “Bus”, or “Truck”.

Step 2: Select <Zone> to setup virtual lines. Click on <New> in the Detect Zone, and a new zone will appear in the live video pane. Left-clicking the circle on the zone allows users to drag and reshape the virtual line, while the square allows users to add an anchor point, splitting the line into two for further adjustments. Right-clicking the circle on the zone to remove an anchor point.

Click on <Reset> to reset the zone’s settings, and click on <Delete> to delete the zone. The maximum amount of virtual lines is 4.

Step 3: Select the specific zone and set up the direction in which the movement of objects is restricted from <Trigger Conditions for Detect Zone>. Click on <Change> to change the direction. The white arrows next to the line show the restricted direction. Actions are triggered when objects cross the line in the direction of the arrows.

Step 4: Use Exclude Zone to create an area where users don’t want detected objects to trigger actions. Click on <New> in the exclude zone and a new ex-zone will appear in the live video pane. Left-clicking the circle on the zone allows users to drag and reshape the virtual zone, while the square allows users to add an anchor point, splitting the line into two for further adjustments. Right-clicking the circle on the zone to remove an anchor point.

Click on <Reset> to reset the ex-zone’s settings, and click on <Delete> to delete the ex-zone. The maximum amount of detection zones is 4.

Step 5: Select <Object> to set up the object size and trigger condition. Click <Edit> to set the minimum and maximum size of the detected objects.

Users can adjust the blue or pink frame or enter the width (FOV) and height (FOV) in the input fields. Click <Close> to finish the setting.

NOTE: All analytics share the same object size setting.

Step 6: Select <Object> and choose either “Bottom Center Overlay” or “Center Overlay” from the trigger condition drop-down menu. Please refer to Appendix E: Trigger Type for further details.

Step 7: Select <Alarm> and set up “Keep Alarm Time (1~1000 seconds)”. This feature allows the alarm to continue for a specified time after the trigger condition ends.

Step 8: Select <Schedule> to specify schedule time. Please refer to section System> Schedule Profile for further details.

Step 9: Set up the actions to take when an event occurs, and specify the filename if required, under the <Triggered Action> and <File> sections. Please refer to Appendix D: Standard Setting for further details.

Step 10: This step is only for PTZ Cameras. Proceed to next step if the camera is not a PTZ camera.

Select <Preset Position> and select a specific preset position from the drop-down menu. Click <Copy> to copy current analytics settings to this specific preset position, allowing the analytics to execute when the camera is at that preset position. Please refer to PTZ> Preset to setup the preset point before using this function.

Step 11: Click <Save All Settings> to apply the settings, or click <Restore Default> to revert to the default settings.

3.5.3.14 People Gathering

The People Gathering setting can be found under this path: **Analytics> Video Analytics - AI> Others> People Gathering**.

People Gathering function detects when people gather in a zone for longer than a specified time. Users can configure detection zones, zone positions, and set trigger actions, etc., by following these steps. This function is NOT available for Fisheye Cameras.

Step 1: Configure the people gathering density from <Detection>. Once the distance between individuals reaches the specified density, they will be recognized as a group. The density value ranges from 1% to 100%. A higher percentage means a shorter distance is required for people to form a group, whereas a lower percentage indicates a larger distance. The default value is set to 50%.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

The information below is based on 8MP pixel cameras with full wide zoom (focal length = 3.6 mm), mounted on a 2.25-meter-high wall with a tilt angle of 30°. The distance from the floor under the camera-installed wall to the zone's bottom edge is 1.5 meters. The zone size is set to monitor a 2m x 1.5m area.

Gathering density	Distance to form a group
30	135cm
40	90cm
50 (default)	50cm
70	33cm

Step 2: Select <Zone> to setup virtual zones. Click on <New> in the Detect Zone, and a new zone will appear in the live video pane. Left-clicking the circle on the zone allows users to drag and reshape the virtual zones. Left-clicking the square allows users to add an anchor point, splitting the line into two for further adjustments. Right-clicking the circle on the zone to remove an anchor point.

Click on <Reset> to reset the zone's settings, and click on <Delete> to delete the zone. The maximum amount of detection zones is 4.

Step 3: Select the specific detect zone and setup <Trigger Conditions for Detect Zone> in <Zone>. Enter a value for "Object Allowed Time" to specify the amount of time allowed for objects to move within this zone. The available time ranges from 1 to 1800 seconds.

Set up a value for "Number of People" in the range of 2 to 10.

Actions will be triggered if the group in the zone exceeds the "Object Allowed Time" and the number of people in the group meets the set value for "Number of People"

Step 4: Use Exclude Zone to create an area where users don't want detected objects to trigger actions. Click on <New> in the exclude zone and a new ex-zone will appear in the live video pane. Left-clicking the circle on the zone allows users to drag and reshape the virtual zone. Left-clicking the square allows users to add an anchor point, splitting the line into two for further adjustments. Right-clicking the circle on the zone to remove an anchor point.

Click on <Reset> to reset the ex-zone's settings, and click on <Delete> to delete the ex-zone. The maximum amount of detection zones is 4.

Step 5: Select <Object> to set up the object size and trigger condition. Click <Edit> to set the minimum and maximum size of the detected objects. Users can adjust the blue or pink frame or enter the width (FOV) and height (FOV) in the input fields. Click <Close> to finish the setting.

NOTE: All analytics share the same object size setting.

Step 6: Select <Object> and choose either “Bottom Center Overlay”, “Center Overlay”, “Edge Overlay” or “Fully Inside Overlay” from the trigger condition drop-down menu. Please refer to Appendix E: Trigger Type for further details.

Step 7: Select <Alarm> and set up “Keep Alarm Time (1~1000 seconds)”. This feature allows the alarm to continue for a specified time after the trigger condition ends.

Step 8: Select <Schedule> to specify schedule time. Please refer to section System> Schedule Profile for further details.

Step 9: Set up the actions to take when an event occurs, and specify the filename if required, under the <Triggered Action> and <File> sections. Please refer to Appendix D: Standard Setting for further details.

Step 10: This step is only available for PTZ Cameras. Proceed to next step if the camera is not a PTZ camera.

Select <Preset Position> and select a specific preset position from the drop-down menu. Click <Copy> to copy current analytics settings to this specific preset position, allowing the analytics to execute when the camera is at that preset position. Please refer to PTZ> Preset to setup the preset point before using this function.

Step 11: Click <Save All Settings> to apply the settings, or click <Restore Default> to revert to the default settings.

3.5.3.15 Abandoned Object

The Abandoned Object setting can be found under this path: **Analytics> Video Analytics - AI> Others> Abandoned Object**.

Abandoned Object function detects objects that remain in a zone for longer than a specified time. Users can configure detection zones, zone positions, and set trigger actions, etc., by following these steps.

Step 1: Select <Zone> to setup virtual zones. Click on <New> in the Detect Zone, and a new zone will appear in the live video pane. Left-clicking the circle on the zone allows users to drag and reshape the virtual zones. Left-clicking the square allows users to add an anchor point, splitting the line into two for further adjustments. Right-clicking the circle on the zone to remove an anchor point.

Click on <Reset> to reset the zone’s settings, and click on <Delete> to delete the zone. The maximum amount of detection zones is 4.

Step 2: Select the specific zone and set up <Trigger Conditions for Detect Zone> in <Zone>. Enter a value for "Object Allowed Time" to specify the amount of time allowed for an object to move within this zone. Actions will be triggered if an object exceeds this time. The available time ranges from 1 to 1800 seconds.

Step 3: Use Exclude Zone to create an area where users don't want detected objects to trigger actions. Click on <New> in the exclude zone and a new ex-zone will appear in the live video pane. Left-clicking the circle on the zone allows users to drag and reshape the virtual zone. Left-clicking the square allows users to add an anchor point, splitting the line into two for further adjustments. Right-clicking the circle on the zone to remove an anchor point.

Click on <Reset> to reset the ex-zone's settings, and click on <Delete> to delete the ex-zone. The maximum amount of detection zones is 4.

Step 4: Select <Object> to set up the object size and trigger condition. Click <Edit> to set the minimum and maximum size of the detected objects. Users can adjust the blue or pink frame or enter the width (FOV) and height (FOV) in the input fields. Click <Close> to finish the setting.

NOTE: All analytics share the same object size setting.

Step 5: Select <Object> and choose either "Bottom Center Overlay", "Center Overlay", "Edge Overlay" or "Fully Inside Overlay" from the trigger condition drop-down menu. Please refer to Appendix E: Trigger Type for further details.

Step 6: Select <Alarm> and set up "Keep Alarm Time (1~1000 seconds)". This feature allows the alarm to continue for a specified time after the trigger condition ends.

Step 7: Select <Schedule> to specify schedule time. Please refer to section System> Schedule Profile for further details.

Step 8: Set up the actions to take when an event occurs, and specify the filename if required, under the <Triggered Action> and <File> sections. Please refer to Appendix D: Standard Setting for further details.

Step 9: This step is only available for PTZ Cameras. Proceed to next step if the camera is not a PTZ camera.

Select <Preset Position> and select a specific preset position from the drop-down menu. Click <Copy> to copy current analytics settings to this specific preset position, allowing the analytics to execute when the camera is at that preset position. Please refer to PTZ> Preset to setup the preset point before using this function.

Step 10: Click <Save All Settings> to apply the settings, or click <Restore Default> to revert to the default settings.

3.5.3.16 Removed Object

The Removed Object setting can be found under this path: **Analytics> Video Analytics - AI> Others> Removed Object**.

Removed Object function detects the absence of objects that were previously in a zone. Users can configure detection zones, zone positions, and set trigger actions, etc., by following these steps.

Step 1: Select <Zone> to setup virtual zones. Click on <New> in the Detect Zone, and a new zone will appear in the live video pane. Left-clicking the circle on the zone allows users to drag and reshape the virtual zones. Left-clicking the square allows users to add an anchor point, splitting the line into two for further adjustments. Right-clicking the circle on the zone to remove an anchor point.

Click on <Reset> to reset the zone's settings, and click on <Delete> to delete the zone. The maximum amount of detection zones is 4.

Step 2: Select the specific zone and set up <Trigger Conditions for Detect Zone> in <Zone>. Enter a value for "Object Allowed Time" to specify the amount of time allowed for an object to move within this zone. Actions will be triggered if an object exceeds this time. The available time ranges from 1 to 1800 seconds.

Step 3: Use Exclude Zone to create an area where users don't want detected objects to trigger actions. Click on <New> in the exclude zone and a new ex-zone will appear in the live video pane. Left-clicking the circle on the zone allows users to drag and reshape the virtual zone, while the square allows users to add an anchor point, splitting the line into two for further adjustments. Right-clicking the circle on the zone to remove an anchor point.

Click on <Reset> to reset the ex-zone's settings, and click on <Delete> to delete the ex-zone. The maximum amount of detection zones is 4.

Step 4: Select <Object> to set up the object size and trigger condition. Click <Edit> to set the minimum and maximum size of the detected objects. Users can adjust the blue or pink frame or enter the width (FOV) and height (FOV) in the input fields. Click <Close> to finish the setting.

NOTE: All analytics share the same object size setting.

Step 5: Select <Object> and choose either "Bottom Center Overlay", "Center Overlay", "Edge Overlay" or "Fully Inside Overlay" from the trigger

condition drop-down menu. Please refer to Appendix E: Trigger Type for further details.

Step 6: Select <Alarm> and set up "Keep Alarm Time (1~1000 seconds)". This feature allows the alarm to continue for a specified time after the trigger condition ends.

Step 7: Select <Schedule> to specify schedule time. Please refer to section System> Schedule Profile for further details.

Step 8: Set up the actions to take when an event occurs, and specify the filename if required, under the <Triggered Action> and <File> sections. Please refer to Appendix D: Standard Setting for further details.

Step 9: This step is only available for PTZ Cameras. Proceed to next step if the camera is not a PTZ camera.

Select <Preset Position> and select a specific preset position from the drop-down menu. Click <Copy> to copy current analytics settings to this specific preset position, allowing the analytics to execute when the camera is at that preset position. Please refer to PTZ> Preset to setup the preset point before using this function.

Step 10: Click <Save All Settings> to apply the settings, or click <Restore Default> to revert to the default settings.

3.5.3.17 Face Recognition

The Face Recognition setting can be found under this path: **Analytics> Video Analytics - AI> Face Recognition**.

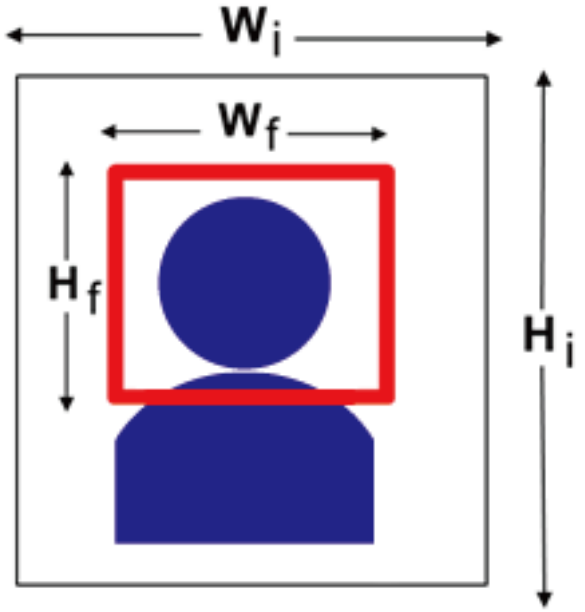
Face Recognition function detects or extract face information to identify a person's identity. Users can configure detection zones, zone positions, and set trigger actions, etc., by following these steps. This function is NOT available for Fisheye Cameras.

Step 1: Select <Database> to create a database and predefines the data into different action list—allow, block or undefined. Click <Open>, and the <Database Overview> page will appear, displaying all the data information.

Step 2: Click <New User> to add new user information. Enter the user's name in the "Name" field. Select "Group" from the drop-down menu if necessary. Please refer to <Edit Group> to create group names prior to making a selection. Select an "Action List" to categorize users by choosing "Allow", "Block" or "Undefined" from the drop-down menu. Enter the description about the user in the "Description" field if necessary. Click <> to upload facial images for the user. At least one image is required, it is recommended to upload images taken from three different angles. Click <Add User> to save the setting.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

The face must take up at least 12% and at most 25% of the image. **See the formula below to understand how the range of ratios is calculated.** More images with multiple angles (both eyes should be revealed) or various looks of the user, e.g., with/without glasses, with different hairstyles, are preferred. Supported image formats are JPEG/PNG/BMP. Recommended image size is between 200x200 to 1920x1080 pixels.



Formula:
(Width **f** x Height **f**) / (Width **i** x Height **i**) =
The ratio of the face (**f**) taking up space in an image (**i**)

Step 3: To edit user's information, access <Database Overview> and click < > to edit information of the specific user. The screen will redirect to <Edit User> page for that specific user. Click on <Update User> after updating the user's information.

Step 4: Click <Edit Group> to create new groups. Enter the new group's name in "New Group", click <Add> to save the setting. The maximum number of groups is 32.

Select the specific group name in "Group Name", and click <Edit> or <Delete> to edit or delete the group.

NOTE: The user and group data can be imported into other cameras. To export the data into a database file or to import a database file, please refer to Appendix F: Edit Database for further details. If not, please proceed to **Step 5**.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Step 5: Click <Close> to finish the setting.

Step 6: Set up “Mode”, “Extra Face Information” and “Recognition Confidence Threshold” from <Detection>.

Mode

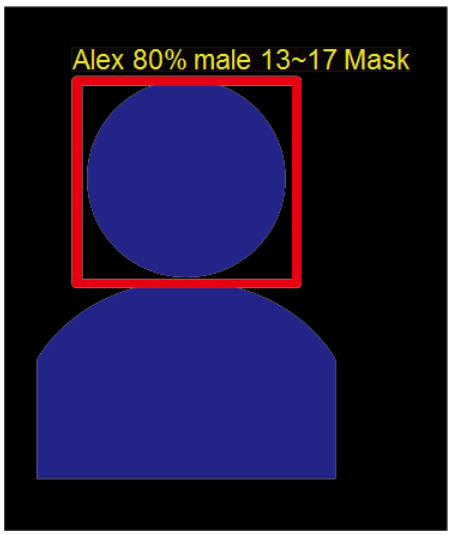
Users can select from the dropdown menu to perform either face detection only or both face detection and recognition. “Face Detection Only” detects only the face, while “Face Detection and Recognition” detects the face and performs recognition. Face image database is required when choosing “Face Detection and Recognition”.

Extra Face Information

This function allows users to define the information displayed when a face is detected or recognized with options including “Age,” “Gender,” or “Mask”.

Recognition Confidence Threshold

Select “Recognition Confidence Threshold” to set up a threshold value. Predictions with a confidence score lower than the threshold value are ignored. If the prediction value of the detected face is higher than the threshold, it will be considered as valid face. For face recognition, the corresponding person’s name will be displayed. The threshold ranges from 1 to 100%.



Example:
The verification passes when the prediction value (80%)
is higher than “Recognition Confidence Threshold” value (75%).

NOTE: The recognition threshold value will display only when object confidence level data is selected, please refer to section Analytics>Common Setting for further details.

Step 7: Select <Zone> to setup virtual zones. Click on <New> in the Detect Zone, and a new zone will appear in the live video pane. Left-clicking the circle on the zone allows users to drag and reshape the virtual zones. Left-clicking the square allows users to add an anchor point, splitting the line into two for further adjustments. Right-clicking the circle on the zone to remove an anchor point.

Click on <Reset> to reset the zone's settings, and click on <Delete> to delete the zone. The maximum amount of detection zones is 4.

Step 8: Use Exclude Zone to create an area where users don't want detected objects to trigger actions. Click on <New> in the exclude zone and a new ex-zone will appear in the live video pane. Left-clicking the circle on the zone allows users to drag and reshape the virtual zone. Left-clicking the square allows users to add an anchor point, splitting the line into two for further adjustments. Right-clicking the circle on the zone to remove an anchor point.

Click on <Reset> to reset the ex-zone's settings, and click on <Delete> to delete the ex-zone. The maximum amount of detection zones is 4.

Step 9: Select <Object> to set up the object size and trigger condition. Click <Edit> to set the minimum and maximum size of the detected objects. Users can adjust the blue or pink frame or enter the width (FOV) and height (FOV) in the input fields. Click <Close> to finish the setting.

NOTE: All analytics share the same object size setting.

Step 10: Select <Alarm> and set up "Keep Alarm Time (1~1000 seconds)". This feature allows the alarm to continue for a specified time after the trigger condition ends.

Step 11: Select <Schedule> to specify schedule time. Please refer to section System> Schedule Profile for further details.

Step 12: Select <Trigger Action> and set up the actions to take for individuals in Allow, Block and Undefined List, and specify the filename if required, under the <Triggered Action> and <File> sections. Please refer to Appendix D: Standard Setting for further details.

Select "If people in the Allow List are triggered" to set up a trigger action when individuals on the allow list enter the zone.

Select "If people in the Block List are triggered" to set up a trigger action when individuals on the block list enter the zone.

Select "If people in the Undefined List are triggered" to set up a trigger action when individuals on the undefined list enter the zone.

Step 13: This step is only available for PTZ Cameras. Proceed to next step if the camera is not a PTZ camera.

Select <Preset Position> and select a specific preset position from the drop-down menu. Click <Copy> to copy current analytics settings to this specific preset position, allowing the analytics to execute when the camera is at that preset position. Please refer to PTZ> Preset to setup the preset point before using this function.

Step 14: Click <Save All Settings> to apply the settings, or click <Restore Default> to revert to the default settings.

3.5.3.18 License Plate Recognition

The License Plate Recognition setting can be found under this path: **Analytics> Video Analytics - AI> License Plate Recognition**.

License Plate Recognition function detects and extract license plate information from vehicles. Users can configure detection zones, zone positions, and set trigger actions, etc., by following these steps. This function is NOT available for Fisheye Cameras.

Step 1: Select <Database> to create a database and predefines the data into different action list—allow, block or undefined. Click <Open>, and the <Database Overview> page will appear, displaying all the data information.

Step 2: Click <New License Plate> to add new license plate information. Enter the license plate number in the “License Plate Number” field. Select “Group” from the drop-down menu if necessary. Please refer to <Edit Group> to create group names prior to making a selection. Select an “Action List” to categorize users by choosing “Allow”, “Block” or “Undefined” from the drop-down menu. Enter the description about the user in the “Description” field if necessary. Click <Add> to save the setting.

NOTE: When entering license plate information in the database, there is no need to include spaces or symbols. For example, when a license plate is ABC-567, users can input ABC567.

Step 3: Click <Edit Group> to create new groups. Enter the new group’s name in “New Group”, click <Add> to save the setting. The maximum number of groups is 32.

Select the specific group name in “Group Name”, and click <Edit> or <Delete> to edit or delete the group.

NOTE: The license plate and group data can be imported into other cameras. To export the data into a database file or to import a database file, please refer to Appendix F: Edit Database for further details. If not, please proceed to **Step 4**.

Step 4: Click <Close> to finish the setting.

Step 5: Set up “License Plate Region for Recognition”, “Min Plate Characters” and “Recognition Confidence Threshold” from <Detection>.

License Plate Region for Recognition
Users can select license plate region from the dropdown menu for recognition. Refer to Appendix G: License Plate Region for further details.

Min Plate Characters
Users can set the required string length for license plate recognition. A license plate must have at least the specified string length to trigger action. The range is from 3 to 12.

Recognition Confidence Threshold
Select “Recognition Confidence Threshold” to set up a threshold value. Predictions with a confidence score lower than the threshold value are ignored. If the prediction value of the detected license plate number is higher than the threshold, it will be considered as valid license plate number. The threshold ranges from 1 to 100%.

Step 6: Select <Zone> to setup virtual zones. Click on <New> in the Detect Zone, and a new zone will appear in the live video pane. Left-clicking the circle on the zone allows users to drag and reshape the virtual zones. Left-clicking the square allows users to add an anchor point, splitting the line into two for further adjustments. Right-clicking the circle on the zone to remove an anchor point.

Click on <Reset> to reset the zone’s settings, and click on <Delete> to delete the zone. The maximum amount of detection zones is 4.

Step 7: Use Exclude Zone to create an area where users don’t want detected objects to trigger actions. Click on <New> in the exclude zone and a new ex-zone will appear in the live video pane. Left-clicking the circle on the zone allows users to drag and reshape the virtual zone. Left-clicking the square allows users to add an anchor point, splitting the line into two for further adjustments. Right-clicking the circle on the zone to remove an anchor point.

Click on <Reset> to reset the ex-zone’s settings, and click on <Delete> to delete the ex-zone. The maximum amount of detection zones is 4.

Step 8: Select <Object> to set up the object size and trigger condition. Click <Edit> to set the minimum and maximum size of the detected objects. Users can adjust the blue or pink frame or enter the width (FOV) and height (FOV) in the input fields. Click <Close> to finish the setting.

NOTE: All analytics share the same object size setting.

Step 9: Select <Alarm> and set up “Keep Alarm Time (1~1000 seconds)”. This feature allows the alarm to continue for a specified time after the trigger condition ends.

Step 10: Select <Schedule> to specify schedule time. Please refer to section System> Schedule Profile for further details.

Step 11: Select <Trigger Action> and set up the actions to take for individuals in Allow, Block and Undefined List, and specify the filename if required, under the <Triggered Action> and <File> sections. Please refer to Appendix D: Standard Setting for further details.

Select “If License Plate in the Allow List are triggered” to set up a trigger action when license plate number on the allow list enter the zone.

Select “If License Plate in the Block List are triggered” to set up a trigger action when license plate number on the block list enter the zone.

Select “If License Plate in the Undefined List are triggered” to set up a trigger action when license plate number on the undefined list enter the zone.

Step 12: This step is only available for PTZ Cameras. Proceed to next step if the camera is not a PTZ camera.

Select <Preset Position> and select a specific preset position from the drop-down menu. Click <Copy> to copy current analytics settings to this specific preset position, allowing the analytics to execute when the camera is at that preset position. Please refer to PTZ> Preset to setup the preset point before using this function.

Step 13: Click <Save All Settings> to apply the settings, or click <Restore Default> to revert to the default settings.

3.5.3.19 Auto Tracking

The Auto Tracking setting can be found under this path: **Analytics> Video Analytics - AI> Auto Tracking**.

Auto Tracking function detects an object and continuously tracks its movement. Users can configure detection zones, zone positions, and set trigger actions, etc., by following these steps. This function is only available for PTZ Cameras.

Step 1: Select the maximum tracking duration for the object and the detection objects from <Detection>.

Select “No limit” to allow unlimited tracking time for a detected object,, or “Limit” to specific tracking duration from the Max. Tracking Time drop-down menu. The limit time range is from 1 to 3600 seconds.

The detection object options are “Human”, “Human Head”, “All Vehicles”, or a specific vehicle type by selecting “Bicycle”, “Car”, “Motorcycle”, “Bus”, or “Truck”.

Step 2: Select <Zone> to setup virtual zones. Click on <New> in the Detect Zone, and a new zone will appear in the live video pane. Left-clicking the circle on the zone allows users to drag and reshape the virtual zones. Left-clicking the square allows users to add an anchor point, splitting the line into two for further adjustments. Right-clicking the circle on the zone to remove an anchor point.

Click on <Reset> to reset the zone’s settings, and click on <Delete> to delete the zone. The maximum amount of detection zones is 4.

Step 3: Use Exclude Zone to create an area where users don’t want detected objects to trigger actions. Click on <New> in the exclude zone and a new ex-zone will appear in the live video pane. Left-clicking the circle on the zone allows users to drag and reshape the virtual zone, while the square allows users to add an anchor point, splitting the line into two for further adjustments. Right-clicking the circle on the zone to remove an anchor point.

Click on <Reset> to reset the ex-zone’s settings, and click on <Delete> to delete the ex-zone. The maximum amount of detection zones is 4.

Step 4: Select <Object> to set up the object size and trigger condition. Click <Edit> to set the minimum and maximum size of the detected objects. Users can adjust the blue or pink frame or enter the width (FOV) and height (FOV) in the input fields. Click <Close> to finish the setting.

NOTE: All analytics share the same object size setting.

Step 5: Select <Object> and choose either “Bottom Center Overlay”, “Center Overlay” or “Edge Overlay” from the trigger condition drop-down menu. Please refer to Appendix E: Trigger Type for further details.

Step 6: Select <Alarm> and set up “Keep Alarm Time (1~1000 seconds)”. This feature allows the alarm to continue for a specified time after the trigger condition ends.

Step 7: Select <Schedule> to specify schedule time. Please refer to section System> Schedule Profile for further details.

Step 8: Set up the actions to take when an event occurs, and specify the filename if required, under the <Triggered Action> and <File> sections. Please refer to Appendix D: Standard Setting for further details.

Step 9: This step is only for PTZ Cameras. Proceed to next step if the camera is not a PTZ camera.

Select <Preset Position> and select a specific preset position from the drop-down menu. Click <Copy> to copy current analytics settings to this specific preset position, allowing the analytics to execute when the camera is at that preset position. Please refer to PTZ> Preset to setup the preset point before using this function.

Step 10: Click <Save All Settings> to apply the settings, or click <Restore Default> to revert to the default settings.

3.5.3.20 Heat Map

The Heat Map setting can be found under this path: **Analytics> Video Analytics - AI> Heat Map**.

Heat Map function counts objects and track the duration of their presence in zones. It generates a color-coded map highlighting areas where objects are most frequently concentrated. Users can configure detection zones, zone positions, and set trigger actions, etc., by following these steps. This function can only be enabled when the camera view is static. For PTZ cameras, a preset position must be specified to use this feature.

Note: The Heat Map function requires an SD Card for operation.

Note: Changing the settings of <Detection>, <Zone> and <Object> and click <Partial Restore> from System> Restore Factory Settings Only (Keep Network Setting) will clear the heat map's historical data.

Step 1: Select the detection objects from <Detection>. The available options are “Human”, “Human Head”, “All Vehicles”, or a specific vehicle type by selecting “Bicycle”, “Car”, “Motorcycle”, “Bus”, or “Truck”.

Step 2: Select <Zone> to setup virtual zones. Click on <New> in the Detect Zone, and a new zone will appear in the live video pane. Left-clicking the circle on the zone allows users to drag and reshape the virtual zones, while the square allows users to add an anchor point, splitting the line into two for further adjustments. Right-clicking the circle on the zone to remove an anchor point.

Click on <Reset> to reset the zone’s settings, and click on <Delete> to delete the zone. The maximum amount of detection zones is 4.

Step 3: Use Exclude Zone to create an area where users don’t want detected objects to trigger actions. Click on <New> in the exclude zone and a new ex-zone will appear in the live video pane. Left-clicking the circle on the zone allows users to drag and reshape the virtual zone, while the square allows users to add an anchor point, splitting the line into two for

further adjustments. Right-clicking the circle on the zone to remove an anchor point.

Click on <Reset> to reset the ex-zone's settings, and click on <Delete> to delete the ex-zone. The maximum amount of detection zones is 4.

Step 4: Select <Object> to set up the object size and trigger condition. Click <Edit> to set the minimum and maximum size of the detected objects. Users can adjust the blue or pink frame or enter the width (FOV) and height (FOV) in the input fields. Click <Close> to finish the setting.

NOTE: All analytics share the same object size setting.

Step 5: Select <Object> and choose either "Bottom Center Overlay" or "Center Overlay" from the trigger condition drop-down menu. Please refer to Appendix E: Trigger Type for further details.

Step 6: Select <Schedule> to specify schedule time. Please refer to section System> Schedule Profile for further details.

Step 7: Select <Report> and choose the format from "Report Type" for presenting heat map data. The available options are daily, weekly, monthly, or annual reports.

For "Date Range", set up the date range for viewing the heat map data.

"Limited Hour" displays the heat map data for the specified time range within each day of the selected date range.

Click <Generate> to generate report. Heat Map data is presented in two ways: <Spatial Heat Map> and <Temporal Heat Map>.

Spatial Heat Map

<Spatial Heat Map> presents different concentrations of objects using color on the image.

Select "Number of Objects" from the drop-down menu to view the color distribution of object concentration. Refer to the color scheme below the live view pane: colors closer to "low" indicate lower object concentrations in the area, while colors closer to "high" indicate higher object concentrations in the area.

Select "Dwell Time" from the drop-down menu to see the color distribution representing the duration that objects are present. Refer to the color scheme below the live view pane: colors closer to "low" indicate shorter presence durations in the area, while colors closer to "high" indicate longer presence durations in the area.

Click <Download> to download an image of the <Spatial Heat Map> data.

Temporal Heat Map

<Temporal Heat Map> presents different concentrations of objects using line chart.

Select “Number of Objects” from the drop-down menu to view the line chart representing the relationship between the number of objects in the scene and time within the specified time range.

Select “Dwell Time” from the drop-down menu to see the line chart representing the duration that objects are present, and select “Average Dwell Time” to view the average duration of object presence.

Click <Export CSV> to export the data.

Step 8: This step is only for PTZ Cameras. Proceed to next step if the camera is not a PTZ camera.

Select <Preset Position> and select a specific preset position from the drop-down menu. Click <Copy> to copy current analytics settings to this specific preset position, allowing the analytics to execute when the camera is at that preset position. Please refer to PTZ> Preset to setup the preset point before using this function.

Step 9: Click <Save All Settings> to apply the settings, or click <Restore Default> to revert to the default settings.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

3.5.4 Video Analytics - Legacy

The Video Analytics - Legacy setting can be found under this path: **Analytics> Video Analytics - Legacy**.

3.5.4.1 Motion Detection

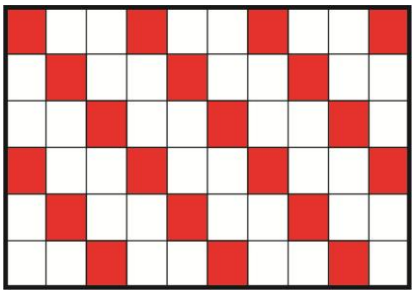
The Motion Detection setting can be found under this path: **Analytics> Video Analytics - Legacy> Motion Detection**.

Motion Detection function allows the camera to detect suspicious motion and trigger alarms by comparing sampling pixels in the detection area of two consecutive live images. When motion volume in the detection area reaches / exceeds the determined sensitivity threshold value, the alarm will be triggered.

Step 1: Select a group number from the <Motion Detection Group> drop-down menu for configuration. The function supports up to 4 groups of Motion Detection Settings.

Step 2: Select <Detection Setting> to set up “Sampling Pixel Interval”, “Detection Level”, “Sensitivity Level” and “Time Interval (sec)”.

Sampling Pixel Interval [1-10]
This item is used to examine the differences between two frames. Users can configure the interval of sampling pixel. The default value is 1. For instance, if users set the interval as 3, the camera system will take one sampling pixel from every 3 pixels of each row and each column in detection area (refer to the figure below). The alarm will be triggered when differences are detected.



Detection Level [1-100]
Users can configure detection level for each sampling pixel. Detection level is how much the camera can accept the differences between two sampling pixels. A smaller value indicates the detection of more subtle motions. The default level is 10.

Sensitivity Level [1-100]

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

The default level is 80, which means if 20% or more sampling pixels are detected differently, system will detect motion. The bigger the value, the more sensitive it is. Meanwhile, when the value is bigger, the red horizontal line in the motion indication window will be lower accordingly.

Time Interval (sec) [0-7200]
The value is the interval between each detected motion. The default interval is 10.

Step 3: Select <Zone>. Check the box <Enable brush> and select the brush size, 1x1, 3x3 or 5x5. Then, left click and drag the mouse cursor to draw the preferred detection region. To erase the drawn detection region, left click and drag the mouse cursor on the colored grids.

The camera divides the detection area into 1200 (40x30) detection grids; users can draw the motion detection region using the paintbrush.

Step 4: Select <Schedule> to specify schedule time. Please refer to section System> Schedule Profile for further details.

Step 5: Set up the actions to take when an event occurs, and specify the filename if required, under the <Triggered Action> and <File> sections. Please refer to Appendix D: Standard Setting for further details.

Step 6: Click <Save All Settings> to apply the setting.

Motion Indicator
When Motion Detection function is activated from System Overview> System: Other Analytics and the motion is detected, the signals will be displayed on the motion indicator. The motion indicator will go green or red when there is any motion occurrence in the detection region.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Green suggests the occurring motion is detected and does not exceed the threshold of detection level and sensitivity level. No alarms will be triggered.

Red suggests the ongoing motion exceeds the threshold of detection level and sensitivity level. The alarm will be triggered.

3.5.4.2 Tampering

The Tampering setting can be found under this path: **Analytics> Video Analytics - Legacy> Tampering**.

Tampering Alarm function helps the camera against tampering, such as deliberate redirection, blocking, paint spray, and lens cover, etc., through video analysis and reaction to such events by sending out notifications or uploading snapshots to the specified destination(s).

Detection of camera tampering is achieved by measuring the differences between the older frames of video (which are stored in buffers) and more recent frames.

This function is **NOT** available for PTZ Cameras.

Tampering Alarm

The default setting for the Tampering Alarm function is <Off>. Activate the function from Analytics> System Overview> System: Other Analytics. Users can also select the specify schedule time. Please refer to section System> Schedule Profile for further details.

Tampering Duration

Tampering Duration is the minimum time required to determine if camera tampering has occurred. The Tampering Duration time range is from 10 to 3600 sec. The Default value is 20 sec.

Triggered Action and File Name

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Set up the actions to take when an event occurs, and specify the filename if required, under the <Triggered Action> and <File> sections. Please refer to Appendix D: Standard Setting for further details.

Save
Click on <Save> to save all the settings mentioned above.

3.5.5 Audio Analytics

The Audio Analytics setting can be found under this path: **Analytics> Audio Analytics**.

Audio Analytics function allows the camera to detect audio and trigger alarms when audio volume in the detected area reaches / exceeds the determined sensitivity threshold value.

NOTE: Audio Analytics function is only available for models equipped with Audio I/O function.

Audio Detection
In Audio Detection Setting, the default setting for the Audio Detection function is <Off>. Enable the function by selecting <On>.

Audio Detection Setting
Users could adjust various parameters of Audio Detection in this section.

- **Detection level [1-100]:**
  The item is to set detection level for each sampling volume; the smaller the value, the more sensitive it is. The default level is 10.

- **Time Interval (sec) [0-7200]:**
  The value is the interval between each detected audio. The default interval is 10.

Triggered Action and File Name
Set up the actions to take when an event occurs, and specify the filename if required, under the <Triggered Action> and <File> sections. Please refer to Appendix D: Standard Setting for further details.

Save
Click on <Save> to save all the settings mentioned above.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

3.5.6 Alarm Input

The Alarm Input setting can be found under this path: **Analytics> Alarm Input**.

The camera supports alarm input and output for cooperation with alarm system to catch event images. Refer to alarm pin definition below to connect alarm devices to the camera if needed.

Alarm Switch
Select to specify the schedule time. Please refer to section System> Schedule Profile for further details.

Alarm Type
Select an alarm type, <Normal Close> or <Normal Open> that corresponds with the alarm application.

Triggered Action and File Name
Set up the actions to take when an event occurs, and specify the filename if required, under the <Triggered Action> and <File> sections. Please refer to Appendix D: Standard Setting for further details.

Save
Click on <Save> to save all the settings mentioned above.

3.5.7 General

The General setting can be found under this path: **Analytics> General**.

3.5.7.1 Network Failure Detection

The Network Failure Detection setting can be found under this path: **Analytics> General> Network Failure Detection**.

Network Failure Detection allows the camera to ping another IP device (e.g. NVR, VSS, Video Server, etc.) within the network periodically and generates some actions in case of network failure occurs, for instance, a Video Server is somehow disconnected.

Being capable of implementing local recording (through microSD/SD card) or remote recording (via Network Storage) when network failure happens, the camera can be a backup recording device for the surveillance system.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Detection Switch
Select to specify the schedule time. Please refer to section System> Schedule Profile for further details.

Detection Type
Input the IP device address and the period of ping time to ping. The camera will ping the IP device every N minute(s). If it fails for up to three times, the alarm will be triggered. The ping interval setting range is from 1 to 6000 seconds.

Triggered Action
Set up the actions to take when an event occurs under the <Triggered Action>. Please refer to Appendix D: Standard Setting for further details.

Save
Click on <Save> to save all the settings mentioned above.

3.5.7.2 Periodical Event

The Periodical Event setting can be found under this path: **Analytics> General> Periodical Event**.

With Periodical Event setting, users can set the camera to upload images periodically to an FTP site or an E-mail address. For example, if the time interval is set to 60 seconds, the camera will upload images to the FTP site or the E-mail address every 60 seconds. The images to be uploaded are the images before and after the triggered moment. Users can define how many images to be uploaded in the <Triggered Action> section of this setting page.

Periodical Event
The default setting for the Periodical Event function is <Off>. Enable the function by selecting <On>.

Time Interval
The default value of the time interval is 60 seconds. The setting range of the time interval is from 60 to 3600 seconds.

Triggered Action and File Name
Set up the actions to take when an event occurs, and specify the filename if required, under the <Triggered Action> and <File> sections. Please refer to Appendix D: Standard Setting for further details.

Save
Click on <Save> to save all the settings mentioned above.

3.5.7.3 Manual Trigger

The Manual Trigger setting can be found under this path: **Analytics> General> Manual Trigger**.

With Manual Trigger setting, the current image(s) or video can be uploaded to the appointed destination, such as an FTP site or an E-mail address. The administrator can specify the triggered actions that will take when the users switch the Manual Trigger button to ON. All options are listed as follows.

Manual Trigger
The default setting for the Manual Trigger function is <Off>. Enable the function by selecting <On>. After the Manual Trigger function is enabled, click the Manual Trigger button on the Home page to start uploading data. Click again to stop uploading.

Triggered Action and File Name
Set up the actions to take when an event occurs, and specify the filename if required, under the <Triggered Action> and <File> sections. Please refer to Appendix D: Standard Setting for further details.

Save
Click on <Save> to save all the settings mentioned above.

3.5.7.4 Shock Detection

The Shock Detection setting can be found under this path: **Analytics> General> Shock Detection**.

When the Shock Detection function is enabled, the camera continuously monitors its position and acceleration. If the camera is tilted, displaced, or subjected to impacts such as punches or hard blows, an alarm is triggered, and the camera generates a shock detection event.

The alarm activates instantly upon impact or displacement, with no pre-trigger time. After the alarm is triggered, monitoring resumes from the camera's new position. To avoid generating multiple events for the same displacement, a new shock detection event will not occur until 5 seconds have elapsed.

This function is only available for Zoom Lens and Box Camera.

Shock Indication Bar

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

When shock detection is activated from <System Overview> and the motion is detected, the signals will be displayed on the shock indication bar. The shock indication bar will go green or red when the camera experiences impact or displacement.

Green suggests the impact or displacement is detected and does not exceed the threshold of detection level and sensitivity level. No alarms will be triggered.

Red suggests the ongoing impact or displacement exceeds the threshold of detection level and sensitivity level. The alarm will be triggered.

Shock Detection
Select the specify schedule time. Please refer to section System> Schedule Profile for further details.

Shock Detection Setting
The item is to set Detection level [1-100] for each shocking volume; the smaller the value, the more sensitive it is. The default level is 10.

Shock Detection Setting can be adjusted between 0 and 100. A low detection setting means that even minor displacements, such as vibrations, will trigger alarms. In contrast, a high detection setting means that a significant impact is required to trigger an alarm.

Triggered Action and File Name
Set up the actions to take when an event occurs, and specify the filename if required, under the <Triggered Action> and <File> sections. Please refer to Appendix D: Standard Setting for further details.

Save
Click on <Save> to save all the settings mentioned above.

3.5.8 License Management

The License Management setting can be found under this path: **Analytics> License Management**.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

VA License Status

The VA License Status shows if the Video Analytics function is a trial or registered version.

Update License

Enter license key and click on <Upload License> to upload license. Please contact the sales representatives for the license key.

NOTE: Authentication failed more than 3 times, the entry field will be grayed out. Please press the default button from System> Maintenance> Factory Default and enter the license key again.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

3.6 Camera

Under the tab <**Camera**>, there are submenus including: <Exposure Mode>, <Exposure Tweak>, <White Balance>, <Picture Adjustment>, <Auto Focus>, <Day/Night Mode>, <Illumination>, <Noise Reduction>, <HDR>, <Image Stabilizer>, <Digital Zoom>, <Backlight>, <User Setting Profile> and <TV System>.

3.6.1 Exposure Mode

The Exposure Mode setting can be found under this path: **Camera> Exposure Mode**.

Exposure Mode is the amount of light received by the image sensor. It is determined by the width of lens diaphragm opening, the shutter speed and other exposure parameters. With these items, users can define how the Auto Exposure function works. Users can select one of the exposure modes according to the operating environment. Each exposure mode is specified as follows.

Function \ Lens		Motorized / Zoom Lens with P-Iris	Zoom Lens with Auto Iris	Fisheye	Others (6)
Max Gain			V	V	V
P-Iris Priority	Iris Size Setting	V	V		
	P-Iris(Close, Open, Reset, Push)	V			
	Max Gain	V			
	Auto Detect		V		
	Manual Mode		V		
	Min Shutter Speed	V	V		
Auto Iris	Min Shutter Speed		V		V
Iris Priority	Iris Size		V		
	Min Shutter Speed				
Auto Shutter	Min Shutter Speed		V	V	V
Shutter Priority			V		V
Manual Mode	Iris size setting (Close, Open, Reset, Push) /	V	V		V

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

	Iris size				
	Shutter Speed	V	V	V	V
	Gain	V	V	V	V

NOTE: The red “V” indicates the default exposure mode of the lens.

Window Setting

With this function, users can determine which area of the camera scene is used to calculate the exposure. Follow the steps below to set the Auto Exposure (AE) window.

- Point the camera to the monitoring area.
- Select <On> to enable the function.
- Click and drag the center of the AE window to move it to the interested location; click and drag the edge of the window outward / inward to resize the window.
- Click on <Set>, and the camera will automatically adjust the exposure parameters according to the light condition of the user defined area.

NOTE: Window Setting function is **NOT** available when TV System is set as “HDR 2x shutter”.

Max Gain

Maximum Gain can be set to reduce image noises. The Max Gain ranges from 3dB to 48dB, or select <Off> to disable the function. The default setting is 48dB. For the Fisheye Camera, the Max Gain ranges from 3dB to 45dB, the default setting is 45dB.

Auto Iris

In this mode, the camera will automatically adjust the iris to suit the environment illumination. AGC (Auto Gain Control) will function automatically according to the light conditions of the subject. The default setting is 1/4 sec. (NTSC) or 1/3 sec. (PAL). The configuration will vary according to different camera models.

P-Iris Priority

P-iris priority mode is only available for Motorized Lens and Zoom Lens. In addition, applied with different lens, the related setting options also vary. Refer to the following for further details. The configuration will vary according to different camera models.

- Zoom Lens with Auto Iris

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Select <Auto Detect>, the camera will automatically detect the best iris size for the environment. Alternatively, users can manually adjust the iris size by selecting <Manual>. Click <Open> and <Close> to adjust the iris size.

- Motorized Lens and Zoom Lens with P-Iris
  Click on <Push>, and the camera will automatically detect the best iris size for the environment. Alternatively, click on <Reset> to reset the iris to the largest size. Users can select <Open> and <Close> manually to adjust the iris size.

Iris Priority Mode

Iris priority mode is only available for Zoom Lens with Auto Iris. In this mode, it is the iris that has premier priority in control of the exposure. The range of the iris size is from 0 to 9, or select <Full open> to fully open the iris.

Auto Shutter Mode

Auto Shutter mode is **NOT** available for Motorized Lens and Zoom Lens with P-Iris. In this mode, the camera will automatically adjust the shutter speed and the iris size according to the light intensity. It is also effective if a fixed iris lens is being used. The default setting is 1/4 sec. (NTSC) or 1/3 sec. (PAL). The configuration will vary according to different camera models.

Shutter Priority Mode

Shutter Priority mode is **NOT** available for Motorized Lens or Zoom Lens with P-Iris and Fisheye Camera. In this mode, it is the shutter speed that takes the main control of the exposure. The range is configurable from 1/500 to 1/30 sec. (NTSC) or 1/425 or 1/25 sec. (PAL), or 1/500 to 1/60 sec. (NTSC) or 1/425 or 1/50 sec. (PAL). The configuration will vary according to different camera models.

Manual Mode

With this mode, users can select the suitable shutter speed, iris size and gain value according to the environmental illumination. The default setting is 1/60 sec. (NTSC) or 1/50 sec. (PAL).

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

The range of the iris size is from 0 to 9, or select <Full open> to fully open the iris. The gain value range is from 3dB to 48dB. For Fisheye Camera the gain value range is from 3db to 45db, or select <Off> to disable the function.

NOTE: The <Iris Size> setting is only available for models with Zoom Lens.

NOTE: Click on <Push>, and the camera will automatically detect the best iris size for the environment. Alternatively, click on <Reset> to reset the iris to the largest size. Users can select <Open> and <Close> manually to adjust the iris size.

3.6.2 Exposure Tweak

The Exposure Tweak setting can be found under this path: **Camera> Exposure Tweak**.

AE Priority

The Auto Exposure Priority function automatically adjusts the camera's exposure settings to ensure that the images remain clear and bright under low-light conditions. There are two modes available, each with a distinct order of adjusting Gain and Shutter Speed. Users can opt for either mode depending on their requirements.

- **Realtime**
  <Realtime> mode prioritizes increasing gain to the maximum over slowing down shutter speed. Shutter speed will be slowed down only when maximum gain is reached. Select <Realtime> mode if users prefer to maintain the frame rate.

- **Image Quality**
  To maintain the brightness of the image, gain and shutter speed in <Image Quality> mode will be progressively adjusted under low light conditions. Shutter speed will progressively slow down with the increasing gain until the image is bright enough.

Night Mode Priority

- **Normal**

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

With this mode, the suitable exposure can be automatically adjusted depending on the environment.

- **High Light Detail**
  It is recommended to choose high light detail mode in the dark environment if users want to see details of high light object. With this mode, the camera will automatically adjust the exposure and make the high light object more visible. Note that the dark place will become darker when this mode is turned on.

Color Style

Color Style can automatically adjust the brightness, allowing users to select the best Color Style mode based on the operating environment. Refer to the descriptions of each mode below to select a suitable mode.

- **Normal**
  Normal mode is the default setting mode.
- **Dark Detail Brighter**
  This mode increases brightness on dark areas of the image.
- **Highlight Detail Brighter**
  This mode increases brightness on general-illuminated areas of the image.

3.6.3 White Balance

The White Balance setting can be found under this path: **Camera> White Balance**.

A camera needs to find reference color temperature, which is a way of measuring the quality of a light source, for calculating all the other colors. The unit for measuring this ratio is in degree Kelvin (K). Users can select one of the White Balance Control modes according to the operating environment. The following table shows the color temperature of some light sources for reference.

Light Sources	Color Temperature in K
Cloudy Sky	6,000 to 8,000
Noon Sun and Clear Sky	6,500
Household Lighting	2,500 to 3,000
75-watt Bulb	2,820

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Candle Flame	1,200 to 1,500

AWB.normal

The **AWB (Auto White Balance).normal** mode is suitable for environments with light source having color temperature in the range roughly from 2700K to 7800K.

AWB.wide

With **AWB (Auto White Balance).wide** function, the white balance in a scene will be automatically adjusted while temperature color is changing. The ATW Mode is suitable for environments with light source having color temperature in the range roughly from 2500K to 10000K.

AWB.all

The **AWB (Auto White Balance).all** mode is suitable for environments with light source having color temperature under 2500K or over 10000K.

Smart

The Smart mode is suitable for environments with one single background color which is strongly saturated, for instance, in a forest.

One Push

With One Push function, white balance is adjusted and fixed according to the scene the camera sees at the moment. This function is best for situations with minimal scene changes and continuous lighting. The function is suitable for light sources with any kind of color temperature. Follow the steps below to set the white balance.

- Point the camera to the monitoring area.
- Select <One Push> in the White Balance setting menu
- Click the <Push> button to adjust the color tone of the live images.

NOTE: In this mode, the value of white balance will not change as the scene or the light source varies. Therefore, users might have to re-adjust the white balance by clicking the <Push> button again when needed.

Smart Touch Mode

With Smart Touch function, users can select an area in the camera scene as the reference point for white balance. Please ensure that the background color of the selected area is white. Smart Touch function is suitable for environments with

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

unchanged brightness level. Click the <Push> button to adjust the color tone of the live images.

Manual Mode

In this mode, users can manually adjust the White Balance value. Input a number between 0 to 249 for “Rgain / Bgain” to adjust the red / blue illuminant on the Live Video Pane. The following describes several situations that might occur during the White Balance manual adjustment.

Click on <Set>to confirm the setting.

- The video image turns reddish (as the left picture below).
  The higher the Rgain value, the redder the image will be. To solve the problem, reduce the Rgain value, and the video image will turn less reddish.


Reddish Image


Corrected White Balance

- The video image turns greenish (as the left picture below).
  The lower the Rgain value, the greener the image will be. To solve the problem, Increase the Rgain value, and the video image will turn less greenish.


Greenish Image


Corrected White Balance

- The video image turns bluish (as the left picture below).

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

The higher the Bgain value, the bluer the image will be. To solve the problem, reduce the Bgain value, and the video image will turn less bluish.

Bluish Image

Corrected White Balance

- The video image turns yellowish (as the left picture below).
  The lower the Bgain value, the yellower the image will be. To solve the problem, Increase the Bgain value, and the video image will turn less yellowish.

Yellowish Image

Corrected White Balance

The following image displays the general color shifts of the scene when different Rgain / Bgain combinations are applied.

3.6.4 Picture Adjustment

The Picture Adjustment setting can be found under this path: **Camera> Picture Adjustment**.

Brightness
The brightness level of the images is adjustable from -12 to +13. The default value is 0.

Sharpness
The sharpness level of the images is adjustable from +0 to +15. The edge of the objects is enhanced as the sharpness level increases. The default value is +4.

Contrast
The contrast level of the images is adjustable from -6 to +19. The default value is 0.

Saturation
The saturation level of the images is adjustable from -6 to +19. The default value is 0.

Hue

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

The hue level of the images is adjustable from -12 to +13. The default value is 0.

3.6.5 Auto Focus

The Auto Focus setting can be found under this path: **Camera> Auto Focus**.

Users can adjust auto focus performance by choosing Auto Focus with PTZ or zoom box cameras, which are equipped with high-ratio zoom lenses. If users wish to use manual focus, they can make adjustments using the auto focus mode or select the <Manual> button from the live view pane.

Method

- **Gen 2**
  The Gen2 provides stable focusing performance, allowing the image to be focused efficiently in most circumstances.

Mode

- **Auto**
  The camera will keep in focus automatically and continuously regardless of zoom changes or any view changes. Please refer to Function Items on Home Page> Manual Focus Adjustment> Manual / Auto for further details.

- **Manual**
  User can manually adjust the focus by clicking Near / Far button. Please refer to Function Items on Home Page> Manual Focus Adjustment> Near / Far for further details.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Zoom Tracking

- **On**
  Select “On” to enable continuous focus adjustment during the zooming process.

- **Off**
  Select “Off”, the focus will keep current focus position during the zooming process.

3.6.6 Day/Night Mode

The Day/Night Mode setting can be found under this path: **Camera> Day/Night Mode**.

NOTE: This function is **ONLY** available for models with IR function.

Day/Night Function

This item is for users to define the action of the IR cut filter and IR LED lights. Refer to the descriptions of each option below to select a suitable mode.

- **Auto Mode**
  With this mode, the camera can decide the occasion to remove the IR cut filter. Please refer to IR Function: Day/Night Threshold for further details.

- **Night Mode**
  Use this mode when the environment light level is low. The IR cut filter will be removed to allow the camera to deliver clear images in black and white.

- **Day Mode**
  Select this mode to turn on the IR cut filter. The IR cut filter can filter out the IR light and allows the camera to deliver high quality images in color.

Day/Night Threshold

This item is for users to set when the camera should switch from day mode to night mode or vice versa. The camera will sense the surrounding brightness, and the threshold value stands for the level of the light. Once the camera detects the

light level reaches the set threshold, the camera will automatically switch to Day/Night Mode. The range of the level is from 0 to 10, (darker = 0; brighter = 10).

- **Night back to Day**
  The lower the value, the earlier the camera switches to Day mode. The default value is 7.

- **Day into Night**
  The higher the value, the earlier the camera switches to Night mode. The default value is 3.

NOTE: Equipped with different CMOS sensors, the time the camera switches to Day/Night mode may also vary according to different camera models even if the threshold is set to the same value.

Adaptive IR

With the IR Light Compensation function, the camera can prevent the center object close to the camera from being too bright when IR LED lights are turned on.

IR Heating (PTZ Only)

IR heating function is provided for cameras installed under icy and humid environment. Please select “Disabled”, “Colder” and “Warmer” from the drop-down menu to avoid possible ice up on the surface. The IR heating starts at a higher ambient temperature in “warmer” mode than in “colder” mode.

3.6.7 Illumination

The Illumination setting can be found under this path: **Camera> Illumination**.

Mode

Select the Illumination mode, <Synchronize>, <Manual On>, and <Manual Off>, to turn on/off the IR LED light. This function is only available for cameras with LED function.

- **Synchronize**
  With this mode, the camera can decide the occasion to turn on or turn off the IR LED light.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

- **Manual On**
  Use this mode to turn on the IR LED light manually.

- **Manual Off**
  Use this mode to turn of the IR LED light manually.

3.6.8 Noise Reduction

The Noise Reduction setting can be found under this path: **Camera> Noise Reduction**.

The camera provides multiple <Noise Reduction> options for delivering optimized image quality especially in extra low-light conditions.

3DNR
3DNR (3D Noise Reduction) function delivers optimized image quality especially in extra low-light conditions.

Different levels of 3DNR are provided, including 3DNR Low, 3DNR Mid and 3DNR High. Higher level of 3DNR generates relatively enhanced noise reduction.

2DNR
2DNR (2D Noise Reduction) function delivers clear images without motion blurs in extra low-light conditions.

Select <on> to turn on 2DNR function; otherwise, select <off> to turn off 2DNR function.

ColorNR
In a dark or insufficient light environment and the camera is under color mode, ColorNR (Color Noise Reduction) can eliminate color noise.

Three levels of ColorNR, including Color Low, Color Mid and Color High, are provided. The higher level of ColorNR generates relatively enhanced noise reduction.

3.6.9 HDR

The HDR setting can be found under this path: **Camera> HDR**.

Shutter ratio

Shutter ratio refers to the ratio between the longest exposure and the shortest exposure. This function is **NOT** available for PTZ Cameras.

- **Auto**
  Auto mode can automatically alter the shutter ratio to solve the problem of changing light in the environment. It is recommended to select this mode when the light of the environment change dynamically.

- **Fixed**
  The shutter ratio would be fixed when users select this mode.

NOTE: This function is **ONLY** available when TV system is set as HDR 2x shutter.

Gamma HDR

The Gamma HDR function is for solving high contrast or changing light issues. Different level options for Gamma HDR include Low, Mid, High and Auto. Users can select the most suitable Gamma HDR mode based on the brightness of operating environment. Note that image noise could be visible when this function is turned on.

NOTE: Auto mode of Gamma HDR function is **NOT** available when (1) TV system is set as Linear mode or (2) TV system is set as HDR mode and the Shutter ratio option under HDR Type is set as Fixed.

Low light performance

Image noise would become clearly visible when the light is weak and gain value is high. With this function, users can select the best mode based on the operating environment to minimize image noise. Refer to the descriptions of each option below to select a suitable mode.

- **HDR**
  It is recommended to select this mode when the environmental illumination is not low and the effect of the HDR would like to be retained.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

- **Linear**
  Linear mode would minimize image noise in low light conditions. It is recommended to select this mode when users want to reduce image noise in dimly-lit environment.

NOTE: This function is **ONLY** available when TV system is set as HDR 2x shutter.

3.6.10 Image Stabilizer

The Image Stabilizer setting can be found under this path: **Camera> Image Stabilizer**.

With the Image Stabilizer function, the camera can keep the image steady and suppress vibrating effects on images caused by external vibration. Select <On> from the “EIS” drop-down list to enable the Image Stabilizer function. This function is only available on PTZ cameras or cameras equipped with high zoom lenses, as specified by the customer.

3.6.11 Digital Zoom

The Digital Zoom setting can be found under this path: **Camera> Digital Zoom**.

The digital zoom of the camera is adjustable from x2 to x10 (for Zoom Lens is x2 to x12).

NOTE: This function is **NOT** available for Fisheye IP Camera models.

3.6.12 Backlight

The Backlight setting can be found under this path: **Camera> Backlight**.

The Backlight Compensation function prevents the center object from being too dark in surroundings where excessive light is behind the center object. Select <on> to turn on the function; otherwise, select <off> to turn off the function.

NOTE: Backlight function is **NOT** available when (1) “Window Setting” function from Exposure Mode is enabled or (2) TV system is set as “HDR 2x Shutter”.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

3.6.13 User Setting Profile

The User Setting Profile setting can be found under this path: **Camera> User Setting Profile**.

Camera Profile allows users to setup the desired image parameters for specific environments with different time schedules. Users can setup at most 10 sets of camera parameter configuration under the Camera tab. To enable this function, users must setup the schedules in advance. Refer to section System> Schedule Profile for further details of schedule setup. Then, follow the steps below to setup a camera profile.

Select Profile Number

Step 1: In the “Camera” tab, setup the camera parameters, such as White Balance, Picture Adjustment, etc., excluding TV System.

Step 2: Click on User Setting Profile and its setting menu will be displayed. Select a number from the Num drop-down menu.

Step 3: Input a name for the profile in the Name field.

Step 4: Tick and check the desired schedule(s) from the Schedule drop-down menu. Multiple schedules can be applied to one profile.

Step 5: Click on <Save> to confirm the setting.

Step 6: Follow the steps above to set the rest of the profiles.

Now, the camera will automatically switch profiles according to the schedule. Alternatively, manually select a number from the Num drop-down menu. Then, click on <Go>, the camera will load and applied the setting of the profile.

NOTE: If users wish to set the camera parameters to factory default setting, select <OFF> from the Num drop-down menu. The camera will start loading the default values.

NOTE: If there are gaps between schedules, the camera will apply the most recent settings configured by the user.

3.6.14 TV System

The TV System setting can be found under this path: **Camera> TV System**.

Select the video format that matches the present TV system from the drop-down menu. The following table shows the available video formats for different types of models. The supported video formats for each model are marked by “v”.

Model / Video Format		Fisheye	Others
NTSC	60 fps	v	v
	HDR 2x Shutter	-	v
PAL	50 fps	v	v
	HDR 2x Shutter	-	v

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

3.7 Pan Tilt

Under the tab <**Pan Tilt**>, there are submenus including: <Preset>, <Sequence> and <Pan/Tilt Control>.

NOTE: Pan Tilt function is only available for camera models with RS-485.

With RS-485 support, the camera is capable of working with a Pan Tilt Head for pan and tilt control. Before implementing pan/tilt control, please ensure the Pan & Tilt Head is correctly connected to the camera's RS-485 port.

Pin Definition for Camera's RS-485 Port

The pin definition may vary according to different camera models, please refer to Quick Guide for more details.

3.7.1 Preset

The Preset setting can be found under this path: **Pan Tilt> Preset**.

NOTE: Before setting this function, users must enable the Pan/Tilt Control first. Please refer to section Pan Tilt> Pan/Tilt Control for more details.

A preset position is a predefined viewpoint that allows for quick navigation of the camera to a specific location. There are up to 256 preset points that can be set in the Preset setup page. Please follow the steps below to set and run preset points.

Setting

Follow the steps to setup a Preset Point.

Step 1: Move the cursor to the live view pane.

Step 2: Left click and drag the yellow arrow to a desired position and adjust the zoom / focus ratio.

Step 3: Assign a number for the current position from "Positions", and enter its descriptive name.

Step 4: Click the <Save> button to save the settings, click the <Clear> button to delete the settings, and click the <Go> button to display the save settings.

Go

To have the camera move to a specified preset position, please select the Preset Point from the drop-down Preset list. Then the camera shall move to the target position.

3.7.2 Sequence

The Sequence setting can be found under this path: **Pan Tilt> Sequence**.

The Sequence function allows users to predefine preset points along a path, along with their dwell time and speed. By combining all the presets, users can create a desired viewing route. The camera supports a total of 8 Sequence Lines; each Sequence Line consists of up to 64 Preset Points. Please refer to the instructions below to program a Sequence Line.

NOTE: Before setting this function, users must pre-define at least two Preset Points.

Setting

Follow the steps to setup a Sequence Path.

Step 1: Select a path number from the “Select Sequence Path” drop-down list.

Step 2: Setup each Preset Point of the programmed Sequence Line in order.

Step 3: Select a Preset Point from the <Preset Name> drop-down list for the specified number of Preset Point after setup from “Preset”.

Step 4: Enter both Dwell Time (0 to 127) and Speed (0 to 14) into the corresponding fields.

Step 5: Click the <Set> button to save the setting, or click “Clear” to delete the setting.

Step 6: Click the <Go> button to display the save settings.

Run

Select the specified Sequence Line from the “Run” drop-down list and then the camera will start moving forward each scene sequentially as programmed.

To view the camera executing a Sequence Line in full screen mode, please move the cursor onto the live view pane, please click <Max Window> from the bottom right to active “full screen”. Then users can view the camera navigation in full screen.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

To stop running the Sequence Line, simply move the cursor to the live view pane and move the camera in any direction.

3.7.3 Pan/Tilt Control

The Pan/Tilt Control setting can be found under this path: **Pan Tilt> Pan/Tilt Control**.

This page is for users to activate the pan/tilt function and select the RS-485 protocol which the Pan Tilt Head uses.

Pan/Tilt Control
This item allows users to disable or enable the Pan/Tilt Control.

RS-485 Protocol Type
With the correct RS-485 protocol selected, users will be able to remotely control the Pan Tilt Head from the web browser or the backend software. Check the RS-485 protocol type of the Pan Tilt Head. Then select the RS-485 protocol which the Pan Tilt Head uses from the drop-down menu. The available types are DSCP / PelcoD / PelcoP / Universal. Please refer to the following descriptions. After the protocol type is selected, users can adjust the parameters from the drop-down menus on the right. Click <Set> to confirm the setting.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

- **DSCP / PelcoD / PelcoP:**
  With these protocols, users can control the Pan Tilt Head from the web browser. Users can use the mouse to pan/tilt, set preset points and set sequence lines. To pan/tilt the Pan Tilt Head, click and drag the mouse in the live video window at the home page. To set preset points and sequence lines, please refer to sections Preset and Sequence. Users can also type API (Application Programming Interface) commands at the URL bar of the web browser interface to control the Pan Tilt Head.

- **Universal:**
  Universal protocol covers functions that are not provided by the protocols listed above. Users can control the Pan Tilt Head by entering the API command of the Universal protocol at the URL bar of the web browser.

NOTE: For API commands, please contact TKH Security support team.

Click on <Set> to confirm the setting.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

3.8 PTZ

Under the tab <**PTZ**>, there are categories including: <Preset>, <Cruise>, <Auto Pan>, <Sequence>, <Home Function>, <Tilt Range>, <PTZ Setting> and <RS485>.

NOTE: PTZ function is only available for PTZ Cameras.

3.8.1 Preset

The Preset setting can be found under this path: **PTZ> Preset**.

A preset position is a predefined viewpoint that allows for quick navigation of the camera to a specific location. Users can change the camera direction by selecting the configured preset from the drop-down menu under “Run” in PTZ> Preset, or live view pane under “Go Preset”. Please refer to the section Function Items on the Home Page> Go Preset / Run Sequence / Run Cruise for further details. The camera supports up to 256 Preset Points. Please refer to the instructions below to set a Preset Point.

Setting
Follow the steps to setup a Preset Point.

Step 1: Move the cursor to the live view pane.

Step 2: Left click and drag the yellow arrow with the PTZ controls to a desired position and adjust the zoom / focus ratio.

Step 3: Assign a number for the current position from “Positions”, and enter its descriptive name.

Step 4: Click the <Save> button to save the settings, click the <Clear> button to delete the settings, and click the <Go> button to display the save settings.

Go
To have the camera move to a specified preset position, please select the Preset Point from the drop-down Preset list. Then the camera shall move to the target position.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

3.8.2 Cruise

The Cruise setting can be found under this path: **PTZ> Cruise**.

The Cruise function allows users to set up desired viewing routes in advance. Users can change the camera's path by selecting the configured cruise from the drop-down menu under “Run” in PTZ> Cruise, or live view pane under “Run Cruise”. Please refer to the section Function Items on the Home Page> Go Preset / Run Sequence / Run Cruise for further details. The camera supports up to 8 Cruise Paths. Please follow the instructions below for Cruise Path setup.

Setting
Refer to the steps below to setup a Cruise Path.

Step 1: Select a path number from the “Select Cruise Path” drop-down list.

Step 2: Move the cursor to the live view pane, and move the camera to a desired view (PTZ controls) as the start point of a Cruise Path.

Step 3: Click the <Start> button of <Record Cruise Path Start> and start programming the Cruise Path via PTZ controls.

Step 4: When finishing programming, click the <End> button of <Record Cruise Path End> to complete recording the Cruise Path.

Step 5: Click the <Go> button to display the save settings.

Run
Select the specified Cruise Path from the drop-down list and then the camera will start touring around as recorded.

To view the camera touring in full screen mode, please move the cursor onto the live view pane, please click <Max Window> from the bottom right to active “full screen”. Then users can view the camera navigation in full screen.

To stop running a Cruise Path, simply move the cursor to the live view pane and move the camera in any direction.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

3.8.3 Auto Pan

The Auto Pan setting can be found under this path: **PTZ> Auto Pan**.

The Auto Pan function allows users to predefine desired panning routes. Users can change the camera's pan path by selecting the configured auto pan from the drop-down menu under "Run" in PTZ> Auto Pan. The camera supports 4 Auto Pan Paths. Please refer to the instructions below to set an Auto Pan Path.

Setting

Follow the steps to setup an Auto Pan Path.

Step 1: Select a path number from the “Select Auto Pan Path” drop-down list.

Step 2: Select the speed ratio from the <Speed> drop-down list; the speed ratio ranges from 0 (low) to 3 (fast).

Step 3: Choose to run the Auto Pan Path in right / left direction from the <Direction> drop-down list.

Step 4: Move the cursor to the live view pane, and move the camera to a desired view as the Start Point of an Auto Pan Path.

Step 5: Click the <Set> button of <Assign Start Position> and the current view will be automatically saved as the start point of the Auto Pan Path.

Step 6: Move the camera to another desired position as the end point of the Auto Pan Path.

Step 7: Click the <Set> button of <Assign End Position> to save the setting.

Step 8: Click the <Go> button to display the save settings.

NOTE: The zoom ratio and tilt angle of an Auto Pan’s Start Point remains the same throughout the path.

Run

Select the specified Auto Pan Path from the drop-down list and the camera will start moving horizontally as recorded.

To view the camera panning in full screen mode, please move the cursor onto the live view pane, please click <Max Window> from the bottom right to active “full screen”. Then users can view the camera navigation in full screen.

To stop running an Auto Pan Path, simply move the cursor to the live view pane and move the camera in any direction.

3.8.4 Sequence

The Sequence setting can be found under this path: **PTZ> Sequence**.

The Sequence function allows users to predefine preset points along a path, along with their dwell time and speed. By combining all the presets, users can create a desired viewing route. Users can change the camera's path by selecting the configured sequence from the drop-down menu under “Run” in PTZ> Sequence, or live view pane under “Run Sequence”. Please refer to the section Function Items on the Home Page> Go Preset / Run Sequence / Run Cruise for further details. The camera supports a total of 8 Sequence Lines; each Sequence Line consists of up to 64 Preset Points. Please refer to the instructions below to program a Sequence Line.

Setting

Follow the steps to setup a Sequence Path.

Step 1: Select a path number from the “Select Sequence Path” drop-down list.

Step 2: Setup each Preset Point of the programmed Sequence Line in order.

Step 3: Select a Preset Point from the <Preset Name> drop-down list for the specified number of Preset Point after setup from “Preset”.

Step 4: Enter both Dwell Time (0 to 127) and Speed (0 to 14) into the corresponding fields.

Step 5: Click the <Set> button to save the setting, or click “Clear” to delete the setting.

Step 6: Click the <Go> button to display the save settings.

Run

Select the specified Sequence Line from the “Run” drop-down list and then the camera will start moving forward each scene sequentially as programmed.

To view the camera executing a Sequence Line in full screen mode, please move the cursor onto the live view pane, please click <Max Window> from the bottom right to active “full screen”. Then users can view the camera navigation in full screen.

To stop running the Sequence Line, simply move the cursor to the live view pane and move the camera in any direction.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

3.8.5 Home Function

The Home Function setting can be found under this path: **PTZ> Home Function**.

Home Function allows users to set an operation mode to ensure constant monitoring. If the camera idles for a period of time, the selected function will be activated automatically. The Home function allows constant and accurate monitoring to avoid the camera idling or missing events.

On/Off
Select <On> or <Off> to activate or disable the Home Function Setting.

Operation Idle Time to Return Home
The time here represents the duration of camera idle time previous to running a Preset Position / Auto Pan Path / Sequence Path / Cruise Path. When the Home function is activated, the camera will start to count down when it idles, and then execute the predefined action as time expires. The time period ranges from 1 min. to 128 min.; specify it in the field. Click the <Set> button to save the settings.

Home Position Type
Select a Home action type (Preset Position / Auto Pan Path / Sequence Path / Cruise Path) and specify the number of Preset Position / Auto Pan Path / Sequence Path / Cruise Path from the drop-down lists. Click the <Set> button to save the Home settings.

3.8.6 Tilt Range

The Tilt Range setting can be found under this path: **PTZ> Tilt Range**.

The tilt angle will vary based on the image flip settings. Please refer to PTZ Setting> Image Flip for more settings.

Users can enter desired minimum and maximum tilt angle into the corresponding fields respectively to configure the tilt range of the camera. Following table lists the available minimum and maximum tilt angle range for different camera models.

Model	Minimum Tilt Angle	Maximum Tilt Angle	
		Image Flip Off/ M.E.	Image Flip Digital
PD950DC	-10° to 10°	80° to 100°	170° to 190°
PD950NW	-20° to 10°	80° to 100°	170° to 200°
PD950, PD980	-20° to 10°	80° to 100°	-

Click on <Set> to save the tilt range settings.

3.8.7 PTZ Setting

The PTZ Setting can be found under this path: **PTZ> PTZ Setting**.

Image Flip
With Flip function turned on, users can track an object continuously when it passes under the camera.

NOTE: If a Preset Position or Cruise Path can only be reached through Flip motion, the position and path cannot be reached anymore once the Flip function is turned off.

NOTE: The Digital function is not available for 851 model PTZ camera with wiper.

- **Mechanical**
  As the camera tilts to the maximum angle, it will pan 180°, and then continue tilting to keep tracking objects.

- **Digital**

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Image Flip works when camera tilt angle reaches 90°. The image will be rotated 180°, and then continue tilting to keep tracking objects.

NOTE: The Image Flip Digital function is not available for PTZ Cameras with wiper.

Select “Off” to disable the Image Flip function.

Speed by Zoom

This function allows the camera to adjust the pan/tilt speed automatically by the internal algorithm when the zoom ratio is changed. The rotating speed will become slower as the zoom ratio gets larger.

Auto Calibration

Integrating Servo Feedback technology, the camera would calibrate and precisely return to the previous position without stalling when the deviation of dome pivot is detected.

Set Pan 0 Degrees

Click on the <Set> button to set the camera’s currently shooting position as the start point for panning (0 degree).

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

3.9 Logout

Click on the tab <Logout > on the top of the page, and the login window will popup. This enables login with another username.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

4 Cyber security

This chapter aims to be a practical guideline for how to implement the general and sometimes abstract advice found in the Security hardening guide on the TKH Security web site.
To download this hardening guide, browse to tkhsecurity.com> Products> Surveillance cameras> (any camera)> Links and Downloads> Security hardening guide.
At the time of writing, the direct download link for the Security hardening guide is: https://tkhs-install-files.s3.eu-central-1.amazonaws.com/Siqura/Manuals/TKH+Security_hardening_guide.pdf

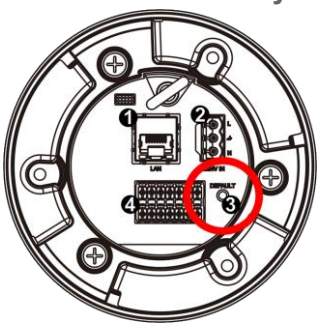
Use this chapter to find the practical steps you can take to make your camera more secure.

4.1 Camera

4.1.1 Factory Default

Before installing make sure that the camera is in its factory default state.
If in doubt, force the camera to its factory defaults again.

Reset the camera by hardware reset button:



Press the button with a proper tool for at least 20 seconds to restore the system.

Reset the camera by web page access:
Refer to section 3.2.11.2.

Reset the camera by using the SDM2 Device Manager software:

1. Connect to the camera, such that it is Online
2. Right-click on the camera to show the device context menu
3. From this menu, select Tools> Factory defaults:

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

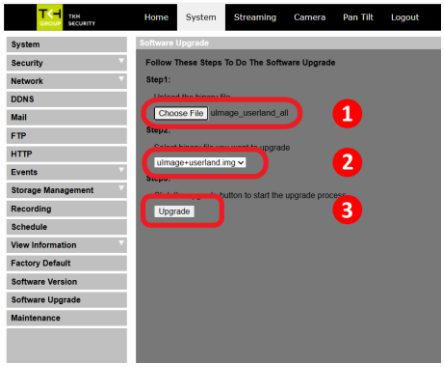
4. In the Factory defaults dialog, select the way of resetting and click OK.

4.1.2Firmware update

Update the camera firmware to the latest version available from TKH Security. Regularly check for updates to ensure the device is protected against the latest vulnerabilities.

Update the camera firmware via the camera web page:

1. Download the zip file from the TKH Security web site. The latest firmwares can be found here: https://tkhsecurity.atlassian.net/wiki/spaces/KB/pages/1169195040/Camera+firmware
2. Unpack the zip file, you will have a folder that includes a file named “UpgradeRules.ini”, and a “bin” folder containing the actual firmware files.
3. Open the camera’s web page in your browser, login as administrator, and navigate to System> Software Upgrade:



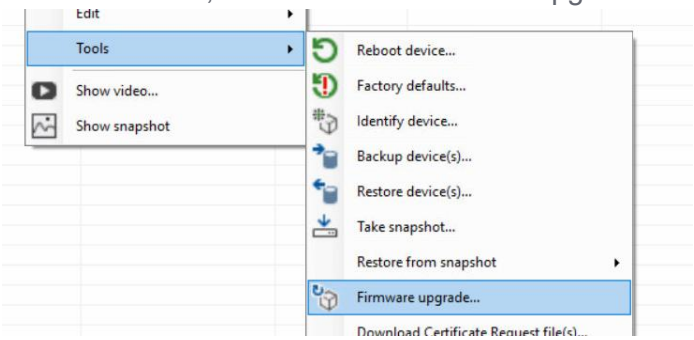
4. Click on Choose File and select file “uImage_userland_all” in the firmware “bin” folder.
5. Make sure that the firmware type combo has the “uImage+userland” item selected.
6. Click on Upgrade. You will see a progress bar running until it is full, then the page will refresh.
7. Click on Choose File and select file “uImage_userland_all_TKH” in the firmware “bin” folder.
8. Make sure that the firmware type combo has the “uImage+userland” item selected.
9. Click on Upgrade. You will see a progress bar running until it is full, then the page will refresh.
10. Navigate to System> Software version and validate that the shown firmware version is correct.
11. If you downgraded the firmware to an older version, you may need to reset the camera to factory defaults. Newer firmware is kept backwards compatible, but this guarantee is not given for downgrading back to an older version.
12. Also refer to section 3.2.11.1.

Update the firmware with the SDM2 Device Manager software:

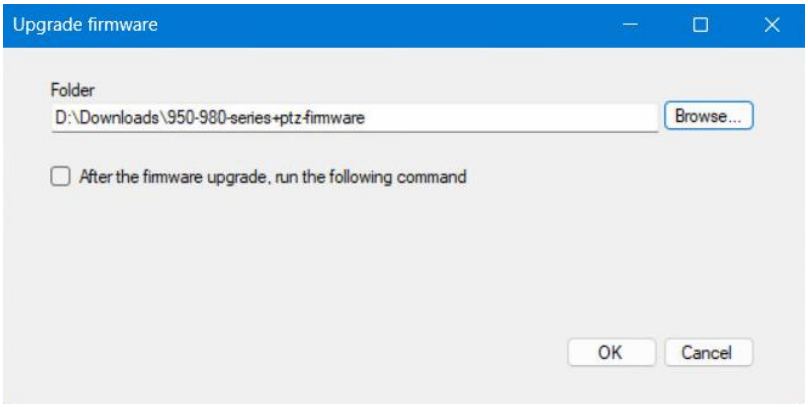
1. Connect to the camera, such that it is Online
2. Right-click on the camera to show the device context menu

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

3. From this menu, select Tools> Firmware upgrade:



4. In the Firmware upgrade dialog, select the right folder location:



   Make sure that you select the location of the folder that includes a file named “UpgradeRules.ini”.
5. Click OK to start the firmware upgrade. The camera may reboot several times, and this operation may take a long time to complete.
6. After the firmware upgrade is finished, a dialog appears with the result, which should be OK. You can save the log file from this dialog by clicking on the Log button.

4.1.3Strong password

The administrator password should be unique and as strong as possible (minimum of 8 characters with a mix of letters, numbers, and symbols).
It is recommended to avoid subsequent series such as 1234, 555, or abcd, or the use of existing words.
Generally, the best random passwords are generated by using a password generator tool.

When unpacking the camera and connecting to it for the first time, the camera will be accessible via its default IP address which is found on the product sticker as well as on the product box. This address should be a 10.x.y.z address with subnet mask 255.0.0.0. It would be best if you set your computer’s network adapter in this network range, to that you can directly open this camera’s web page in the browser.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

When you show the camera web page for the first time, it will ask you to enter and re-enter a new administrator password of your choice. Make sure that you enter a password that will:

1. Have at least 8 characters as length
2. Contain at least one uppercase letter
3. Contain at least one lowercase letter
4. Contain at least one special character (valid are "**!#$%&'-.@^_~**" excluding the quotes)
5. Avoid mentioning the username. Such as "Admin1234"
6. Avoid using series, such as "123", "bbb"

Also refer to section 3.2.3.

When adding another user, make sure that this user's password will be set using the same rules and best practices.

4.1.4Change password regularly

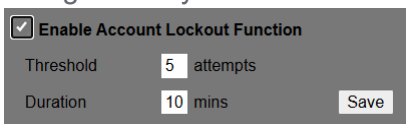
Change your passwords regularly. The best practice is to change the passwords every 90 days.

4.1.5Authentication lockout

Enable the account lockout policies after a defined number of failed login attempts to protect against brute-force attacks.

To do this via the camera web page:

1. Open the camera web page in your browser and login as administrator
2. Navigate to System> User:



3. Make sure that the Enable Account Lockout Function checkbox is checked;
4. Set the Threshold value to the desired number of attempts, the default is 5x.
5. Set the Duration value to the desired lockout time, the default is 10 minutes.
6. Click on the Save button.

4.1.6User accounts with least privileges

Assign user roles with the principle of least privileges. Limit administrative access to only those who need it.
VMS clients, support engineers or operators may access the camera as "Operator" or "Viewer". Be aware that some VMS clients require "administrator" access.

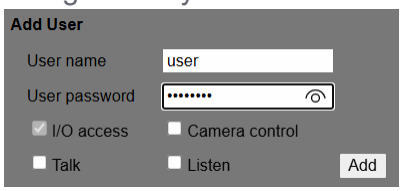
As a general guideline, following principle roles exist (not limited to):

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

- Administrator: full control of all camera features and functions
- Supervisors: full control except for user management and restoring factory defaults
- Operators: access to view cameras, control PTZ
- Viewers: access to view cameras

To do this via the camera web page:

1. Open the camera web page in your browser and login as administrator
2. Navigate to System> User:



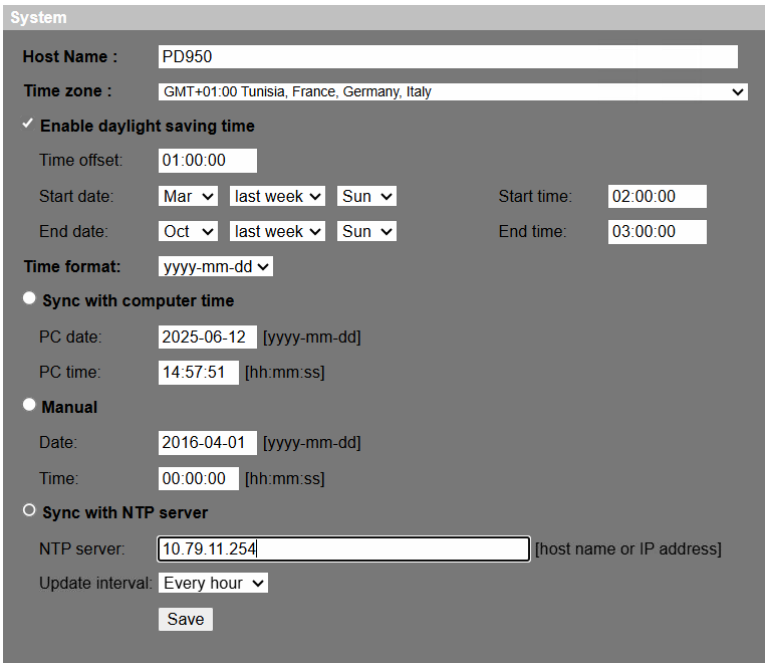
3. The shown rights are the least privileges you can assign to this new user. Only assign the desired rights if these are actually needed for this user.

4.1.7Time synchronization

Use a single time provisioning source, and configure the camera to synchronize against this single time source regularly.

To do this via the camera web page:

1. Open the camera web page in your browser and login as administrator
2. Navigate to System> System:



3. Make sure that the Time zone / Date and Time / Daylight Saving Time settings are set to the correct values.
4. Check the Sync with NTP server radio button
5. Enter the appropriate NTP server's IP address or hostname in the NTP Server text box.
6. Make sure that the Update interval value is set to the desired interval.
7. Click on the Save button.

Also refer to section 3.2.2.

4.1.8Disable unused protocols

Turn off unnecessary network protocols such as Telnet and FTP to reduce the attack surface.
Only keep those protocols enabled that are used, and document these.
Do not use SNMPv1, SNMPv2, TLSv1.0, TLSv1.1, UPnP, Telnet, FTP, Basic authentication, Bonjour, DDNS.
Whenever these protocols are used during installation, make sure that these are disabled upon completion of the work.

To do this via the camera web page:

1. Open the camera web page in your browser and login as administrator
2. Navigate to System> Network> Basic
3. Uncheck the Enable IPv6 checkbox, if you will not be using IPv6; click Save to confirm
4. Navigate to System> Network> SNMP
5. Uncheck the Enable SNMP v1 checkbox, and/or Enable SNMP v2 checkbox, and/or Enable SNMP v3 checkbox, such that only those checkboxes are checked for those versions you will actually be using.
6. Navigate to System> Network> UPnP
7. Uncheck the Enable UPnP checkbox, if you will not be using UPnP
8. Navigate to System> Network> Diamond Protocol
9. Check only those check boxes if you will be using the corresponding Diamond Protocol mechanism.
10. Navigate to System> Network> PelcoD Protocol
11. Check only those check boxes if you will be using the corresponding PelcoD Protocol mechanism. Note that this will not affect the possible RS485 function of the camera.
12. Navigate to System> Network> TACACS+
13. Set the TACACS+ Enabled combo box to "no", if you will not be using the TACACS+ protocol.
14. Navigate to System> DDNS
15. Uncheck the Enable DDNS checkbox, if you will not be using the camera's DDNS function.
16. Navigate to System> Mail
17. Clear the (1st and 2nd) SMTP (mail) server input fields, if you will not be using the camera's mailing function.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

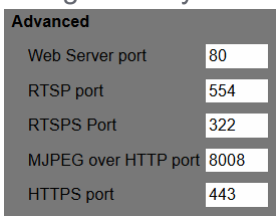
18. Navigate to System> FTP
19. Clear the (1st and 2nd) FTP server input fields, if you will not be using the camera's FTP notification function
20. Navigate to System> HTTP
21. Clear the (1st and 2nd) HTTP server input fields, if you will not be using the camera's HTTP notification function

4.1.9Change the default ports

It is recommended to change the service default ports (like HTTP-80, HTTPS-443, etc.) to reduce the risk of outsiders being able to access.

To do this via the camera web page:

1. Open the camera web page in your browser and login as administrator
2. Navigate to System> Network> Basic



3. Alter the shown ports to the desired different port settings, diverting from the defaults shown in the above screenshot.
4. Note: after you alter these settings, you will need to explicitly mention the port number in your client application, since the client would otherwise attempt to use the default port.

4.1.10 Review Settings

Regularly review and adjust camera settings to enhance security.

4.1.11 Audio input

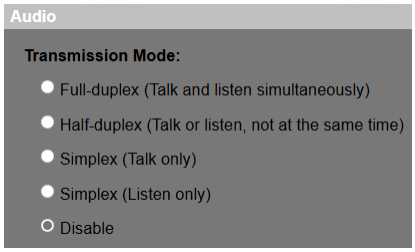
Disable the audio feature of the camera if this is not used.

To do this via the camera web page:

1. Open the camera web page in your browser and login as administrator

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

2. Navigate to Streaming> Audio



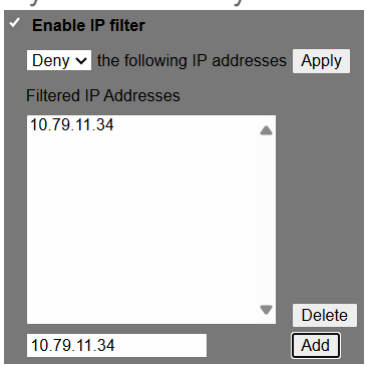
3. Select the Disable radio button, if you will not be using the camera's audio function.

4.1.12 IP filtering

Use black and white list to filter the IP address. This will prevent everyone, except those specified IP addresses from accessing the system.

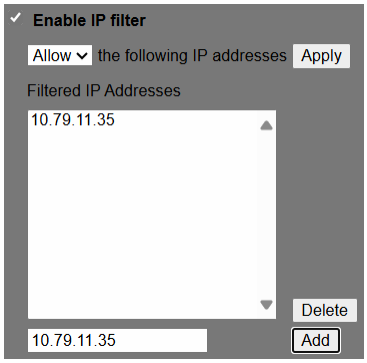
To do this via the camera web page:

1. Open the camera web page in your browser and login as administrator
2. Navigate to System> Security> IP Filter
3. Check the Enable IP Filter checkbox
4. If you wish to deny access to selected hosts, use the blacklilst mode:



Here, all hosts are allowed except 10.79.11.34 which is blocked.

5. If you wish to allow access only to selected hosts, use the whitelist mode:



Here, only host 10.79.11.35 has access, all other hosts are blocked.
Be cautious with this white list function, making sure that you will not lock yourself out.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

4.1.13 Session logout

Inactive users will be logged out after a set period.

Note that this camera does not support the Session lockout security function.

4.1.14 SD card encryption (securing local recording)

If the camera supports encryption of the recordings then it is highly recommended to use/enable this function.

Note that this camera does not support the encryption of SD cards.

4.1.15 Physical Security

Ensure cameras are physically secured to prevent tampering or unauthorized access. This includes using tamper-resistant mounts and enclosures.

4.2 Network

4.2.1 Network segmentation

Place security cameras on a dedicated VLAN separate from the main network. This minimizes the risk of cross-network infections or attacks.

4.2.2 Controlled access to the network

Use a Virtual Private Network (VPN) for remote access to the camera system.
Do not expose to the public network or the Internet.

4.2.3 Set the router firewall

It is recommended to set the firewall of your router.
Note that some important ports cannot be closed (like HTTP port, HTTPS port, Data Port).

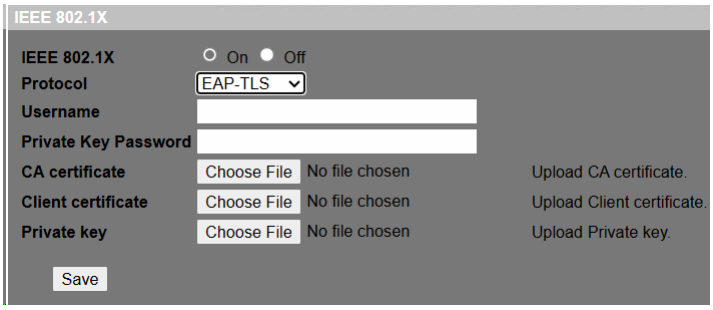
4.2.4 Port authentication (802.1x)

Make use of network access control using IEEE 802.1x with at least EAP-TLS (MD5 is listed as a vulnerability). Use the safely stored private key that is generated by the camera itself to request a CA client certificate.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

To do this via the camera web page:

1. Open the camera web page in your browser and login as administrator
2. Navigate to System> Security> IEEE 802.1x



3. Enable the IEEE 802.1x On radio button to show the complementary fields.
4. Select the EAP-TLS protocol.
5. The remaining details will need to be acquired via the network or system administrator.

Refer also to section 3.2.6.3.

4.2.5Multicast

Avoid the use of multicast in an open accessible network. It is very easy to eavesdrop on multicast streams.

This is a system wide discipline that cannot be enabled or disabled by the camera. The camera's multicast functionality is always available for use by the system, and it will be possible to slightly modify the camera's behaviour to assist the system's multicast functional behavior. However, using or avoiding the use of multicast in the system is principally a system wide commissioning choice.

4.3 Data Security

4.3.1SSL/TLS versions

TLS versions 1.0 and 1.1 are not to be used. They accept simple encryptions schemes that are hacked. The current TLS version is TLSv1.3.

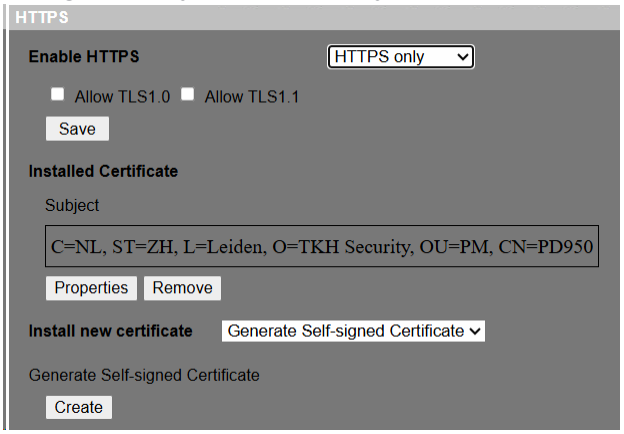
The camera supports TLV v1.2 as well as v1.3, both for HTTPS and for 802.1x.

To do this for HTTPS via the camera web page:

1. Open the camera web page in your browser and login as administrator

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

2. Navigate to System> Security> HTTPS



3. Make sure that the Enable HTTPS combo box has “HTTPS only” selected.
4. Make sure that Allow TLS1.0 and TLS1.1 checkboxes are unchecked.
5. Click on Save to save the above settings.
6. The above screenshot shows a self-signed certificate is installed. To have an official CA issued certificate, contact the system or network administrator.

To do this for 802.1x port authentication via the camera web page:

1. Follow the instructions noted in section 4.2.4, Port authentication (802.1x).

4.3.2HTTP authentication

Select digest authentication for HTTP. It encrypts the passwords over the network.
Basic authentication is considered unsafe, as it transmits the password in plain text over the network.

To do this via the camera web page:

1. Open the camera web page in your browser and login as administrator
2. Navigate to System> Security> User

3. Make sure that the Type combo box has “digest” selected.
4. Click the Save button

4.3.3RTSP authentication

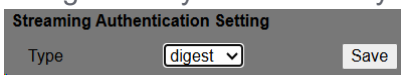
Using Digest Authentication with RTSP makes the video stream only accessible when you have the proper credentials. Digest Authentication should be chosen over the unsafe Basic Authentication.

To do this via the camera web page:

1. Open the camera web page in your browser and login as administrator

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

2. Navigate to System> Security> User



3. Make sure that the Type combo box has “digest” selected.
4. Click the Save button

4.3.4HTTPS

Enable HTTPS for accessing the camera’s web interface to ensure that data transmitted between the camera and the user is encrypted.

To do this via the camera web page:

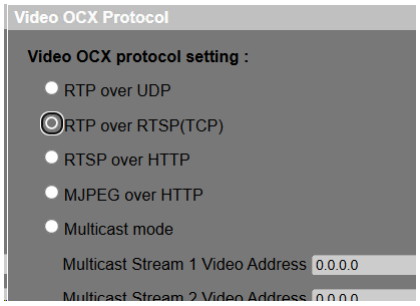
1. Follow the instructions noted in section 4.3.1, SSL/TLS versions.

4.3.5Encrypted streaming (RTP/RTSP/HTTPS, SRTP)

In HTTPS mode HTTP tunnelling of RTP/RTSP encrypts the stream over the secure socket. Only the receiving VMS is able to decrypt the video content.
If the camera supports the SRTP protocol, then this protocol is preferred over the RTP protocol.

To do this via the camera web page:

1. Open the camera web page in your browser and login as administrator
2. Navigate to Streaming> Video OCX Protocol



3. Make sure that the RTP over RTSP radio button is selected.

4.3.6Data Retention Policy

Establish a data retention policy to regularly delete or archive old footage in a secure manner.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

4.4 Monitoring and Logging

4.4.1 Logging

Logging is by default enabled on the camera to monitor access and configuration changes. The log files are store securely on the device.

To retrieve the camera log file, refer to section 3.2.10.

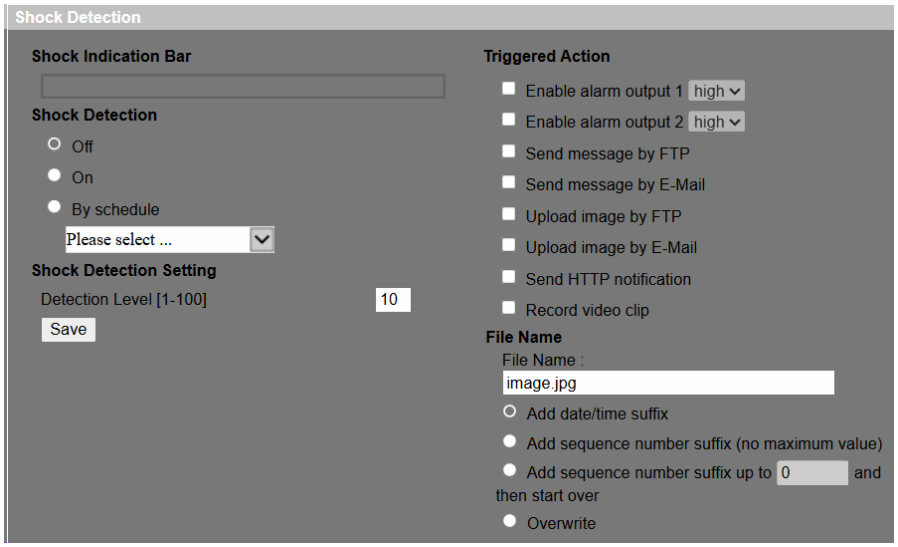
4.4.2 Tamper Detection

The camera is fitted with a Tamper Detection System to monitor the quality and integrity of the image.

Since the camera is a moveable PTZ camera, the Tamper detection function is not available. However, a similar function can be achieved by using the camera's shock detection function.

To do this via the camera web page:

1. Open the camera web page in your browser and login as administrator
2. Navigate to System> Events> Shock Detection



3. Configure the actions you need the camera to take in case of a shock detection event.

4.4.3 Check the log file regularly

Regularly inspect the log files to stay informed of reported irregularities.

4.4.4Network Traffic

Analyse network traffic to detect potential anomalies related to the cameras.

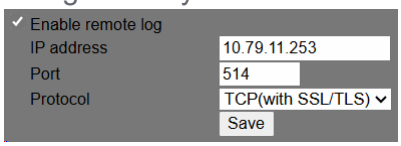
To confirm potential anomaly behaviour related to the camera, the network specialist shall first need to confirm what is considered normal behaviour, by extensively monitoring the network traffic under normal conditions.

4.4.5Use secure syslog with TLS

The best practise for logging is the use of remote syslog over a secure channel (TLS). If the camera is not supporting secure syslog, use local logging with the minimum options.
Make sure that the logging server is adequately secured to allow authorized access only.

To do this via the camera web page:

1. Open the camera web page in your browser and login as administrator
2. Navigate to System> View Information> Log File



3. Make sure that the Enable remote log checkbox is checked
4. Enter the syslog server’s IP address
5. Enter the port to be used for the logging
6. Make sure that the Protocol combo box has “TCP (with SSL/TLS)“ item selected.
7. Click Save button

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Appendix A Install UPnP Components

Please follow the instructions below to install UPnP components on Windows 11 / Windows 7, 8, 10 / Windows Vista / Windows XP.

For Windows 11:
Step 1: Click <Control Panel>.

Step 2: Click <Network and Internet>.

Step 3: Click the <Network and Sharing Center>.

Step 4: Click <Change advanced sharing settings> in the left pane.

Step 5: Turn on <Network discovery> in <Public Networks> to complete the setup.

For Windows 7, 8, 10:
Step 1: Click on <Control Panel>.

Step 2: Click on <Network and Internet>.

Step 3: Click on the <Network and Sharing Center>.

Step 4: Click on <Change advanced sharing settings> in the left pane.

Step 5: Select <Turn on network discovery> in <Network Discovery>.

Step 6: Click on <Save changes> to complete the setup.

For Windows Vista:
Step 1: Click on <Control Panel>.

Step 2: Click on <Network and Sharing Center>.

Step 3: Click the arrow button from <Network discovery> in <Sharing and Discovery>.

Step 4: Click on <Turn on network discovery>.

Step 5: Click on <Apply> to complete the setup.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

For Windows XP:

Step 1: Click on <Control Panel>, and then double click on <Add or Remove Programs>.

Step 2: Click on <Add/Remove Windows Components> in the <Add or Remove Programs> page.

Step 3: Select <Networking Services> from the Components list in Components Wizard window of the Windows, and then click <Details>.

Step 4: Select <UPnP User Interface> in the Networking Services' subcomponents list and then click on <OK>.

Step 5: Click on <Next> in the Windows Components Wizard window.

Step 6: Click on <Finish> to complete installation.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Appendix B IP Addresses from Decimal to Binary

Follow the example below to convert the IP addresses to binary numbers. Use the calculator on the computer for conversion. The calculator can be found under this path: Start > All Programs > Accessories > Calculator. For Windows XP and Windows Vista, click <View> on the calculator and click <Scientific>. For Windows 7 and Windows 8, click <View> on the calculator and click <Programmer>. Then follow the steps in the following example to convert the IP addresses.

The example below shows how to convert 192.168.2.81 to binary numbers.

Step 1: On the left of the calculator, select <Dec>. Then enter the first decimal number of the IP address, “192”. Select <Bin> and the number will be converted to binary number. Repeat the same procedure with the rest of decimal numbers. Remember to select <Dec> before entering the next decimal number. Otherwise a decimal number cannot be entered. The table below shows the binary number of each decimal number.

Decimal Numbers	Binary Numbers
192	11000000
168	10101000
2	10
81	1010001

Step 2: Each binary number should have eight digits. If a binary number does not have eight digits, please add 0 in front of it until it does. The binary number of each decimal number should be as follow.

Decimal Numbers	Binary Numbers
192	11000000
168	10101000
2	00000010
81	01010001

Step 3: Therefore, the binary numbers of IP address 192.168.2.81 is 11000000.10101000.00000010.01010001.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Appendix C Installation

Recommendation for Camera Installation

Target size

The suggested target size that can be detected

Effective field of view

Due to the possibility of lens distortion, it is suggested to set the detection zone within the FOV.

Camera mounting height

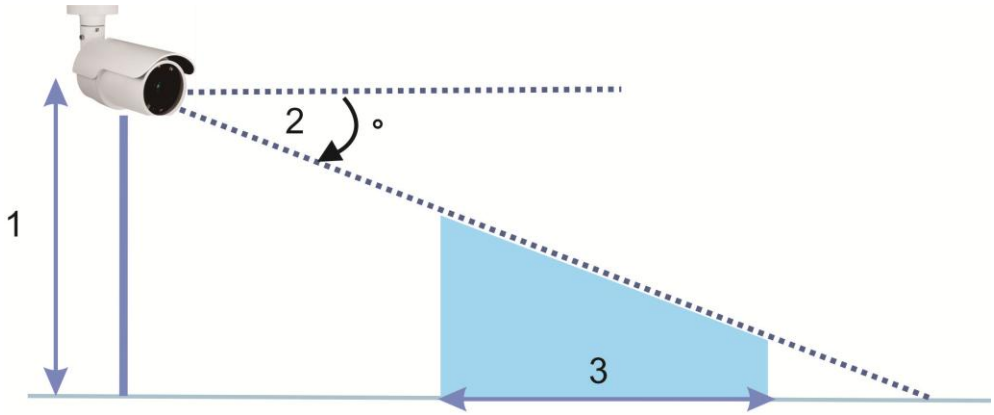
The suggested mounting height for camera

Detection range

The detectable distance range between camera and target object

Camera tilt angle

The included angle between camera and ceiling

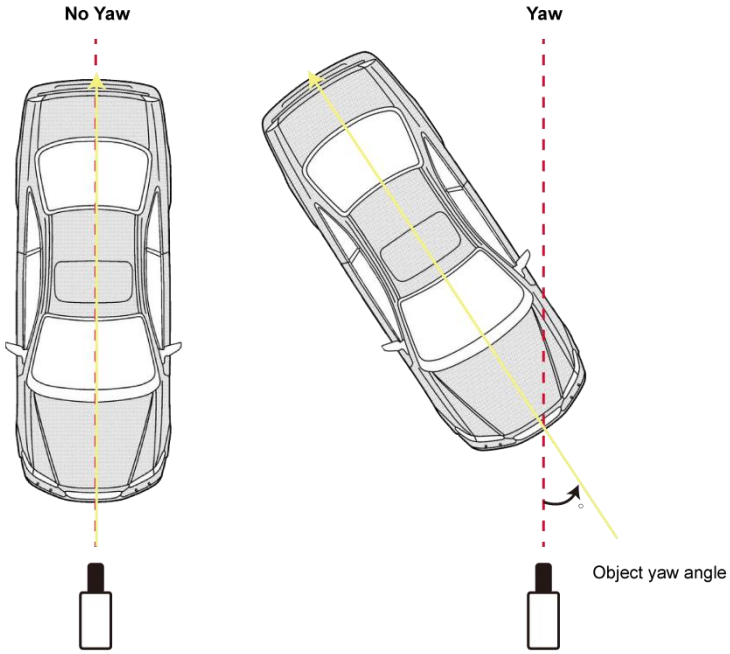


1. Camera mounting height
2. Camera tilt angle
3. Detection range

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

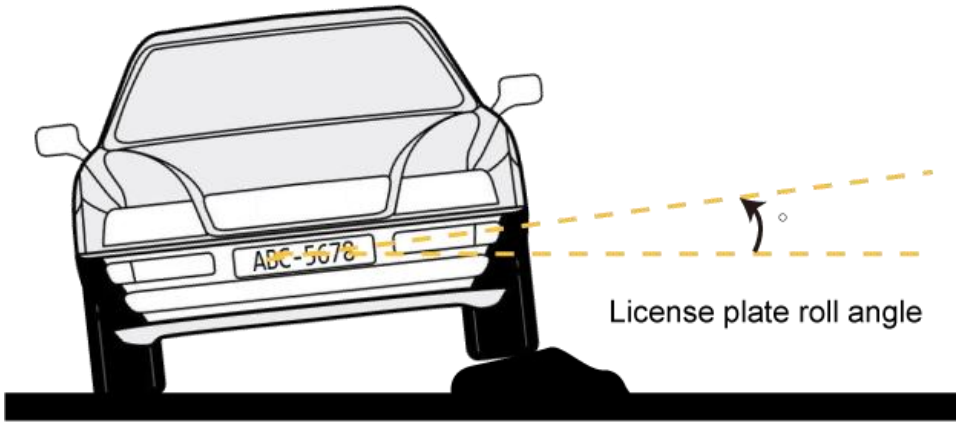
Object yaw angle

The angle between camera direction and the object facing direction



Roll angle

Rotation angle of the object



Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Scene Requirement

- Keep the camera lens clean and free from rain and water drops. Prevent camera from condensation.
- Position the camera in a place where the scene is predominantly non-reflective.
- To eliminate camera shake, the camera must be placed and installed in a sturdy and secured location, e.g., on a pole. Incorrect camera installation may cause poor camera performance.
- The distinction of the target object from the background must be very clear and obvious, e.g., of color and texture. There should be no camouflage, i.e., making the color and texture of the target object similar to the one of the background.
- Good video analytics performance requires steady and sufficient illumination source.
- With the installation of external illuminators, low light condition can be avoided, and the target object can be distinguished under both natural and artificial lighting conditions. Note that the effect of shadow should be taken into account when planning the illumination. For the best performance, white light mode is preferable compared to IR mode.
- Avoid backlight scenes and unexpected light sources (e.g., from vehicles, street lights) projecting in the detection zone.
- Make sure that the target object can be seen clearly, and there are no occlusions, e.g., trees, pillars, buildings and furniture.
- Poor camera performance may occur if there are clouds, fog or other moving objects with similar appearance to the target object in the detection zone.
- Bad weather conditions, e.g., heavy rain, fog or snow, might affect and reduce detection range and accuracy.
- It is suggested to turn on WDR/HDR function in high dynamic range scene for sufficient image details.
- To improve the camera performance, turn on noise reduction to prevent the image from flickering noise and artifacts.
- As long as the target object does not move fast, the Video Analytics-AI functions can still work properly.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Appendix D Standard Setting

Here is to set the definition of an event and what actions to take when an event occurs. The following describes the definition of each setting item.

Triggered Action

Users can specify alarm actions when an event occurs. All options are listed as follows.

- **Enable Alarm Output (High/Low)**
  Check the item and select the predefined type of alarm output to enable alarm relay output when motion is detected.

- **IR Cut Filter**
  For Alarm Input and Manual Trigger functions, select the item and the IR cut filter (ICR) of the camera will be removed (on) or blocked (off) when alarm input is triggered. This function is only available for models with IR cut filter. This function is **NOT** available for PTZ cameras.

  NOTE: The IR Function (refer to section Camera> IR Function) could not be set as <Auto> mode if this triggered action is enabled.

- **Send HTTP Notification**
  Check the item and select the destination HTTP address, and specify the parameters for HTTP notification. When an alarm is triggered, the HTTP notification will be sent to the specified HTTP server.

  For instance, if the custom parameter is set as "action=1&group=2", and the HTTP server name is "http://192.168.0.1/admin.php", the notification will be sent to HTTP server as "http://192.168.0.1/admin.php?action=1&group=2" when alarm is triggered.

- **Record Video Clip**
  Check the item and select a video recording storage type, <SD Card> or <Network Storage> (Network-Attached Storage>. The recording will be saved into the microSD/SD card or the Network Storage.

  Pre-trigger buffer recording function allows users to check what caused the trigger. The pre-trigger buffer time range is from 1 sec. to 15 sec. Select <Upload for __ sec> to set the recording duration after the function is triggered. The setting range is from 1 to 99999 sec. Select <Upload During the Trigger Active> or <Upload While the Trigger Is Active > to record the triggered video until the trigger is off.

NOTE: Please make sure the local recording (with microSD/SD card) or the remote recording (with Network Storage) is activated so that this function can be implemented. Refer to section Recording for further details.

- **PTZ Function**

Assign a camera function: Preset, Sequence, Autopan or Cruise, and specify a Function Line for the camera to perform when an alarm is triggered. The function line is used to select the desired execution positions or paths. If selected the Preset function, please also set up a Dwell Time. This function is only available for the Alarm Input and Manual Trigger functions on PTZ Cameras.

NOTE: Please refer to the sections Preset, Cruise, Autopan, and Sequence for details of Preset Point / Cruise Line / Autopan Path / Sequence Line setups.

If the selected function is <Preset>, it is required to enter its dwell time (1 sec. to 256 sec.) in the corresponding field. When the alarm is triggered, the camera will go to the selected Preset Point and stay there for a user-defined period of time. As for other function modes, the camera will keep executing the specified function; to stop the performance, simply change the camera's status.

NOTE: The dwell time is only adjustable when <Preset> is selected. When the dwell time is up, the camera will go back to its trigger position and recheck the alarm pin status.

- **Send Alarm Message by FTP/E-Mail**

The administrator can select whether to send an alarm message by FTP and/or E-mail when an alarm is triggered.

- **Upload Image by FTP**

Select this item and the administrator can assign an FTP site and configure various parameters. When an alarm is triggered, event images will be uploaded to the appointed FTP site. Note that to implement this function, one of the streaming MUST be set as **MJPEG**; otherwise, this function will be grayed out and cannot be accessed.

<Pre-trigger buffer> function allows users to check what caused the trigger. The <Pre-trigger buffer> frame rate could be pre-determined. On the other hand, <Post-

trigger buffer> is for users to upload certain amount of images after the event occurs.

NOTE: <Pre-trigger buffer> generally ranges from 1 to 20 frames. However, the range will change accordingly if the frame rate of MJPEG on Streaming> Video Configuration is 6 or smaller.

Check the box <Continue Image Upload> to upload the triggered images during certain time or keep uploading until the trigger is off. Select <Upload for __sec> and enter the duration in the blank. The images of the duration will be uploaded to FTP when the event occurs. The setting range is from 1 to 99999 sec. Select <Upload During the Trigger Active> or <Upload While the Trigger Is Active> to make the images keep being uploaded to FTP during the trigger active until the event stops. Set the Image frequency as the upload frame rate. The setting range is from 1 to 15 frames per second. This <Continue Image Upload> function is not available for <Periodical Event>.

NOTE: Make sure FTP configuration has been completed. Refer to section System> Events Management > FTP for further details.

- **Upload Image by E-Mail**

Select this item and the administrator can assign an E-mail address and configure various parameters. When an alarm is triggered, event images will be sent to the appointed E-mail address. Note that to implement this function, one of the streaming **MUST** be set as **MJPEG**; otherwise, this function will be grayed out and cannot be accessed.

<Pre-trigger buffer> function allows users to check what caused the trigger. The <Pre-trigger buffer> frame rate could be pre-determined. On the other hand, <Post-trigger buffer> is for users to upload certain amount of images after the event occurs.

NOTE: <Pre-trigger buffer> generally ranges from 1 to 20 frames. However, the setting range will change accordingly if the frame rate of MJPEG on Streaming> Video Configuration is 6 or smaller.

Check the box <Continue Image Upload> to upload the triggered images during certain time or keep uploading until the trigger is off. Select <Upload for __sec> and enter the duration in the blank. The images of the duration will be uploading by E-mail when the event occurs. The setting range is from 1 to 99999 sec. Select

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

<Upload During the Trigger Active> or <Upload While the Trigger Is Active> to make the images keep being uploaded to E-mail during the trigger active until the event stops. Set the Image frequency as the upload frame rate. The setting range is from 1 to 15 frames per second. This <Continue Image Upload> function is not available for <Periodical Event>.

NOTE: Make sure SMTP configuration has been completed. Refer to section System> Events Management> Mail for further details.

- **Upload Image to SD Card**

Select this item, and then the images will be uploaded to the SD card periodically. Note that to implement this function, one of the streaming MUST be set as MJPEG; otherwise, this function will be grayed out and cannot be accessed.

The <Pre-trigger buffer> function can define how many images to be uploaded before the triggered moment. The <Post-trigger buffer> function can define how many images to be uploaded after the triggered moment.

This function is only available for Periodical Event function.

NOTE: <Pre-trigger buffer> generally ranges from 1 to 20 frames. However, the range will change accordingly if the frame rate of MJPEG on Streaming> Video Configuration is 6 or smaller.

NOTE: Before implementing <Upload Image to SD Card>, please make sure that the SD Card is properly detected and installed. Refer to Recording> Storage Management> SD Card for further details.

File Name

Enter a file name in the blank, e.g., image.jpg. The file name format of the uploaded image can be set in this section. Please select the one that meets the requirements.

- **Add Date/Time Suffix**

File name: imageYYMMDD_HHNNSS_XX.jpg
Y: Year, M: Month, D: Day
H: Hour, N: Minute, S: Second
X: Sequence Number

- **Add Sequence Number Suffix (No Maximum Value)**

File name: imageXXXXXXX.jpg
X: Sequence Number

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

- **Add a Serial Number Suffix, up to #, Then Start Again.**
  File Name: imageXX.jpg
  X: Serial Number

  The file name suffix will end at the number being set. For example, if the setting is up to “10”, the file name will start from 00, end at 10, and then start all over again.

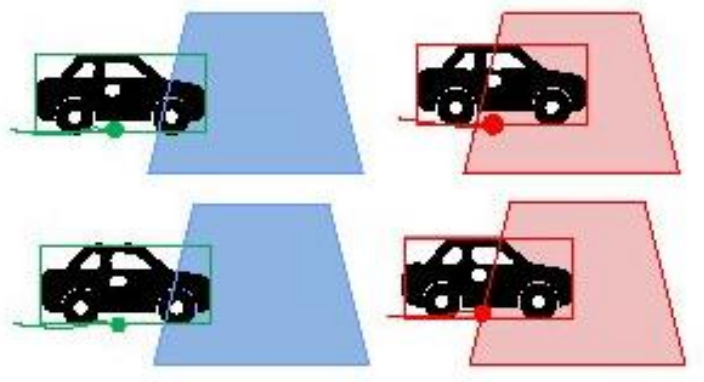
- **Overwrite**
  The original image in the FTP site will be overwritten by the new uploaded file with a static filename.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

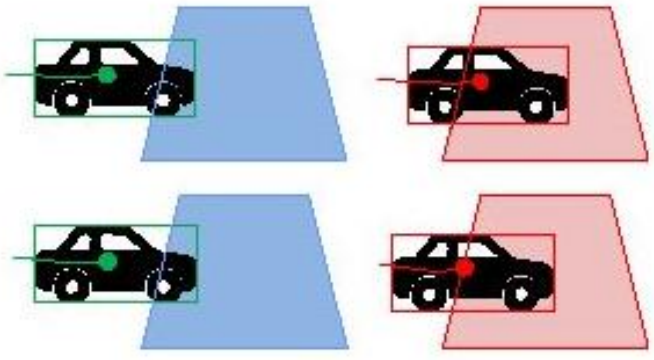
Appendix E Trigger Type

There are five options available as below.

- **Bottom Center Overlay**
  The trigger occurs when the bottom center point of the object's bounding box touches or is within the detection zone.

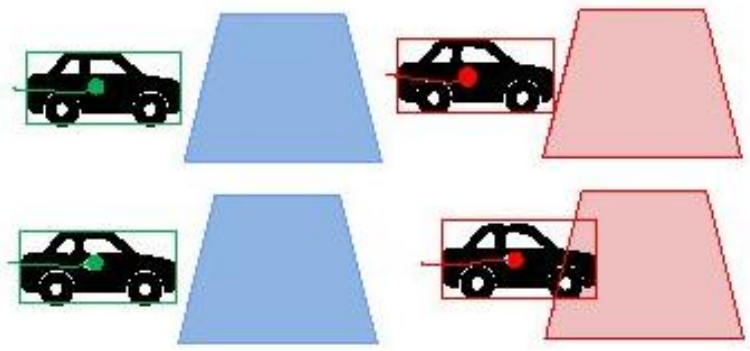


- **Center Overlay**
  The trigger occurs when the center point of the object's bounding box touches or is within the detection zone.

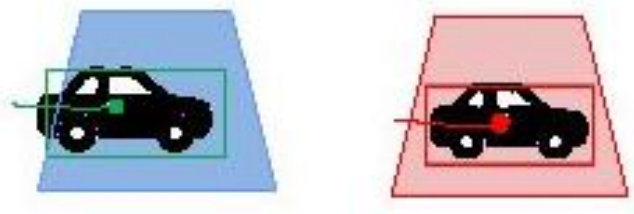


Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

- **Edge Overlay**
  The trigger occurs when the edge of the object's bounding box intersects the detection zone.



- **Fully inside**
  The trigger occurs when the object's bounding box is fully inside the detection zone.



- **Fully Cover Overlay**
  The trigger occurs when the object's bounding box is fully covers the detection zone.

Werner von Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Appendix F Edit Database

To export data into a database file or to import a database file, please follow the instructions below.

Database Statistics

This function shows the number of users (User or License Plates) and groups existed in the database.

Database Operation

Import the database from the local data file. Please create the data file by clicking the link shown below.

1. Select a database to import: To select a database to import, click <Browse> to select file.
2. Replace or append to old database: Select "Overwrite" from the drop-down menu to replace the original database, or choose "Append" to add data to the database.
3. Start importing the new database: Click <Import> to start importing the new database.

Export the current database to a CSV file. Please click <Export> to export the database.

Delete and reset the current database to default: Enter **“Delete All”** in the text field and click <Delete> to remove all data from the database. The database will be reset to its default setting.

Werner von
Siemensstraat 7
2712 PN Zoetermeer
The Netherlands

Appendix G License Plate Region

The following information lists the countries and cities supported by this feature.

Africa

Includes Algeria, Angola, Botswana, Benin, Burkina Faso, Ethiopia, Ghana, Kenya, Liberia, Mozambique, Mayotte, Namibia, Nigeria, Senegal, South Africa, Swaziland, Tanzania, Tunisia, Uganda, Zambia and Zimbabwe.

America

Includes Bolivia, Brazil, Chile, Canada, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, Nicaragua, Panama, Peru, Suriname and United States.

Asia

Includes Armenia, Azerbaijan, Bahrain, Bangladesh, Bhutan, Brunei, Cyprus, Georgia, India, Indonesia, Israel, Japan, Kazakhstan, Kuwait, Kyrgyzstan, Lebanon, Malaysia, Mongolia, Philippines, Russia, Singapore, Taiwan, Tajikistan, Turkey, Turkmenistan, Uzbekistan and Vietnam.

Europe

Includes Austria, Belarus, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Ireland, Italy, Kyrgyzstan, Latvia, Lithuania, Luxembourg, Moldova, Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Ukraine and United Kingdom.

Oceania

Includes Australia and New Zealand.