




A large, bold, black icon of a camera or video frame, consisting of a thick black border with a small square cutout in the top-left corner.

TruVision 6MP and 12MP 360° Camera Configuration Manual

Copyright	<p>© 2021 Carrier. All rights reserved. Specifications subject to change without prior notice.</p> <p>This document may not be copied in whole or in part or otherwise reproduced without prior written consent from Carrier, except where specifically permitted under US and international copyright law.</p>
Trademarks and patents	<p>TruVision names and logos are a product brand of Aritech, a part of Carrier.</p> <p>Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.</p>
Manufacturer	<p>PLACED ON THE MARKET BY:</p> <p>Carrier Fire & Security Americas Corporation Inc. 13995 Pasteur Blvd, Palm Beach Gardens, FL 33418, USA</p> <p>AUTHORIZED EU REPRESENTATIVE:</p> <p>Carrier Fire & Security B.V. Kelvinstraat 7, 6003 DH Weert, Netherlands</p>
FCC compliance	<p>Class A: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.</p>
FCC conditions	<p>This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:</p> <p>(1) This device may not cause harmful interference.</p> <p>(2) This Device must accept any interference received, including interference that may cause undesired operation.</p>
ACMA compliance	<p>Notice! This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.</p>
Product warnings and disclaimers	<p>THESE PRODUCTS ARE INTENDED FOR SALE TO AND INSTALLATION BY QUALIFIED PROFESSIONALS. CARRIER FIRE & SECURITY CANNOT PROVIDE ANY ASSURANCE THAT ANY PERSON OR ENTITY BUYING ITS PRODUCTS, INCLUDING ANY "AUTHORIZED DEALER" OR "AUTHORIZED RESELLER", IS PROPERLY TRAINED OR EXPERIENCED TO CORRECTLY INSTALL FIRE AND SECURITY RELATED PRODUCTS.</p> <p>For more information on warranty disclaimers and product safety information, please check https://firesecurityproducts.com/policy/product-warning/ or scan the following code:</p>
Certification	    
EU directives	<p>This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the RoHS Directive 2011/65/EU.</p>



2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info.



2013/56/EU & 2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info.

Contact information

EMEA: <https://firesecurityproducts.com>

Australian/New Zealand: <https://firesecurityproducts.com.au/>

Product documentation

Please consult the following web link to retrieve the electronic version of the product documentation. The manuals are available in several languages.



Content

Important information 1

- Limitation of liability 1
- Product Warnings 1
- Warranty Disclaimers 2
- Intended Use 3
- Advisory messages 3

Introduction 4

Network access 5

- Checking your web browser security level 5
- Activating the camera 6
- Overview of the camera web browser 8

Camera configuration 13

- Local configuration 13
- Configuration 14
 - Defining the system time 16
 - Defining RS-485 settings 17
- Maintenance 17
- Configuring the network settings 19
- Recording parameters 26
- Video image 29
- OSD (On Screen Display) 33
- Privacy masks 34
- Picture overlay 35
- Motion detection alarms 36
- Video tampering 41
- Alarm inputs and outputs 42
- Exception alarms 43
- Audio exception detection 44
- Intrusion detection 46
- Cross line detection 48
- Region entrance detection 50
- Region exiting detection 52
- Unattended baggage detection 53
- Object removal detection 54
- Recording schedule 56
- Snapshot parameters 58
- Formatting the storage devices 60
- Configuring NAS settings 61
- People counting 62
- Heat map 65
- Intersection analysis 67

Application 69

- People counting statistics 69
- Heat map statistics 71
- Intersection analysis statistics 73

Camera management 75

- User management 75
- RTSP authentication 78
- IP address filter 78
- Defining the security service 79
- Restore default settings 80
- Import/export a configuration file 80
- Upgrade firmware 80
- Reboot camera 82

Camera operation 83

- Log on and off 83
- Live view mode 83
- Play back recorded video 83
- Snapshots 86
- Search event logs 86
- Operating PTZ control 88

Index 91

Important information

Limitation of liability

To the maximum extent permitted by applicable law, in no event will Carrier be liable for any lost profits or business opportunities, loss of use, business interruption, loss of data, or any other indirect, special, incidental, or consequential damages under any theory of liability, whether based in contract, tort, negligence, product liability, or otherwise. Because some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages the preceding limitation may not apply to you. In any event the total liability of Carrier shall not exceed the purchase price of the product. The foregoing limitation will apply to the maximum extent permitted by applicable law, regardless of whether Carrier has been advised of the possibility of such damages and regardless of whether any remedy fails of its essential purpose.

Installation in accordance with this manual, applicable codes, and the instructions of the authority having jurisdiction is mandatory.

While every precaution has been taken during the preparation of this manual to ensure the accuracy of its contents, Carrier assumes no responsibility for errors or omissions.

Product Warnings

YOU UNDERSTAND THAT A PROPERLY INSTALLED AND MAINTAINED ALARM/SECURITY SYSTEM MAY ONLY REDUCE THE RISK OF EVENTS SUCH AS BURGLARY, ROBBERY, FIRE, OR SIMILAR EVENTS WITHOUT WARNING, BUT IT IS NOT INSURANCE OR A GUARANTEE THAT SUCH EVENTS WILL NOT OCCUR OR THAT THERE WILL BE NO DEATH, PERSONAL INJURY, AND/OR PROPERTY DAMAGE AS A RESULT.

THE ABILITY OF CARRIER PRODUCTS, SOFTWARE OR SERVICES TO WORK PROPERLY DEPENDS ON A NUMBER OF PRODUCTS AND SERVICES MADE AVAILABLE BY THIRD PARTIES OVER WHICH CARRIER HAS NO CONTROL AND FOR WHICH CARRIER SHALL NOT BE RESPONSIBLE INCLUDING, BUT NOT LIMITED TO, INTERNET, CELLULAR AND LANDLINE CONNECTIVITY; MOBILE DEVICE AND OPERATING SYSTEM COMPATIBILITY; MONITORING SERVICES; ELECTROMAGNETIC OR OTHER INTERFERENCE, AND PROPER INSTALLATION AND MAINTENANCE OF AUTHORIZED PRODUCTS (INCLUDING ALARM OR OTHER CONTROL PANEL AND SENSORS).

ANY PRODUCT, SOFTWARE, SERVICE OR OTHER OFFERING MANUFACTURED, SOLD OR LICENSED BY CARRIER, MAY BE HACKED, COMPROMISED AND/OR CIRCUMVENTED AND CARRIER MAKES NO REPRESENTATION, WARRANTY, COVENANT OR PROMISE THAT ITS PRODUCTS (INCLUDING SECURITY PRODUCTS), SOFTWARE, SERVICES OR OTHER OFFERINGS WILL NOT BE HACKED, COMPROMISED AND/OR CIRCUMVENTED.

CARRIER DOES NOT ENCRYPT COMMUNICATIONS BETWEEN ITS ALARM OR OTHER CONTROL PANELS AND THEIR WIRELESS OUTPUTS/INPUTS INCLUDING BUT NOT LIMITED TO, SENSORS OR DETECTORS UNLESS REQUIRED BY

APPLICABLE LAW. AS A RESULT THESE COMMUNICATIONS MAY BE INTERCEPTED AND COULD BE USED TO CIRCUMVENT YOUR ALARM/SECURITY SYSTEM.

THE EQUIPMENT SHOULD ONLY BE OPERATED WITH AN APPROVED POWER ADAPTER WITH INSULATED LIVE PINS.

DO NOT CONNECT TO A RECEPTACLE CONTROLLED BY A SWITCH.

THIS UNIT INCLUDES AN ALARM VERIFICATION FEATURE THAT WILL RESULT IN A DELAY OF THE SYSTEM ALARM SIGNAL FROM THE INDICATED CIRCUITS. THE TOTAL DELAY (CONTROL UNIT PLUS SMOKE DETECTORS) SHALL NOT EXCEED 60 SECONDS. NO OTHER SMOKE DETECTOR SHALL BE CONNECTED TO THESE CIRCUITS UNLESS APPROVED BY THE LOCAL AUTHORITY HAVING JURISDICTION.

WARNING! The equipment should only be operated with an approved power adapter with insulated live pins.

Caution: Risk of explosion if battery is replaced by an incorrect type. Dispose of batteries according to the instructions. Contact your supplier for replacement batteries.

Warranty Disclaimers

CARRIER HEREBY DISCLAIMS ALL WARRANTIES AND REPRESENTATIONS, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING ANY IMPLIED WARRANTIES, THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

(USA only) SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. YOU MAY ALSO HAVE OTHER LEGAL RIGHTS THAT VARY FROM STATE TO STATE.

CARRIER DOES NOT MAKE ANY CLAIMS OR WARRANTIES TO YOU OF ANY KIND REGARDING ANY PRODUCT, SOFTWARE OR SERVICE'S POTENTIAL, ABILITY, OR EFFECTIVENESS TO DETECT, MINIMIZE, OR IN ANYWAY PREVENT DEATH, PERSONAL INJURY, PROPERTY DAMAGE, OR LOSS OF ANY KIND WHATSOEVER.

CARRIER DOES NOT REPRESENT TO YOU THAT ANY PRODUCT (INCLUDING SECURITY PRODUCTS), SOFTWARE, SERVICE OR OTHER OFFERING MAY NOT BE HACKED, COMPROMISED AND/OR CIRCUMVENTED.

CARRIER DOES NOT WARRANT THAT ANY PRODUCT (INCLUDING SECURITY PRODUCTS), SOFTWARE OR SERVICE MANUFACTURED, SOLD OR LICENSED BY CARRIER WILL PREVENT, OR IN ALL CASES PROVIDE ADEQUATE WARNING OF OR PROTECTION FROM, BREAK-INS, BURGLARY, ROBBERY, FIRE, OR OTHERWISE.

CARRIER DOES NOT WARRANT TO YOU THAT ITS SOFTWARE OR PRODUCTS WILL WORK PROPERLY IN ALL ENVIRONMENTS AND APPLICATIONS AND DOES NOT WARRANT ANY PRODUCTS AGAINST HARMFUL ELECTROMAGNETIC INTERFERENCE INDUCTION OR RADIATION (EMI, RFI, ETC.) EMITTED FROM EXTERNAL SOURCES

CARRIER DOES NOT PROVIDE MONITORING SERVICES FOR YOUR ALARM/SECURITY SYSTEM ("MONITORING SERVICES"). IF YOU ELECT TO HAVE MONITORING SERVICES YOU MUST OBTAIN SUCH SERVICE FROM A THIRD PARTY AND CARRIER MAKES NO REPRESENTATION OR WARRANTY WITH RESPECT TO SUCH SERVICES INCLUDING WHETHER OR NOT THEY WILL BE COMPATIBLE WITH THE PRODUCTS, SOFTWARE OR SERVICES MANUFACTURED, SOLD OR LICENSED BY CARRIER.

Intended Use

Use this product only for the purpose it was designed for; refer to the data sheet and user documentation. For the latest product information, contact your local supplier or visit us online at firesecurityproducts.com.

The system should be checked by a qualified technician at least every 3 years and the backup battery replaced as required.

Advisory messages

Advisory messages alert you to conditions or practices that can cause unwanted results. The advisory messages used in this document are shown and described below.

WARNING: Warning messages advise you of hazards that could result in injury or loss of life. They tell you which actions to take or to avoid in order to prevent the injury or loss of life.

Caution: Caution messages advise you of possible equipment damage. They tell you which actions to take or to avoid in order to prevent the damage.

Note: Note messages advise you of the possible loss of time or effort. They describe how to avoid the loss. Notes are also used to point out important information that you should read.

Introduction

This is the configuration manual for the following TruVision IP camera models:

- TVF-5201 (TruVision 6MP 360° IP Dome, indoor, 1.29 mm)
- TVF-5202 (TruVision 12MP 360° IP Dome, indoor, 1.29 mm)
- TVF-5203 (TruVision 6MP 360° IP Dome, outdoor, 1.29 mm)
- TVF-5204 (TruVision 12MP 360° IP Dome, outdoor 1.29 mm)

Network access

This manual explains how to configure the camera over the network with a web browser.

TruVision IP cameras can be configured and controlled using Microsoft Internet Explorer (IE) and other browsers. The procedures described use Microsoft Internet Explorer (IE) web browser.

Checking your web browser security level

When using the web browser interface, you can install ActiveX controls to connect and view video using Internet Explorer (the camera is not compatible with Microsoft Edge). However, you cannot download data, such as video and images due to the increased security measure. Consequently, you should check the security level of your PC so that you are able to interact with the cameras over the web and, if necessary, modify the Active X settings.

Configuring IE ActiveX controls

You should confirm the ActiveX settings of your web browser.

To change the web browser's security level:

1. In Internet Explorer click **Internet Options** on the **Tools** menu.
2. On the Security tab, click the zone to which you want to assign a web site under "Select a web content zone to specify its security settings".
3. Click **Custom Level**.
4. Change the **ActiveX controls and plug-ins** options that are signed or marked as safe to **enable**. Change the **ActiveX controls and plug-ins** options that are unsigned to **Prompt** or **Disable**. Click **OK**.

- Or -

Under **Reset Custom Settings**, click the security level for the whole zone in the Reset To box, and select **Medium**. Click **Reset**.

Then click **OK** to the Internet Options Security tab window.

5. Click **Apply** in the **Internet Options** Security tab window.

Windows users

Internet Explorer operating systems have increased security measures to protect your PC from any malicious software being installed.

To have complete functionality of the web browser interface with Windows 7, 8 and 10, do the following:

- Run the Browser interface as an administrator in your workstation
- Add the camera's IP address to your browser's list of trusted sites

To add the camera's IP address to Internet Explorer's list of trusted sites:

1. Open Internet Explorer.
2. Click **Tools**, and then **Internet Options**.
3. Click the **Security** tab and then select the **trusted sites** icon.
4. Click the **Sites** button.
5. Clear the "Require server verification (https :) for all sites in this zone" check box.
6. Enter the IP address in the "Add this website to the zone" field.
7. Click **Add**, and then click **Close**.
8. Click **OK** in the Internet Options dialog window.
9. Connect to the camera for full browser functionality.

Activating the camera

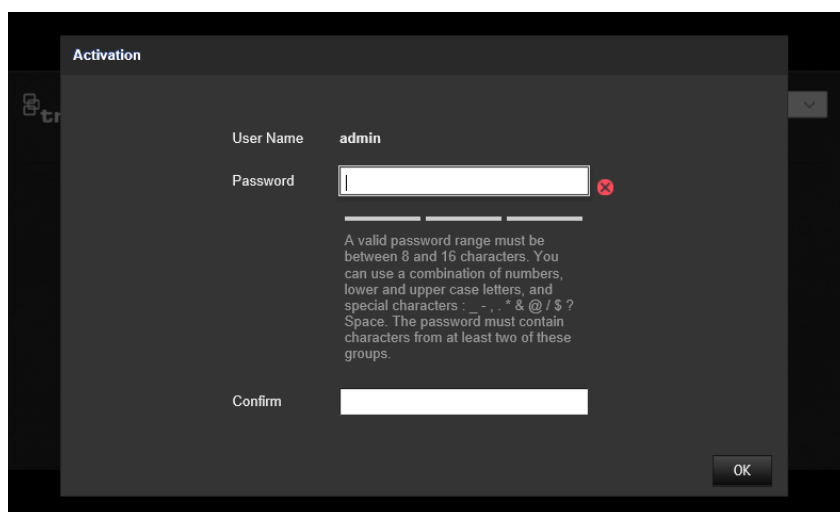
When you first start up the camera, the Activation window appears. You must define a high-security admin password before you can access the camera. There is no default password provided.

You can activate a password via a web browser and via TruVision Device Manager.

Warning: When the 360° camera is operating, the surface of the housing will be hot to the touch. The heat buildup is due to the processing power that is required to operate the camera

Activation via the web browser:

1. Power on the camera and connect the camera to the network.
2. Input the IP address into the address bar of the web browser, and click **Enter** to enter the activation interface.



Note:

- The default IP address of the camera is 192.168.1.70.

- For the camera to enable DHCP by default, you must activate the camera via TruVision Device Manager. Please refer to the following section, “Activation via TruVision Device Manager”.

3. Enter the password in the password field.

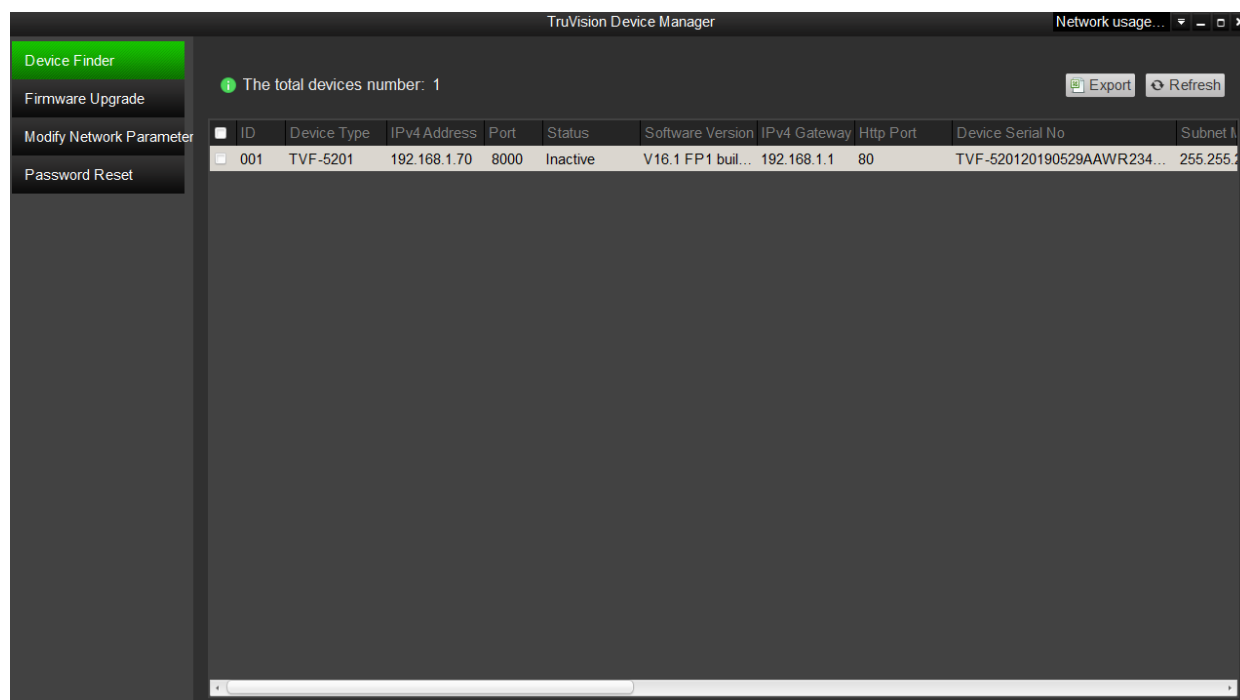
Note: A valid password range must be between 8 and 16 characters. You can use a combination of numbers, lower and upper case letters, and special characters: _ - , * & @ / \$? Space. The password must contain characters from at least two of these groups. We also recommend that you reset your password regularly. For high security systems, it is particularly recommended to reset the password monthly or weekly for better protection.

4. Confirm the password.

5. Click **OK** to save the password and enter the live view interface.

Activation via *TruVision Device Manager*:

1. Run the *TruVision Device Manager* to search for online devices.
2. Check the device status from the device list, and select the inactive device.



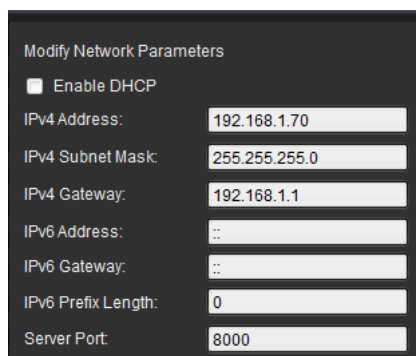
3. Enter the password in the password field, and confirm it.

Note: A valid password range must be between 8 and 16 characters. You can use a combination of numbers, lower and upper case letters, and special characters: _ - , * & @ / \$? Space. The password must contain characters from at least two of these groups. We also recommend that you reset your password regularly. For high security systems, it is particularly recommended to reset the password monthly or weekly for better protection.

4. Click **OK** to save the password.

A pop-up window appears to confirm activation. If activation fails, confirm that the password meets the requirements and try again.

5. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the check box of Enable DHCP.



Modify Network Parameters

☐ Enable DHCP

IPv4 Address: 192.168.1.70

IPv4 Subnet Mask: 255.255.255.0

IPv4 Gateway: 192.168.1.1

IPv6 Address: ::

IPv6 Gateway: ::

IPv6 Prefix Length: 0

Server Port: 8000

6. Input the password and click the **Save** button to activate your IP address modification.

Overview of the camera web browser











Use the camera web browser to view, record, and play back recorded videos as well as manage the camera from any PC with access to the same network as the camera. The browser's easy-to-use controls provide quick access to all camera functions.

If there is more than one camera connected over the network, open a separate web browser window for each individual camera.

Note: For accurate analysis *Ceiling Mount* should be selected when setting up the camera. See "Display control" on page 10. If *Ceiling Mount* is not selected, the *Application* tab will not be visible during setup.

Figure 1: Browser interface (Live view shown)



	Name	Description
1.	Live view	Click to view live video.
2.	Playback	Click to play back video.
3.	Picture	Click to search snapshots.
4.	Application	Click to enter the heat map statistics interface and search, view, download the counting data stored in the local storage or network storage.
5.	Log	Click to search for event logs. There are three main types: Alarm, Exception and Operation.
6.	Configuration	Click to display the configuration window for setting up the camera.
7.	Admin	Displays current user logged on.
8.	Help	Click to find function.
9.	Logout	Click to log out from the system. This can be done at any time.
10.	Live view toolbar	 Click to manually capture the snapshot.
		 Click to manually start/stop recording.
		 Click to start/stop digital zoom function. Note: Appears when using the hardware display mode only.
		 Click to select live view with main stream or substream.
		 Audio on and adjust Volume/Mute.
		 Manual alarm.
		 The window size is 4:3.
		 The window size is 16:9.
		 The original window size.
		 Self-adaptive window size.

Name	Description
11.	Display control. See Table 1 below for further information.
12.	PTZ control. See “Operating PTZ control” on page 88 for further information.

Display control




















You can select a display mode for the layout of the live view window. The description of each display mode is shown in the table below.





360° View: In *360° View* mode, the entire wide-angle view of the 360° camera is displayed.

Panoramic View: In *Panoramic View* mode, the round 360° image is transformed into a rectangular 180° image.

PTZ View: The *PTZ View* is the close-up view of a defined area within the 360° View or Panoramic View.

Table 1: Description of display control panel

Name	Description
Mount Type	 Ceiling mount.
	 Wall mount.
	 Table mount.
Software display mode	 360° view.
	 180° panoramic view.
	 360° panoramic view.
	 Live view with a 360° panoramic view and a PTZ view.
	 Live view with a 360° panoramic view and eight PTZ views.
	 Live view with a 360° panoramic view and six PTZ views.
	 Live view with a 360° panoramic view and eight PTZ views.
	 Live view with two PTZ views.
	 Live view with four PTZ views.
	 Live view with one 360° view and three PTZ views.
	 Live view with one 360° view and eight PTZ views.
	 Live view with sphere view.
	 Live view with AR half sphere view.
	 Live view with a cylinder view.
Hardware display mode	 360° view.
	 180° panoramic view

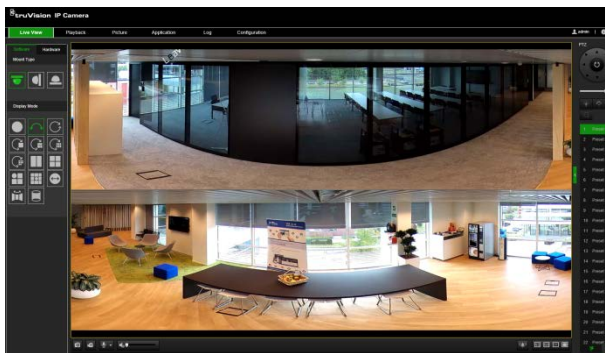
Name	Description
	Panoramic view.
	Live view with four PTZ views.
	Live view with one 360° view and three PTZ views.
	Live view with a four-PTZ-fusion view.

In display mode, **Software display** means that the obtained live view video is decoded using the CPU of your PC that is running the web browser. The live view performance depends on the decoding ability of your PC. **Hardware display** means that the obtained live view video is decoded by the camera itself.

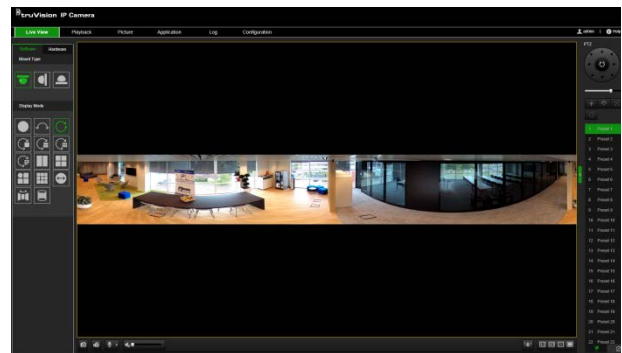
Note: When the selected mount type is **Table** and the hardware display mode is **Live view with four PTZ views** or **Live view with one 360° view and three PTZ views**, the pan operation is opposite from what is expected. When the pan moves left, the real direction is right. When the pan moves right, the real direction is left.

Some examples of the different software display modes:

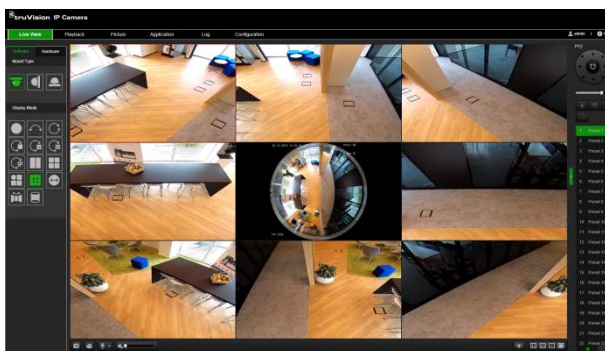
180° panoramic view



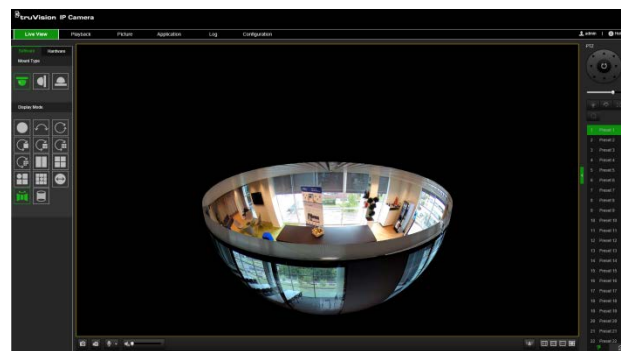
360° panoramic view



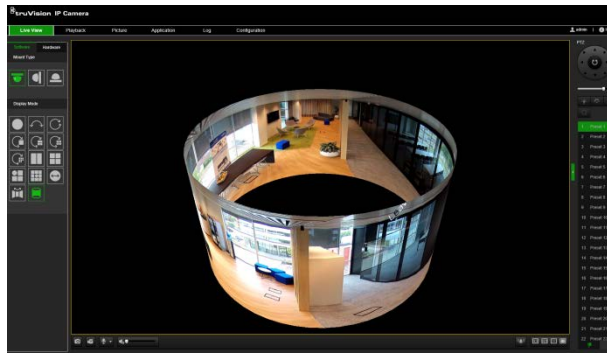
Live view with one 360° view and eight PTZ views



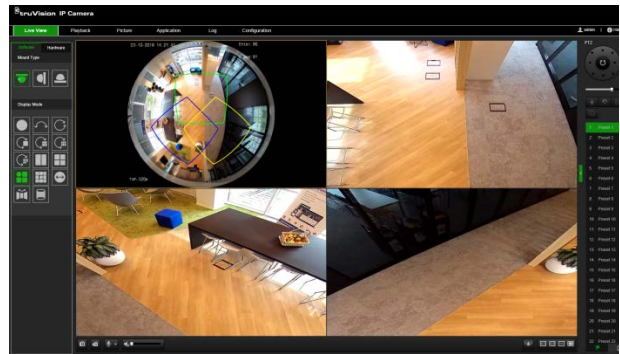
Live view with AR half sphere view.



Live view with a cylinder view



Live view with one 360° view and three PTZ views



Camera configuration

This chapter explains how to configure the cameras through a web browser.

Once the camera hardware has been installed, configure the camera's settings through the web browser. You must have administrator rights in order to configure the cameras over the internet.

The camera web browser lets you configure the camera remotely using your PC. Web browser options may vary depending on camera model.

There are two main folders in the configuration panel:

- Local configuration
- Configuration

Local configuration

Use the Local Configuration menu to manage the protocol type, live view performance and local storage paths. In the Configuration panel, click **Local Configuration** to display the local configuration window. See Figure 2 below for descriptions of the different menu parameters.

Figure 2: Local Configuration window

The screenshot shows the 'truVision IP Camera' web interface. The top navigation bar includes 'Live View', 'Playback', 'Picture', 'Application', 'Log', and 'Configuration' (highlighted in green). The left sidebar shows a tree view with 'Local Configuration' expanded, containing 'Browser Configuration' (highlighted) and 'Camera Configuration'. The main content area is titled 'Live View Parameters' and contains three sections:

- Live View Parameters** (marked with a circled 1):
 - Protocol: ☐ TCP, ☐ UDP, ☐ MULTICAST, ☐ HTTP
 - Latency: ☐ Shortest Delay, ☐ Auto, ☐ Fluent, ☐ Custom
 - Enable Meta Data Overlay: ☐ Enable, ☐ Disable
 - Display POS Information: ☐ Enable, ☐ Disable
 - Snapshot Image Format: ☐ JPEG, ☐ BMP
- Record File Settings** (marked with a circled 2):
 - Video File Size: ☐ 256M, ☐ 512M, ☐ 1G
 - Save Videos in Live View to: [Browse] [Open]
 - Save Downloaded Files to: [Browse] [Open]
- Picture and Clip Settings** (marked with a circled 3):
 - Save Snapshots in Live View to: [Browse] [Open]
 - Save Snapshots When Playing Back To: [Browse] [Open]
 - Save Clips during Playback to: [Browse] [Open]

A 'Save' button is located at the bottom left of the main content area.

Parameters	Description
1. Live View Parameters	
Protocol	Specifies the network protocol used.

Parameters	Description
	Options include: TCP, UDP, MULTICAST and HTTP. TCP: Ensures complete delivery of streaming data and better video quality, yet the real-time transmission will be affected. UDP: Provides real-time audio and video streams. HTTP: Allows the same quality as of TCP without setting specific ports for streaming under some network environments. MULTICAST: It's recommended to select MCAST type when using the Multicast function.
Latency	Set the live view performance to Shortest Delay, Auto, Fluent or Custom. For Custom, you can set the frame rate for live view.
Enable Meta Data Overlay	Enable this option to detect real-time alarm such as motion detection. The area which detected the alarm will be highlighted as green.
Display POS Information	Enable the function, feature information of the detected target is dynamically displayed near the target in the live image. The feature information of different functions are different. For example, ID and waiting time for Queue Management, height for People Counting, etc.
Snapshot Image Format	Specifies the snapshot format as JPEG or BMP.
2. Record File Settings	
Video File Size	Specifies the maximum file size. Options include: 256 MB, 512 MB, and 1G.
Save Video Files to	Specifies the directory for recorded files.
Save Downloaded Files to	Specifies the directory for downloaded files.
3. Snapshot and Clip Settings	
Save Video In Live View To	Specifies the directory for saving snapshots in live view mode.
Save Clips During Playback To	Specifies the directory for saving snapshots in playback mode.
Save Clips To	Specifies the directory for saving video clips in playback mode.

Configuration

Use the **Configuration** window to configure the camera system, network, video audio, alarms, users, transactions and other parameters such as upgrading the firmware. See Figure 3 on page 15 for descriptions of the configuration folders available.

Figure 3: Configuration window (Device Information window selected)

truVision IP Camera

Live View Playback Picture Application Log **Configuration**

▼ Local Configuration
 ▼ Browser Configuration
 ▼ Camera Configuration
 ① ▶ System
 ② ▶ Security
 ③ ▶ Network
 ④ ▶ Video/Audio
 ⑤ ▶ Image
 ⑥ ▶ Alarm/Event
 ⑦ ▶ Storage
 ⑧ ▶ People Counting
 ⑨ ▶ Heat Map Configuration
 ⑩ ▶ Intersection Analysis

Basic Information

Device Name: IP CAMERA

Device No.: 88

Model: TVF-5201

Serial No.: TVF-520120190529AAWR23455356

Firmware Version: V16.1 FP1

Encoding Version: V7.3 build 190524

Web Version: V4.0.53 build 190325

Plugin Version: V3.0.6.2601

Number of Channels: 1

Number of HDDs: 1

Number of Alarm Input: 1

Number of Alarm Output: 1

Firmware Version Property: C-R-H3-0

Save

Parameters	Description
1. System	Displays the basic device information including serial number and the current firmware version, time settings, RS-485 serial port parameters, maintenance, and about the system. See pages 16 and 17 for further information.
2. Security	Defines who can use the camera, their passwords and access privileges, RTSP authentication, IP address filter, and telnet access.
3. Network	Defines the network parameters required to access the camera over the internet. See page 19 for further information.
4. Video/Audio	Defines recording parameters. See page 21 for further information.
5. Image	Defines the image parameters, OSD settings, overlay text, and privacy masking. See page 26 for further information.
2. Alarm/Event	Defines motion detection, tamper-proof, alarm input/output, exception and snapshot configuration. See pages 36 to 54 for further information.
3. Storage	Defines recording schedule, storage management and NAS configuration. See pages 56 to 61 for further information.
8. People Counting	Defines the rule of people counting, upload data and advanced setting. See page “People counting” on page 62 for further information.
9. Heat Map Configuration	Defines the parameters and generates reports for the heat map function. See page “Heat map” on page 65 for further information.

Parameters	Description
10 Intersection Analysis	Intersection Analysis is used to monitor the human flow in an intersection-like scene. See “Intersection analysis” on page 67 for further information.

Defining the system time

NTP (Network Time Protocol) is a protocol for synchronizing the clocks of network devices, such as IP cameras and computers. Connecting network devices to a dedicated NTP time server ensures that they are all synchronized.


To define the system time and date:

1. Click **Configuration > System > Time Settings**.

2. From the **Time Zone** drop-down menu, select the time zone that is the closest to the camera's location.
3. Under **Time Sync**, select one of the options for setting the time and date:

Synchronize with an NTP server: Select **NTP** and enter the server NTP address. The time interval can be set from 1 to 10080 minutes.

- Or -

Set manually: Enable the **Manual Time Sync** function and then click  to set the system time from the pop-up calendar.

Note: You can also select the **Sync with computer time** check box to synchronize the time of the camera with the time of your computer.

4. Select **Enable DST** to enable the DST function, and set the start and end dates of the DST period.
5. Click **Save** to save changes.

Defining RS-485 settings

The RS-485 serial port is used to control extra devices that support the 485 protocol (Pelco D or Pelco P), such as PTZ devices, lighting devices or other devices. You can also connect it to an analog PTZ camera, using a 360° camera to control PTZ movement.

You need to configure these parameters before connecting the camera to any devices.

To set up RS-485 settings:

1. Click **Configuration > System > RS485**.



The screenshot shows the 'truVision IP Camera' configuration web interface. The top navigation bar includes 'Live View', 'Playback', 'Picture', 'Application', 'Log', and 'Configuration' (which is highlighted in green). On the left, a sidebar menu lists various configuration categories: 'Local Configuration', 'Browser Configuration', 'Camera Configuration', 'System' (expanded), 'Basic Information', 'Time Settings', 'RS-485' (highlighted in green), 'Maintenance', 'About', 'Security', 'Network', 'Video/Audio', 'Image', 'Alarm/Event', 'Storage', 'People Counting', 'Heat Map Configuration', and 'Intersection Analysis'. The main content area is titled 'RS-485' and contains the following settings:

Parameter	Value
Baud Rate	9600
Data Bit	8
Stop Bit	1
Parity	None
Flow Ctrl	None
PTZ Protocol	PELCO-D
PTZ Address	0

At the bottom of the settings area is a 'Save' button with a floppy disk icon.

2. Select the RS-485 port parameters.

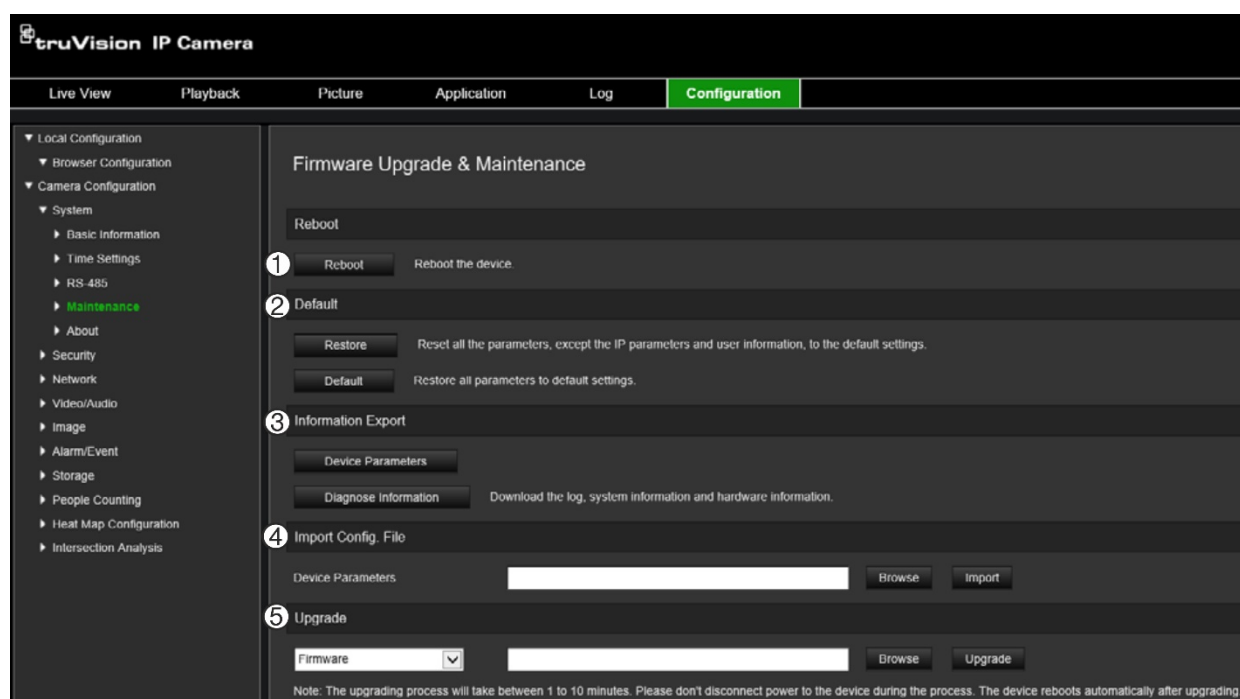
Note: The Baud Rate, PTZ Protocol, and PTZ Address parameters should be exactly the same as the PTZ camera parameters.

3. Click Save to save changes.

Maintenance

The upgrade and maintenance interface allows you to process the operations, including reboot, partly restore, restore to default, export/import the configuration files, and upgrade the device.

Figure 4: Maintenance window

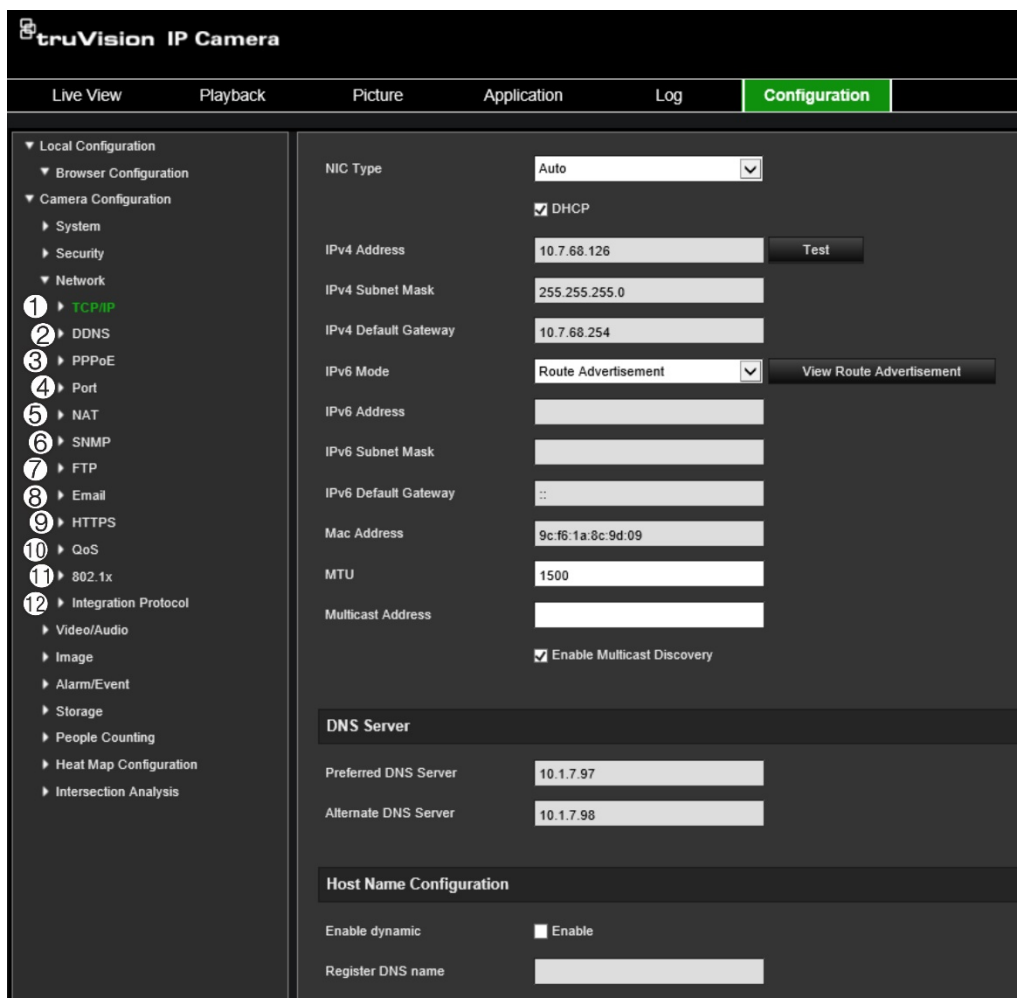


Parameters		Description	
1.	Reboot	Reboot the device	
2.	Default	Restore	Reset all the parameters, except the IP parameters and user information, to the default settings.
		Default	Restore all the parameters to the factory default. Notes: <ul style="list-style-type: none"> After restoring the default settings, the IP address is also restored to the default IP address, please be careful for this action. For camera that supports Wi-Fi, wireless dial, or WLAN function, Restore action does not restore the related settings of mentioned functions to default.
3	Information Export	Device Parameters	Click to export the current configuration file of the camera. This operation requires admin password to proceed
		Diagnose Information	Click to download log and system information.
4	Import Config File	Configuration file is used for the batch configuration of the cameras. Note: You need to reboot the camera after importing configuration file	
5	Upgrade	Upgrade the device. Note: The upgrading process will take between 1 and 10 minutes. Please do not disconnect power of the camera during the process. The camera reboots automatically after upgrade.	

Configuring the network settings

Accessing the camera through a network requires that you define certain network settings. Use the “Network” folder to define the network settings. See Figure 5 below for further information.

Figure 5: Network window (TCP/IP window shown)



Menu tabs	Description
1. TCP/IP	<p>NIC Type: Enter the NIC type. Default is Auto. Other options include: 10M Half-dup, 10M Full-dup, 100M Half-dup and 100M Full-dup.</p> <p>DHCP: Enable to automatically obtain an IP address and other network settings from that server.</p> <p>IPv4 Address: Enter the IPv4 address of the camera.</p> <p>IPv4 Subnet Mask: Enter the IPv4 subnet mask.</p> <p>IPv4 Default Gateway: Enter the IPv4 gateway IP address.</p> <p>IPv6 Mode: Enter the IPv6 mode: Manual, DHCP or Router Advertisement.</p> <p>IPv6 Address: Enter the IPv6 address of the camera.</p> <p>IPv6 Subnet Prefix Length: Enter the IPv6 prefix length.</p> <p>IPv6 Default Gateway: Enter the IPv6 gateway IP address.</p> <p>Mac Address: Enter the MAC address of the devices.</p> <p>MTU: Enter the valid value range of MTU. Default is 1500.</p> <p>Multicast Address: Enter a D-class IP address between 224.0.0.0 to</p>

Menu tabs	Description
	<p>239.255.255.255. Only specify this option if you are using the multicast function. Some routers prohibit the use of multicast function in case of a network storm.</p> <p>Enable Multicast Discovery: Enables the automatic detection of the online network camera via private multicast protocol in the LAN.</p> <p>DNS Server: Specifies the DNS server for your network.</p> <p>Host name Configuration: Specifies the DNS name the user can define when the option is enabled.</p>
2. DDNS	<p>DDNS is a service that maps Internet domain names to IP addresses. It is designed to support dynamic IP addresses, such as those assigned by a DHCP server.</p> <p>Specify DynDNS, No-IP and ezDDNS.</p> <p>DynDNS (Dynamic DNS): Manually create your own host name. You will first need to create a user account using the hosting web site, DynDDNS.org.</p> <p>ezDDNS: Activate the DDNS auto-detection function to set up a dynamic IP address. The server is set up to assign an available host name to your recorder.</p> <p>No-IP: Enter the address of the NO-IP, host name for your camera, the port number, your user name and password.</p> <p>See page 21 for setup information.</p>
3. PPPoE	Retrieves a dynamic IP address. See page 22 for setup information.
4. Port	<p>HTTP Port: The HTTP port is used for remote internet browser access. Enter the port used for the Internet Explorer (IE) browser. Default value is 80.</p> <p>RTSP Port: RTSP (Real Time Streaming Protocol) is a network control protocol designed for use in entertainment and communications systems to control streaming media servers. Enter the RTSP port value. The default port number is 554.</p> <p>HTTPS Port: HTTPS (Hyper Text Transfer Protocol Secure) allows video to be securely viewed when using a browser. Enter the HTTPS port, value. The default port number is 443.</p> <p>Server Port: This is used for remote client software access. Enter the server port value. The default port number is 8000.</p> <p>Alarm Host IP: Specifies the IP address of the alarm host.</p> <p>Alarm Host Port: Specifies the port of the alarm host.</p> <p>See page 22 for setup information.</p>
5. NAT	A NAT (Network Address Translation) is used for network connection. Select the port mapping mode: auto or manual. See page 22 for setup information.
6. SNMP	SNMP is a protocol for managing devices on networks. Enable SNMP to get camera status and parameter related information. See page 22 for setup information.
7. FTP	Enter the FTP address and folder to which snapshots of the camera can be uploaded. See page 23 for setup information.
8. Email	Enter the email address to which messages are sent when an alarm occurs. See page 23 for setup information.
9. HTTPS	Specifies authentication of the web site and its associated web server, which protects against Man-in-the-middle attacks.

Menu tabs	Description
10. QoS	QoS (Quality of Service) can help solve the network delay and network congestion by configuring the priority of data sending. Enable the option in order to solve network delay and network congestion by configuring the priority of data sending. See page 25 for setup information.
11. 802.1.X	When the feature is enabled, the camera data is secured and user authentication is needed when connecting the camera to the network. See page 25 for setup information.
12. Integration protocol	If you need to access to the camera through the third party platform, you can enable STD-CGI function. And if you need to access to the device through ONVIF protocol, you can configure ONVIF user in this interface. Refer to ONVIF standard for detailed configuration rules.

To define the TCP/IP parameters:

1. From the menu toolbar, click **Configuration > Network > TCP/IP**.
2. Configure the NIC settings, including the NIC Type, IPv4 settings, IPv6 settings, MTU settings, and Multicast Address.
3. If the DHCP server is available, select **DHCP**.
4. If the DNS server settings are required for some applications (e.g., sending email), you should configure the **Preferred DNS Server or Alternate DNS Server**.
5. Click **Save** to save changes.

To define the DDNS parameters:

1. From the menu toolbar, click **Configuration > Network > DDNS**.
2. Select **Enable DDNS** to enable this feature.
3. Select **DDNS Type**. There are three options are available: DynDNS, ezDDNS and NO-IP.
 - **DynDNS:** Enter the DNSS server address, members.ddns.org (which is used to notify DDNS about changes to your IP address), the host name for your camera, the port number (443 (HTTPS)), and your user name and password used to log into your DDNS account. The domain name displayed under “Host Name” is that which you created on the DynDNS web site.
 - **ezDDNS:** Enter the host name. It will automatically register it online. You can define a host name for the camera. Make sure you entered a valid DNS server in the network settings and have the necessary ports forwarded in the router (HTTP, Server port, RSTP port).
 - **NO-IP:** Enter the address of the NO-IP, host name for your camera, the port number, your user name and password.
4. Click **Save** to save changes.

To define the PPPoE parameters:

1. From the menu toolbar, click **Configuration > Network > PPPoE**.
2. Select **Enable PPPoE** to enable this feature.
3. Enter User Name, Password, and Confirm password for PPPoE access.
4. Click **Save** to save changes.

To define the port parameters:

1. From the menu toolbar, click **Configuration > Network > Port**.
2. Set the HTTP port, RTSP port, HTTPS port and Server port of the camera.

HTTP Port: The default port number is 80, and it can be changed to any port No. which is not occupied.

RTSP Port: The default port number is 554. It can be changed to any port number in the range from 1 to 65535.

HTTPS Port: The default port number is 443. It can be changed to any port number that is not occupied.

Server Port: The default server port number is 8000. It can be changed to any port number in the range from 2000 to 65535.

3. Enter the IP address and port if you want to upload the alarm information to the remote alarm host. Also select the **Notify Alarm Recipient** option in the normal Linkage of each event page.
4. Click **Save** to save changes.

To set up the NAT parameters:

1. Click **Configuration > Network > NAT**.
2. Select the **NAT** check box.
3. Select **Port Mapping Mode** to be Auto or Manual. When you choose Manual mode, you can set the external port as you want.
4. Click **Save** to save changes.

To define the SNMP parameters:

1. From the menu toolbar, click **Configuration > Network > SNMP**.
2. Select the corresponding version of SNMP: v1 or v2c.
3. Configure the SNMP settings. The configuration of the SNMP software should be the same as the settings you configure here.
4. Click **Save** to save changes.

Note: Before setting the SNMP, please download the SNMP software and manage to receive the camera information via the SNMP port. By setting the Trap Address, the camera can send the alarm event and exception messages to the surveillance center. The SNMP version you select should be the same as that of the SNMP software.

To define the FTP parameters:

1. From the menu toolbar, click **Configuration > Network > FTP**.
2. Configure the FTP settings, including server address, port, user name, password, directory, and upload type.

Anonymous: Select the check box to enable the anonymous access to the FTP server.

Directory: In the Directory Structure field, you can select the root directory, Main directory and Subdirectory. When the Main directory is selected, you have the option to use the Device Name, Device Number or Device IP for the name of the directory; and when the Subdirectory is selected, you can use the Camera Name or Camera No. as the name of the directory.

Upload Picture: To enable uploading the snapshots to the FTP server.

3. Click **Save** to save changes.

To set up the email parameters:

1. In **Configuration > Network**, click the **Email** tab to open its window.

The screenshot shows the 'Configuration' window of a TruVision IP Camera. The 'Email' tab is selected. The left sidebar lists various configuration categories, with 'Email' highlighted under the 'Network' section. The main area contains the following settings:

- Sender:** Text input field with a green checkmark.
- Sender's Address:** Text input field with a green checkmark.
- SMTP Server:** Text input field with a red error message: "The item cannot be empty."
- SMTP Port:** Text input field with the value "25" and a green checkmark.
- E-mail Encryption:** Dropdown menu set to "None".
- Attached Image:** Check box (unchecked).
- Interval:** Text input field with the value "2" and a unit "s".
- Authentication:** Check box (unchecked).
- User Name:** Text input field.
- Password:** Text input field.
- Confirm:** Text input field.

Below these settings is a table for configuring email receivers:

Receiver		
No.	Receiver	Receiver's Address
1		
2		
3		

At the bottom of the configuration area are two buttons: "Test" and "Save".

2. Configure the following settings:

Sender: The name of the email sender.

Sender's Address: The email address of the sender.

SMTP Server: The SMTP Server, IP address or host name.

SMTP Port: The SMTP port. The default is 25.

E-mail Encryption: Encrypt via SSL, TLS. NONE is default.

Attached Snapshot: Select the check box of **Attached Snapshot** if you want to send emails with attached alarm images.

Interval: This is the time between two actions of sending attached images.

Authentication: If your email server requires authentication, select this check box to use authentication to log in to this server. Enter the login user name and password.

User Name: The user name to log in to the server where the images are uploaded.

Password: Enter the password.

Confirm: Confirm the password.

Receiver1: The name of the first user to be notified.

Receiver's Address1: The email address of user to be notified.

Receiver2: The name of the second user to be notified.

Receiver's Address2: The email address of user to be notified.

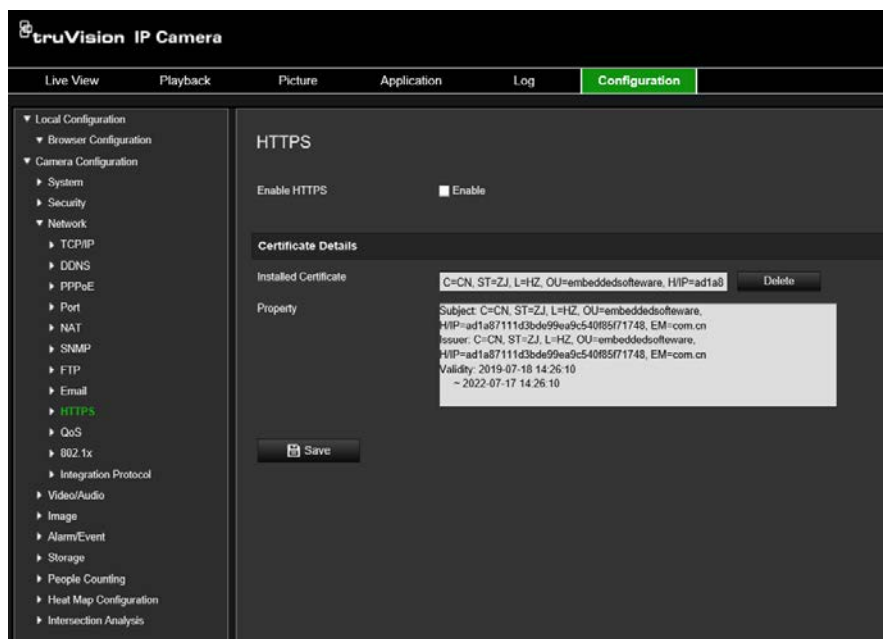
Receiver3: The name of the second user to be notified.

Receiver's Address3: The email address of user to be notified.

3. Click **Test** to test the email parameters set up.
4. Click **Save** to save changes.

To set up the HTTPS parameters:

1. In the **Network** folder, click the **HTTPS** tab to open its window.



2. To create a self-signed certificate:

Click the **Create** button beside “Create Self-signed Certificate”. Enter the country, host name/IP, validity and the other information requested.

Click **OK** to save the settings.

-Or-

To create a certificate request:

Click the **Create** button beside “Create Certificate Request”. Enter the country, host name/IP and the other information requested.

3. Click **OK** to save the settings. Download the certificate request and submit it to the trusted certificate authority for signature, such as Symantec or RSA. After receiving the signed valid certificate, upload the certificate to the device

To define the QoS parameters:

1. From the menu toolbar, click **Configuration > Network > QoS**.
2. Configure the QoS settings, including Video / Audio DSCP, Event / Alarm DSCP and Management DSCP. The valid value range of the DSCP is 0-63. The bigger the DSCP value is the higher the priority is.
3. Click **Save** to save changes.

To define the 802.1X parameters:

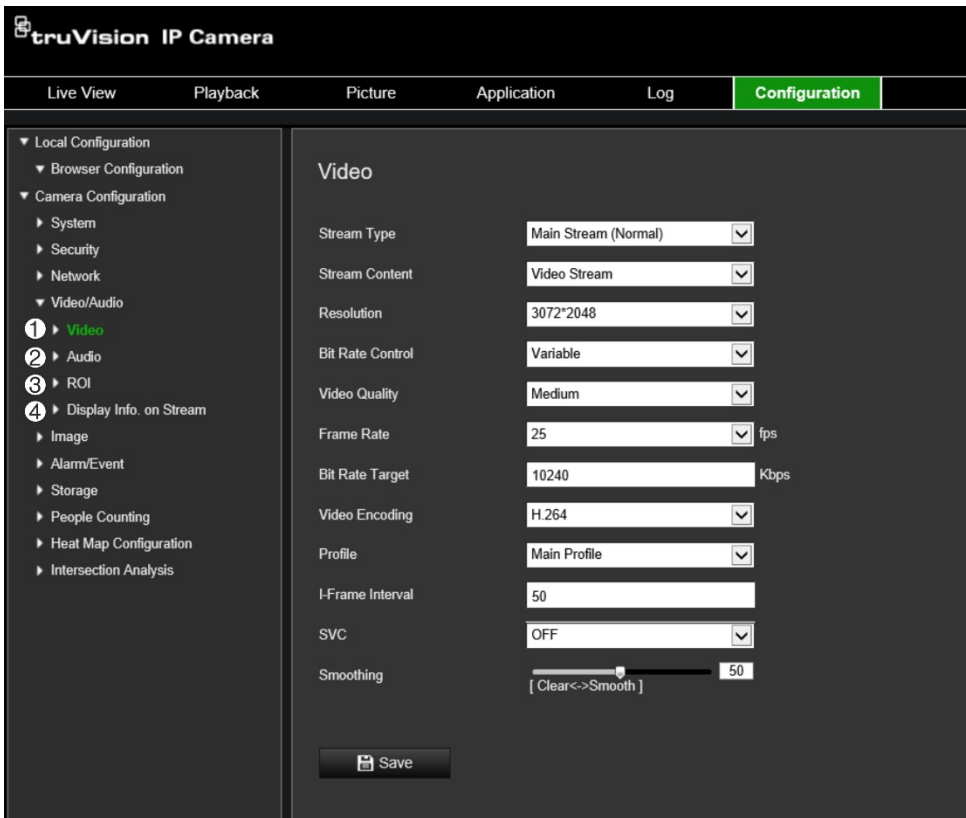
1. From the menu toolbar, click **Configuration > Network > 802.1X**.
2. Select **Enable IEEE 802.1X** to enable the feature.
3. Configure the 802.1X settings, including EAPOL version, user name, and password. The EAPOL version must be identical with that of the router or the switch.
4. Click **Save** to save changes.

Note: The switch or router to which the camera is connected must also support the IEEE 802.1X standard, and a server must be configured. Please apply and register a user name and password for 802.1X in the server.

Recording parameters

You can adjust the video and audio recording parameters to obtain the picture quality and file size best suited to your needs. Figure 6 below list the video and audio recording options you can configure for the camera.

Figure 6: Video/Audio Settings menu (Video tab shown)

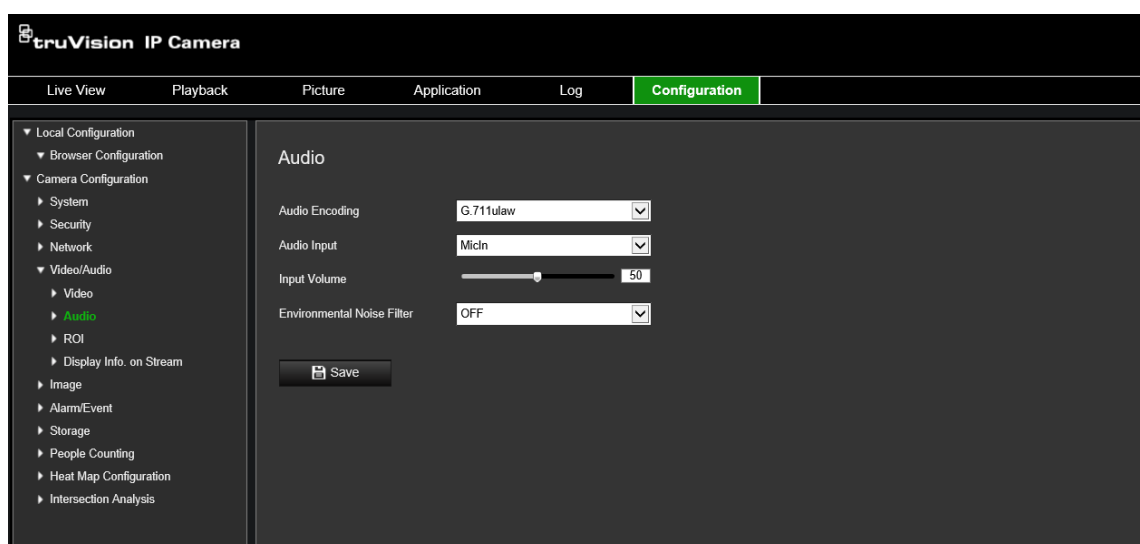


Tab	Parameter descriptions
1. Video	<p>Stream Type: Specifies the streaming method used. Options include: Main Stream (Normal), Sub Stream. Note: The Third stream is only available when the this function is enabled in System > System Service</p> <p>Stream Content: Specifies the stream type you wish to record. Select Video Stream to record video stream only. Select Video&Audio to record both video and audio streams. Note: Video&Audio is only available for those camera models that support audio.</p> <p>Resolution: Specifies the recording resolution. A higher image resolution provides a higher image quality but also requires a higher bit rate. The resolution options listed depend on the type of camera and on whether main sub or third stream is being used. Note: Resolutions can vary depending on the camera model.</p>

Tab	Parameter descriptions
	<p>Bit Rate Control: Specifies whether variable or fixed bit rate is used. Variable produces higher quality results suitable for video downloads and streaming. Default is Constant.</p> <p>Video Quality: Specifies the quality level of the image. It can be set when variable bit rate is selected. Options include: Lowest, Lower, low, Medium, Higher and Highest.</p> <p>Frame Rate: Specifies the frame rate for the selected resolution. The frame rate is the number of video frames that are shown or sent per second.</p> <p>Note: The maximum frame rate depends on the camera model and selected resolution. Please check the camera specifications in its datasheet.</p> <p>Video Encoding: Specifies the video encoder used.</p> <p>Profile: Different profile indicates different tools and technologies used in compression. Options include: High Profile, Main Profile.</p> <p>I Frame Interval: A video compression method. It is strongly recommended not to change the default value 50.</p> <p>SVC: Scalable Video Coding is an extension of the H.264/AVC standard. Select OFF / ON to disable / enable the SVC function. Select Auto, and the device will automatically extract frames from the original video when the network bandwidth is insufficient.</p> <p>Smoothing: Adjust the smoothness of the stream.</p>
2. Audio	<p>Audio Encoding: G.722.1, G.711ulaw, G.711alaw, MP2L2, G.726 and PCM are optional.</p> <p>Audio Input: Mic In and Line In are selectable for the connected microphone and pickup respectively</p> <p>Input Volume: Specifies the volume from 0 to 100.</p> <p>Environmental Noise Filter: Set it as OFF or ON. When you set the function on, the noise detected can be filtered.</p>
3. ROI	<p>Enable to assign more encoding resources to the region of interest (ROI) to increase the quality of the ROI whereas the background information is less focused.</p>
4. Display Info. On Stream	<p>When Dual-VCA mode is enabled, the camera sends video analytics results (metadata) to an NVR or other platforms to generate a VCA alarm.</p>

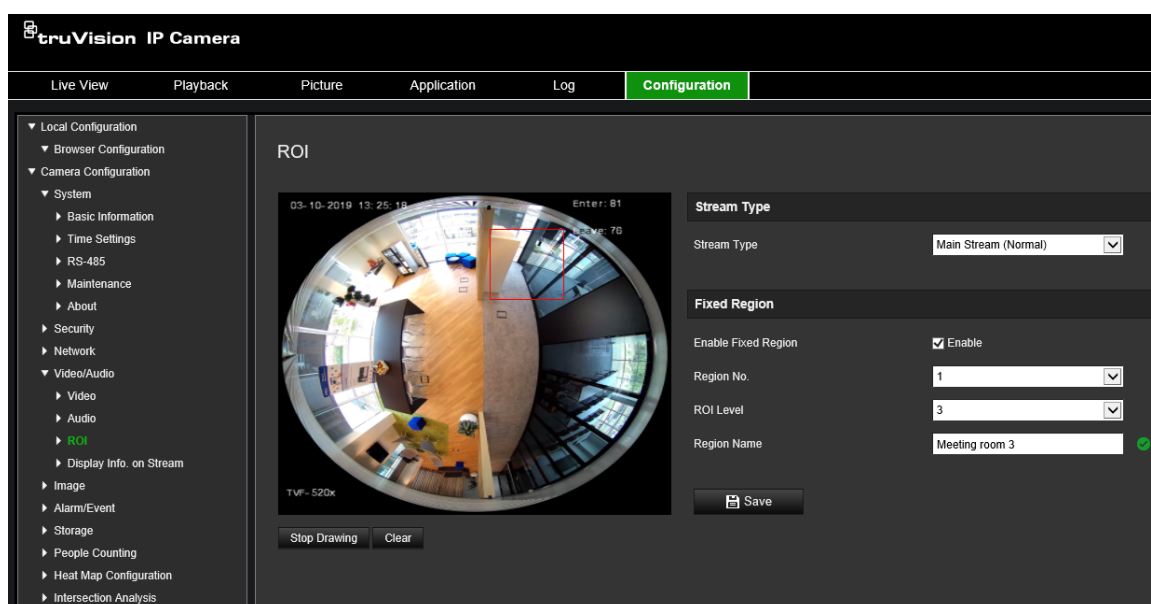
To configure audio settings:

From the menu toolbar, click **Configuration > Video/Audio > Audio**.



To configure ROI settings:

1. From the menu toolbar, click **Configuration > Video/Audio > ROI**.



2. Draw the region of interest on the image. Up to four regions can be drawn.
3. Choose the stream type to set the ROI encoding.
4. Enable **Fixed Region** to manually configure the area.

Region No.: Assign a number to the region.

ROI Level: Choose the image quality enhancing level.

Region Name: Set the desired region name.

Dual-VCA (Video Content Analysis)

When Dual-VCA mode is enabled, the camera sends video analytics results (metadata) to an NVR or other platforms to generate a VCA alarm.

For example, with an TruVision NVR (please check TruVision website for the latest NVR models supporting this feature), you can draw a virtual line in the NVR playback window, and search the objects or people crossing this virtual line.

Note: Only cross line and intrusion detection can support dual-VCA mode.

To define dual-VCA parameters:

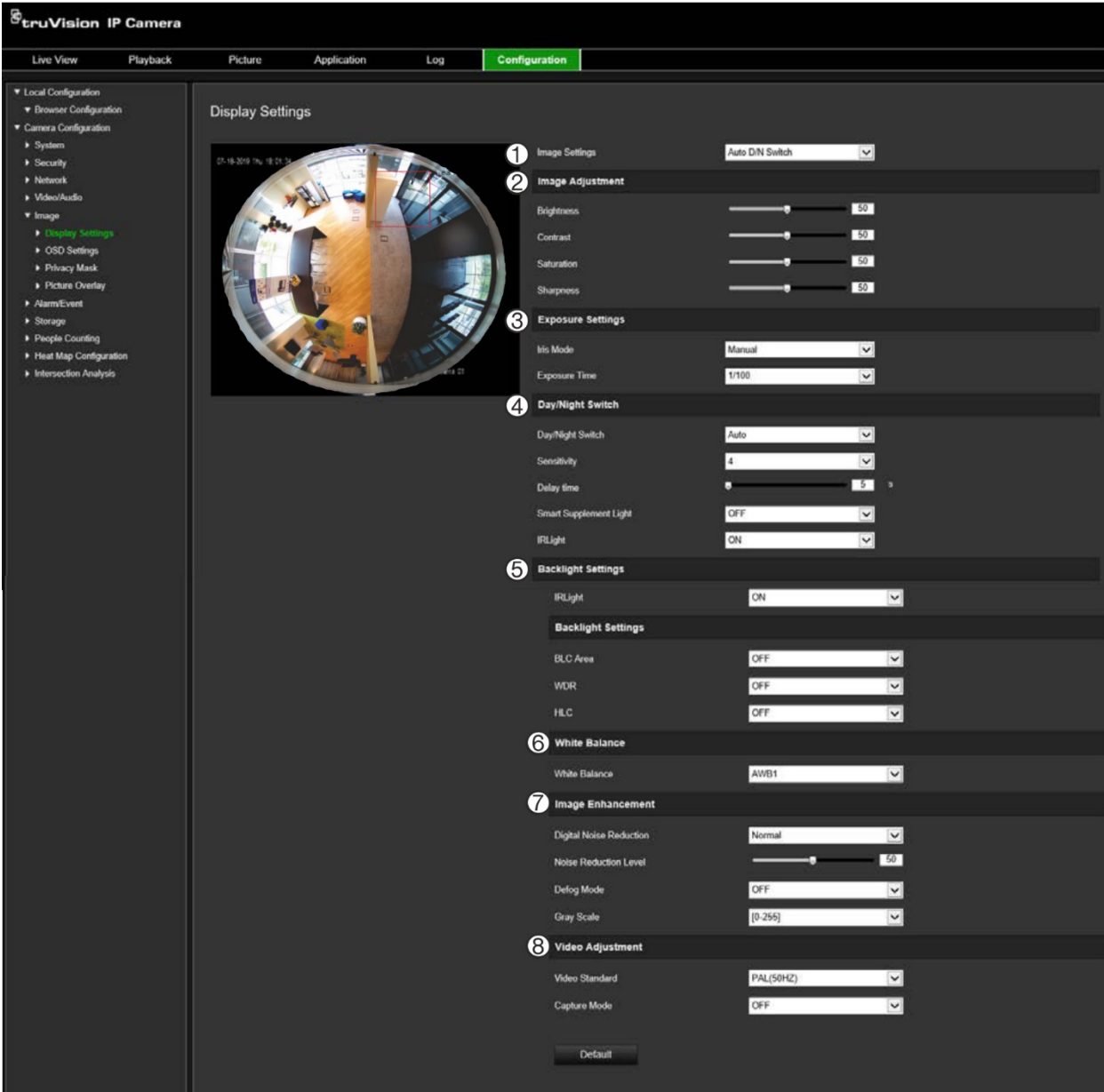
1. In the **Video/Audio** panel, click the **Display Info. On Stream** tab to open its window.
2. Select the check box to enable Dual-VCA.
3. Click **Save** to save changes.

Video image

You may need to adjust the camera image depending on the camera model or location background in order to get the best image quality. You can adjust the brightness, contrast, saturation, hue, and sharpness of the video image. See Figure 7 below for more information.

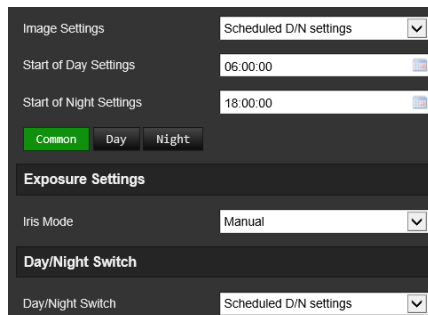
Use this menu to also adjust camera behavior parameters such as exposure time, iris mode, video standard, day/night mode, image flip, WDR, digital noise reduction, white balance, and indoor/outdoor mode.

Figure 7: Camera image settings menu – Display Settings tab



Parameter	Description
1. Image Settings	
Auto D/N Switch	<p>The camera automatically switches between day and night modes. All image settings remain the same for both modes.</p> <p>The image settings are: Image Adjustment, Exposure Settings, Day/Night Switch, Backlight Settings, White Balance, Image Enhancement, and Video Adjustment.</p> <p><i>Common:</i> Set each image parameter individually for D/N switch.</p> <p><i>Default:</i> Only use default settings.</p>
Custom 24-h settings	<p>Customize the camera switch schedule for 24-hour settings.</p> <p>There are three tabs to configure the Custom 24-hour settings: <i>Common, Day, Night.</i></p> <p>See “Scheduled D/N Switch” below for further information.</p>

Parameter	Description
Scheduled D/N Switch	<p>The camera switches between the day and night modes according to the schedule configured (see figure below). The start and end times shown are for day mode. The other time period is for night mode.</p> <p>There are three tabs to configure the day/night settings:</p> <p>Common: The settings are identical for both day and night modes for Exposure Settings, Day/Night Switch, and Video Adjustment.</p> <p>Day: Image Adjustment, Exposure Settings, Backlight Settings, White Balance, and Image Enhancement for day mode only.</p> <p>Night: Image Adjustment, Exposure Settings, Backlight Settings, White Balance, and Image Enhancement for night mode only.</p>



2. Image Adjustment

Brightness, Contrast, Saturation, Sharpness	Modify the different elements of picture quality by adjusting the values for each of parameter.
---	---

3. Exposure Settings

Iris Mode	Only <i>Manual iris mode</i> .
Exposure Time	<p>The exposure time controls the length of time that the aperture is open to let light into the camera through the lens.</p> <p>Select a higher value if the image is dark and a lower value to see fast moving objects.</p>

4. Day/Night Switch

Day/Night Switch	<p>Defines whether the camera is in day or night mode. The day (color) option could be used, for example, if the camera is located indoors where light levels are always good.</p> <p>Select one of the options:</p> <p>Day: Camera is always in day mode.</p> <p>Night: Camera is always in night mode.</p> <p>Auto: The camera automatically detects which mode to use.</p> <p>Schedule: The camera switches between day and night modes according to the configured time period.</p> <p>Triggered by Alarm Input: The camera switches to day or night mode after an alarm is triggered.</p>
Sensitivity	<p>Only available when <i>Auto D/N switch</i> mode is selected. It defines the sensitivity of the switch between day and night.</p> <p>Set it between 0 and 7.</p>
Delay Time	<p>Only available when <i>Auto D/N switch</i> mode is selected. The filtering time refers to the interval time between switchover the day/night switch.</p> <p>Set it between 5 and 120 s.</p>

Parameter	Description
Smart Supplement Light	When enabled, it can avoid over exposure issue.
IR Light	<p>Select On/OFF to Enable/disable IR.</p> <p>On: The IR LEDs are ON when the camera changes to night mode.</p> <p>Off: The IR LEDs are OFF when the camera changes to night mode</p> <p>Note: The IR LEDs are always OFF in day mode.</p>
5. Backlight Settings	
BLC Area	<p>This function improves image quality when the background illumination is high. It prevents the object in the center of the image from appearing too dark.</p> <p>Select Off, Up, Down, Left, Right, Center, Custom or Auto.</p> <p>When WDR is enabled, BLC cannot be configured.</p>
WDR	When enabled, wide dynamic range (WDR) provides clear images when there is high contrast between light and dark areas in the field of view of the camera. Both bright and dark areas can be displayed in the frame.
HLC	Highlight Compensation is a function that detects if there are any strong sources of light in the image and compensates for exposure in those areas as needed to produce clearer images. Default is Off.
6. White Balance	
White Balance	<p>White balance (WB) tells the camera what the color white looks like. Based on this information, the camera will then continue to display all colors correctly even when the color temperature of the scene changes such as from daylight to fluorescent lighting, for example. Select one of the options:</p> <p>MWB: Manually adjust the color temperature to meet your own requirements.</p> <p>AWB1: Apply for small range of 2500 to 9500K, for environments where the lighting is always stable.</p> <p>Locked WB: Locks the WB to the current environment color temperature.</p> <p>Fluorescent Lamp: For use where there are fluorescent lamps installed near the camera.</p> <p>Incandescent Lamp: For use with incandescent lighting.</p> <p>Warm Light Lamp: For use where the indoor light is warm.</p> <p>Natural Light: For use with natural light.</p>
7. Image Enhancement	
Digital Noise Reduction	<p>Digital noise reduction (DNR) reduces noise, especially in low light conditions, to improve image performance.</p> <p>Select Normal Mode, Advanced Mode, or OFF. Default is Normal.</p>
Noise Reduction Level	Only available when DNR is set to Normal Mode. Set the level of noise reduction in the Normal Mode. Higher value has a stronger noise reduction. Default is 50.
8. Video Adjustment	
Mirror	<p>It mirrors the image so you can see it inversed.</p> <p>Select Left/Right, Up/Down, Center, or OFF. Default is OFF.</p>
Scene Mode	Select indoor or outdoor according to the current environment.

Parameter	Description
Video Standard	Select 50 Hz or 60 Hz. Select the value depending on the video standards; normally 50 Hz for PAL standard and 60 Hz for NTSC standard.
Capture Mode	It's the selectable video input mode to meet the different demands of field of view and resolution. Lens Distortion Correction: Select ON / OFF to enable / disable the lens distortion correction. The distorted image caused by the wide-angle lens can be corrected if this function enabled.

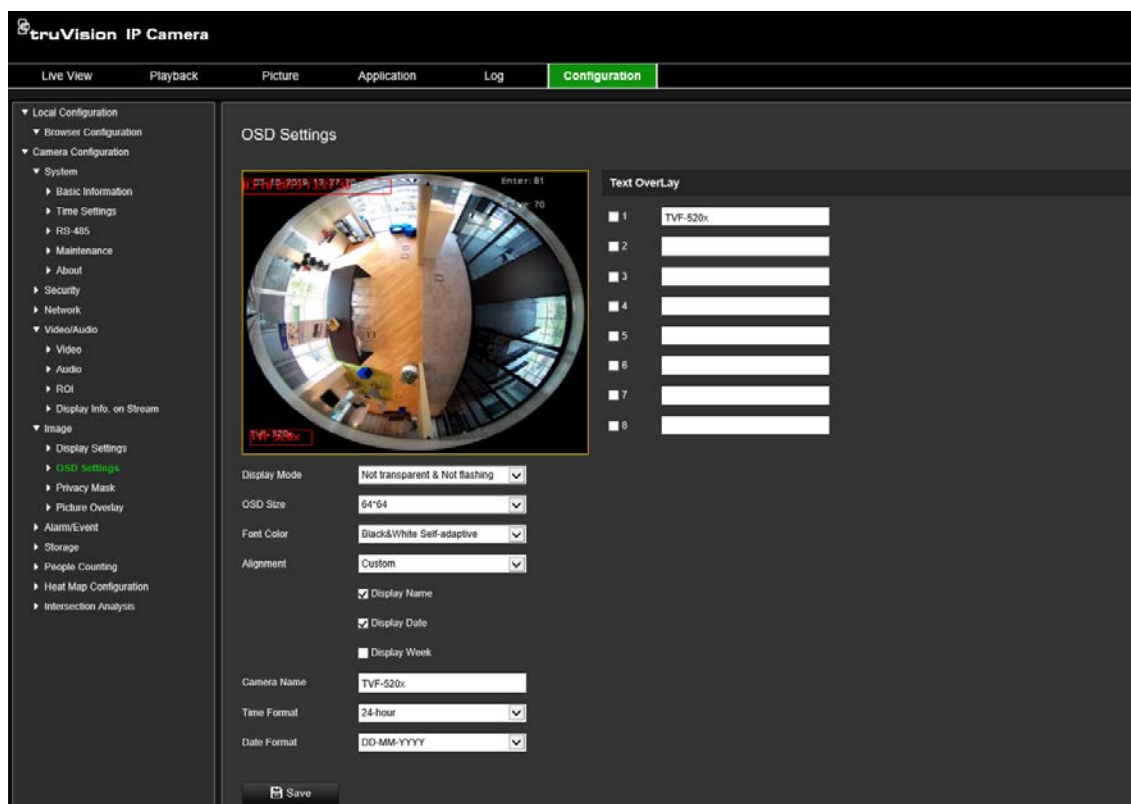
Note: Click the **Default** button to default all the image settings.

OSD (On Screen Display)

In addition to the camera name, the camera also displays the system date and time on screen. You can also define how the text appears on screen.

To position the date/time and name on screen:

1. From the menu toolbar, click **Configuration > Image > OSD Settings**.



2. Select the **Display Name** check box to display the camera's name on screen. You can modify the default name in the text box of **Camera Name**.
3. Select the **Display Date** check box to display the date/time on screen.
4. Select the **Display Week** check box to include the day of the week in the on-screen display.
5. In the **Camera Name** box, enter the camera name.

6. Select the time and date formats from the **Time format** and **Date format** drop-down list boxes.
7. Select a display mode for the camera from the **Display Mode** drop-down list box. Display modes include:
 - **Transparent & Not flashing.** The image appears through the text.
 - **Transparent & Flashing.** The image appears through the text. The text flashes on and off.
 - **Not transparent & Not flashing.** The image is behind the text. This is default.
 - **Not transparent & Flashing.** The image is behind the text. The text flashes on and off.
8. Select the desired OSD size.
9. Select the desired font color.
10. Select the desired alignment (Custom, Align Left or Align Right).
11. Click **Save** to save changes.

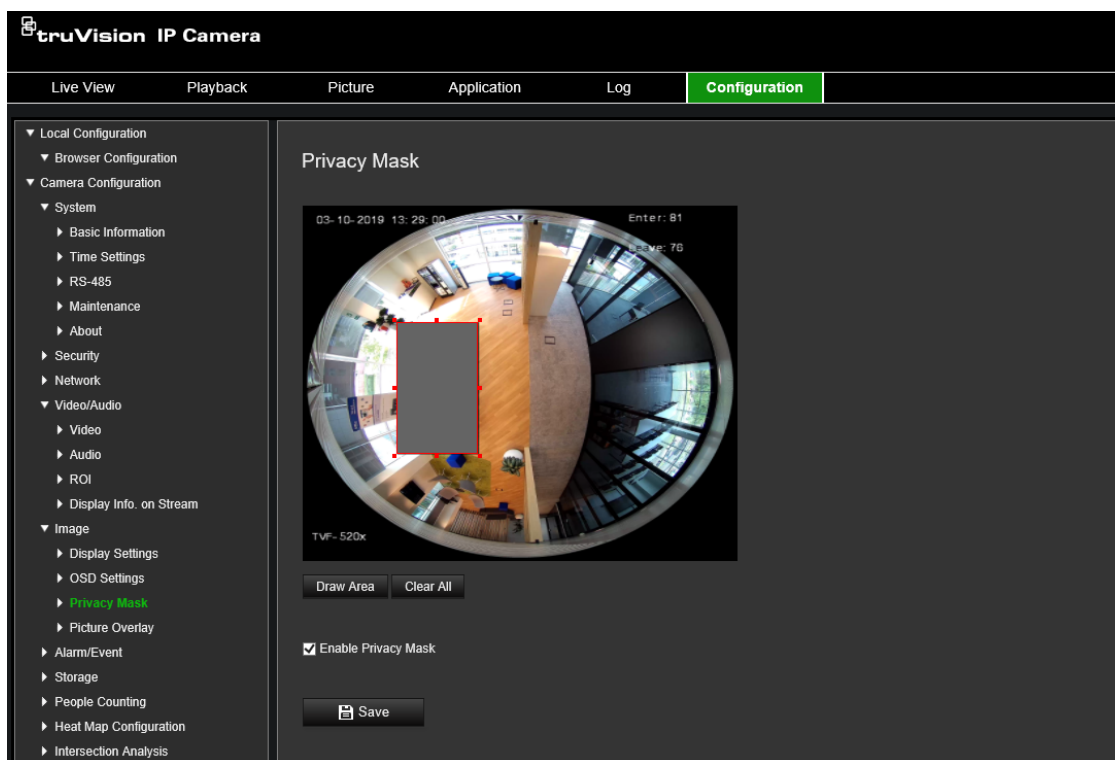
Note: If the display mode sets as transparent, the text varies according the background. With some backgrounds, the text may be not easily readable.

Privacy masks

Privacy masks let you conceal sensitive areas (such as neighboring windows) to protect them from view on the monitor screen and in the recorded video. The masking appears as a blank area on screen. You can create up to four privacy masks per camera.

Note: There may be a small difference in size of the privacy mask area depending on whether local output or the web browser is used.

Figure 8: Camera image settings menu – Privacy mask window



To add privacy mask area:

1. From the menu toolbar, click **Configuration > Image > Privacy Mask**.
2. Select the **Enable Privacy Mask** check box.
3. Click **Draw Area**.
4. Click and drag the mouse in the live video window to draw the mask area.

Note: You are allowed to draw up to four areas on the same image.

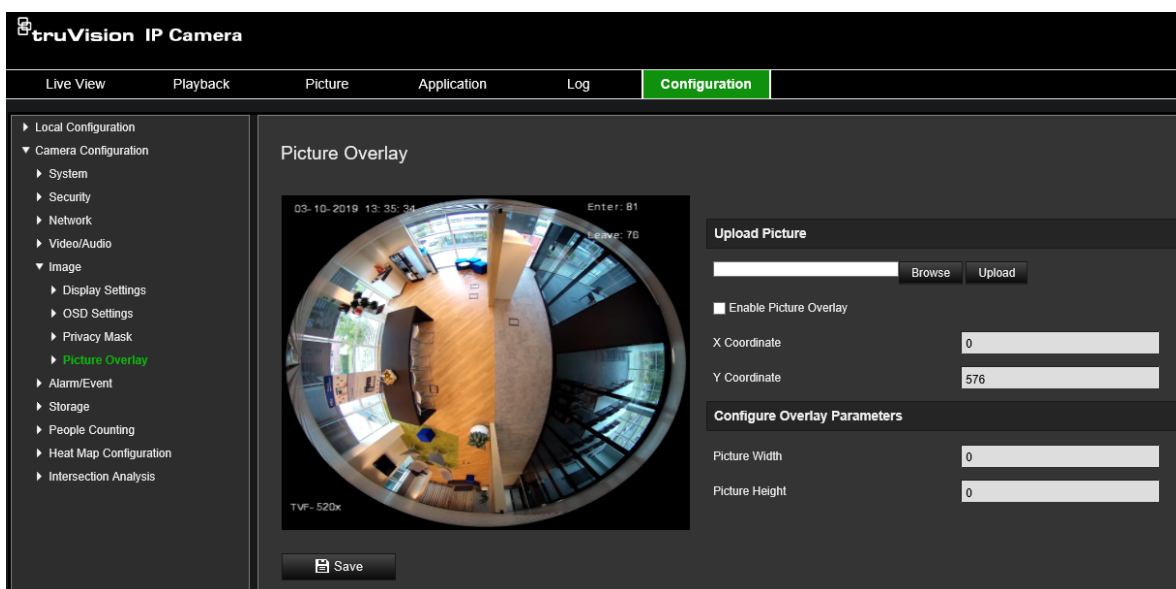
5. Click **Stop Drawing** to finish drawing, or click **Clear All** to clear all of the areas you set without saving them.
6. Click **Save** to save changes.

Picture overlay

Picture overlay enables you to overlay a picture on the image. This function enables a certain enterprise or users to overlay their logo on the image.

To add a picture:

1. From the menu toolbar, click **Configuration > Image > Picture Overlay**.



2. Click **Browse** to select a picture.
3. Click **Upload** to upload it.
4. Select the **Enable Picture Overlay** check box to enable the function.
5. Drag the red rectangle to adjust the position.
6. Click **Save** to save settings.

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

Motion detection alarms

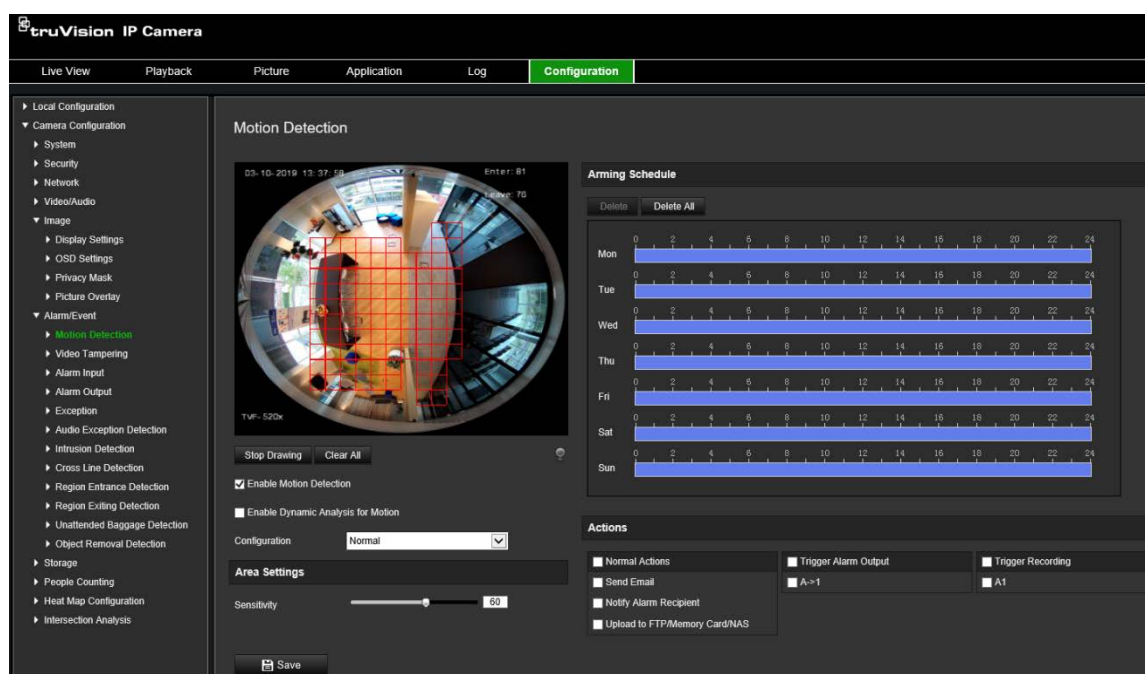
You can define motion detection alarms. A motion detection alarm refers to an alarm triggered when the camera detects motion. However, the motion alarm is only triggered if it occurs during a programmed time schedule.

Select the level of sensitivity to motion as well as the target size so that only objects that could be of interest can trigger a motion recording. For example, the motion recording is triggered by the movement of a person but not that of a cat.

You can define the area on screen where the motion is detected, the level of sensitivity to motion, the schedule when the camera is sensitive to detecting motion as well as which methods are used to alert you to a motion detection alarm.

You can also enable dynamic analysis for motion. When there is motion, the area will be highlighted as green.

Figure 9: Motion detection window



Defining a motion detection alarm requires the following tasks:

1. **Area settings:** Define the on-screen area that can trigger a motion detection alarm and the detection sensitivity level (see Figure 9, item 1).
2. **Arming schedule:** Define the schedule during which the system detects motion (see Figure 9, item 2).
3. **Recording schedule:** Define the schedule during which motion detection can be recorded. See “Recording schedule” on page 56 for further information.
4. **Actions:** Specify the method of response to the alarm (see Figure 9, item 3).
5. **Normal and advanced configuration:** Normal configuration allows you to set the sensitivity level of the motion detection (see Figure 9, item 4). Advanced configuration gives you much more control over how motion is detected. It lets you set the sensitivity level as well as define the percentage of the motion detection area that the object must occupy, select day or night mode, and set up eight differently configured defined areas.

To set up motion detection in normal mode:


1. From the menu toolbar, click **Configuration > Alarm/Event > Motion Detection**.
2. Select the **Enable Motion Detection** check box. Select the **Enable Dynamic Analysis for Motion** check box if you want to see real-time motion events.

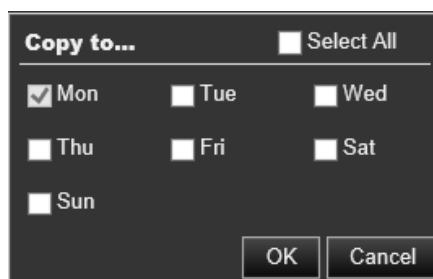
Note: If you do not want the detected object to be marked with the green frame, select **Disable** from Configuration > Local Configuration > Live View Parameters > Enable Meta Data Overlay.

3. Select **Normal** mode from the drop-down list.

- Click **Draw Area**. Click and drag the mouse on the live video image to draw an area sensitive to motion detection.
- Note:** You can draw up to 8 motion detection areas on the same image.
- Click **Stop Drawing** to finish drawing. Click **Clear All** to delete all areas marked and restart drawing.
- Move the **Sensitivity** slider to set the sensitivity of the detection. All areas will have the same sensitivity level.
- Drag and click the time bar to edit the arming schedule.



- Click  to copy the schedule to other days or to the whole week.



- Click **OK** to save changes.
- Specify the **linkage method** when an event occurs. Select one or more response methods for the system when a motion detection alarm is triggered.

Send Email	<p>Send an email to a specified address when there is a motion detection alarm.</p> <p>Note: You must configure email settings before enabling this option. See "To set up the email parameters" on page 23 for further information. If you want to send the event snapshot together with the email, Select the Attached Snapshot option.</p>
Notify Alarm Recipient	<p>Send an exception or alarm signal to remote management software when an event occurs.</p>
Upload to FTP/Memory Card/NAS	<p>Capture the image when an alarm is triggered and upload the snapshot to NAS, Memory Card or FTP server.</p> <p>Note: To upload the snapshot to NAS, you must first configure the NAS settings. See "Configuring NAS settings" on page 61 for further information.</p> <p>To upload the snapshot to an FTP, you must first configure the FTP settings. See "To define the FTP parameters" on page 23 for further information. Enable the Upload Type option.</p> <p>To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also enable Enable Event-triggered Snapshot under the snapshot parameters. See "Snapshot parameters" on page 58 for further information.</p>

Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Select “Select All” or each individual alarm output. Note: This option is only supported by cameras that support alarm output.
Trigger Recording	Triggers the recording to start in the camera.

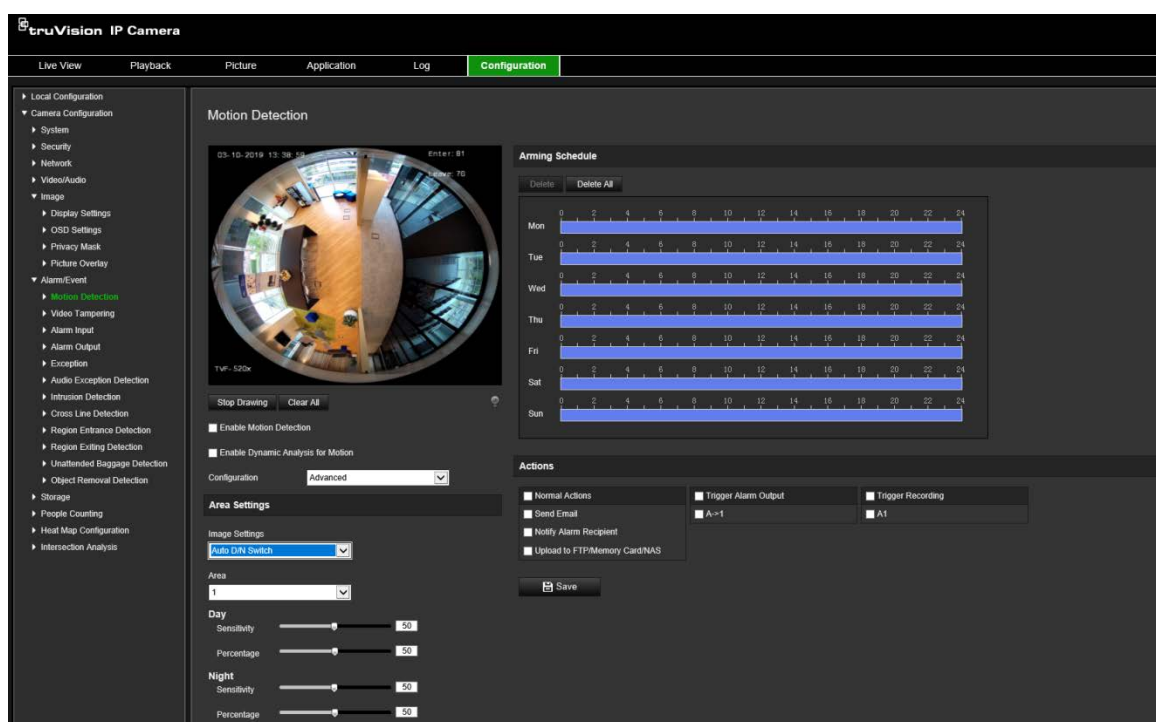
11. Click **Save** to save changes.

To set up motion detection in advanced mode:

1. From the menu toolbar, click **Configuration > Alarm/Event > Motion Detection**.
2. Select the **Enable Motion Detection** check box. Select **Enable Dynamic Analysis for Motion** if you want to see where motion occurs in real-time.

Note: Select Local Configuration > Enable Meta Data Overlay > Disable if you do not want the detected objects displayed with the green rectangles.

3. Select **Advanced** mode from the Configuration drop-down list.



4. Under **Image Settings**, select OFF, Auto D/N Switch or Scheduled D/N settings. Default is OFF.

Auto D/N Switch and Scheduled D/N settings allow you to set different settings for day and night as well as different periods.

5. Select **Area No.** and click **Draw Area**. Click and drag the mouse on the live video image to draw an area sensitive to motion detection.

Note: You can draw up to eight motion detection areas on the same image. **Stop Drawing** shows up after **Draw Area** is clicked.

6. Click **Stop Drawing** to finish drawing. Click **Clear All** to delete all areas marked and restart drawing.

7. Move the **Sensitivity** slider to set the sensitivity of the detection for the selected areas.
8. Move the **Percentage** slider to set the proportion of the object that must occupy the defined area to trigger an alarm.
9. Click **Save** to save the changes for that area.
10. Repeat steps 7 to 9 for each area to be defined.
11. Click **Edit** to edit the arming schedule. See the figure below for the editing interface of the arming schedule.



12. Click **OK** to save changes.
13. Specify the linkage method when an event occurs. Select one or more response methods for the system when a motion detection alarm is triggered.

Send Email	<p>Send an email to a specified address when there is a motion detection alarm.</p> <p>Note: You must configure email settings before enabling this option. See "To set up the email parameters" on page 23 for further information. If you want to send the event snapshot together with the email, select the Attached Snapshot option.</p>
Notify Alarm Recipient	<p>Send an exception or alarm signal to remote management software when an event occurs.</p>
Upload to FTP/Memory Card/NAS	<p>Capture the image when an alarm is triggered and upload the snapshot to NAS, Memory Card or FTP server.</p> <p>Note: To upload the snapshot to NAS, you must first configure the NAS settings. See "Configuring NAS settings" on page 61 for further information.</p> <p>To upload the snapshot to an FTP, you must first configure the FTP settings. See "To define the FTP parameters" on page 23 for further information. Enable the Upload Type option.</p> <p>To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also enable Enable Event-triggered Snapshot under the snapshot parameters. See "Snapshot parameters" on page 58 for further information.</p>

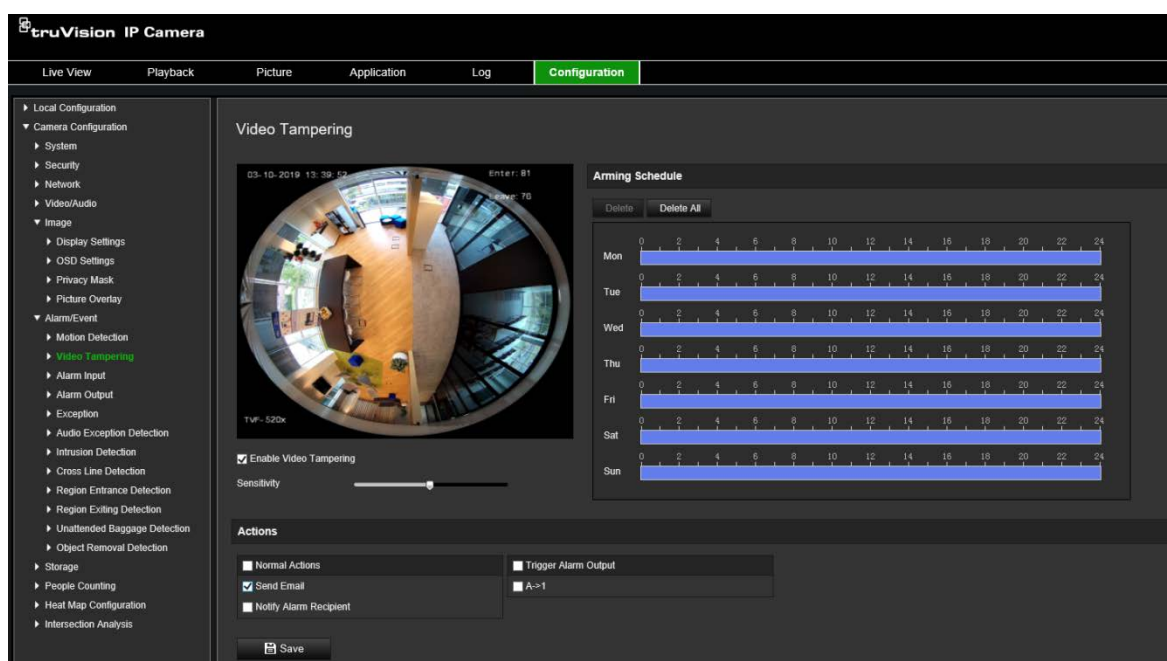
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Check “Select All” or each individual alarm output. Note: This option is only supported by cameras that support alarm output.
Trigger Recording	Triggers the recording to start in the camera.

14. Click **Save** to save changes.

Video tampering

You can configure the camera to trigger an alarm when the lens is covered and to take an alarm response action.

Figure 10: Video Tampering window



To set up tamper-proof alarms:

1. From the menu toolbar, click **Configuration > Alarm Event > Video Tampering**.
2. Select the **Enable Video Tampering** check box.
3. Move the **Sensitivity** slider to set the detection sensitivity.
4. Edit the arming schedule for video tampering. The arming schedule configuration is the same as that for motion detection. See “To set up motion detection” on page 36 for more information.
5. Specify the linkage method when an event occurs. Select one or more response methods for the system when a video tampering is triggered.

Send Email	<p>Send an email to a specified address when there is a motion detection alarm.</p> <p>Note: You must configure email settings before enabling this option. See "To set up the email parameters" on page 23 for further information. If you want to send the event snapshot together with the email, select the Attached Snapshot option.</p>
Notify Alarm Recipient	<p>Send an exception or alarm signal to remote management software when an event occurs.</p>
Trigger Alarm Output	<p>Trigger external alarm outputs when an event occurs. Select "Select All" or each individual alarm output.</p> <p>Note: This option is only supported by cameras that support alarm output.</p>

6. Click **Save** to save changes.

Alarm inputs and outputs

To define the external alarm input:

1. From the menu toolbar, click **Configuration > Alarm/Event > Alarm Input**.
2. Choose the **Alarm Input No.** and the **Alarm Type**. The alarm type can be NO (Normally Open) and NC (Normally Closed). Enter a name for the alarm input.
3. Set the arming schedule for the alarm input. See "To set up motion detection" for more information.
4. Select the check box to select the linkage method.

Send Email	<p>Send an email to a specified address when there is a motion detection alarm.</p> <p>Note: You must configure email settings before enabling this option. See "To set up the email parameters" on page 23 for further information. If you want to send the event snapshot together with the email, select the Attached Snapshot option.</p>
Notify Alarm Recipient	<p>Send an exception or alarm signal to remote management software when an event occurs.</p>
Upload to FTP/Memory Card/NAS	<p>Capture the image when an alarm is triggered and upload the snapshot to NAS, Memory Card or FTP server.</p> <p>Note: To upload the snapshot to NAS, you must first configure the NAS settings. See "Configuring NAS settings" on page 61 for further information.</p> <p>To upload the snapshot to an FTP, you must first configure the FTP settings. See "To define the FTP parameters" on page 23 for further information. Enable the Upload Type option.</p> <p>To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also enable Enable Event-triggered Snapshot under the snapshot parameters. See "Snapshot parameters" on page 58 for further information.</p>
Trigger Alarm Output	<p>Trigger external alarm outputs when an event occurs. Select "Select All" or each individual alarm output.</p> <p>Note: This option is only supported by cameras that support alarm output.</p>

5. Click **Save** to save changes.

To define an alarm output:

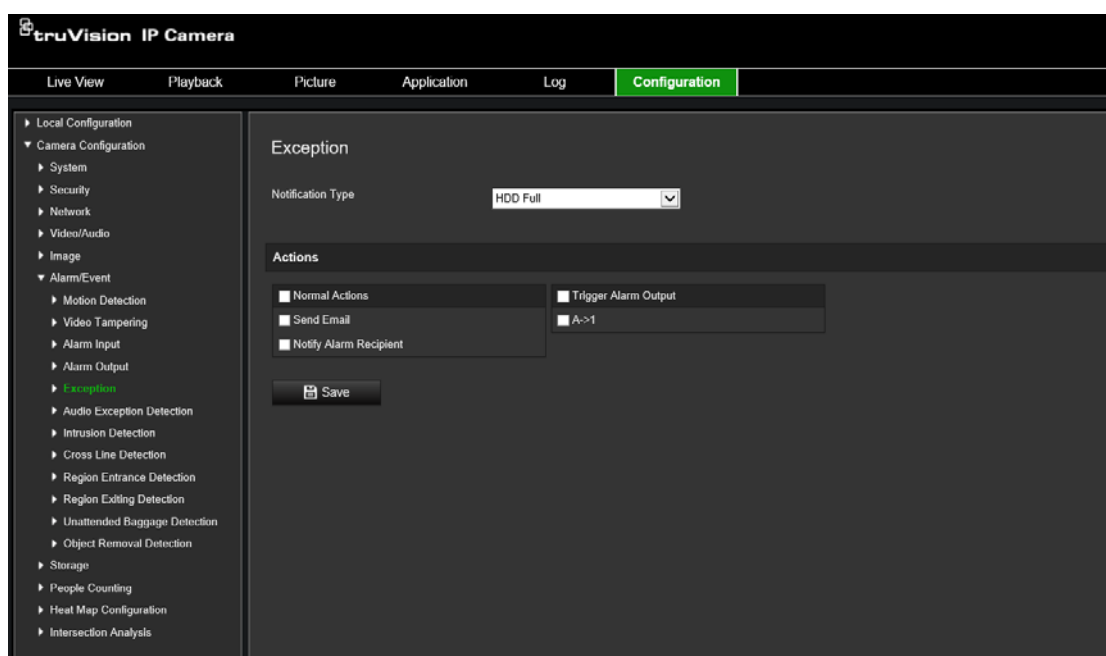
1. From the menu toolbar, click **Configuration > Basic Event > Alarm Output**.
2. Select one alarm output channel from the **Alarm Output** drop-down list. You can also set a name for the alarm output.
3. Set the delay time to 5 s, 10 s, 30 s, 1 min, 2 min, 5 min, 10 min or manual. The delay time refers to the time duration that the alarm output remains in effect after the alarm occurs.
4. Set the arming schedule for the alarm input. See “To set up motion detection” on page 36 for more information.
5. Click **Save** to save changes.

Exception alarms

You can set up the camera to notify you when irregular events occur and how you should be notified. These exception alarms include:

- **HDD Full:** All recording space of NAS is full.
- **HDD Error:** Errors occurred while files were being written to the storage, no storage or storage had failed to initialize.
- **Network Disconnected:** Disconnected network cable.
- **IP Address Conflicted:** Conflict in IP address setting.
- **Invalid Login:** Wrong user ID or password used to login to the cameras.

Figure 11: Exception window



To define exception alarms:

1. From the menu toolbar, click **Configuration > Basic Event > Exception**.
2. Under **Exception Type**, select an exception type from the drop-down list.
3. Specify the linkage method when an event occurs. Select one or more response methods for the system when a tamper-proof alarm is triggered.

Send Email	Send an email to a specified address when there is a motion detection alarm. Note: You must configure email settings before enabling this option. See “To set up the email parameters” on page 23 for further information. If you want to send the event snapshot together with the email, select the Attached Snapshot option.
Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Select “Select All” or each individual alarm output. Note: This option is only supported by cameras that support alarm output.

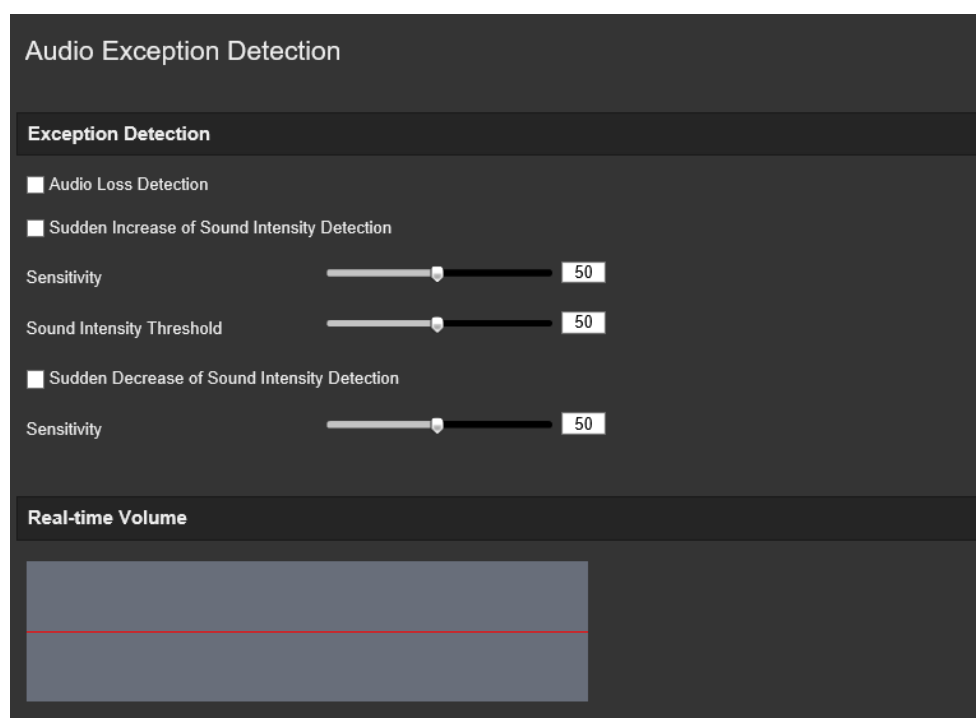
4. Click **Save** to save changes.

Audio exception detection

Audio exception detection function detects the abnormal sounds in the surveillance scene, such as the sudden increase/decrease of the sound intensity and the actions to be taken when the alarm is triggered.

To define audio exception detection:

1. Enter the Audio Exception Detection settings interface, **Configuration > Event > Smart Event > Audio Exception Detection**.



2. Select the **Audio Loss Exception** check box to enable the audio loss detection function.
3. Select the **Sudden Increase of Sound Intensity Detection** check box to detect sudden increase in sound in the surveillance scene. You can set the detection sensitivity and threshold for the sudden increase in sound.
4. Select the **Sudden Decrease of Sound Intensity Detection** check box to detect sudden decrease in sound in the surveillance scene. You can set the detection sensitivity and threshold for the sudden decrease in sound.

Notes:

Sensitivity: Range [1-100], the smaller the value, the larger the change needs to be to trigger detection.

Sound Intensity Threshold: Range [1-100], it can filter the sound in the environment. The louder the environment sound, the higher the value needs to be. You can adjust it according to the real environment.

You can view the real-time volume of the sound on screen.

5. Click **Arming Schedule** to set the arming schedule and set the arming times.

The image shows the 'Arming Schedule' configuration window. At the top, there are 'Delete' and 'Delete All' buttons. Below is a grid for setting arming times for each day of the week (Mon-Sun). Each day has a horizontal bar with a timeline from 0 to 24 hours, marked every 2 hours. The bars are currently all set to be active (blue) from 0 to 24 hours. Below the grid is an 'Actions' section with several checkboxes: 'Normal Actions', 'Send Email', 'Notify Alarm Recipient' (which is checked), 'Trigger Alarm Output', 'A->1', 'Trigger Recording', and 'A1'.

6. Click **Linkage Method** and select the linkage methods for audio exception, including Notify Surveillance Center, Send Email, Upload to FTP/Memory Card/NAS, Trigger Channel for recording, and Trigger Alarm Output.

Notify Alarm Recipient	Send an exception or alarm signal to the remote management software when an event occurs.
-------------------------------	---

Send Email	<p>Sends an email to a specified address when there is a motion detection alarm.</p> <p>Note: You must configure email settings before enabling this option. See “To set up the email parameters” on page 23 for further information. If you want to send the event snapshot together with the email, select the Attached Snapshot option.</p>
Upload to FTP/Memory Card/NAS	<p>Capture the image when an alarm is triggered and upload the snapshot to NAS, Memory Card or FTP server.</p> <p>Note: To upload the snapshot to NAS, you must first configure the NAS settings. See “Configuring NAS settings” on page 61 for further information.</p> <p>To upload the snapshot to an FTP, you must first configure the FTP settings. See “To define the FTP parameters” on page 23 for further information. Enable the Upload Type option.</p> <p>To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also enable Enable Event-triggered Snapshot under the snapshot parameters. See “Snapshot parameters” on page 58 for further information.</p>
Trigger Channel	Triggers the recording to start in the camera.
Trigger Alarm Output	<p>Trigger external alarm outputs when an event occurs. Select “Select All” or each individual alarm output.</p> <p>Note: This option is only supported by cameras that feature an alarm output.</p>

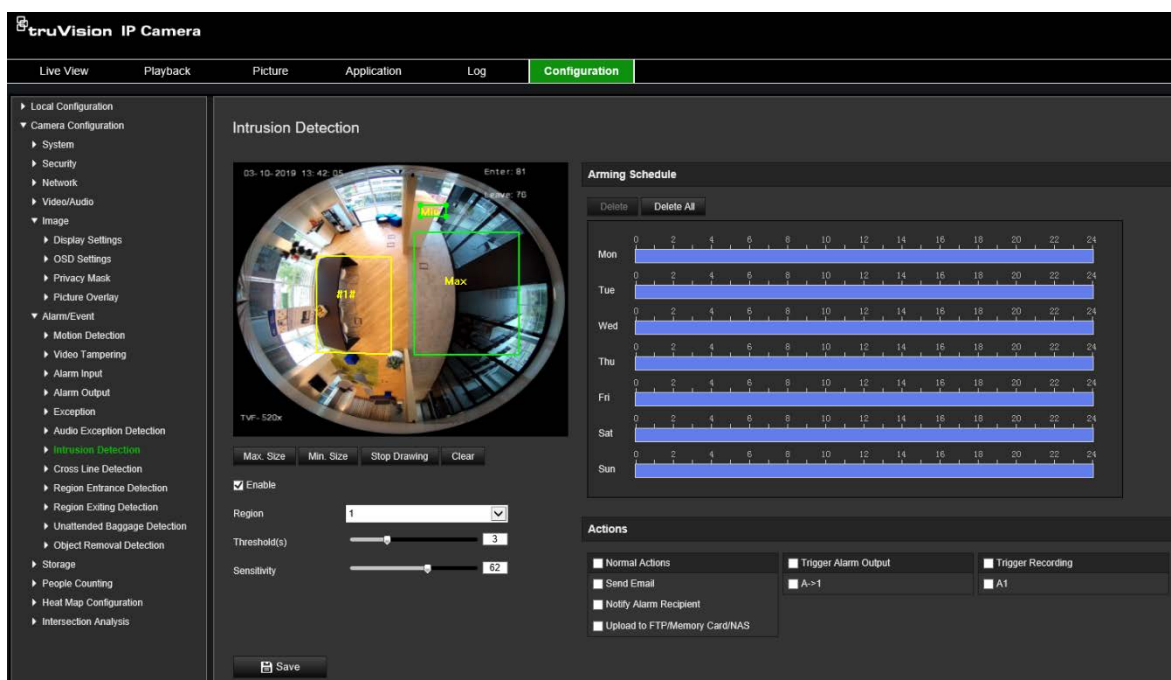
- Click **Save** to save the settings.

Intrusion detection

You can set up an area in the surveillance scene to detect when intrusion occurs. Up to four intrusion detection areas are supported. If someone enters the area, a set of alarm actions can be triggered.

To define intrusion detection:

1. From the menu toolbar, click **Configuration > Alarm/Event > Intrusion Detection**.



2. Select the **Enable Intrusion Detection** check box to enable the function.
3. Click **Draw Area**, and then draw a rectangle on the image as the defense region.

When you draw the rectangle, all lines should connect end-to-end to each other. Up to four areas are supported. Click **Clear** to clear the areas you have drawn. The defense region parameters can be set up separately.

Note: The area can only be quadrilateral.

4. Select the region to be configured from the drop-down list and define its time threshold and size sensitivity value:

Threshold: This is the time threshold that the object remains in the region. If you set the value as 0 s, the alarm is triggered immediately after the object enters the region. The range is between 0 and 10.

Sensitivity: The sensitivity value defines the size of the object that can trigger the alarm. When the sensitivity is high, a small object can trigger an alarm. The range is between 1 and 100.

5. Set the arming schedule for the alarm input. See “To set up motion detection” on page 36 for more information.
6. Specify the linkage method when an event occurs. Select one or more response methods for the system when an intrusion detection alarm is triggered.

Send Email	<p>Send an email to a specified address when there is a motion detection alarm.</p> <p>Note: You must configure email settings before enabling this option. See "To set up the email parameters" on page 23 for further information. If you want to send the event snapshot together with the email, select the Attached Snapshot option.</p>
Notify Alarm Recipient	<p>Send an exception or alarm signal to remote management software when an event occurs.</p>
Upload to FTP/Memory Card/NAS	<p>Capture the image when an alarm is triggered and upload the snapshot to NAS, Memory Card or FTP server.</p> <p>Note: To upload the snapshot to NAS, you must first configure the NAS settings. See "Configuring NAS settings" on page 61 for further information.</p> <p>To upload the snapshot to an FTP, you must first configure the FTP settings. See "To define the FTP parameters" on page 23 for further information. Enable the Upload Type option.</p> <p>To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also enable Enable Event-triggered Snapshot under the snapshot parameters. See "Snapshot parameters" on page 58 for further information.</p>
Trigger Alarm Output	<p>Trigger external alarm outputs when an event occurs. Select "Select All" or each individual alarm output.</p> <p>Note: This option is only supported by cameras that support alarm output.</p>
Trigger Recording	<p>Triggers the recording to start in the camera.</p>

7. Click **Save** to save changes.

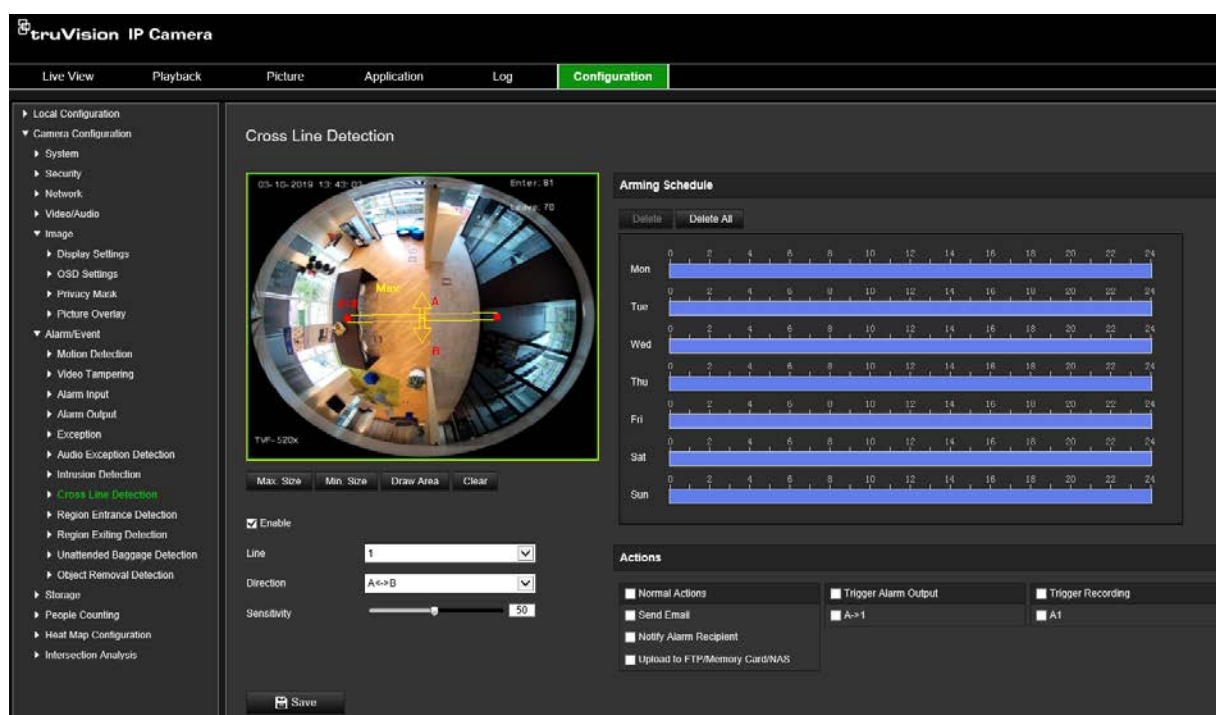
Cross line detection

This function can be used to detect people, vehicles and objects crossing a pre-defined line or an area on-screen. Up to four cross lines are supported. The cross line direction can be set as unidirectional or bidirectional. Unidirectional crossing is crossing the line from left to right or from right to left. Bidirectional crossing is crossing the line from both directions.

A series of linkage methods can be triggered if an object is detected crossing the line.

To define cross line detection:

1. From the menu toolbar, click **Configuration > Alarm Event > Cross Line**.



2. Select the **Enable Cross Line** detection check box to enable the function.
3. Click **Draw Area**. A crossing plane appears on the image.
4. Click the line. Two red squares appear at each end. Drag one of the red squares to define the arming area.
Select the direction as A<->B, A ->B, or B->A from the drop-down list (3):
A<->B: Only the arrow on the B side is displayed. When an object moves across the plane in both directions, it is detected and alarms are triggered.
A->B: Only an object crossing the pre-defined line from the A to the B side can be detected and trigger an alarm.
B->A: Only an object crossing the pre-defined line from the B to the A side can be detected and trigger an alarm.
5. Set the sensitivity level (4) between 1 and 100. The higher the value, the more easily the cross line detection action can be detected.
6. If desired, select another line crossing area to configure from the dropdown menu. Up to four cross line detection areas can be configured.
7. Set the arming schedule for the alarm input. See “To set up motion detection” on page 36 for more information.
8. Click **Linkage Method** to select the linkage methods. Select one or more response methods for the system when a cross line detection alarm is triggered.

Send Email	<p>Send an email to a specified address when there is a motion detection alarm.</p> <p>Note: You must configure email settings before enabling this option. See “To set up the email parameters” on page 23 for further information. If you want to send the event snapshot together with the email, select the Attached Snapshot option.</p>
Notify Alarm Recipient	<p>Send an exception or alarm signal to remote management software when an event occurs.</p>
Upload to FTP/Memory Card/NAS	<p>Capture the image when an alarm is triggered and upload the snapshot to NAS, Memory Card or FTP server.</p> <p>Note: To upload the snapshot to NAS, you must first configure the NAS settings. See “Configuring NAS settings” on page 61 for further information.</p> <p>To upload the snapshot to an FTP, you must first configure the FTP settings. See “To define the FTP parameters” on page 23 for further information. Enable the Upload Type option.</p> <p>To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also enable Enable Event-triggered Snapshot under the snapshot parameters. See “Snapshot parameters” on page 58 for further information.</p>
Trigger Alarm Output	<p>Trigger external alarm outputs when an event occurs. Select “Select All” or each individual alarm output.</p> <p>Note: This option is only supported by cameras that support alarm output.</p>
Trigger Recording	<p>Triggers the recording to start in the camera.</p>

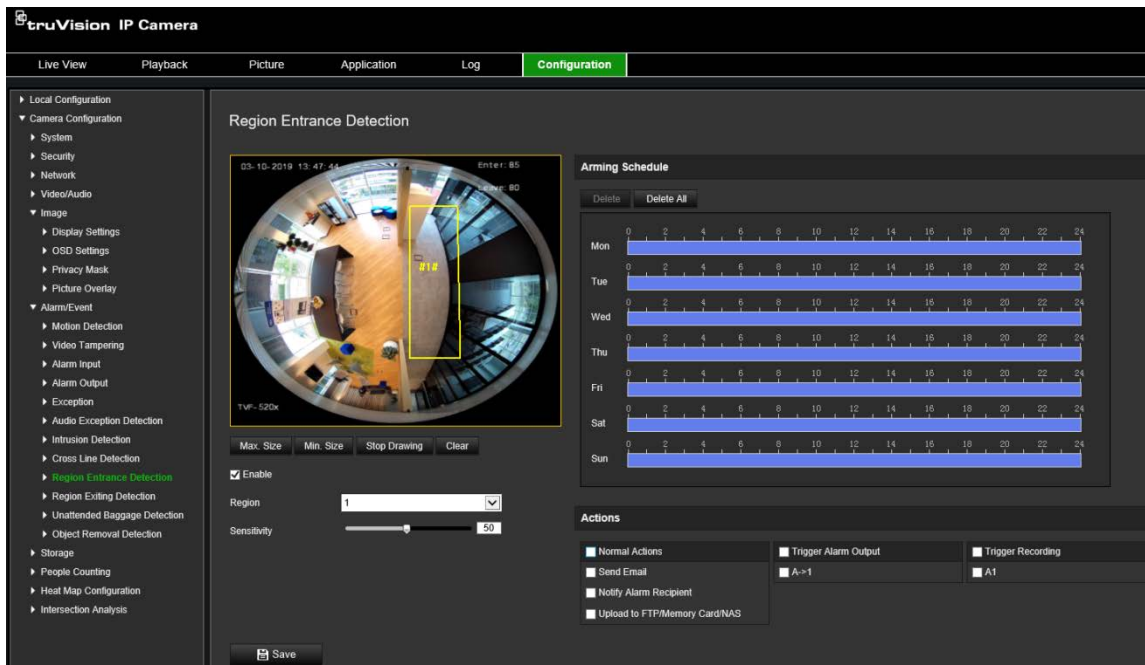
9. Click **Save** to save changes.

Region entrance detection

Region entrance detection function detects people, vehicle or other objects which enter a pre-defined virtual region from the outside place, and some certain actions can be taken when the alarm is triggered.

To define region entrance detection:

1. From the menu toolbar, click **Configuration > Event > Smart Event > Region Entrance Detection**.



2. Select the **Enable** check box to enable the function.
3. Select the region to be configured from the drop-down list.
4. Click the **Draw Area** button and then draw a rectangle on the image as the designated region.

When you draw the rectangle, all lines should connect end-to-end to each other. Up to four areas are supported. Click **Clear** to clear the areas you have drawn. The designated region parameters can be set up separately.

Note: The area can only be quadrilateral.

5. Set the maximum and minimum sizes for valid targets. Targets smaller or larger than the valid target size are not able to trigger detection.

Max. Size: The maximum size of a valid target. Targets larger than this will not trigger detection.

Min. Size: The minimum size of a valid target. Targets smaller than this will not trigger detection.

6. Click **Stop Drawing** when finish drawing.
7. Drag the slider to set the sensitivity value.

Sensitivity: Range [1-100]. Sensitivity stands for the percentage of the body part of an acceptable target that enters the pre-defined region.

$$\text{Sensitivity} = 100 - S1/ST*100$$

Where S1 stands for the target body part that enters the pre-defined region and ST stands for the complete target body.

Example: If you set the value as 60, the action can only be counted as a region entrance action when at least 40% of the body part enters the region.

8. Repeat the above steps to configure other regions. Up to four regions can be set. You can click the **Clear** button to clear all pre-defined regions.

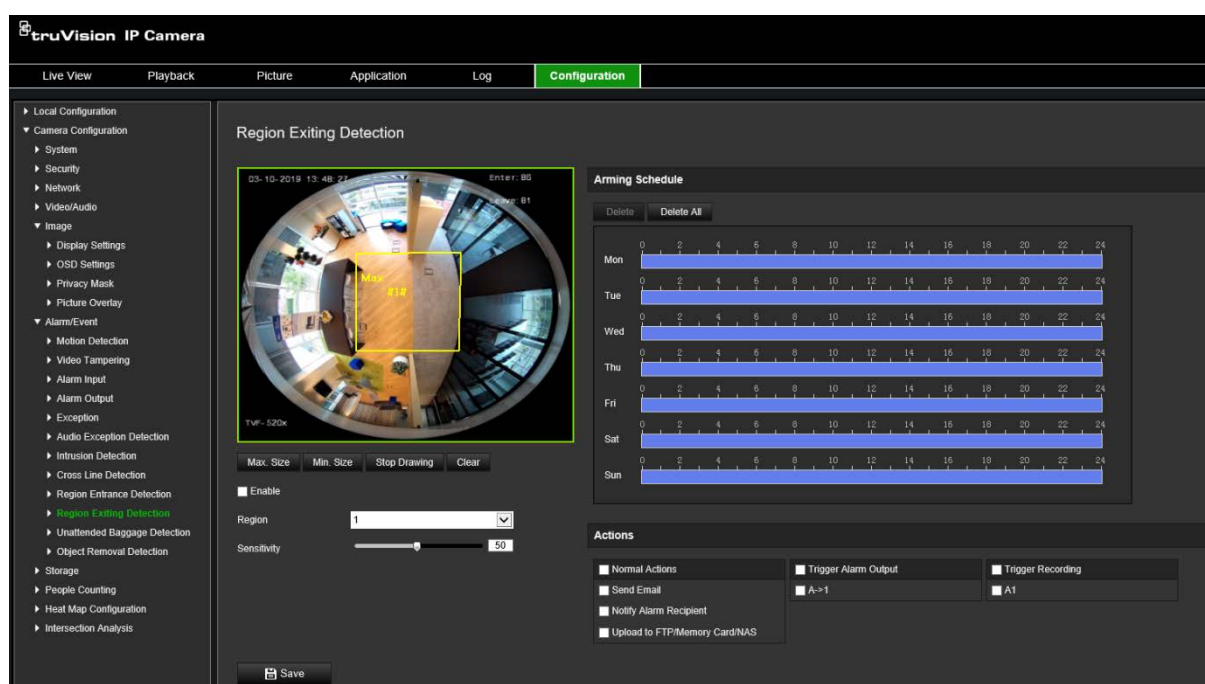
9. Click **Arming Schedule** to set the arming schedule.
10. Click **Linkage Method** to select the linkage methods. Select one or more response methods for the system when a region entrance detection alarm is triggered.
11. Click **Save** to save the settings.

Region exiting detection

Region exiting detection function detects people, vehicle or other objects which exit from a pre-defined virtual region, and some certain actions can be taken when the alarm is triggered.

To define region exit detection:

1. From the menu toolbar, click **Configuration > Event > Smart Event > Region Exiting Detection**.



2. Select the **Enable** check box to enable the function.
3. Select the region to be configured from the drop-down list.
4. Click **Area Settings**. Click the **Draw Area** button and then draw a rectangle on the image as the designated region.

When you draw the rectangle, all lines should connect end-to-end to each other. Up to four areas are supported. Click **Clear** to clear the areas you have drawn. The designated region parameters can be set up separately.

Note: The area can only be quadrilateral.

5. Set the maximum and minimum sizes for valid targets. Targets smaller or larger than the valid target size are not able to trigger detection.

Max. Size: The maximum size of a valid target. Targets larger than this will not trigger detection.

Min. Size: The minimum size of a valid target. Targets smaller than this will not trigger detection.

6. Click **Stop Drawing** when finish drawing.
7. Drag the slider to set the sensitivity value.

Sensitivity: Range [1-100]. Sensitivity stands for the percentage of the body part of an acceptable target that exits the pre-defined region.

$$\text{Sensitivity} = 100 - S1/ST \times 100$$

Where S1 stands for the target body part that exits the pre-defined region, and ST stands for the complete target body.

Example: If you set the value as 60, the action can only be counted as a region entrance action when at least 40% of the body part enters the region.

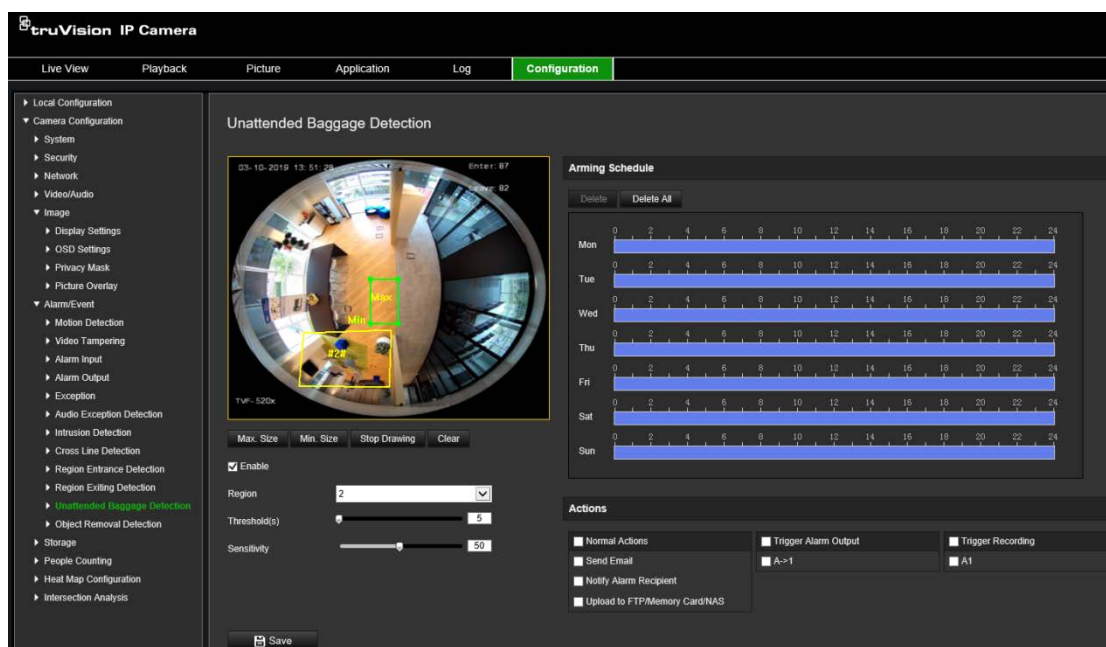
8. Repeat the above steps to configure other regions. Up to four regions can be set. You can click the **Clear** button to clear all pre-defined regions.
9. Click **Arming Schedule** to set the arming schedule.
10. Click **Linkage Method** to select the linkage methods. Select one or more response methods for the system when a region exit detection alarm is triggered.
11. Click **Save** to save the settings.

Unattended baggage detection

Unattended baggage detection function detects the objects left in the designated region such as baggage, a purse, dangerous materials, etc. A series of actions can be configured to occur when the alarm is triggered.

To define unattended baggage detection:

1. From the menu toolbar, click **Configuration > Event > Smart Event > Unattended Baggage Detection**.



2. Select the **Enable** check box to enable the function.
3. Select the region to be configured from the drop-down list.
4. Click the **Draw Area** button and then draw a rectangle on the image as the designated region.

When you draw the rectangle, all lines should connect end-to-end to each other. Up to four areas are supported. Click **Clear** to clear the areas you have drawn. The designated region parameters can be set up separately.

Note: The area can only be quadrilateral.

5. Set the maximum and minimum sizes for valid targets. Targets smaller or larger than the valid target size are not able to trigger detection.

Max. Size: The maximum size of a valid target. Targets larger than this will not trigger detection.

Min. Size: The minimum size of a valid target. Targets smaller than this will not trigger detection.

6. Click **Stop Drawing** when you have finished drawing.
7. Set the time threshold and detection sensitivity for unattended baggage detection.

Sensitivity: Range [5-100s]. Sensitivity stands for the percentage of the body part of an acceptable target that enters the pre-defined region.

$$\text{Sensitivity} = 100 - S1/ST*100$$

Where S1 stands for the target body part that enters the pre-defined region, and ST stands for the complete target body.

Example: If you set the value as 60, the action can only be counted as a region entrance action when at least 40% of the body part enters the region.

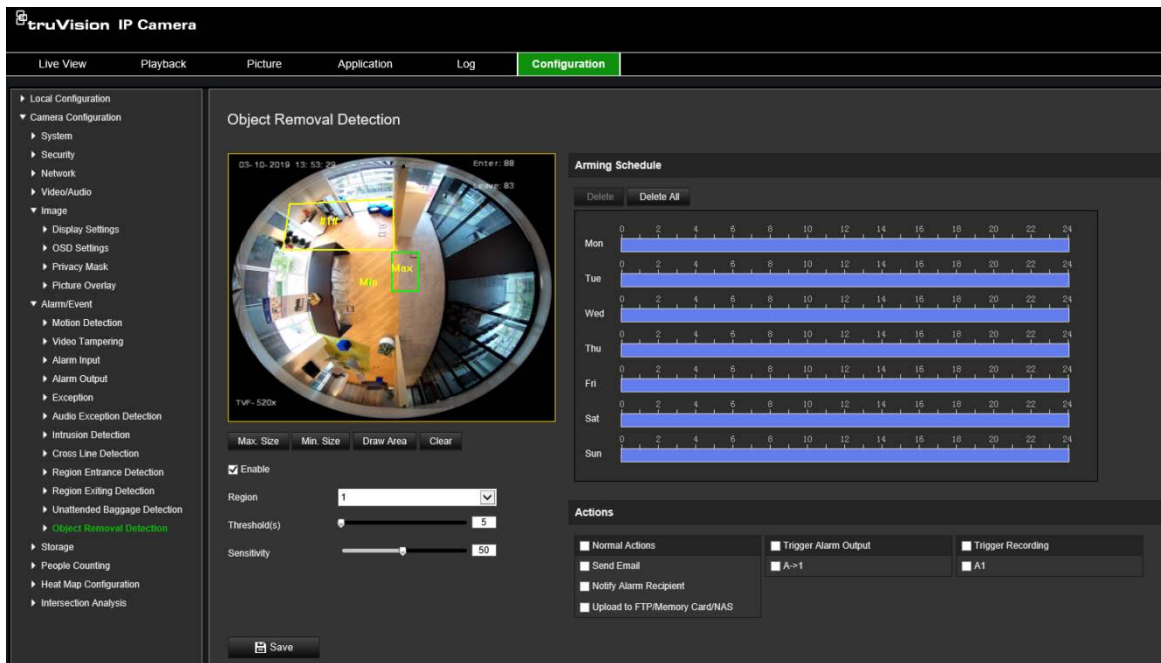
8. Repeat the above steps to configure other regions. Up to four regions can be set. You can click the **Clear** button to clear all pre-defined regions.
9. Click **Arming Schedule** to set the arming schedule.
10. Click **Linkage Method** to select the linkage methods. Select one or more response methods for the system when an unattended baggage detection alarm is triggered.
11. Click **Save** to save the settings.

Object removal detection

The object removal detection function detects the objects removed from the pre-defined region, such as the exhibits on display, and responds with a series of actions to be taken when the alarm is triggered

To define object removal detection:

1. From the menu toolbar, click **Configuration > Event > Smart Event > Object Removal Detection**.



2. Select the **Enable** check box to enable the function.
3. Select the region to be configured from the drop-down list.
4. Click **Area Settings** and click **Draw Area** to start the area drawing.
5. Click on the live video to specify the four vertexes of the detection region, and right click to complete drawing.
6. Set the maximum and minimum sizes for valid targets. Targets smaller or larger than the valid target size are not able to trigger detection.

Max. Size: The maximum size of a valid target. Targets larger than this will not trigger detection.

Min. Size: The minimum size of a valid target. Targets smaller than this will not trigger detection.

7. Click **Stop Drawing** when finish drawing.
8. Set the time threshold for object removal detection.

Threshold: Range [5-100 s], the threshold for the time of the objects removed from the region. If you set the value as 10, alarm is triggered after the object disappears from the region for 10 s.

9. Drag the slider to set the sensitivity value.

Sensitivity: Range [1-100]. Sensitivity stands for the percentage of the body part of an acceptable target that enters the pre-defined region.

$$\text{Sensitivity} = 100 - S1/ST \times 100$$

Where S1 stands for the target body part that enters the pre-defined region and ST stands for the complete target body.

Example: If you set the value as 60, the action can only be counted as a region entrance action when at least 40% of the body part enters the region.

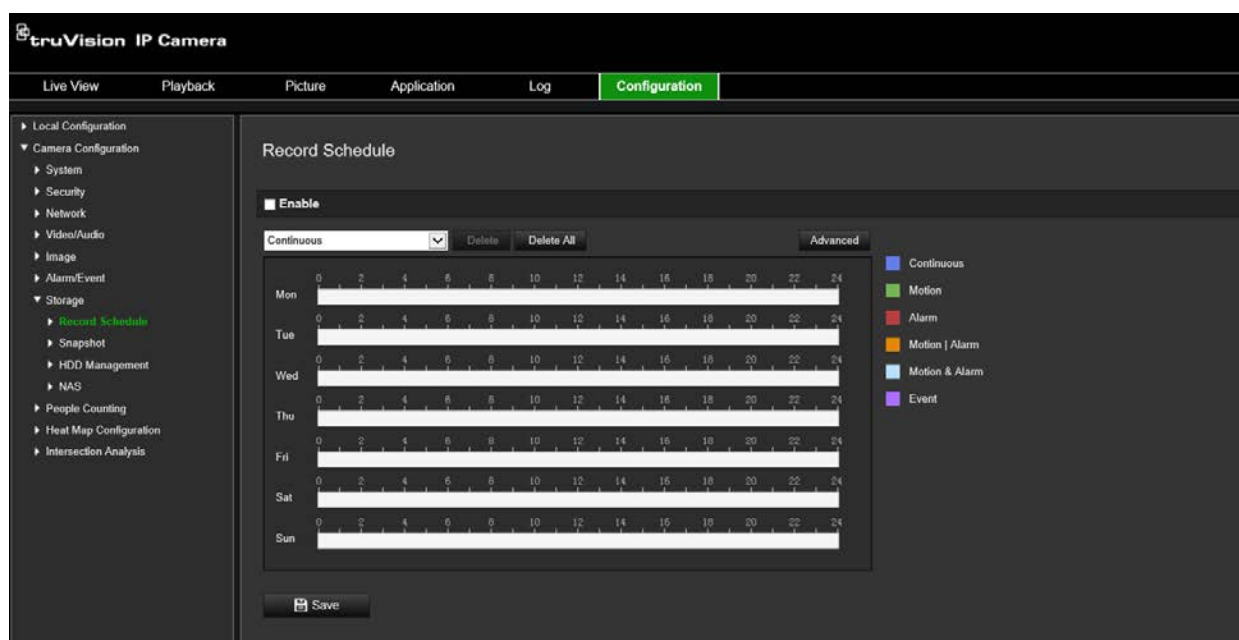
10. Repeat the above steps to configure other regions. Up to four regions can be set.
You can click the **Clear** button to clear all pre-defined regions.
11. Click **Arming Schedule** to set the arming schedule.
12. Click **Linkage Method** to select the linkage methods. Select one or more response methods for the system when an unattended baggage detection alarm is triggered.
13. Click **Save** to save the settings.

Recording schedule

You can define a recording schedule for the camera in the “Record Schedule” window. The recording is saved on to the SD card or NAS in the camera. The camera’s SD card provides a backup in case of network failure. The SD card is not provided with the camera.

The selected recording schedule applies to all alarm types.

Figure 12: Record schedule window



Pre-record time

The pre-record time is set to start recording before the scheduled time or event. For example, if an alarm triggers recording at 10:00, and the pre-record time is set to 5 seconds, the camera starts to record at 9:59:55. The pre-record time can be configured as No Pre-record, 5 s, 10 s, 15 s, 20 s, 25 s, 30 s, or Not Limited.

Post-record time

The post-record time is set to stop recording after the scheduled time or the event. For example, if an alarm triggered recording ends at 11:00, and the post-record time is set to 5 seconds, the camera records until 11:00:05. The post-record time can be configured as 5 s, 10 s, 30 s, 1 min, 2 min, 5 min, or 10 min.

Overwrite

The camera record is overwritten when *Overwrite* is enabled.

Recording stream

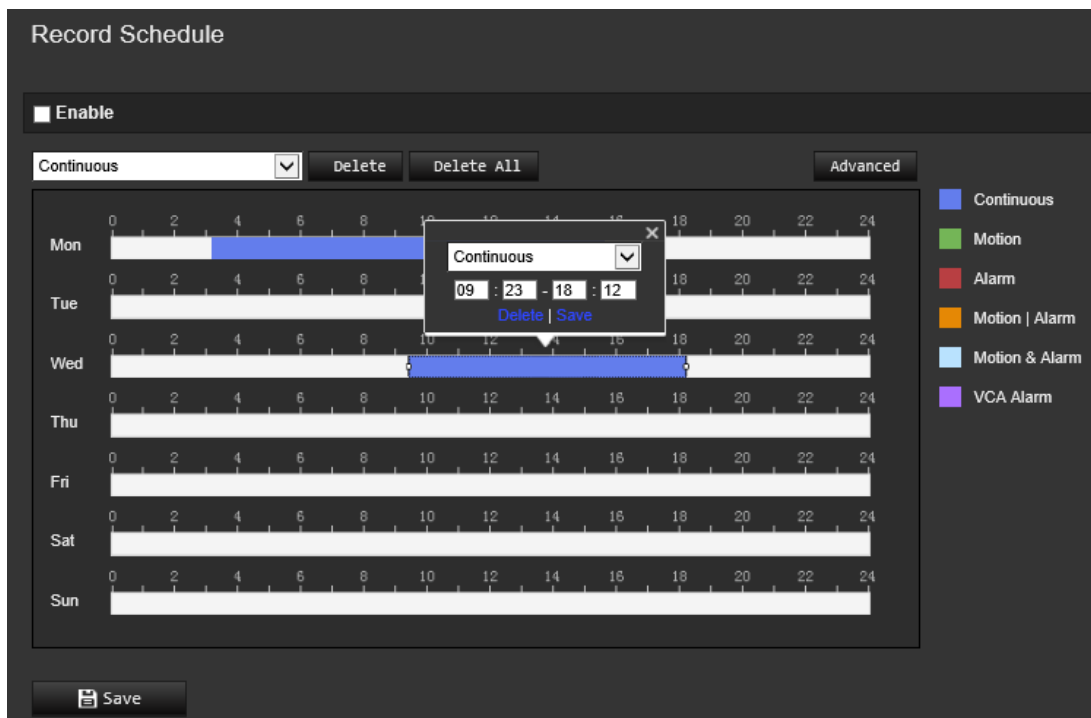
You can select Main Stream (Normal) or Substream for the recording stream.

To set up a recording schedule:

1. From the menu toolbar, click **Configuration > Storage > Record Schedule**.
2. Select the **Enable Record Schedule** check box to enable recording.

Note: To disable recording, deselect the option.

3. Edit the recording schedule. The following window appears:



4. Select whether the recording will be for the whole week (**All Day** recording) or for specific days of the week.

If you have selected “All day”, select one of the record types to record from the drop-down list:

- **Continuous:** This is continuous recording.
- **Motion:** Video is recorded when the motion is detected. See page 36.
- **Alarm:** Video is recorded when the alarm is triggered via the external alarm input channels. Besides configuring the recording schedule, you have to set the Alarm Type and select the *Trigger Channel* check box in the Linkage Method of Alarm Input Settings window. For detailed information, please refer to *Alarm Input* on page 42.
- **Motion | Alarm:** Video will be recorded when the external alarm is triggered or the motion is detected. Besides configuring the recording schedule, you have to

configure the settings in the Motion Detection (see page 36) and Alarm Input (see page 42) windows.

- **Motion & Alarm:** Video will be recorded when the motion and alarm are triggered at the same time. Besides configuring the recording schedule, you have to configure the settings in the Motion Detection (see page 36) and Alarm Input (see page 42) windows.
- **VCA events:** Video will be recorded when the either of the VCA events is triggered. Besides configuring the recording schedule, you have to configure the settings on the VCA interface. See page 28.

Note: Up to eight record types can be selected.

5. Set the recording periods for the other days of the week if required.

Click **Copy** to copy the recording periods to another day of the week.

6. Click **OK** and **Save** to save changes.

Note: If you set the record type to “Motion detection” or “Alarm”, you must also define the arming schedule in order to trigger motion detection or alarm input recording.

Snapshot parameters

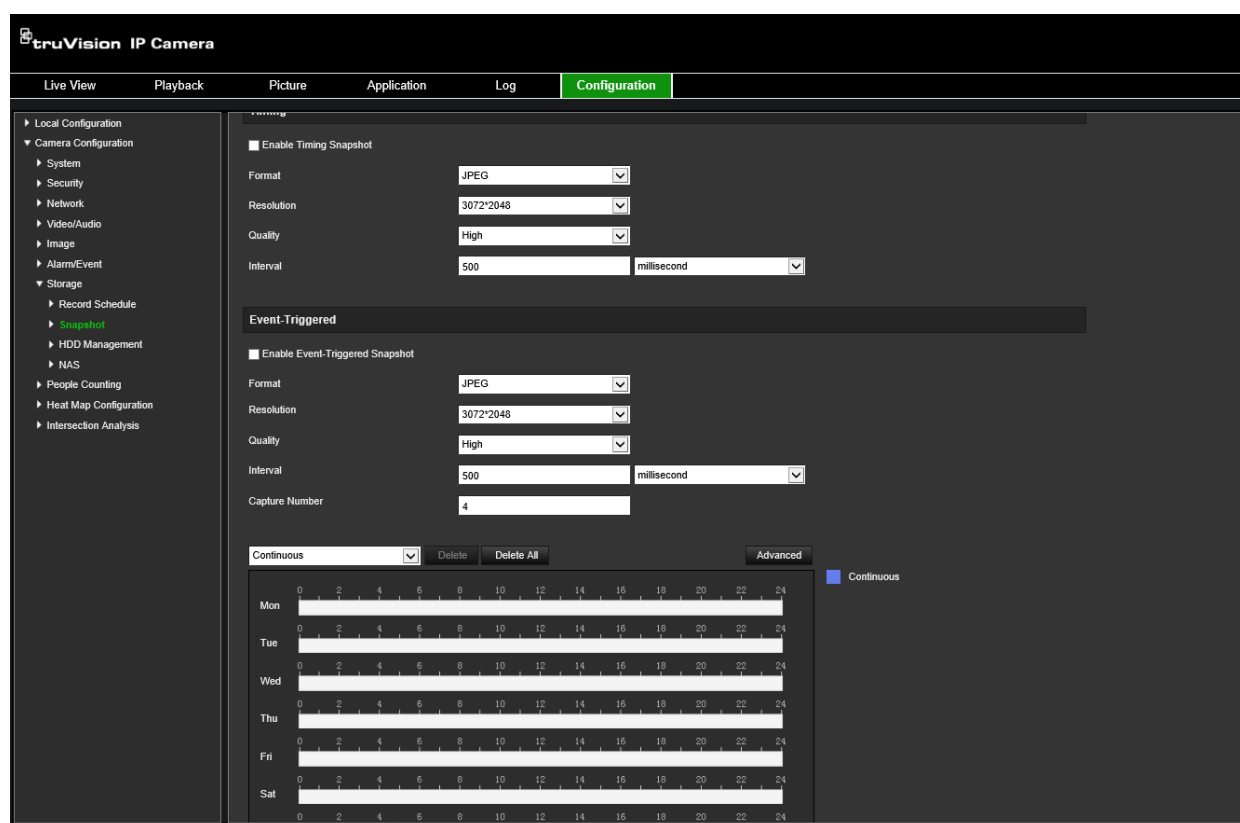
You can configure scheduled snapshots and event-triggered snapshots. The captured snapshots can be stored in the SD card (if supported) or the NAS. You can also upload the snapshots to an FTP server.

You can set up the format, resolution and quality of the snapshots. The quality can be low, medium, or high.

You must enable the option **Enable Timing Snapshot** if you want snapshots to be uploaded to the FTP. If you have configured the FTP settings and selected **Upload Type** in the Network > FTP tab, the snapshots will not be uploaded to the FTP if the **Enable Timing Snapshot** option is disabled.

You must enable the option **Enable Event-Triggered Snapshot** if you want snapshots to be uploaded to the FTP and NAS when motion detection or an alarm input is triggered. If you have configured the FTP settings and selected **Upload Type** in the Network > FTP tab for motion detection or an alarm input, the snapshots will not be uploaded to the FTP if this option is disabled.

Figure 13: Snapshot menu

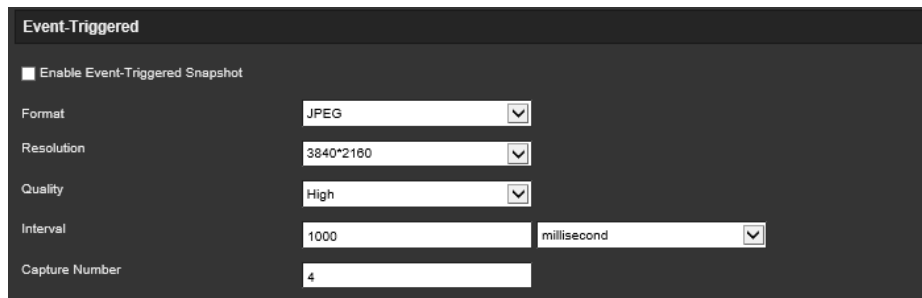


To set up scheduled snapshots:

1. From the menu toolbar, click **Configuration > Storage > Snapshot**.
2. Select **Enable Timing Snapshot** check box to enable continuous snapshots.
3. Select the desired format of the snapshot, such as JPEG.
4. Select the desired resolution and quality of the snapshot.
5. Enter the time interval between two snapshots. Select the unit of time from the drop-down list: milliseconds, seconds, minutes, hour, or day.
6. Set the schedule for when you want snapshots to be taken. Enter the desired schedule for each day of the week. Click advanced to select stream type, such as main stream (Normal).
7. Click **Save** to save changes.

To set up event-triggered snapshots:

1. From the menu toolbar, click **Configuration > Storage > Snapshot**.
2. Select the **Enable Event-triggered Snapshot** check box to enable event-triggered snapshots.



Event-Triggered

☒ Enable Event-Triggered Snapshot

Format: JPEG

Resolution: 3840*2160

Quality: High

Interval: 1000 millisecond

Capture Number: 4

3. Select the desired format of the snapshot, such as JPEG.
4. Select the desired resolution and quality of the snapshot.
5. Enter the time interval between two snapshots. Select the unit of time from the drop-down list: milliseconds or seconds.
6. Under **Capture Number**, enter the total number of snapshots that can be taken.
7. Click **Save** to save changes.

Formatting the storage devices

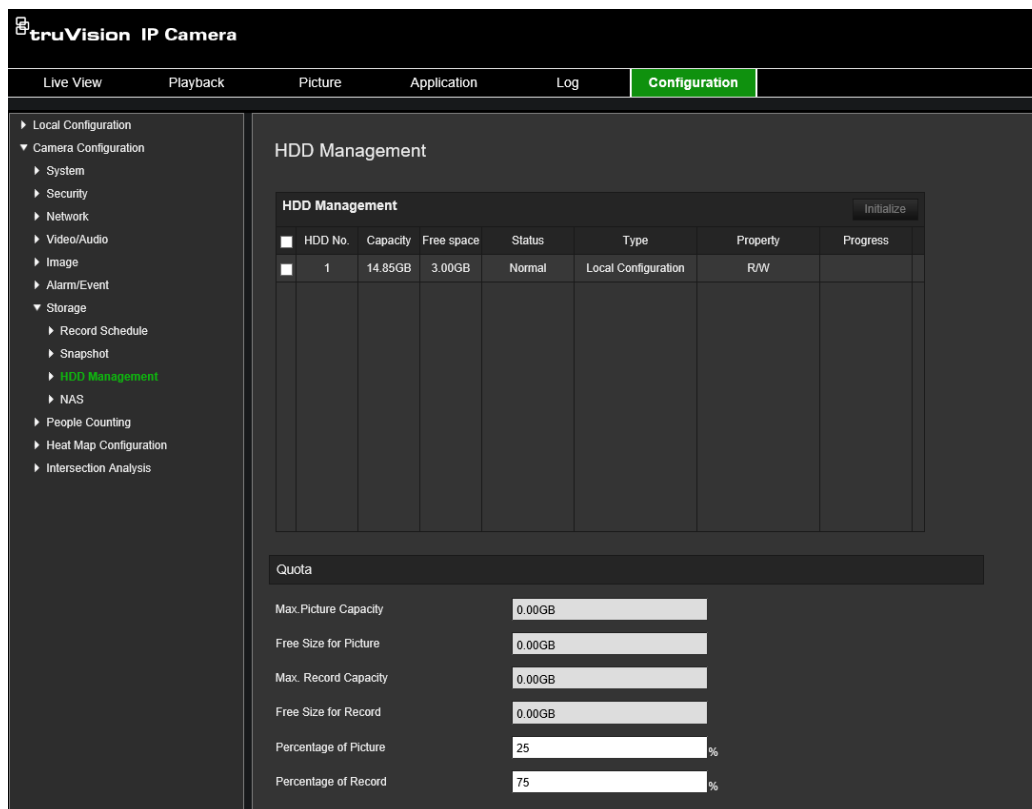
Use the storage management window to display the capacity, free space available, and the working status of the HDD of the NAS and the SD card in the camera. You can also format these storage devices.

Before formatting the storage device, stop all recording. Once formatting is completed, reboot the camera as otherwise the device will not function properly.

If *Overwrite* is enabled, the oldest files are overwritten when the storage becomes full.

To format the storage devices:

1. Click **Configuration > Storage > Storage Management**.



2. Select the **HDD No.** tab to select the storage.
3. Click **Format**. A window appears to check your formatting permission.
4. Click **OK** to start formatting.

To define the quota for recordings and snapshots:

1. Under **Quota**, enter the quota percentage for snapshots and recordings.
2. Click **Save** and refresh the browser page to activate the settings.

Configuring NAS settings

You can use a network storage system (NAS) to remotely store recordings

To configure record settings, please ensure that you have the network storage device within the network.

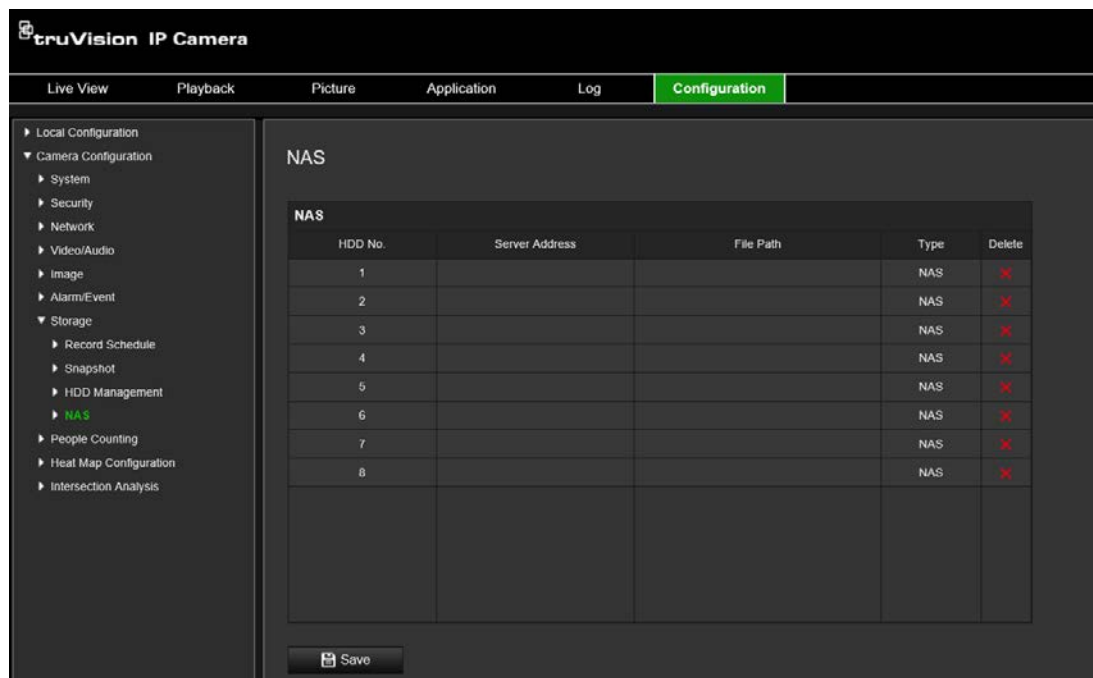
The NAS disk should be available within the network and correctly configured to store the recorded files, log files, etc.

Notes:

1. Up to eight NAS disks can be connected to the camera.
2. The recommended capacity of NAS should be between 9G and 2T as otherwise it may cause formatting failure.

To set up a NAS system:

1. Click **Configuration > Storage > NAS**.



2. Enter the IP address of the network disk, and the NAS folder path.
3. Click **Save** to save the settings.

People counting

This function helps calculate the number of people entering or exiting a configured area and is primarily used with entrances or exits.

Note: It is recommended to install the camera directly above the entrance/exit and aimed down at the entry/exit point to improve counting accuracy.

For accurate analysis *Ceiling Mount* should be selected when setting up the camera. See “Display control” on page 10. If *Ceiling Mount* is not selected, the *Application* tab will not be visible during setup.

The people counting option is only available when *Ceiling Mount* and a *360° View* mode are selected.


Notes:

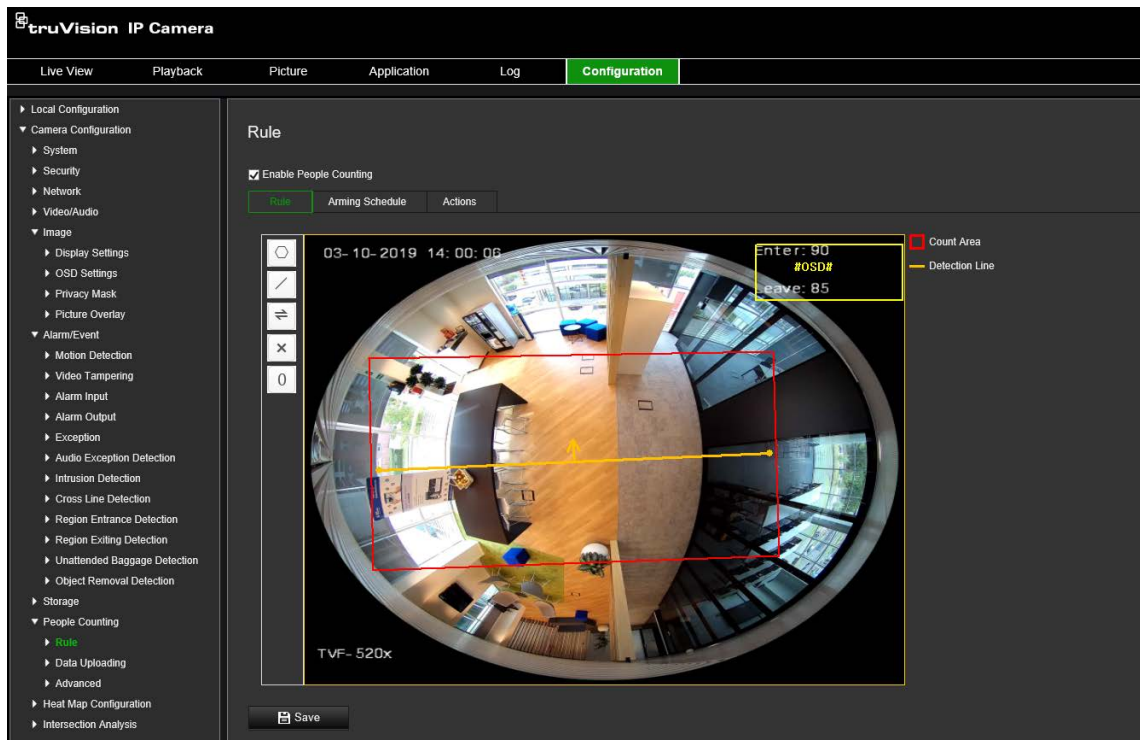
- The detection of targets is influenced by the validity parameters and minimum and maximum size of targets, which are set under the Heat Map menu. See “Heat map” on page 65.
- Depending on the shape of the detected object, it might be interpreted as being a person. Increasing the validity setting reduces the risk of this happening. However, if the value is too high, it may also result in people not being detected.


To set up people counting:

A. Rule settings:

1. From the menu toolbar, click **Configuration > People Counting**.
2. Select the **Enable People Counting** check box to enable the function.




- Under the **Rule** submenu, click  on the left of the live view image and draw a red count area.
 - Set the detection line.
- Draw a yellow detection line on the live video to detect and count the objects entering or exiting across the line.



- Click  to draw a detection line. An orange detection line will appear on the image.

Note:

- The detection line should be drawn directly below the camera and it should cover the entire entrance/exit region.
- Draw the detection line where people do not linger to improve the accuracy of the count.
- The detection line should be drawn within the red count area. Otherwise you will get a Parameter Error when saving.

- Click and drag the detection line to adjust its position.
- Click and drag the two end points of the detection line to adjust its length.
- Click  to delete the detection line.
- Click  to change the direction. The yellow arrow indicates the direction of entering.
- Click  to reset the counter to zero.

- Click **Save** to save the settings.

B. Arming schedule:

1. Under the **Rule** submenu, click **Arming Schedule** to edit the arming schedule.
2. Click on the time bar and drag the mouse to select the time period.



Note: Click the selected time period. You can adjust the time period to the desired time by either moving the time bar or input the exact time period.

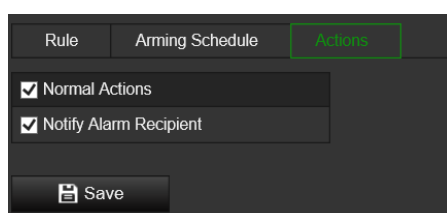
3. (Optional) Click **Delete** to delete the current arming schedule, or click **Save** to save the settings.
4. Move the mouse to the end of each day. A copy dialogue box pops up. You can copy the current settings to other days of the week.
5. Click **Save** to save the settings.

Note: The time periods cannot overlap. Up to eight periods can be configured for each day.

C. Linkage method:

1. Under the **Actions** submenu, select the linkage method. Enable the linkage method *Notify Alarm Recipient* to send an exception or alarm signal to remote management software when an event occurs.

Note: The linkage methods vary according to the different camera models.



Data uploading setting:

The **Data Uploading** submenu lets you select how and when the counting data can be sent to clients and users.

- You can upload people counting data to alarm recipient and client software through SDK and HTTP (if configured).

To upload real-time data, select the *Real-Time Upload Data* check box.

To upload data regularly, set the *Data Statistics Cycle* as desired.

Note: If data uploading by HTTP is required, set up the HTTP Data Transmission parameters.

- You can send the people counting report to a configured email address.

Select report type (daily report, weekly report, monthly report, and annual report) to activate the function.

Note: Go to **Configuration > Network > Advanced Settings > Email** to set up email.

Advanced settings:

The **Advanced** submenu shows maintenance settings:

- Flow Overlay

It displays real-time flow information on screen. You can select the displayed data type from the drop-down list.

- Daily Reset Time

You can set up a daily reset time or you can reset the counter manually by clicking *Manual Reset*.

Heat map

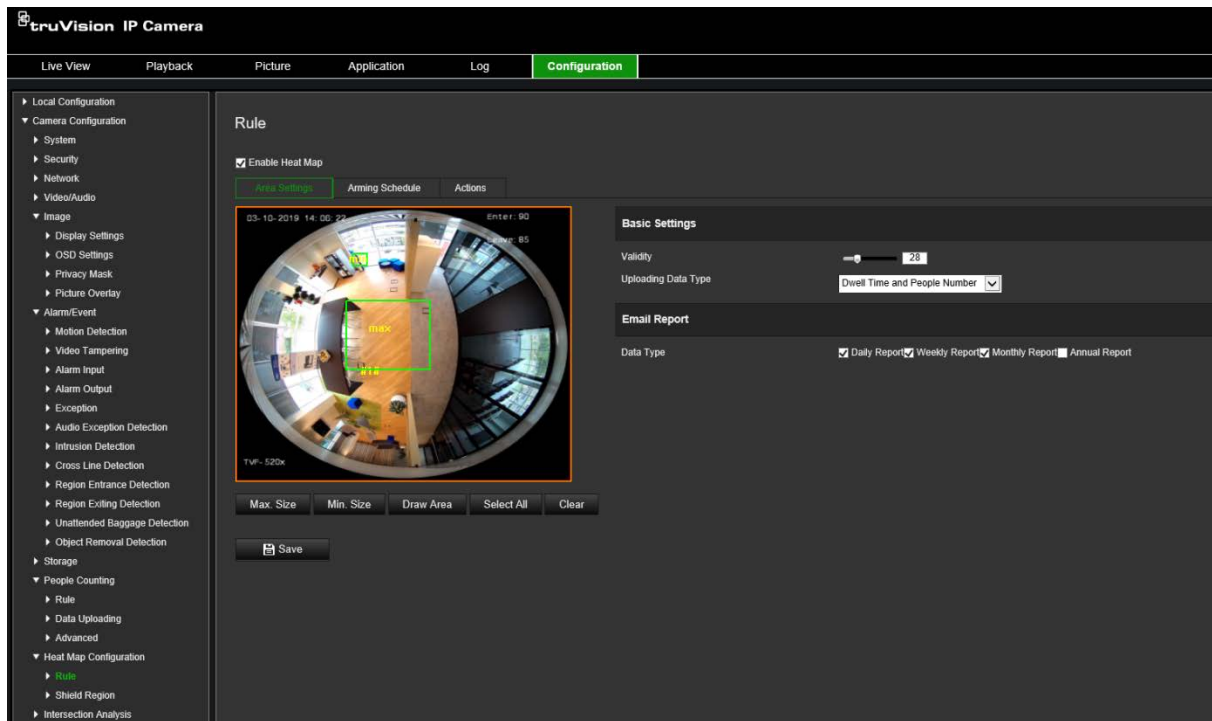
A heat map is a color-coded graphical representation of the movement of people through a scene. The colors correspond to the amount of traffic and the amount of time spent stationary in the configured scene. Heat maps are most commonly used for retail applications to measure customer interaction within a store.

Note: To use *Heat Map Statistics*, please ensure that you have installed and formatted an SD card to provide the memory necessary for storing the heat map data.

For an accurate analysis *Ceiling Mount and 360° View* must be selected when setting up the camera as otherwise the heat map function will not be available. See “Display control” on page 10. If *Ceiling Mount* is not selected, the *Application* tab will not be visible during setup.

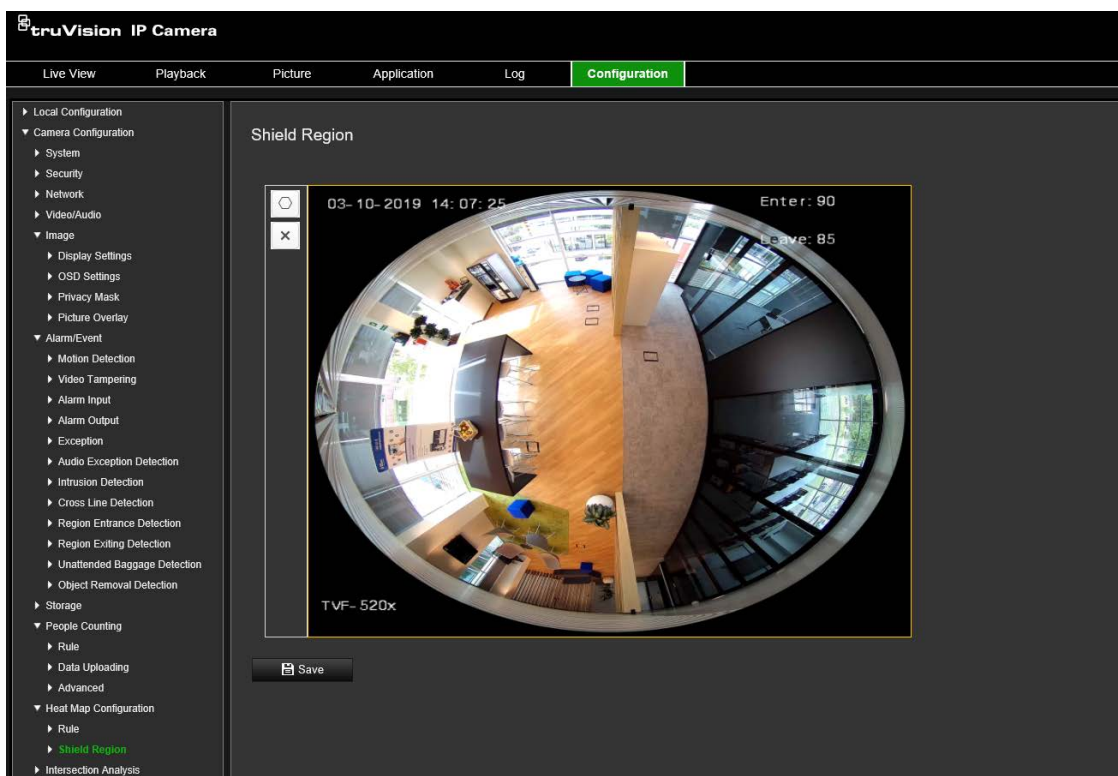
To set up the heat map:



1. From the menu toolbar, click **Configuration > Heat Map Configuration**.
2. Select the **Enable Heat Map** check box to enable the function.
3. Under the submenu **Rule**, go to **Area Settings** to draw the detection area.



- 1) Click **Draw Area** to draw a detection area. Draw an area by left-clicking the end-points in the live view window, and right-clicking to complete the area drawn.
Note: Click **Select All** to select the whole live view window as the configured area. Click **Clear** to delete the current drawn area.
- 2) Set the maximum and minimum sizes for valid targets. Targets smaller or larger than the valid target size are not able to trigger detection.
Max. Size: The maximum size of a valid target. Targets larger than this will not trigger detection.
Min. Size: The minimum size of a valid target. Targets smaller than this will not trigger detection.
- 3) Click **Stop Drawing** when finished drawing.
4. Set the validity value. The range is between 0 and 100.
Validity: The camera uses this value to judge if a target it detects is a valid or not. An invalid target will not be included in the statistics. The higher value, the lower the number of targets detected.
Important: The validity value also impacts target detection for intersection analysis (see “Intersection analysis statistics” on page 73) and people counting (see “People counting statistics” on page 69).
5. Select the uploading data type:
Dwell Time and People Number: Uploads the number of people detected and average time they spent in the heat map area.
Dwell Time: Uploads the average time people spent in the heat map area.
Note: Please note that it takes up to one hour for counting results to be included in the heat map report generated under the menu Application > Heat Map.

6. Under Email Reports, select the frequency of sending email reports (daily report, weekly report, monthly report, or annual report). Heat map reports will be sent to all configured email addresses (see page 23 for information on setting up email addresses).
7. Under the **Arming Schedule** tab, click-and-drag the mouse on the time bar to set the arming schedule.
8. Under the Actions tab, select the **Linkage Method** by enabling *Notify the surveillance center*, if required.
9. Under the submenu **Shield Region**, draw a shielded area in which no heat map analysis will be done.



Click  to draw a shielded area. Draw an area by left-clicking the end-points in the live view window, and right-clicking to complete the area drawn. The drawn area can have up to 10 sides. Up to four shielded areas can be drawn. Click  to delete all drawn areas.

Note: Shielded areas cannot be drawn if live view stops.

10. Click **Save** to save the settings.

Note: The heat map statistics is calculated under the Application tab. Go to **Application** to check the heat map statistics.

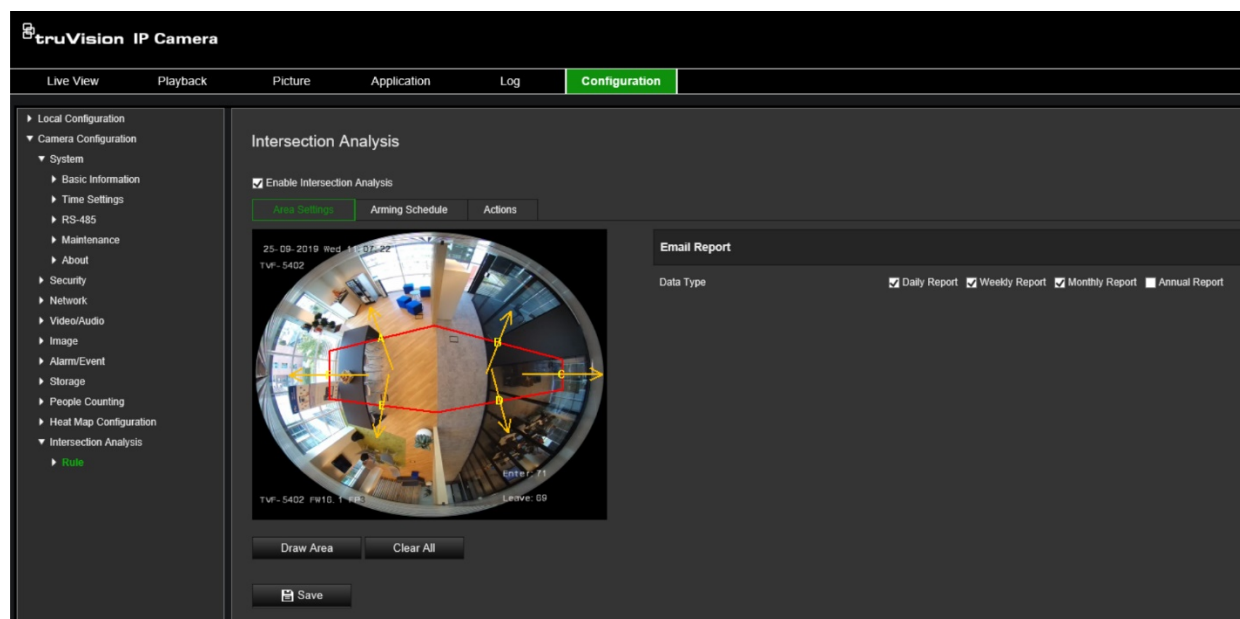
Intersection analysis

Intersection analysis is used to monitor the flow of people in an identified area.

Note: 360° View must be selected when setting up the camera as otherwise the intersection analysis function will not be available.

Note: The detection of targets is influenced by the validity parameters and minimum and maximum size of targets, which are set under the Heat Map menu. See “Heat map” on page 65.

Figure 14: Intersection analysis window



To set up the intersection analysis:

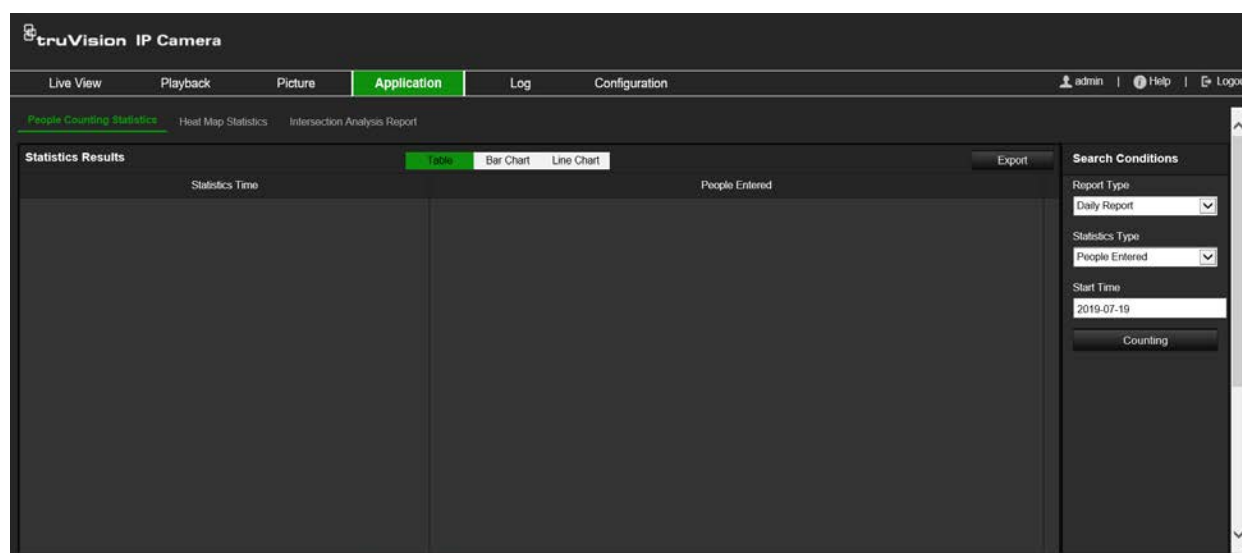
1. From the menu toolbar, click **Configuration > Intersection Analysis**.
2. Select the **Enable Intersection Analysis** check box to enable the function.
3. Set up the rules.
 - 1) Go to the tab **Area Settings**.
 - 2) Click **Draw Area**. Draw an area in the live view window by left-clicking the end-points. The area should be a polygon with no more than 10 sides. Each side of the defined intersection area monitors one direction of flow.
 - 3) Adjust the arrow direction on each side of the polygon area. The arrow indicates the direction of flow leaving the intersection area.
 - 4) Under Email Reports, select the frequency of sending email reports (daily report, weekly report, monthly report, or annual report). Intersection analysis reports will be sent to all configured email addresses (see page 23 for information on setting up email addresses).
4. Go to the **Arming Schedule** tab, and click-and-drag the mouse on the time bar to set the arming schedule.
5. Under the Actions tab, select the **Linkage Method** by enabling *Notify the surveillance center*, if required.
6. Click **Save** to save the settings.

Note: The intersection analysis statistics are calculated in the *Application* tab. Go to **Application** to check the reports.

Application

You can search, view, and download the counting data on people counting, heat map statistics, and intersection analysis that is stored in the local storage or network storage. An SD card must be installed in the camera in order to have the Application menu appear in the camera web browser.

Figure 15: Application window



People counting statistics

After you enable the people counting function, you can view and download the people counting data from the application tab. You can display the data in different charts.

Before you start:

You have to configure the *People Counting* setting before you can view and download the people counting data from the application tab. Refer to the section “People counting” on page 62 for detailed information.

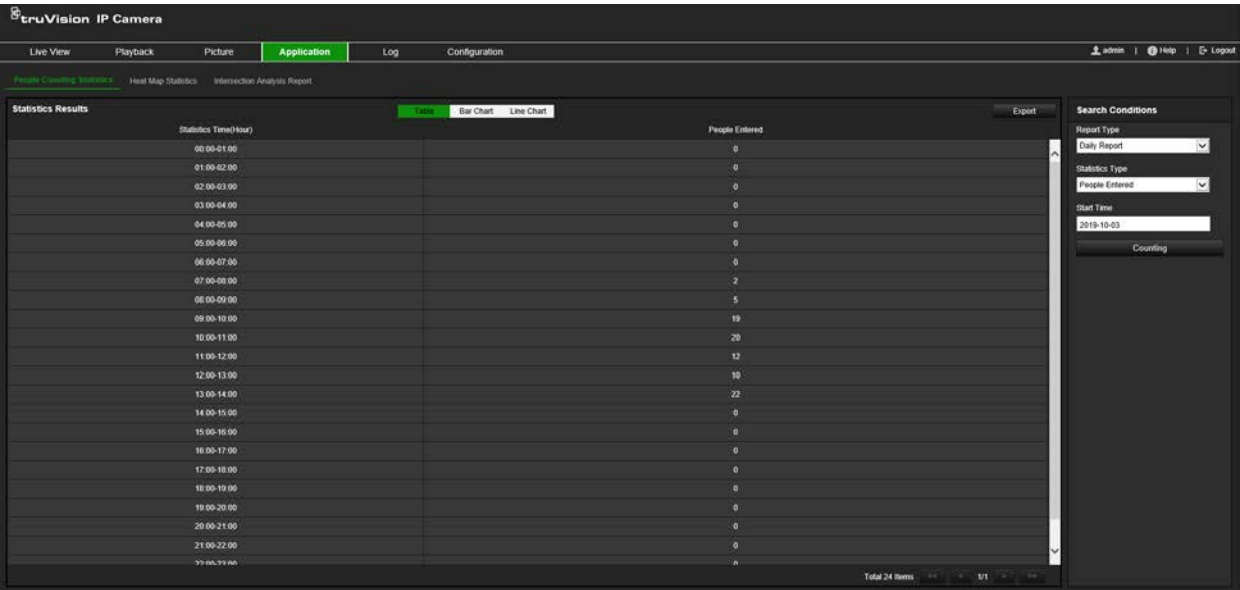
To obtain people counting statistics:

1. From the menu toolbar, click **Application > People Counting Statistics**.
2. Select the report type from the drop-down list: Daily Report, Weekly Report, Monthly Report, or Annual Report.
 - The daily report calculates the data on the date you selected.
 - The weekly report calculates for the week in which your selected date belongs.
 - The monthly report calculates for the month in which your selected date belongs.
 - The annual report calculates for the year in which your selected date belongs.
3. Select the statistics type: People Entered or People Exited.

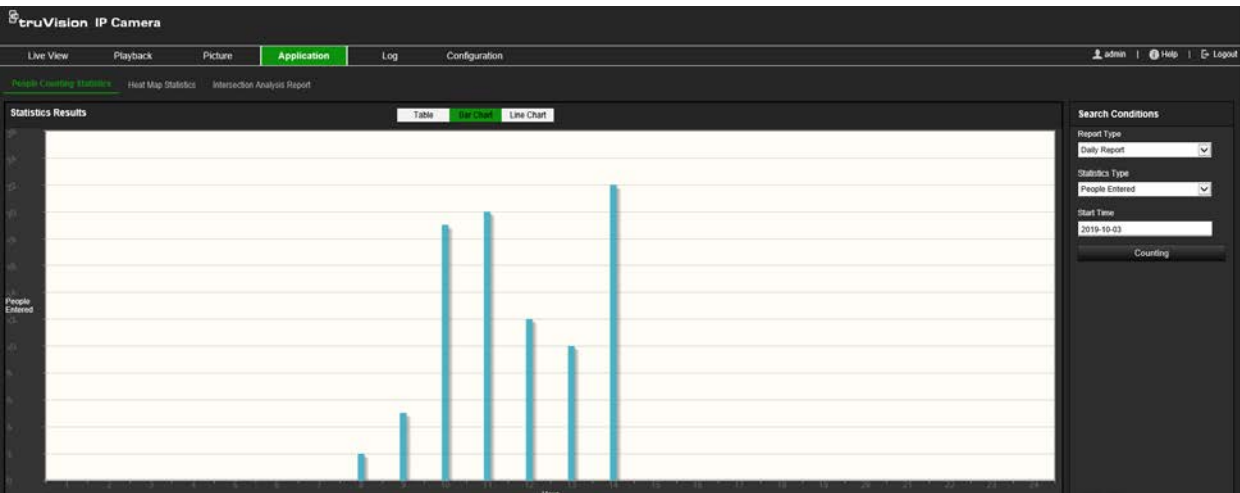
4. Select the start time and then click **Counting**.

The counting result displays in the statistic result area. Click Table, Bar Chart, or Line Chart to display the result in different ways.

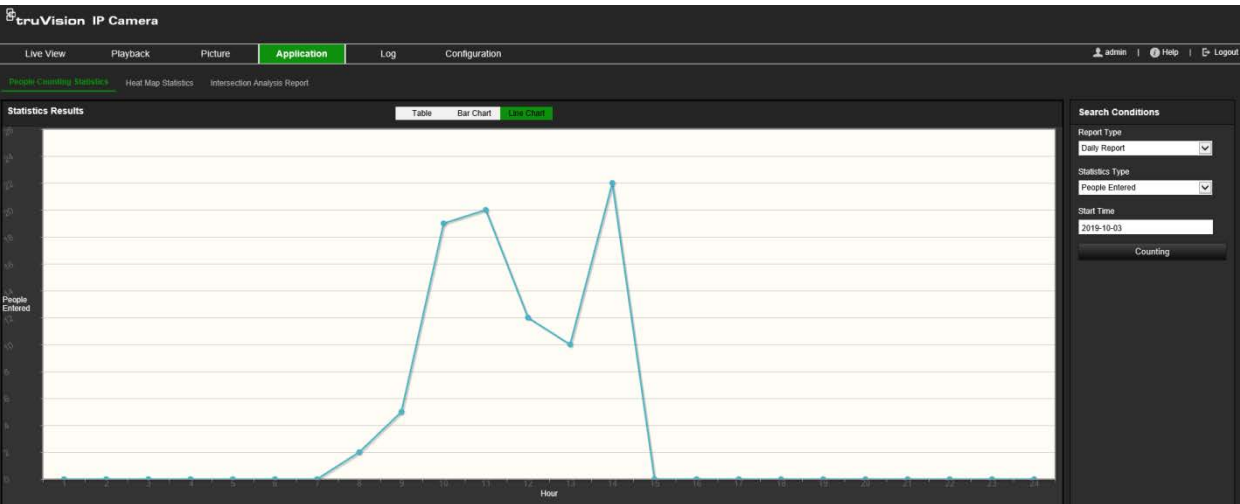
Example of table format:



Example of bar chart:



Example of line chart:



Note: If you select *Table* to display the statistics, click the **Export** button to export the data to an Excel file.

Heat map statistics

A heat map is a graphical representation of data represented by colors. The heat map function of the camera is usually used to analyze the visit times and dwell time of people in a configured area. You can display the data in different charts.

Before you start:

You have to configure the *Heat Map* setting before you can view and download the heat map data from the application tab. Refer to the section “Heat map” on page 65 for detailed information.

Note: The heat map function is not supported when you choose the hardware display mode as *180 Panoramic View* or *Four PTZ View*. Consequently, you will not see the Application tab on the menu toolbar when these modes have been selected.

To obtain heat map statistics:

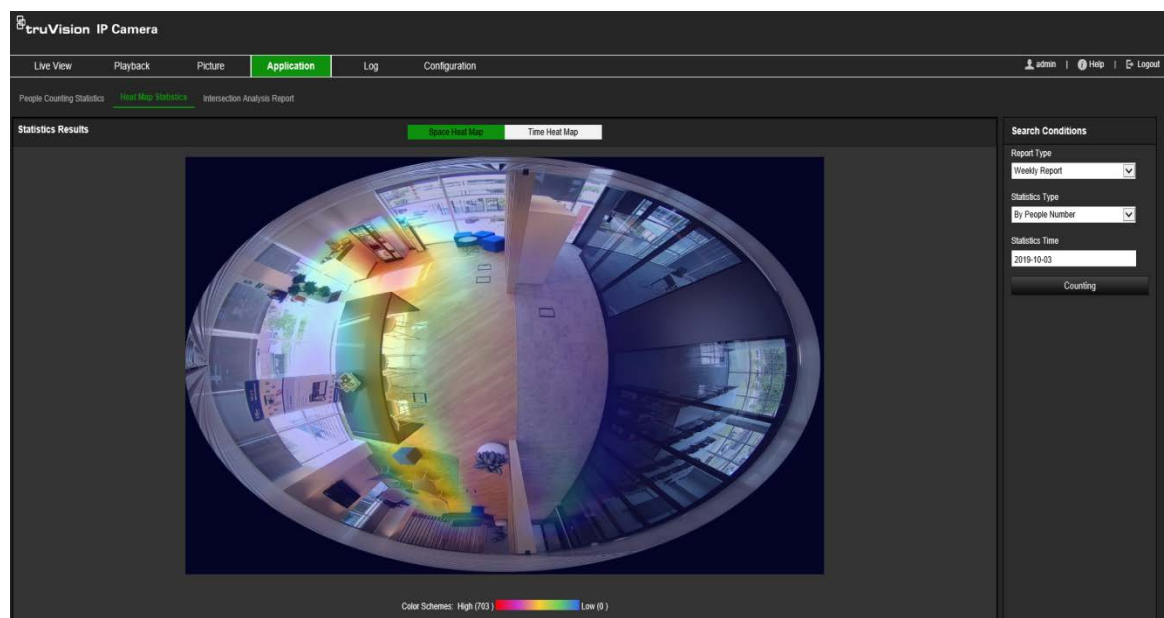
1. From the menu toolbar, click **Application > Heat Map Statistics**.
2. Select the report type from the drop-down list: Daily Report, Weekly Report, Monthly Report, or Annual Report.
 - The daily report calculates the data on the date you selected.
 - The weekly report calculates for the week in which your selected date belongs.
 - The monthly report calculates for the month in which your selected date belongs.
 - The annual report calculates for the year in which your selected date belongs.
3. Select the statistics type to display from the drop-down list: Dwell time or People Counting.
4. Select the statistics time for the period of time to display: Day, Week, Month, or Year, and select where on date on the calendar to start the search. For week, month, and year, the date selected is the end date for the search.
5. Click **Counting** to generate the heat map data.
6. Select **Space Heat Map** or **Time Heat Map** to display the results.

Space heat map:

The different colors that mark areas in the surveillance scene stand for the different frequency of visits. The closer the color to the red end of the color scheme, the higher the number of visits.

The duration displayed next to “High” or “Low” stands for the cumulative time of visit frequency for that the area.

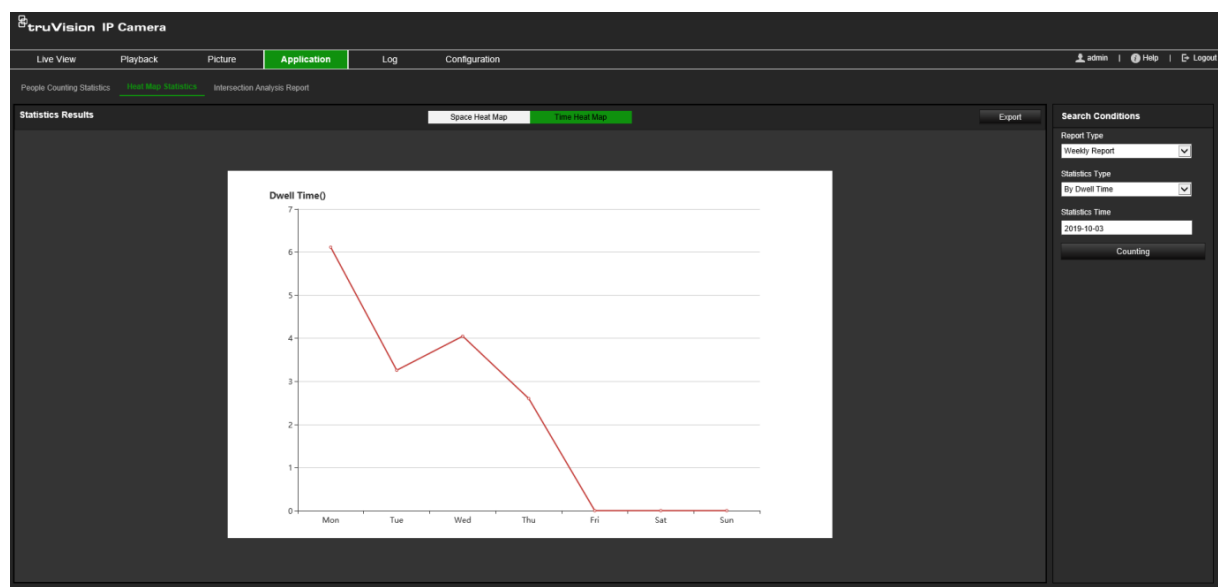
Figure 16: Example of a space heat map weekly report



Time heat map:

The **Dwell time** or **People number** of the pre-defined area is calculated by hour, day, or month. Click the **Export** button to export the data to an Excel file.

Figure 17: Example of a time heat map weekly report



Note: It is recommended that you do not adjust the electronic lens after the installation is completed as this may cause some inaccuracy to the data.

Intersection analysis statistics

When enabled, the intersection analysis function lets you view and download the intersection analysis data from the Application tab. It displays the direction of flow of people in the configured area. You can display the data in different charts.

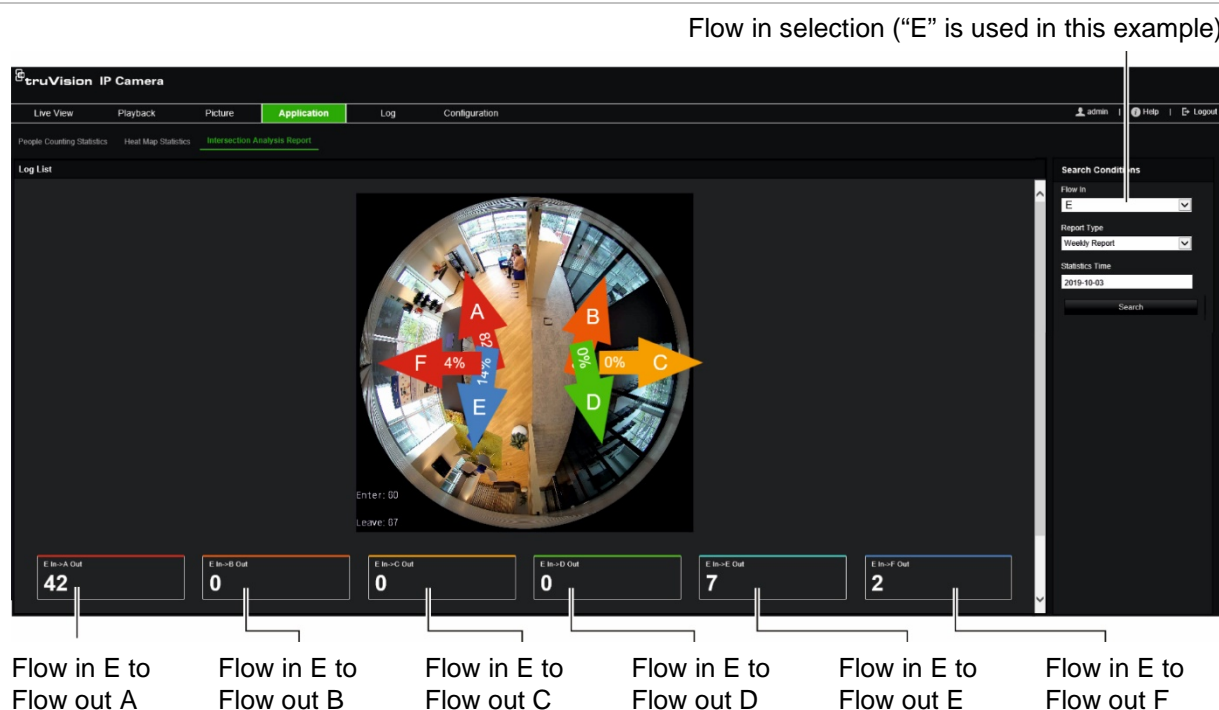
An example of the results of an analysis is shown in Figure 18 below. See Figure 14 on page 68 for the monitored area set up for this example. The results of the analysis are listed below the 360° view, the colors of the boxes matching that of the arrows.

The arrows display the percentage of people flowing in the direction of the arrow. The boxes display the number of people detected flowing into the selected *flow in* arrow point and then flowing out from each of the other arrow points. In the example below, the *Flow in* is E and the results show the flow of people from E to each of the other five arrows. The *flow out* arrows are always shown in alphabetical order.

You can set up the analysis on how you want to be notified of these results, such as by email for example. See the section “Intersection analysis” on page 67 for further information.

Note: The direction of the requested flow in arrow head does not indicate the direction of the flow in.

Figure 18: Example of the results of an intersection analysis



Before you start:

You have to configure the *Intersection Analysis* setting before you can view and download the intersection analysis data from the application tab. Refer to the section “Intersection analysis” on page 67 for detailed information.

To obtain intersection analysis statistics:

1. From the menu toolbar, click **Application > Intersection Analysis Report**.
2. Select a **Flow In** entrance from the drop-down list.
3. Select the report type: Daily report, Weekly report, Monthly report, or Annual report.
 - The daily report calculates the data on the date you selected.
 - The weekly report calculates for the week in which your selected date belongs.
 - The monthly report calculates for the month in which your selected date belongs.
 - The annual report calculates for the year in which your selected date belongs.
4. Select the statistics time for the dates during which you want the analysis done.
5. Click **Search** to start calculating.

Camera management

This chapter describes how to use the camera once it is installed and configured. The camera is accessed through a web browser.

User management

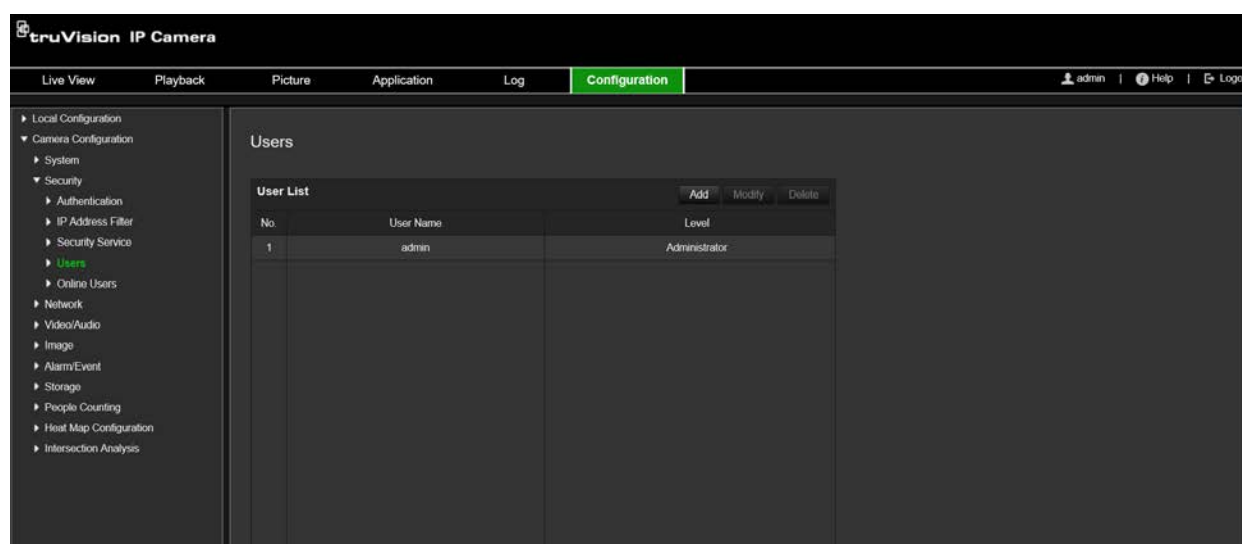
This section describes how to manage users. You can:

- Add or delete users
- Modify permission
- Modify passwords

Only the administrator can manage users. The administrator can create up to 31 individual users for the cameras listed in this manual.

When new users are added to the list, the administrator can modify permissions and password of each user. See Figure 19 below.

Figure 19: User management window



Passwords limit access to the camera and the same password can be used by several users. When creating a new user, you must give the user a password. There is no default password provided for all users. Users can modify their passwords.

Note: Keep the admin password in a safe place. If you forget it, please contact technical support.

Types of users

A user's access privileges to the system are automatically defined by their user type. There are three types of user:

- **Admin:** This is the system administrator. The administrator can configure all settings. Only the administrator can create and delete user accounts. Admin cannot be deleted.
- **Operator:** This user can only change the configuration of his/her own account. An operator cannot create or delete other users.
- **User:** This user has the permission of live view, playback and log search. However, they cannot change any configuration settings.

Add and delete users

The administrator can create up to 31 users. Only the system administrator can create or delete users.

To add a user:

1. From the menu toolbar, click **Configuration > Security > Users**.
2. Select the **Add** button. The user management window appears.

3. Enter a user name.

4. Assign the user a password. Passwords can have up to 16 alphanumeric characters.
5. Select the type of user from the drop-down list. The options are Viewer and Operator.
6. Assign permissions to the user. Check the desired options:

Basic Permissions	Camera Configuration
Remote: Parameters Settings	Remote: Live View
Remote: Log Search/Interrogate Working Status	Remote: PTZ Control
Remote: Upgrade/Format	Remote: Manual Record
Remote: Two-way Audio	Remote: Playback
Remote: Shutdown/Reboot	
Remote: Notify Alarm Recipient/Trigger Alarm Output	
Remote: Video Output Control	
Remote: Serial Port Control	

7. Click **OK** to save the settings.

To delete a user:

1. Select the desired user under the **User** tab.
2. Click **Delete** button. A message box appears.

Note: Only the administrator can delete a user.

3. Click **Save** to save the changes.

Modify user information

You can easily change the information about a user such as their name, password and permissions.

To modify user information:

1. Select the desired user under the **User** tab.
2. Click the **Modify** button. The user management window appears
3. Change the information required.

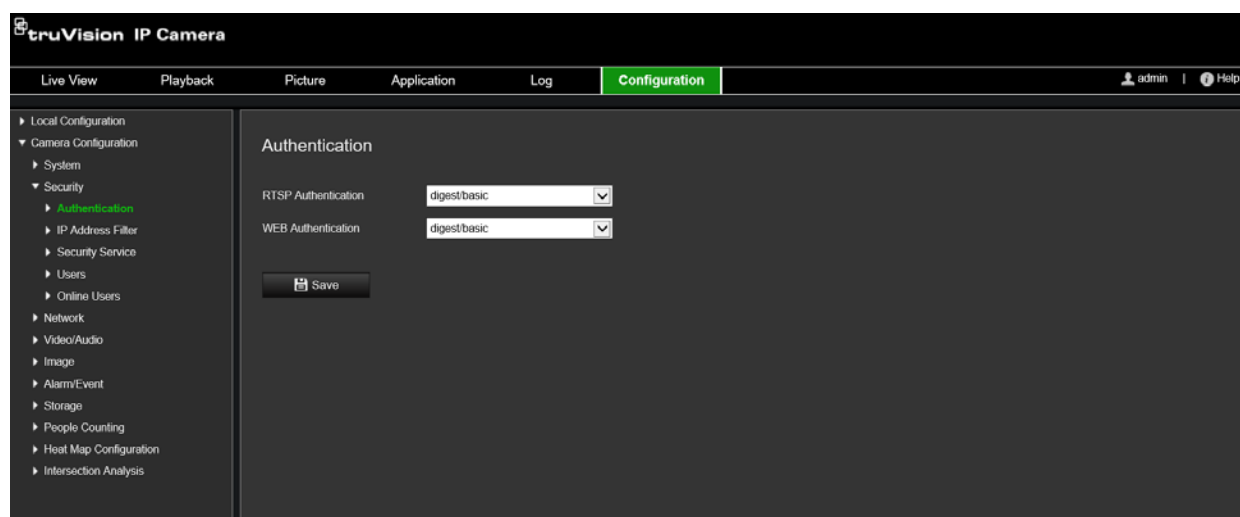
Note: The user “Admin” can only be changed by entering the admin password.

4. Click **Save** to save the changes.

RTSP authentication

You can specifically secure the stream data of the live view.

Figure 20: RTSP authentication window



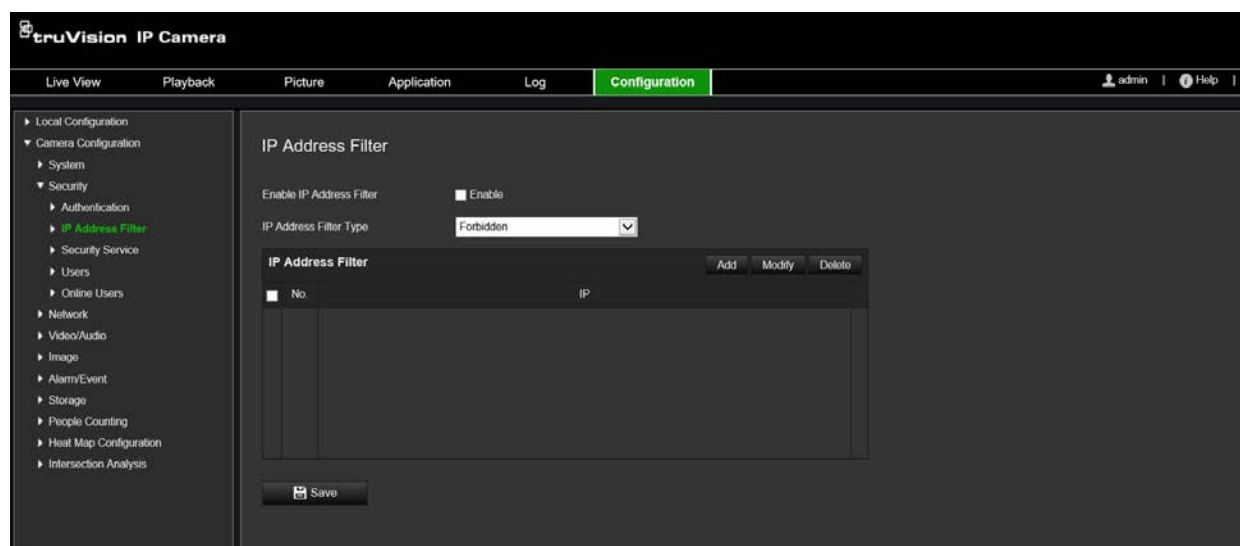
To define RTSP authentication:

1. From the menu toolbar, click **Configuration > Security > RTSP Authentication**.
2. Select the **RTSP Authentication** type **Digest/basic** or **Digest** in the drop-down list
3. Select the **WEB Authentication** type **Digest/basic** or **Digest** in the drop-down list
4. Click **Save** to save the changes.

IP address filter

This function allows you to give or deny access rights to defined IP addresses. For example, the camera is configured so that only the IP address of the server hosting the video management software is allowed to be accessed.

Figure 21: IP address filter window



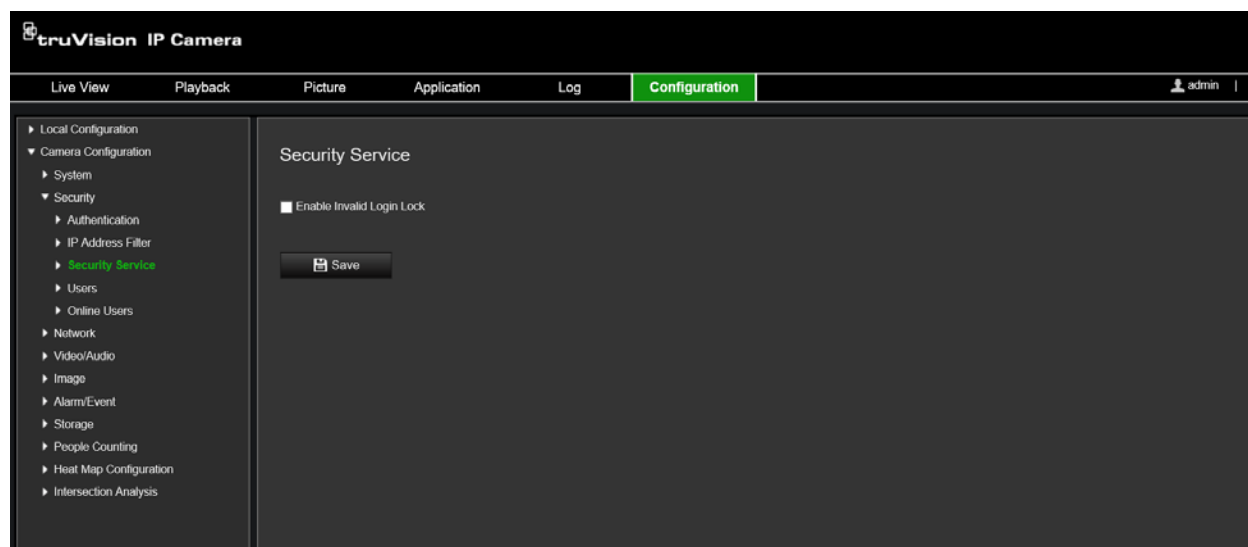
To define the IP address filter:

1. From the menu toolbar, click **Configuration > Security > IP Address Filter**.
2. Select the **Enable IP Address Filter** check box.
3. Select the type of IP Address Filter in the drop-down list: Forbidden or Allowed.
4. Click **Add** to add an IP address and enter the address.
5. Click **Modify** or **Delete** to modify or delete the selected IP address.
6. Click **Clear** to delete all the IP addresses.
7. Click **Save** to save the changes.

Defining the security service

This function enables Telnet and let you define its password. It is only used by Technical Support.

Figure 22: Security service window



To enable the illegal login lock:

1. Click **Configuration > Security > Security Service**.
2. Select the **Enable Illegal Login Lock** check box
3. Click **Save** to save the changes.

Note:

- The IP address will be locked if the admin user performs seven failed user name/password attempts (10 attempts for the operator/user).
- If the IP address is locked, you can try to login the device after five minutes.

Restore default settings

Use the Default menu to restore default settings to the camera. There are two options available:

- **Restore:** Restore all the parameters, except the IP parameters, to the default settings.
- **Default:** Restore all the parameters to the default settings.

Note: If the video standard is changed, it will not be restored to its original setting when **Restore** or **Default** is used.

To restore default settings:

1. From the menu toolbar, click **Configuration > System > Maintenance**.
2. Click either **Restore** or **Default**. A window showing user authentication appears.
3. Enter the admin password and click OK.
4. Click **OK** in the pop-up message box to confirm restoring operation.

Import/export a configuration file

The administrator can export and import configuration settings from the camera. This is useful if you want to copy the configuration settings to camera, or if you want to make a backup of the settings.

Note: Only the administrator can import/export configuration files.

To import/export configuration file

1. In **Camera Configuration > System**, click the **Maintenance** tab to open its window.
2. Click **Browse** to select the local configuration file and then click **Import** to start importing configuration file.
3. Click **Device Parameters** and set the saving path to save the configuration file.

Upgrade firmware

The camera firmware is stored in the flash memory. Use the upgrade function to write the firmware file into the flash memory.

You need to upgrade firmware when it has become outdated. When you upgrade the firmware, all existing settings are unchanged. Only the new features are added with their default settings.

The camera will select the corresponding firmware file automatically. Cookies and data in the web browser are automatically deleted when the firmware is updated.

To upgrade firmware version:

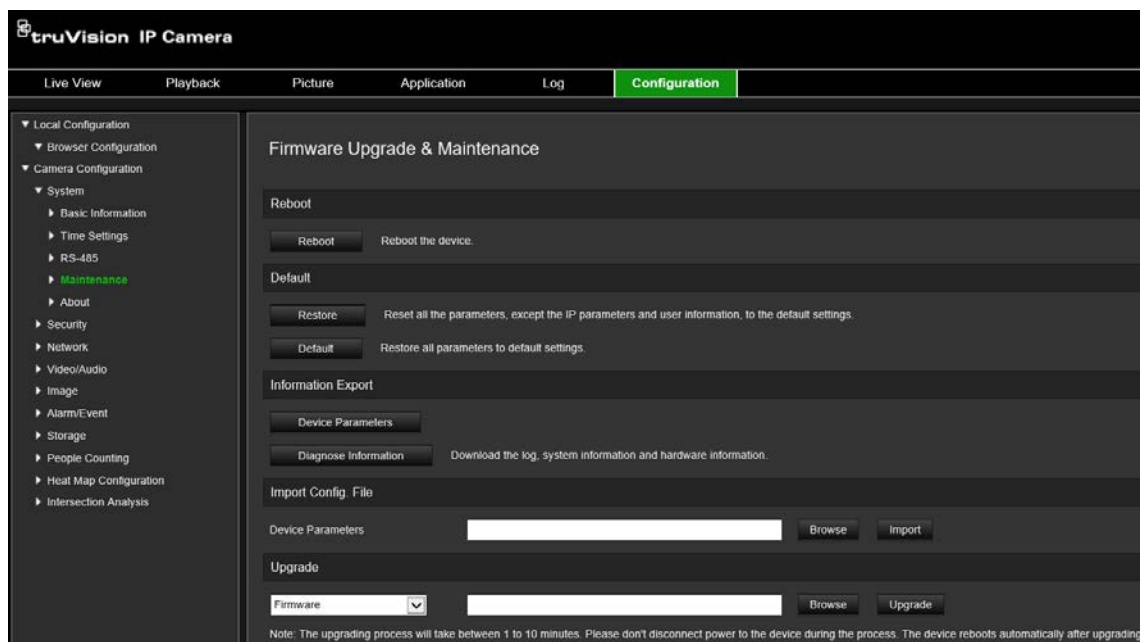
1. Download on to your computer the latest firmware from our web site at:

<https://firesecurityproducts.com>

2. When the firmware file is downloaded to your computer, extract the file to the desired destination.

Note: Do not save the file on your desktop.

3. From the menu toolbar, click **Configuration > Camera Configuration > System > Maintenance**. Under **Upgrade**, select the **Firmware** or **Firmware Directory** option. Then click the Browse button to locate latest firmware file on your computer.
 - **Firmware directory** – Locate the upgrading folder of Firmware files. The camera will choose the corresponding firmware file automatically.
 - **Firmware** – Locate the firmware file manually for the camera.



4. Click **Upgrade**. You will receive a prompt asking you to reboot the camera.
5. When the upgrade is finished, the device will reboot automatically. The browser will also be refreshed.

To upgrade the firmware via TruVision Device Manager:

1. In the **FW upgrader** panel, select a device or hold the Ctrl or Shift key to select multiple devices for simultaneous upgrading.
2. Click the **Browse** button to locate the firmware file to use.

If you want the device to automatically reboot after the upgrade, check **Reboot the device after upgrading**. When checked, it will also display **Restore default settings** option. Check it if you want to restore all parameters.

3. Click **Upgrade**.

Note: The upgrading process will be 1 to 10 minutes, please don't disconnect power to the device during the process. The device reboots automatically after upgrading.

Reboot camera

It is easy to reboot the camera remotely.

To reboot the camera through the web browser:

1. In **Camera Configuration > System**, click the **Maintenance** tab.
2. Click the **Reboot** button to reboot the device.
3. Click **OK** in the pop-up message box to confirm reboot operation.

Camera operation

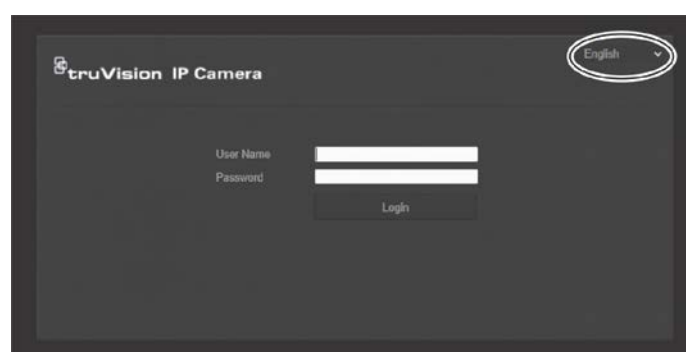
This chapter describes how to use the camera once it is installed and configured.

Log on and off

You can easily log out of the camera browser window by clicking the Logout button on the menu toolbar. You will be asked each time to enter your user name and password when logging in.

On the upper left corner of the logon window, you can select the language of the Browser. It supports several languages.

Figure 23: Login dialog box



Live view mode

Once logged in, click “Live View” on the menu toolbar to access live view mode. See Figure 1 on page 9 for the description of the interface.

Play back recorded video

You can easily search and play back recorded video in the playback interface.

Note: You must configure NAS or insert an SD card in the camera to be able to use the playback functions.

To search recorded video stored on the camera’s storage device for playback, click **Playback** on the menu toolbar. The Playback window appears. See Figure 24 on page 84.

Figure 24: Playback window




Name	Description
1. Search calendar	Click the day required to search.
2. Search	Start search.
3. Timeline	<p>The timeline bar displays the 24-hour period of the day being played back. It moves left (oldest) to right (newest). The bar is color-coded to display the type of recording.</p> <p>Click a location on the timeline to move the cursor to where you want playback to start. The timeline can also be scrolled to earlier or later periods for play back.</p> <p>Click to zoom out/in the timeline bar.</p>
4. Control playback	Click to control how the selected file is played back: play, stop, slow, and fast forward playback.
5. Archive functions	<p>Click these buttons for the following archive actions:</p> <p> Capture a snapshot image of the playback video.</p> <p> Start/Stop clipping video files.</p>
6. Audio control	Modify the audio level.
7. Time bar	The vertical bar shows where you are in the playback recording. The current time and date are also displayed.
8. Download functions	Download video files.
9. Recording type	<p>The color code displays the recording type in the timeline. Blue indicates continuous recording. Red indicates alarm recording. Yellow indicates manual recording. Black is no recording.</p> <p>The recording type name is also displayed in the current status window.</p>
10. Set playback time	Input the time and click to locate the playback point.
11. Zoom in/out	Click to zoom in or out of the timeline bar.


To play back recorded video

1. Select the date and click the **Search** button. The searched video is displayed in the timeline.
2. Click **Play** to start playback. While playing back a video, the timeline bar displays the type and time of the recording. The timeline can be manually scrolled using the mouse.


Note: You must have playback permission to playback recorded images. See “Modify user information” on page 77 for more information.

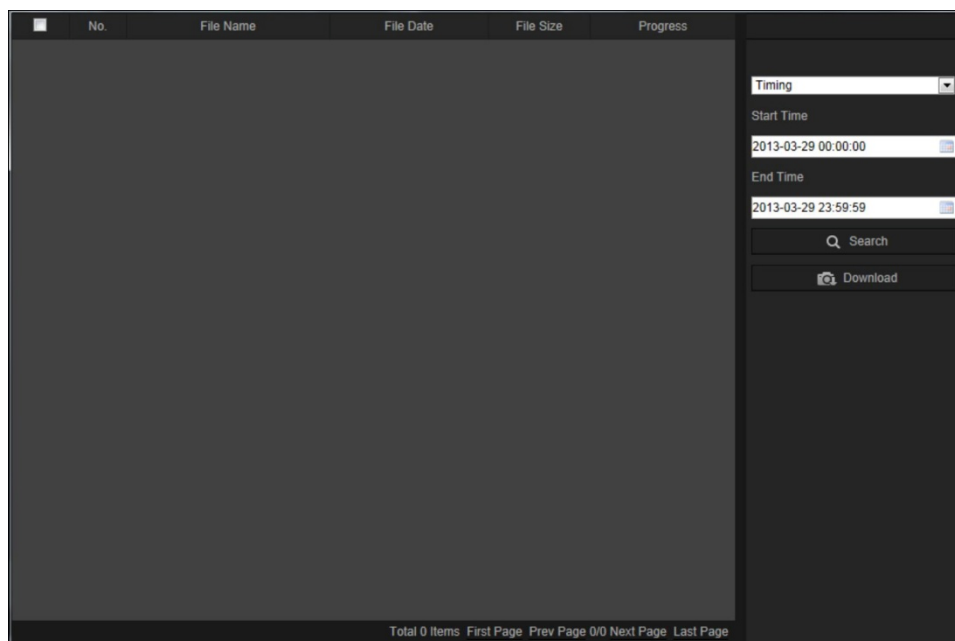
3. Select the date and click the **Search** button to search for the required recorded file.
4. Click  to search the video file.
5. In the pop-up window, select the box of the video file and click **Download** to download the video files.

To archive a recorded video segment during playback:

1. While playing back a recorded file, click  start clipping. Click it again to stop clipping. A video segment is created.
2. Repeat step 1 to create additional segments. The video segments are saved on your computer.

To archive recorded snapshots:

1. Click  to open the snapshots search window.



2. Select the snapshot type as well as the start and end times.
3. Click **Search** to search for the snapshots.
4. Select the desired snapshots, and click **Download** to download them.

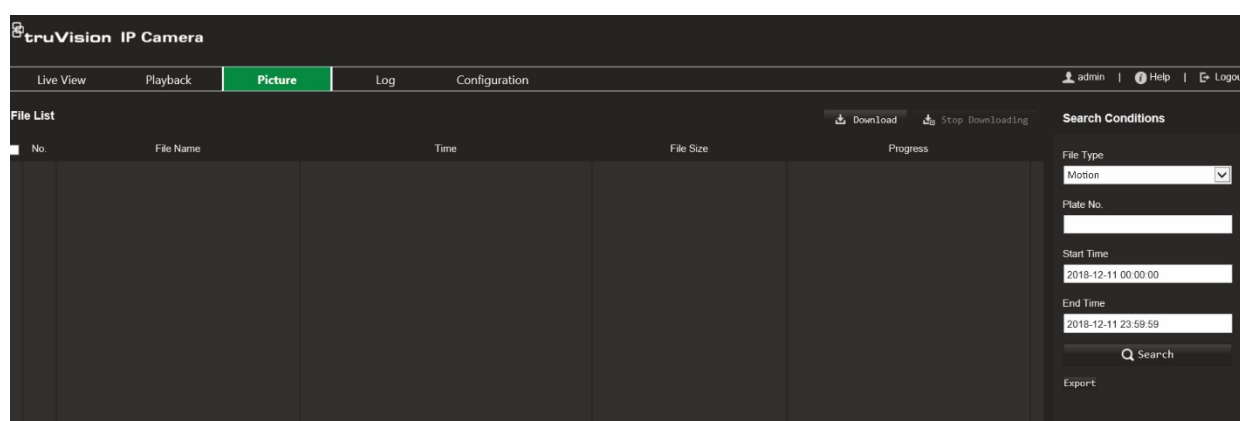
Snapshots

Click *Picture* to enter the interface to search for snapshots. You can search, view, and download the snapshots stored in the local storage or network storage.

Notes:

- Make sure that the HDD, NAS, or memory card are properly configured before you carry out the snapshot search.
- Make sure that the capture schedule is configured. Go to Configuration > Storage > Snapshot to set the capture schedule.

Figure 25: Picture window



To search snapshots:

1. From the menu toolbar, click **Picture**.
2. Select the file type from the dropdown list: Continuous, Motion, Alarm, Cross Line Detection, Intrusion Detection, Region Entrance Detection, Region Exiting Detection, Unattended Baggage Detection, or Object Removal Detection.
3. Select the start time and end time.
4. Click **Search** to search the matched snapshot.
5. Select the check box for snapshots and click **Download** to download the selected snapshots.

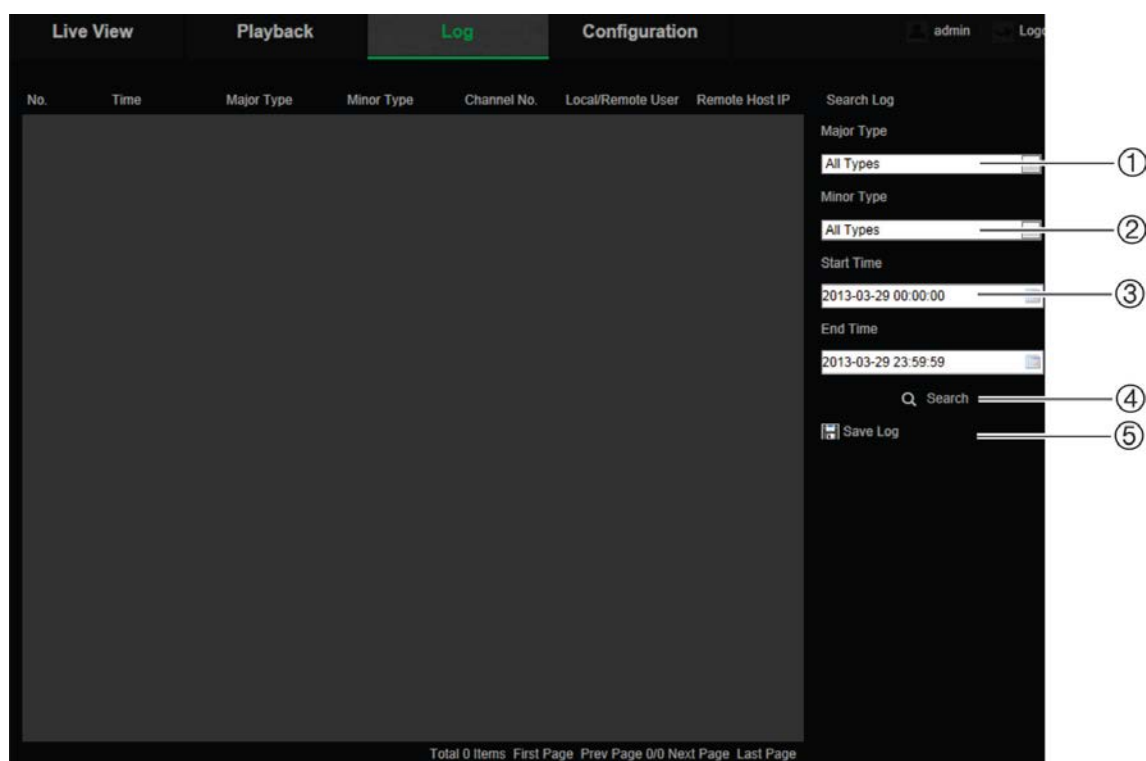
Search event logs

You must configure NAS or insert a SD card in the dome camera to be able to use the log functions.

The number of event logs that can be stored on NAS or SD card depends on the capacity of the storage devices. When this capacity is reached, the system starts deleting older logs. To view logs stored on storage devices, click **Log** on the menu toolbar. The Log window appears.

Note: You must have view log access rights to search and view logs. See “Modify user information” on page 77 for more information.

Figure 25: Log window



1. Major Type
2. Minor Type
3. Start and end search time
4. Start search
5. Save searched logs

You can search for recorded logs by the following criteria:

Major type: There are three types of logs: Alarm, Exception, and Operation. You can also search all logs. See Table 2 below for their descriptions.

Minor type: Each major type has some minor types. See Table 2 below for their descriptions.

Date and Time: Logs can be searched by start and end recording time.

Table 2: Types of logs

Log type	Description of events included
Alarm	Start Motion Detection, Stop Motion Detection, Start Tamper-proof, Stop Tamper-proof
Exception	Invalid Login, HDD Full, HDD Error, Network Disconnected and IP Address Conflicted
Operation	Power On, Unexpected Shutdown, Remote Reboot, Remote Login, Remote Logout, Remote Configure parameters, Remote upgrade, Remote Start Record, Remote Stop Record, Remote PTZ Control, Remote Initialize HDD, Remote Playback by File, Remote Playback by Time, Remote Export Config File, Remote Import Config File, Remote Get Parameters, Remote Get Working Status, Start Bidirectional Audio, Stop Bidirectional Audio, Remote Alarm Arming, Remote Alarm Disarming

To search logs:

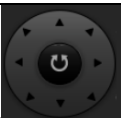










1. From the menu toolbar, click **Log** to display the Log window.
2. In the Major Type and Minor Type drop-down list, select the desired option.
3. Select start and end time of the log.
4. Click **Search** to start your search. The results appear in the left window.

Operating PTZ control

On the live view page, click  to show the PTZ control panel, and click  to hide it.

Figure 26: PTZ control panel



Icon	Description
	Directional buttons: Controls the movements and directions of the PTZ. Center button is used to start auto-pan by the camera.
	Adjust Zoom out/Zoom in.
	Adjust Focus - / Focus +.
	Adjust Iris - / Iris +.
	Adjust the speed of pan/tilt movements
	Turns on/off the LED. This function is supported by cameras with a RS-485 port.
	Turns on/off camera wiper. This function is supported by cameras with a RS-485 port.
	Auxiliary focus.
	Initialize the lens.
	Start manual tracking.
	Start 3D zoom.

Preset and preset tours



Presets are defined locations of a PTZ dome camera that allow you to quickly move the PTZ dome camera to a desired position.

A preset tour is a memorized series of presets. The camera stays at a preset for a set dwell time before moving on to the next preset. A preset tour can be configured with up to 32 presets.

Figure 27: Preset tour panel





To set a preset:

1. Click  to show the PTZ control panel.
2. Click the directional / zoom buttons on the PTZ control panel to adjust the PTZ view as desired.
3. Select a preset number from the preset list.
4. Click the icon  to save the current PTZ View as the preset.


The preset name turns from grey to black.

To call up a preset:

1. Click  to show the PTZ control panel.
2. Select the preset number from the Preset list.
3. Click the icon  to call the selected preset.

The selected PTZ view will move to the pre-defined preset scene.

To delete a preset:







1. Select the desired preset number from the Preset list.
2. Click the icon  to delete the selected preset.

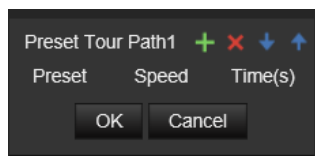
The preset name turns from black to grey.

To set a preset tour:

Before you start:

At least two presets are required to set a preset tour.




1. Click the icon  to enter the preset tour configuration interface.
2. Select a path number from the drop-down list, and click the icon  to configure preset tour path.
3. Click  to add a preset to the path, and click  to delete a preset.
4. Set the preset number, speed, and dwell time for each preset. You can adjust the order of presets by using  and .




5. Click **OK** to save preset tour path.

Note: Up to 32 patrol paths can be set, and each path supporting up to 16 key points.

To call a preset tour:

1. Click  to show the PTZ control panel.
2. Select the preset tour path number from the drop-down list.
3. Click the icon  to start the selected preset tour and  to stop it.

To delete a preset tour:

1. Select the preset tour path number from the preset tour list.
2. Click the icon  to delete the selected preset tour path.

Index

A

- alarm inputs
 - set up, 41
- alarm outputs
 - set up, 41
- alarm types
 - motion detection, 35
- archive files
 - recorded files, 84
 - snapshots of recorded files, 84
- archived files
 - play back, 84
- archiving files
 - default directories, 12
- audio parameters, 25

B

- backlight setup, 31

C

- camera image
 - set up, 28
- camera name
 - display, 32
- config file
 - import, 16
- configuration file
 - import/export, 79

D

- day/night switch, 30
 - scheduled, 30
- day/night switch, 28
- default settings
 - restore, 79
- detection
 - audio exception, 43
 - cross line, 47
 - intrusion, 45
 - object removal, 53
 - region entrance, 49
 - region exiting, 51
 - unattended baggage, 52
- display control, 9
- display information
 - set up, 32
- dual-VCA, 27

E

- email parameters
 - set up, 22

events

- search logs, 85
- exception alarms
 - types, 42

F

- firmware upgrade, 79
 - use TruVision Navigator, 80

H

- hard drive
 - capacity, 59
 - card full, 59
 - formatting, 59
- hardware display mode, 9
 - heat map statistics, 70
- HDD error alarm, 42
- HDD full alarm, 42
- heat map
 - set up, 64
 - statistics, 70
- HTTPS parameters
 - set up, 23

I

- intersection analysis
 - results, 72
 - set up, 66
- invalid login alarm, 42
- IP address conflicted alarm, 42

L

- language
 - change, 82
- live view
 - start, 82
- log on and off, 82
- logs
 - information type, 86
 - search logs, 85
 - view logs, 85

M

- motion detection
 - advanced mode, 38
 - normal mode, 36

N

- NAS settings, 60
- network, 42
- network protocol

- setup, 12
- network settings
 - 802.1x, 24
 - DDNS, 20
 - FTP, 22
 - local camera parameters, 12
 - port parameters, 21
 - PPPoE, 21
 - QoS, 24
 - SNMP, 21
 - TC/IP, 20
- network settings, 18
- NTP synchronization, 15

P

- password activation, 5
- passwords
 - modify, 76
- people counting
 - set up, 61
 - statistics, 68
- picture overlay, 34
- playback
 - play back recorded files, 84
 - search recorded video, 82
- post-recording times
 - description, 55
- pre-recording times
 - description, 55
- preset
 - set/call up/delete, 88
- privacy masks, 33
- PTZ control, 87

R

- reboot camera, 16, 81
- record
 - playback, 82
- recording
 - parameters, 25
 - recoding schedule, 55
- region of interest, 27
- restore default settings, 16
- RS-485 set up, 16
- RTSP authentication, 77

S

- SDHC card
 - formatting, 59
 - free space available, 59
- self-signed certificate set up, 23
- snapshot setup
 - event-triggered snapshots, 57
 - scheduled snapshots, 57
- snapshots
 - archive snapshots, 84
- software display mode, 9
- streaming
 - main/sub setup, 12
- system time
 - set up, 15

T

- tamper-proof alarms
 - set up, 40
- TruVision Navigator
 - upgrade firmware, 80

U

- upgrade firmware, 16
- user settings, 74
- users
 - add new user, 75
 - delete user, 76
 - modify password, 76
 - types of users, 74

V

- video parameters, 25
- video quality, 28

W

- web browser
 - overview of the interface, 7
- web browser security level, 4
- white balance, 31