



TruVision Series 7 IP Camera Configuration Manual

Copyright	© 2020 Carrier. All rights reserved.
Trademarks and patents	Trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.
Disclaimer	Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Carrier Global Corporation or its affiliate companies.
Manufacturer	Carrier Fire & Security B.V. Kelvinstraat 7, 6003 DH Weert, The Netherlands
FCC compliance	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.
FCC conditions	This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference. (2) This Device must accept any interference received, including interference that may cause undesired operation.
Canada	This Class A digital apparatus complies with CAN ICES-003 (A)/NMB-3 (A). Cet appareil numérique de la classe A est conforme à la norme CAN ICES-003 (A)/NMB-3 (A).
cUL	Safety Instructions: Improper use or replacement of the battery may result in explosion hazard. Replace with the same or equivalent type only. Dispose of used batteries in conformance with the local codes. Instructions de sécurité : L'utilisation ou le remplacement inadéquats de la pile peuvent entraîner un risque d'explosion. Remplacez-la par le même type ou l'équivalent du même type seulement. Jetez les piles usagées conformément aux directives fournies par le fabricant de la pile.
ACMA compliance	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.
Certification	   
EU directives	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.
 	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.

**Product warnings and
disclaimers**

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.

For more information on warranty disclaimers and product safety information, please check www.firesecurityproducts.com/policy/product-warning/ or scan the following code:



Content

Introduction 3

Contact information and manuals /tools /firmware 4

Network access 5

Access with browsers other than Microsoft Internet Explorer 5

Checking your web browser security level 6

Activating the camera 7

Overview of the camera web browser 9

Camera configuration 11

Local configuration 11

Configuration 12

Basic information 14

Time settings 14

RS-485 16

Metadata Settings 16

Housing settings 17

Open source software available 17

Maintenance 18

Security 19

Authentication 19

IP address filter 20

Security service 21

Advanced security 22

Certificate management 24

Security audit log 27

Users 29

Online users 32

Network 33

Video and Audio 48

Image 53

OSD (On Screen Display) 56

Privacy masks 58

Picture overlay 59

Image parameters switch 59

Motion detection alarms 60

Video tampering 66

Alarm inputs and outputs 68

Exception alarms 69

Audio exception detection 70

Defocus detection 72

Scene change detection 73

Face detection 74

Intrusion detection 76

Cross line detection	78
Region entry detection	80
Region exit detection	82
Unattended baggage detection	83
Object removal detection	85
Recording schedule	86
Scheduled snapshots	89
HDD management	91
NAS management	93
Object counting	94
e-PTZ	95
Camera management	98
Restore default settings	98
Import/export a configuration file	98
Upgrade firmware	99
Reboot camera	100
Camera operation	101
Logging on and off	101
Live view mode	101
Playing back recorded video	101
Search snapshots	104
Search application statistics	105
Search event logs	106
PTZ and General control panels	107
Index	111

Introduction

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

- TVC-5711 (2MP IP box camera)
- TVC-5712 (4MP IP box camera)
- TVC-5713 (8MP IP box camera)
- TVC-5714 (12MP IP box camera)

- TVB-5711 (2MP IP bullet camera, 2.8 to 12 mm)
- TVB-5712 (2MP IP bullet camera, 8 to 32 mm)
- TVB-5713 (4MP IP bullet camera, 2.8 to 12 mm)
- TVB-5714 (4MP IP bullet camera, 8 to 32 mm)
- TVB-5715 (8MP IP bullet camera, 2.8 to 12 mm)
- TVB-5716 (8MP IP bullet camera, 8 to 32 mm)
- TVB-5717 (12MP IP bullet camera, 2.8 to 12 mm)

- TVD-5711 (2MP IP indoor dome, 2.8 to 12 mm)
- TVD-5712 (4MP IP indoor dome, 2.8 to 12 mm)
- TVD-5713 (8MP IP indoor dome, 2.8 to 12 mm)
- TVD-5714 (12MP IP indoor dome, 2.8 to 12 mm)
- TVD-5715 (2MP IP outdoor dome, 2.8 to 12 mm)
- TVD-5716 (2MP IP outdoor dome, 8 to 32 mm)
- TVD-5717 (4MP IP outdoor dome, 2.8 to 12 mm)
- TVD-5718 (4MP IP outdoor dome, 8 to 32 mm)
- TVD-5719 (8MP IP outdoor dome, 2.8 to 12 mm)
- TVD-5720 (8MP IP outdoor dome, 8 to 32 mm)
- TVD-5721 (12MP IP outdoor dome, 2.8 to 12 mm)

You can download the following manuals from our web site:

- TruVision Series 7 IP Camera Installation Guide
- TruVision Series 7 IP Camera Configuration Manual

The manuals are available in several languages on the EMEA web site.

Contact information and manuals /tools /firmware

For contact information and to download the latest manuals, tools, and firmware, go to the web site of your region:

EMEA:	firesecurityproducts.com Manuals are available in several languages.
Australia/New Zealand:	utcfs.com.au

Network access

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

TruVision IP cameras can be configured and fully controlled using Microsoft Internet Explorer (IE) and other browsers. The procedures described in this manual are based on Microsoft Internet Explorer (IE) web browser.

Access with browsers other than Microsoft Internet Explorer

In addition to Microsoft Internet Explorer the camera can also be accessed using other browsers like Google Chrome (from version 45), Apple Safari (from version 12) and Firefox (from version 52). These additional browsers don't support ActiveX plugins like Internet Explorer and therefore some limitations apply.

When using Chrome, Safari or Firefox, the maximum supported resolution is 1080p.

Table 1: Comparison between the different browsers

Model	Function	Chrome, Safari & Firefox	MS Internet Explorer
Live View	Live view	Resolution <= 1080P Bit rate <= 2048 Kbps	✓
	Audio	✓	✓
	Capture	✓	✓
	Digital zoom	✓	✓
	Window division	✓	✓
	Full screen	✓	✓
	Record	✓ (Chrome only)	✓
	Audio on	✗	✓
Playback	Playback	✗	✓
	Download video	✗	✓
Picture	Picture	✗	✓
Counting Statistics	Counting Statistics	✗	✓
Configuration	Export device parameters	✓	✓
	Import device parameters	✓	✓
	Upgrade	✓ (Only the dav format file supported)	✓
	Draw area	✓	✓

Model	Function	Chrome, Safari & Firefox	MS Internet Explorer
	Counting	Only supports drawing detection line. OSD display is not supported.	
	Export log	✓	✓
	Local	✗	✓
	File path setting	✗	✓

We always recommend using the latest browser versions.

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. 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.

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".

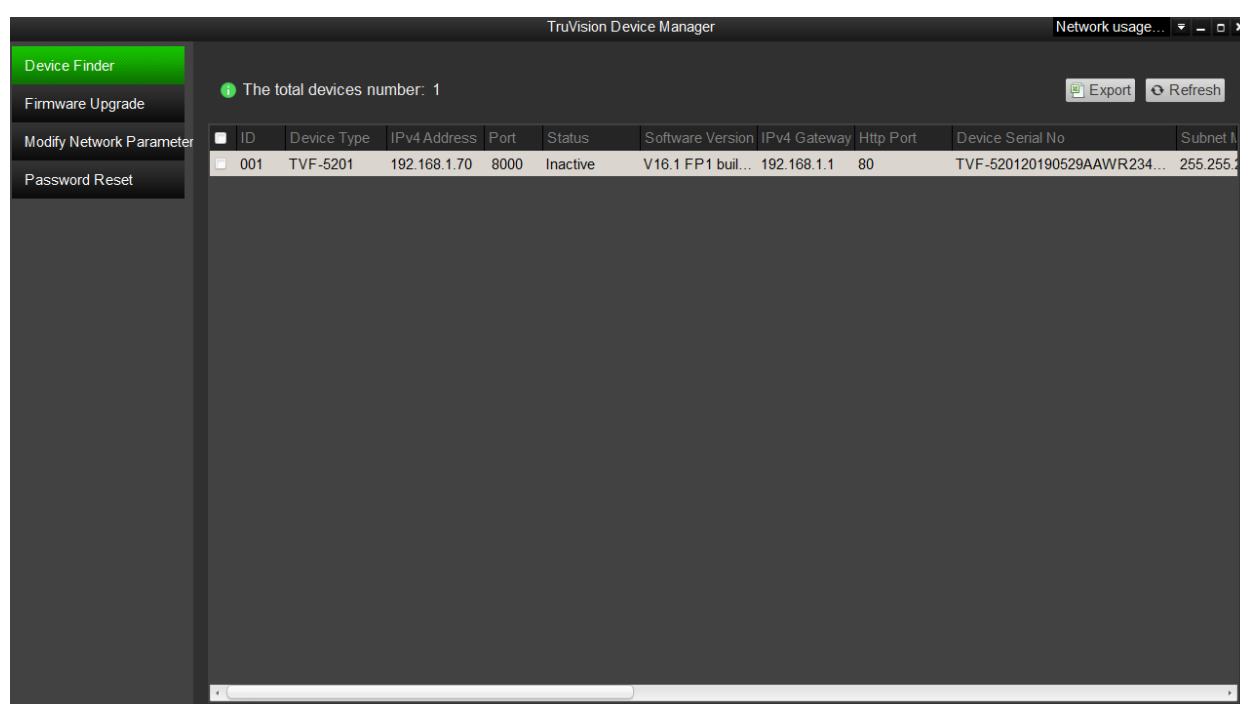
3. Enter the password in the password field.

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. Select 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 selecting 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

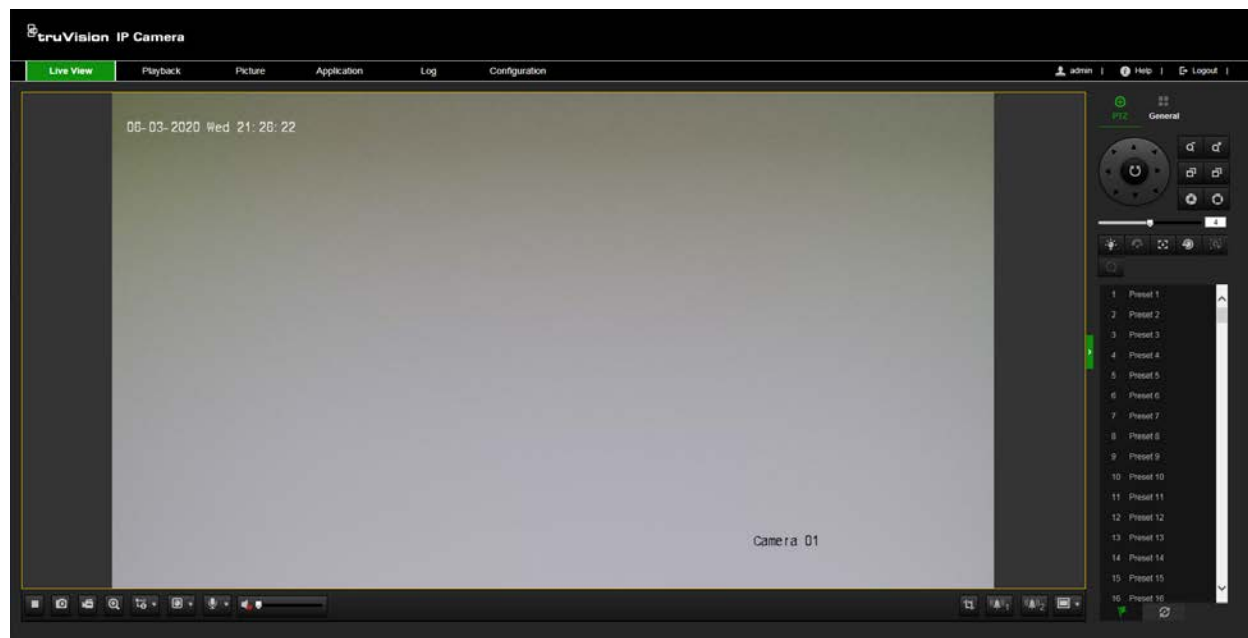
- Input the password and click the **Save** button to activate your IP address modification.

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.

Figure 1: Browser interface (Live view shown)



Name	Description
Live view	Click to view live video.
Playback	Click to play back video.
Picture	Click to search snapshots.
Application	Click to search, view, download the counting data stored in the local storage or network storage.
Log	Click to search for event logs.

Name	Description
Configuration	Click to configuration the camera.
Admin	Displays current user logged on.
Help	Click to open the camera help pages.
Logout	Click to log out from the system.

In the live view window, click the toolbar to start the live view of the camera.

Icon	Description
	Manually start/stop live view
	Take a snapshot of selected camera channel (Run browser as administrator)
	Manually start/stop recording (Run browser as administrator)
	Start/stop digital zoom function
	Turn on/off microphone
	Switch between live main stream and substream
	Audio on and adjust volume or make mute
	Count pixels in the image
	Manual alarm output control
	Aspect ratio of 4:3
	Aspect ratio of 16:9
	The original size
	Original ratio in the adapted window
	Self-adaptive aspect ratio

PTZ and General control panels

On the live view page, you can click  to show the PTZ/General control panels and click  to hide. See “PTZ and General control panels” on page 107 for further information on using these panels.

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.

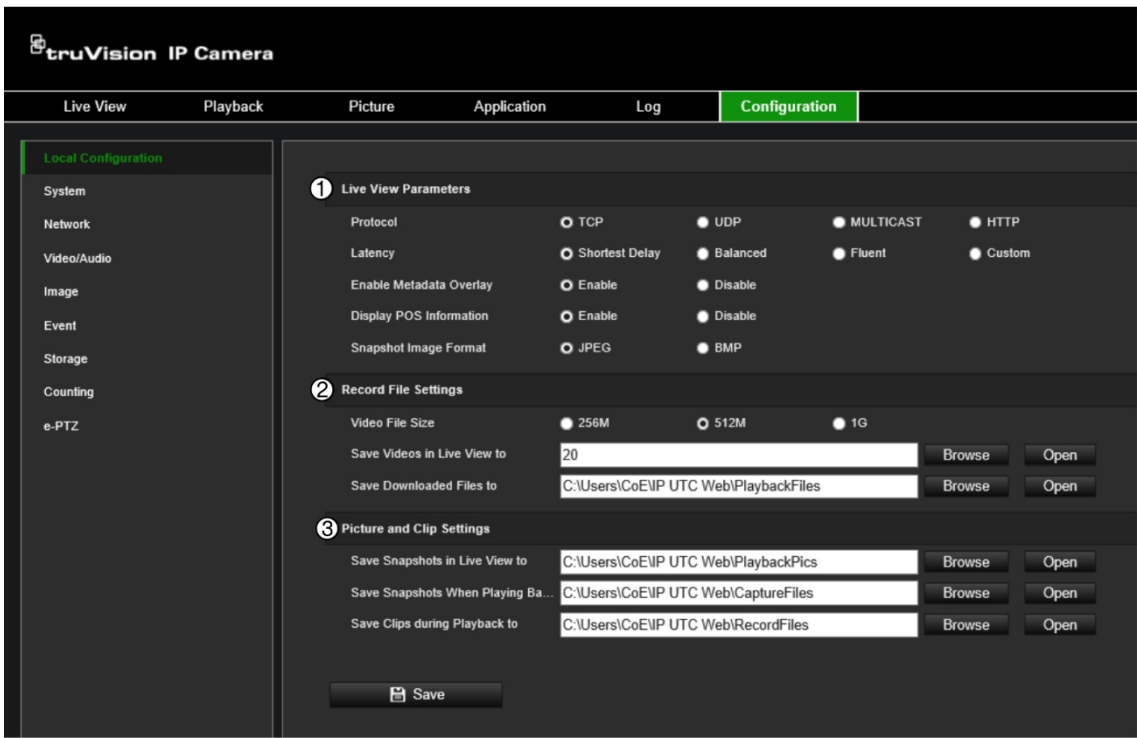
There are two main folders in the configuration panel:

- 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



Parameters	Description
1. Live View Parameters	
Protocol	Specifies the network protocol used. Options include TCP, UDP, MULTICAST and HTTP.

Parameters	Description
	TCP: Ensures complete delivery of streaming data and better video quality. However 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 is 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	Enabling this function will dynamically display (detected) targets/ objects/ movements in the live image.
Display POS Information	Enable the function, feature information of the detected target is dynamically displayed near the target in the live image.
Snapshot Image Format	Specifies the snapshot format as JPEG or BMP.
2. Record File Settings	
Record File Size	Specifies the maximum file size for manually recorded video Options include: 256 MB, 512 MB, and 1 G.
Save Record Files to	Specifies the directory for recorded files.
Save Downloaded Files to	Specifies the directory for downloaded files.
3. Snapshot and Clip Settings	
Save Snapshots In Live View To	Specifies the directory for saving snapshots in live view mode.
Save Snapshots When 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 13 for descriptions of the configuration folders available.

Figure 3: Configuration window (Basic Information window selected)

truVision IP Camera

Live View Playback Picture Application Log **Configuration**

Local Configuration

- 1 System
 - System Settings**
 - Maintenance
 - Security
 - Users
- 2 Network
- 3 Video/Audio
- 4 Image
- 5 Event
- 6 Storage
- 7 Counting
- 8 EPTZ

Basic Information Time Settings RS-485 metadata Settings About

Device Name	IP CAMERA
Device No.	88
Model	
Serial No.	20200509AAWRD75315847
Firmware Version	V19.1 FP1
Encoding Version	V7.3 build 190918
Web Version	V4.0.51 build 200601
Plugin Version	3.0.7.1802
Number of Channels	1
Number of HDDs	0
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 device number and the current firmware version, maintenance, security settings and user settings. See “Basic information” on page 14 for further information.
2. Network	Defines the network parameters required to access the camera over the internet. See page 19 for further information.
3. Video/Audio	Defines the recording parameters. See page 33 for further information.
4. Image	Defines the image parameters, OSD settings, overlay text, and privacy masking. See page 48 for further information.
5. Event	Defines motion detection, tamper-proof, alarm input/output, exception settings, audio exception, defocus detection, scene change detection, face detection, intrusion detection, cross line detection, region entrance detection, region exiting detection, unattended baggage detection, object removal detection. See pages 60 to 85 for further information on the different event types.
6. Storage	Defines recording schedule, storage management and NAS configuration. See pages 86 to 93 for further information.
7. Counting	Defines the calculations of the number of objects crossing line configured in the camera view. It is and is widely used for entrances or exits. See “Object counting” on page 94 for more information.
8. e-PTZ	Defines the PTZ style application in the field of non-PTZ camera. Only available via the fourth stream. See “e-PTZ” on page 95 for more information.

Basic information

This menu under **Configuration > System > Basic Information** displays the following information:

Device name	Plugin version
Device number	Number of channels
Model	Number of HDDs
Serial number	Number of alarm inputs
Firmware version	Number of alarm outputs
Encoding version	Firmware version property
Web version	

Only the device name and device number can be changed (see “Configuration” on page 12). All other information is read-only.

Time settings

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 > System Settings > Time Settings**.

The screenshot shows the 'truVision IP Camera' configuration interface. The top navigation bar includes 'Live View', 'Playback', 'Picture', 'Application', 'Log', and 'Configuration' (highlighted in green). The left sidebar lists 'Local Configuration' with sub-items: 'System' (highlighted), 'Maintenance', 'Security', 'Users', 'Network', 'Video/Audio', 'Image', 'Event', 'Storage', 'Counting', and 'EPTZ'. The main content area is titled 'Time Settings' and includes tabs for 'Basic Information', 'Time Settings' (active), 'metadata Settings', 'Housing', and 'About'.

Under 'Time Settings', the 'Time Zone' is set to '(GMT+01:00) Amsterdam, Berlin, Rome, Paris'. The 'NTP' section has a radio button selected for 'NTP', with fields for 'Server Address' (time.windows.com), 'NTP Port' (123), and 'Interval' (1440 minute(s)), plus a 'Test' button. The 'Manual Time Sync.' section has a radio button selected for 'Manual Time Sync.', with fields for 'Device Time' (2020-06-01T09:46:59) and 'Set Time' (2020-06-01T02:46:58), and a checkbox for 'Sync. with computer time'. The 'Daylight Savings Time' section has a checkbox for 'Enable DST', and fields for 'Start Time' (Mar, Last, Sun, 02), 'End Time' (Oct, Last, Sun, 02), and 'DST Offset' (60minute(s)). A 'Save' button is at the bottom.

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 the **NTP** enable check box 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.

RS-485

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 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 > System Settings > RS485**.

Basic Information	Time Settings	RS-485	metadata Settings	About
Baud Rate		9600		
Data Bit		8		
Stop Bit		1		
Parity		None		
Flow Ctrl		None		
PTZ Protocol		PELCO-D		
PTZ Address		0		

Save

2. Select the RS-485 port parameters.

Note: The Baud Rate, PTZ Protocol, and PTZ Address parameters should be identical to the PTZ camera parameters.

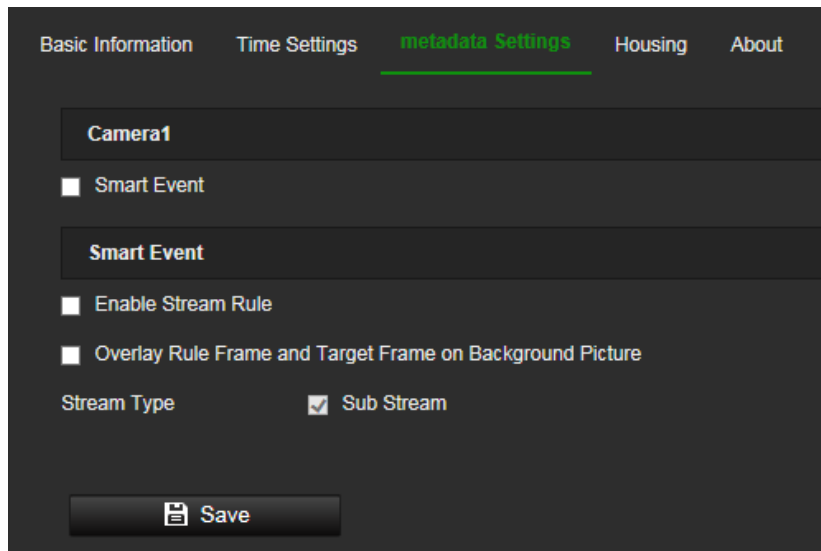
3. Click Save to save changes.

Metadata Settings

Metadata is the raw data the camera collects before algorithm processing. The metadata of intrusion detection, line crossing detection, region entrance detection, region exiting detection, unattended baggage detection, object removal and face capture can be uploaded. If enabled, the metadata of the corresponding event are available for users to explore the possibility of various data usage.

To set up metadata settings:

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

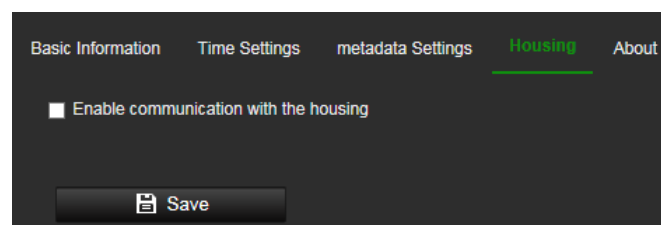


2. Select the **Smart Event** check box to enable the metadata function. The metadata of the smart event includes the target ID, target coordinates and time information.
3. Select **Enable Stream Rule** to overlay the stream rule metadata on the live view stream. The metadata in the video stream requires certain players to decode and display. Make sure you have selected **Substream** here and **Substream** in live view.
4. Select **Overlay Rule Frame and Target Frame on Background Picture** to enable the function. The bounding boxes does not require proprietary players to decode and display. Make sure you have selected **Substream** here and **Substream** in live view.

Housing settings

This page only applies to the TVC-571x Box cameras. Select the option **Enable** communication with the housing to allow communication between the box camera and the TVC-OH3-HT housing connected to it. The communication between camera and housing is done via a wired RS-485 connection and is used for the camera to tell the housing when the IR LEDs of the housing need to be switched on. This typically happens when the camera switches to night mode.

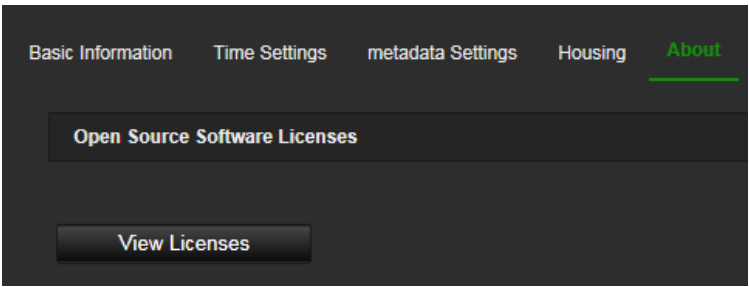
Figure 4: Housing window



Open source software available

To obtain information about the open source software that applies to the IP camera, select **Configuration > System Settings > About**. Click the button “View Licenses” to review Open Source Software Licenses.

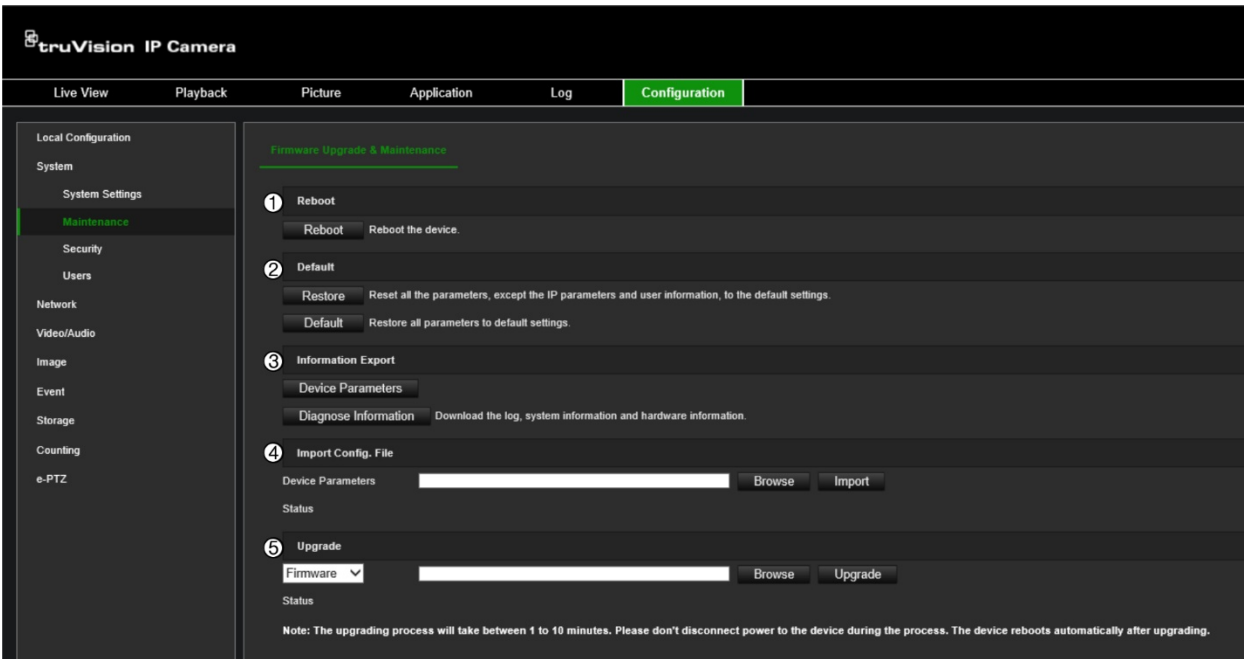
Figure 5: Open Source Software Licenses



Maintenance

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

Figure 6: Maintenance window



Parameters	Description
1. Reboot	Reboot the device.
2. Default	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. Notes: • After restoring the default settings, the IP address is also restored to the default IP address. Please use this function carefully. • For cameras that support Wi-Fi, wireless dial, or WLAN function. This restore action does not restore the related settings of mentioned functions to default.

3.	Information Export	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. When exporting a file, you need to create an encrypted password, which then required when later importing the file to another camera. Note: Only the administrator can import/export configuration files. The Diagnose Information button is used only by Technical Support.
4.	Import Config File	The configuration file is used for the batch configuration of cameras. Note: You need to reboot the camera after importing the configuration file
5.	Upgrade	Upgrade the device to the latest available firmware version. 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. You can also upgrade the firmware version using TruVision Device Manager. However, we recommend restoring the camera to factory defaults after upgrading the firmware Note: The firmware upgrade process can take between 1 to 10 minutes. Do not disconnect power to the camera during the process. The camera reboots automatically after upgrade.

Security

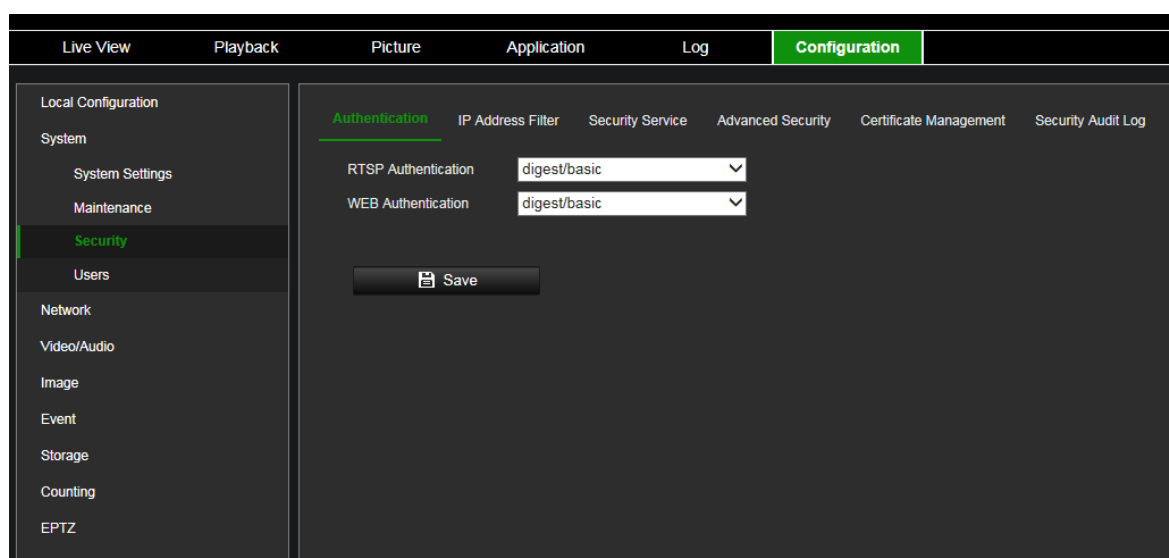
Security related parameters, such as user accounts and IP address filter, can be managed via the camera menu **Configuration > Security**.

Authentication

You can secure the stream data of the live view.

To define RTSP authentication:

1. From the menu toolbar, click **Configuration > System > Security > Authentication**.



2. Select the **RTSP Authentication** type: **digest/basic** or **digest** in the drop-down list.

Note: Digest/Basic is the default value and needs to be used when the camera is used with TruVision Navigator.

3. Select the **Web Authentication** type: **digest/basic** or **digest** in the drop-down list.

Note: Web authentication is the authentication between the camera and the web browser.

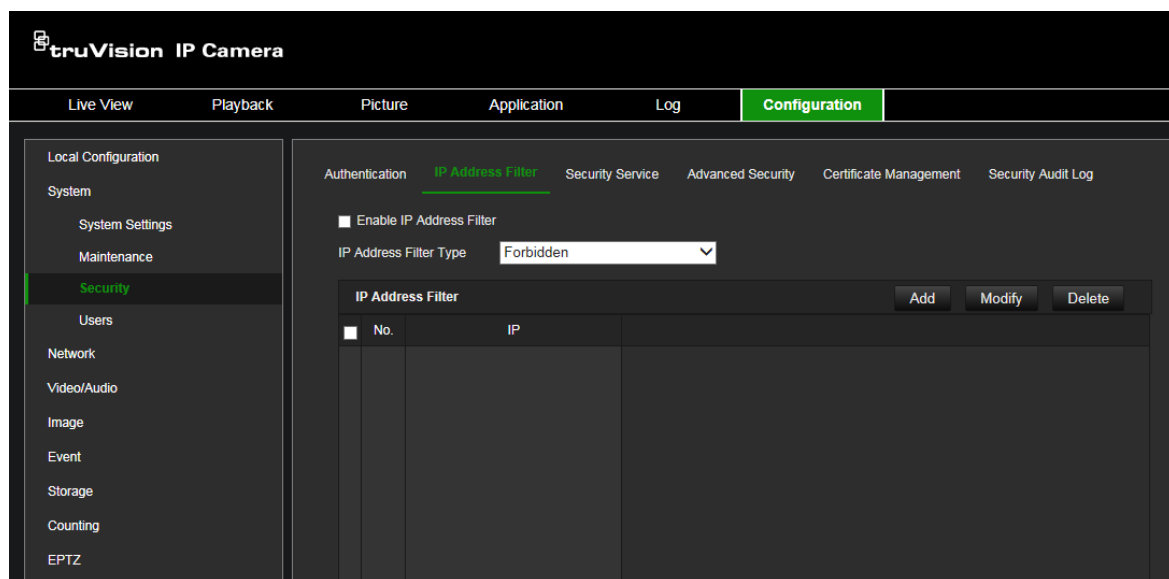
4. Click **Save** to save the changes.

IP address filter

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

To define the IP address filter:

1. From the menu toolbar, click **Configuration > System > 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.

Security service

Use this menu to enable the following login and logout functions:

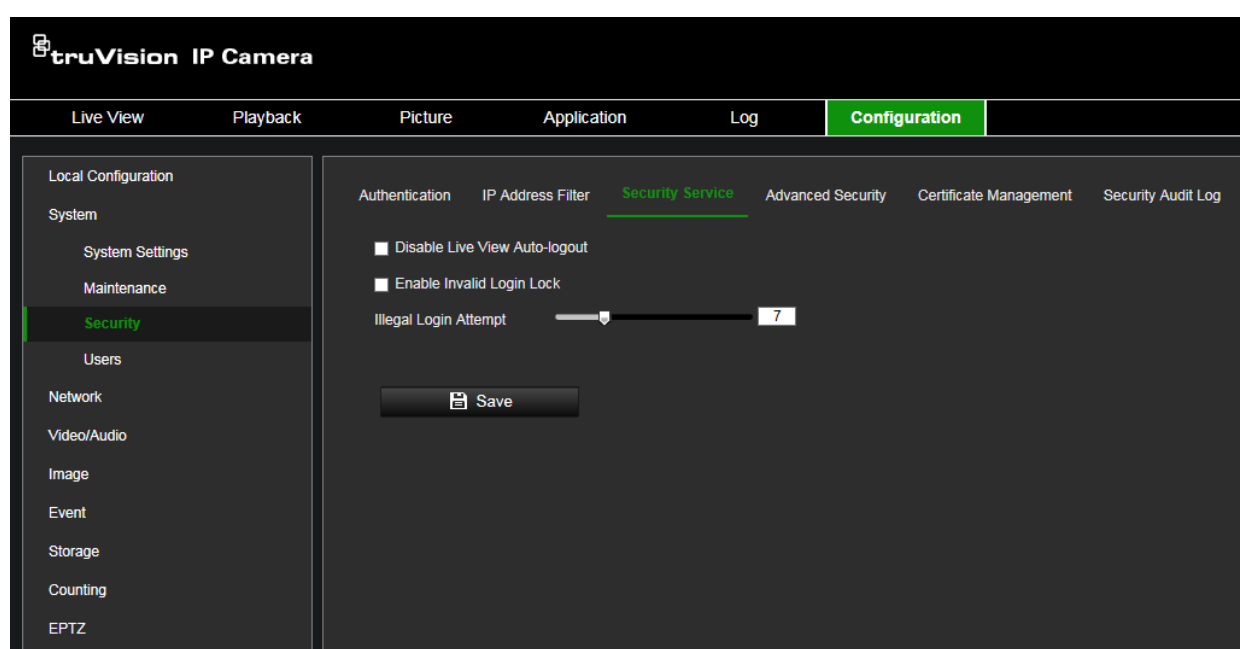
Disable Live View Auto-logout: By default, when logged into the live view webpage and there is no activity for at least five minutes, the system will automatically log out. Select this function to disable automatic log out.

Enable Invalid Login Lock: When enabled, this function will lock a user out of the system after a certain number of failed login attempts. It is enabled by default.

- The IP address will be locked if the admin user performs seven failed user name/ password attempts (five attempts for the operator/user).
- If the IP address is locked, you can log into the device after 30 minutes.

To enable the illegal login lock:

1. Click **Configuration > System > Security > Security Service**.



2. Select the **Disable Live View Auto-logout** check box to disable auto-logout when staying at the live view webpage.
3. Select the **Enable Invalid Login Lock** check box to check the login attempts.
4. Select the number of invalid attempts from 3 to 20 by adjusting the slider or changing the number in the box.
5. Click **Save** to save the changes.

Notes:

- A. The IP address will be blocked if the user performs the set times of failed user name/ password attempts (no different times of attempts for the admin/operator/user).
- B. If the IP address is blocked, you can try to log in to the device again after 30 minutes.

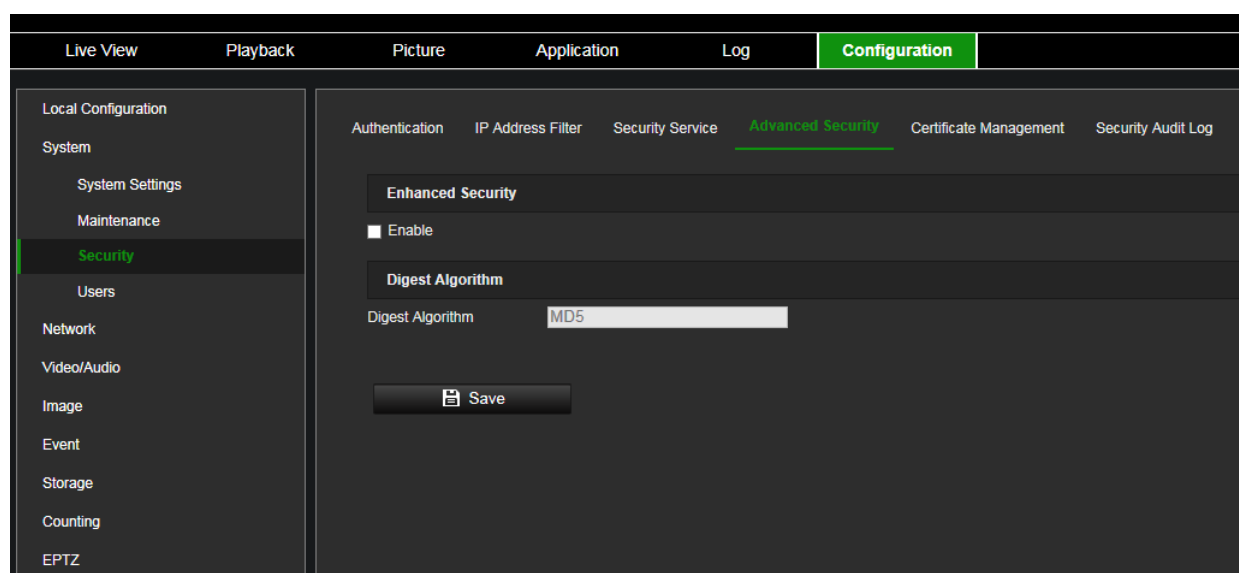
Advanced security

Enabling the Enhanced Security function will enhance the cyber security level. The camera uses two different cryptographic, or digest, algorithms depending on whether the advanced security function is enabled or disabled. When enabled, the Digest Algorithm displays SHA256. When disabled, the Digest Algorithm displays MD5. The function is disabled by default.

Only the administrator can enable/disable this function.

Go to **Configuration > Security > Advanced Security** and enable or disable the function.

Figure 7: Advanced Security window



When the advanced security function is enabled, the following conditions apply:

- HTTPS, WebSockets and Enhanced SDK Service must be enabled to secure your webpages.
- RTSP, SDK and WebSocket are no longer available for webpages. TLS 1.2 must be enabled. SNMP is also not available.
- HTTPS must be used when accessing the camera via a web browser. HTTP does not work even if automatic redirecting is supported in a device.
- HTTP (80), RTSP (554), WebSocket (7681) and SDK (8000) can no longer be configured from the *Port* tab (see page 37).
- ONVIF, STD-CGI are no longer available from the *Integration Protocol* tab (see page 45). ONVIF active multicast discovery is disabled.
- RTSP Authentication is no longer available from the *Authentication* tab (see page 19). WEB Authentication uses *Digest*.
- Playback, Picture, Application (Counting/Counting statistics) and Log are no longer available. Storage features are also no longer available although the menu tree will still display it. "Upload to FTP/Memory Card/NAS" is no longer available from smart event actions.

- UDP, TCP and Multicast streaming methods are no longer supported. Third-party plug-ins are also not supported.
- Port mapping of HTTP, RTSP, SDK (Server Port) and WebSocket is no longer available from the NAT tab (see page 37).
- The default 1024-bit self-signed certificate is changed to 2048-bit when *Advanced Security* is enabled. While if a certificate is created by users, users will see a notification to recreate a 2048-bit certificate if it was 1024-bit. Otherwise, parameter error will pop up.
- Stream encryption is supported by RTSP OVER HTTPS via IE browser and WebSockets via a plug-in free browser such as Chrome.
- Port Mapping in NAT tab is disabled by default. The camera cannot be discovered in the SADP tool or library.
- FTP and Email are no longer available (see pages 41 and 42). The two options are also no longer available from smart event actions.
- “Enable Multicast Discovery” is no longer available from the TCP/IP tab (see page 33). The Multicast tab is also no longer available.
- DDNS and PPPOE tabs are no longer available.

When the Advanced Security function is enabled and then disabled, the following conditions apply:

- RTSP, SDK and WebSocket return to their previous status.
- HTTPS and TLS1.2 remain enabled.
- SNMP returns to its previous status.
- HTTP port 80 recovers and is enabled by default. RTSP (554), WebSocket (7681) and SDK (8000) rolls back to the previous settings.
- Record, Snapshot and Storage Management tabs are available again.
- ONVIF and STD-CGI rolls back to the previous status. ONVIF multicast discovery is supported.
- RTSP Authentication rolls back to the previous status. Web Authentication stays in Digest mode.
- UDP, TCP and Multicast streaming recover. The third-party plug-in is supported.
- Port mapping of HTTP, RTSP, SDK (Server Port) and WebSocket are available again in the NAT tab.
- NAT remains disabled. Cameras can be discovered by the SADP tool and library.
- FTP and Email roll back to their previous status.
- “Enable Multicast Discovery” are available again in the TCP/IP tab. Multicast tab also recovers.
- DDNS and PPPOE tabs are no longer not available.

Certificate management

The system can manage server/client certificates and the CA certificate and send an alarm if the certificates will soon expire or are expired/abnormal.

To manage certificates:

1. Click **Configuration > System > Security > Certificate Management**.

The screenshot displays 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 structure under 'Local Configuration' with categories like 'System', 'System Settings', 'Maintenance', 'Security' (highlighted in green), 'Users', 'Network', 'Video/Audio', 'Image', 'Event', 'Storage', 'Counting', and 'EPTZ'. The main content area is titled 'Certificate Management' and contains two sections: 'Server/Client Certificate' and 'CA certificate'. The 'Server/Client Certificate' section has buttons for 'Create Self-sign...', 'Create Certificate...', 'Import', 'Export', 'Delete', and 'Certificate Propert...'. It contains a table with columns: 'Certificate ID', 'Valid From', 'Valid To', 'Status', and 'Functions'. The 'CA certificate' section has buttons for 'Import', 'Delete', and 'Certificate Propert...'. It also contains a table with the same columns. Below these tables is the 'Certificate Expiration Al...' section, which includes a checkbox for 'Enable Certificate Expiration Alarm', a slider for 'Remind Me Before Expira...' set to 7, a dropdown for 'Alarm Frequency(day)' set to 1, a slider for 'Detection Time (hour)' set to 10, and a 'Normal Actions' section with checkboxes for 'Send Email' and 'Notify Alarm Recipient' (checked). A 'Save' button is at the bottom.

Certificate ID	Valid From	Valid To	Status	Functions
default	2020-05-09 10:51:51	2023-05-09 10:51:51	Normal	HTTPS,WebSockets,Enhanced...

Certificate ID	Valid From	Valid To	Status	Functions
----------------	------------	----------	--------	-----------

Certificate Expiration Al...

☐ Enable Certificate Expiration Alarm

Remind Me Before Expira...

Alarm Frequency(day)

Detection Time (hour)

Normal Actions

☐ Send Email

☒ Notify Alarm Recipient

To create self-signed certificate:

1. Click **Configuration > System > Security > Certificate Management**.

2. Click the **Create Self-signed Certificate** tab.
3. Enter certificate ID, country, hostname/IP, validity and other information. The certificate ID can be numbers or letters less than 64 characters.

Create Self-signed Certificate

Certificate ID *

Public Key Length 2048

Country *

Hostname/IP *

Validity * Day(s)

Password

State or province

Locality

Organization

Organizational Unit

Email

OK Cancel

4. Click **OK** to save.
5. (Optional) After selecting a certificate, click **Export** to export the certificate, **Delete** to delete the certificate, or **Certificate Properties** to view the certificate details.

To create certificate request:

1. Click **Configuration > System > Security > Certificate Management**.
2. Select a saved self-signed certificate.
3. Click the **Create Certificate Request** tab.

Create Certificate Request

Certificate ID * default

Country * NL

Hostname/IP * 5ec0326f45dd8657e46bd8a51e6

Validity * 0 Day(s)

State or province

Locality

Organization embeddedsoftware

Organizational Unit

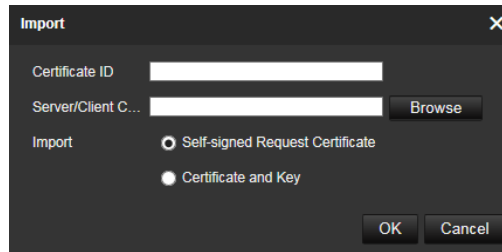
Email 1@gmail.com

OK Cancel

4. Enter the information requested.
5. Click **OK** to save.

To import certificate:

1. Click **Configuration > System > Security > Certificate Management**.
2. In the *Server/Client Certificate* section, click the **Import** tab.



3. Enter the certificate ID. Click **Browse** to select the desired server/client certificate, select the desired import method and enter the required information.
4. Click **OK** to save the changes.

Note:

- Up to 16 certificates are allowed.
- If certain functions are using the certificate, it cannot be deleted.
- You can view the functions that are using the certificate in the Functions column.
- You cannot create a certificate that has the same ID with that of the existing certificate and import a certificate that has the same content with that of the existing certificate.

To manage CA certificate:

1. Click **Configuration > System > Security > Certificate Management**.
2. In the *CA Certification* section, click the **Import** tab.
3. Enter certificate ID. Click **Browse** to select the desired server/client certificate. Select the import method and enter the required information.
4. Click **OK** to save the changes.

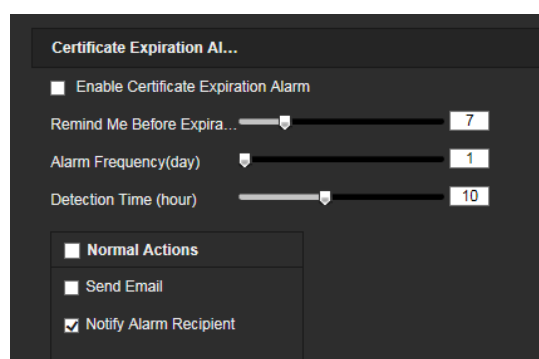
Note:

- Up to 16 certificates are allowed.

To enable a certificate expiration alarm:

1. Click **Configuration > System > Security > Certificate Management**.
2. Select the **Enable Certificate Expiration Alarm** check box.

When enabled, notification messages that certificates will soon expire, have expired, or are abnormal will be sent to the saved email box or alarm recipient.



3. Select the **Remind Me Before Expiration (day)**, **Alarm Frequency (day)** and **Detection Time (hour)** values by adjusting the sliders.

Remind Me Before Expiration (day): this is the number of days before the certificate expires that you will receive the first notification. If you set the number of days for the notification of the certificate expiration to 1, the camera will remind you the day before the expiration day. You can select between 1 and 30 days to receive the reminder. The default notification value is seven days before expiration.

Alarm Frequency (day): this is the interval in days between reminders sent after the first notification that the certificate will expire. In the example shown in the screen shoot, if you set the alarm frequency to 2, you will receive the reminder notifications every two days after the first notification of the certificate expiration.

Detection Time (hour): this is the time of day when the expiration notifications are sent.

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

Security audit log

You can search and analyze the security log files of the device to see if there has been any invalid access. After the camera boots up, security audit logs are saved to the device flash memory every 30 minutes.

Due to limited space for storing in the flash memory, you can save the logs on a log server. Configure the server settings under **Advanced Settings**.

Figure 8: Security Audit Log window

The screenshot displays the 'Security Audit Log' window with the following components:

- Navigation Bar:** Authentication, IP Address Filter, Security Service, Advanced Security, Certificate Management, and **Security Audit Log** (highlighted).
- Log Query Section:**
 - ① Major Type: All Types (dropdown)
 - ② Minor Type: All Types (dropdown)
 - ③ Start Time: 2020-07-22 00:00:00
 - End Time: 2020-07-22 23:59:59
 - ④ Search (button)
- Log List Section:**
 - Export (button) ⑤
 - Table with columns: No., Time, Major Type, Minor Type, Channel No., Local/Remote User, Remote Host IP.
 - Footer: Total 0 Items, navigation buttons (<<, <, 0/0, >, >>).
- Advanced Settings Section:**
 - ☐ Enable Log Upload Server
 - ☐ Enable Encrypted Transmission
- Server Settings Section:**
 - Log Server IP: 0
 - Log Server Port: 1
 - Test (button)
 - Client Certificate: No certificate (dropdown)
 - CA certificate: No certificate (dropdown)
 - Save (button)

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

You can search for recorded logs by the following criteria:

Major type: There are three types of logs: Operation, Event and Other (reserved). You can also search All.

Minor type: Each major type has some minor types.

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

To search logs:

1. Click **Configuration > System > Maintenance > Security Audit Log**.
2. Set the search conditions to specify Major Type, Minor Type, Start Time and End Time. In the Major Type and Minor Type drop-down lists, select the desired options.
3. Click **Search** to search logs. The matched logs appear in the window.
4. To export the log files, click **Export** to save the log files.

To configure a log server:

1. Click **Configuration > System > Maintenance > Security Audit Log**.
2. Select **Enable Log Upload Server** to enable the function.
3. Enter the values for **Log Server IP** and **Log Server Port**.
4. Click **Test** to test the settings.
5. (Optional) select **Enable Encrypted Transmission** to encrypt the transmitted data between the device and the log server.
6. (Optional) select the desired **Client Certificate** from the drop-down list. "No certificate" is the default option.
7. (Optional) select the desired **CA Certificate** from the drop-down list. "No certificate" is the default option.

Note:

- The certificates are managed in the *Certificate Management* tab.
- The CA certificate must be issued by a certification authority. Self-signed certificates will be refused when you click the Test button.
- The log server must be able to check the validity of the imported certificates inside the camera when encrypted transmission is used.

Users

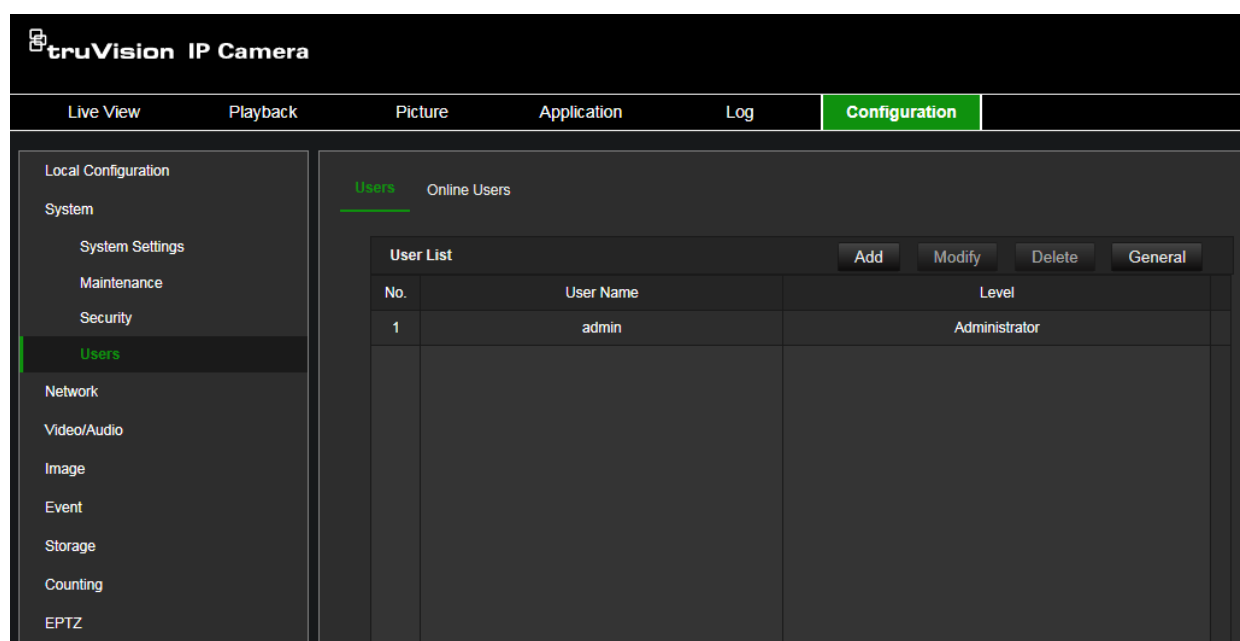
This section describes how to manage users. You can:

- 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 9 below.

Figure 9: 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 > System > Security > User**.
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.
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. The password may not contain the user name.
5. Select the type of user from the drop-down list. The options are Viewer and Operator.
6. Assign permissions to the user. Select 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

Basic Permissions	Camera Configuration
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.

Online users

Use this menu to see who is connecting to the camera. You can see the following user information: user name, level, IP address, and operation time.

To view online users:

Click **Configuration > System > Maintenance > Online Users**. The list of users currently online is displayed. Click **Refresh** to update the list.

Users		Online Users			
		User List			
		Refresh			
No.	User Name	Level	IP Address	User Operation Time	
1	admin	Administrator	10.7.70.3	2020-06-04 20:38:29	

Network

Use the Network menu to set the desired network parameters to be able to access the camera. There are two groups of network settings, Basic Settings and Advanced Settings.

TCP/IP parameters

You can set up the following TCP/IP parameters:

Function	Description
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
DHCP	Enable to automatically obtain an IP address and other network settings from that server.
IPv4 Address	Enter the IPv4 address of the camera.
IPv4 Subnet Mask	Enter the IPv4 subnet mask.
IPv4 Default Gateway	Enter the IPv4 gateway IP address.
IPv6 Mode	Enter the IPv6 mode: Manual, DHCP or Router Advertisement.
IPv6 Address	Enter the IPv6 address of the camera.
IPv6 Subnet Prefix Length	Enter the IPv6 subnet prefix length value of the camera.
IPv6 Default Gateway	Enter the IPv6 default gateway value of the camera.
MAC Address	Shows the MAC address of the devices.
MTU	Enter the valid value range of MTU. Default is 1500.
Multicast Address	Enter a D-class IP address between 224.0.0.0 to 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.
Enable Multicast Discovery	This function is optional. It enables the automatic detection of the online network camera via private multicast protocol in the LAN.
DNS server	Specifies the DNS server for your network.

To set up the TCP/IP parameters:

1. Click **Configuration > Network > Basic Settings > TCP/IP**.

The screenshot displays the 'TCP/IP' configuration page with tabs for TCP/IP, DDNS, PPPoE, Port, NAT, and Multicast. The TCP/IP tab is active. The settings are as follows:

Parameter	Value	Action
NIC Type	Auto	
DHCP	☒	
IPv4 Address	10.7.70.4	Test
IPv4 Subnet Mask	255.255.255.0	
IPv4 Default Gateway	10.7.70.254	
IPv6 Mode	Route Advertisement	View Route Advertisement
IPv6 Address		
IPv6 Subnet Mask		
IPv6 Default Gateway	::	
Mac Address	84:9a:40:b1:a9:7d	
MTU	1500	
Enable Multicast Discovery	☒	

DNS Server

Parameter	Value
Preferred DNS Server	10.1.7.97
Alternate DNS Server	10.1.7.98

Domain Name Settings

Parameter	Value
Enable Dynamic Domain Name	☐
Register Domain Name	

Save

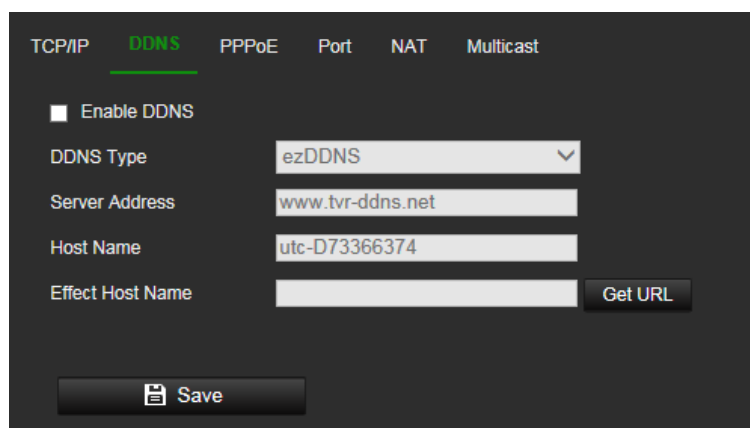
2. Configure the NIC settings, including the NIC Type, IPv4 settings, IPv6 settings and MTU settings.
3. If the DHCP server is available, select **DHCP**.
4. If the DNS server settings are required for some applications (e.g., sending email), you should configure the **Preferred DNS Server** or **Alternate DNS Server**.
5. Click **Save** to save changes.
6. Reboot the device for the changes to take effect.

DDNS parameters

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.

To set up the DDNS parameters:

1. Click **Configuration > Network > Basic Settings > DDNS**.



TCP/IP **DDNS** PPPoE Port NAT Multicast

☒ Enable DDNS

DDNS Type: ezDDNS

Server Address: www.tvr-ddns.net

Host Name: utc-D73366374

Effect Host Name: [Get URL](#)

[Save](#)

2. Select **Enable DDNS** to enable this feature.
3. Select the **DDNS Type**. Three options are available: DynDNS, ezDDNS and NO-IP.

DynDNS: Select **DynDNS** and enter the server address for DynDNS. In the recorder domain name field, enter the domain name obtained from the DynDNS web site. Then enter your user name and password registered in the DynDNS network.

For example:

Server address: members.dyndns.org

Domain: mycompanydvr.dyndns.org

User name: myname

Password: mypassword

- Or -

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).

- Or -

NO-IP: Enter the server address (for example, dynupdate.no-ip.com). In the host name field, enter the host obtained from the NO-IP web site. Then enter the user name and password that are registered with the No-IP network.

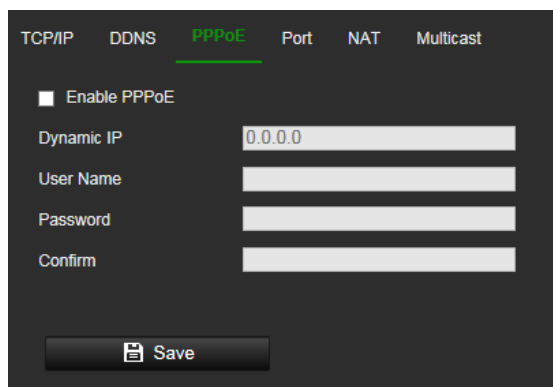
4. Click **Save** to save changes.
5. Reboot the device for the changes to take effect.

PPPoE parameters

This allows you to retrieve a dynamic IP address.

To set up the PPPoE parameters:

1. From the menu toolbar, click **Configuration > Network > Basic Settings > PPPoE**.



2. Select **Enable PPPoE** to enable this feature.
3. Enter the dynamic IP address.
4. Enter User Name, Password, and Confirm password for PPPoE access.
5. Click **Save** to save changes.
6. Reboot the device for the changes to take effect.

Port parameters

You can set up several ports:

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 is 554 and it can be changed to any port No. ranges from 1 to 65535.

SRTP Port: The default port is 322.

HTTPS Port: The default port number is 443, and it can be changed to any port No. which is not occupied.

Server Port: The default server port is 8000, and it can be changed to any port No. ranges from 2000 to 65535.

Enhanced SDK Service Port: The default server port is 8433, and it can be changed to any port No. ranges from 2000 to 65535.

WebSocket Port: The default port is 7681. It can be changed to any port No. ranges from 1 to 65535.

WebSockets Port: The default server port is 7682. It can be changed to any port No. ranges from 1 to 65535.

Alarm Host IP: A configurable IP address of a server that will listen and receive alarm messages.

Alarm Host Port: The network port of the server that is listening at. The default server port is 5001. It can be changed to any port No. ranges from 1 to 65535.

To set up the port parameters:

1. From the menu toolbar, click **Configuration > Network > Basic Settings > Port**.

Parameter	Value
HTTP Port	80
RTSP Port	554
SRTP Port	322
HTTPS Port	443
Server Port	8000
Enhanced SDK Service P...	8443
WebSocket Port	7681
WebSockets Port	7682
Alarm Host IP	0.0.0.0
Alarm Host Port	5001

Save

2. Set the HTTP port, RTSP port, HTTPS port and Server port of the camera.
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.
5. Reboot the device for the changes to take effect.

NAT parameters

A NAT (Network Address Translation) is used for network connection. Select the port mapping mode: auto or manual.

To set up the NAT parameters:

1. Click **Configuration > Network > Basic Settings > NAT**.

TCP/IP DDNS PPPoE Port **NAT** Multicast

☐ Enable Port Mapping

Friendly Name

Port Mapping Mode

Port Type	External Port	External IP Address	Internal Port	Status
HTTP	80	0.0.0.0	80	Not Valid
HTTPS	443	0.0.0.0	443	Not Valid
RTSP	554	0.0.0.0	554	Not Valid
Server Port	8000	0.0.0.0	8000	Not Valid
Enhanced SDK...	8443	0.0.0.0	8443	Not Valid
Websocket	7681	0.0.0.0	7681	Not Valid
Websockets	7682	0.0.0.0	7682	Not Valid
SRTP	322	0.0.0.0	322	Not Valid

2. Select the **Enable Port Mapping** check box to enable the UPnP™ function.
3. Select **Port Mapping Mode** to be Auto or Manual.

If you choose **Manual** mode, you can set the external port as you want.

Note: If you choose **Auto** mode, enable the UPnP™ function at the router.

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

Multicast parameters

Multicast is a protocol for discovering devices on networks. Configuring multicast to make the device discoverable.

To set up the Multicast parameters:

1. Click **Configuration > Network > Basic Settings > Multicast**.

TCP/IP DDNS PPPoE Port NAT **Multicast**

IP Address

Stream Type

RTSP

Video Port

Audio Port

FEC Port

FEC Ratio %

SRTP

Video Port

Audio Port

Save

2. Enter a class D IP address between 224.0.0.19 to 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.
3. Video port and audio port of each video stream of each camera channel can be specified by selecting a stream in Video Stream and inputting port number in Video Port and Audio Port.
4. FEC Port and FEC Ratio: Set the port and ratio of Forward Error Correction.
5. SRTP: The default video port is 18860 and the default audio port is 18862.

Note: Only certain camera models support FEC port and FEC ratio.

SNMP parameters

SNMP is a protocol for managing devices on networks. Enable SNMP to get the camera status and parameter related information.

To set up the SNMP parameters:

1. Click **Configuration > Network > Advanced Settings > SNMP**.

The screenshot shows the 'SNMP' configuration page in a web interface. The page has a dark theme with a top navigation bar containing links for 'SNMP', 'FTP', 'Email', 'HTTPS', 'QoS', '802.1x', and 'Integration Protocol'. The 'SNMP' link is highlighted with a green underline. Below the navigation bar, there are three main sections: 'SNMP v1/v2', 'SNMP v3', and 'SNMP Other Settings'. The 'SNMP v1/v2' section includes checkboxes for 'Enable SNMPv1' and 'Enable SNMPv2c', both of which are currently unchecked. Below these are text input fields for 'Read SNMP Community' (set to 'public'), 'Write SNMP Community' (set to 'private'), 'Trap Address' (empty), 'Trap Port' (set to '162'), and 'Trap Community' (set to 'public'). The 'SNMP v3' section includes a checkbox for 'Enable SNMPv3' (unchecked). Below this are two identical sets of configuration fields for Read and Write operations. Each set includes a 'Read/Write UserName' field, a 'Security Level' dropdown menu (set to 'no auth, no priv'), an 'Authentication Algorithm' radio button selection (MD5 selected, SHA unselected), an 'Authentication Password' field (masked with dots), a 'Private-key Algorithm' radio button selection (DES selected, AES unselected), and a 'Private-key password' field (masked with dots). The 'SNMP Other Settings' section includes an 'SNMP Port' field set to '161'. At the bottom of the page is a 'Save' button with a floppy disk icon.

SNMP v1/v2

☐ Enable SNMPv1

☐ Enable SNMPv2c

Read SNMP Community: public

Write SNMP Community: private

Trap Address:

Trap Port: 162

Trap Community: public

SNMP v3

☐ Enable SNMPv3

Read UserName:

Security Level: no auth, no priv

Authentication Algorithm: ☒ MD5 ☐ SHA

Authentication Password:

Private-key Algorithm: ☒ DES ☐ AES

Private-key password:

Write UserName:

Security Level: no auth, no priv

Authentication Algorithm: ☒ MD5 ☐ SHA

Authentication Password:

Private-key Algorithm: ☒ DES ☐ AES

Private-key password:

SNMP Other Settings

SNMP Port: 161

Save

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 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.

FTP parameters

Configure the FTP server to allow the camera to upload snapshot pictures of an event to the server for storage.

To set up the FTP parameters:

1. Click **Configuration > Network > Advanced Settings > FTP**.

SNMP **FTP** Email HTTPS QoS 802.1x Integration Protocol

FTP Protocol

Server Address

Port

User Name

Password

Confirm

☐ Anonymous

Directory Structure

Picture Filing Interval Day(s)

Picture Name

☐ Upload Picture

☐ Enable Automatic Network Replenishment

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.

Email parameters

Enter the email address to which messages are sent when an alarm event occurs.

To set up the email parameters:

1. Click **Configuration > Network > Advanced Settings > Email**.

Receiver		
No.	Receiver	Receiver's Address
1		
2		
3		

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.

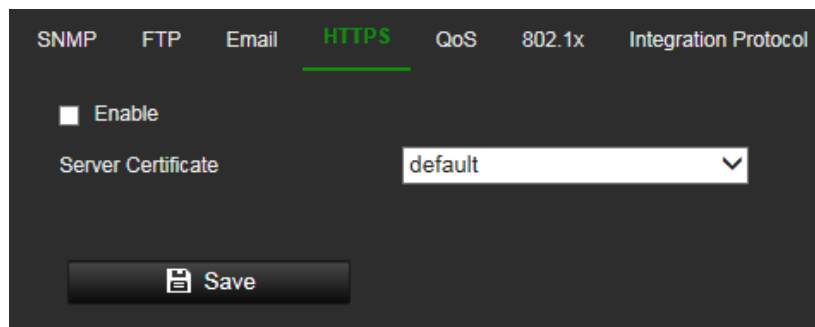
3. Click **Test** to test the email parameters set up.
4. Click **Save** to save changes.

HTTPS parameters

Specifies authentication of the web site and its associated web server, which protects against Man-in-the-middle attacks.

To set up the HTTPS parameters:

1. Click **Configuration > Network > Advanced Settings > HTTPS**.



2. To select a server certificate in the drop-down list.
3. Select the **Enable** check box to enable HTTPS function.
4. Click **Save** to save changes.

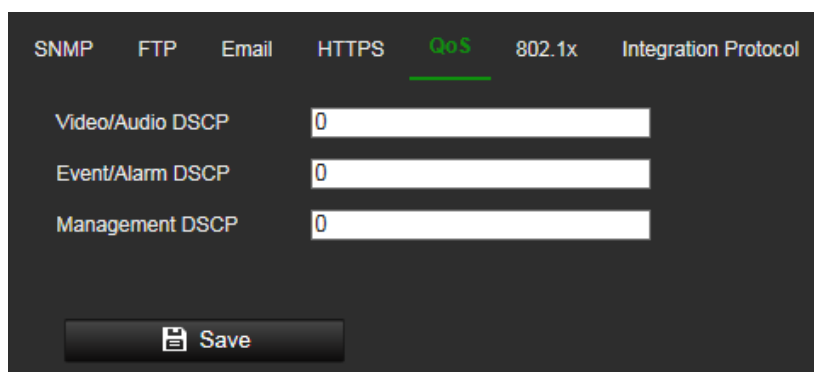
QoS parameters

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.

To define the QoS parameters:

1. Click **Configuration > Network > Advanced Settings > QoS**.

The screenshot shows the 'QoS' configuration page. At the top, there is a navigation bar with tabs: SNMP, FTP, Email, HTTPS, QoS (highlighted in green), 802.1x, and Integration Protocol. Below the tabs, there are three input fields for DSCP values: 'Video/Audio DSCP' with a value of 0, 'Event/Alarm DSCP' with a value of 0, and 'Management DSCP' with a value of 0. At the bottom of the page, there is a 'Save' button with a floppy disk icon.

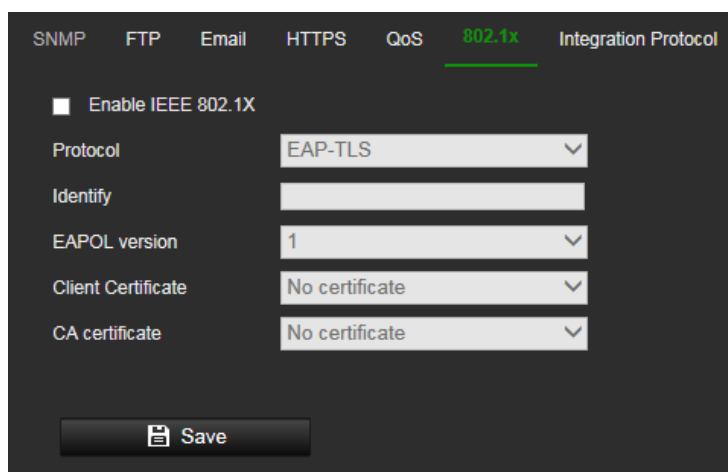
2. Configure the QoS settings, including Video / Audio DSCP, Event / Alarm DSCP and Management DSCP. The valid value range of the DSCP is 0-63. The bigger the DSCP value is, the higher the priority is.
3. Click **Save** to save changes.

802.1x parameters

When the feature is enabled, the camera data is secured, and user authentication is needed when connecting the camera to the network.

To set up the 802.1x parameters:

1. Click **Configuration > Network > Advanced Settings > 802.1X**.

The screenshot shows the '802.1x' configuration page. At the top, there is a navigation bar with tabs: SNMP, FTP, Email, HTTPS, QoS, 802.1x (highlighted in green), and Integration Protocol. Below the tabs, there is a checkbox labeled 'Enable IEEE 802.1X'. Below this, there are several configuration options: 'Protocol' set to 'EAP-TLS', 'Identify' (empty field), 'EAPOL version' set to '1', 'Client Certificate' set to 'No certificate', and 'CA certificate' set to 'No certificate'. At the bottom of the page, there is a 'Save' button with a floppy disk icon.

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.

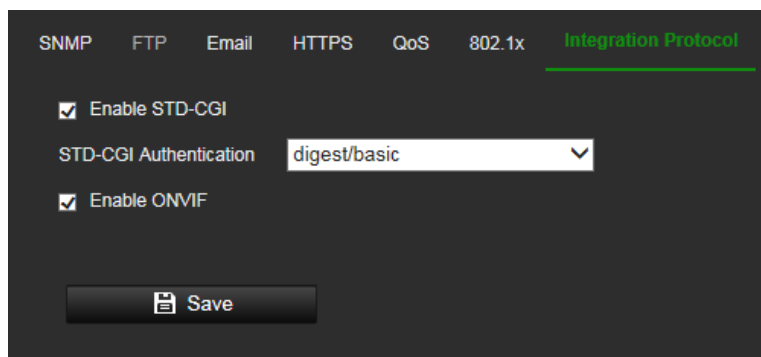
Note: The switch or router to which the camera is connected must also support the IEEE 802.1X standard. A server must also be configured. Please apply and register a user name and password for 802.1X in the server.

Integration protocol parameters

If you need to access the camera through the third-party platform, you can enable STD-CGI function. If you need to access the camera through the ONVIF protocol, you can configure ONVIF from this interface. Refer to ONVIF standard for detailed configuration rules.

To set up the integration protocol parameters:

1. Click **Configuration > Network > Advanced Settings > Integration Parameters**.



2. Select the STD-CGI Authentication method. Digest/basic indicates using digest as priority if supported by the communication. If it is not supported, basic authentication will be the backup.
3. Select the **Enable STD-CGI** check box to enable the STD-CGI protocol.
4. Select the **Enable ONVIF** check box to enable the ONVIF protocol.
5. Click **Save** to save changes.

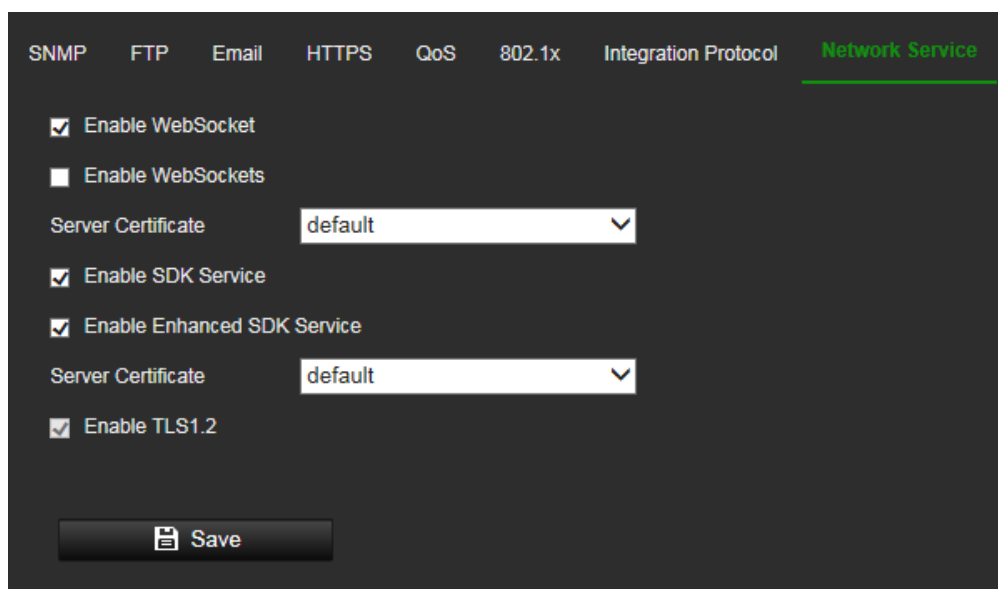
Network service parameters

Use this function to enable or disable certain protocols supported by the camera. Unused functions should be disabled for security reasons. Supported functions depend on the camera model.

- **WebSocket:** To access the camera, enable this function if using Google Chrome version 45 and higher or Mozilla Firefox 52 and higher. If not enabled, live view, image capture and digital zoom cannot be used with these browsers.
- **Websockets:** To access the camera, enable this function if using Microsoft Internet Explorer.
- **SDK Service** and **Enhanced SDK Service:** Enable these functions to be able to use the device with a VMS (like TruVision Navigator or a third-party software using the SDK). **SDK Service** uses the SDK protocol. **Enhanced SDK Service** uses SDK over TLS (Transport Layer Security).

To set up the network service parameters:

1. Click **Configuration > Network > Advanced Settings > Network Service**.



The screenshot shows the 'Network Service' configuration page. At the top, there are tabs for SNMP, FTP, Email, HTTPS, QoS, 802.1x, Integration Protocol, and Network Service (which is highlighted in green). Below the tabs, there are several settings:

- ☒ Enable WebSocket
- ☐ Enable WebSockets
- Server Certificate: default (dropdown menu)
- ☒ Enable SDK Service
- ☒ Enable Enhanced SDK Service
- Server Certificate: default (dropdown menu)
- ☒ Enable TLS1.2

At the bottom, there is a 'Save' button with a floppy disk icon.

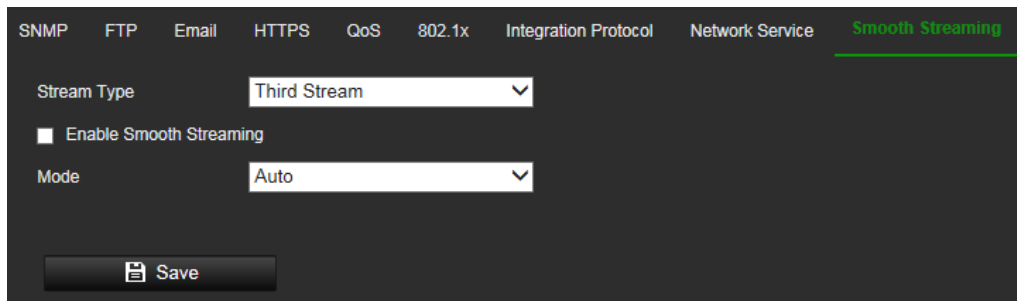
2. Select the **Enable WebSocket** check box to enable WebSocket service for live viewing over HTTP protocol without the plug-in.
3. Select the **Enable WebSockets** check box to enable WebSockets service for live viewing over HTTPS protocol without the plug-in.
4. Select the **Enable SDK Service** check box to enable SDK protocol over HTTP protocol. Client software communicates with the device via SDK service or Enhanced SDK service.
5. Select the **Enable Enhanced SDK Service** check box to enable SDK protocol over HTTPS protocol.
6. Select a certificate in the Server Certificate drop-down list.
7. TLS1.2 is enabled by default and cannot be changed as HTTPS protocols rely on it.
8. Click **Save** to save changes.

Smooth streaming parameters

Smooth Streaming is used to view the live view smoothly via a client software or Web Browser through the third stream when the network is unstable or inadequate for high quality video transmission.

To set up the smooth streaming parameters:

1. Click **Configuration > Network > Advanced Settings > Smooth Streaming**.



2. Select the stream type. The smooth stream feature can only work with the third stream.
3. Select the **Enable Smooth Streaming** check box to enable Smooth Streaming
4. Select the **Mode** of smooth streaming. There are four modes selectable: Auto, Resolution Priority, Frame Rate Priority and Error Correction.

Auto: The resolution and bitrate will be adjusted automatically, the upper limits of which will not exceed the values you set on

Resolution Priority: The resolution stays the same as the set value in Video page, and the bitrate will be adjusted automatically. Go to the Configuration > Video/Audio > Video page and set the *Max. Bitrate* before you enable smooth streaming function.

Frame Rate Priority: The frame rate stays the same when setting the resolution, bitrate, quality and other parameters on the Video page.

Error Correction: The resolution and bitrate stay the same as the set values in the Video page. This mode is used to correct the data error during transmission. You can configure the error correction proportion within range of 0 to 100. When the proportion is 0, the data error will be corrected by data retransmission. When the proportion is higher than 0, the error data will be recovered via redundant data that is added to the stream. The higher the value, the more redundant data will be generated, and the larger bandwidth is required. When the proportion is 100, the redundant data will be as large as the original data.

Note: Make sure the bandwidth is sufficient in the *Error Correction* mode.

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

HTTP listening parameters

Alarm information can be sent to destination IP or Host via HTTP protocol.

To set up the HTTP listening parameters:

1. Click **Configuration > Network > Advanced Settings > HTTP**.

Destination IP or Host Name	URL	Protocol	Port	Test
0.0.0.0	/	HTTP	80	Test

2. Enter destination IP or host name, URL, protocol type and port number.
3. Click the **Test** button to test if the service is available.

Note: the IP address or host name of a server should be available. The server should listen to the designated port.

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

SRTP parameters

SRTP (Secure Real-time Transport Protocol) provides encryption, message authentication and integrity for the data being streamed in both unicast and multicast applications.

To set up the SRTP parameters:

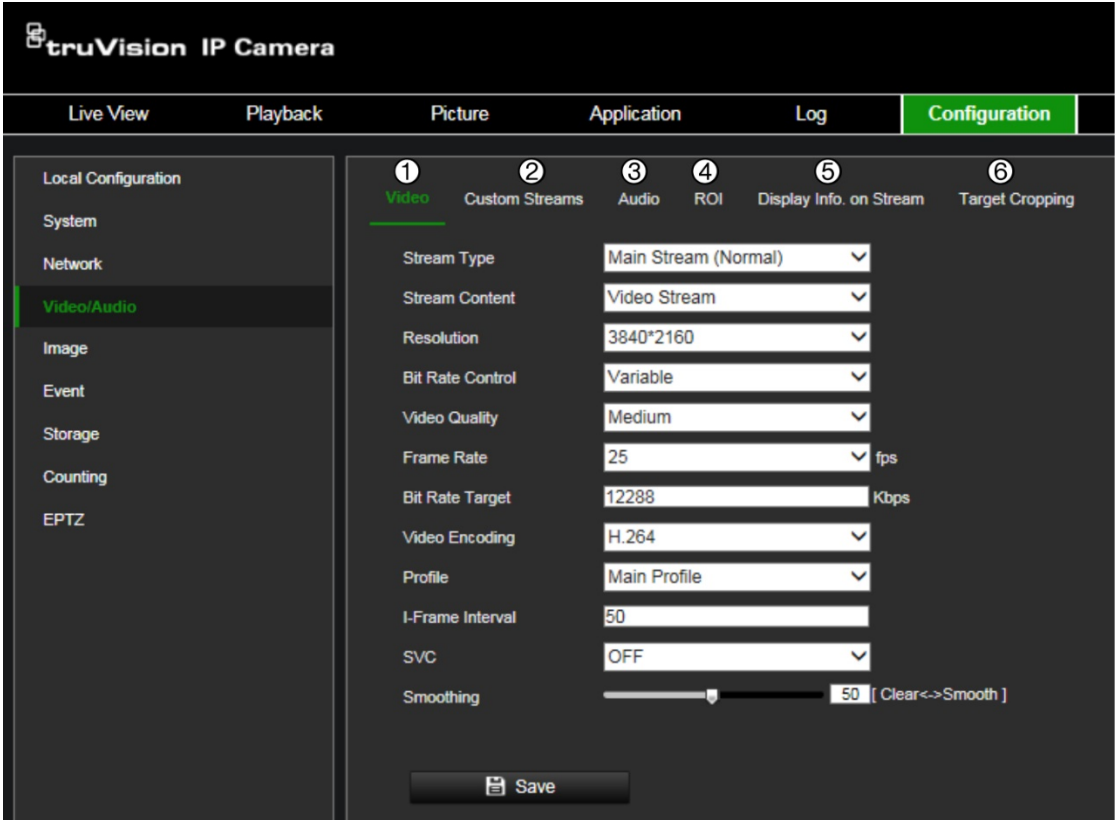
1. Click **Configuration > Network > Advanced Settings > SRTP**.

2. Select the server certificate in the drop-down list
3. Select the encrypted algorithm in the drop-down list
4. Click **Save** to save changes.

Video and Audio

You can adjust the video and audio recording parameters to obtain the snapshot quality and file size best suited to your needs. Figure 10 below list the video and audio recording options you can configure for the camera.

Figure 10: Video/Audio Settings menu (Video tab shown)

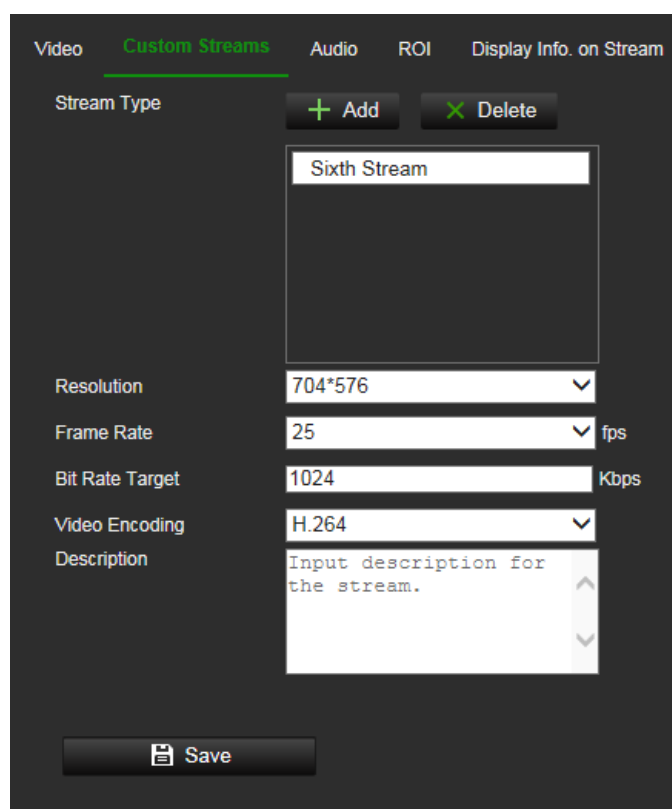


Tab	Parameter descriptions
1. Video	Stream Type: Specifies the streaming method used. Options include: Main Stream (Normal), Substream, Third Stream, Fourth Stream and Fifth Stream. Stream Content: Specifies the stream type you wish to record. Select Video Stream to record video stream only. Select Video&Audio to record both video and audio streams. Note: Video&Audio is only available for those camera models that support audio. 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, third, fourth or fifth stream is being used. Note: Resolutions can vary depending on the camera model. 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. 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. 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. Note: The maximum frame rate depends on the camera model and selected resolution. Please check the camera specifications in its datasheet. Video Encoding: Specifies the video encoder used.

Tab	Parameter descriptions
	Profile: Different profile indicates different tools and technologies used in compression. Options include: High Profile, Main Profile. I-Frame Interval: A video compression method. It is strongly recommended not to change the default value 50. 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. Smoothing: Adjust the smoothness of the stream.
2. Custom Streams	Stream Type: Specifies the streaming method used. Live view is supported only. Recording or playback is not available. Options include: Sixth Stream, Seventh Stream, Eighth Stream, Ninth Stream and Tenth Stream. Resolution: Specifies the live view resolution. The resolution options listed depend on whether sixth seventh, eighth, ninth or tenth stream is being used. Note: Resolutions in Custom Streams can be up to 1920 x 1080 Frame Rate: Specifies the frame rate for the selected resolution. Bit Rate Target: Specifies the target of the bit rate of the selected stream Video Encoding: Specifies the video encoder used. Description: Specifies remarks of the selected stream.
3. Audio	Audio Encoding: G.722.1, G.711ulaw, G.711alaw, MP2L2, G.726, PCM and MP3 are optional. Audio Input: Mic In and Line In are selectable for the connected microphone and pickup, respectively. Note: Options can vary depending on the camera model. Input Volume: Specifies the volume from 0 to 100. Environmental Noise Filter: Set it as OFF or ON. When you set the function on the noise detected can be filtered.
4. ROI	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.
5. Display Info. On Stream	When Dual-VCA mode is enabled, the camera sends video analytics results (metadata) to an NVR or other platforms to generate a VCA alarm.
6. Target Cropping	Specify a target area on the live video, and then the specified video area can be displayed via the third stream in certain resolution, providing more details of the target area if needed.

To configure custom streams settings:

1. Click **Configuration > Video/Audio > Custom Streams**.



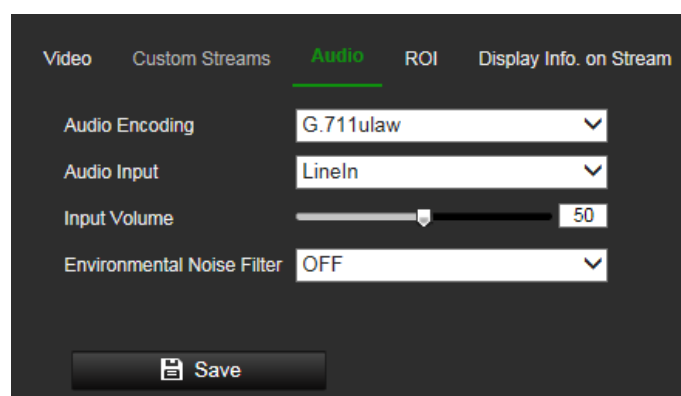
The screenshot shows the 'Custom Streams' configuration page. At the top, there are tabs: 'Video', 'Custom Streams' (highlighted in green), 'Audio', 'ROI', and 'Display Info. on Stream'. Below the tabs, there's a 'Stream Type' section with a '+ Add' button and a '- Delete' button. A list box shows 'Sixth Stream'. Below this, there are several configuration fields: 'Resolution' (704*576), 'Frame Rate' (25 fps), 'Bit Rate Target' (1024 Kbps), 'Video Encoding' (H.264), and 'Description' (Input description for the stream.). At the bottom, there is a 'Save' button.

2. Click **+ Add** to add a stream.
3. Modify the name of the selected stream if needed.
Note: the stream name can have up to 32 letters and symbols (except &, <, >, ', or ").
4. Customize the stream parameters.
5. (Optional) If a custom stream is not needed, click "X" to delete it.
6. Click **Save** to save changes.

The new streams added here can be accessed from the camera live view web page.

To configure audio settings:

Click **Configuration > Video/Audio > Audio**. Enter the required settings.



The screenshot shows the 'Audio' configuration page. At the top, there are tabs: 'Video', 'Custom Streams', 'Audio' (highlighted in green), 'ROI', and 'Display Info. on Stream'. Below the tabs, there are several configuration fields: 'Audio Encoding' (G.711ulaw), 'Audio Input' (LineIn), 'Input Volume' (a slider set to 50), and 'Environmental Noise Filter' (OFF). At the bottom, there is a 'Save' button.

To configure ROI settings:

1. Click **Configuration > Video/Audio > ROI**.

Video Custom Streams Audio **ROI** Display Info. on Stream Target Cropping

05-08-2020 Mon 14:50:44

Camera 01

Draw Area Clear

Stream Type

Stream Type Main Stream (Normal) ▼

Fixed Region

☐ Enable

Region No. 1 ▼

ROI Level 3 ▼

Region Name

Dynamic Region

☐ Enable Face Tracking

ROI Level 3 ▼

Save

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. Under the *Fixed Region* section, select **Enable** to manually configure the area.

Region No.: Select the desired region.

ROI Level: Choose the image quality enhancing level. The larger the value selected, the better the image quality.

Region Name: Set the desired region name.

5. Under the *Dynamic Region* section, select **Enable Face Tracking** to be able to track faces. For this feature to operate, you must first enable **Face Detection** under Configuration > Event > Smart Event (see page 74).
6. Click **Save** to save changes.

Display Info On Stream

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 a TruVision NVR (please check our 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. Click **Configuration > Video/Audio > Display Info. On Stream.**
2. Select the check box to enable Dual-VCA.
3. Click **Save** to save changes.

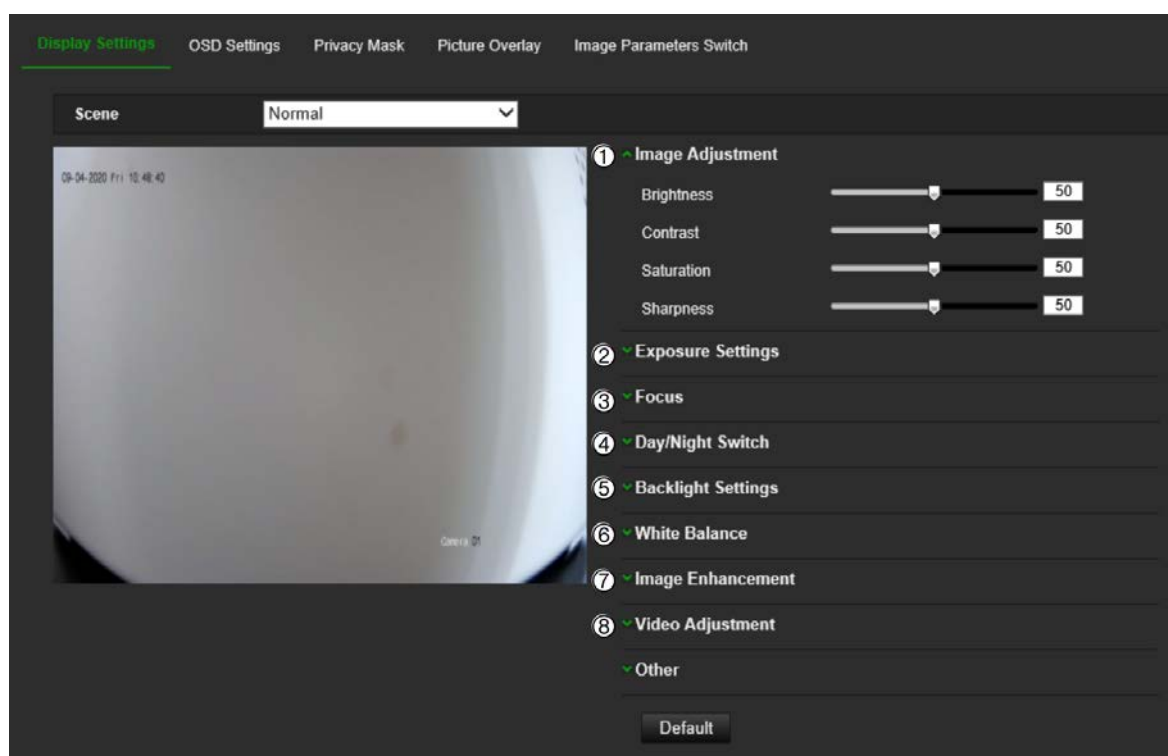
To configure target cropping:

1. Click **Configuration > Video/Audio > Target Cropping.**
2. Select **Enable Target Cropping** check box to enable the function.
3. Set **Third Stream** as the stream type.
4. Select the cropping resolution for the video display of target area. A red rectangle is displayed on the live video to mark the target area, and you can click-and-drag the rectangle to locate the target area as desired.
5. Click **Save** to save the settings.

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 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. See Figure 11 below for more information.

Figure 11: Camera image settings menu – Display Settings tab



Parameter	Description
1. Image Adjustment	
Brightness, Contrast, Saturation, Sharpness	Modify the different elements of picture quality by adjusting the values for each of parameter.
2. Exposure Settings	
Iris Mode	Auto and Manual iris modes can be selected. P-iris also supported on some S7 camera models.
Exposure Time	The exposure time controls the length of time that the aperture is open to let light into the camera through the lens. Select a higher value if the image is dark and a lower value to see fast moving objects.
3. Focus	
Focus Mode	<i>Auto, Manual and Semi-auto focus</i> modes are optional.
4. Day/Night Switch	
Day/Night Switch	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. Select one of the options: Day: Camera is always in day mode. Night: Camera is always in night mode. Auto: The camera automatically detects which mode to use. Schedule: The camera switches between day and night modes according to the configured time period. Triggered by Alarm Input: The camera switches to day or night mode after an alarm is triggered.

Parameter	Description
Sensitivity	Only available when <i>Auto D/N switch</i> mode is selected. It defines the sensitivity of the switch between day and night. Set it between 0 and 7.
Filtering Time	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. Set it between 5 and 120 s.
Smart Supplement Light	When enabled, it can avoid over exposure problem.
IR Light	Select On/OFF to Enable/disable IR. ON: The IR LEDs are ON when the camera changes to night mode. Off: The IR LEDs are OFF when the camera changes to night mode Note: The IR LEDs are always OFF in day mode.

5. Backlight Settings

BLC Area	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. Select OFF, Up, Down, Left, Right, Center, Custom or Auto. When WDR is enabled, BLC cannot be configured.
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	High Light Compression function can be used when there are strong lights in the scene affecting the image quality.

6. White Balance

White Balance	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: MWB: Manually adjust the color temperature to meet your own requirements. AWB1: Apply for small range of 2500 to 9500K, for environments where the lighting is always stable. Locked WB: Locks the WB to the current environment color temperature. Fluorescent Lamp: For use where there are fluorescent lamps installed near the camera. Incandescent Lamp: For use with incandescent lighting. Warm Light Lamp: For use where the indoor light is warm. Natural Light: For use with natural light.
---------------	---

7. Image Enhancement

Digital Noise Reduction	Digital noise reduction (DNR) reduces noise, especially in low light conditions, to improve image performance. Select Normal Mode, Advanced Mode, or OFF. Default is Normal.
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.

Parameter	Description
Defog Mode	You can enable the defog function when the environment is foggy, and the image is misty. It enhances details to obtain clearer image.
EIS	EIS (Electrical Image Stabilizer) reduces the effects of vibration in a video.
Gray Scale	You can choose the range of the gray scale as [0-255] or [16-235].
8. Video Adjustment	
Mirror	It mirrors the image so you can see it inversed. Select Left/Right, Up/Down, Center, or OFF. Default is OFF.
Hallway View	To make a complete use of the 16:9 aspect ratio, you can enable the rotate function when you use the camera in a narrow view scene. When installing, turn the camera to the 90 degrees or rotate the 3-axis lens to 90 degrees, and set the rotate mode as on, you will get a normal view of the scene with 9:16 aspect ratio to ignore the needless information such as the wall, and get more meaningful information of the scene.
Scene Mode	Select indoor or outdoor according to the current environment.
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.

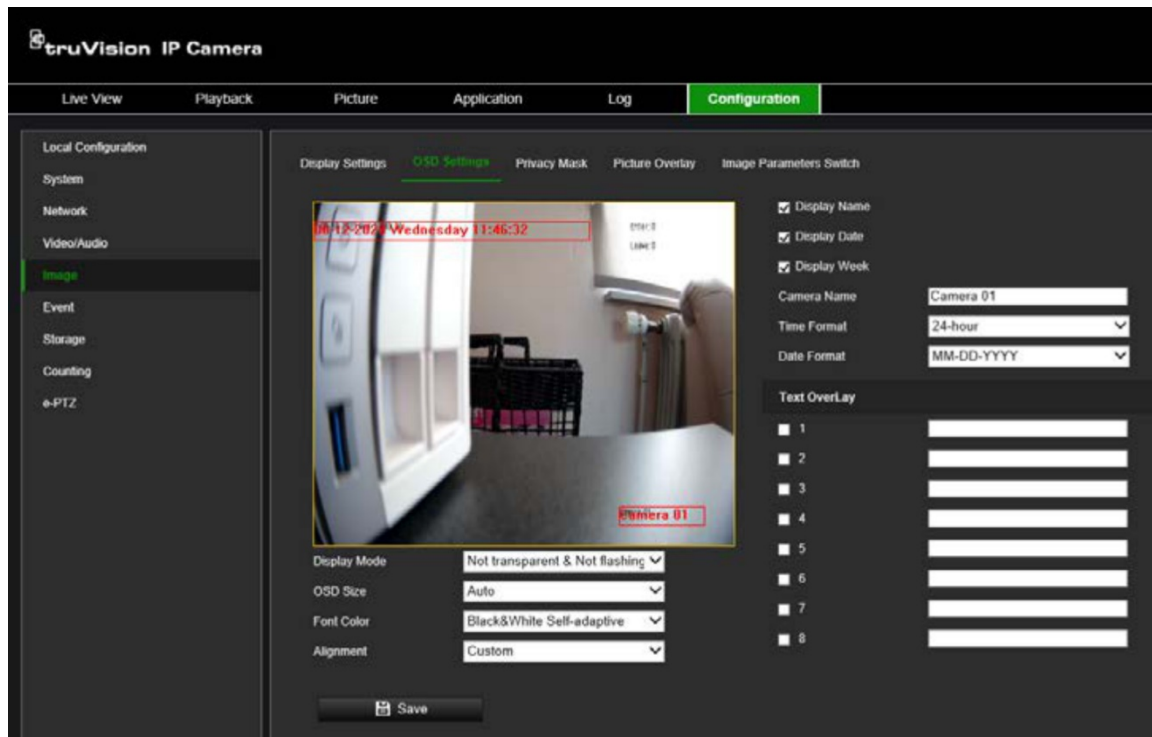
Note: Click the **Default** button to default all the image settings.

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. Click **Configuration > Image > OSD Settings**.



2. Select the **Display Name** 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.

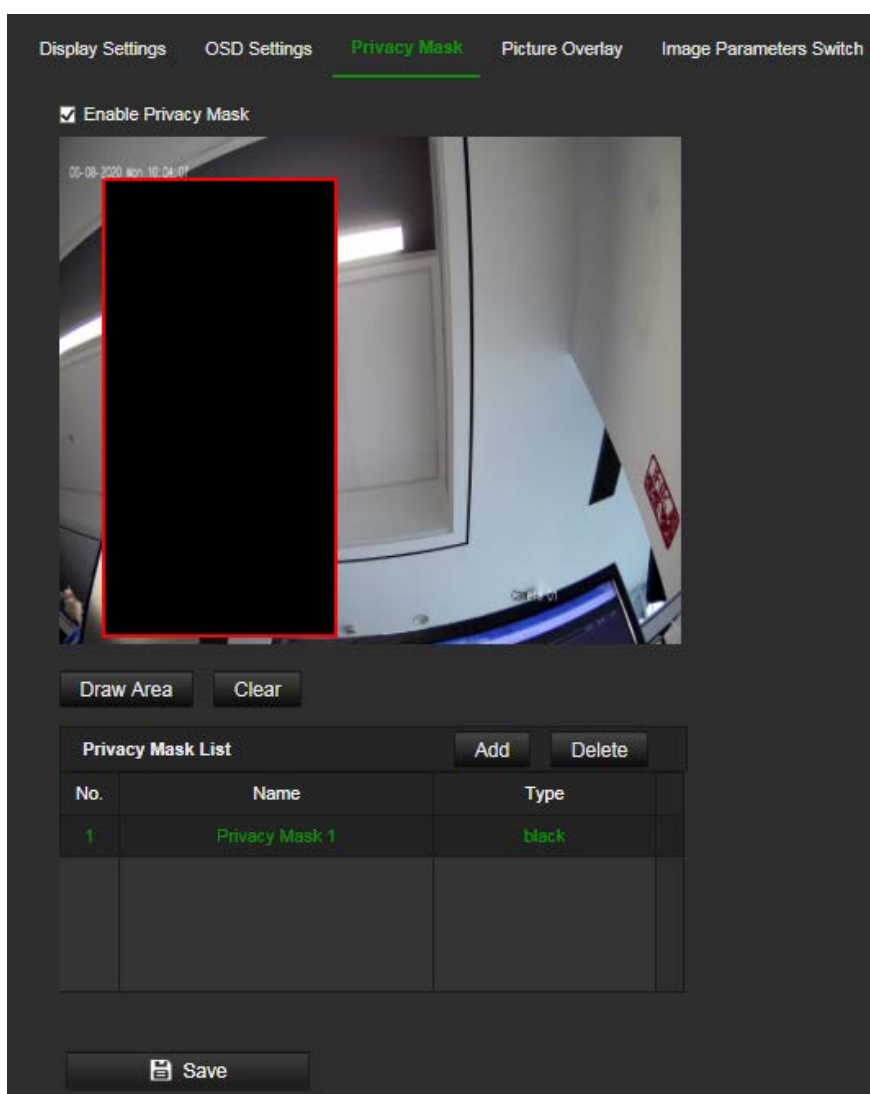
Note: If the display mode sets as transparent, the text varies according the background. With some backgrounds, the text may be not easily readable.

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 12: Camera image settings menu – Privacy mask window



To add a privacy mask area:

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

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

5. Release the mouse to generate a mask area

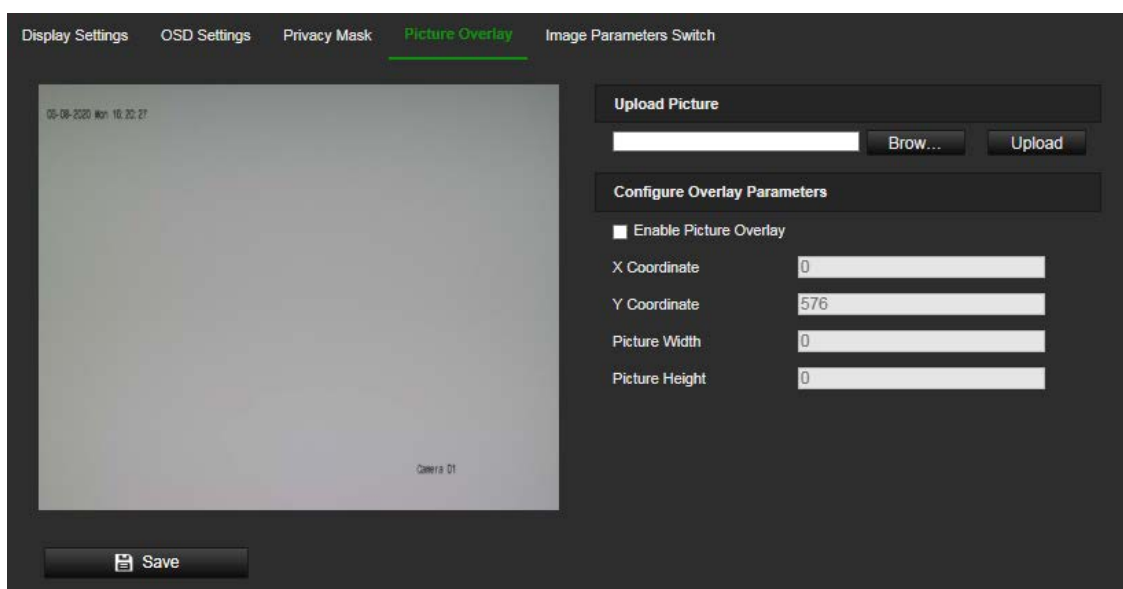
6. Click **Add** button to save the privacy mask. It will be listed in the Privacy Mask List.
7. Modify the **Name** of the saved privacy masks.
8. Choose **Type** of the masks. Black and Mosaic are available for a single privacy mask.
9. (optional) To delete a saved mask, select the mask in the list, and click Delete.
10. Click **Save** to save changes.

Picture overlay

The Picture Overlay function enables you to overlay a picture, such as a company logo, on the image, for example. The picture must be in RGB24 bmp format and the maximum size of the picture is 128*128.

To add a picture overlay:

1. Click **Configuration > Image > Picture Overlay**.



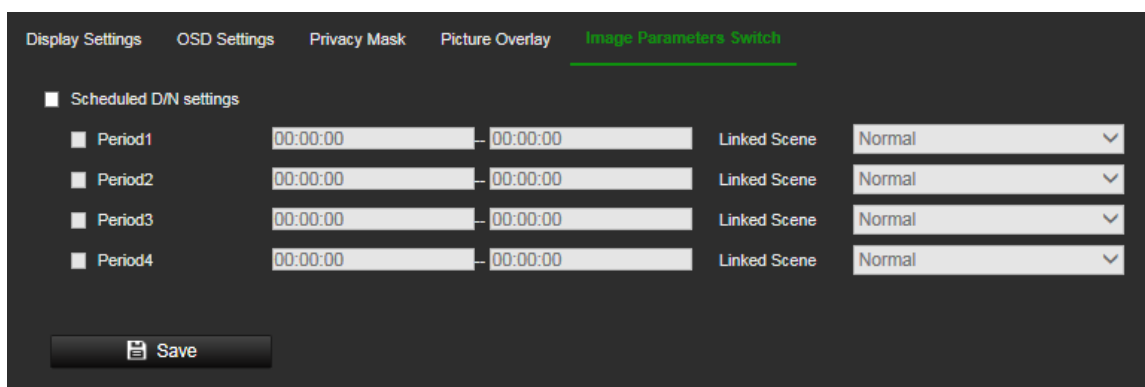
2. Click **Browse** to select a picture.
3. Click **Upload** to upload it.
4. Select the **Enable Picture Overlay** check box to enable the function.
5. Drag the red rectangle to adjust the position.
6. Click **Save** to save settings.

Image parameters switch

You can link different lighting scenes to a D/N schedule. Before linking the lighting scenes to the D/N schedule, define the scenes under the Image settings menu (see "Image" on page 53 for further information). You can link up to four lighting scenes to the scheduled D/N.

To set up an image parameter switch:

1. Click **Configuration > Image > Image Parameters Switch**.



The screenshot shows the 'Image Parameters Switch' configuration window. At the top, there are tabs: 'Display Settings', 'OSD Settings', 'Privacy Mask', 'Picture Overlay', and 'Image Parameters Switch' (which is highlighted in green). Below the tabs, there is a section titled 'Scheduled D/N settings' with a checkbox that is currently unchecked. Under this section, there are four rows, each representing a time period: 'Period1', 'Period2', 'Period3', and 'Period4'. Each row has a checkbox to its left, followed by two time input fields (start and end times, both currently set to '00:00:00'), a 'Linked Scene' label, and a dropdown menu currently set to 'Normal'. At the bottom left of the window is a 'Save' button with a floppy disk icon.

2. Select the **Scheduled D/N settings** check box to enable this function.
3. Select the required *Period* check box, set the time period and the linked scene.
4. Click **Save** to save changes.

Motion detection alarms

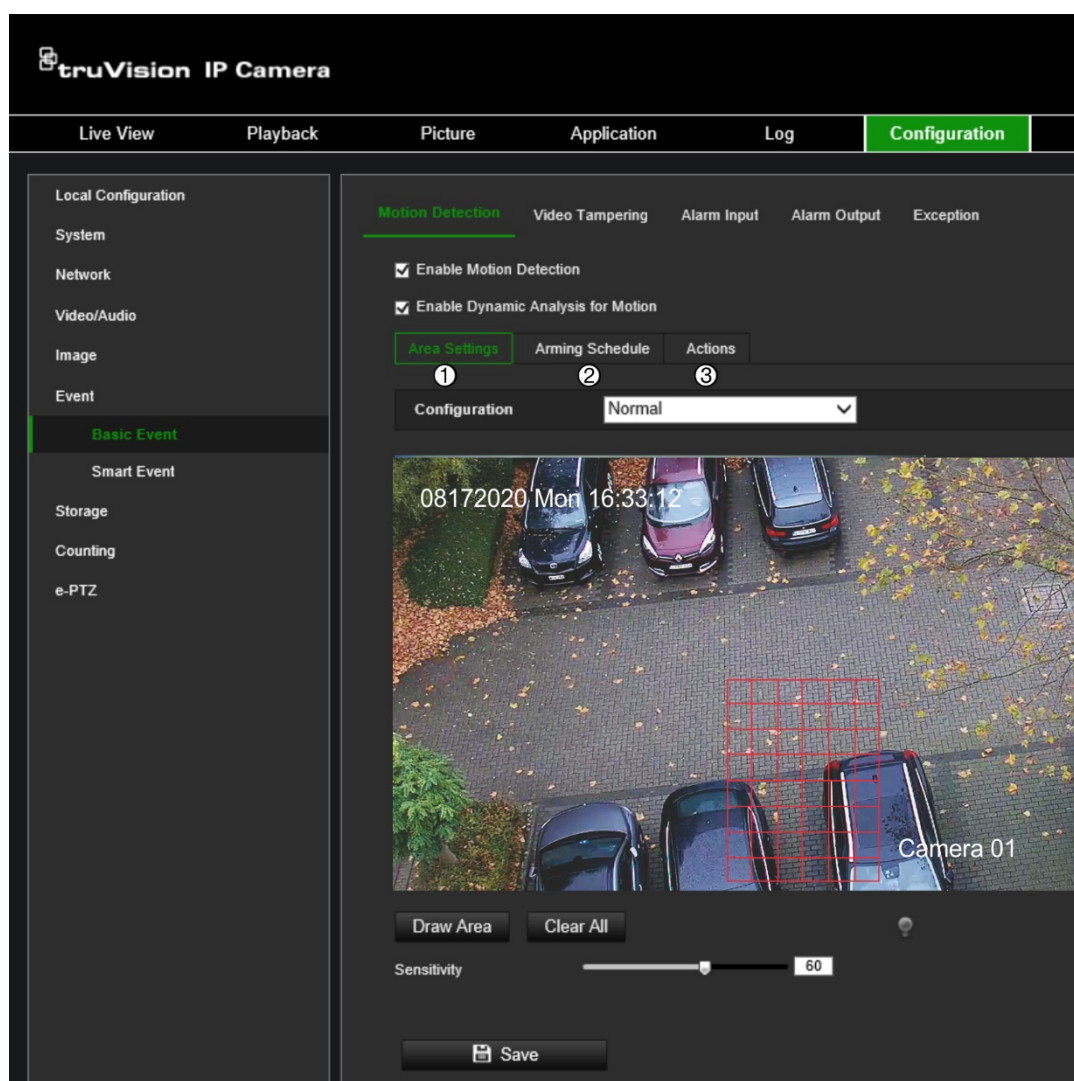
You can define motion detection alarms. A motion detection alarm refers to an alarm triggered when the camera detects motion. However, the motion alarm is only triggered if it occurs during a programmed time schedule.

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 13: 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 13, item 1).
2. **Arming schedule:** Define the schedule during which the system detects motion (see Figure 13, item 2).
3. **Recording schedule:** Define the schedule during which motion detection can be recorded. See “Recording schedule” on page 86 for further information.
4. **Actions:** Specify the method of response to the alarm (see Figure 13, item 3).
5. **Normal and advanced configuration:** Normal configuration allows you to set the sensitivity level of the motion detection (see Figure 13, item 4). Advanced configuration gives you much more control over how motion is detected. It allows you to set the sensitivity level 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. Click **Configuration > Event > Basic Event > Motion Detection**.

- **Set up the motion detection area:**

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.

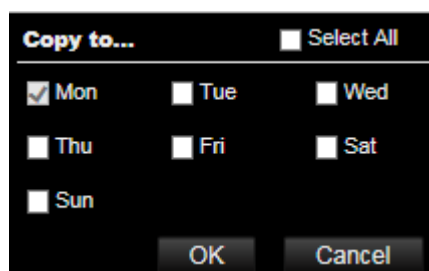
3. Select **Normal** mode from the drop-down list.
4. Click **Draw Area**. Click and drag the mouse on the live video image to draw an area sensitive to motion detection.

Note: You can draw up to eight motion detection areas on the same image.

5. Click **Stop Drawing** to finish drawing. Click **Clear All** to delete all areas marked and restart drawing.
6. Move the **Sensitivity** slider to set the sensitivity of the detection. All areas will have the same sensitivity level.

- **Set up the arming schedule:**

7. Drag and click the time bar to edit the arming schedule. In the pop-up box, enter the start and end times (hour and minutes).
8. Click  to copy the schedule to other days or to the whole week.



- **Set up linking method to the motion detection alarm:**

9. Click **Actions** to specify when an event occurs. Select one or more response methods for the system when a motion detection alarm is triggered:

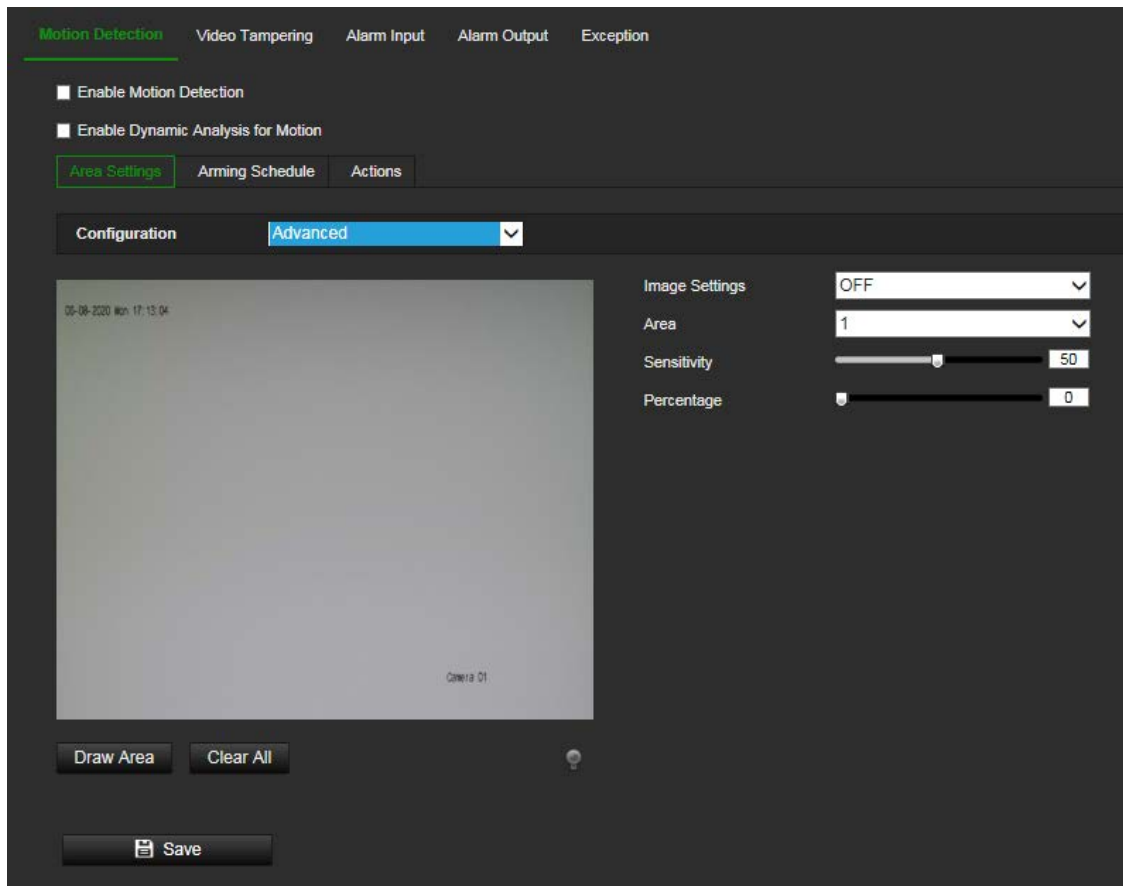
Send Email	Send an email to a specified address when there is a motion detection alarm. Note: You must configure email settings before enabling this option. See "To set up the email parameters" on page 42 for further information. If you want to send the event snapshot together with the email, check the Attached Snapshot option.
Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.

Upload to FTP/Memory Card/NAS	Capture the image when an alarm is triggered and upload the picture to NAS, Memory Card or FTP server. Note: To upload the snapshot to NAS, you must firstly configure the NAS settings. See “NAS” on page 93 for further information. To upload the snapshot to an FTP, you must firstly configure the FTP settings. See “To define the FTP parameters” on page 41 for further information. Enable the Upload Type option. To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also Enable Event-triggered Snapshot under the snapshot parameters. See “Scheduled snapshot” on page 89 for further information.
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.

10. Click **Save** to save changes.

To set up motion detection in advanced mode:

1. Click **Configuration > Event > Basic Event > Motion Detection**.
 - **Set up the motion detection area:**
 2. Select the **Enable Motion Detection** box. Select **Enable Dynamic Analysis for Motion** if you want to see where motion occurs in real-time.
- Note:** If you do not want the detected object to be marked with the green frame, select **Disable** from Configuration > Local > Live View Parameters > Rules.
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.

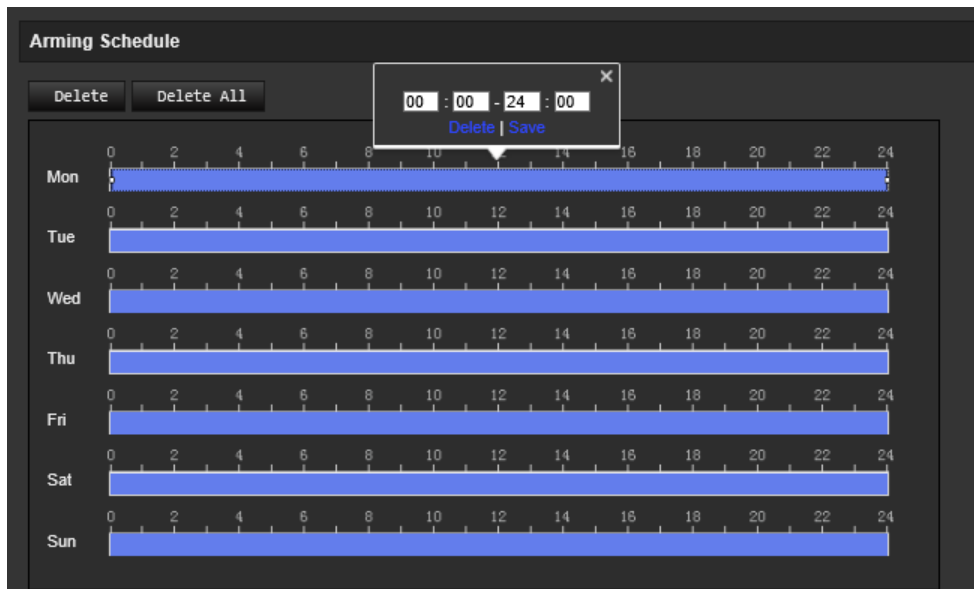
5. Select **Area No.** and click **Draw Area**. Click and drag the mouse on the live video image to draw an area sensitive to motion detection.

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

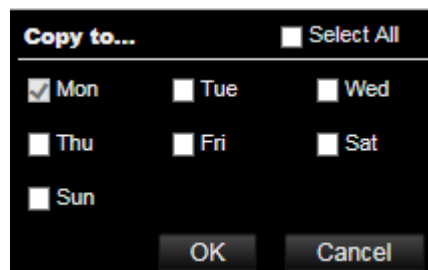
6. Click **Stop Drawing** to finish drawing. Click **Clear All** to delete all areas marked and restart drawing.
7. Move the **Sensitivity** slider to set the sensitivity of the detection for the selected areas.
8. Move the **Percentage** slider to set the proportion of the object that must occupy the defined area to trigger an alarm. Default is zero.
9. Click **Save** to save the changes for that area.
10. Repeat steps 7 to 9 for each area to be defined.

- **Set up the arming schedule:**

11. Under **Arming Schedule**, click the day you want to schedule. The Time pop-box appears. Enter the desired start and end times to detect motion.



12. If you want to copy a day's schedule, position the mouse on the desired day and click  to copy the schedule to other days or to the whole week. The *Copy to* pop-up window appears. Select the desired days to which to copy the schedule and click **OK** to save the changes.



13. Click **OK** to save changes.

- **Set up linking method to the motion detection alarm:**

14. Click **Actions** to specify when an event occurs. Select one or more response methods for the system when a motion detection 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 42 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.

Upload to FTP/Memory Card/NAS	Capture the image when an alarm is triggered and upload the picture to NAS, Memory Card or FTP server. Note: To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS” on page 93 for further information. To upload the snapshot to an FTP, you must first configure the FTP settings. See “To define the FTP parameters” on page 41 for further information. Enable the Upload Type option. To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also Enable Event-triggered Snapshot under the snapshot parameters. See “Scheduled snapshot” on page 89 for further information.
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.

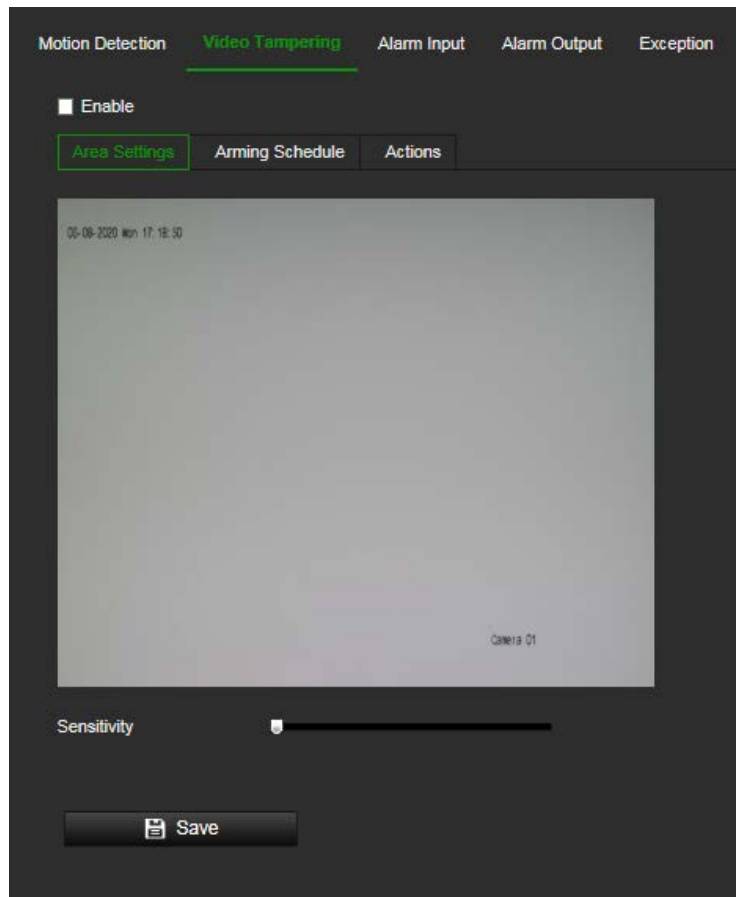
15. Click **Save** to save changes.

Video tampering

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

To set up tamper-proof alarms:

1. Click **Configuration > Event > Basic Event > Video Tampering**.



2. Select the **Enable** box to enable this detection of event.
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 62 for more information.
5. Specify the actions when an event occurs. Select one or more response actions when a video tampering 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 42 for further information. If you want to send the event snapshot together with the email, check 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. Check “Select All” or each individual alarm output. Note: This option is only supported by cameras that support alarm output.

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

Alarm inputs and outputs

To set up the external alarm input:

1. Click **Configuration > Event > Basic 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 actions.

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 42 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.
Upload to FTP/Memory Card/NAS	Capture the image when an alarm is triggered and upload the picture to NAS, Memory Card or FTP server. Note: To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS” on page 93” on page 91 for further information. To upload the snapshot to an FTP, you must first configure the FTP settings. See “To define the FTP parameters” on page 41 for further information. Enable the Upload Type option. To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also Enable Event-triggered Snapshot under the snapshot parameters. See “Scheduled snapshot” on page 89 for further information.
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.

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

To set up alarm output:

1. Click **Configuration > Event > 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 62 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 14: Exception window

The screenshot shows the 'Exception' configuration window. At the top, there are tabs for 'Motion Detection', 'Video Tampering', 'Alarm Input', 'Alarm Output', and 'Exception' (which is highlighted in green). Below the tabs, there is a 'Notification Type' dropdown menu set to 'HDD Full'. The main area is divided into two columns. The left column is titled 'Normal Actions' and contains two checkboxes: 'Send Email' and 'Notify Alarm Recipient'. The right column is titled 'Trigger Alarm Output' and contains two checkboxes: 'A->1' and 'A->2'. At the bottom of the window, there is a 'Save' button with a floppy disk icon.

To set up exception alarms:

1. Click **Configuration > Event > Basic Event > Exception**.
2. Under **Exception Type**, select an exception type from the drop-down list.
3. Specify the actions when an event occurs. Select one or more response actions when an exception 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 42 for further information. If you want to send the event snapshot together with the email, check 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.

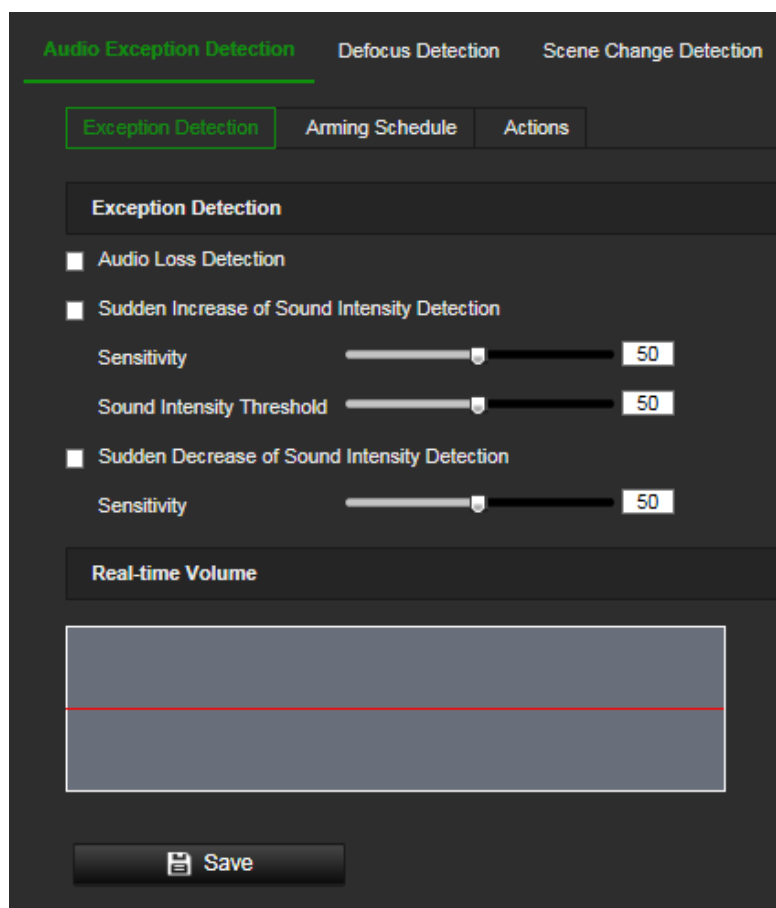
4. Click **Save** to save changes.

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 some certain actions can be taken when the alarm is triggered.

To set up audio exception detection:

1. Click **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 the sound steep rise in the surveillance scene. You can set the detection sensitivity and threshold for sound steep rise.
4. Select the **Sudden Decrease of Sound Intensity Detection** check box to detect the sound steep drop in the surveillance scene. You can set the detection sensitivity and threshold for sound steep drop.

Notes:

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

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

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

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



6. Select **Actions** and select the linkage methods for audio exception:

Normal Actions	This is a group selection. It automatically selects "Send Email" and "Notify Alarm Recipient"
Send Email	Sends 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 42 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 the 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 feature an alarm output.
A->1	Trigger the alarm input A->1.
A->2	Trigger the alarm input A->2.
Trigger Recording	Triggers the recording to start in the camera.
A1	The camera has only one channel.

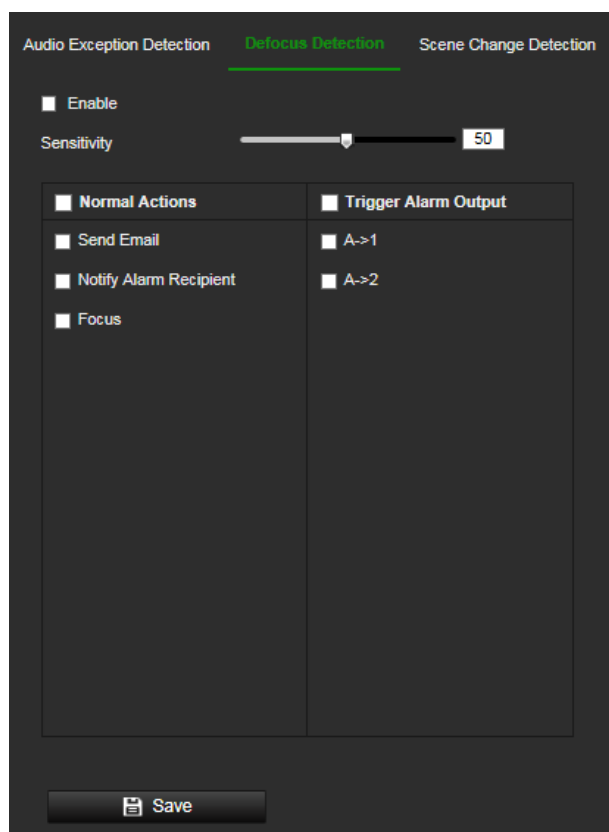
- Click **Save** to save the settings.

Defocus detection

The camera can detect image blur caused by defocusing of the lens, triggering a series of alarm actions. This can be set up to trigger a series of alarm actions.

The sensitivity level determines how much blur is tolerated by the camera before triggering an alarm. When enabled, the camera regularly checks the level of image focus (to allow for variations in light during the day) and then compares the current image to that of the reference image to see if there is a difference. A high sensitivity level means that there cannot be a large variance between the reference and current image.

Figure 15: Defocus detection window



To set up defocus detection:

1. Click **Configuration > Event > Smart Event > Defocus Detection**.
2. Select the **Enable** check box to enable the function.

Sensitivity: The range is between 1 and 100. The higher the sensitivity level, the smaller the defocus required to trigger an alarm.

3. Specify the linkage method when an event occurs. Select one or more response methods for the system when a defocus detection alarm is triggered.

Normal Actions	This is a group selection. It automatically selects "Send Email" and "Notify Alarm Recipient".
Send Email	Sends 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 42 for further information. If you want to send the event snapshot together with the email, select the Attached Snapshot option.
Notify Alarm Recipient	Sends an exception or alarm signal to the remote management software when an event occurs.
Focus	Tries to refocus the camera by adjusting the back-focus.
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 feature an alarm output.
A->1	Trigger the alarm input A->1.
A->2	Trigger the alarm input A->2.

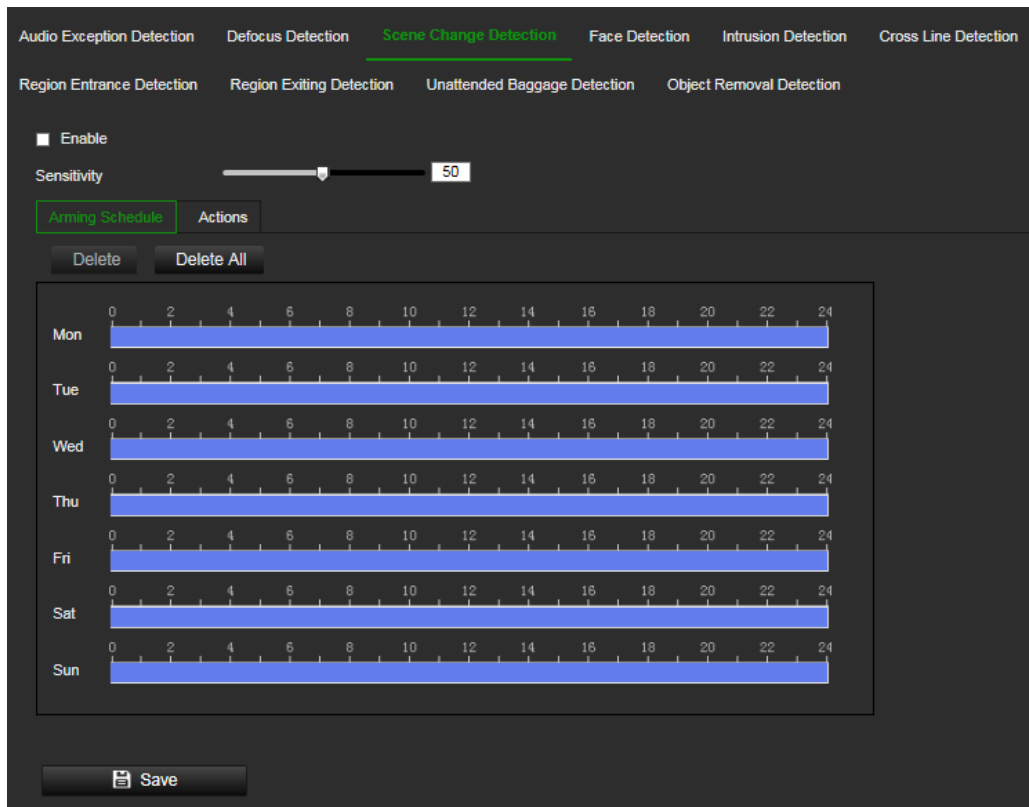
4. Click **Save** to save changes.

Scene change detection

You can configure the camera to trigger an alarm when the camera detects a change in the scene caused by a physical repositioning of the camera. It can be set up to trigger a series of alarm actions.

To set up scene change detection:

1. Click **Configuration > Event > Smart Event > Scene Change Detection**.
2. Select the **Enable** check box to enable the function.
3. Configure the sensitivity ranging from 1 to 100, the higher the sensitivity, the easier the change of scene can trigger the alarm.
4. Click the **Arming Schedule** tab to set the arming schedule for the alarm input.



- Click the **Actions** tab to specify the linkage method when an event occurs. Select one or more response methods for the system when a scene change detection alarm is triggered.

Normal Actions	This is a group selection. It automatically selects "Send Email" and "Notify Alarm Recipient".
Send Email	Sends 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 42 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 the 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 feature an alarm output.
A->1	Trigger the alarm input A->1.
Trigger Recording	Triggers the recording to start in the camera.
A1	The camera has only one channel.

- Click **Save** to save changes.

Face detection

This function can detect faces that appear in the surveillance scene. It can be set up to trigger a series of alarm actions.

To set up face detection:

1. Click **Configuration > Event > Smart Event > Face Detection**.

The screenshot shows the 'Face Detection' configuration page. At the top, there are tabs for various detection types: Audio Exception Detection, Defocus Detection, Scene Change Detection, Face Detection (highlighted), Intrusion Detection, and Cross Line Detection. Below these are more specific event types: Region Entrance Detection, Region Exiting Detection, Unattended Baggage Detection, and Object Removal Detection. The main configuration area includes two checkboxes: 'Enable Face Detection' and 'Enable Dynamic Analysis for Face Detection'. A 'Sensitivity' slider is set to 3. There are two buttons: 'Arming Schedule' (highlighted) and 'Actions'. Below these are 'Delete' and 'Delete All' buttons. The 'Arming Schedule' section shows a 7-day calendar (Mon-Sun) with a 24-hour time scale (0 to 24). Each day has a blue bar indicating the arming schedule, which covers the entire 24 hours. At the bottom is a 'Save' button.

2. Select the **Enable Face Detection** check box to enable the function.
3. Select the **Enable Dynamic Analysis for Face Detection** check box. The detected face is marked with a green rectangle in the live mode.
Note: To be able to mark the detected face in live view mode, go to **Configuration > Local** to enable the rules.
4. Click-and-drag the slider to set the detection sensitivity. The Sensitivity ranges from 1 to 5. The higher the value is, the more easily the face can be detected.
5. Set the arming schedule for the alarm input. See “To set up motion detection” on page 62 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	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 42 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.
Upload to FTP/Memory Card/NAS	Capture the image when an alarm is triggered and upload the picture to NAS, Memory Card or FTP server. Note: To upload the snapshot to NAS, you must first configure the NAS settings. See ““NAS” on page 93 for further information. To upload the snapshot to an FTP, you must first configure the FTP settings. See “To define the FTP parameters” on page 41 for further information. Enable the Upload Type option. To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also select Enable Event-triggered Snapshot under the snapshot parameters. See “Scheduled snapshot” on page 89 for further information.
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.

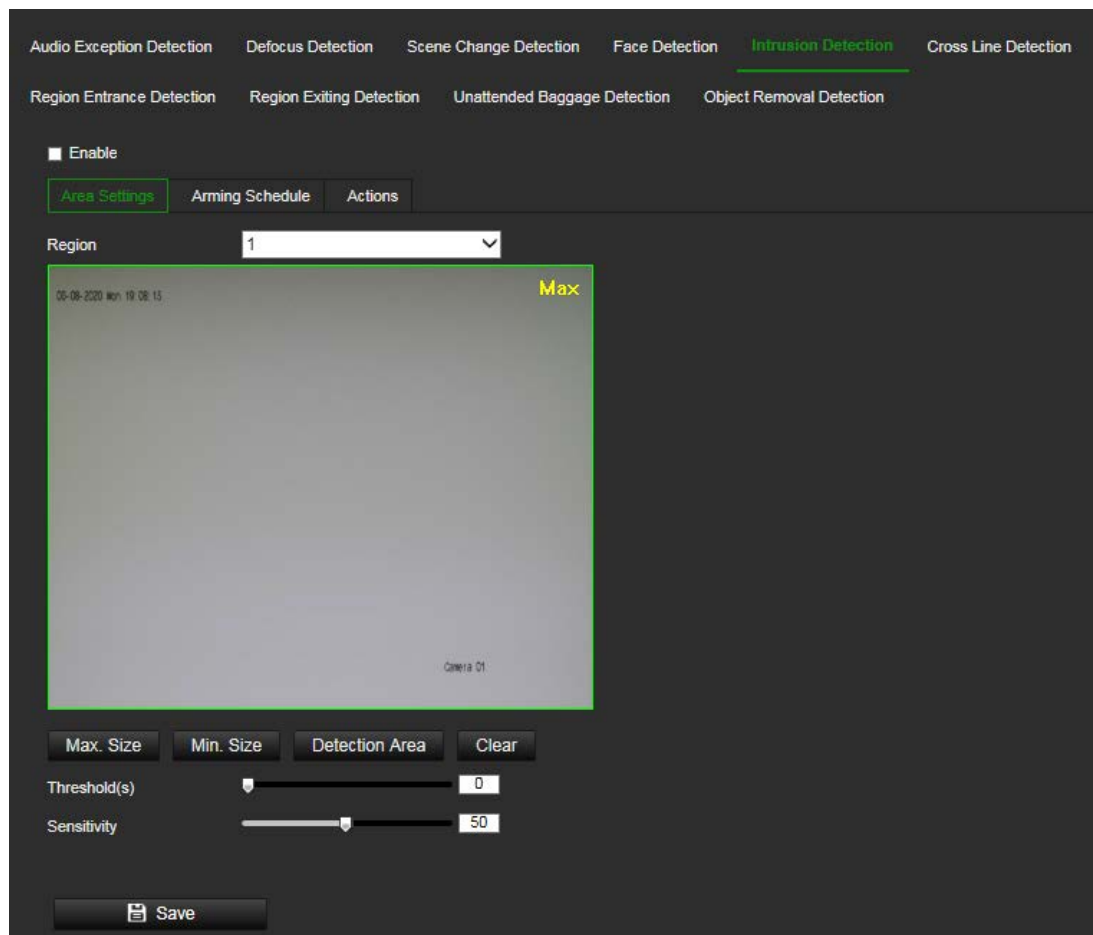
7. Click **Save** to save changes.

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 set up intrusion detection:

1. Click **Configuration > Event > Smart 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. Choose the region to be configured.

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 62 for more information.
6. Specify the actions when an event occurs. Select one or more response actions when an intrusion detection 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 42 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.
Upload to FTP/Memory Card/NAS	Capture the image when an alarm is triggered and upload the picture to NAS, Memory Card or FTP server. Note: To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS for further information. To upload the snapshot to an FTP, you must first configure the FTP settings. See “To define the FTP parameters” on page 41 for further information. Enable the Upload Type option. To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also Enable Event-triggered Snapshot under the snapshot parameters. See “Scheduled snapshot” on page 89 for further information.
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.

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

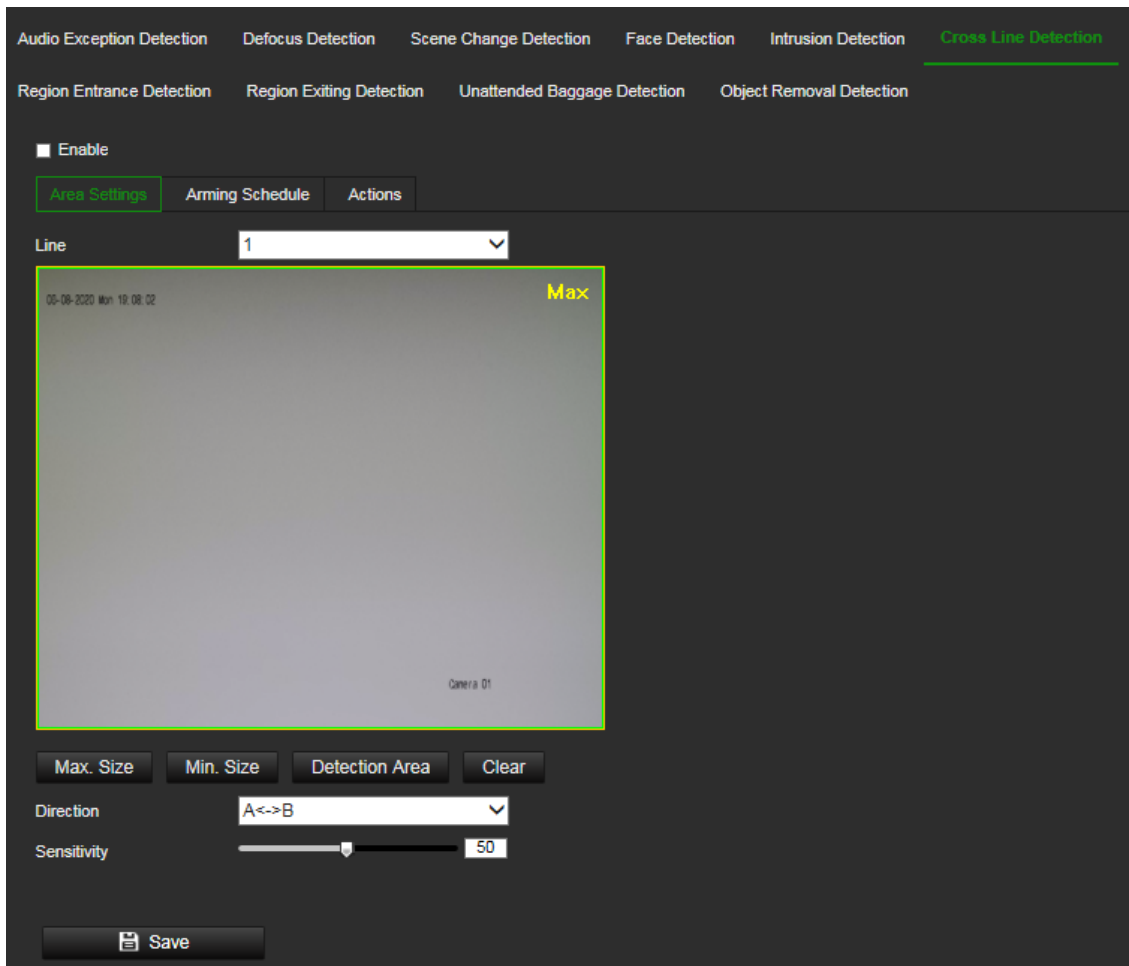
Cross line detection

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 is crossing the line from left to right or from right to left. Bidirectional is crossing the line from both directions.

A series of actions can be triggered if an object-person is detected crossing the line.

To set up cross line detection:

1. Click **Configuration > Event > Smart 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 and 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 is, the more easily the line crossing action can be detected.
6. If desired, select another line crossing area to configure from the dropdown menu. Up to four cross line areas can be configured.
7. Set the arming schedule for the alarm input. See “To set up motion detection” on page 62 for more information.
8. Specify the linkage method when an event occurs. Select one or more response methods for the system when a line cross detection 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 42 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.
Upload to FTP/Memory Card/NAS	Capture the image when an alarm is triggered and upload the picture to NAS, Memory Card or FTP server. Note: To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS” on page 93 for further information. To upload the snapshot to an FTP, you must first configure the FTP settings. See “To define the FTP parameters” on page 41 for further information. Enable the Upload Type option. To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also Enable Event-triggered Snapshot under the snapshot parameters. See “Scheduled snapshot” on page 89 for further information.
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.

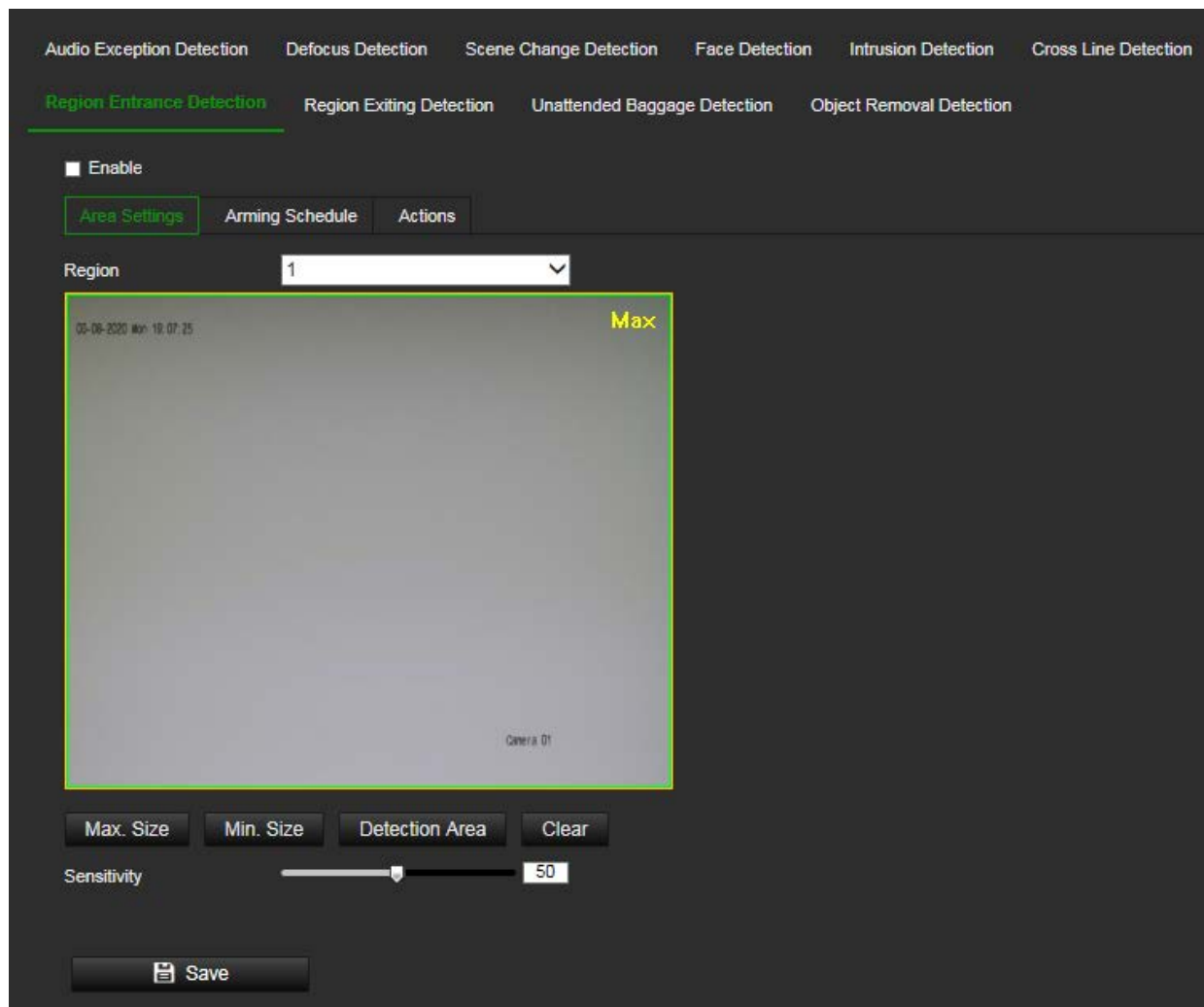
9. Click **Save** to save changes.

Region entry detection

This function detects people or objects that enter a pre-defined virtual region from the outside place. It can be set up to trigger a series of alarm actions.

To set up the region entrance detection:

1. Click **Configuration > Event > Smart Event > Region Entrance Detection**.



2. Select the **Enable** check box to enable the function.
3. Select **Region** from the drop-down list for detection settings.
4. Click **Area Settings** and click **Draw Area** button to start the area drawing.
5. Click on the live video to specify the four vertexes of the detection region and release the mouse to complete drawing.
6. Set the maximum and minimum sizes of valid targets. Targets that are smaller or larger than the valid target size cannot trigger detection.
Max. Size: The maximum size of a valid target. Targets with larger sizes would not trigger detection.
Min. Size: The minimum size of a valid target. Targets with smaller sizes would not trigger detection.
7. Click **Stop Drawing** when finish drawing.
8. Drag the slider to set the sensitivity value.
Sensitivity: Range [1-100]. Sensitivity stands for the percentage of the body/object part of an acceptable target that enters the pre-defined region.

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

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

Example: if you set the value as 60, the action can be counted as a region entrance action only when 40 percent body part enters the region.

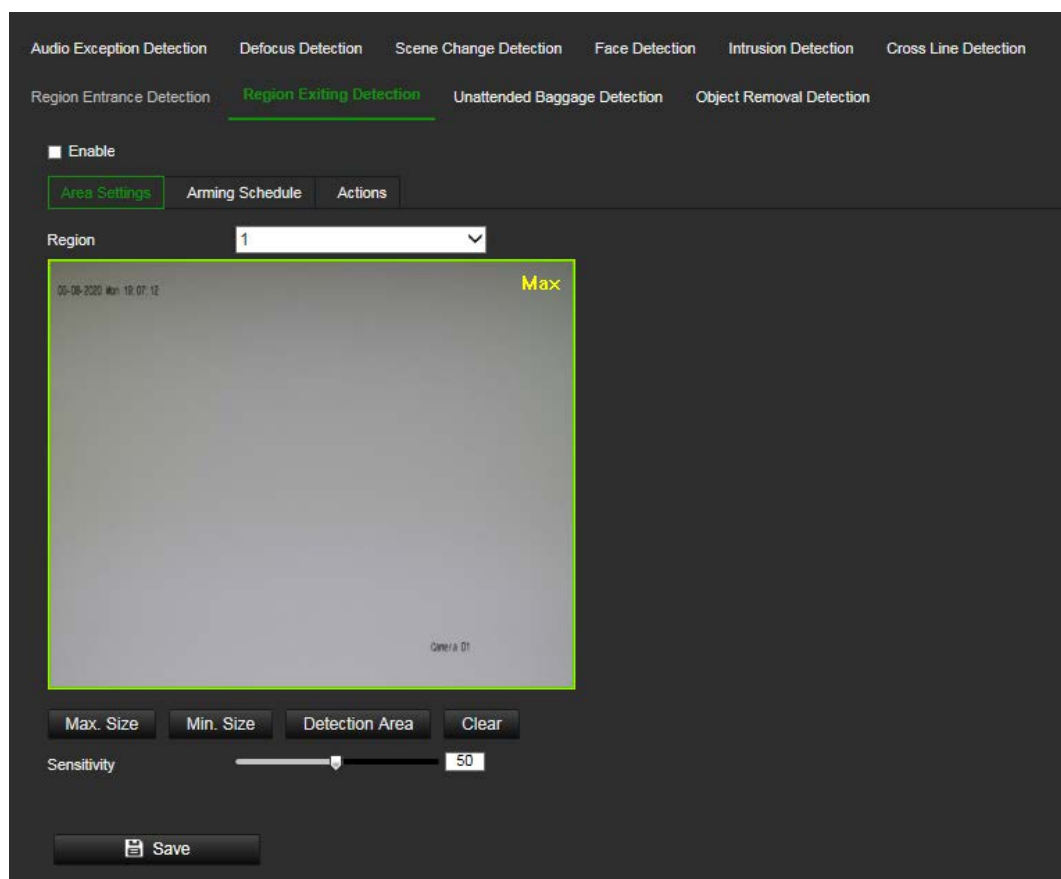
9. Repeat the above steps to configure other regions. Up to four regions can be set. You can click the **Clear** button to clear all pre-defined regions.
10. Click **Arming Schedule** to set the arming schedule.
11. Click **Actions** to select the linkage methods.
12. Click **Save** to save the settings.

Region exit detection

This function detects people, vehicle or other objects which exit from a pre-defined virtual region. It can be set up to trigger a series of alarm actions.

To set up the region of exit detection:

1. Click **Configuration > Event > Smart Event > Region Exiting Detection**.



2. Select the **Enable** check box to enable the function.
3. Select **Region** from the drop-down list to set up.
4. Click **Area Settings** and click **Draw Area** button to start the drawing area.

5. Click on the live video to specify the four vertexes of the detection region and release the mouse to complete drawing.
6. Set the Max. Size and Min. Size for valid targets. Targets that are smaller or larger than the valid target size cannot trigger detection.

Max. Size: The maximum size of a valid target. Targets with larger sizes would not trigger detection.

Min. Size: The minimum size of a valid target. Targets with smaller sizes would not trigger detection.

7. Click **Stop Drawing** when finished drawing.
8. Drag the slider to set the sensitivity value.

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

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

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

Example: if you set the value as 60, the action can be counted as a region exiting action only when 40 percent body part leaves the region.

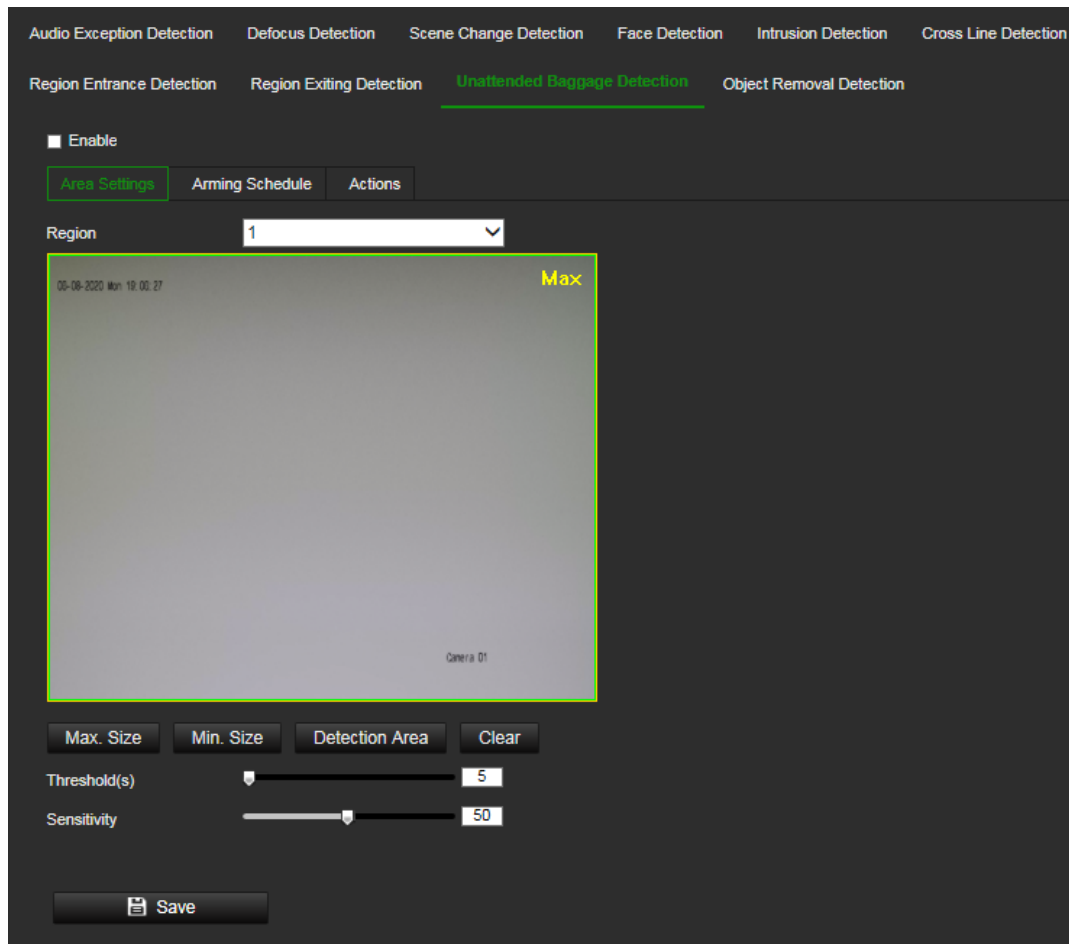
9. Repeat the above steps to configure other regions. Up to four regions can be set. You can click the **Clear** button to clear all pre-defined regions.
10. Click **Arming Schedule** to set the arming schedule.
11. Click **Actions** to select the linkage methods.
12. Click **Save** to save the settings.

Unattended baggage detection

This function detects the objects left behind in the pre-defined region such as a suitcase, purse, dangerous materials, etc. It can be set up to trigger a series of alarm actions. Please note that this feature is not able to properly detect unattended objects in complex and low contrast environments.

To set up unattended baggage detection:

1. Click **Configuration > Event > Smart Event > Unattended Baggage Detection**.



2. Select the **Enable** check box to enable the function.
3. Select **Region** from the drop-down list to set up.
4. Click **Area Settings** and click **Draw Area** button to start the drawing area.
5. Click on the live video to specify the four vertexes of the detection region and release the mouse to complete drawing.
6. Set the maximum and minimum sizes of valid targets. Targets that are smaller or larger than the valid target size cannot trigger detection.
Max. Size: The maximum size of a valid target. Targets with larger sizes would not trigger detection.
Min. Size: The minimum size of a valid target. Targets with smaller sizes would not trigger detection.
7. Click **Stop Drawing** when finished drawing.
8. Set the time threshold and detection sensitivity for unattended baggage detection.
Threshold: Range [1-100]. The threshold for the time of the objects left over in the region. If you set the value as 10, alarm is triggered after the object has appeared in the region for 10s.
9. Drag the slider to set the sensitivity value.
Sensitivity: Range [1-100]. Sensitivity stands for the percentage of the body/object part of an acceptable target that enters the pre-defined region.

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

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

Example: if you set the value as 60, a target is possible to be counted as an unattended baggage only when 40 percent body part of the target enters the region.

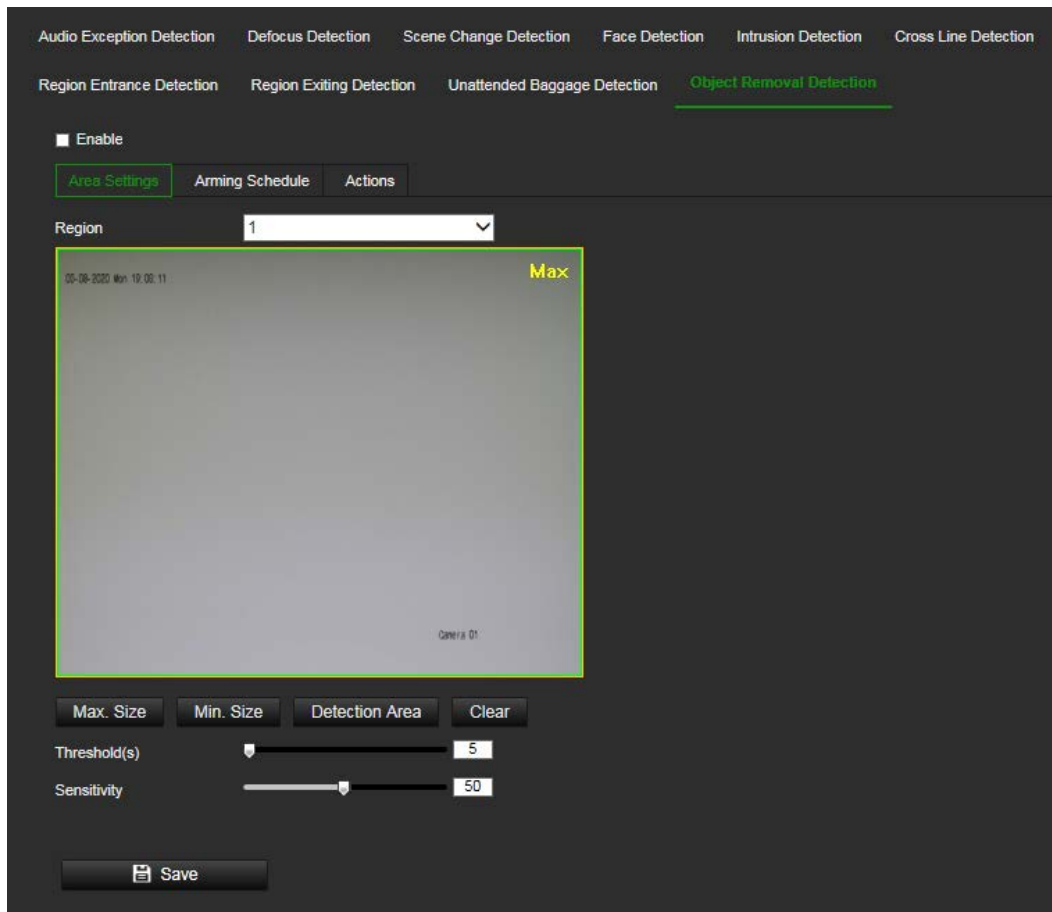
10. Repeat the above steps to configure other regions. Up to four regions can be set.
You can click the Clear button to clear all pre-defined regions.
11. Click Arming Schedule to set the arming schedule.
12. Click Actions to select the linkage methods.
13. Click Save to save the settings.

Object removal detection

This function detects the objects removed from the pre-defined region, such as the exhibits on display. It can be set up to trigger a series of alarm actions. Please note that this feature is not able to properly detect removed objects in complex and low contrast environments.

To set up object removal detection:

1. Click **Configuration > Event > Smart Event > Object Removal Detection**.



2. Select the **Enable** check box to enable the function.

3. Select **Region** from the drop-down list to set up.
4. Click **Area Settings** and click **Draw Area** button to start the drawing area.
5. Click on the live video to specify the four vertexes of the detection region and release the mouse to complete drawing.
6. Set the maximum and minimum sizes of valid targets. Targets that are smaller or larger than the valid target size cannot trigger detection.

Max. Size: The maximum size of a valid target. Targets with larger sizes would not trigger detection.

Min. Size: The minimum size of a valid target. Targets with smaller sizes would not trigger detection.
7. Click **Stop Drawing** when finished drawing.
8. Set the time threshold and detection sensitivity for object removal detection.
Threshold: Range [1-100]. The threshold for the time of the objects left over in the region. If you set the value as 10, alarm is triggered after the object has disappeared from the region for 10s.
9. Drag the slider to set the sensitivity value.

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

$$\text{Sensitivity} = 100 - S1/ST \times 100$$
S1 stands for the target body part that enters the pre-defined region ST stands for the complete target body.

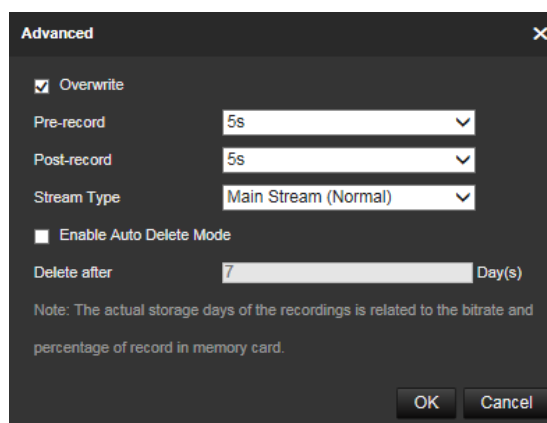
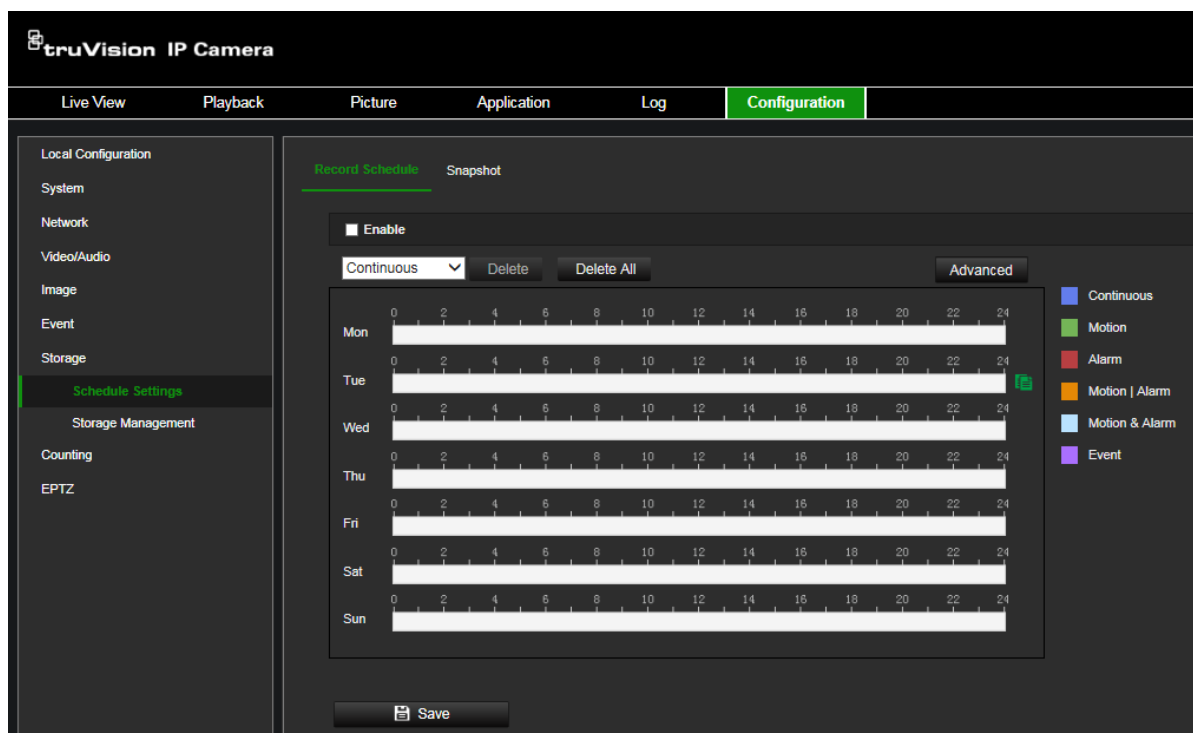
Example: if you set the value as 60, a target is possible to be counted as a removed object only when 40 percent body part of the target leaves the region.
10. Repeat the above steps to configure other regions. Up to four regions can be set.
You can click the **Clear** button to clear all pre-defined regions.
11. Click **Arming Schedule** to set the arming schedule.
12. Click **Actions** to select the linkage methods.
13. Click **Save** to save the settings.

Recording schedule

You can define a recording schedule for the camera in the “Record Schedule” window. The video recordings are saved onto 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 16: Record schedule window



Overwrite

When enabled, older camera recordings are overwritten.

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.

Stream type

You can select to record main stream or substream.

Enable Auto Delete Mode

When enabled, recorded video older than the number of days defined by “Delete after” will be automatically deleted, even if the full storage capacity has not been reached.

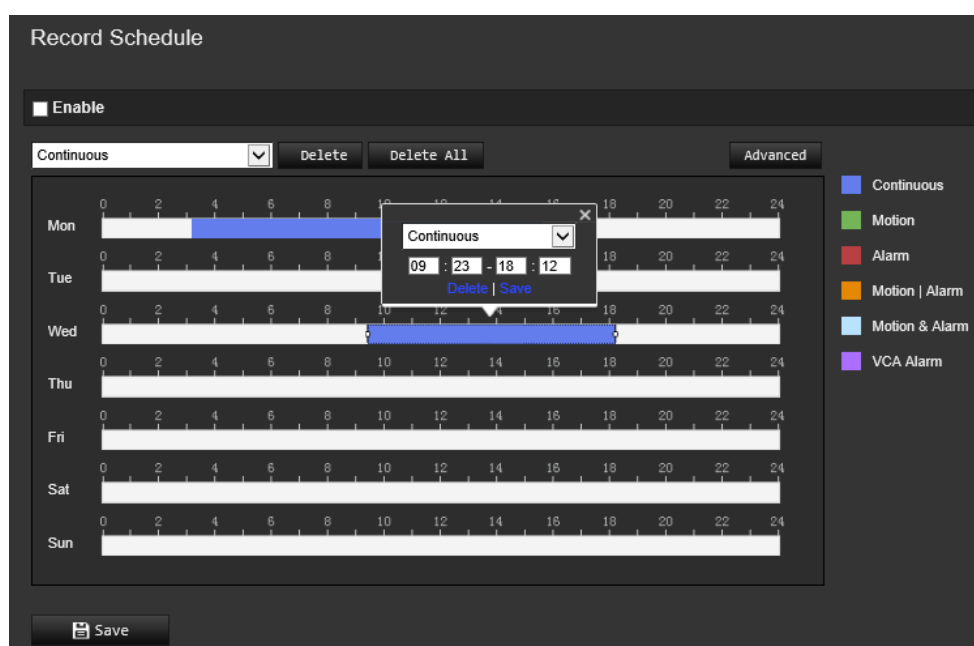
To set up a recording schedule:

1. From the menu toolbar, click **Configuration > Storage > Schedule Settings > Record Schedule**.

2. Select the **Enable** 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 box:

- **Continuous:** This is continuous recording.
- **Motion:** Video is recorded when the motion is detected.
- **Alarm:** Video is recorded when the alarm is triggered via the external alarm input channels. Besides configuring the recording schedule, you must also set the alarm type and enable the *Trigger Channel* check box in the *Linkage Method of Alarm Input Settings* interface. For detailed information, please refer to the section on alarm inputs on page 68.
- **Motion | Alarm:** Video will be recorded when the external alarm is triggered, or the motion is detected. Besides configuring the recording schedule, you must also configure the settings on the *Motion Detection* and *Alarm Input Settings*

interfaces. For detailed information, please refer to the section on alarm inputs on page 68.

- **Motion & Alarm:** Video will be recorded when the Motion and Alarm are triggered at the same time. Besides configuring the recording schedule, you must also configure the settings on the *Motion Detection* and *Alarm Input Settings* interfaces. For detailed information, please refer to the section on alarm inputs on page 68.
- **VCA Alarm:** Video will be recorded when a VCA event is triggered. Besides configuring the recording schedule, you must configure the settings of the selected VCA event type: Audio Exception Detection, Defocus Detection, Scene Change Detection, Face Detection, Intrusion Detection, Cross Line Detection, Region Entrance Detection, Region Exit Detection, Unattended Baggage Detection, Object Removal Detection.

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 define the arming schedule in order to trigger motion detection or alarm input recording.

Scheduled snapshots

You can configure scheduled snapshots and event-triggered snapshots. The captured snapshots can be stored on the SD card (if installed) 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 with a fixed interval to the FTP server. If you have configured the FTP settings and enabled **Upload Type** in the **Network > Advanced Settings > 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 > Advanced Settings > FTP** tab for motion detection or an alarm input, the snapshots will not be uploaded to the FTP if this option is disabled.

To set up continuous and event-triggered snapshots:

1. From the menu toolbar, click **Configuration > Storage > Schedule Settings > Snapshot > Capture Schedule**.

Note: *Continuous* is the only recording type available.

Record Schedule **Snapshot**

Capture Schedule Capture Parameters

Continuous ▼ Delete Delete All Advanced

Mon 0 2 4 6 8 10 12 14 16 18 20 22 24

Tue 0 2 4 6 8 10 12 14 16 18 20 22 24

Wed 0 2 4 6 8 10 12 14 16 18 20 22 24

Thu 0 2 4 6 8 10 12 14 16 18 20 22 24

Fri 0 2 4 6 8 10 12 14 16 18 20 22 24

Sat 0 2 4 6 8 10 12 14 16 18 20 22 24

Sun 0 2 4 6 8 10 12 14 16 18 20 22 24

Continuous

Save

2. Click-and-drag the mouse on the time bar of the desired days to set the capture schedule.
3. Click **Advanced** to select the stream type.
4. Select the **Capture Parameters** tab to configure the captured snapshot parameters.

Record Schedule **Snapshot**

Capture Schedule **Capture Parameters**

Timing

☐ Enable Timing Snapshot

Format JPEG ▼

Resolution 3840*2160 ▼

Quality High ▼

Interval 1000 millisecond ▼

Event-Triggered

☐ Enable Event-Triggered Snapshot

Format JPEG ▼

Resolution 3840*2160 ▼

Quality High ▼

Interval 1000 millisecond ▼

Capture Number 4

Save

5. In the *Timing* section, select the parameters for continuous snapshots:

- a) Select the **Enable Timing Snapshot** check box.
- b) Select the desired format of the snapshot. Default is JPEG.
- c) Select the desired resolution and quality of the snapshot.
- d) Enter the time interval between two snapshots. Select the unit of time from the drop-down list: milliseconds, seconds, minutes, hour, or day.

In the *Event-Triggered* section, select the parameters for event-triggered snapshots:

- a) Select the **Enable Event-Triggered Snapshot** check box.
- b) Select the desired format of the snapshot. Default is JPEG.
- c) Select the desired resolution and quality of the snapshot.
- d) Enter the time interval between two snapshots. Select the unit of time from the drop-down list: milliseconds, seconds, minutes, hour, or day.

6. Under **Capture Number**, enter the total number of snapshots that can be taken.
7. Click **Save** to save changes.

HDD management

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.

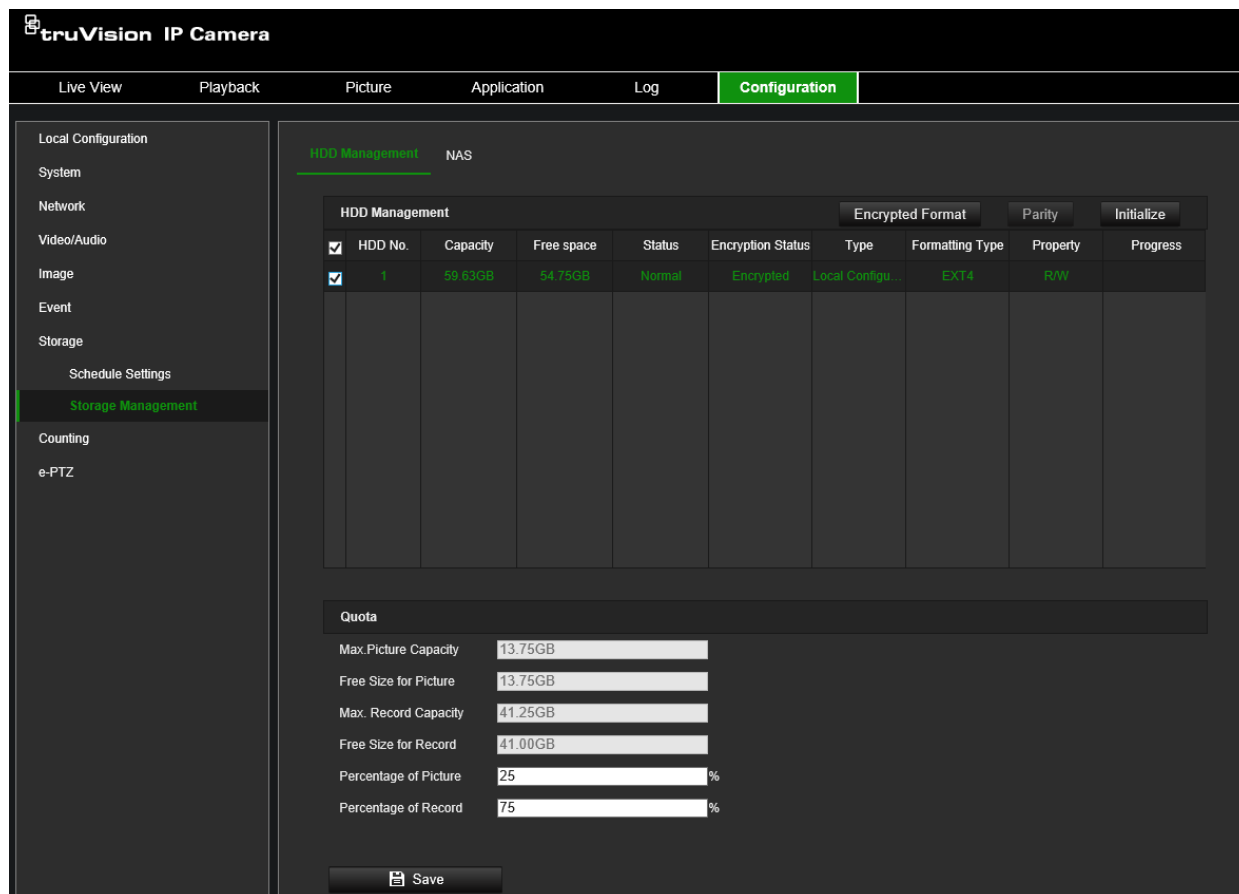
If Overwrite is enabled, the oldest files are overwritten when the storage becomes full.

To ensure an efficient use of the storage space available on HDDs, you can control the camera's storage capacity using HDD quota management. This function lets you allocate different storage capacities for main stream/substream recordings and snapshots.

Note: If the overwrite function is enabled, the maximum capacity for both recordings and snapshots is set to zero by default.

To format the storage devices:

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



2. Select the **HDD No.** to select the storage.
3. Click the **Encrypted format** button. A window appears for you to select your formatting permission. Some SD cards can support **Encrypted formatting** that provides extra encryption for the data stored on the SD card.
4. Click **OK** and enter the admin password to start the formatting process.
5. Select an HDD and do one of the following steps
 - a) If the disk status is Uninitialized, click **Initialize** to initialize it. When initialization is finished, the status becomes Normal.
 - b) If the disk status is Unencrypted, click **Encrypted Format** to format it. The encryption password is required for this process.
 - c) The status of the encrypted memory card is Encrypted or Verification Failed. If the status is *Verification Failed*, click **Parity** and enter a password for verification. If the verification is successful, the status becomes Encrypted.

To set the quota storage for recordings and snapshots:

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

2. Enter the quota percentage for snapshots and for main stream/substream recordings.
3. Click **Save** and refresh the browser page to activate the settings.

NAS management

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.

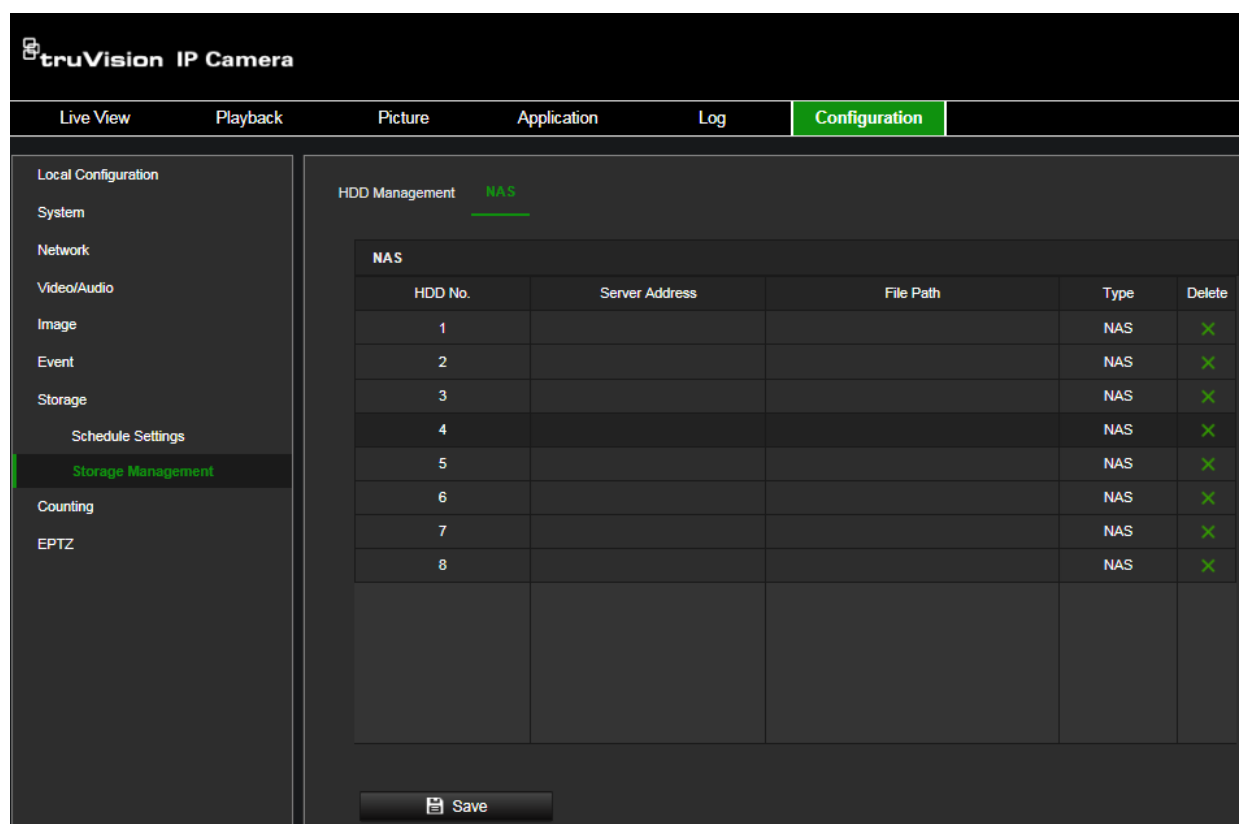
The NAS disk should be available within the network and correctly configured to store the recorded files, log files, etc.

Notes:

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

To set up a NAS system:

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



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

Object counting

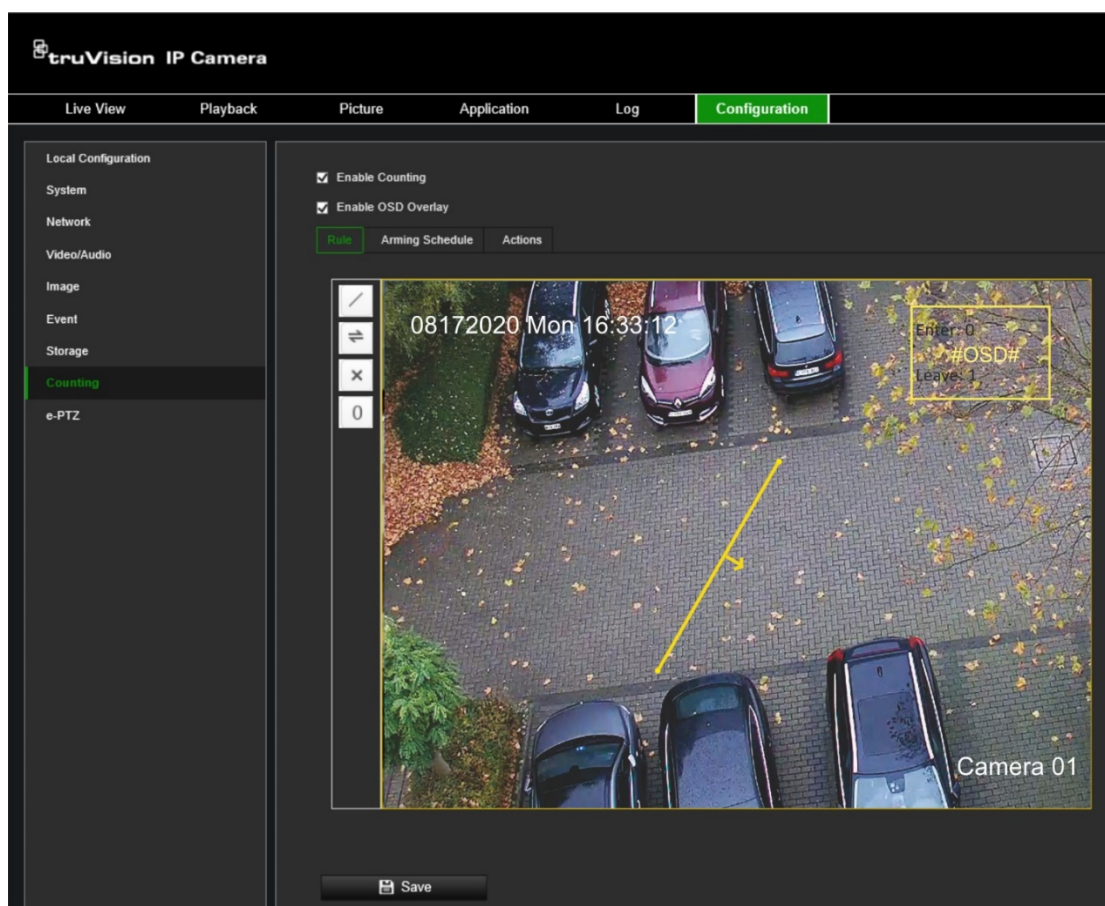
This function helps to calculate the number objects entering or exiting a configured area and is primarily used with entrances or exits

It is recommended that the camera is installed directly above the entrance or exit. It must be horizontally positioned for accuracy.

Important note: this function cannot distinguish between a moving person and a moving object. For accurate people counting we recommend using TruVision people counting cameras TVS-PC1 and TVS-PC2.

To count objects crossing a set line:

1. Click **Configuration > Counting**.



2. Select the **Enable Counting** check box to enable the counting feature.
3. Select the **Enable OSD Overlay** check box to show the “Enter” and “Leave” counting values in the camera OSD.
4. Click  and draw the detection line. If necessary, click  to change the direction of flow.



Detection line: Click this button to draw the detection line (yellow line). The object entering or exiting across the line will be detected and counted.

Note:

The detection line should be drawn directly below the camera and cover the whole entrance or exit.

Draw the detection line where fewer objects move back and forth.



Reverse flow: Click this button to change the entry/exit counting direction of the detection line or A/B regions.



Delete: Click this button to remove the detection line used for counting.



Reset: Click this button to reset the number of entry and exit values counted to zero.

5. Set up the arming schedule:

- Under the *Arming Schedule* tab, click the day you want to schedule. The Time pop-box appears. Enter the desired start and end times to detect motion.
- If you want to copy a day's schedule, move the mouse cursor to the end of the day. A pop-dialog box appears. Copy the schedule to other days or to the whole week. The Copy to pop-up window appears. Select the desired days to which to copy the schedule and click OK to save the changes.

6. Set up linking method when a counting event alarm occurs.

Under the *Actions* tab, select one or more response methods for the system when a motion detection alarm is triggered:

Normal Actions	This is a group selection. It automatically selects "Send Email", "Notify Alarm Recipient" and "Upload to FTP/NAS".
Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.

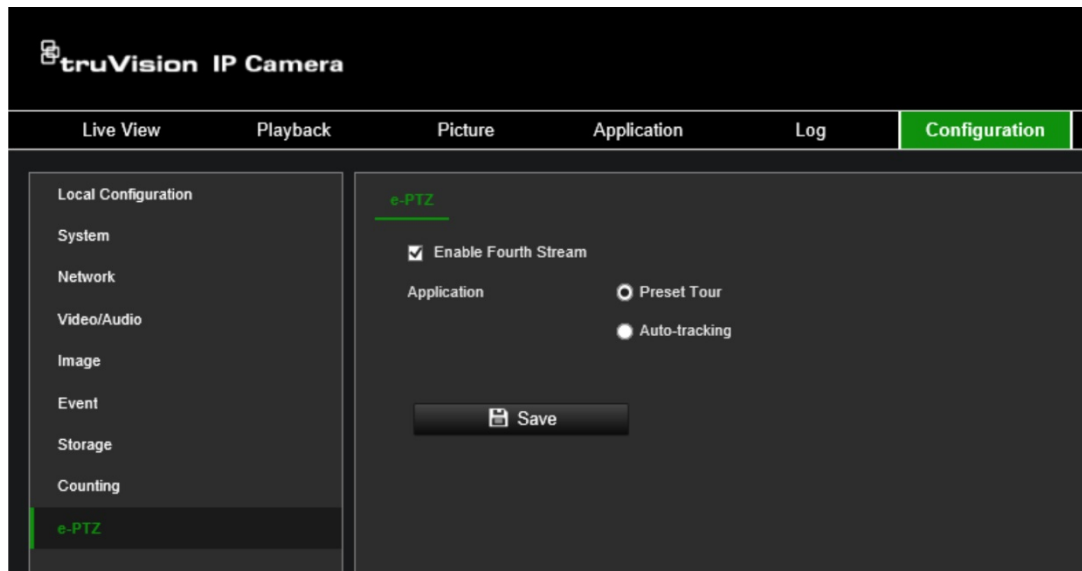
- Click **Save** to save changes.

e-PTZ

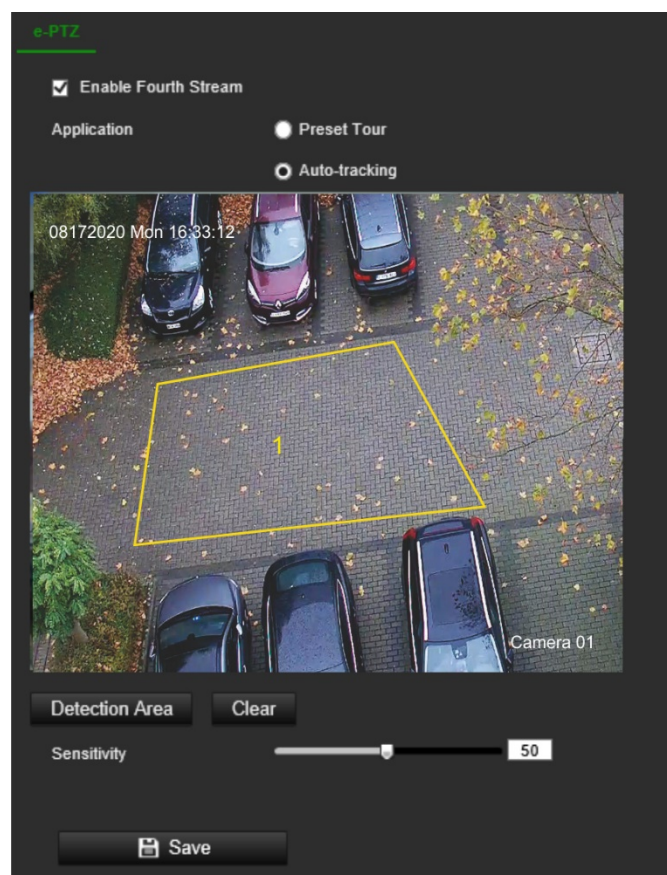
The e-PTZ (electronic pan, tilt and zoom) function is only supported via the fourth stream.

To set up e-PTZ:

- Click **Configuration > e-PTZ**.



2. Select **Enable Fourth Stream**.
3. Select **Preset Tour** or **Auto-tracking**.



Preset Tour: Lets you zoom in and out using the fourth stream in live view. Go to “PTZ and General control” on page 107 for further information on operating PTZ in live view.

Auto-tracking: The camera can detect and track a moving object in a scene.

- a) Click **Detection Area** to start drawing.
- b) Click four points on the live video image to mark the scene area for auto-tracking.

- c) Set sensitivity for the feature.

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

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

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

Example: if you set the value as 60, the target will be tracked only when 40 percent of the complete body enters the region.

- 4. Click **Save** to save the settings.
- 5. Go to Live View to switch the stream to the fourth stream.

Note: Auto-tracking does not allow PTZ control even if the fourth stream is enabled.

Camera management

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

Restore default settings

The administrator can reset the camera to the factory default settings. Network information such as IP address, subnet mask, gateway, MTU, NIC working mode, server port, and default route are not restored to factory default settings.

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. Click **Configuration > System > Maintenance**.
2. Click **Browse** to select the local configuration file and then click **Import** to start importing configuration file. Click **Device Parameters** and set the saving path to save the configuration file.

– Or –

Click **Export** to export the recorder's configuration settings into an external storage device.

Upgrade firmware

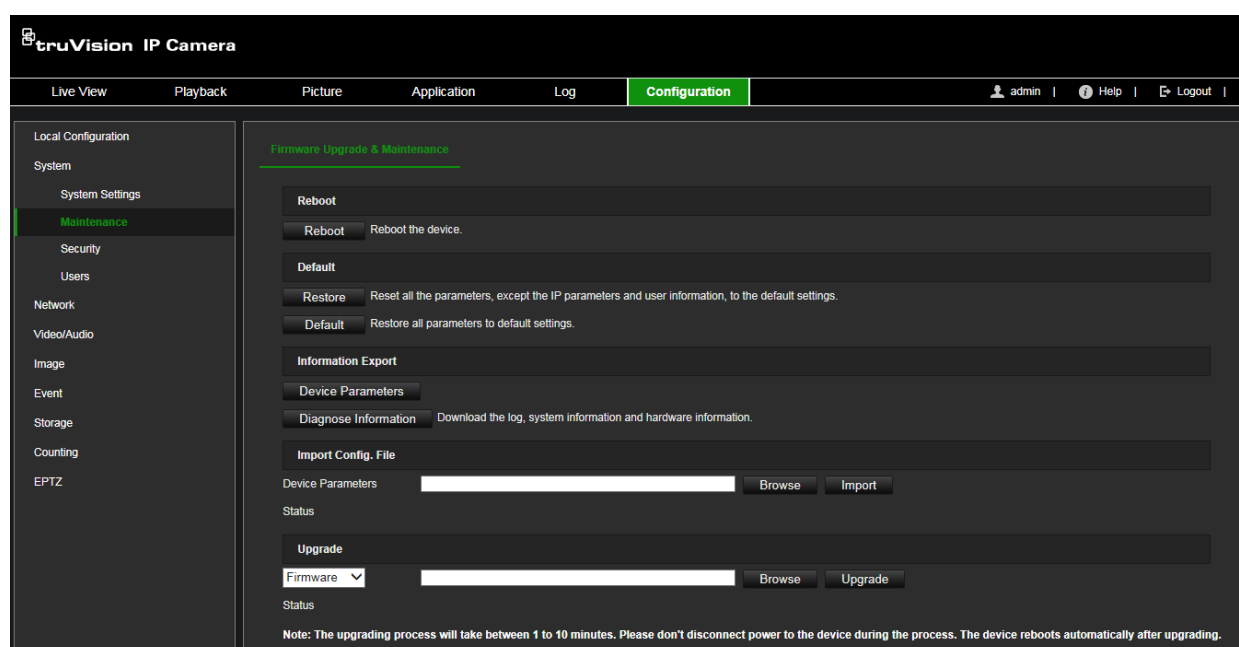
The camera firmware is stored in the flash memory. Use the upgrade function to write the firmware file into the flash memory.

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 the latest firmware on to your computer from our web site at:
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. Click **Configuration > System > Maintenance**. Under the section Firmware, 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 **Update**. 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.
 6. In most cases, it is recommended to perform a factory default after upgrading the firmware.

To upgrade the firmware via TruVision Device Manager:

1. In the **FW Upgrade** window of TruVision Device Manager select a device or hold the Ctrl or Shift key to select multiple devices for simultaneous upgrading.
2. Click the browse to locate the firmware file to use.

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

3. Click **Upgrade**.

Note: The upgrading process will be 1 to 10 minutes. Please do not disconnect power to the device during the process. The device reboots automatically after upgrading.

4. In most cases, it is recommended to perform a factory default after upgrading the firmware.

Reboot camera

It is easy to reboot the camera remotely.

To reboot the camera through the web browser:

1. Click **Configuration > System > Maintenance**.
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.

Logging 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 English, Chinese, Spanish, German, Russian, French, Portuguese, Polish, Turkish, Finnish, Italian and Dutch.

Figure 17: Logon window and language selection



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.

You can stop and start live view by clicking the Start/stop live view button  on the bottom of the window.

Record

You can record live video and store it in the directory that you have configured. In the live view window, click the **Record** button at the bottom of the window. To stop recording, click the button again.

Take a snapshot

You can take a snapshot of a scene when in live view. Simply click the **Capture** button located at the bottom of the window to save an image. The image is in JPEG format. Snapshots are saved on the hard drive.

Playing 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 18 below.

Figure 18: Playback window



Name	Description
1. Playback button	Click to open the Playback window.
2. Search calendar	Click the day required to search.
3. Search	Start search.
4. Control playback	Click to control how the selected file is played back: play, stop, slow and fast forward playback.
5. Archive functions	Click these buttons for the following archive actions:  Capture a snapshot image of the playback video.  Start/stop video clip during playback. Sections of a recording are saved to a local computer folder.
6. Digital zoom	Zoom in and out of the selected camera image.
7. Audio control	Modify the audio level.

Name	Description
8. Timeline	The timeline moves from left (oldest video) to right (newest video). It shows where you are in the playback recording. The current time and date are also displayed.
9. Timeline bar	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. 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. Click  to zoom out/in the timeline bar.
10. Download functions	 Download video files.
11. Recording type	The color code displays the recording type. Recording types are schedule recording, alarms recording and manual recording. The recording type name is also displayed in the current status window.
12. Zoom in/out	Click to zoom in or out of the timeline bar.
13. Jump start	Enter a precise time in the box and click  to jump start the playback from this selected time.

To play back recorded video

1. From the menu toolbar, click **Playback**.
2. Select the date and click the **Search** button. The searched video is displayed in the timeline.
3. 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 “Add and delete users” on page 30 to permit to play back recorded video files.

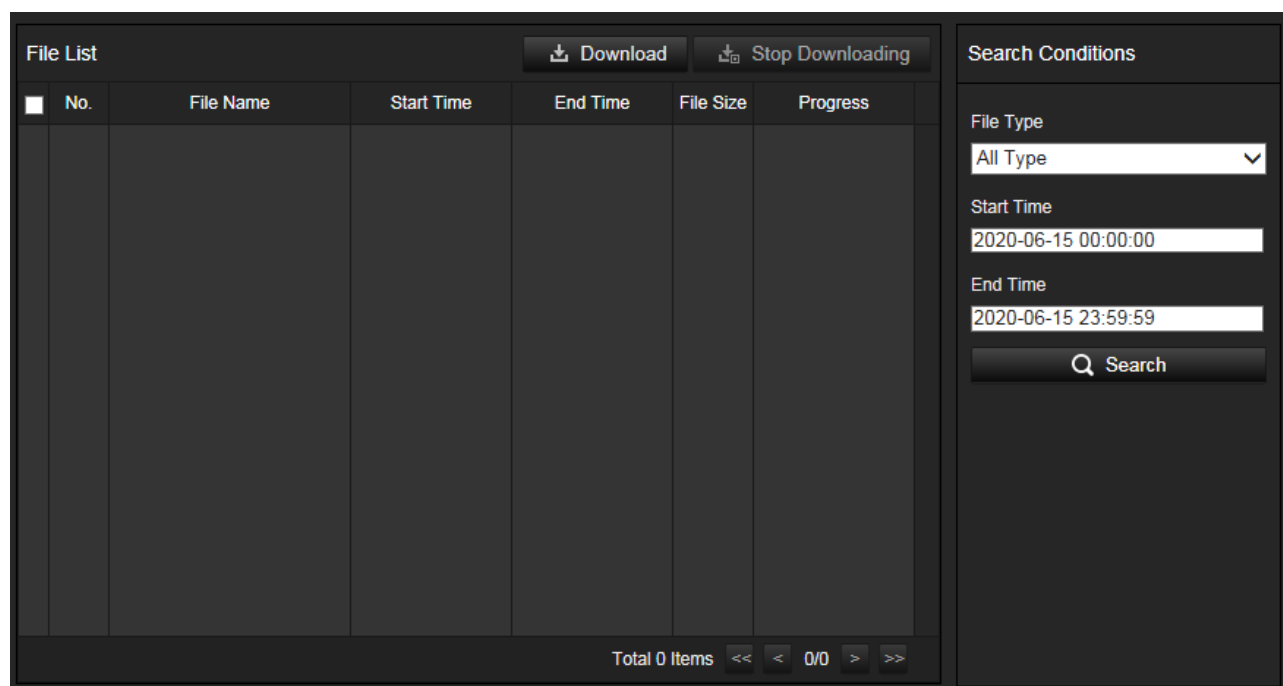
4. Select the date and click the **Search** button to search for the required recorded file.
5. Click **Search** to search the video file.
6. In the pop-up window, select the box of the video file and click  to download the video files.

To archive a recorded video segment during playback:

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

To archive recorded snapshots:

1. Click  to open the snapshots search window.



No.	File Name	Start Time	End Time	File Size	Progress
-----	-----------	------------	----------	-----------	----------

Search Conditions

File Type: All Type

Start Time: 2020-06-15 00:00:00

End Time: 2020-06-15 23:59:59

Search

Total 0 Items

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

Search snapshots

This function is only available with Internet Explorer.

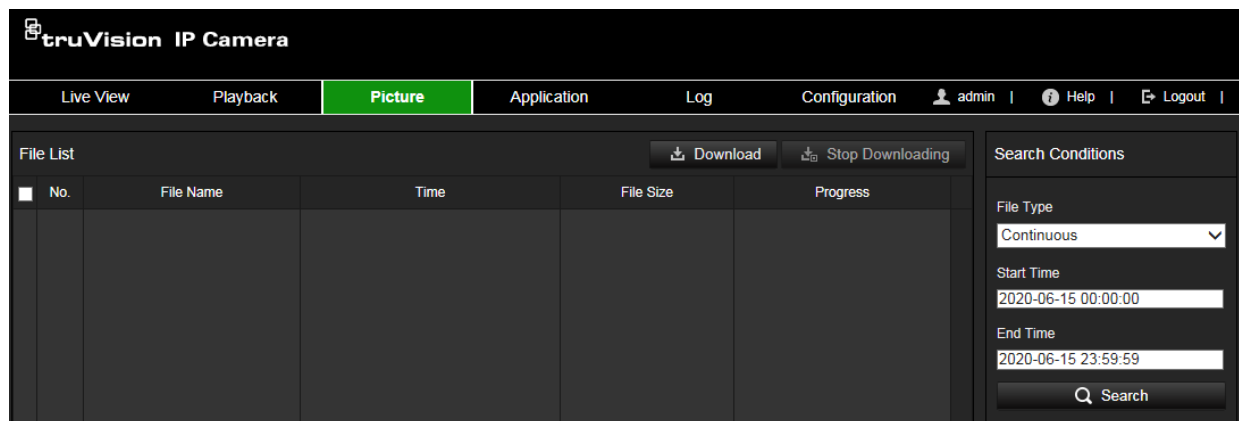
Click **Picture** on the menu toolbar to enter the window to search for snapshots. You can search, view, and download the pictures stored in the local storage, network or memory card storage.

Notes:

- Make sure the HDD, NAS or memory card are correctly configured before you process the snapshot search.
- Make sure the capture schedule is configured. Go to **Configuration > Storage > Schedule Settings > Snapshot** to set the capture schedule. See “Scheduled snapshots” on page 89.

To search recorded snapshots:

1. From the menu toolbar, click **Picture**.



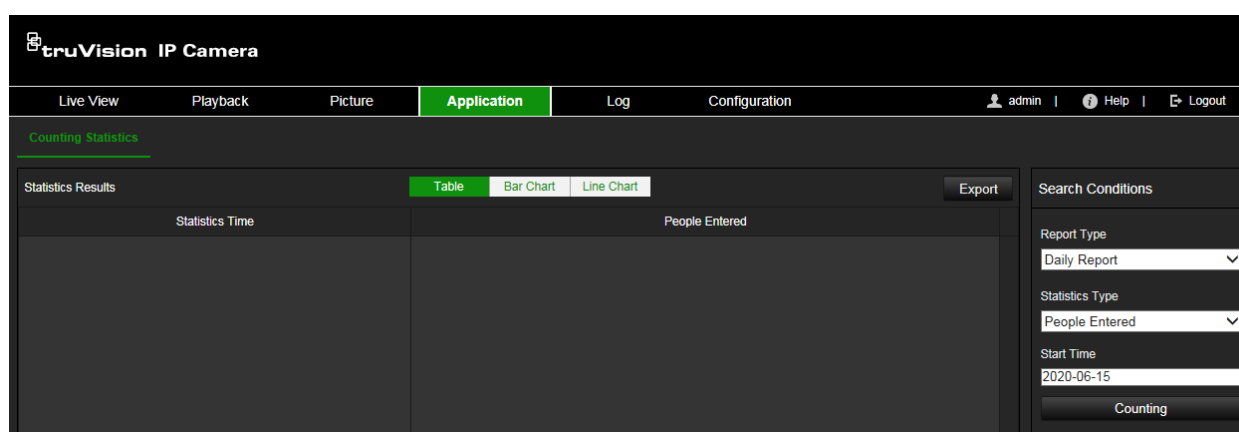
2. From the drop-down list, select the file type for which you want to search: Continuous, Motion, Alarm, Face Detection, Cross Line Detection and other supported VCA.
3. Select the start time and end time.
4. Click **Search** to search the matched files.
5. In the list of snapshots, select the check box of the desired files to download and click **Download**.

Search application statistics

You must configure NAS or insert a SD card in the camera to be able to use the Application functions. You can search, view, and download the counting data stored in local or network storage.

Steps:

1. From the menu toolbar, click **Application**.



2. Select a report type from the drop-down list: Daily report, weekly report, monthly report, and annual report. The daily report calculates the data on the date you selected. The weekly report calculates for the week. The monthly report calculates for the month. The annual report calculates for the year.
3. Select the **Statistics Type**: People Entered or People Exited.
4. Select the start time and click **Search**. The camera calculates according to the selected Report Type and Statistics Type.
5. Click **Table**, **Bar Chart** or Line Chart to display the counting statistics in according presentations.

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

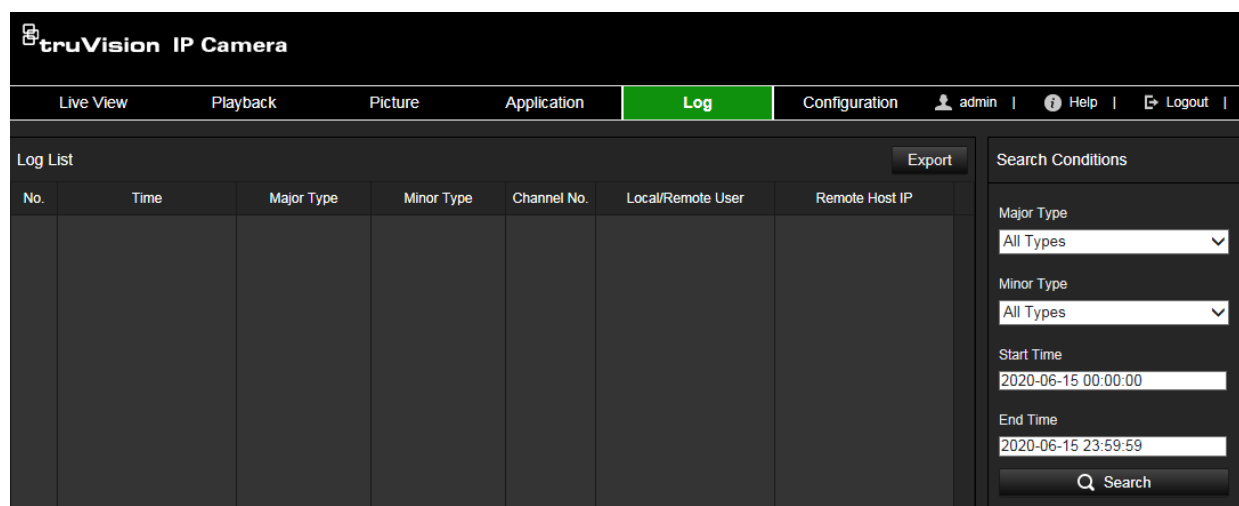
Search event logs

You must configure NAS or insert a SD card in the 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 viewing log access rights to search and view logs. See “Add and delete users” on page 30 to permit to search and view logs.

Figure 19: Log window



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. See Table 2 below for their descriptions.

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

Start Time and End 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**.
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.

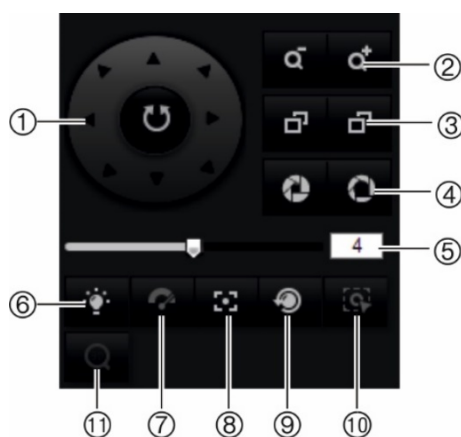
PTZ and General control panels

On the right-hand side of the live view page, you can click  or  to hide or show the PTZ and General control panels.

PTZ control panel

Some of the PTZ functions, such as pan/tilt, are not available because they are not supported by the camera hardware.

Figure 20: PTZ control panel



No.	Description
1.	Directional buttons: Controls the movements and directions of the PTZ. Center button is used to start auto-pan by the PTZ dome camera.
2.	Zoom in/out: Adjusts zoom.

No.	Description
3.	Focus +/-: Adjusts focus.
4.	Iris +/-: Adjusts iris.
5.	PTZ movement: Adjusts the speed of PTZ movement.
6.	Turns on/off the light. Not applicable for these cameras.
7.	Turns on/off camera wiper. Not applicable for these cameras.
8.	Auxiliary focus
9.	Initializes the lens
10.	Start manual tracking
11.	Enable/Disable 3D Zoom

Presets and preset tours:

- A preset is a preconfigured action for the camera that will run automatically after a defined dwell time.
- A preset tour is a memorized series of presets. The camera stays at a step for a set dwell time before moving on to the next step. The steps are defined by presets. A preset tour can be configured with up to 32 presets.

Figure 21: Preset panel

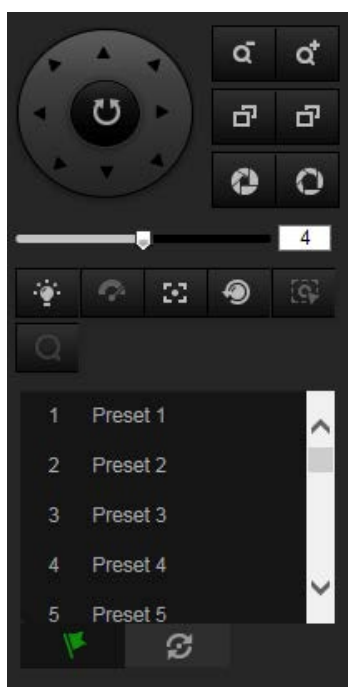
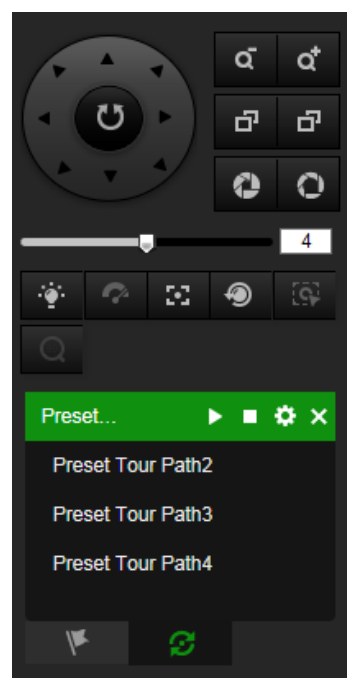


Figure 22: Preset Tour panel



To set a preset

1. Click the icon  to select the preset configuration interface.
2. Use the directional and zoom buttons on the PTZ control panel to move the camera to the desired position.
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 gray to black.

To call up a preset:

1. Click the icon  to select the preset configuration interface.
2. Select a desired preset number from the 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:

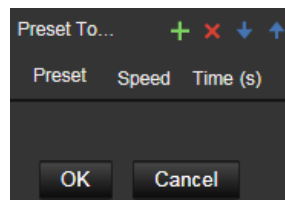
1. Select a desired preset number from the list.
2. Click the icon  to delete the selected preset.

The preset name turns from black to gray.

To set a preset tour:

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

1. Click the icon  to enter the tour configuration interface.



2. Select a preset tour path number from the drop-down list and click the icon  to configure the path.
3. Click  to add a preset into the path and click  to delete a preset.
4. Set the preset number, speed and lingering time at each preset. You can adjust the order of preset by using  and .
5. Click **OK** to save preset tour path.

Note: Up to 32 preset tour paths can be set. Each path can support up to 16 steps.

To call a preset tour:

1. Click the icon  to enter the preset tour configuration interface.
2. Select the preset tour path number from the drop-down list
3. Click the icon  to start the selected preset tour and icon  to stop it.

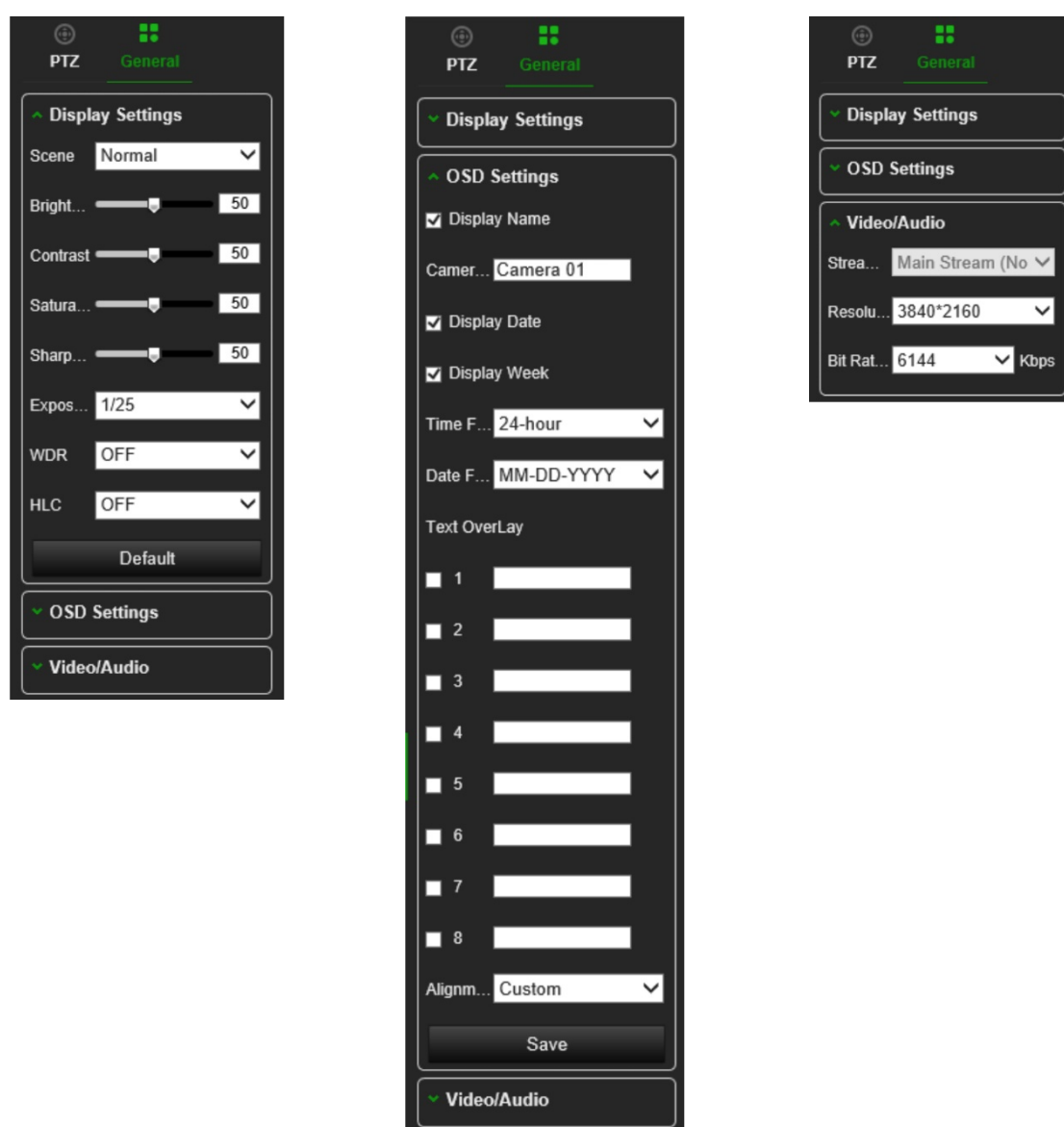
To delete a preset tour:

1. Select the preset tour path number from the drop-down list
2. Click the icon  to delete the preset tour path.

General control panel

Use the General tab to change the display, OSD and video/audio settings without having to go into the Configuration menu. Note that your camera user account must have the permissions to change settings

Figure 23: General control panel



The figure displays three screenshots of the General control panel interface, showing different sections of the configuration menu.

Left Screenshot: Display Settings

- Scene: Normal
- Bright...: 50
- Contrast: 50
- Satura...: 50
- Sharp...: 50
- Expos...: 1/25
- WDR: OFF
- HLC: OFF
- Default button

Middle Screenshot: OSD Settings

- Display Name: ☒
- Camera...: Camera 01
- Display Date: ☒
- Display Week: ☒
- Time F...: 24-hour
- Date F...: MM-DD-YYYY
- Text OverLay: 1, 2, 3, 4, 5, 6, 7, 8 (checkboxes and input fields)
- Alignm...: Custom
- Save button

Right Screenshot: Video/Audio Settings

- Strea...: Main Stream (No)
- Resolu...: 3840*2160
- Bit Rat...: 6144 Kbps

Index

8

802.1x parameters
set up, 44

A

Alarm inputs
set up, 68
Alarm outputs
set up, 68
Alarm types
motion detection, 60
Archive files, 103, 104
Archiving files
set up default directories, 11, 12
Audio parameters, 48

C

Camera image
set up, 53
Camera name
create, 14
display, 56
Configuration file
import/export, 98

D

Date format set up, 56
Day/Night switch, 53
DDNS parameters
set up, 34
Default settings
restore, 98
Detection
audio exception, 70
cross line, 78
defocus, 72
face, 74
intrusion, 76
object removal, 85
region entrance, 80
region exiting, 82
scene change, 73
unattended baggage, 83
Display info on stream
set up, 53
Display information
set up, 56
Dual VCA mode, 53

E

Email parameters

set up, 42
Events
search logs, 106
Exception alarm, 69

F

Firmware upgrade, 99
using TruVision Navigator, 100
FTP parameters
set up, 41

H

Hard drive
capacity, 91
formatting, 91
HTTP listening parameters
set up, 47
HTTPS parameters
set up, 43

I

Image parameters switch, 59
Integration protocol parameters
set up, 45

L

Language
change, 101
Live view mode
starting, 101
Log on and off, 101
Logs
information type, 28, 106
search, 106
security audit log, 27
viewing, 106

M

Motion detection
advanced mode, 63
normal mode, 62
Multicast parameters
set up, 38

N

NAS management, 93
NAT parameters
set up, 37
Network protocol
setup, 11, 12
Network service parameters
set up, 45

Network settings
 overview of local camera parameters, 11, 12
NTP synchronization, 14

O

Object counting, 94

P

Password activation, 7
Picture Overlay, 59
Playback
 play back recorded files, 103
 screen, 101
 searching recorded video, 101
Port parameters
 set up, 36
Post-recording times
 description, 87
PPPoE parameters
 set up, 36
Pre-recording times
 description, 87
Privacy masks, 58
PTZ control, 107
PTZ control panel, 10

Q

QoS parameters
 set up, 43

R

Reboot camera, 100
Recording
 manual recording, 101
 parameters, 48
 playback, 101
 recoding schedule, 86
 snapshots in live view mode, 101
Region of interest set up, 52
RS-485 setup, 16

S

SD card
 capacity, 91

SDHC card
 format, 91
Search
 application statistics, 105
 events, 106
 logs, 106
Security audit log, 27
Smooth streaming parameters
 set up, 46
Snapshots
 archive, 104
 event-triggered snapshots, 89
 saving during live view mode, 101
 scheduled snapshots, 89
SNMP parameters
 set up, 39
SRTP parameters
 set up, 48
Streaming
 main/sub setup, 11, 12
System time
 set up, 14

T

Tamper-proof alarms
 set up, 66
TCP/IP parameters
 set up, 33
Time format set up, 56
TruVision Navigator
 upgrade firmware, 100

V

Video clips
 archive, 103
Video parameters, 48
Video quality, 53

W

Web browser
 Chrome, Safari, Firefox, 5
 overview of the interface, 9
Web browser security level
 check, 6