



TruVision S-series Thermal Camera Configuration Manual

Copyright	© 2022 Carrier. All rights reserved. Specifications subject to change without prior notice. This document may not be copied in whole or in part or otherwise reproduced without prior written consent from Carrier, except where specifically permitted under US and international copyright law.
Trademarks and patents	TruVision and associated names and logos are a product brand of Aritech, a part of Carrier. Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.
Manufacturer	PLACED ON THE MARKET BY: Carrier Fire & Security Americas Corporation Inc. 13995 Pasteur Blvd, Palm Beach Gardens, FL 33418, USA AUTHORIZED EU REPRESENTATIVE: Carrier Fire & Security B.V. Kelvinstraat 7, 6003 DH Weert, Netherlands
Certification	    
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.
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.
Canada	This Class A digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.
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.
European Union 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 <https://firesecurityproducts.com/policy/product-warning/> or scan the following code:

Contact information

EMEA: <https://firesecurityproducts.com>

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

Product documentation

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



Content

Important information 3

Limitation of liability 3

Product warnings 3

Warranty disclaimers 4

Intended use 5

Advisory messages 5

Introduction 6

Product overview 6

Contact information and manuals/firmware 6

Access via a web browser 7

Internet Explorer – Checking the browser security level 7

Activating the camera 8

Using non-Internet Explorer web browsers (plugin-free browser) 10

Overview of the camera web browser 11

Local configuration 12

Network setup 14

TCP/IP 14

DDNS 15

PPPoE 17

Port 17

Port mapping 18

Multicast 19

SNMP 20

FTP 22

Email 23

HTTPS 24

QoS 25

802.1x 25

Integration protocol 26

Network service 27

HTTP listening 28

SRTP 29

System setup 30

System settings 30

Maintenance 32

Security 34

User Management 36

Video and audio setup 40

Video settings 40

Audio settings 41
Display info on stream 42
ROI encoding of an image 42

Image setup 44

Display settings 44
OSD Settings (On Screen Display) 49
Privacy masks 50
Picture overlay 51
Defective pixel correction 52
VCA rule display 53

Event setup 54

Alarm inputs and outputs 54
Exception 56
Flashing alarm LED output 57
Audible alarm output 59
Audio exception detection 60

Storage setup 62

Record settings 62
Capture (Scheduled snapshots) 64
Storage management 66

VCA setup 70

Basic settings 70
Camera calibration 71
Shield region 73
Rule 74
Advanced calibration 77

Temperature measurement setup 80

Automatic thermal imaging 80
Manual thermal imaging 89

Camera operation 90

Login and Logout 90
Live view 90
Playing back recorded video 93
Snapshot 96
Log 96

Index 98

Important information

Limitation of liability

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

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

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

Product warnings

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

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

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

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

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

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

DO NOT CONNECT TO A RECEPTACLE CONTROLLED BY A SWITCH.

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

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

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

Warranty disclaimers

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

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

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

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

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

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

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

Intended use

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

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

Advisory messages

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

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

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

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

Introduction

Product overview

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

- TVTH-S01-0001-BUL-G (IP Thermal Bullet Camera, 256×192 bi-spectral, 3 mm)
- TVTH-S01-0002-BUL-G (IP Thermal Bullet Camera, 256×192 bi-spectral, 7 mm)
- TVTH-S01-0003-BUL-G (IP Thermal Bullet Camera, 256×192 bi-spectral, 10 mm)
- TVTH-S01-0004-BUL-G (IP Thermal Bullet Camera, 384×288, 15 mm)

- TVTH-S01-0001-TUR-G (IP Thermal Turret Camera, 256×192 bi-spectral, 2 mm)
- TVTH-S01-0002-TUR-G (IP Thermal Turret Camera, 256×192 bi-spectral, 3 mm)
- TVTH-S01-0003-TUR-G (IP Thermal Turret Camera, 256×192 bi-spectral, 7 mm)

You can download the software and the following manuals from our web site:

- TruVision S-series Thermal Bullet Camera Installation Guide
- TruVision S-series Thermal Turret Camera Installation Guide
- TruVision S-series Thermal Camera Configuration Manual

Contact information and manuals/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:	firesecurityproducts.com.au

Access via a web browser

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

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

Internet Explorer – Checking the 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 ActiveX 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 Internet Explorer

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 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.

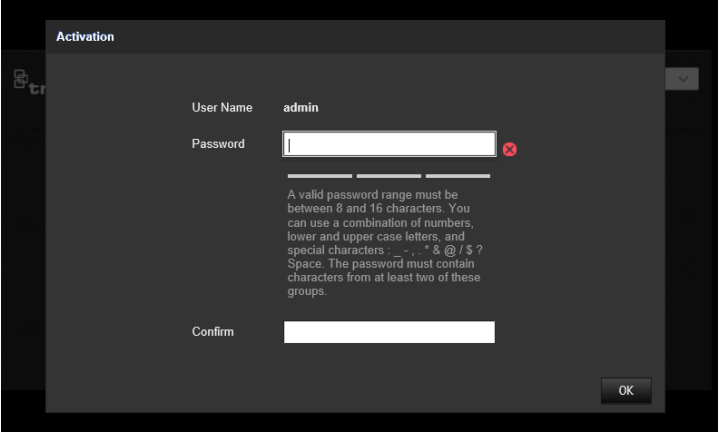
Activating the camera

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 to find the IP address of the camera.

Activating the camera via a 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 meet the following conditions:

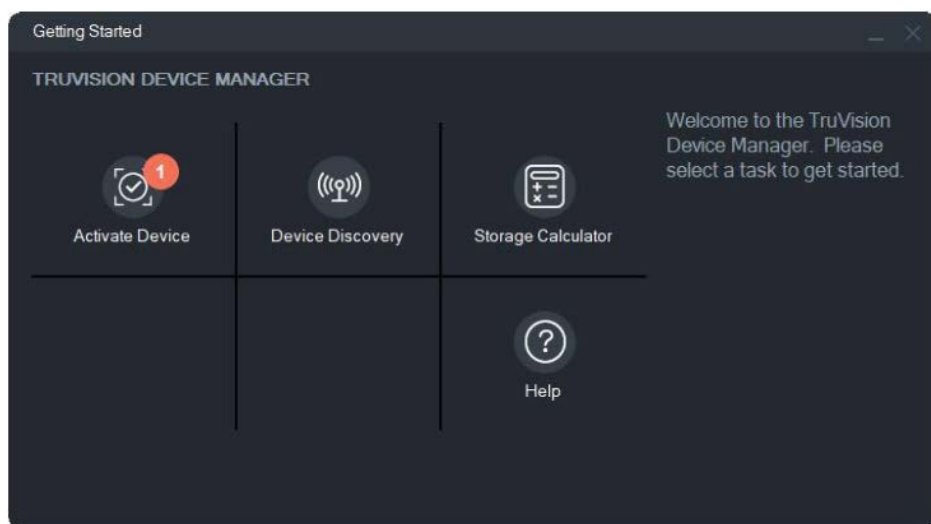
- Between 8 and 16 characters
- At least 1 lower case letter
- At least 1 upper case letter
- At least 1 of following special characters: _ - , . * & @ / \$? Space.

We also recommend that you do not use a space at the start or end of a password, and 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.

Activating the camera via TruVision Device Manager:

1. Run *TruVision Device Manager 9.1* or newer to search for TruVision cameras on your local network.
2. After launching Device Manager, the number of inactive TruVision devices (unconfigured devices recently connected to the network) can be displayed by clicking the Activate Device button. From there you can select the cameras you want to activate.



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

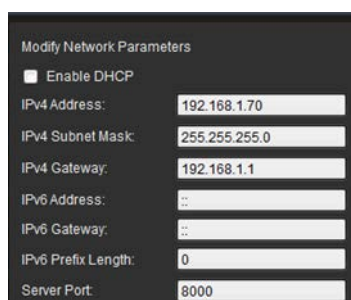
Note: A valid password range must meet the following conditions:

- Between 8 and 16 characters
- At least 1 lower-case letter
- At least 1 upper-case letter
- At least 1 of following special characters : _ - , . * & @ / \$? Space.
- The password is case-sensitive.

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. Change the device IP address, subnet mask and gateway or check the box “Enable DHCP” if you want the camera to automatically receive IP settings from the DHCP server on the network.
5. Click **Apply** to save the password and the new network settings.

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

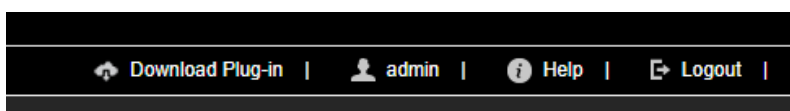


Modify Network Parameters	
☐ Enable DHCP	
IPv4 Address:	192.168.1.70
IPv4 Subnet Mask:	255.255.255.0
IPv4 Gateway:	192.168.1.1
IPv6 Address:	::
IPv6 Gateway:	::
IPv6 Prefix Length:	0
Server Port:	8000

Using non-Internet Explorer web browsers (plugin-free browser)

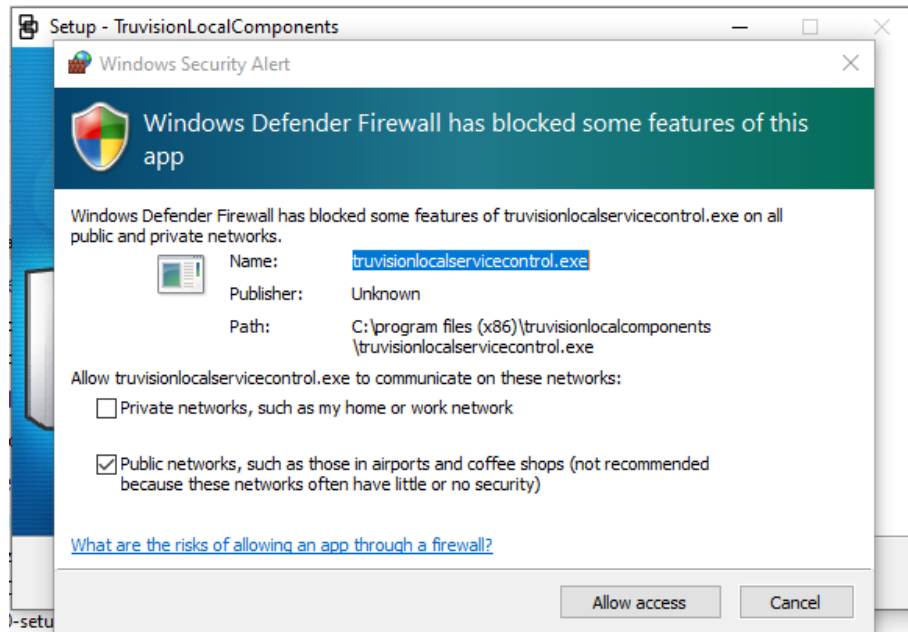
Plugin-free browsers such as Google Chrome, Mozilla Firefox, Microsoft Edge, and Apple Safari have limitations compared to Internet Explorer that uses ActiveX plugins. To solve this, an additional plugin can be download from the camera live view web page. Please note that an internet connection is needed to download this plugin.

After activating the camera, you will be redirected to the camera Live View page where you might see a pop-up to download a plugin. In case the plugin has not downloaded automatically, click the “Download Plug-in” icon at the top right of the camera Live View web page to download the plugin installation file to your PC.

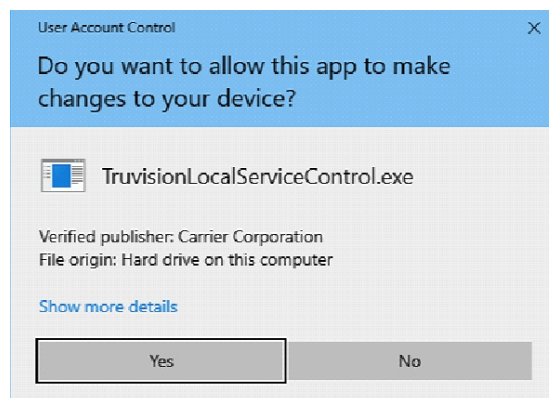


Close the browser and install the downloaded plugin *TruVisionLocalComponents.exe* on your PC. Once the plugin is installed, you can reopen the browser to view and configure the camera.

During installation of the plugin, Windows Defender may show a pop-up message which you should accept by clicking the “Allow access” button.



Note that this application will start automatically when starting Windows. Depending on your Windows configuration you might see below pop-up message after logging on to Windows. Accept the message to enable the plugin for plugin-free browsers.



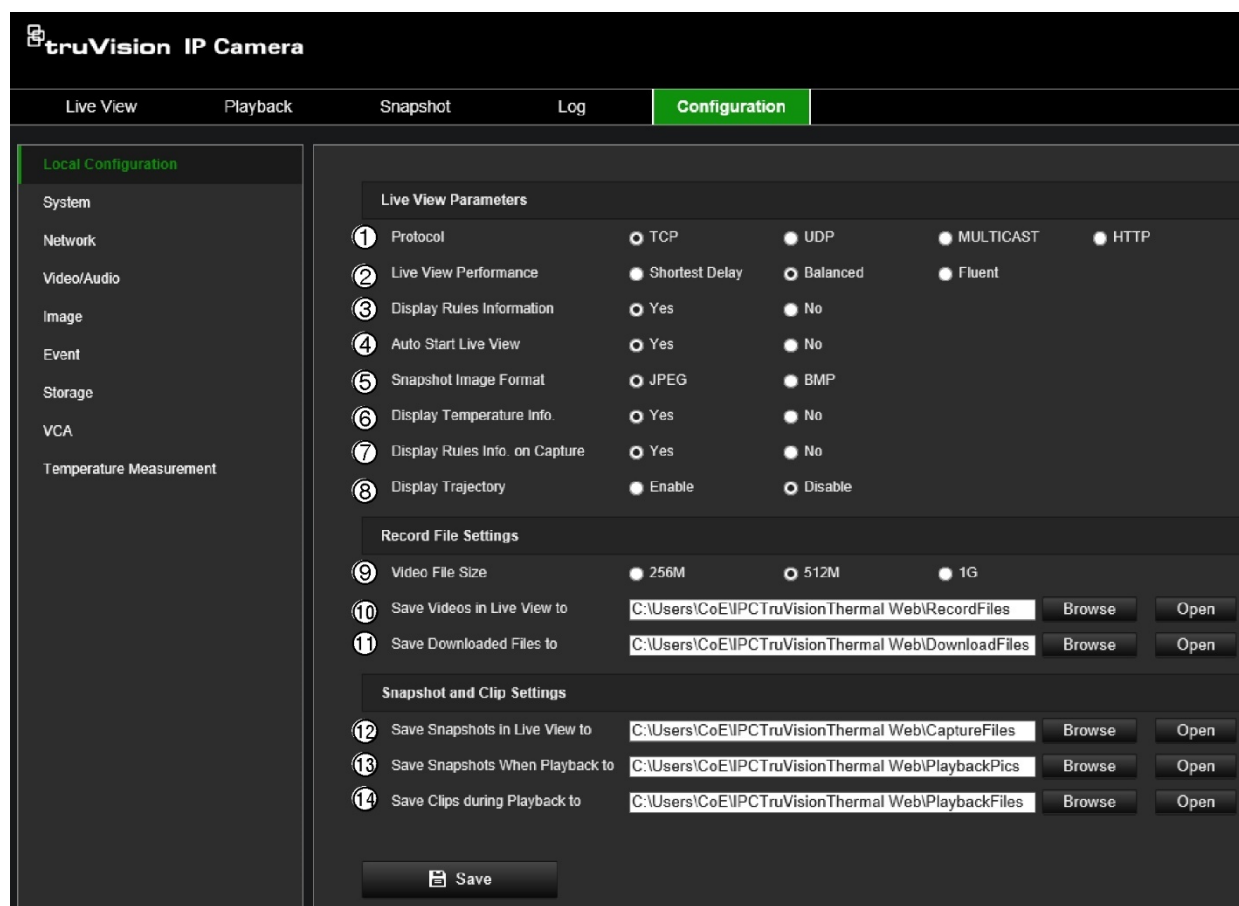
Overview of the camera web browser

The camera web browser lets you view, record, and play back recorded videos as well as manage the camera from any PC with Internet access. The browser's easy-to-use controls give you quick access to all camera functions. See Figure 11 on page 91.

Local configuration

Use the Local Configuration menu to manage the protocol type, live view performance and local storage paths for snapshots, downloads, and camera browser recording. In the Configuration panel, click **Local Configuration** to display the local configuration window. See Figure 1 below for descriptions of the different menu parameters.

Figure 1: Example of the Local configuration window



Parameters	Description
Live View Parameters	
1. Protocol	Specify the network protocol used. Options include TCP, UDP, MULTICAST and HTTP.
2. Live View Performance	Specify the transmission speed. Options include: Shortest Delay, Balanced, or Fluent.
3. Display Rules Information	Enable to display rules information in live view.
4. Auto Start Live View	When enabled, live view starts automatically. This option requires a stable network environment and a high-performance monitoring device.
5. Snapshot Image Format	Select the image format of snapshots: JPEG or BMP.
6. Display Temperature Info.	Enable to display the temperature information in live view.
7. Display Rules Info on Capture	Enable to display rules information in captured files.

Parameters		Description
8.	Display Trajectory	Enable to display the target's moving path in live view.
Record File Settings		
9.	Video File Size	Specify the maximum file size. Options include: 256 MB, 512 MB and 1GB.
10.	Save Videos in Live View to	Specify the directory for recorded files.
11.	Save Downloaded Files to	Specify the directory for downloaded files.
Snapshot and Clip Settings		
12.	Save Snapshots in Live View To	Specify the directory for saving snapshots in live view mode.
13.	Save Snapshots when Playback To	Specify the directory for saving snapshots in playback mode.
14.	Save Clips during Playback to	Specify the directory for saving video clips in playback mode.

Network setup

You need to define the network settings to be able to access the camera through a network. Use the “Network” menu to define the network settings.

Caution: We strongly recommend that you use a strong password for all functions and network devices to protect your privacy and to protect your system against security risks. A valid password range must be at least eight characters. You can use a combination of numbers, lower- and upper-case letters, and special characters. The installer and/or end user are responsible for password management.

TCP/IP

You can set up the following TCP/IP parameters:

Figure 2: TCP/IP parameters

truVision IP Camera

Live View

Playback

Snapshot

Log

Configuration

Local Configuration

System

Network

Basic Settings

Advanced Settings

Video/Audio

Image

Event

Storage

VCA

Temperature Measurement

TCP/IP

DDNS

PPPoE

Port

NAT

Multicast

NIC Type

Auto

☐ DHCP

IPv4 Address

10.61.61.61

Test

IPv4 Subnet Mask

255.0.0.0

IPv4 Default Gateway

10.0.0.1

IPv6 Mode

Route Advertisement

View Route Advertisement

IPv6 Address

IPv6 Subnet Mask

IPv6 Default Gateway

::

MAC Address

9c:f6:1a:91:25:7e

MTU

1500

☒ Enable Multicast Discovery

DNS Server

Preferred DNS Server

8.8.8.8

Alternate DNS Server

Host Name Configuration

Enable dynamic

☐ Enable

Register DNS name

Save

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.
Host Name Configuration	Enable hostname configuration and define a hostname in case you want to use a name instead of an IP address to connect to the camera

To set up the TCP/IP parameters:

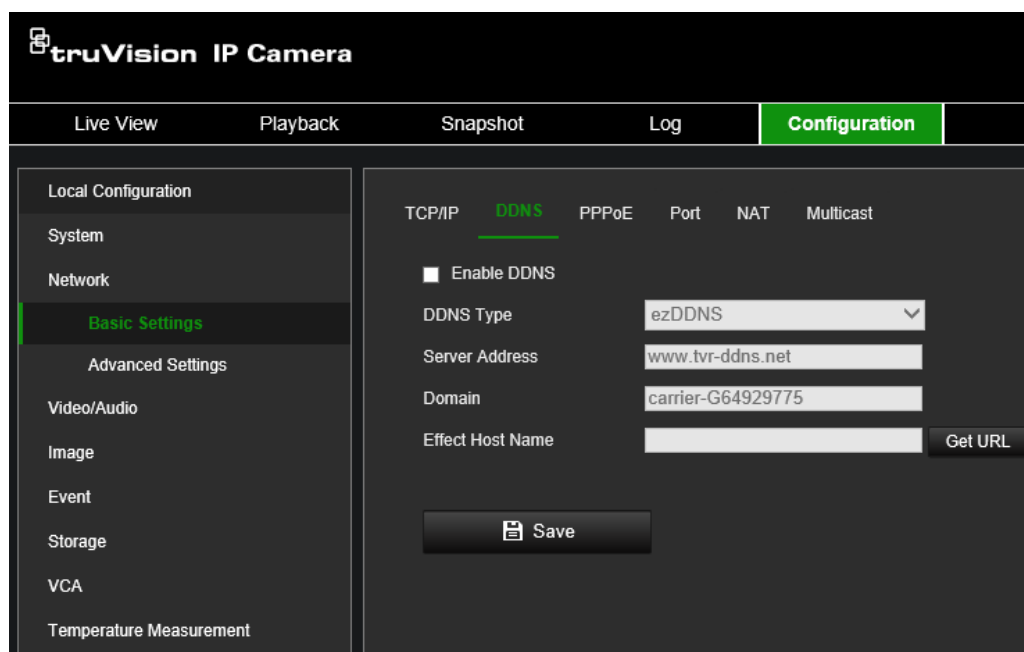
1. Click **Configuration > Network > Basic Settings > TCP/IP**.
2. Configure the NIC settings, including the NIC Type, IPv4 settings, IPv6 settings and MTU settings.
3. If the DHCP server is available, select **DHCP**.
4. If the DNS server settings are required for some applications (e.g., sending email), you should configure the **Preferred DNS Server or Alternate DNS Server**.
5. Assign a hostname to the camera to be used to identify it over the network. Select "Enable dynamic" and enter your DNS name for the system. The DNS name must be unique and can contain letters, numbers, and hyphens
6. Click **Save** to save changes.
7. Reboot the device for the changes to take effect.

DDNS

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**



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.

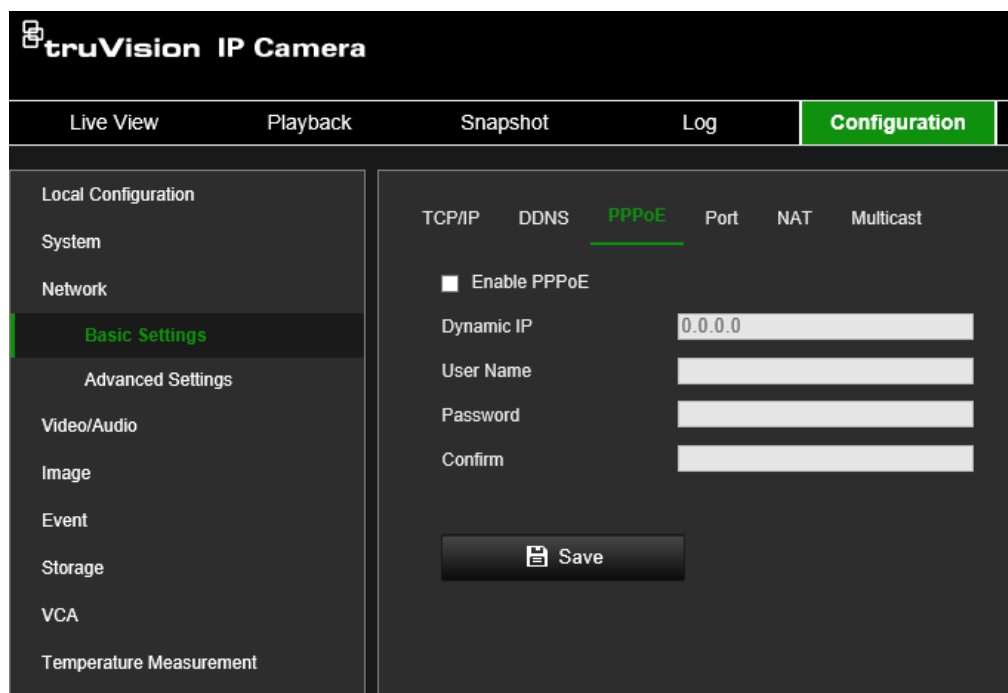
4. Click **Save** to save changes.
5. Reboot the device for the changes to take effect.

PPPoE

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

You can set up several ports:

HTTP Port: The default port number is 80, and it can be changed to any port number that is not occupied.

RTSP Port: The default port is 554 and it can be changed to any port number 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 number that is not occupied.

Server Port: The default server port is 8000, and it can be changed to any port number from 2000 to 65535.

Enhanced SDK Service Port: The default server port is 8433, and it can be changed to any port number from 2000 to 65535.

WebSocket Port: Used for live view on non-IE browsers. The default port is 7681. It can be changed to any port number ranges from 1 to 65535.

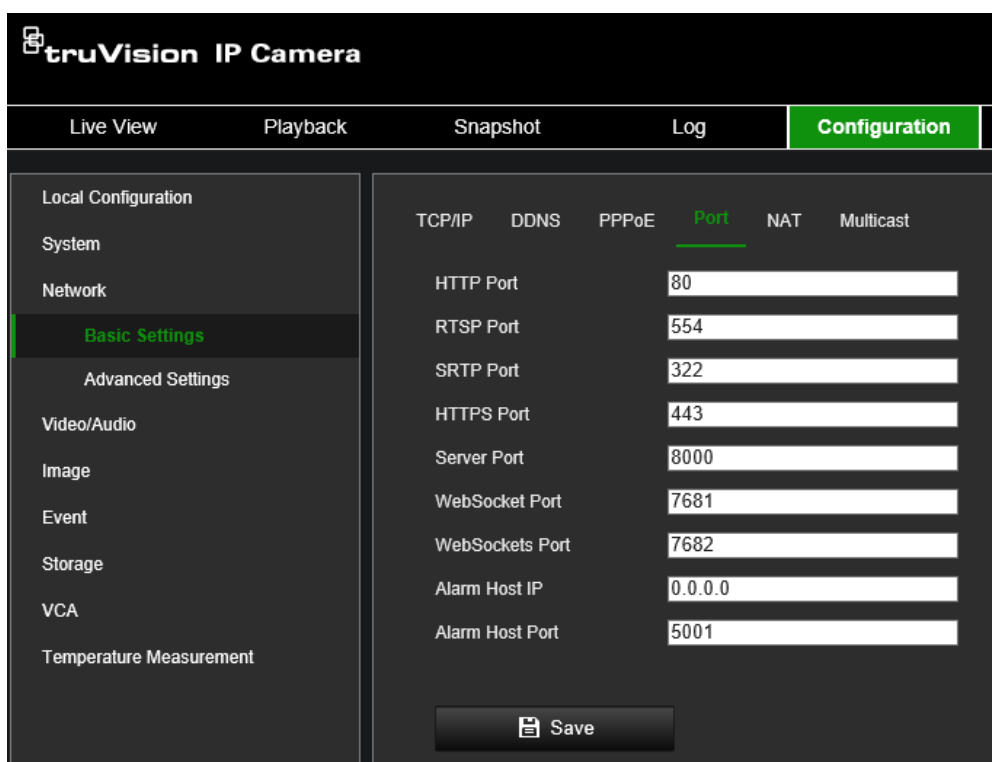
WebSockets Port: Used for live view on IE browsers. The default server port is 7682. It can be changed to any port number from 1 to 65535.

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**.



The screenshot shows the 'truVision IP Camera' configuration interface. The top navigation bar includes 'Live View', 'Playback', 'Snapshot', 'Log', and 'Configuration' (highlighted in green). The left sidebar lists 'Local Configuration' with sub-items: 'System', 'Network', 'Basic Settings' (highlighted in green), 'Advanced Settings', 'Video/Audio', 'Image', 'Event', 'Storage', 'VCA', and 'Temperature Measurement'. The main content area is titled 'Port' and contains a table of port settings:

TCP/IP	DDNS	PPPoE	Port	NAT	Multicast
HTTP Port			80		
RTSP Port			554		
SRTP Port			322		
HTTPS Port			443		
Server Port			8000		
WebSocket Port			7681		
WebSockets Port			7682		
Alarm Host IP			0.0.0.0		
Alarm Host Port			5001		

At the bottom of the configuration area is a 'Save' button.

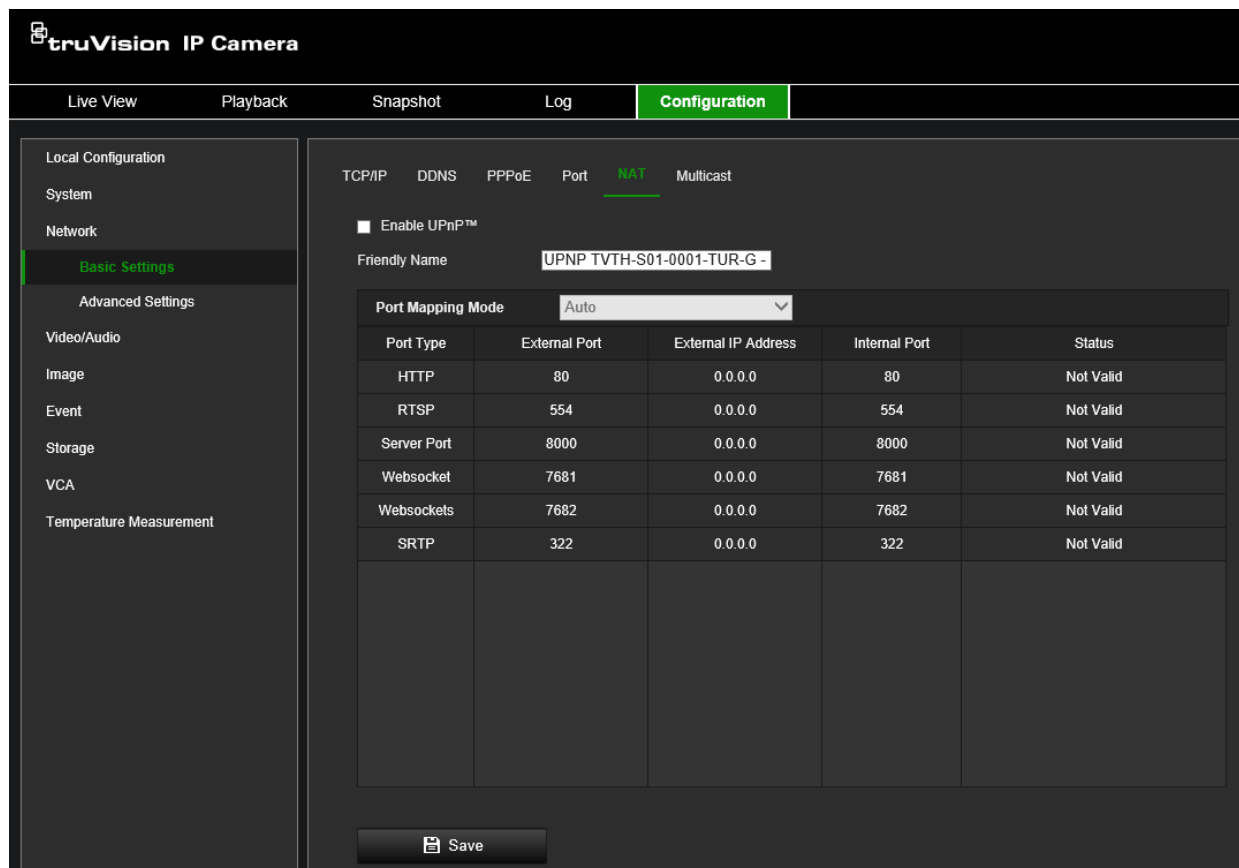
2. Set the HTTP port, RTSP port, HTTPS port and Server port of the camera.
3. Enter the IP address and port if you want to upload the alarm information to the remote alarm host. Also select the **Notify Alarm Recipient** option in the normal Linkage of each event page.
4. Click **Save** to save changes.
5. Reboot the device for the changes to take effect.

Port mapping

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**.



2. Select the **Enable UPnP™** 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

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

To set up the Multicast parameters:

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

The screenshot shows the 'truVision IP Camera' configuration web interface. At the top, there are tabs for 'Live View', 'Playback', 'Snapshot', 'Log', and 'Configuration'. The 'Configuration' tab is active. On the left side, there is a sidebar menu with options: 'Local Configuration', 'System', 'Network', 'Basic Settings' (highlighted in green), 'Advanced Settings', 'Video/Audio', 'Image', 'Event', 'Storage', 'VCA', and 'Temperature Measurement'. The main content area is titled 'Multicast' and contains the following settings:

TCP/IP	DDNS	PPPoE	Port	NAT	Multicast
Channel No.	Camera 01				
IP Address	239.0.0.1				
Stream Type	Main Stream				
Video Port	8860				
Audio Port	8862				
SRTP					
Video Port	18860				
Audio Port	18862				

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

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.

SNMP

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 displays the configuration interface for a truVision IP Camera. The top navigation bar includes 'Live View', 'Playback', 'Snapshot', 'Log', and 'Configuration' (highlighted in green). The left sidebar lists 'Local Configuration' with sub-items: 'System', 'Network', 'Basic Settings', 'Advanced Settings' (highlighted in green), 'Video/Audio', 'Image', 'Event', 'Storage', 'VCA', and 'Temperature Measurement'. The main content area is titled 'SNMP' and contains three sections: 'SNMP v1/v2', 'SNMP v3', and 'SNMP Other Settings'. The 'SNMP v1/v2' section has checkboxes for 'Enable SNMPv1' and 'Enable SNMPv2c', both of which are unchecked. Below these are input fields for 'Read SNMP Community' (public), 'Write SNMP Community' (private), 'Trap Address', 'Trap Port' (162), and 'Trap Community' (public). The 'SNMP v3' section has a checkbox for 'Enable SNMPv3' which is unchecked. It includes input fields for 'Read UserName', 'Security Level' (no auth, no priv), 'Authentication Algorithm' (MD5 selected, SHA unselected), 'Authentication Password', 'Private-key Algorithm' (DES selected, AES unselected), 'Private-key password', 'Write User Name', 'Security Level' (no auth, no priv), 'Authentication Algorithm' (MD5 selected, SHA unselected), 'Authentication Password', 'Private-key Algorithm' (DES selected, AES unselected), and 'Private-key password'. The 'SNMP Other Settings' section has an input field for 'SNMP Port' (161). A 'Save' button is located at the bottom right of the configuration area.

SNMP v1/v2	
☐ Enable SNMPv1	
☐ Enable SNMP v2c	
Read SNMP Community	public
Write SNMP Community	private
Trap Address	
Trap Port	162
Trap Community	public

SNMP v3	
☐ Enable SNMPv3	
Read UserName	
Security Level	no auth, no priv
Authentication Algorithm	☒ MD5 ☐ SHA
Authentication Password	
Private-key Algorithm	☒ DES ☐ AES
Private-key password	
Write User Name	
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.

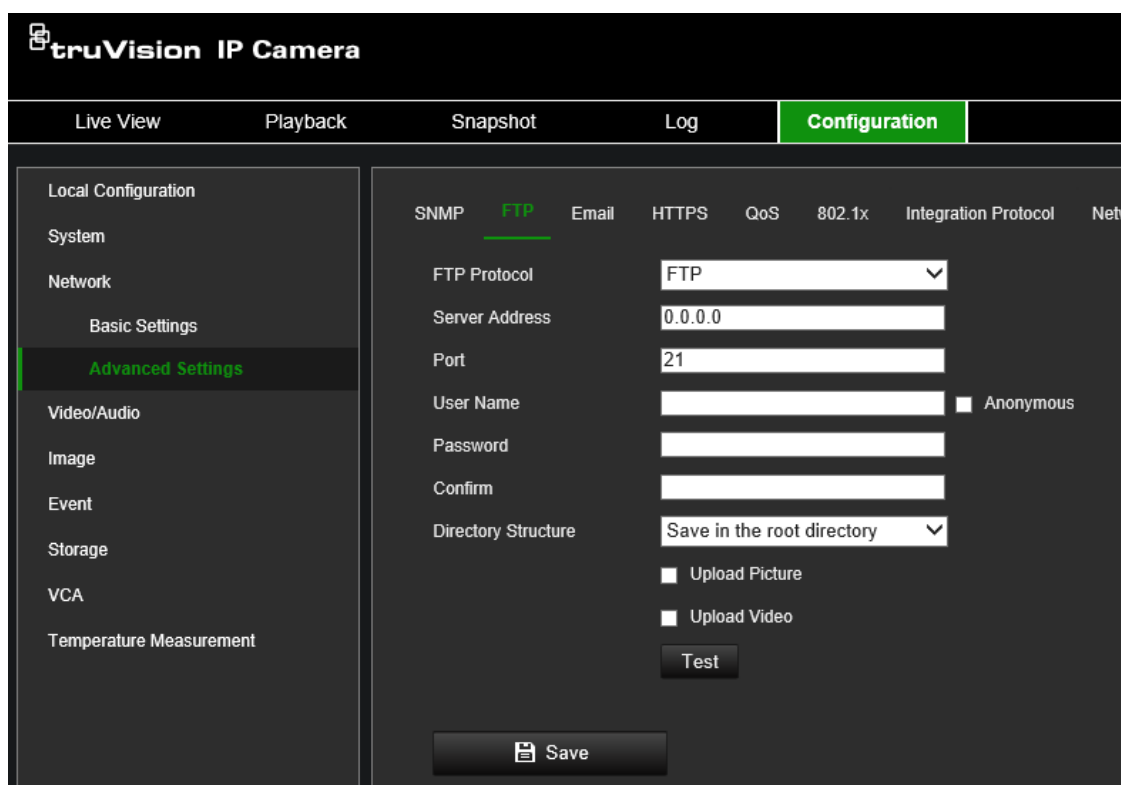
Note: Before setting the SNMP, please download the SNMP software to receive the camera information via the SNMP port. By setting the Trap Address, the camera can send the alarm event and exception messages to the surveillance center. The SNMP version you select should be the same as that of the SNMP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

FTP

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**.



The screenshot displays the configuration interface for a TruVision IP Camera. The top navigation bar includes 'Live View', 'Playback', 'Snapshot', 'Log', and 'Configuration' (highlighted in green). The left sidebar lists 'Local Configuration' categories: 'System', 'Network', 'Basic Settings', 'Advanced Settings' (highlighted in green), 'Video/Audio', 'Image', 'Event', 'Storage', 'VCA', and 'Temperature Measurement'. The main content area shows the 'FTP' settings under the 'Network' tab. Fields include 'FTP Protocol' (set to FTP), 'Server Address' (0.0.0.0), 'Port' (21), 'User Name' (empty), 'Password' (empty), 'Confirm' (empty), and 'Directory Structure' (set to 'Save in the root directory'). There are checkboxes for 'Anonymous', 'Upload Picture', and 'Upload Video'. A 'Test' button is located below the checkboxes, and a 'Save' button is at the bottom.

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

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**.

The screenshot shows the configuration interface for a truVision IP Camera. The top navigation bar includes 'Live View', 'Playback', 'Snapshot', 'Log', and 'Configuration' (highlighted in green). The left sidebar lists 'Local Configuration' with sub-items: 'System', 'Network', 'Basic Settings', 'Advanced Settings' (highlighted in green), 'Video/Audio', 'Image', 'Event', 'Storage', 'VCA', and 'Temperature Measurement'. The main content area is titled 'Email' and contains the following settings:

- Sender**: Text input field.
- Sender's Address**: Text input field.
- SMTP Server**: Text input field.
- SMTP Port**: Text input field with '25' entered.
- Email Encryption**: Dropdown menu with 'None' selected.
- Attached Image**: Check box (unchecked).
- Interval**: Dropdown menu with '2' selected, followed by 's'.
- Authentication**: Check box (unchecked).
- User Name**: Text input field.
- Password**: Text input field.
- Confirm**: Text input field.

Below these settings is the 'Alarm Email Attachment Settings' section:

- Alarm Type**: Dropdown menu with 'VCA Behavior Analysis' selected.
- Attachment Type**: Dropdown menu with 'Image' selected.
- Optical Capture**: Dropdown menu with '1' selected.
- Thermal Capture**: Dropdown menu with '1' selected.

At the bottom is the 'Receiver' section, which is a table with 3 columns: 'No.', 'Receiver', and 'Receiver's Address'.

No.	Receiver	Receiver's Address
1		
2		
3		

At the bottom of the interface are two buttons: 'Test' and 'Save'.

2. Configure the following settings:

Sender: The name of the email sender.

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

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

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

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

Attached Image: Select this check box if you want to send emails with attached alarm snapshots.

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.

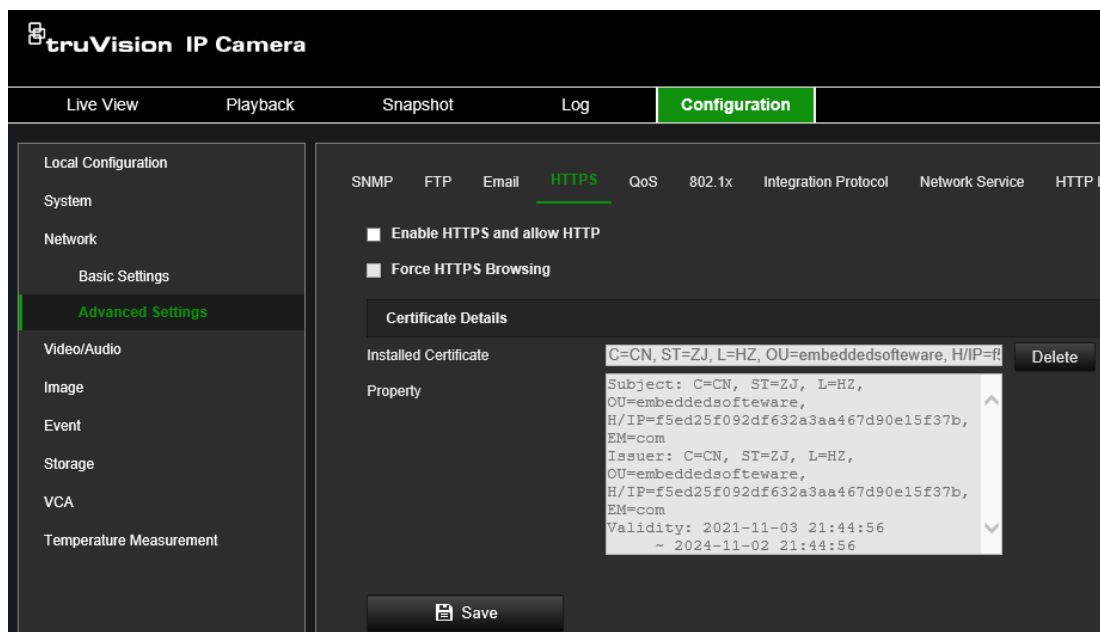
4. Click **Save** to save changes.

HTTPS

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. Select **Enable HTTPS and allow FTP** to allow connections using HTTPS or HTTP.
3. Select **Force HTTPS Browsing** forces to use HTTPS instead of HTTP.



HTTPS certificates can be managed from this page

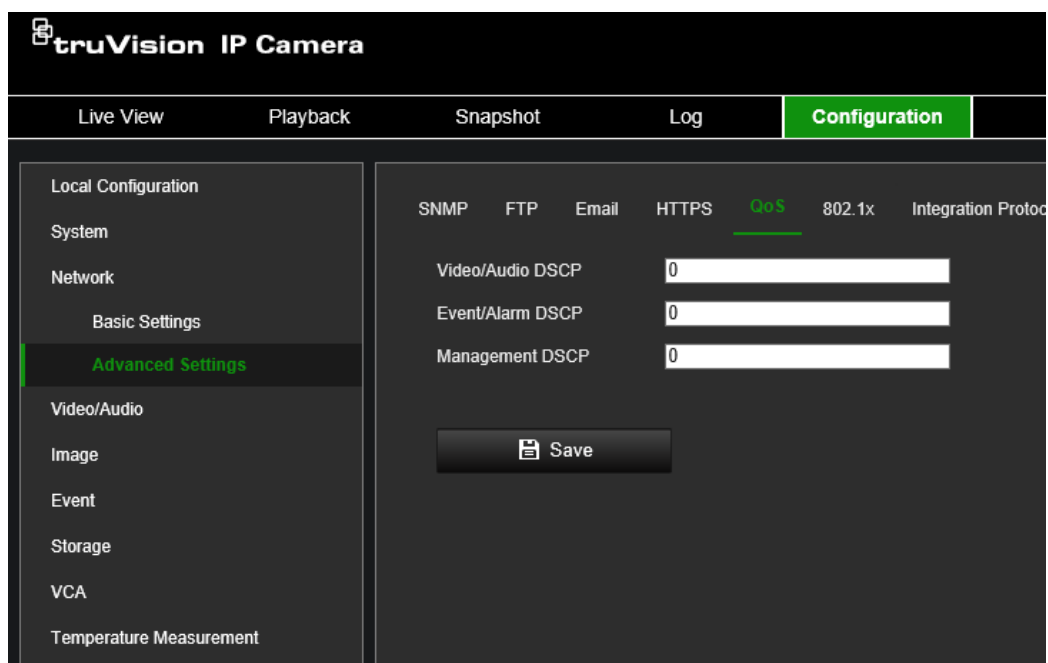
QoS

QoS (Quality of Service) can help solve the network delay and network congestion by configuring the priority of data sending.

Enable the option 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**.



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

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 TruVision IP Camera configuration web interface. The top navigation bar includes 'Live View', 'Playback', 'Snapshot', 'Log', and 'Configuration' (highlighted in green). The left sidebar lists 'Local Configuration' with sub-items: 'System', 'Network', 'Video/Audio', 'Image', 'Event', 'Storage', 'VCA', and 'Temperature Measurement'. Under 'Network', 'Basic Settings' and 'Advanced Settings' (highlighted in green) are visible. The main content area is titled '802.1x' and contains the following settings:

- ☐ Enable IEEE 802.1X
- Protocol: EAP-TLS (dropdown)
- Identify: (text input)
- Private Key Password: (password input)
- EAPOL Version: 1 (dropdown)
- CA Certificate: (text input) with 'Browse' and 'Upload' buttons
- User Certificate: (text input) with 'Browse' and 'Upload' buttons
- Private Key: (text input) with 'Browse' and 'Upload' buttons
- Save button at the bottom.

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.

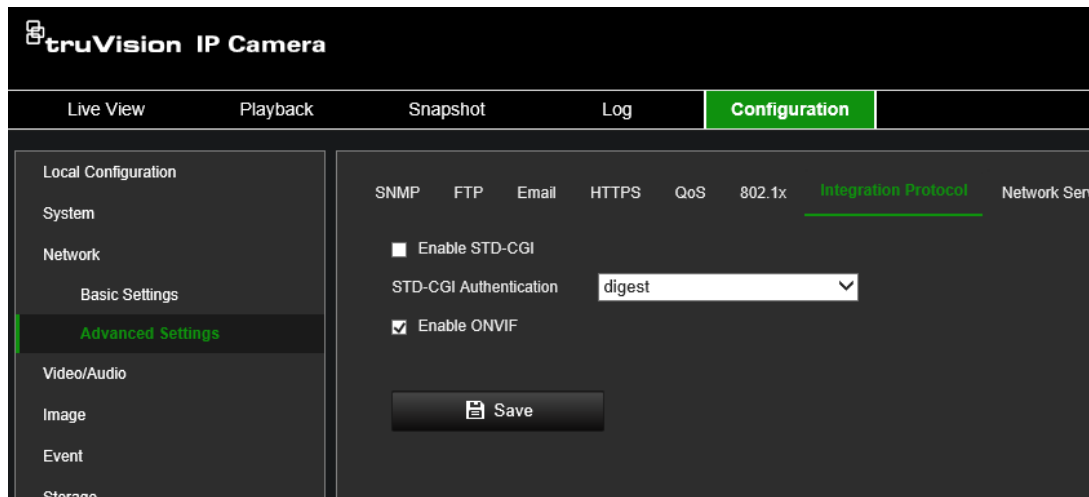
Note: The switch or router to which the camera is connected must also support the IEEE 802.1X standard. A server must also be configured. Please apply and register a user name and password for 802.1X in the server.

Integration protocol

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.

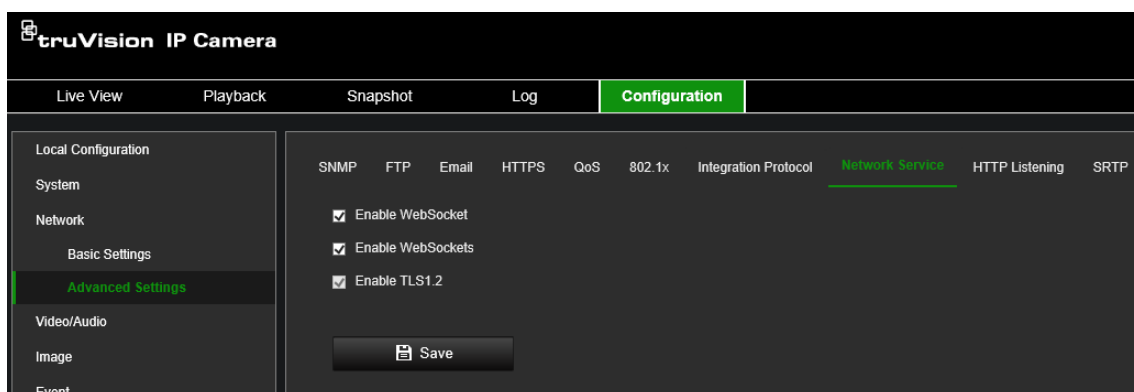
Network service

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**.



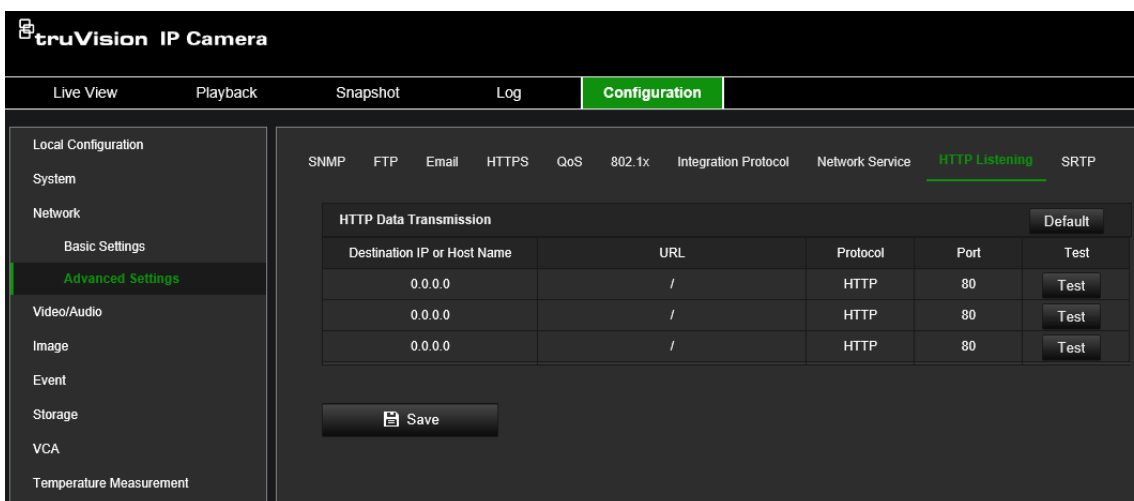
2. Select the **Enable WebSocket** check box to enable WebSocket service for live viewing over HTTP protocol without the plug-in.
3. Select the **Enable WebSockets** check box to enable WebSockets service for live viewing over HTTPS protocol without the plug-in.
4. Select the **Enable SDK Service** check 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. TLS1.2 is enabled by default and cannot be changed as HTTPS protocols rely on it.
7. Click **Save** to save changes.

HTTP listening

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 Listening**.



2. Enter the 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.

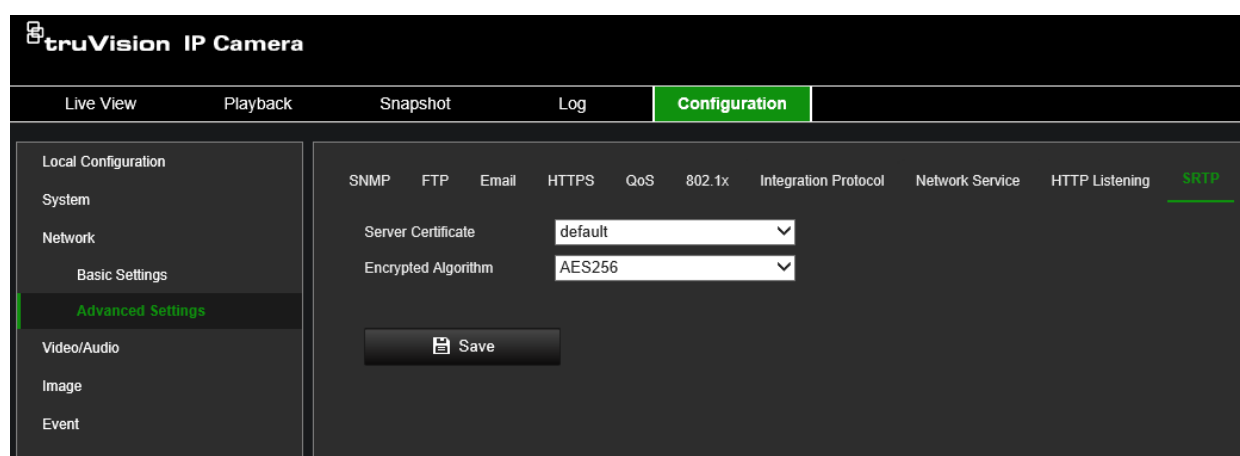
4. Enable ANR to activate Automatic Network Replenishment to have the camera send buffered events to the alarm host after restoring from a network disconnect.
5. Click **Save** to save changes.

SRTP

The Secure Real-time Transport Protocol (SRTP) is a profile for Real-time Transport Protocol (RTP) to provide encryption, message authentication and integrity. It also replays attack protection to the RTP data in both unicast and multicast applications.

To set up the SRTP parameters:

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



2. Select the server certificate type: No certificate or Default.
3. Select the desired encrypted algorithm.
4. Click **Save** to save changes.

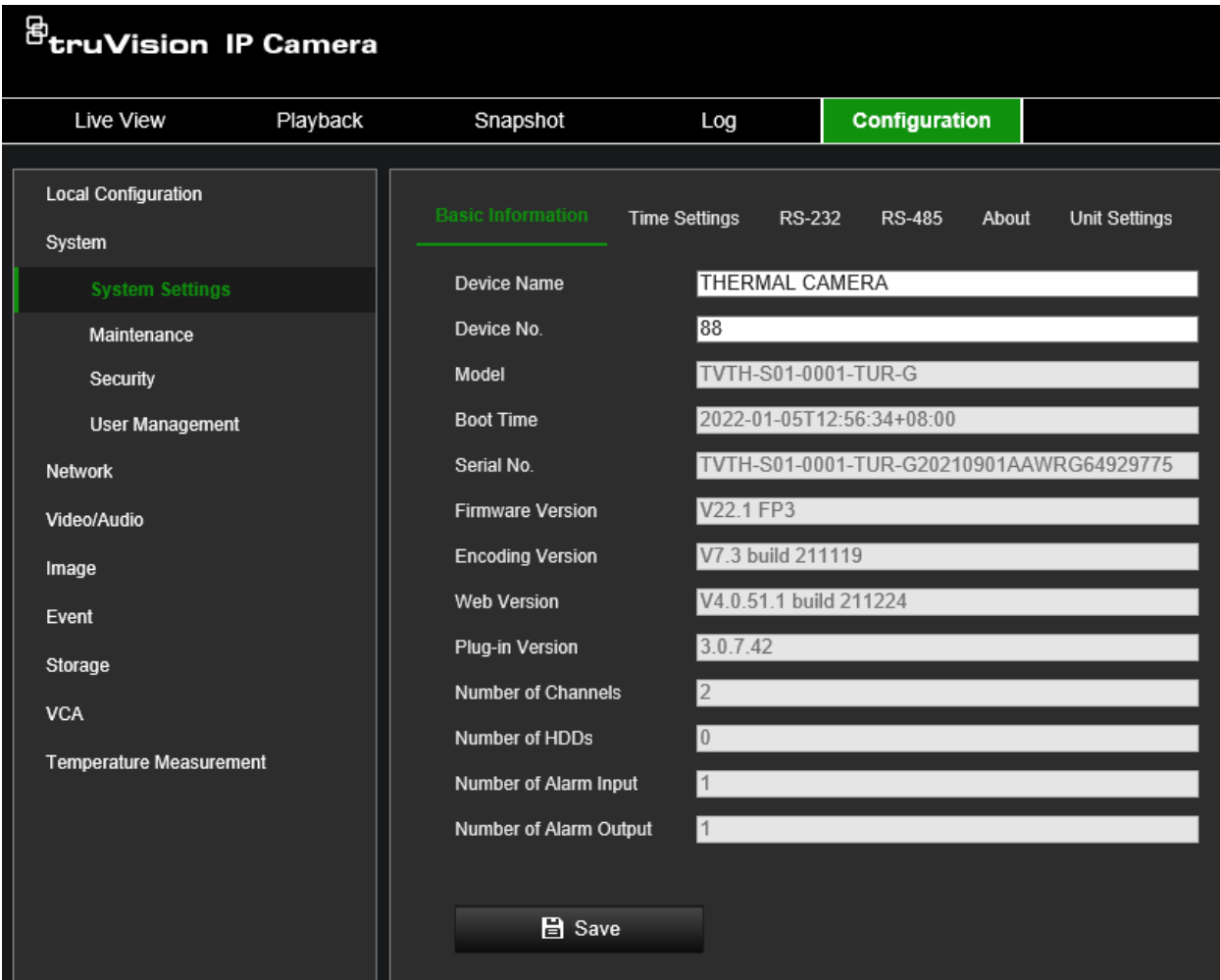
System setup

Use this menu to manage system settings, perform maintenance related tasks, and configure security and user related features.

System settings

System settings include an overview of system settings, date, and time, RS-232 and RS-485 parameters, as well as the measurement to be used by the camera.

Figure 3: System Settings window: Basic menu shown



Basic Information

Displays hardware and firmware related information of the camera.

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. From the menu toolbar, click **Configuration > System > System Settings > Time Settings**.

The screenshot displays the 'truVision IP Camera' configuration web interface. The top navigation bar includes 'Live View', 'Playback', 'Snapshot', 'Log', and 'Configuration' (highlighted in green). The left sidebar lists 'Local Configuration' with sub-items: 'System' (highlighted), 'Maintenance', 'Security', 'User Management', 'Network', 'Video/Audio', 'Image', 'Event', 'Storage', 'VCA', and 'Temperature Measurement'. The main content area is titled 'Time Settings' and includes tabs for 'Basic Information', 'Time Settings' (active), 'RS-232', 'RS-485', 'About', and 'Unit Settings'. Under 'Time Settings', there is a 'Time Zone' dropdown menu set to '(GMT+08:00) Beijing, Urumqi, Singapore, Perth'. Below this is the 'NTP' section with a radio button selected for 'NTP'. It includes input fields for 'Server Address' (time.windows.com), 'NTP Port' (123), and 'Interval' (1440 minute(s)), with a 'Test' button. The 'Manual Time Sync.' section has a radio button selected for 'Manual Time Sync.', showing 'Device Time' (2022-01-07T11:44:42) and 'Set Time' (2022-01-07T11:40:34) with a calendar icon and a checkbox for 'Sync. with computer time'. The 'Daylight Savings Time' section has a checkbox for 'Enable DST' which is unchecked. It includes dropdowns for 'Start Time' (Mar, Last, Sun, 02), 'End Time' (Oct, Last, Sun, 02), and 'DST Bias' (60minute(s)). A 'Save' button is at the bottom.

2. From the **Time Zone** drop-down list, select the time zone that is the closest to the camera's location.
3. To synchronize time and date using the NTP server, select **NTP** to enable this function. Enter the server address, which is the NTP server IP address, the NTP port and interval. The time interval can be set from 1 to 1440 minutes.

— or —

To synchronize time and date manually, select **Manual Time Sync** to enable this function. Select **Sync with computer time** to instantly synchronize the time of the camera with the time of your computer.

4. Select **Enable DST** to enable the DST (Daylight Savings Time) function and set the dates of the DST period.
5. Click **Save** to save changes.

RS-232

RS-232 is used by Technical Support or to access a peripheral device.

RS-485

RS-485 is used to connect the camera to an external device. You need to configure these parameters before you connect any devices.

About

Displays the list of Open-Source Software Licenses used by the camera.

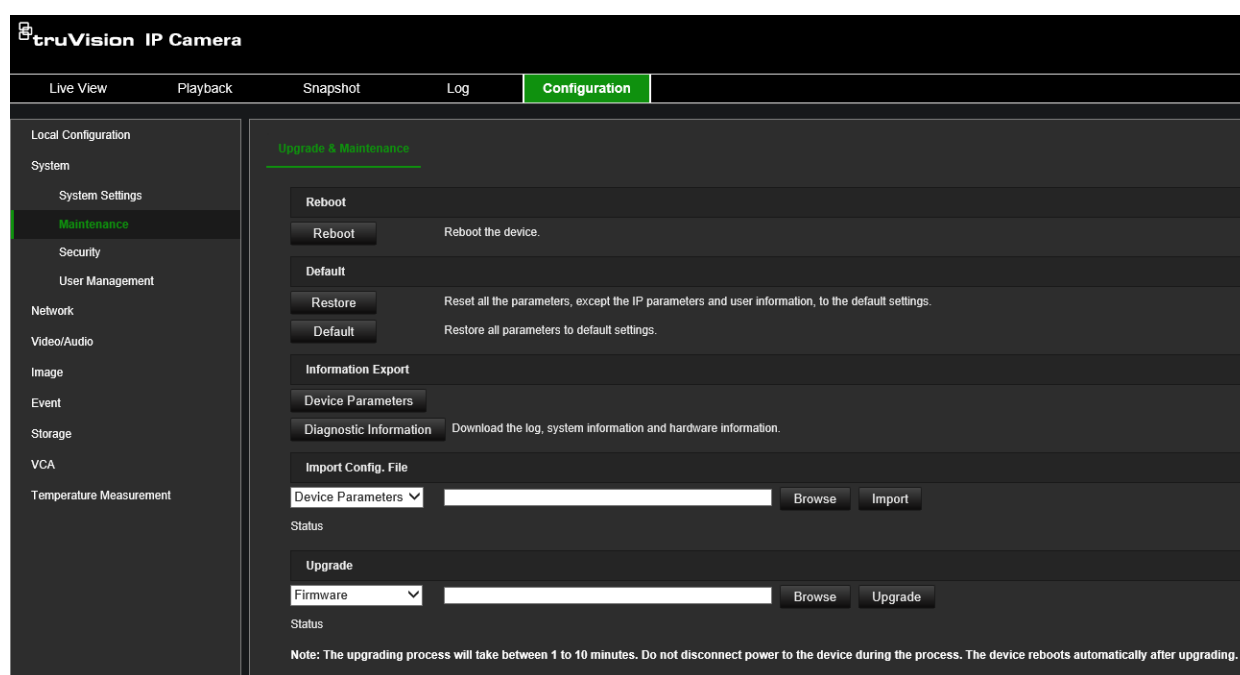
Unit settings

Set the measurement system to be used by the camera. Select the temperature and distance units to be used.

Maintenance

Maintenance tasks like importing/exporting configurations and firmware upgrade can be managed in this menu.

Figure 4: System Maintenance window



Reboot camera

Click **Reboot** to restart the camera.

Restore default settings

Click the **Restore** or **Default** button to restore default settings to the camera. There are two options available:

- **Restore:** Restore all the parameters, except the IP parameters and user information, 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.

The camera will always ask for the admin password when executing a restore operation.

Import a configuration file

The administrator can import configuration settings from the camera. This is useful if you want to copy the configuration settings to another 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. From the menu toolbar, go to **Configuration > System > Maintenance**.
2. Under **Import Config. File**, click **Browse** to select the local configuration file and then click **Import** to start importing a configuration file. Depending on the selected file, a password might be needed to import the configuration file.
3. Click **Device Parameters** and set the saving path to save the configuration file. The camera will ask to encrypt the exported file with a password. Choose any password you want and make sure to remember it when importing the file.

Export the camera's parameters

1. From the menu toolbar, go to **Configuration > System > Maintenance**.
2. Click the **Device Parameters** button.
3. Enter the encryption password to export the current configuration file.
4. Enter the file path enter to define where on the local computer you want to store the file.

Export diagnostic information

Diagnostic information includes the running log, system information, and hardware information.

To export diagnostic information:

1. From the menu toolbar, click **Configuration > System > Maintenance**.
2. Click the **Diagnostic Information** button. A pop-up message will appear asking if you want to open or save the camera's diagnostic file (.txt format). Select an option.

Upgrade firmware

The camera firmware is stored in the flash memory of the camera. 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. In some cases, a factory default might be required after upgrade. Always refer to the FW release note when upgrading.

To upgrade firmware version:

1. Download on to your computer the latest firmware from our web site at:
www.firesecurityproducts.com
2. When the zipped firmware file is downloaded to your computer, extract it to the desired destination.

Note: Do not save the file on your desktop.

3. From the menu toolbar, click **Configuration > System > Maintenance**. 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. (this feature is currently not supported)
 - **Firmware** – Click Browse to locate the firmware file manually for the camera.
4. Click **Upgrade**. You will receive a prompt asking you to reboot the camera.
5. When the upgrade is finished, the device will reboot automatically. The browser will also be refreshed.

Security

You can manage security related parameters, such as user accounts and IP address filter from the Security menu.

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 used 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 access the camera.

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 **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. The option is disabled by default.
- **Enable Failed 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 failed 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. Default is three failed attempts.
5. Select the duration of the lockout.
6. Click **Save** to save the changes.

For security reasons, we recommend leaving the number of failed login attempts to three.

Notes:

- A. The IP address will be blocked when the failed login attempts from a user reach the number of failed username/password attempts configured in the camera (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.

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 storage in the flash memory, you can save the logs on a log server. Configure the server settings under **Advanced Settings**.

Figure 5: Security Audit Log window

The screenshot shows the 'Security Audit Log' window in the 'Configuration' tab of the 'truVision IP Camera' interface. The left sidebar lists various configuration categories, with 'Security' highlighted. The main area is divided into 'Log Query' and 'Log List' sections. The 'Log Query' section includes dropdowns for 'Major Type' and 'Minor Type' (both set to 'All Types'), and date pickers for 'Start Time' (2022-01-07 00:00:00) and 'End Time' (2022-01-07 23:59:59). A 'Search' button is present. The 'Log List' section features a table with columns: No., Time, Major Type, Minor Type, Channel No., Local/Remote User, and Remote Host IP. The table is currently empty. Below the table, it shows 'Total 0 Item(s)' with navigation arrows. The 'Advanced Settings' section at the bottom includes a checkbox for 'Enable Log Upload Server', which is currently unchecked. Under 'Server Settings', there are input fields for 'Log Server IP' and 'Log Server Port' (set to 0), and a 'Test' button. A 'Save' button is located at the bottom of the window.

No.	Time	Major Type	Minor Type	Channel No.	Local/Remote User	Remote Host IP
-----	------	------------	------------	-------------	-------------------	----------------

User Management

This section describes how to manage users. You can:

- Add or delete users
- Modify permission
- Modify passwords

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

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

When creating a new user, you must define a password for the user. There is no default password provided for all users. Users can modify their passwords and will receive a pop-up notification asking to change their password when logging into the camera web page for the first time.

Note:

Keep the admin password in a safe place. If you forget it, please contact Technical Support.

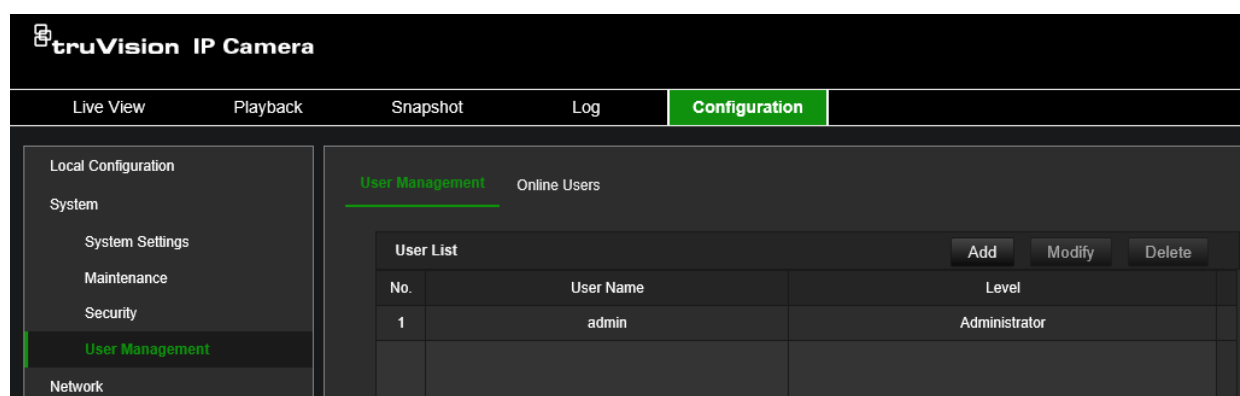
Types of users

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 permission to do live view, playback, and log search. However, they cannot change any configuration settings.

To add a user:

1. From the menu toolbar, click **Configuration > System > User Management**
2. Click the **Add** button which opens the user management window.



3. Enter a user name.
4. Select the type of user from the *Level* drop-down list. The options are User and Operator.
5. Enter the Admin Password
4. In the *Password* and *Confirm* fields enter and confirm a password for the new user.

The passwords must meet following requirements:

- At least 8 characters and a maximum 16 characters
- At least 1 capital letter
- At least 1 small letter
- At least 1 special character among - , . * & @ / \$? Space

5. Assign permissions to the user. Select the desired options:

Select All: Select all the permissions.

Remote: Parameters Settings

Remote: Log Search/Interrogate Working Status

Remote: Upgrade/Format

Remote: Bi-directional Audio

Remote: Shutdown / Reboot

Remote: Notify Surveillance Center/Trigger Alarm Output

Remote: Video Output Control

Remote: Serial Port Control

Remote: Live View

Remote: Manual Record

Remote: PTZ Control

Remote: Playback

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

To delete a user:

1. From the menu toolbar, click **Configuration > System > User Management**
2. Click **Delete** button. A message box appears.

Note: Only the administrator can delete a user.

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

To modify user information:

1. From the menu toolbar, click **Configuration > System > User Management**
2. Click the **Modify** button. The user management window appears
3. Change the information required.

Note: Only the admin user can modify users.

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

Online users

Use this menu to display users currently connected to the camera. You can see the following user information: user name, level, IP address, and operation time.

truVision IP Camera

Live View

Playback

Snapshot

Log

Configuration

Local Configuration

System

System Settings

Maintenance

Security

User Management

User Management

Online Users

User List

Refresh

No.	User Name	Level	IP Address	User Operation Time
1	admin	Administrator	10.0.0.190	2022-01-07 14:07:06
2	admin	Administrator	10.120.22.8	2022-01-06 09:46:55

Video and audio setup

You can adjust the video and audio recording parameters to obtain the snapshot quality and file size best suited to your needs.

Video settings

To define video settings:

1. From the menu toolbar, click **Camera Configuration > Video/Audio > Video**.
2. Select the channel number (1): normal (Camera 01) or thermal (Camera 02).
3. Modify the desired video functions:

The screenshot displays the 'truVision IP Camera' configuration web interface. The top navigation bar includes 'Live View', 'Playback', 'Snapshot', 'Log', and 'Configuration' (highlighted in green). On the left, a sidebar lists configuration categories: 'Local Configuration', 'System', 'Network', 'Video/Audio' (highlighted in green), 'Image', 'Event', 'Storage', 'VCA', and 'Temperature Measurement'. The main content area is titled 'Video' and contains 14 numbered settings:

- 1. Channel No.: Camera 01
- 2. Stream Type: Main Stream(Normal)
- 3. Video Type: Video Stream
- 4. Resolution: 2688*1520
- 5. Bitrate Type: Variable
- 6. Video Quality: Medium
- 7. Frame Rate: 25 fps
- 8. Max. Bitrate: 6144 Kbps
- 9. Video Encoding: H.264
- 10. Profile: High Profile
- 11. I-Frame Interval: 50
- 12. SVC: OFF
- 13. Smoothing: 50 [Clear<->Smooth]
- 14. Display VCA Info By: Player

A 'Save' button is located at the bottom of the settings list.

Function	Description
1. Channel number	Select the channel mode: normal (Camera 01) or thermal (Camera 02).
2. Stream Type	Specifies the streaming method used. Select Main Stream or Substream.

Function	Description
3. Video Type	Specifies the stream information 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.
4. Resolution	Specifies the recording resolution. A higher image resolution provides a higher image quality but also requires a higher bit rate. Note: Resolutions can vary depending on the camera model.
5. Bitrate Type	Specifies whether variable or fixed bit rate is used. Variable produces higher quality results suitable for video downloads and streaming. Default is Constant.
6. Video Quality	Specifies the quality level of the image when the bit rate is set to Variable. Options include: Lowest, Lower, Low, Medium, Higher and Highest. Note: Higher video quality requires a higher bandwidth.
7. 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.
8. Max. Bitrate:	Specifies the maximum allowed bit rate. A high image resolution requires that a high bit rate must also be selected.
9. Video Encoding	Specifies the video encoding used. You can choose between H.264 and H.265 depending on the camera model.
10. Profile	Different profile indicates different tools and technologies used in compression. Options include: Basic Profile, Main Profile, High Profile.
11. I-Frame Interval	A video compression method. It is strongly recommended not to change the default value 50.
12. 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.
13. Smoothing	Adjust the smoothness of the stream. The higher smoothing value, the better fluency of the stream. However, the video quality may be impacted.
14. Display VCA Info By	Select the display media as Player or Video. Player: The VCA info can displayed only by the TruVision player provided. Video: The VCA info can displayed by any general video player.

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

Audio settings

Audio is only available if the hardware supports it.

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

2. Select the channel number (1): normal (Camera 01) or thermal (Camera 02).
3. Modify the desired video functions:

Function	Description
Audio Encoding	Select the desired value from the list: G.722.1, G.711ulaw, G.711alaw, MP2L2, G.726, or PCM.
Audio Input	Select Mic In or Line In 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 to ON, the noise detected can be filtered.

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

Display info on stream

When Dual-VCA mode is enabled, the camera sends video analytics metadata to an NVR or other platforms when reporting a VCA event.

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 display:

1. From the menu toolbar, click **Configuration > Video/Audio > Display Info on Stream**.
2. Select **Enable Dual-VCA**.
3. Click **Save** to save changes.

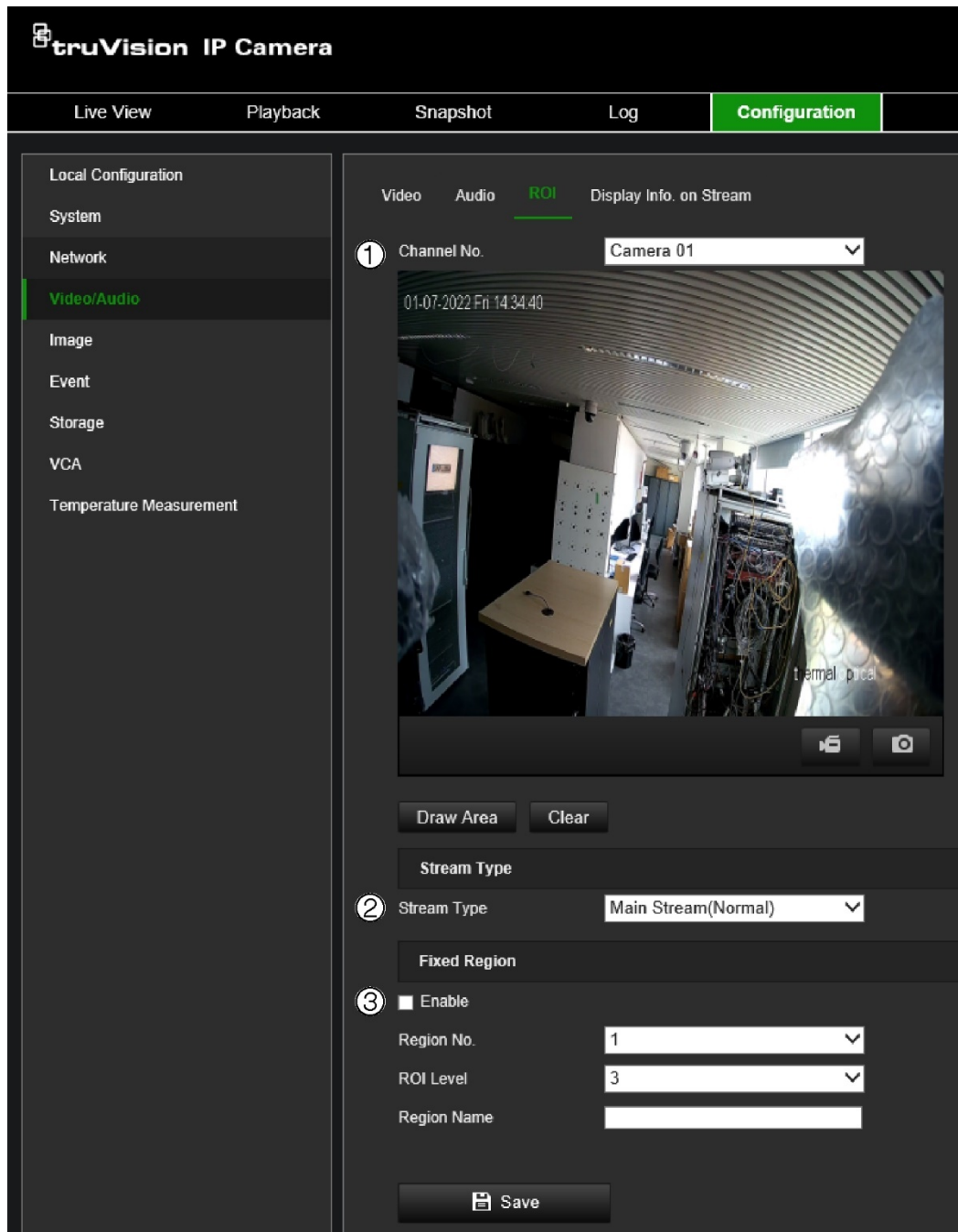
ROI encoding of an image

You can select an important area of detail or ROI (Region of interest) in a stream, such as a number plate or face. The ROI area will have a higher quality image and the non-ROI areas will have a lower image quality.

You can define up to eight ROIs.

To define an ROI:

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



2. Select the channel number (1): normal (Camera 01) or thermal (Camera 02).
3. Select the stream type (2): main stream, or substream.
4. Enable **Fixed Region** (3). This lets you manually configure the image quality enhancement level as well as name the region.
Region No.: Select the region. Default is 1.
ROI Level: Choose the image quality enhancing level. Default is 6.
Region Name: Enter the desired region name.
5. Using the mouse, draw an area on the image.
6. Repeat steps 3 to 5 to set other regions. Up to eight regions can be set.
7. Click **Save** to save changes.

Image setup

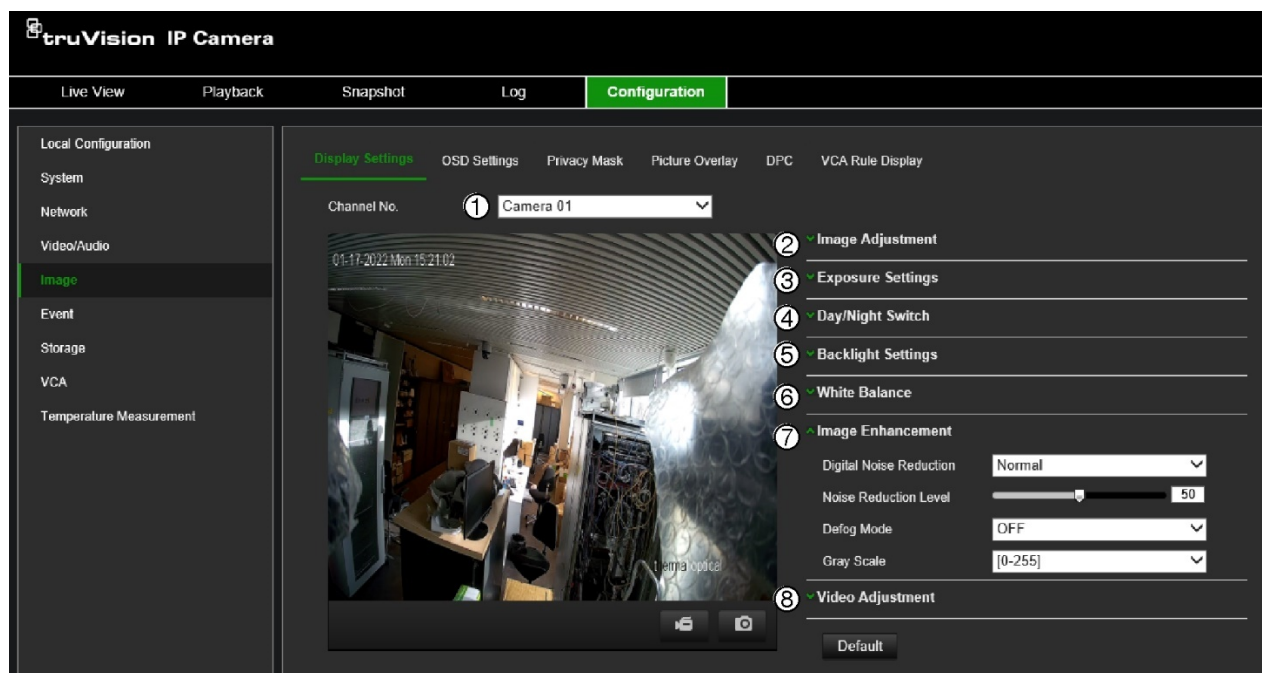
You may need to adjust the camera image depending on the camera model or location background to get the best image quality. You can adjust the camera behavior parameters such as exposure time, iris mode, video standard, day/night mode, image flip, WDR, digital noise reduction, white balance, and indoor/outdoor mode. See Figure 6 below for more information.

Display settings

Use this menu to set up how the image is displayed such as image adjustment, exposure settings, day/night settings, backlight settings, and white balance.

The functions available depend on whether normal or thermal camera mode has been selected when setting up the parameters in Display Settings.

Figure 6: Display Settings tab (normal channel shown (Camera 01))



Function	Description
1. Channel no.	Select the camera mode: normal (Camera 01) or thermal (Camera 02).
2. Image Adjustment	
Brightness and contrast	Adjust the brightness and contrast parameters. Applies to both normal camera mode (Camera 01) and thermal camera mode (Camera 02).
Saturation and Sharpness	Adjust the saturation and sharpness parameters. Applies to both normal camera mode (Camera 01) and thermal camera mode (Camera 02).

Function	Description
Background Correction	Fully cover the lens with an object (a lens cover is recommended) and click the "Defective Pixel Correction" button. The camera then adjusts the image according to the current environment. Applies to only thermal camera mode (Camera 02).
Manual Correction	Click the "Defective Pixel Correction" button. The camera then adjusts the image according to the temperature of the camera itself. Applies to only thermal camera mode (Camera 02).
Thermal AGC Mode	Select the desired AGC mode to balance and improve the image quality depending on the scene. Histogram: Select when there is an obvious WDR and high temperature difference in the scene to improve image contrast and enhancement. It is used when the image contains both indoor and outdoor scenes. Linear: Select when there is a low temperature difference between the target and the scene. When enabled, it improves image contrast and enhancement. It is used, for example, when the field of view is a bird in a tree. Self-Adaptive: Select to have the AGC mode adapt automatically to the current scene. Applies to only thermal camera mode (Camera 02).
3. Exposure Settings (normal channel only – Camera 01)	
Iris Mode	There is only one setting to select, Manual.
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.
Gain	This feature is used to adjust the image gain. The value ranges from 0 to 100.
4. Day/Night Switch (normal channel only – Camera 01)	
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. Scheduled Switch: The camera switches between day and night modes according to the configured time period.
Filtering Time	Only available when Auto D/N switch 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	Supplement light can avoid over exposure problem by decreasing the amount of IR illumination for objects closer to the camera. To enable this function, go to Configuration > Maintenance > System Service and select Enable Supplement Light.
IR Light	Select On/OFF to Enable/disable the 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.

Function	Description
IR LED Mode	When the mode is set to Auto, the supplement light is automatically enabled or disabled according to the image brightness.
Brightness Limit	The maximum limit of light from the IR LEDs.

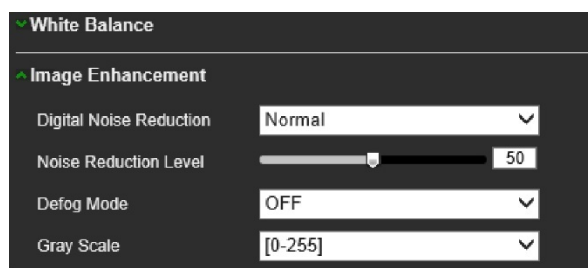
5. Backlight Settings (normal channel only – Camera 01)

BLC	The background light compensation (BLC) 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 set to “Custom”, you can draw a BLC area as a red rectangle in live mode. 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. When WDR is enabled, BLC cannot be configured.

6. White Balance (normal channel only – Camera 01)

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: (Automatic White Balance) Automatically detect white balance. Default. AWB2: (Automatic White Balance) Automatically detect the white balance and use the best option for the application. 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 (normal channel only – Camera 01)



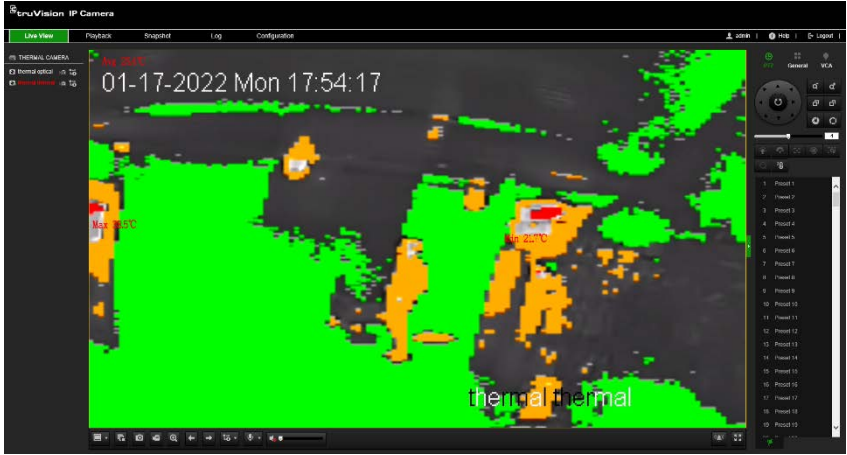
Digital Noise Reduction	Digital noise reduction (DNR) reduces noise, especially in low light conditions, to improve image performance. Select Normal Mode, Expert Mode, or OFF. Default is Normal Mode.
Noise Reduction Level	Only available when DNR is set to <i>Normal Mode</i>. Set the level of noise reduction in Normal Mode. The higher value, the stronger the noise reduction. Default is 50.
Defog Mode	You can enable the defog function when the environment is foggy and obscures the image. It enhances the subtle details so that the image appears clearer. Default is OFF.

Function	Description
Gray Scale	You can choose the range of the gray scale from 0 to 255 or from 16 to 235. Default is 0 to 255.

Image Enhancement (thermal channel only – Camera 02)

The screenshot shows the 'Image Adjustment' section with the 'Image Enhancement' sub-section expanded. It includes settings for Digital Noise Reduction (set to Normal), Noise Reduction Level (slider at 50), and Palettes (set to White Hot). Below this is the 'Target Coloration' section with three color mapping options: 'Above (be colored)' with a red color bar, 'Between (be colored)' with an orange color bar, and 'Below (be colored)' with a green color bar. Each option has a 'Max' and 'Min' temperature slider, both currently set to 0 °C. A 'Save' button is located below the color mapping options. At the bottom, there are additional settings for DDE (set to Normal), DDE Level (slider at 50), Brightness Sudden Change (set to ON), and Regional Image Enhancement (set to OFF). The 'Video Adjustment' section is partially visible at the bottom.

Digital Noise Reduction	Digital noise reduction (DNR) reduces noise, especially in low light conditions, to improve image performance. Select Normal Mode, Expert Mode, or OFF. Default is Normal Mode.
Noise Reduction Level	Only available when DNR is set to <i>Normal Mode</i> . Set the level of noise reduction in Normal Mode. The higher value, the stronger the noise reduction. Default is 50.
Palettes	Select the desired colors for the thermal view. Select White Hot, Black Hot, Fusion 1, Rainbow, Fusion 2, Ironbow 1, Ironbow 2, Sepia, Color 1, Color 2, Ice Fire, Rain, Red Hot, Green Hot, or Dark Blue. Default is White Hot.

Function	Description
Target Coloration	This function lets you select how you want to display the temperature distribution in the thermal image of live view. You can quickly see the areas in the camera image that are above and below specified temperatures. It is a bit like looking at a thermal “weather forecast”. You can select: • The color of areas where the temperature is above a defined maximum temperature (red by default). • The color of areas where the temperature is between a minimum and maximum temperature (orange by default). • The color of areas where the temperature is below a defined maximum temperature (green by default). An example of how the thermal camera image in live view can appear after setting up <i>Target Coloration</i> is shown below:  To easily if there are alarm or pre-alarm temperature points in the thermal image in live view, ensure that you have selected Configuration > Temperature Measurement > Advanced Settings. Under Configuration, select Normal. You will then be able to see the maximum, minimum and average temperatures. In the example above, the temperature text is red, which indicates that there is an alarm warning. The point with the maximum temperature is located on the left edge of the screen.
DDE	DDE (Digital Detail Enhancement) optimizes the image contrast. Select OFF or Normal Mode.
DDE Level	(Only works with Behavior Analysis VCA Resource) When the brightness of target and the background is hugely different (the temperature difference of target and background is huge), the system reduces the difference for viewing.
Brightness Sudden Change	Enable this function when there is a significant temperature difference between the target and the background. The system will reduce the brightness difference to facilitate viewing.
Regional Image Enhancement	Select a desired area in the image to see it in greater detail and more clearly. Select where on screen you want the image enhanced from the drop-down list of options. The red rectangle will appear in a set area on screen if you click up, down, left, right, center_50%, or center_75%. Select “Custom Area” from the drop-down list to a draw the desired area as a customized size anywhere on screen.

Function	Description
8. Video Adjustment	
Mirror	Both normal and thermal channels (Cameras 01 and 02) . It mirrors the image so you can see it inversed. Select Left/Right, Up/Down, Center, or OFF. Default is OFF.
Scene Mode	Normal channel only – Camera 01 Select the scene as indoor or outdoor depending on the current environment.
Video Standard	Normal channel only – Camera 01 Select the video standard. 50 Hz for PAL standard and 60 Hz for NTSC standard.
Digital Zoom	Thermal channel only – Camera 02 Set the digital zoom ratio. Select 2x, 4x, or OFF. Default is OFF.

OSD Settings (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.

You can add up to four lines of text that are superimposed on the stream to provide extra information during recordings. This option can be used, for example, to display emergency contact details. Each text line can be positioned anywhere on screen

To position the date/time and name on screen:

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

The screenshot displays the 'OSD Settings' configuration page for a TruVision IP camera. The left sidebar shows the navigation menu with 'Image' highlighted. The main configuration area includes tabs for 'Display Settings', 'OSD Settings' (active), 'Privacy Mask', 'Picture Overlay', 'DPC', and 'VCA Rule Display'. Under 'OSD Settings', the 'Channel No.' is set to 'Camera 01' and the 'Character Set' is 'GBK'. A live preview window shows a thermal image of a parking lot with two red text overlays: '10-12-2021 Tue 04:17:50' and 'Thermal Camera01'. To the right of the preview, there are checkboxes for 'Display Name', 'Display Date', and 'Display Week', all of which are checked. Below these, the 'Camera Name' is 'thermal optical', 'Time Format' is '24-hour', and 'Date Format' is 'MM-DD-YYYY'. A 'Text OverLay' section contains four numbered input fields. At the bottom, 'Display Mode' is 'Not transparent & Not flashing', 'OSD Size' is 'Auto', and 'Font Color' is 'Black&White Self-adaptive'. 'Copy to...' and 'Save' buttons are at the bottom.

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.

To add overlay text:

1. Click **Configuration > Image > OSD Settings**.
2. Under *Text Overlay*, select the check box for the first line of text and enter the text in the text box.
3. Using the mouse, click and drag the red overlay text in the live view window to the desired position.
4. Repeat steps 2 to 3 for each extra line of overlay text, selecting the next string number.

Note: Remove an overlay text by deselecting its text line.

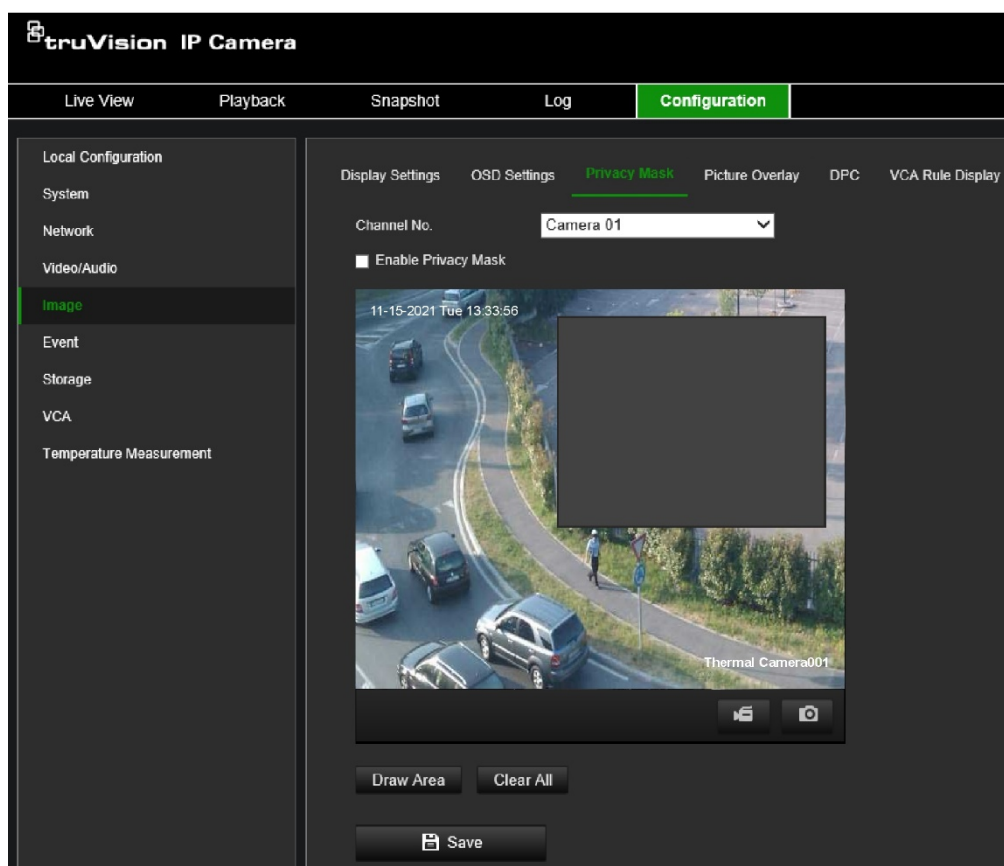
5. Click **Save** to save changes.

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 mask areas per camera. See Figure 7 on page 51 for an example.

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

Figure 7: Privacy mask window



To add a privacy mask area:

1. Click **Configuration** > **Image** > **Privacy Mask**.
2. Select the channel number: normal (Camera 01) or thermal (Camera 02).
3. Select the **Enable Privacy Mask**.
4. Click **Draw Area**.
5. Click and drag the mouse in the live video window to draw the mask areas.
Note: You can draw up to four areas on the same image.
6. (Optional) To delete mask areas, click **Clear All**.
7. 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 BMP format and the maximum size of the picture is 128*128.

To overlay a picture:

1. Click **Configuration > Image > Picture Overlay**.
2. Select a camera image on which to overlay the picture.
3. Under *Upload Picture*, click **Browse** to select a picture from your library or online and click **Upload** to upload it.
4. Select **Enable Picture Overlay** check box to enable the function.
5. Drag the picture to the desired width and height.
6. Click **Save** to save changes.

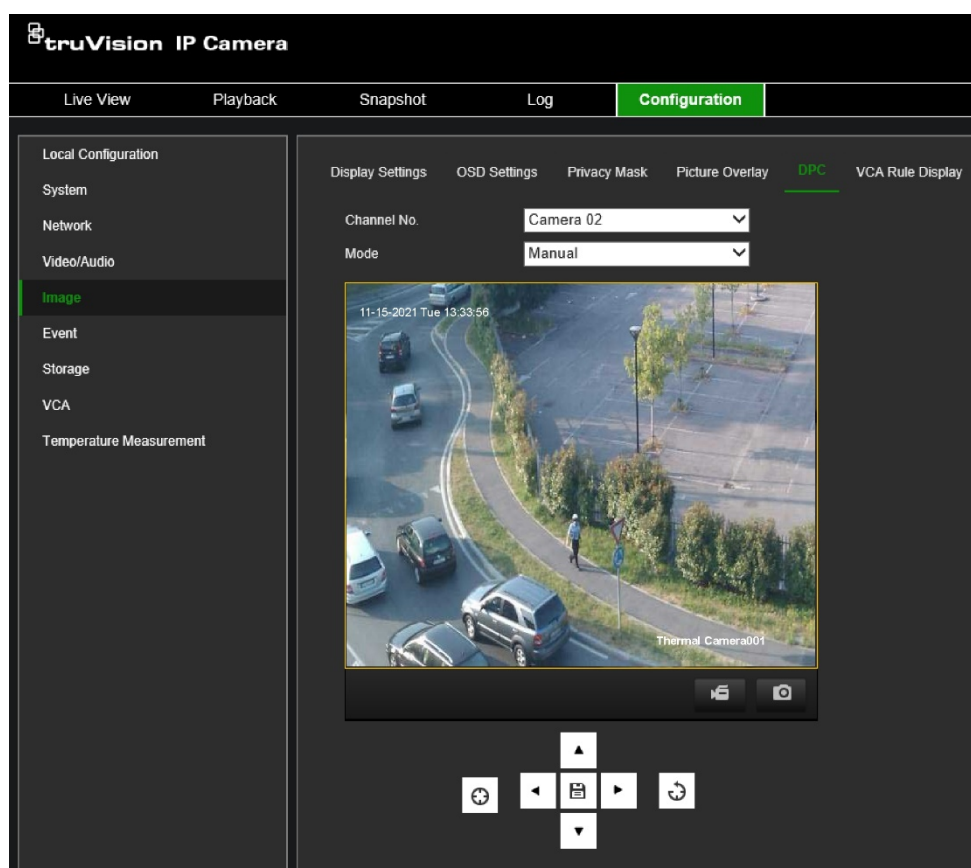
Defective pixel correction

A CCD or CMOS image sensor in a digital camera may have defective pixels, which can fail to sense light levels correctly. The DPC (Defective Pixel Correction) function allows the camera to correct defective pixels.

Note: This function is only available for certain camera models.

To set DPC:

1. From the Configuration panel, click **Configuration > Image > DPC**.



2. Select the channel number: normal (Camera 01) or thermal (Camera 02).
3. Select **Manual Mode**.
4. Click the defective pixel on the image. A cursor appears on the image in live view.

5. Click the arrow buttons to move the cursor up, down, left, right to accurately position the cursor on the defective pixel.
6. Click  then click  to correct defective pixel.

Note: If multiple defective pixels need to be corrected, click  after locating a defective pixel. Then after locating other pixels, click  to correct them simultaneously.

7. Optional. Click  to cancel the correction.

VCA rule display

This function enables you to modify the font size and temperature color of the average, alarm, and pre-alarm modes.

To set:

1. Click **Configuration > Image > VCA Rule Display**.
2. Select the channel number of the thermal channel (Camera 02).
3. Under **Font Size**, select the desired size of font.
4. Under **Temperature Measurement Rule Color Table**, select the desired colors for Normal (average), Pre-alarm and Alarm temperatures that are displayed in normal configuration mode.
5. Click **Save** to save changes. The changes are immediately visible in the Thermal channel screen.

Event setup

Events can be used to trigger actions whenever the camera is triggered by a physical input or, for example, a VCA event. There are two categories, Basic and Smart Events.

Basic events are alarm input alarm, alarm output alarms, exception alarms, flashing alarm LED outputs, and audible alarm outputs.

Smart events include Audio Exceptions. Audio inputs can be used and monitored to trigger an event or action.

Alarm inputs and outputs

The camera can be configured to record when an alarm is triggered by an external alarm device (for example, PIR detector, dry contacts...).

You can connect the camera to an alarm system, such as a siren, which is then activated when an alarm is triggered.

To define an alarm input:

1. From the menu toolbar, click **Configuration > Basic Event > Alarm Input**.

The screenshot shows the 'truVision IP Camera' configuration interface. The top navigation bar includes 'Live View', 'Playback', 'Snapshot', 'Log', and 'Configuration' (which is highlighted). On the left, a sidebar menu lists 'Local Configuration', 'System', 'Network', 'Video/Audio', 'Image', 'Event', 'Basic Event' (highlighted), 'Smart Event', 'Storage', 'VCA', and 'Temperature Measurement'. The main area is titled 'Alarm Input' and contains several tabs: 'Alarm Input' (selected), 'Alarm Output', 'Exception', 'Flashing Alarm LED Output', and 'Audible Alarm Output'. Under the 'Alarm Input' tab, there are fields for 'Alarm Input No.' (set to 'A<1'), 'Alarm Type' (set to 'NO'), 'IP Address' (set to 'Local Configuration'), and 'Alarm Name' (with a '(cannot copy)' note). A checkbox 'Enable Alarm Input Handling' is checked. Below these are buttons for 'Arming Schedule' and 'Actions'. At the bottom of the main area is a calendar grid showing the arming schedule for each day of the week (Mon-Sun) with a 24-hour scale. The 'Mon' through 'Fri' rows show blue bars indicating the arming schedule from 0 to 24 hours. The 'Sat' and 'Sun' rows are empty. At the very bottom are buttons for 'Copy to...' and 'Save'.

2. There is only one alarm input, A<1.
3. Select the alarm input type, NO (normally open) or NC (normally closed). Default is NO.

- Optional. You can enter a name for the alarm.
- Select **Enable Alarm Input Handling** to enable this feature.
- Set up the arming schedule.

Drag the mouse along the timeline of the desired day to draw a period when the alarm can be recorded. You can schedule up to eight time periods in a day.

- When you hover the mouse above a timeline a small green copy button appears at the end of the bar. Click it to copy the selected schedule of that day to another day.
- Click **Save** to save changes.

To define an alarm output:

- From the menu toolbar, click **Configuration > Basic Event > Alarm Output**.

The screenshot shows the 'Configuration' tab of the TruVision IP Camera web interface. The left sidebar lists various configuration categories: Local Configuration, System, Network, Video/Audio, Image, Event, Basic Event (selected), Smart Event, Storage, VCA, and Temperature Measurement. The main panel is titled 'Alarm Output' and contains several settings:

- Alarm Output No.:** A dropdown menu showing 'A->1'.
- Delay:** A dropdown menu showing '5s'.
- Alarm Status:** A dropdown menu showing 'OFF'.
- Alarm Type:** A dropdown menu showing 'NO'.
- IP Address:** A text field showing 'Local Configuration'.
- Alarm Name:** A text field that is disabled and shows '(cannot copy)'.

Below these settings is an 'Arming Schedule' section with a 'Delete' button and a 'Delete All' button. The schedule is represented by a timeline for each day of the week (Mon through Sun). Each day has a horizontal bar with a time scale from 0 to 24 hours. The bars for Monday through Friday are filled with blue, indicating the alarm is armed during these hours. The bars for Saturday and Sunday are white, indicating the alarm is not armed. At the bottom of the interface, there are three buttons: 'Manual Alarm', 'Copy to...', and 'Save'.

- There is only one alarm output, A<1.
- Select a timeout option between 5 and 600 seconds or select "Manually Clear".

The timeout setting lets you define how long an alarm signal remains active after the alarm has ended. If you select **Manual**, the alarm signal remains active until the alarm process that created the trigger clears.

- The alarm status cannot be changed. It is OFF.
- Select the alarm output type, NO (normally open) or NC (normally closed). Default is NO.
- Optional. You can enter a name for the alarm.

7. Set up the arming schedule.

Drag the mouse along the timeline of the desired day to draw a period when the alarm can be recorded. You can schedule up to eight time periods in a day.

8. When you hover the mouse above a timeline a small green copy button appears at the end of the bar. Click it to copy the selected schedule of that day to another day and click **OK**.
9. Click **Save** to save changes.

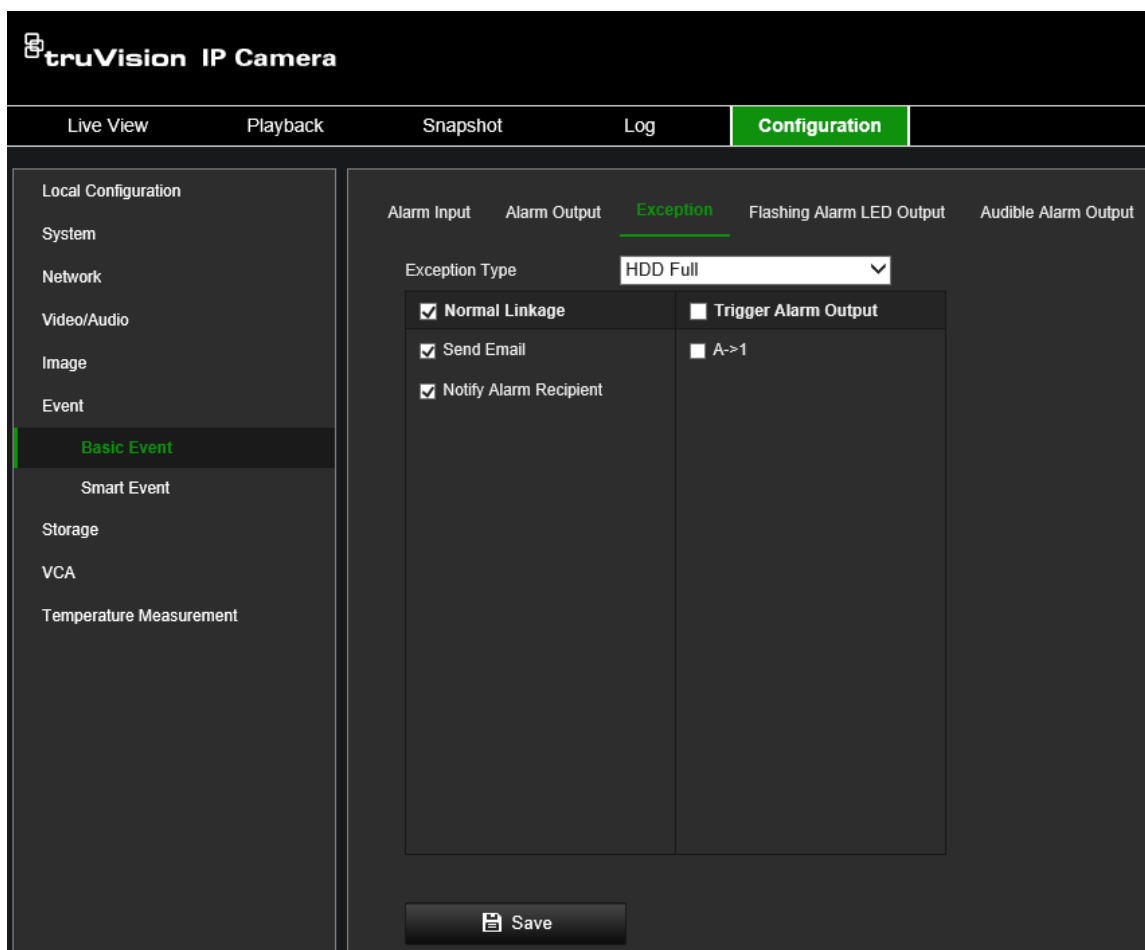
Exception

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.
- **Illegal Login**: Wrong user ID or password used to log in to the cameras.

To define exception alarms:

1. From the menu toolbar, click **Configuration > Basic Event > Exception**.



2. Under **Exception Type**, select an exception type from the drop-down list.
3. Specify the linkage method when an event occurs. Check one or more response methods for the system when a tamper-proof alarm is triggered.

Normal Linkage	Select both “Send Email” and “Notify Alarm Recipient” options.
Send Email	Send an email to a specified address when there is an exception detection alarm. Note: You must configure email settings before enabling this option. See “To set up the email parameters” on page23 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 output (A>1) when an event occurs. Note: This option is only supported by cameras that support alarm output.

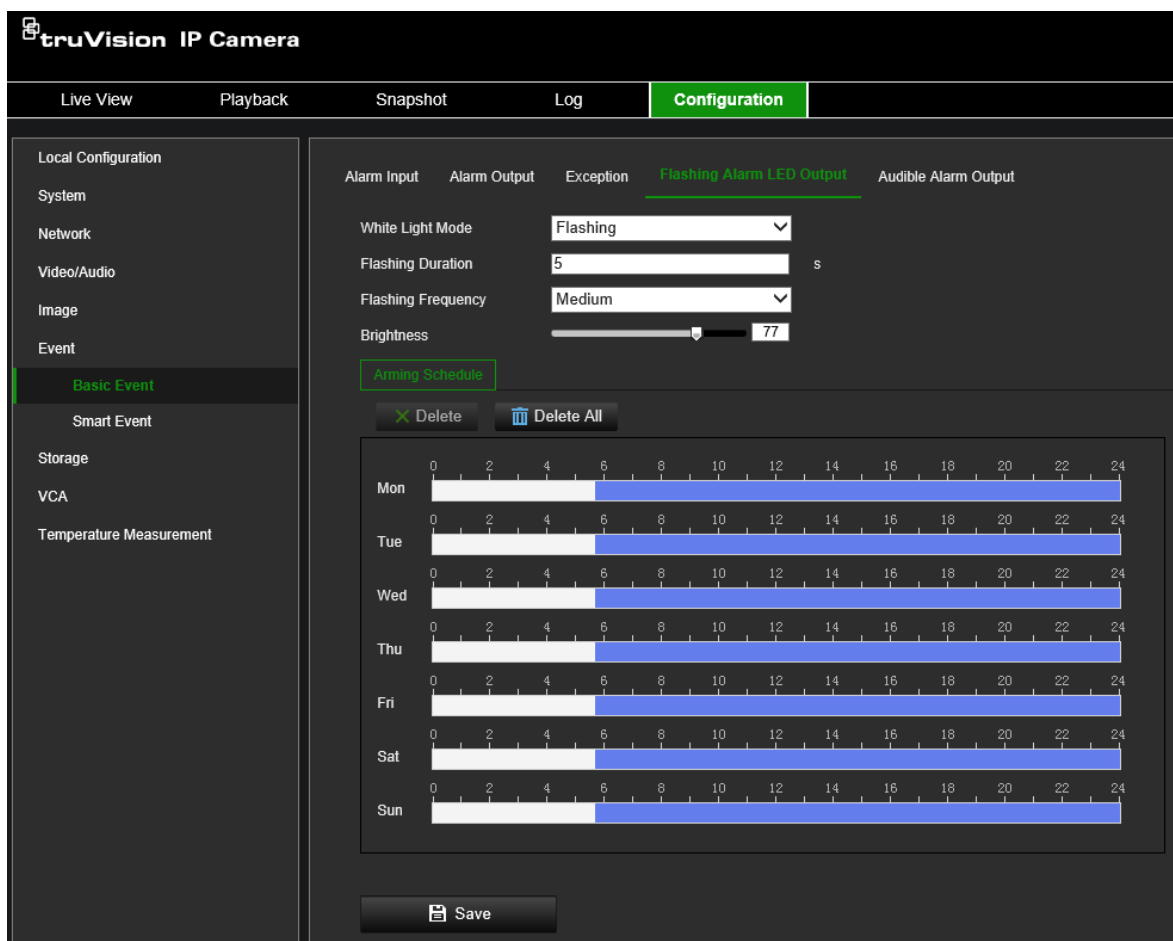
4. Click **Save** to save changes.

Flashing alarm LED output

Use this menu to set up how the strobe light on the camera responds to an alarm, such as the flashing duration and frequency.

To define a flashing alarm output:

1. From the menu toolbar, click **Configuration > Basic Event > Flashing Alarm LED Output**.



2. Select the strobe parameters:

White Light Mode: Select whether you want the LED to flash or be constant.

Flashing Duration: Enter the time in seconds for how long the strobe LED operates. The value can be between 1 and 60 seconds.

Flashing Frequency: If you entered “Flashing” under “White Lighting Mode”, select High, Medium, or Low.

3. Set up the arming schedule.

Drag the mouse along the timeline of the desired day to draw a period when the alarm can be recorded. You can schedule up to eight time periods in a day.

4. When you hover the mouse above a timeline a small green copy button appears at the end of the bar. Click it to copy the selected schedule of that day to another day and click **OK**.
5. Click **Save** to save changes.

Audible alarm output

Use this menu to set up the audible alarm output. For example, you can configure what type of alarm triggers an audible sound, the sound type, how often it plays, and the volume.

To define the audible alarm output:

1. From the menu toolbar, click **Configuration > Basic Event > Audible Alarm Output**.

The screenshot displays the 'truVision IP Camera' configuration web interface. The top navigation bar includes 'Live View', 'Playback', 'Snapshot', 'Log', and 'Configuration' (highlighted in green). The left sidebar shows a tree view with 'Local Configuration' expanded, containing 'System', 'Network', 'Video/Audio', 'Image', 'Event', 'Basic Event' (highlighted in green), 'Smart Event', 'Storage', 'VCA', and 'Temperature Measurement'. The main content area is titled 'Audible Alarm Output' and contains the following settings:

- Alarm Type:** Temperature Measurement (dropdown menu)
- Sound Type:** Warning (dropdown menu)
- Warning:** Temperature abnormality, please deal with it as soon as possible. (dropdown menu) with a 'Test' button.
- Repeat Warning:** 5 (input field)
- Sound Volume:** 100 (slider)
- Arming Schedule:** A button to configure the schedule.
- Buttons:** 'Delete' and 'Delete All' buttons.
- Schedule Table:** A table showing the arming schedule for each day of the week (Mon-Sun). Each row has a time axis from 0 to 24 hours. The 'Arming' period is indicated by a blue bar, which is active from 6:00 to 24:00 for all days.
- Save:** A 'Save' button at the bottom.

2. Select the type of alarm to trigger the audio alarm: VCA Behavior Analysis or Thermal Measurement:
3. Select the sound type:

Warning: A pre-recorder message is played. The message is shown below under Warning. If “Temperature Measurement” was selected as the alarm type, the default warning message is “Temperature abnormality. Please deal with it as soon as possible.” If “VCA Behavior Analysis” was selected as the alarm type, the default warning message is “Warning. This is a restricted area.”

Custom Audio: Upload a custom audio file. The file must be .wav format no larger than 512KB. Its sampling rate should be 8 KHz.

4. Under **Repeat Warning** enter the number of times the warning will be repeated.
5. Using the mouse, drag the scroll bar to select the volume of the alarm sound.
6. Set up the arming schedule.

Drag the mouse along the timeline of the desired day to draw a period when the alarm can be recorded. You can schedule up to eight time periods in a day.

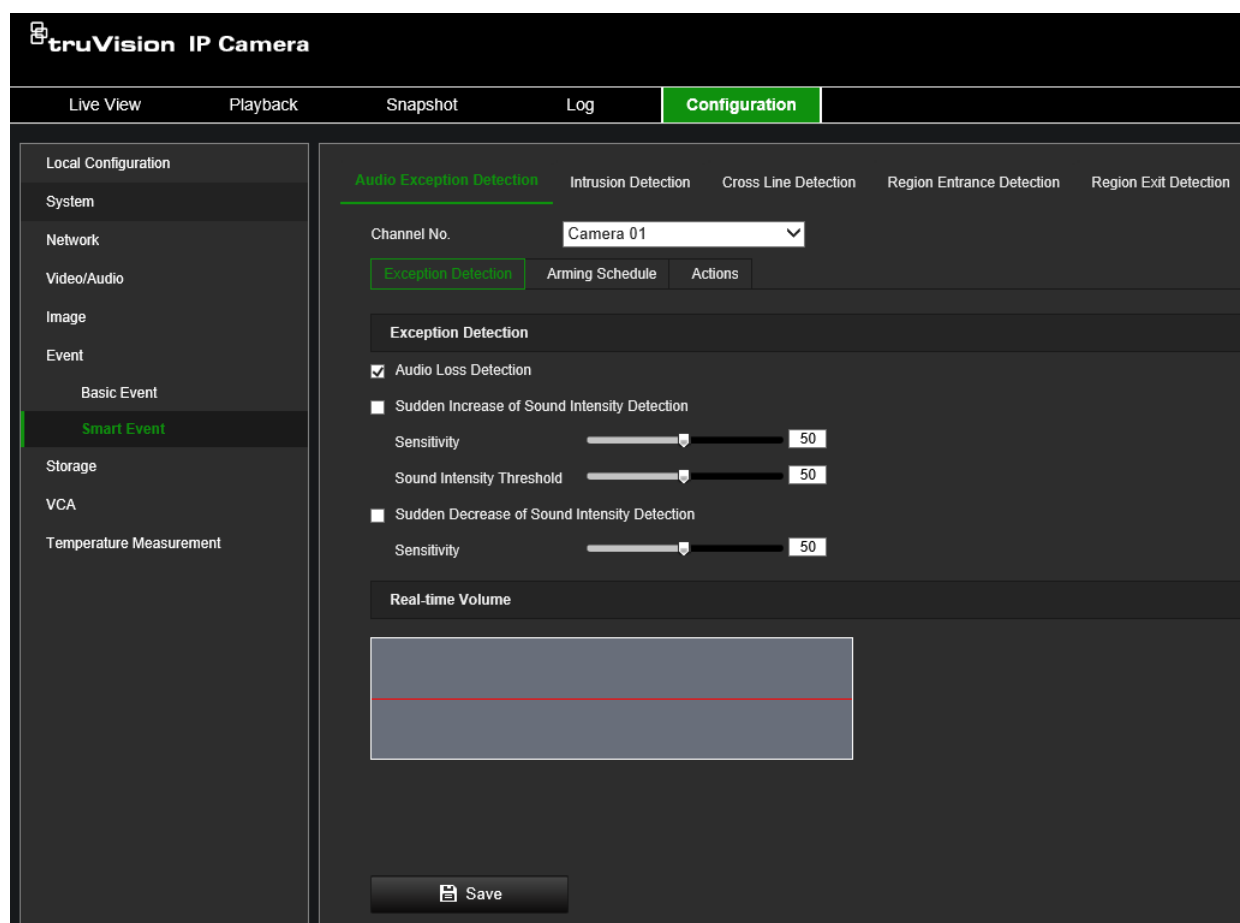
7. When you hover the mouse above a timeline a small green copy button appears at the end of the bar. Click it to copy the selected schedule of that day to another day and click **OK**.
8. Click **Save** to save changes.

Audio exception detection

This function detects the abnormal sounds in the surveillance scene, such as the sudden increase/decrease of the sound intensity. It can be set up to trigger a series of alarm actions.

To define the audio exception detection:

1. From the menu toolbar, click **Configuration > Smart Event > Audible Exception Detection**.
2. From the camera list, select Camera 1, which is the thermal camera. This function is not available in the bi-spectral thermal camera.



3. Click the **Exception Detection** tab and select one or more of the following audio exception detections:

Audio Loss Detection: Detect a sudden loss of sound.

Sudden Increase of Sound Intensity Detection: Detect a sudden increase in sound intensity. Modify the **Sensitivity** and **Sound Intensity Threshold** levels.

Sudden Decrease of Sound Intensity Detection: Detect a sudden decrease in sound intensity. Modify the **Sensitivity** and **Sound Intensity Threshold** levels.

Notes:

Sensitivity: The smaller the value, the greater the change in sound required to be detected.

Sound Intensity Threshold: It is recommended to set this value as the average environmental sound value. The louder the environmental sound, the higher the value required.

You can view the real-time volume of the sound under *Real-time Volume*.

4. Click the **Arming Schedule** tab to set the arming schedule.

Drag the mouse along the timeline of the desired day to draw a period when the alarm can be recorded. You can schedule up to eight time periods in a day.

When you hover the mouse above a timeline a small green copy button appears at the end of the bar. Click it to copy the selected schedule of that day to another day and click **OK**.

5. Click the **Actions** tab to specify to specify the response methods for the system when an alarm is triggered:

Send Email	Send an email to a specified address when there is a motion detection alarm. Note: You must configure email settings before enabling this option. See "To set up the email parameters" on page 23 for further information. If you want to send the event snapshot together with the email, 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 the desired which alarm outputs. Note: This option is only supported by cameras that support alarm output.
Trigger Recording	Trigger the recording to start in the camera.

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

Storage setup

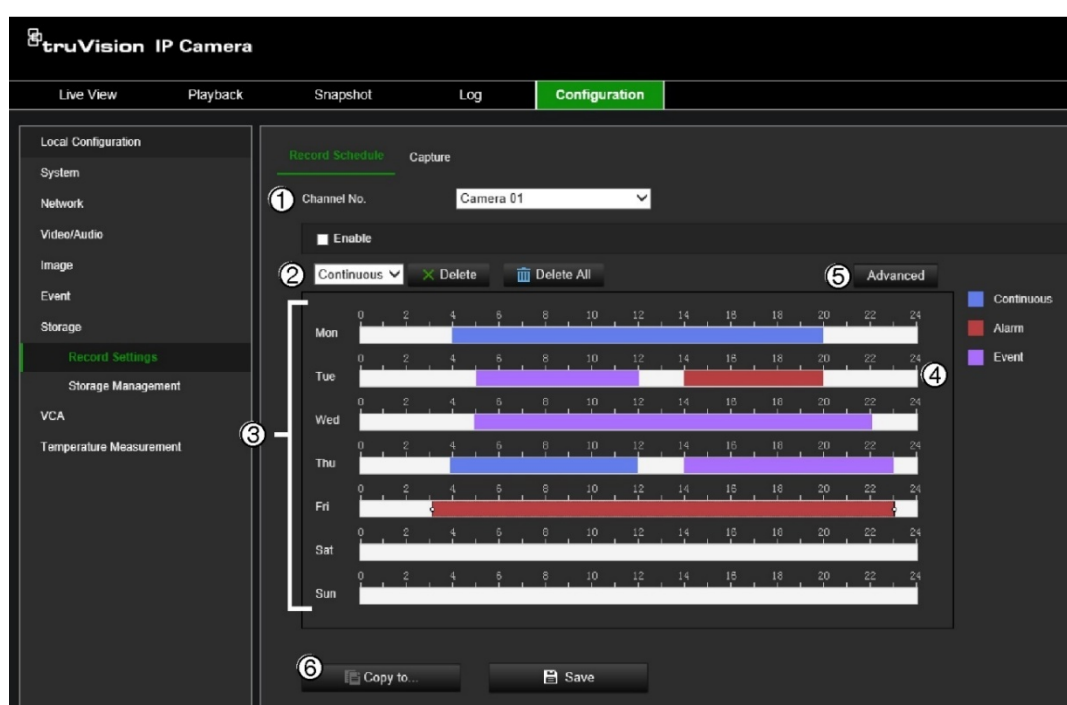
You can define recording schedules for the cameras to specify when recordings occur, and which pre-defined settings are used. Camera streams can be recorded on an optional recording device, NAS or SD card inserted in the camera.

Record settings

You can define a recording schedule for the camera in the “Record Schedule” window. The video recordings are saved onto a SD card inserted in the camera or a NAS. The camera’s SD card can provide a backup in case of network failure. The SD card is not provided with the camera.

The schedules are visually presented on a map for easy reference. See Figure 8 below.

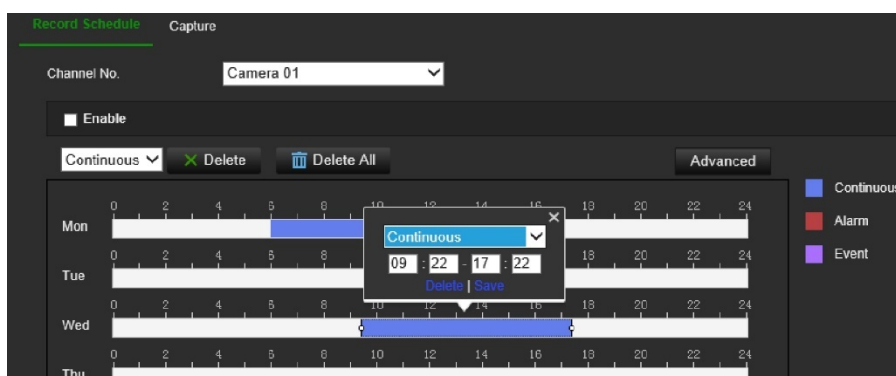
Figure 8: An example of a recording schedule



1. **Camera.** Select a camera.
2. **Recording type.** There are three types of recording to select, which are color-coded:
 - Continuous (Blue): Records continuous recording.
 - Event (Purple): Records all events (basic and smart, alarms and VCA events).
 - Alarm (Red): Records when the alarm is triggered via the external alarm input channels.
3. **Schedule map.** There are eight days to select: Sunday (Sun), Monday (Mon), Tuesday (Tue), Wednesday (Wed), Thursday (Thu), Friday (Fri), and Saturday (Sat), and Holiday (if enabled).
4. **Timeline.** There is a 24-hour time line for each day. Up to eight recording periods can be scheduled during the 24-hour period.
5. **Advanced button.** Click to set extra recording settings such as pre- and post-recording times, stream type, and the number of days to keep videos/snapshots.
6. **Copy button.** Click to copy schedules between cameras.

To set up a recording schedule:

1. From the menu toolbar, click **Configuration > Storage > Record Settings > Record Schedule**.
2. Select the channel number (item 1 in Figure 8 on page 62): normal (Camera 01) or thermal (Camera 02).
3. Select the **Enable** check box to enable recording.
Note: To disable recording, deselect the option.
4. Select the recording type (2) from the drop-down list and then drag the mouse on the desired day to mark a recording schedule (4).
 - **Continuous:** This is continuous recording.
 - **Alarm:** Video is recorded when the alarm is triggered via the external alarm input channels.
 - **Event:** Video is recorded for all events (basic and smart, as well as VCA events).**Note:** Up to eight record types can be selected.
5. To change a schedule, click the scheduled recording in the timeline for the desired day. In the pop-up box that appears, select whether you want to record continuous or event recording and enter the start and end times. Click **Save**.



6. Click the **Advanced** button (5) to set the following parameters:

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, 60 s, 120 s, 300 s, or 600 s.

Stream type: 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.

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

7. Set the recording periods for the other days of the week if required.
8. Click **Copy to... (6)** to copy the recording schedules to another camera.
9. Click **Save** to save changes.

Capture (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.

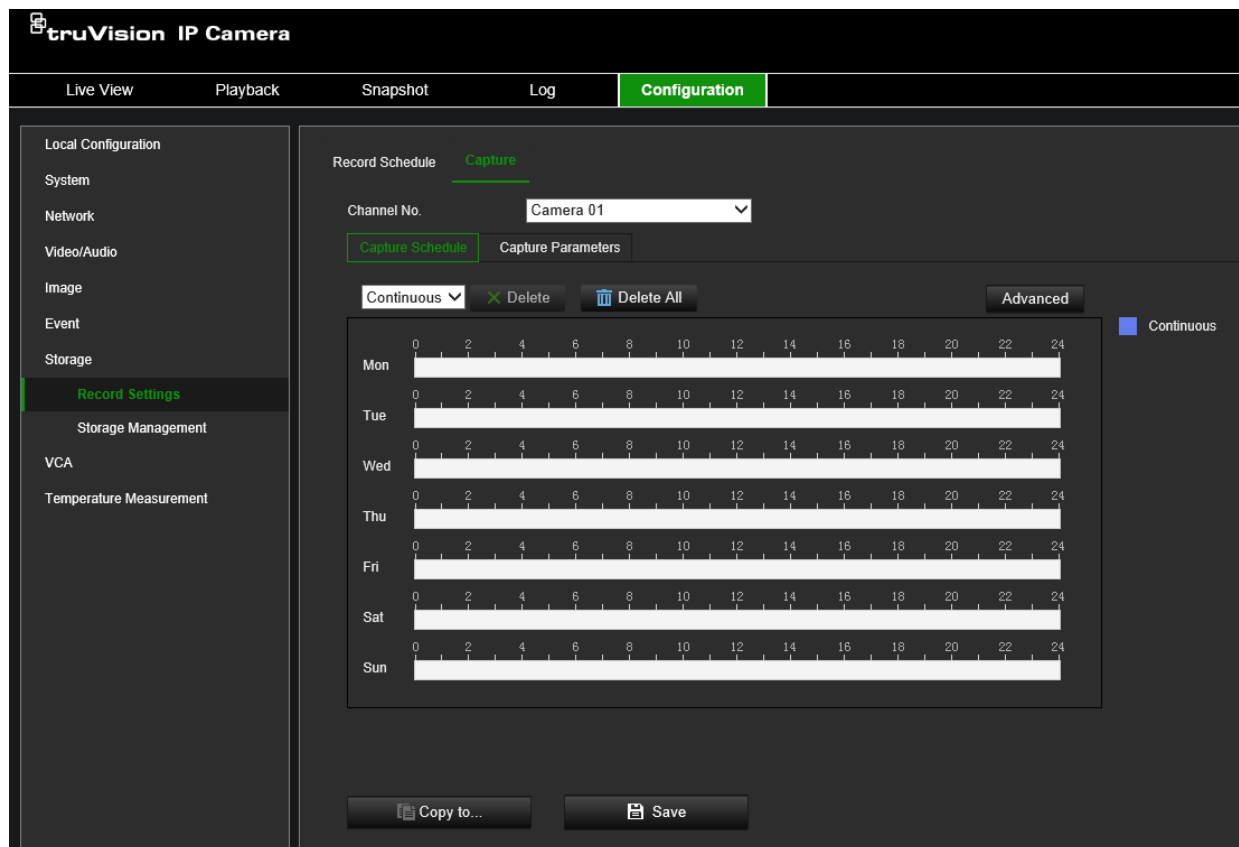
You must enable the option **Enable Timing Snapshot** if you want snapshots to be uploaded with a fixed interval to the FTP server. If you have configured the FTP settings and enabled **Upload Type** in the **Network > Advanced Settings > FTP** tab, the snapshots will not be uploaded to the FTP if the **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 Management > Capture > Capture Schedule**.

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



2. Click and-drag the mouse on the timeline 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.

truVision IP Camera

Live View Playback Snapshot Log **Configuration**

Local Configuration

System

Network

Video/Audio

Image

Event

Storage

Record Settings

Storage Management

VCA

Temperature Measurement

Record Schedule **Capture**

Channel No. Camera 01

Capture Schedule **Capture Parameters**

Timing

☒ Enable Timing Snapshot

Format JPEG

Resolution 2688*1520

Quality High

Interval 500 millisecond

Event-Triggered

☒ Enable Event-Triggered Snapshot

Format JPEG

Resolution 2688*1520

Quality High

Interval 500 millisecond

Capture Number 4

Copy to... Save

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

- Select the **Enable Timing Snapshot** check box.
- Select the desired format of the snapshot. Default is JPEG.
- Select the desired resolution and quality of the snapshot.
- 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:

- Select the **Enable Event-Triggered Snapshot** check box.
- Select the desired format of the snapshot. Default is JPEG.
- Select the desired resolution and quality of the snapshot.
- 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 **Copy to...** to copy the recording schedules to another camera.

8. Click **Save** to save changes.

Storage management

SD card and NAS parameters can be managed in the Storage Management menu.

HDD Management

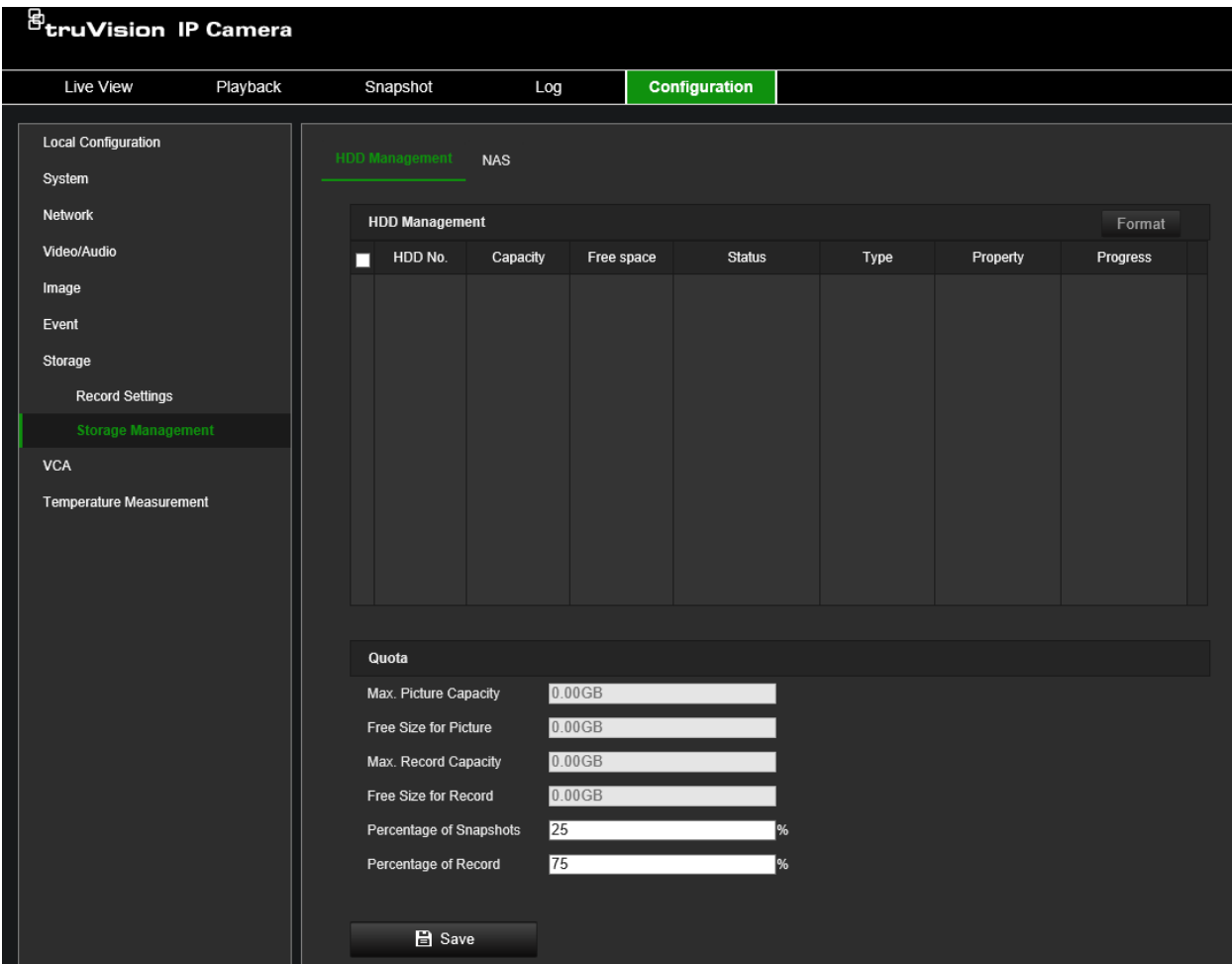
Use the HDD management window to display the capacity, free space available, and the working status of the HDD of the NAS and the SD card in the camera. You can also format these storage devices.

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

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.

To format the storage devices:

1. From the menu toolbar, click **Configuration > Storage > Storage Management > HDD Management**.



2. Select the **HDD No.** to select the storage.
3. Select the **HDD No.** check box of the desired storage device.

Select the check box of the uninitialized disk and click the **Format** button to start initialization. When completed, the status changes to “Normal”.

4. Enter the quota percentage for snapshots and recording to allocate the storage capacities to the camera. Modify the values for each in **Percentage of Snapshot** and **Percentage of Record**.
5. Click **Save** to save changes.

NAS

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.

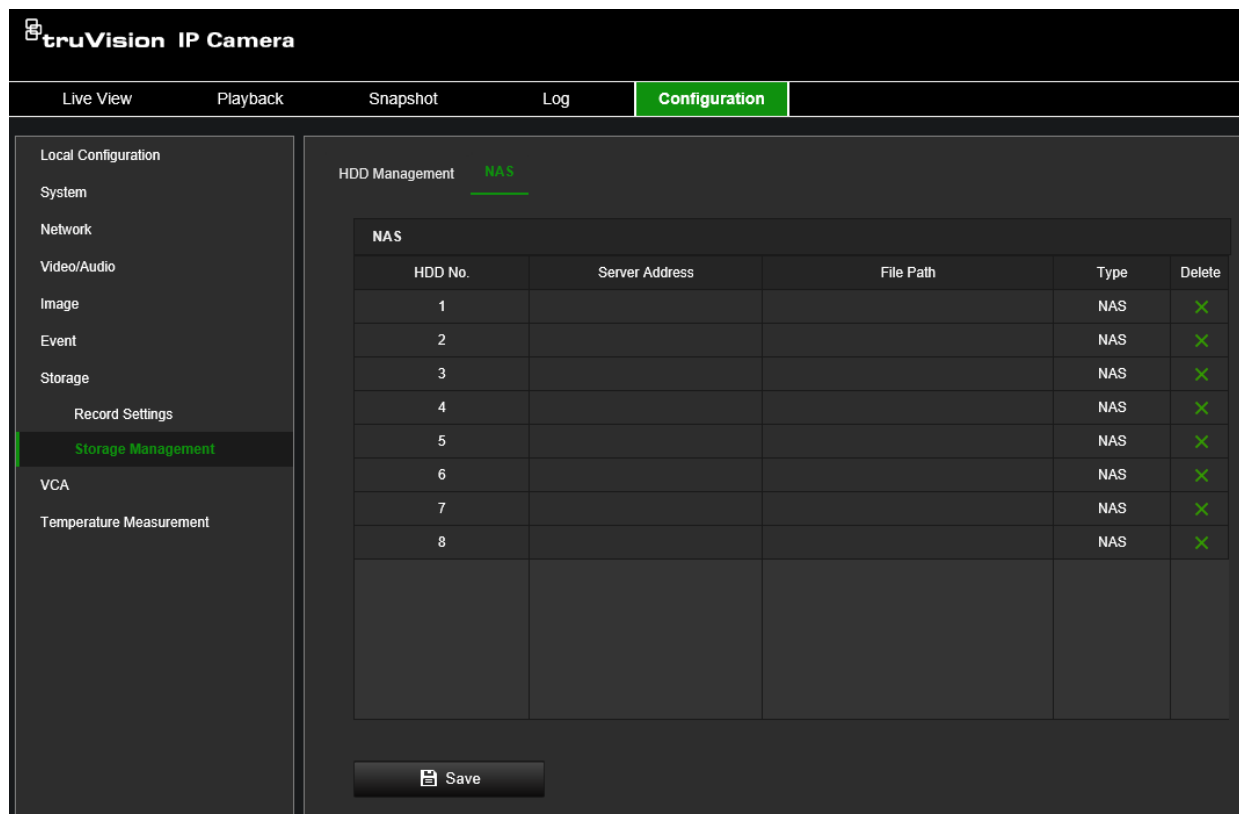
Notes:

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.

Caution: We strongly recommend that you use a strong password for all functions and network devices to protect your privacy and to protect your system against security risks. A valid password range must be at least eight characters. You can use a combination of numbers, lower- and upper-case letters, and special characters. The installer and/or end user are responsible for password management.

To set up a NAS system:

1. Add the network disk.
 - a) From the Configuration panel, click **Configuration > Storage > Storage Management > NAS**.



- b) Under the *Server Address* column, manually enter the IP address in the *Server Address* column.
- c) Under the *File Path* column, manually enter the file path name for where on the remote storage system you want to store the files.
- d) Under the *Type* column, select the mounting type: NFS or SMB/CIFS. If SMB/CIFS is selected, set the user name and password to ensure security.

Note: Please refer to the NAS user manual for information on setting the file path.

- d) Click **Save** to add the disk.

2. Initialize the disk that has been added.

From the Configuration panel, click **Configuration > Storage > Storage Management > HDD Management**. See “HDD Management” on page 67 for further information.

VCA setup

Use this menu to configure how to display VCA information on stream and on snapshots, calibrate the camera, set up shield regions, set up VCA rules, and adjust the configuration parameters for detection.

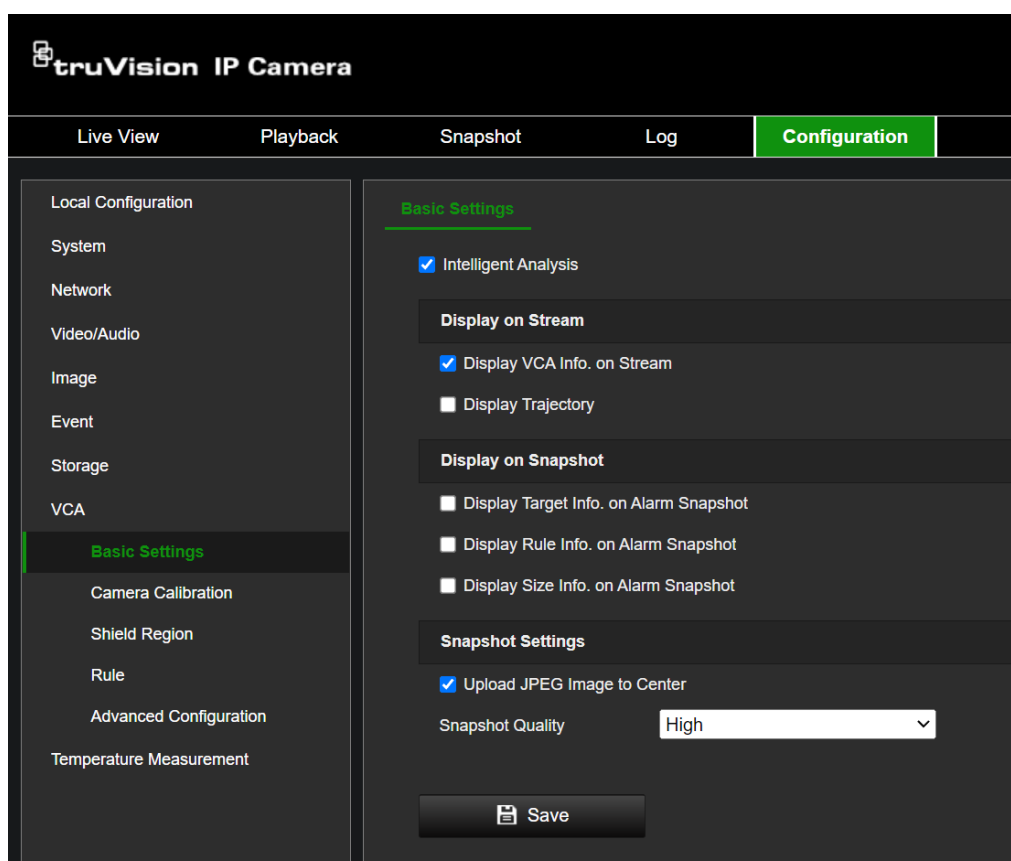
It is recommended not to use the VCA or the temperature measurement functions at the same time.

Basic settings

Set up how information is displayed on stream and on a snapshot. You can also enable snapshots to be uploaded to the surveillance center as well as define the quality of the snapshot image uploaded.

To set up VCA parameters:

1. To display rule information in live view, go to **Configuration > Local** to view the Live View parameters window. Enable **Display Rules Info on Capture** and click **Save**
2. From the menu toolbar, click **Configuration > VCA > Basic Settings**.



3. Select the desired settings:

Display on Stream:

Display VCA Info. on Stream	Display target and rule information on the live view and playback streams.
Display Trajectory	Display the target's path in live view.
Display on Snapshot:	
Display Target info. on Alarm Snapshot	Display the target information on the snapshot.
Display Rule info. on Alarm Snapshot	Display the rule information on the snapshot.
Display Size info. on Alarm Snapshot	Display the target's size information on the snapshot.
Snapshot Settings:	
Upload JPEG Image to Center	Upload the snapshot to the surveillance center when an alarm occurs. You can also set up the quality of the image.

4. Select **Intelligent Analysis** to enable behavior analysis. Online instructions appear that show the steps required to set up the detection rules and areas.
5. Click **Save** to save changes.

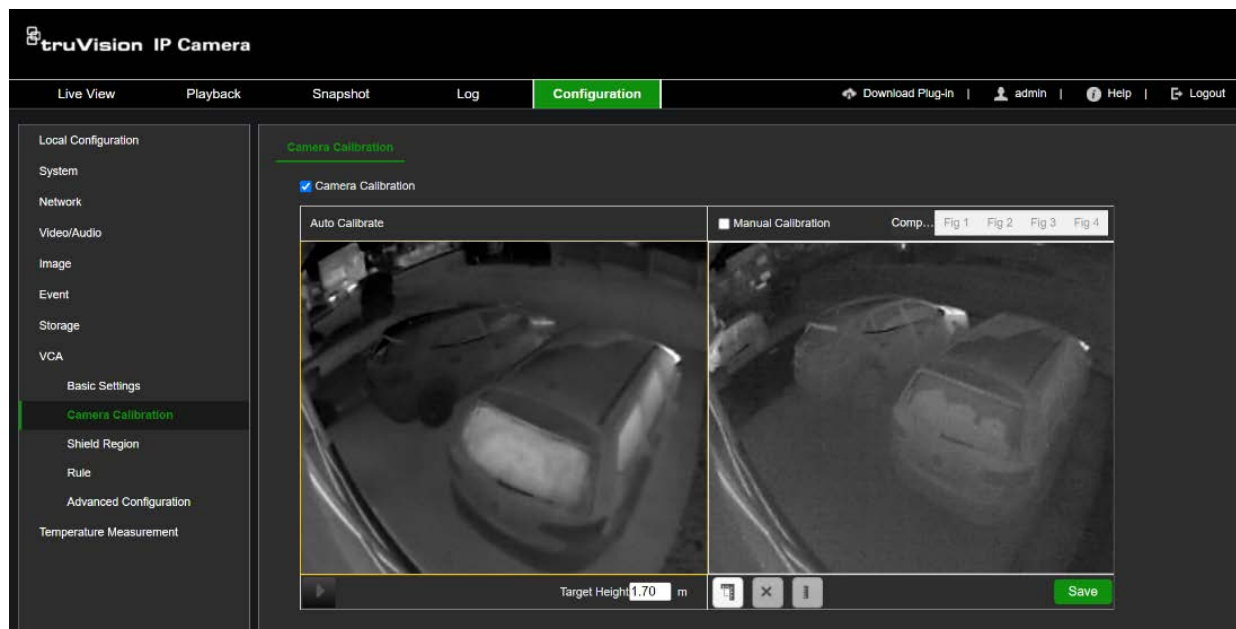
Camera calibration

To automatically calibrate the camera, somebody needs to walk in front of the camera during the test. You need to know the height of the person and they must be the only moving object in view during calibration.

When the camera is automatically calibrating, it will take four snapshots of the person passing in front of the camera (Figures 1 to 4). The calibration is successful if it takes the four snapshots. If it fails to take the four photos, you then need to manually calibrate the camera.

To automatically calibrate the camera:

1. From the menu toolbar, click **Configuration > VCA > Camera Calibration**.



2. Enable **Camera Calibration**.
3. Under **Target Height**, enter the total height of the person.
4. Click the arrow ► button to start calibration.
 - Calibration starts when the whole height of the person is in view. It ends when the person reaches the end point and exits the image.
 - The distance (in meters) between the end point and the camera is four times the lens focal length (mm). For example, for a 7mm lens, the recommended end point is 28 m (7*4).
 - The person should walk in a zigzag path. Two zigzag paths are required. The walking route should cover the left, middle, and right areas of the image.
 - The auto-calibration duration should be at least 10 seconds, and not exceed 10 minutes. The camera will automatically stop calibrating if the duration is less than 10 seconds or exceeds 10 minutes.
 - If there is a moving object in the scene, such as leaves or a tree, set up a shielded area. See “Shield region” on page 73 for more information.
5. When the person exits the image, click ► to stop the calibration.

There will be four snapshots of the person in different locations (Figures 1 to 4). The composite figure shows all four snapshots in one image.

Note: To redo the automatic calibration, enter another target height value and click the arrow ► button.
6. Verify the result of the calibration. See “To verify the calibration result” below for more information.

To manually calibrate the camera:

1. From the menu toolbar, click **Configuration > VCA > Camera Calibration**.
2. Select **Manual Calibration**.

3. In the manual calibration window, click **Fig. 1** and . Drag and adjust the vertical line that appears to the height of the target. Then enter the target's length in meters.

Note: The line can only be vertical.

4. Repeat step 3 for **Fig. 2**, **Fig. 3**, and **Fig. 4**. The lines must not overlap or be too close to one another. Do not position a line on a totally black area as the system may not be able to see the calibration line.

Note: The targets should be not just the person but also other objects such as lampposts and cars.

If required, click  to delete a line in the selected figure.

5. Click **Save** to save changes.
6. Verify the result of the calibration. See “To verify the calibration result” below for more information.

To verify the calibration result:

Use this function to check that the calibrated value is consistent with the actual value.

1. After you have calibrated the camera (automatic or manual), click .
2. Click  and drag the vertical line that appears to one of the areas where you placed a vertical line for the calibration. Adjust the line to the same height of the desired calibration line (Figures 1 to 4).
3. Click  to see the estimated height of the drawn line. Compare this calculated height to the height of the target. If the comparison result is inaccurate, do a manual calibration.
4. Click  to exit verification.

Shield region

Use the shield region to mask an area in the image, such as the sky, where you want VCA detection to be disabled. This can help reduce false alarms. You can add up to four shield regions.

To add a shield region to the image:

1. From the menu toolbar, click **Configuration > VCA > Shield Region**.
2. Click  and draw an area to be masked. Click  to draw each area.

To delete an drawn area, select the desired area and click .



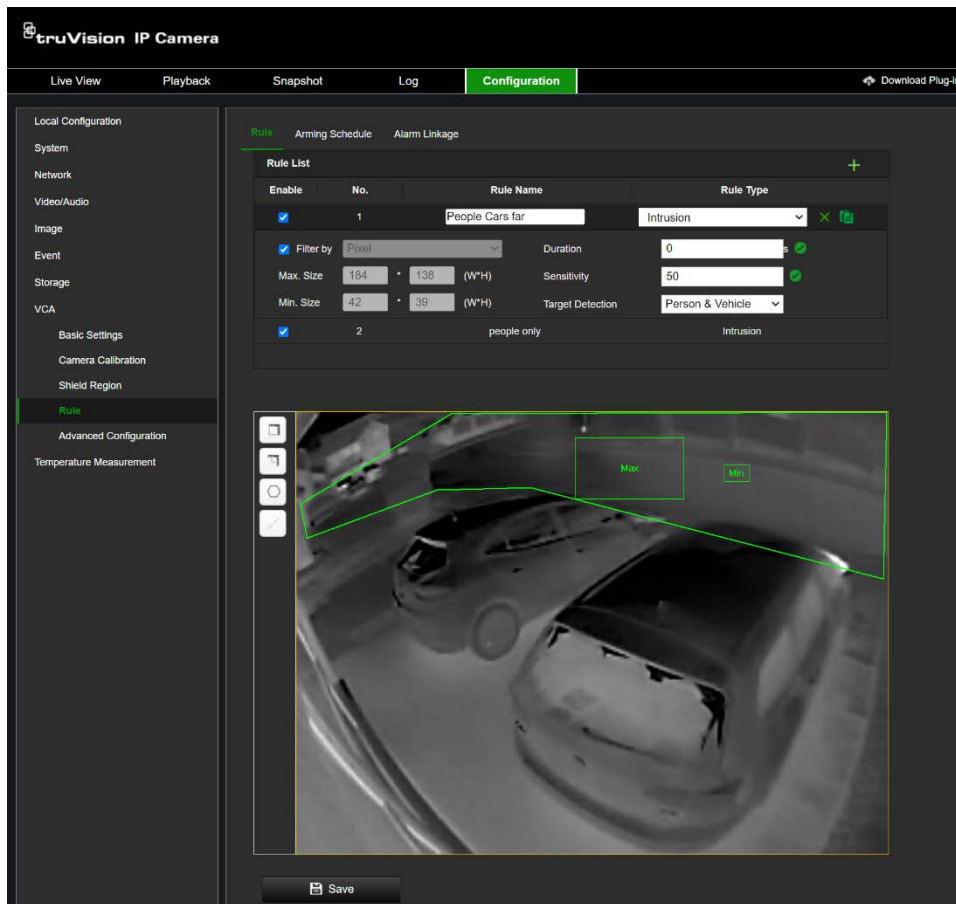
3. Click **Save** to save changes.

Rule

You can set up rules to determine when VCA events trigger alarms. There can be a maximum number of eight rules.

To add a VCA rule:

1. From the menu toolbar, click **Configuration > VCA > Rule**.



2. To create a new rule, click **+**.
3. Select the **Enable** check box to enable the rule and enter its name.
4. Select the desired VCA type.

None	No VCA type selected. The rule cannot be saved if this option is selected.
Cross Line	This function can be used to a target crossing an area on-screen. 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.
Intrusion	You can set up an area in the surveillance scene to detect when intrusion occurs. If a target enters the area, a set of alarm actions can be triggered.
Region Entrance	This function detects a target that enters a pre-defined region.
Region Exit	This function detects a target that exits from a pre-defined region.

5. Select the rule parameters:

Cross Line	Sensitivity: Select the alarm sensitivity value between 0 and 100. The higher the value, the more sensitive the alarm trigger. Cross line: Select Bi-directional, A-to-B, or B-to-A. Target Detection: Select Person, Vehicle, or Person & Vehicle (recommended).
Intrusion	Duration: Select the alarm duration between 0 and 100. Sensitivity: Select the alarm sensitivity between 0 and 100.

	Sensitivity: Select the alarm sensitivity value between 0 and 100. The higher the value, the more sensitive the alarm trigger. Target Detection: Select Person, Vehicle, or Person & Vehicle (recommended).
Region Entrance	Target Detection: Select Person, Vehicle, or Person & Vehicle (recommended).
Region Exit	Target Detection: Select Person, Vehicle, or Person & Vehicle (recommended).

Note: Click  to copy the settings to another rule.

6. Draw the rule.

Intrusion / Region Entrance / Region Exit: Click the  icon and then click up to 10 points on the image to set the area for intrusion, region entrance, or region exit detection (depending on the rule type selected). Right-click the mouse to end drawing. Only one area can be set. If you want to delete the area, select **None** under *Rule Type*.

Cross Line: Click the  icon. A cross line appears on screen. Drag the line to the desired position. Only one line can be set. If you want to delete the line, select **None** under *Rule Type*.

7. Filter the size of a target that can trigger an alarm by setting the minimum and maximum sizes of the target to detect. Only targets that meet these size criteria can trigger an alarm. Select one of the two options:

Filter by Pixel: Click  and draw the minimum-sized rectangle. Click  and draw the maximum-sized rectangle.

As the main difference between a person and an animal is height, it is recommended to size the filter rectangles by height.

Filter by Actual Size: Enter the maximum and minimum height and width in meters.

Note: The *Filter by Actual Size* function is not available if calibration failed or was not completed. *Filter by Pixel* is always available.

8. Click **Save** to save changes to the rule.

9. Set the arming schedule for each rule. Click the Arming Schedule tab.

Click the timeline bar to edit the arming schedule. In the pop-up box, enter the start and end times (hour and minutes). If required, click  to copy the schedule to other days or to the whole week. Click **Save** to save changes.

10. Set up the linking method for a rule.

Click **Alarm Linkage** to trigger an action when the motion 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 23 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 68 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 23 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 "Enable Event-Triggered Snapshot" section on page 66 for further information.
Flashing Alarm	Trigger a flashing light on the camera when an event is detected by the camera.
Audible Warning	Trigger an audible beep when an event is detected by the camera.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Select "Select All" or each individual alarm output. Note: This option is only available for cameras that support alarm outputs.
Trigger Recording	Trigger the recording to start in the camera.

Click **Save** to save changes to the linkage method.

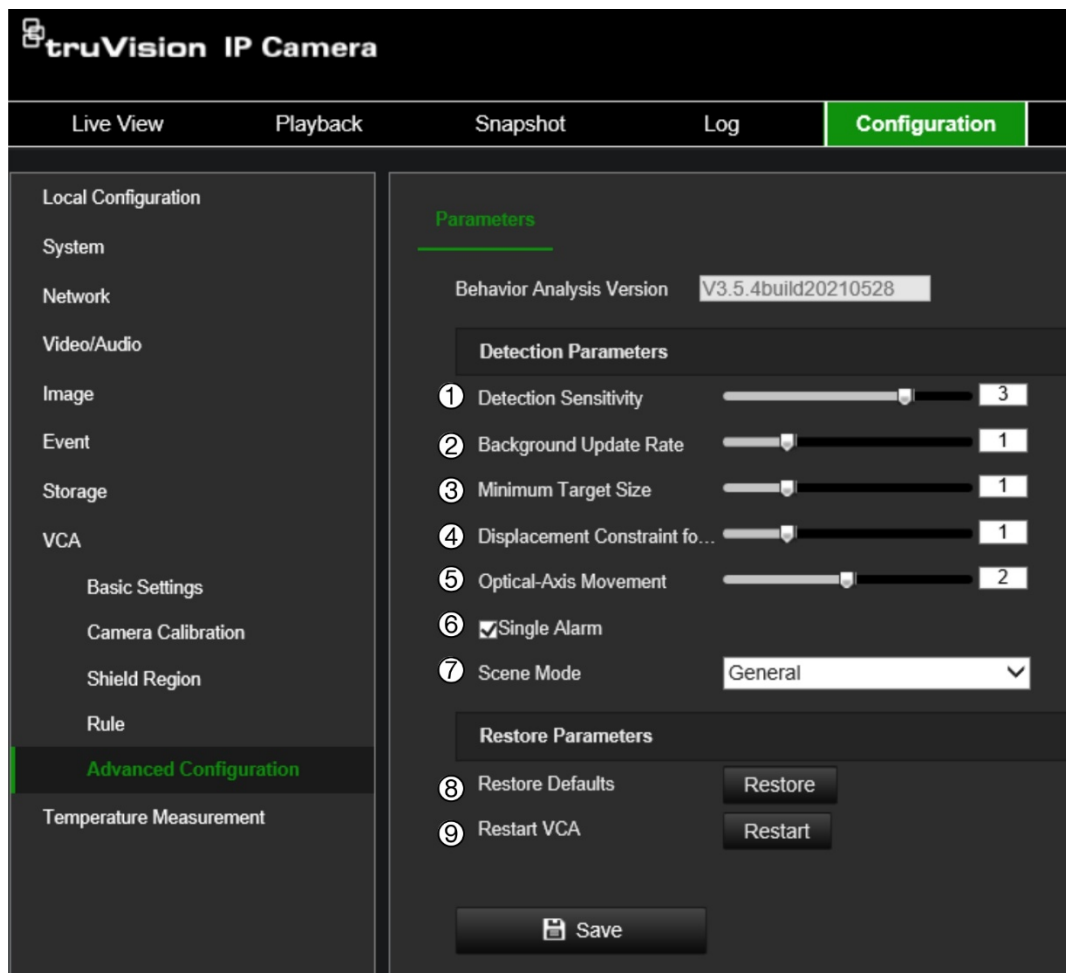
Advanced calibration

The *Advanced Configuration* menu lets you adjust the VCA detection parameters as well as restore and restart default settings.

Normally the default detection parameters are used but there may be occasions when you may need to adjust some, such as when the contrast between the background and objects in the image is poor, making it difficult to distinguish between objects.

To adjust the detection and restore parameters:

1. From the menu toolbar, click **Configuration > VCA > Advanced Configuration**.
2. Adjust the desired parameters.



1. Detection Sensitivity	Adjust this parameter when the contrast between the background and objects in the image is not sharp thereby making it difficult to distinguish between objects. The higher the value, the higher the detection sensitivity. Default is 3.
2. Background Update Rate	If an object remains in the scene for a certain amount of time, the system will then automatically consider it part of the background. The higher the value, the sooner the object is incorporated into the background. Default is 1.
3. Minimum Target Size	This parameter determines the minimum size of a detection box. Targets with a detection box smaller than this value will result in their box not being displayed in live view. Default is 1.
4. Displacement Constraint for Target Generation	This parameter determines the amount of analysis done when generating the detection box around a target. The higher the value, the more accurate the analysis. Default is 1.
5. Optical Axis Movement	If the target is far away from the camera and its movement is unclear, use this parameter to check the target's movement. The higher the value, the greater the analysis done on the target's movement. Default is 2. It is recommended to use a lower value so that a detection box is more quickly generated and triggers an alarm.

6. Single Alarm	If there is more than one target in the same detection box, a continuous alarm will be triggered. To avoid this occurring, enable the parameter so only one alarm is triggered. Default is Enabled.
7. Scene Mode	There are two options, General or Leaves Interfered View. Use Leaves Interfered View if there are shaking items in view such as leaves. Default is General.
8. Restore Defaults	Restore the defaults values of the VCA configuration parameters.
9. Restart VCA	Restart the VCA function.

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

Temperature measurement setup

The camera can measure the actual temperature of a point/line/frame being monitored. The camera triggers an alarm when the temperature exceeds the defined temperature threshold value.

It is recommended not to use the VCA or the temperature measurement functions at the same time.

You can configure the camera to measure temperature automatically and manually.

Notes:

- The target surface should be as vertical to the optical axis as possible. It is recommended that the angle of the oblique image plane should be less than 45°.
- The target image pixels should be more than 5×5 .
- If you use multiple presets for temperature measurement, it is recommended to set the preset tour time greater than 20 s.
- Use line or area thermal imaging when measuring the temperature of a specific area. It is not recommended to use point thermal imaging in case the camera moves as this may impact the accuracy of the temperature measurement.

Automatic thermal imaging

Thermal imaging information automatically appears on screen in live view. When setting up the camera for automatic thermal imaging measurement, you need to do the following steps:

- Set up the parameters for thermal imaging. See below.
- Define the overall temperature range (minimum, maximum, and average) to be displayed in the camera image. No specific targets are defined. See page 82.
- Define the alarm rules for point, line, and area thermal-imaging targets. An alarm is triggered when these rules are met. See page 85.
- Define areas in the camera image to be excluded from temperature detection. See page 89.

The instructions for each step are explained below.

Set up thermal imaging parameters

Configure the thermal imaging parameters. These let you select what thermal information is displayed on screen and how it is displayed.

To set up the parameters for thermal imaging:

1. From the Configuration panel, click **Configuration > Local Configuration**. To ensure that temperature information is displayed:

Enable **Display Temperature Info**.

Enable **Display Rules Info on Capture**.

Click **Save** to save changes.

2. From the Configuration panel, click **Configuration > Temperature Measurement > Basic Settings**.

The screenshot displays the TruVision IP Camera configuration web interface. The top navigation bar includes 'Live View', 'Playback', 'Snapshot', 'Log', and 'Configuration' (highlighted in green). The left sidebar lists 'Local Configuration' categories: System, Network, Video/Audio, Image, Event, Storage, VCA, and 'Temperature Measurement' (highlighted in green). The main content area is titled 'Basic Settings' and includes tabs for 'Basic Settings', 'Advanced Settings', 'Shield Region', and 'Actions'. Under 'Basic Settings', the following parameters are visible: Channel No. (Camera 02), Enable Temperature Measurement (checkbox), Enable Color-Temperature (checkbox), Display Temperature Info. on Stream (checked), Display Temperature in Optical Channel (checkbox), Display Max. Temperature (checked), Display Min. Temperature (checkbox), Display Average Temperature (checkbox), Position of Thermometry Info (Near Target), Add Original Data on Capture (checkbox), Add Original Data on Stream (checkbox), Data Refresh Interval (3 s), Unit (Degree Celsius(°C)), Temperature Range (-20.0~150.0), Version (V2.0.10build20210104), Calibration File Version (V1.0.0.0 build210610), and Alarm Interval (3 s). Below these are sections for 'Reflect Light Filter' and 'Forklift Filter', each with an 'Enable' checkbox, a 'Sensitivity' slider (set to 50), and a 'Restart VCA' button. A 'Save' button is located at the bottom of the configuration area.

Note: The parameters available depend on the camera model.

3. Select the parameters:

Function	Description
Enable Temperature Measurement	Select to enable temperatures to be measured.
Enable Color Temperature	Select to display the temperature color bar in live view. The bar appears on the right side of the thermal image. However, its color shading is not represented in the point/line/area items displayed on screen.
Display Temperature Info on Stream	Select to display the temperature information on stream.
Display Temperature in Optical Stream	Select to display the thermal channel temperature information on the optical channel.
Display Max. Temperature	Select to display the maximum temperature information in live view when the temperature measurement rule is Line or Area.
Display Min. Temperature	Select to display the minimum temperature information in live view when the temperature measurement rule is Line or Area.
Display Average Temperature	Select to display the average temperature information in live view when the temperature measurement rule is Line or Area.
Position of Thermometry Info	Select where the thermal information will be displayed on screen. Select Near Target or Top Left . "Near Target" displays the information beside the temperature measurement rule. "Top Left" displays the information on the top left of the screen.
Add Original Data on Capture	Select to add alarm-triggered data from the thermal camera.
Add Original Data on Stream	Select to add original data on the thermal view.
Data Refresh Interval	Enter a value in for the refresh time in seconds on the temperature information.
Unit	Select how the temperature will be shown: Celsius, Fahrenheit, or Kelvin.
Temperature Range	Select the desired temperature range from the drop-down list.
Version	View the current version of the algorithm.
Calibration File Version	View the version of the calibration file.
Alarm Interval	Enter the interval between alarms in seconds.
Reflect Light Filter.	To avoid false alarms if there is strong reflected light, adjust the sensitivity level and click Restart .
Enable Forklift Filter	Enable to avoid false alarms if forklift trucks operate in the area.

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

Display the overall temperature range of the camera image

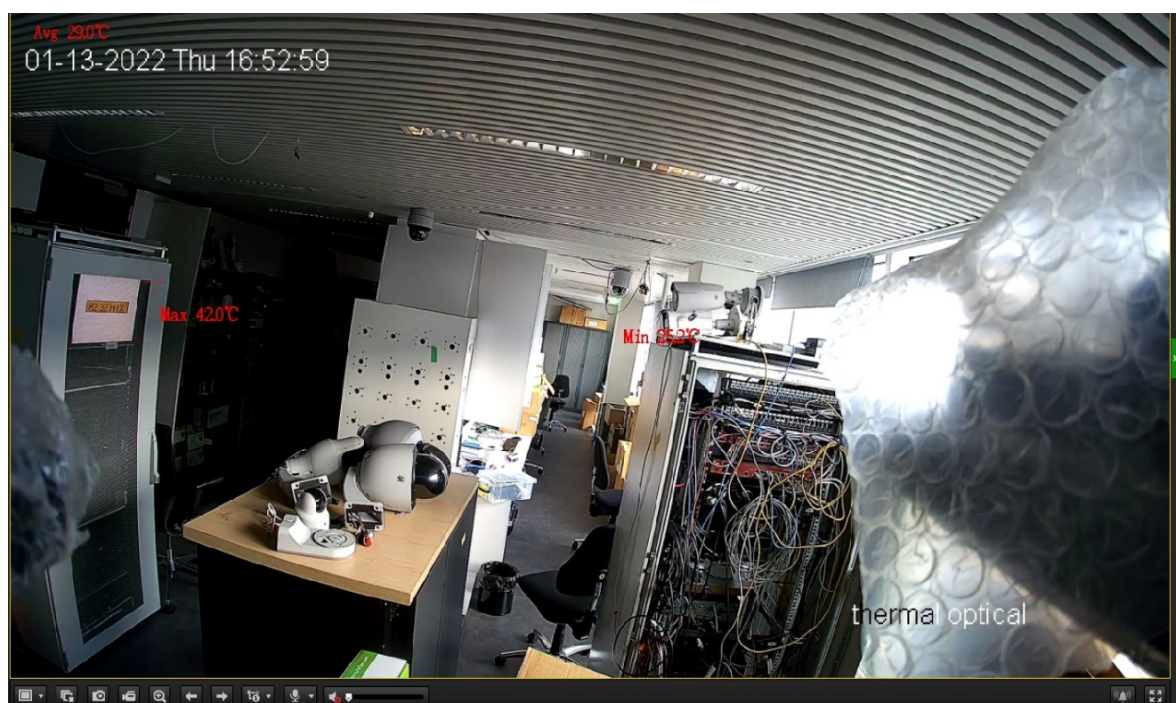
The Normal configuration menu lets you define how to display the temperature range on the camera image. It shows the maximum, minimum and average temperatures. It also lets you select where the average temperature information is displayed on screen.

The maximum and minimum temperatures are displayed where these temperatures occur.

The color of the temperature text depends on whether the pre-alarm or alarm temperature thresholds have been triggered.

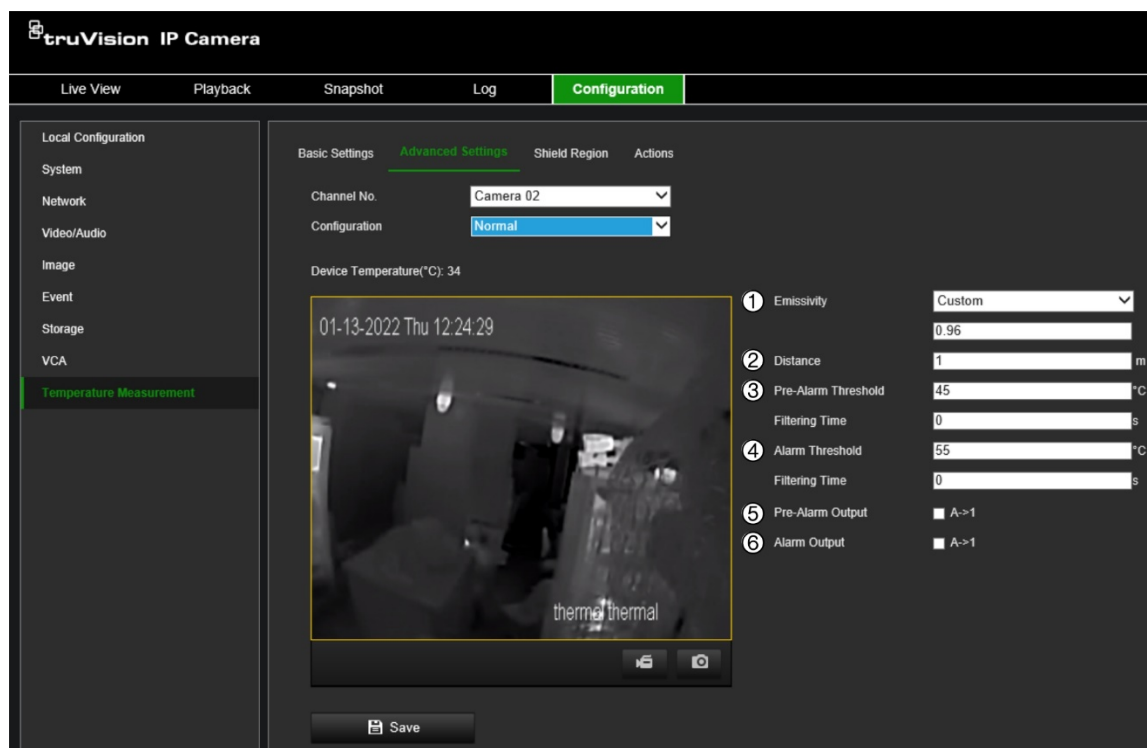
- **Green text:** No area in the camera image has triggered a pre-alarm or alarm temperature.
- **Yellow text:** The pre-alarm temperature threshold has been triggered.
- **Red text:** The alarm temperature threshold has been triggered.

Figure 9: An example of the overview of the temperature range in a camera image



To measure the temperature of the camera image and alarms:

1. From the Configuration panel, click **Configuration > Temperature Measurement > Advanced Settings**.



2. Select the camera and **Normal** configuration.
3. Select the parameters:

Function	Description
1. Emissivity	Select the emissivity of the camera scene from the drop-down list.
2. Distance	Enter the distance in meters from where to measure the temperatures. The camera will display the areas on screen that have the maximum and minimum temperatures as well as display the average temperature.
3. Pre-alarm Threshold	Enter the pre-alarm temperature. A pre-alarm is triggered when the temperature of an area in the camera image exceeds the pre-alarm threshold, and that this status is maintained for longer than the filtering time. When triggered, all temperatures are displayed in yellow.
4. Alarm Threshold	Enter the alarm temperature. An alarm is triggered when the temperature of an area in the camera image exceeds the alarm threshold, and that this status is maintained for longer than the filtering time. When triggered, all temperatures are displayed in red.
5. Pre-alarm Output	Select to link the pre-alarm to the connected device.
6. Alarm Output	Select to link the alarm to the connected device.

Click **Save** to save changes.

4. Click the **Actions > Arming Schedule** to set the arming schedule. By default, the schedule is set to 24 hours for each day. To change the schedule, drag the start or end of the schedule bar to the desired time.

Click **Actions** to select the linkage method by which you want the camera to notify you of the alarm. The options are:

Normal Linkage	This is a group selection. It automatically selects “Send Email”, “Notify Alarm Recipients”, “Upload to FTP/Memory Card/NAS”, “Flashing Alarm”, and “Audible Warning”.
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 “Email” on page 23 for further information. If you want to send the alarm 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 68 for further information. To upload the snapshot to an FTP, you must first configure the FTP settings. See “FTP” on page 22 for further information. Enable the Upload Picture 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 “Enable Event-Triggered Snapshot” section on page 66 for further information.
Flashing Alarm	Trigger an LED on the camera to flash.
Audible Warning	Trigger an audible beep when an alarm is detected by the camera.
Trigger Recording	Trigger the recording to start in the camera.
A1	Trigger alarm input 1.
A2	Trigger alarm input 2.

Click **Save** to save changes

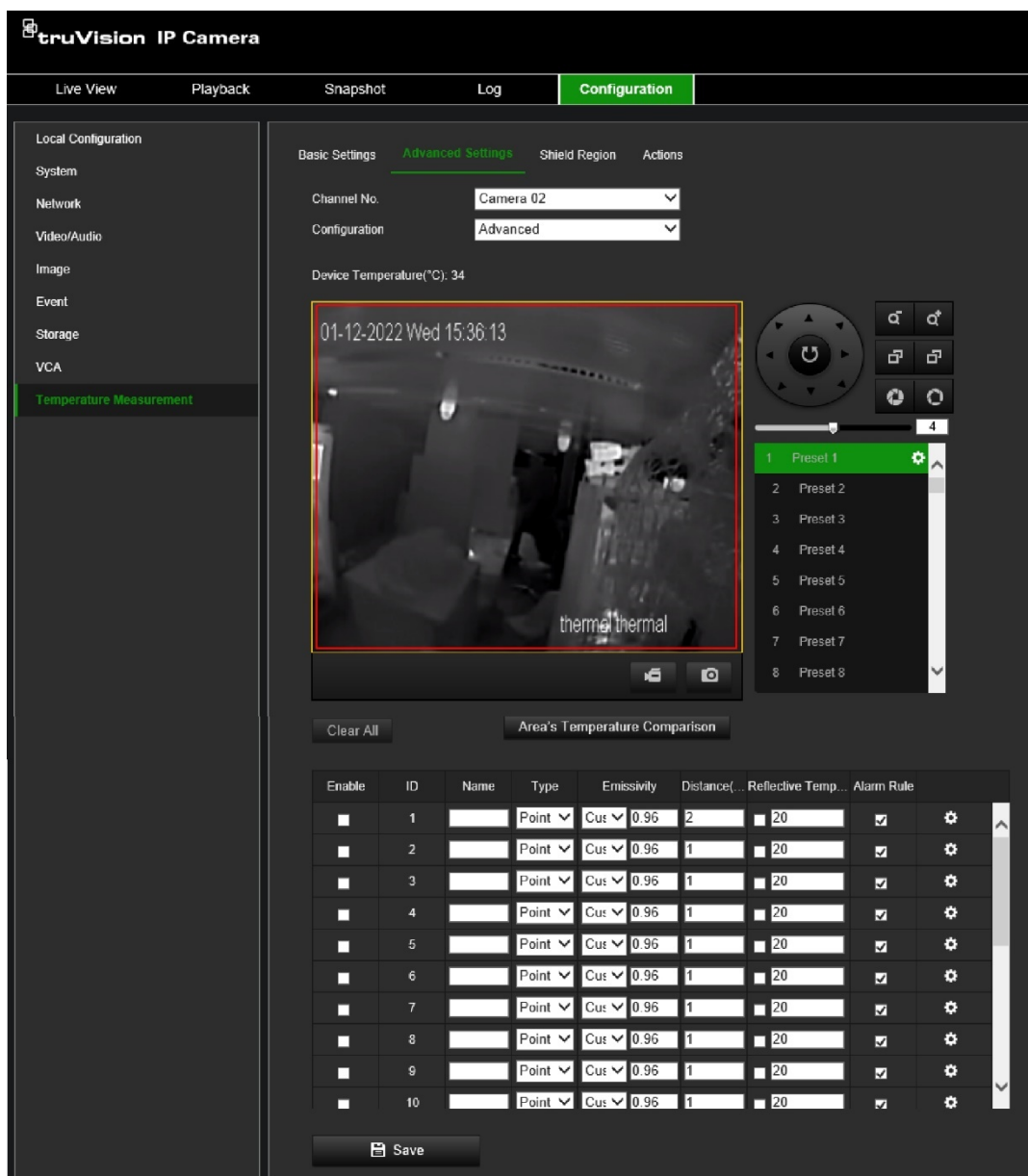
Note: To modify the fonts size and the temperature color of the average, alarm, and pre-alarm text, go to **Configuration > Image > VCA Rules Display** on page 53.

Create rules for point, line, and area thermal-imaging targets

You can set up the camera so that it can monitor the temperature of specific points, lines, or areas in the camera image.

To define the alarm rules for point, line, and area temperatures:

1. From the Configuration panel, click **Configuration > Temperature Measurement > Advanced Settings**. Select **Advanced**.



2. Select the channel number (1): normal (Camera 01) or thermal (Camera 02).
3. Set up the thermal imaging parameters. See “Set up thermal imaging parameters” on page 80 for more information.
4. To set up an alarm rule, enter a name for the rule in a field box.
5. Select the desired alarm rule type, Point, Line, or Area.

Point: A red cross appears in the live view viewer. Use the mouse to move this cross to the desired location.

Line: Left click two points on the live view viewer to draw the line.

Area: Left click three or more points to create an area on the live view viewer. Right click to stop adding a point to the area.

The position and size of the rule point/line/area in the live view viewer can be changed at any time. You can set up to 21 alarm rules.

Click an entry in an alarm rule to see the rule appear in the viewer.

6. Configure the temperature parameters for the rule.

Select the emissivity type. Different objects have different emissivity.

Enter the distance in meters in a straight line between the camera and the target.

Enter the reflective temperature. If an object has a high emissivity, check and set the reflective temperature to ensure the correct reflective temperature. The reflective temperature should be the same as the object's temperature.

7. Click the alarm rule button  to set up more temperature parameters.

Alarm Rule: Select **Above (Average Temperature)** or **Below (Average Temperature)**.

Alarm Temperature and Filtering Time: Enter the temperature that will trigger an alarm.

Pre-alarm Temperature and Filtering Time: Enter the temperature that will trigger an alarm.

Filtering Time: Enter the filtering time, which is the duration of time that the temperature reaches or exceeds the alarm or pre-alarm temperature. An alarm is triggered when the temperature exceeds the alarm/pre-alarm threshold, and that this status is maintained for longer than the filtering time.

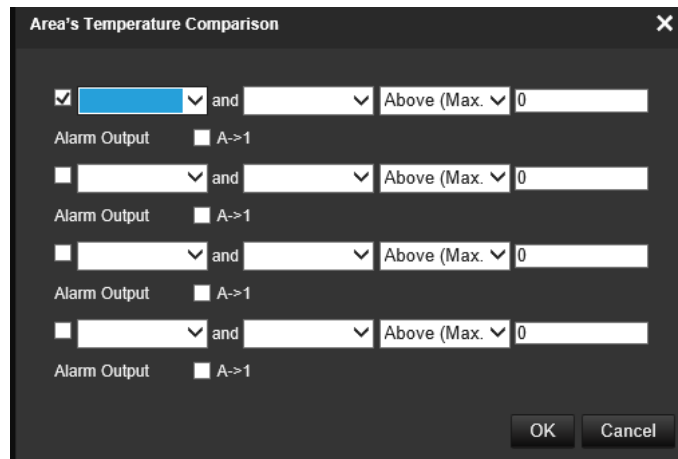
Tolerance Temperature: Enter the tolerance temperature. This is the temperature that the alarm temperature must vary to cancel the alarm. For example, if the alarm temperature is 35 °C and the tolerance temperature is 3 degrees, the alarm is cancelled when the temperature falls below 32 °C.

Set the tolerance temperature to prevent the constant temperature change to affect the alarm. E.g., set tolerance temperature as 3°C, set alarm temperature as 55°C, and set pre- alarm temperature as 50°C. The device sends pre-alarm when its temperature reaches 50°C and it alarms when its temperature reaches 55°C and only when the device temperature is lower than 52°C will the alarm be cancelled

Pre-alarm and Alarm Outputs: Select the alarm outputs to be triggered.

Click **OK** to save the changes.

8. Optional: Click the **Area's Temperature Comparison** button to set the alarm output rules for temperature.



Click **OK** to save the changes.

9. Click **Save** to save changes.
10. Repeat steps 4 to 9 for each rule.
11. Select the **Enable** check box to activate the rule. It can then appear in live view if live view is enabled to view the rules.
12. Click the **Actions > Arming Schedule** to set the arming schedule. By default, the schedule is set to 24 hours for each day. To change the schedule, drag the start or end of the schedule bar to the desired time.

Click **Actions** to select the linkage method by which you want the camera to notify you of the alarm. The options are:

Normal Linkage	This is a group selection. It automatically selects "Send Email", "Notify Alarm Recipients", "Upload to FTP/Memory Card/NAS", "Flashing Alarm", and "Audible Warning".
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 "Email" on page 23 for further information. If you want to send the alarm 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 68 for further information. To upload the snapshot to an FTP, you must first configure the FTP settings. See "FTP" on page 22 for further information. Enable the Upload Picture 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 "Enable Event-Triggered Snapshot" section on page 66 for further information.
Flashing Alarm	Trigger an LED on the camera to flash.
Audible Warning	Trigger an audible beep when an alarm is detected by the camera.
Trigger Recording	Trigger the recording to start in the camera.

A1	Trigger alarm output 1.
A2	Trigger alarm output 2.

Click **Save** to save changes

13. Optional: Call a preset to check if the rules work correctly. You can also take a snapshot or capture a clip of the view.

Note: To modify the fonts size and the temperature color of the average, alarm, and pre-alarm text, go to **Configuration > Image > VCA Rules Display** on page 53.

Exclude areas from temperature detection

You can conceal areas on screen from being detected.

To define areas to be excluded from temperature detection:

1. From the Configuration panel, click **Configuration > Temperature Measurement > Shield Region**.
2. Select **Enable Shield Area**.
3. Click  and drag the mouse in the live view viewer to draw the area. Up to four shield areas can be drawn.

To delete a shield area, select it and click .

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

Manual thermal imaging

You can easily see the actual thermal image temperature in live view.

To manually detect thermal image temperature in live view:

1. From the Configuration panel, click **Configuration > Local Configuration**. Select **Display Temperature Info**.

Click **Save** to save changes

2. From the Configuration panel, click **Configuration > Temperature Measurement > Basic Settings**. Select **Enable Temperature Measurement**.

Click **Save** to save changes

3. Go to **Live View** and under the PTZ menu select . Then click any area in the live view image to see the actual temperature displayed.

Camera operation

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

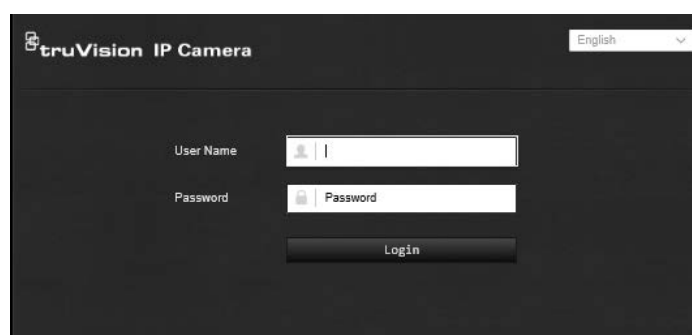
Login and Logout

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.

Note: When an incorrect user name or password has been entered, a message appears showing how many login attempts remain (“Incorrect user name or password. By default, the device will be locked after 3 failed login attempts.”). From a security perspective, we recommend that you to leave the default setting. However, login settings can be changed under **Configuration > System > Security > Security Service**.

You can change the language of the interface from the drop-down menu in the top right corner of the window.

Figure 10: Login dialog box



Live view

Once logged in, click **Live View** on the menu toolbar to access live view mode. See Figure 11 on page 91 for the complete description of the interface.

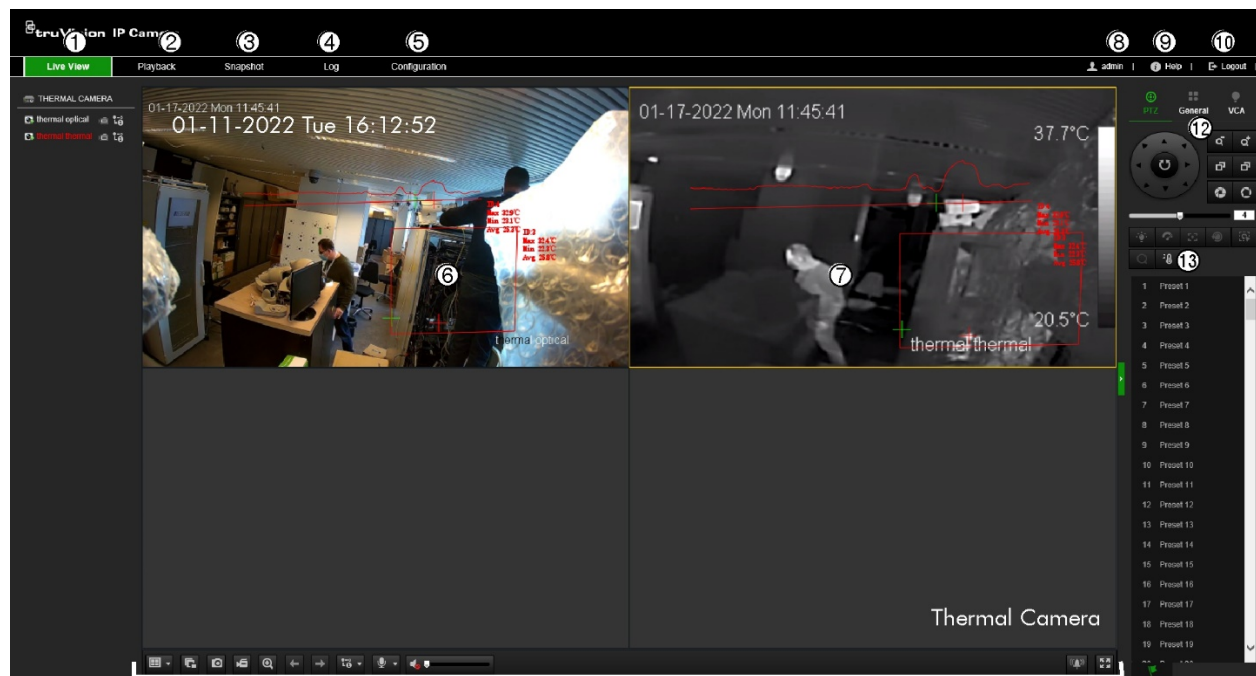
Although there is only one thermal camera connected, you will see two images on screen. The image on the left is the normal non-thermal image and that on the right is the thermal image. They both show identical thermal imaging information.

The thermal imaging information displayed on screen depends on the Live View parameter settings under “Local configuration” on page 12:

- Display Rule information
- Display Temperature information
- Display Trajectory

For the VCA image information displayed, see “Basic settings” on page 70.

Figure 11: Web browser window: Live view shown



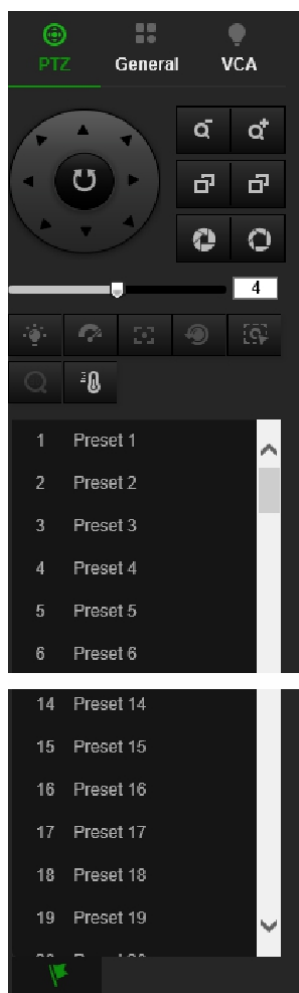
11

	Name	Description
1.	Live view	Click to view live video.
2.	Playback	Click to play back video.
3.	Snapshot	Click to search snapshots.
4.	Log	Click to search for event logs. There are three main types: Alarm, Exception, and Operation.
5.	Configuration	Click to display the configuration window for setting up the camera.
6.	Normal image	View the normal live video image.
7.	Thermal image	View the thermal live video image.
8.	Admin	Displays current user logged on.
9.	Help	Click to find function.
10.	Logout	Click to log out from the system. This can be done at any time.
11.	Live view toolbar	 Click to switch between the different multiview options from the drop-down list: 1x1, 2x2, 3x3, 4x4.  Click to start/stop live view.  Click to manually capture the snapshot and stored it in the directory configured.  Click to manually start/stop recording and stored it in the directory configured.  Click to start/stop digital zoom function.  Click to move to previous page.  Click to move to next page.  Live view with main stream or substream.  Turn on/off microphone.

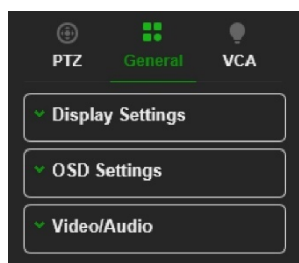
Name	Description
	Audio on and adjust Volume/Mute.
	Manually activate camera alarm output (green when enabled).
	Full screen.

12. PTZ / General / VCA Configuration options for PTZ, General, and VCA. They can be changed from the live view menu if the user permission allows this. See more details below.

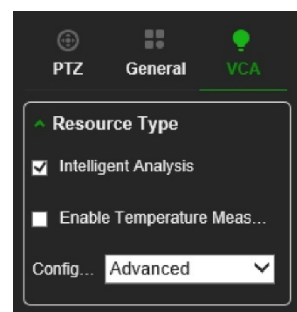
PTZ control panel



General control panel



VCA control panel



13. Temperature icon Click a point on screen to see its actual thermal image temperature. This icon only appears when the thermal image is selected. See “Manual thermal imaging” on page 89 for more information.

Display thermal imaging information in live view

The instructions below assume that you have set up both normal and advanced temperature measurement settings (see “Automatic thermal imaging” on page 80 for more information).

To display temperature measurements on screen, ensure that:

- **Configuration > Local Configuration > Display Temperature Info** is enabled.

- **Configuration > Temperature Measurement > Basic Settings > Enable Temperature Measurement** is enabled.

To display no thermal imaging information:

1. From the Configuration panel, click **Configuration > Temperature Measurement > Basic Settings**. Deselect **Display Temperature Info. On Stream** and deselect **Display Temperature in Optical Channel**.
2. Click **Save** to save changes.

To display the maximum, minimum and average thermal imaging information in the live view:

1. From the Configuration panel, click **Configuration > Temperature Measurement > Advanced Settings**. Under Configuration, select **Normal** and click **Save**.

To display the advanced thermal imaging information only in the normal image of live view:

1. From the Configuration panel, click **Configuration > Temperature Measurement > Basic Settings**. Deselect **Display Temperature Info. On Stream** and click **Save**.
2. From the Configuration panel, click **Configuration > Temperature Measurement > Advanced Settings**. Under Configuration, select **Advanced** and click **Save**.

To display the advanced thermal imaging information only in the thermal image of live view:

1. From the Configuration panel, click **Configuration > Temperature Measurement > Basic Settings**. Deselect **Display Temperature in Optical Channel** and click **Save**.

To display the temperature distribution in the thermal image of live view:

1. From the Configuration panel, click **Configuration > Temperature Measurement > Basic Settings**. Deselect **Display Temperature Info. On Stream** and click **Save**.
2. From the Configuration panel, click **Configuration > Temperature Measurement > Advanced Settings**. Under Configuration, select **Advanced** and click **Save**.

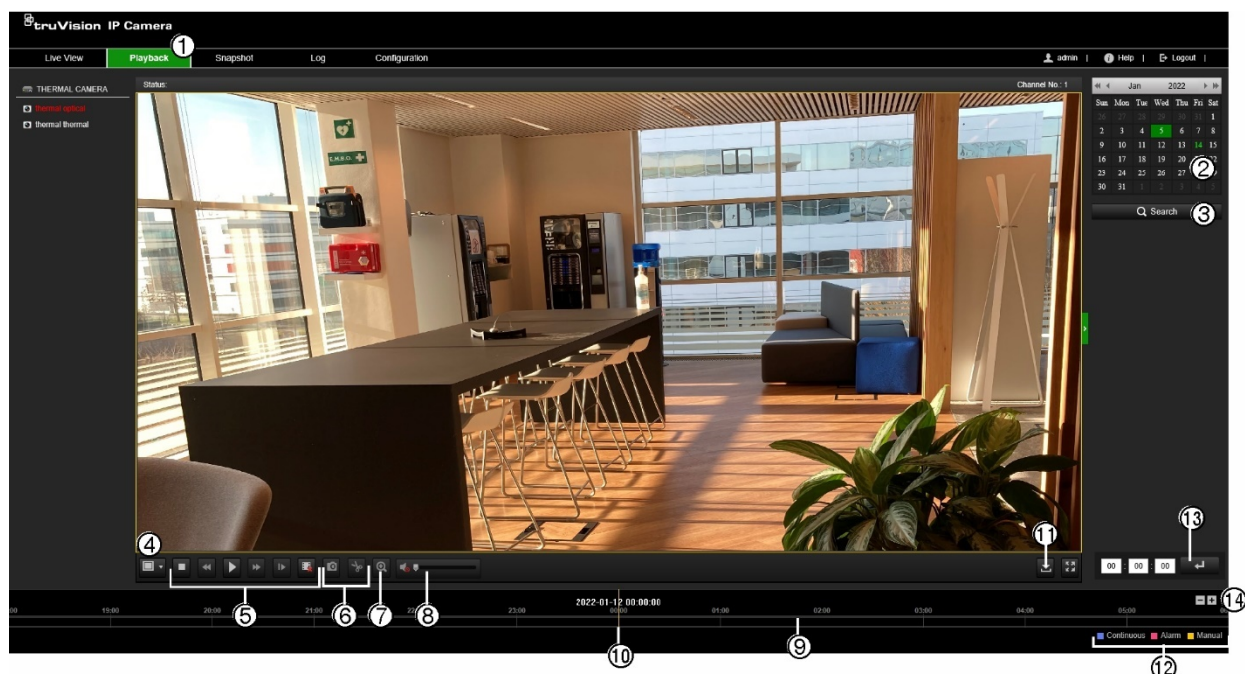
Playing back recorded video

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 12 on page 94.

Figure 12: 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. Multiview	Switch between the different multiview options from the drop-down list.
5. Control playback	Click to control how the selected file is played back: play, stop, slow, and fast forward playback as well as start and stop.
6. 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.
7. Digital zoom	Zoom in and out of the selected camera image.
8. Audio control	Modify the audio level.
9. 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.
10. Time bar	The time 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.
11. Download functions	 Download video files.
12. Recording type	The color code displays the recording type. Recording types are continuous recording, alarms recording, and manual recording.
13. Zoom in/out	Click to zoom in or out of the timeline.

Name	Description
14. 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 a camera as well as the date. 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 displays the type and time of the recording. The timeline can be manually scrolled using the mouse.

Note: You must have viewing log access rights to search and view logs. See “Capture (Scheduled snapshots)” on page 64 to permit to search and view logs.

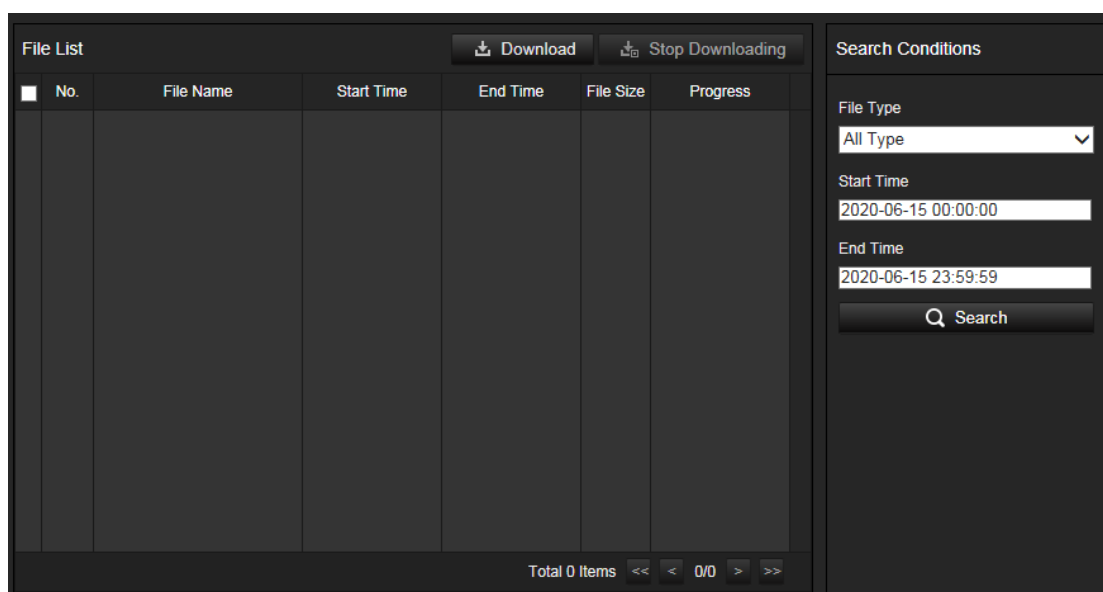
4. Select the date and click the **Search** button to search for the required recorded file.
5. In the pop-up window, select the check box of the video file and click  to download the video files.

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 video files:

1. Click  to open the recorded file search window.



2. Select the file type and set start and end time.
3. Click **Search** to search for the recorded video files.

4. Select the desired video files and click **Download** to download them. Downloading files from a NAS or SD card can take some time. A progress bar will be displayed to indicate the download progress.

Snapshot

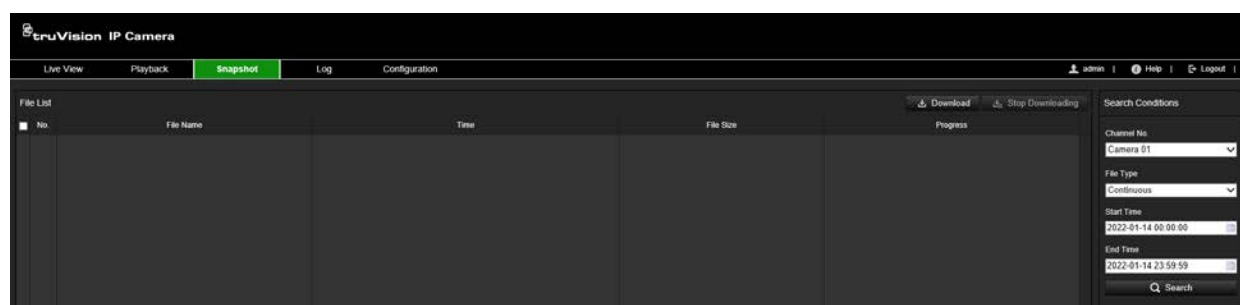
Click **Snapshot** on the menu toolbar to enter the window to search for snapshots. You can search, view, and download the pictures stored in the NAS or memory card storage.

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 > Record Settings > Capture** to set the capture schedule. See “Capture (Scheduled snapshots)” on page 64.

To search recorded snapshots:

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



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

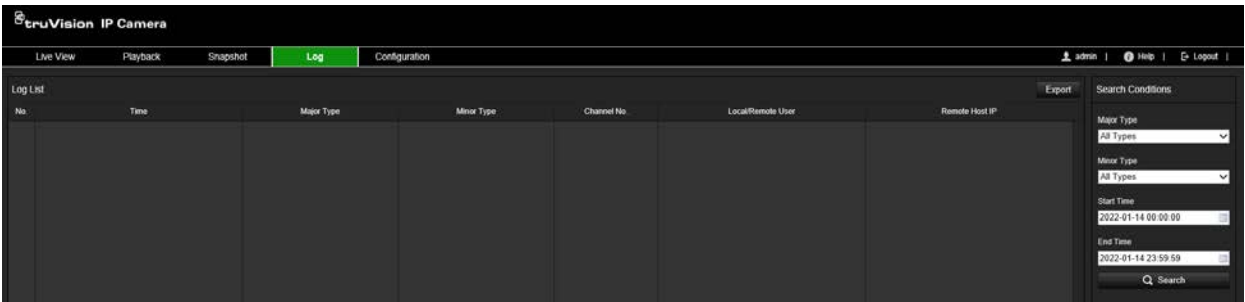
Log

You must configure NAS or install a SD card in the camera to be able to search for log events from the camera.

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 will start overwriting older logs. To view log events stored on storage devices, click **Log** on the menu toolbar to open the log menu.

Note: You must have viewing log access rights to search and view logs. See “Capture (Scheduled snapshots)” on page 64 to permit to search and view logs.

Figure 13: Log window



You can search for recorded log events by the following criteria:

Major Type: There are three types of logs: Alarm, Exception, and Operation. You can also search All.

Minor Type: Each major type has some minor types that can help to refine your search.

Start Time and End Time: Set the time window in which you want to search for log events.

To search logs:

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

Index

8

802.1x parameters
set up, 26

A

Archive files, 94

C

Camera name
display, 49
Configuration file
export, 33
import, 33

D

Date format set up, 49
DDNS parameters
set up, 15
Default settings
restore, 32
Defective pixel correction, 52
Display information
set up, 49
DPC, 52

E

Email
link to motion detection, 61
Email parameters
set up, 23
Events
search logs, 95

F

fifth topic
subdivision one, 70, 74
subdivision two, 73, 74
Firmware upgrade, 33
FTP parameters
set up, 22

H

Hard drive
capacity, 67
formatting, 67
HTTP listening parameters
set up, 28
HTTPS parameters
set up, 24

I

Integration protocol parameters
set up, 26

L

Language
change, 89
Log on and off, 89
Logs
information type, 96
search, 95
security audit log, 36
viewing, 95

M

Multicast parameters
set up, 19

N

NAS management, 68
NAT parameters
set up, 18
Network service parameters
set up, 27
NTP synchronization, 30

P

Password activation, 8
Picture overlay, 51
Playback
play back recorded files, 94
screen, 92
searching recorded video, 92
Port parameters
set up, 17
Post-recording times
description, 63
PPPoE parameters
set up, 17
Pre-recording times
description, 63

Q

QoS parameters
set up, 25

R

Reboot camera, 32
Recording
playback, 92
Recording settings, 62

S

- SD card
 - capacity, 67
- SDHC card
 - format, 67
- Search
 - events, 95
 - logs, 95
- Security audit log, 36
- Snapshots
 - archive, 94
 - event-triggered snapshots, 64
 - scheduled snapshots, 64
- SNMP parameters
 - set up, 20
- System time
 - set up, 30

T

- TCP/IP parameters
 - set up, 14
- Temperature measurement
 - set up, 79
- third topic
 - subdivision two, 50
- Time format set up, 49

V

- Video clips
 - archive, 94

W

- Web browser
 - interface overview, 11

