



TruVision S02 Series Panoramic 360° Camera Configuration Manual

Copyright
Trademarks and
patents

© 2025 Aritech. All rights reserved.

TruVision and associated names and logos are a product brand of Aritech, a part of Kidde Global Solutions.

Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.

Manufacturer

KGS Fire & Security Australia Pty Ltd
Suite 4.01, 2 Ferntree Place, Notting Hill, VIC 3168 Australia

Certification



Product warnings and
disclaimers



THESE PRODUCTS ARE INTENDED FOR SALE TO AND INSTALLATION BY QUALIFIED PROFESSIONALS. KGS 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://aritech.com.au/aritech-product-warranty/> or scan the following code:

Contact information

EMEA: <https://firesecurityproducts.com>

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

Product
documentation



Please consult the following web link to retrieve the electronic version of the product documentation.

Content

Important information#iii

Limitation of liability#iii

Product warnings#iii

Warranty disclaimers#iv

Intended use#v

Advisory messages#v

Introduction#1

Product overview#1

Contact information and manuals/firmware#1

Network access#2

Internet Explorer – Checking the browser security level#2

Activating the camera#3

Using non-Internet Explorer web browsers (plugin-free browsers)#5

Enabling IE mode in Microsoft Edge#6

Overview of the camera web browser#7

Camera menu structure#8

Configuration#9

Common settings#9

Local#9

Configuration menu overview#11

System#12

Network#18

Video/Audio#31

Image#34

Storage#41

Event#48

Maintenance and Security#64

Maintenance#64

Security#70

VCA Configuration#77

People Management#78

People Counting#83

Smart Event#86

Camera operation#95

Login and Logout#95

Live view#95

Playback#97

Application Data#99

Important information

Limitation of liability

To the maximum extent permitted by applicable law, in no event will Kidde 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 Kidde 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 Kidde 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, Kidde 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 KIDDE PRODUCTS, SOFTWARE OR SERVICES TO WORK PROPERLY DEPENDS ON A NUMBER OF PRODUCTS AND SERVICES MADE AVAILABLE BY THIRD PARTIES OVER WHICH KIDDE HAS NO CONTROL AND FOR WHICH KIDDE 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 KIDDE, MAY BE HACKED, COMPROMISED AND/OR CIRCUMVENTED AND KIDDE 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.

KIDDE 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 the battery is replaced by an incorrect type. Dispose of batteries according to the instructions. Contact your supplier for replacement batteries.

Warranty disclaimers

KIDDE 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.

KIDDE 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 ANY WAY PREVENT DEATH, PERSONAL INJURY, PROPERTY DAMAGE, OR LOSS OF ANY KIND WHATSOEVER.

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

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

KIDDE 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

KIDDE 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 KIDDE 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 KIDDE.

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 camera models:

TVPA-S02-0601-360-G: TruVision 360° IP camera, 6MP, 360° fisheye lens

TVPA-S02-1201-360-G: TruVision 360° IP camera, 12MP, 360° fisheye lens

You can download the firmware and the following manuals from our website:

- TruVision S02 Series Panoramic 360° Camera Installation Guide
- TruVision S02 Series Panoramic 360° Camera Configuration Manual

Contact information and manuals/firmware

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

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

Network access

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

TruVision IP cameras can be configured and 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, due to the increased security measure, you cannot download data, such as video and images. Consequently, you should check the security level of your PC so that you can 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 website 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** on 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, 10, and 11 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.

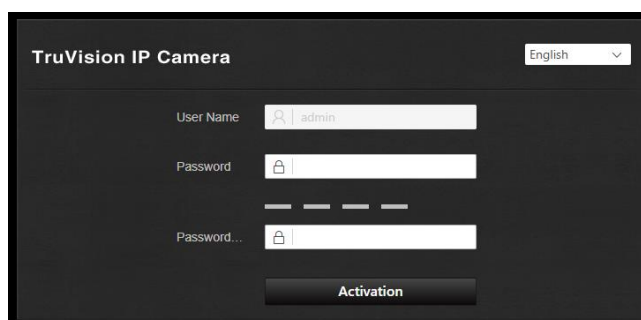
Activating the camera

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:

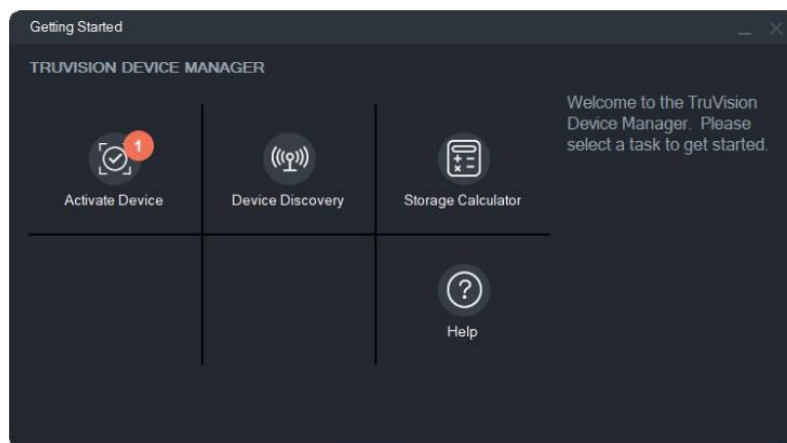
- Between 8 and 16 characters
- At least 1 lowercase letter
- At least 1 uppercase letter
- At least 1 of the following special characters _ : - , . * & @ / \$? Space.

We 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 9.3* 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 the following special characters : _ - , . * & @ / \$? Space.
- The password is case-sensitive.

We 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. Change the device IP address, subnet mask and gateway, or select 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.

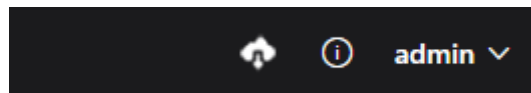
A pop-up window appears to confirm the activation. If activation fails, confirm that the password meets the requirements and try again.

The screenshot displays the network configuration page of a TruVision camera. At the top, there are tabs for 'TCP/IP', 'DDNS', 'PPPoE', 'SNMP', '802.1X', and 'QoS'. The 'TCP/IP' tab is selected. Below the tabs, the 'NIC Type' is set to 'Auto'. A 'DHCP' toggle switch is turned off. The 'IPv4' section includes fields for 'Device IPv4 Address' (192.168.1.70), 'IPv4 Subnet Mask' (255.255.255.0), and 'IPv4 Default Gateway' (192.168.1.1), each with a 'Test' button. The 'IPv6 Mode' is set to 'Route Advertisement', with options for 'Manual', 'DHCP', and 'Route Advertisement'. Below this, there are fields for 'Device IPv6 Address', 'IPv6 Subnet Mask', and 'IPv6 Default Gateway'. The 'MAC Address' is displayed as '9c:f6:1a:ba:cc:2a'. At the bottom, the 'MTU' is set to '1500'.

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

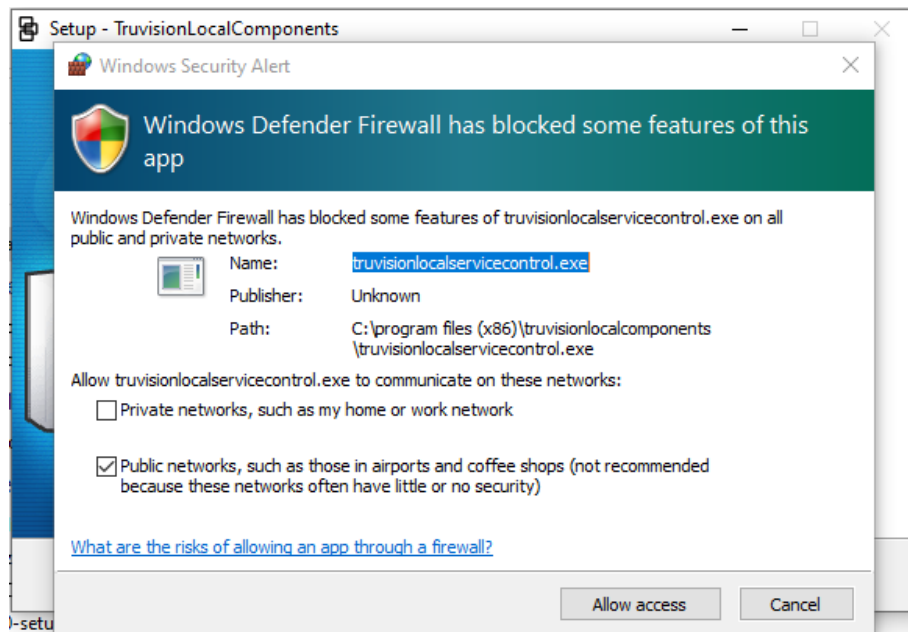
Plugin-free browsers such as Google Chrome, Mozilla Firefox, Microsoft Edge, and Apple Safari have limitations compared to Internet Explorer which uses ActiveX plugins. To solve this, an additional plugin can be downloaded through the camera live view web page. Please note that an internet connection 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” cloud icon at the top right of the camera Live View web page to download the plugin installation file to your PC.

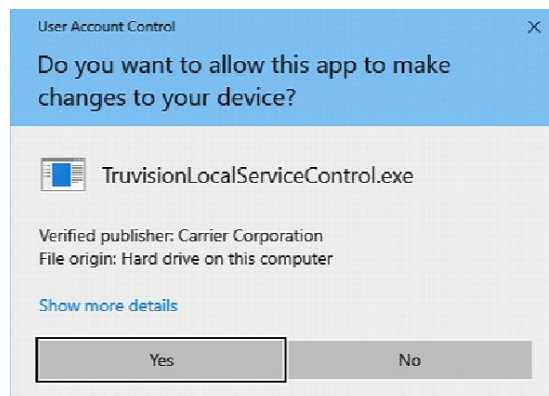


Close the browser and install the downloaded plugin *TruVisionLocalComponents.exe* on your PC. Once the plugin is installed, you can reopen the browser to view and configure the camera.

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



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



Enabling IE mode in Microsoft Edge

For the best compatibility of this camera with the Microsoft Edge browser, you must enable IE compatibility mode. Using this mode allows you to open certain websites in IE mode within Edge.

To use Microsoft IE mode in Edge:

1. Open Microsoft Edge.
2. Click on the three dots in the top right corner of the window.
3. Select **Settings** from the drop-down menu.
4. Click **Default browser**.
5. Go to **Allow sites to be reloaded in Internet Explorer mode (IE mode)** and click **Allow**.
6. Restart Edge.

7. Click on the three dots in the top right corner of the window.
8. Select **Reload in Internet Explorer mode** from the dropdown menu.
9. Type in the URL of the website you want to open in IE and press Enter.

The website will open in a new tab within Edge, but it will be rendered using the IE engine.

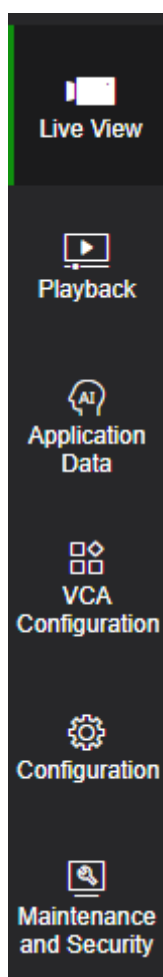
Overview of the camera web browser

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 1, "Example of the Local configuration window", on page 10 for an example.

Camera menu structure

After login, the camera web interface shows six main menu options that allow you manage the camera. The different menus are explained in more detail further in this document.

Main menu - Camera



Live View allow you to stream live images from the camera and perform other actions like PTZ, snapshot, real-time recording etc.

Via **Playback** you can search for recorded video. This function only works when SD card or NAS storage is used.

Application Data can generate statistics regarding certain specific camera features.

VCA Configuration allows you to configure smart events like Line crossing, Intrusion zone detection, etc.

The Configuration section contains all configurable parameters. Only admin users can edit settings in this menu.

Via **Maintenance and Security**, you can update the camera, import/export configuration and other maintenance tasks.

Configuration

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

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

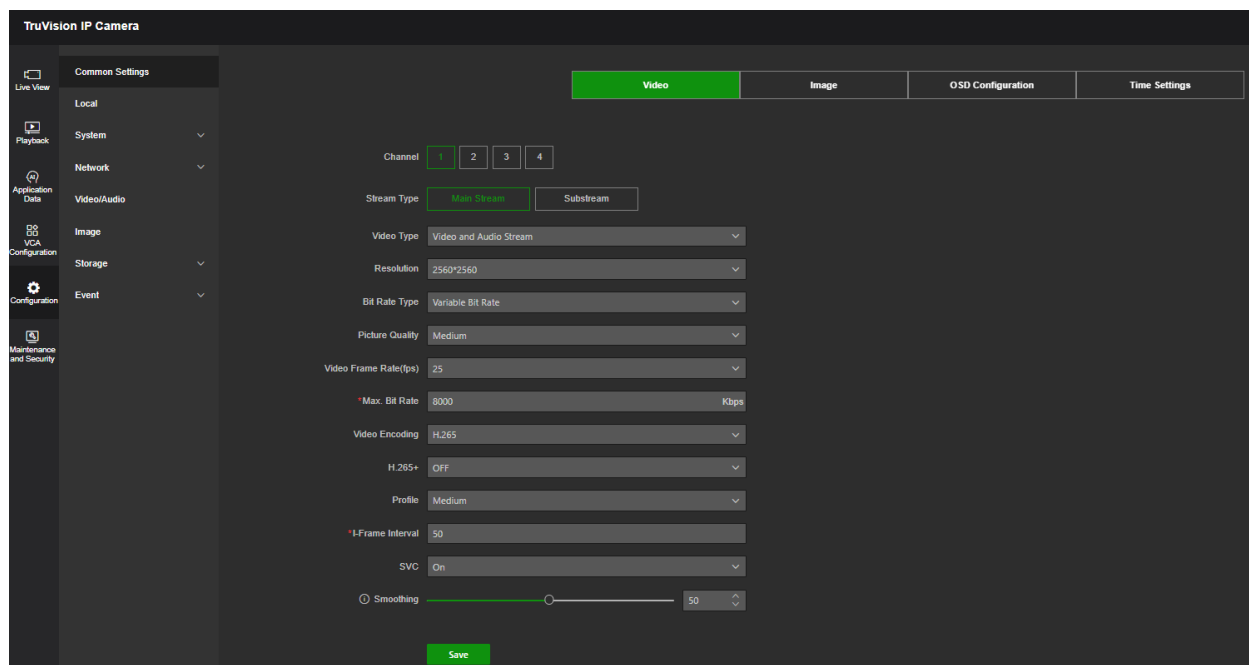
The camera web browser lets you configure the camera remotely using your PC. Web browser options may vary depending on the camera model.

There are three sections in the configuration panel:

- Common settings
- Local
- Configuration (System, network, video/audio, etc.)

Common settings

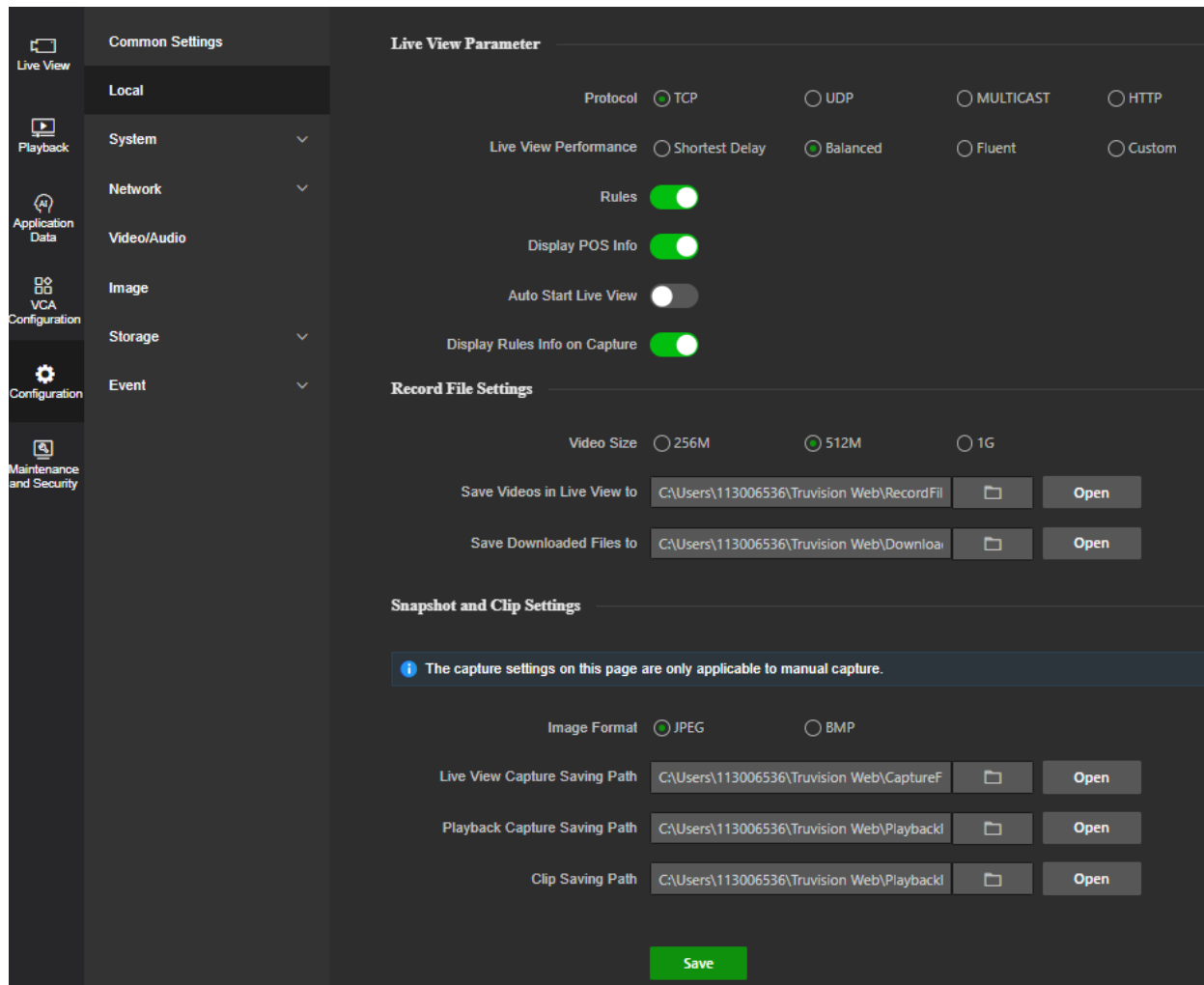
The Common settings section provides direct access to some of the settings that can be found in the main configuration sections. From here you have direct access to common settings like Video, Image, OSD Configuration, and Time Settings.



Local

Use the Local 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** to display the local configuration window. See Figure 1 on page 10 for descriptions of the different menu parameters.

Figure 1: Example of the Local configuration window



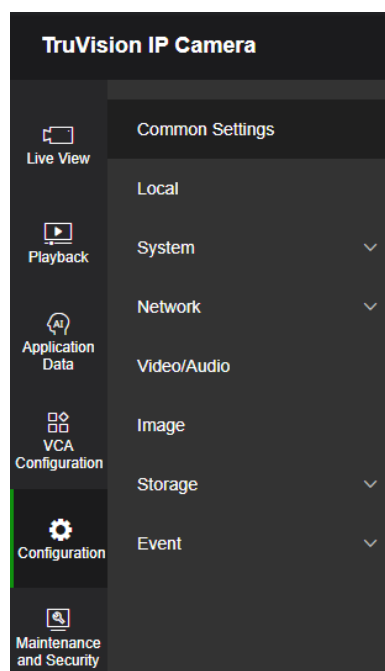
Parameters	Description
Live View Parameters	
1. Protocol	Specify the network protocol used. Options include TCP, UDP, MULTICAST, and HTTP.
2. Live View Performance	Specify the transmission speed. Select one of the options: Shortest Delay: Real-time video has priority over video fluency. Balanced: The device ensures both real-time video and fluency. Fluent: Video fluency has priority over real-time video. In a poor network environment, the camera cannot ensure video fluency even if this option is enabled. Custom: Set the frame rate manually. In a poor network environment, reducing the frame rate improves the fluency of live view. However, the rule information may not be displayed.
3. Rules	It refers to the rules on your local browser. Specify whether to display the colored marks when motion detection, face detection, and intrusion detection are triggered. For example, when the rules option is enabled and an object of interest is detected, it will be marked with a green rectangle in live view.

Parameters	Description
4. Display POS Info	Enable external data to be displayed as text overlay on camera image (currently not used)
5. Auto Start Live View	Enable to automatically open camera streams after login
6. Display Rules Info. on Capture	Enable to display the rules information on a captured image.
Record File Settings	
7. Video Size	Specify the maximum file size. Options include 256 MB, 512 MB, and 1GB.
8. Save Videos in Live View to	Specify the directory for recorded files.
9. Save Downloaded Files to	Specify the directory for downloaded files.
Snapshot and Clip Settings	
10. Snapshot Format	Select the desired file format JPEG or BMP for snapshots.
11. Live View Capture Saving Path	Specify the directory for saving snapshots in live view mode.
12. Playback Capture Saving Path	Specify the directory for saving snapshots in playback mode.
13. Clip Saving Path	Specify the directory for saving video clips in playback mode.

Configuration menu overview

Use the Configuration panel to configure the server, network, camera, alarms, users, transactions, and other parameters such as upgrading the firmware. See Figure 2 below for descriptions of the configuration menus available.

Figure 2: Configuration menu overview



Configuration menus	Description
1. System	Displays device basic information including SN and the current firmware version, time settings, maintenance, and serial port parameters. You can only modify the device name and device number. See “System” below for further information.
2. Network	Defines the network parameters required to access the camera over a network. See “Network” on page 18 for further information on the setup.
3. Video/Audio	Defines recording parameters. See “Video/Audio” on page 31 for further information.
4. Image	Defines the image parameters, OSD settings, overlay text, and privacy mask. See “Image” on page 34 for further information on the setup.
5. Storage	Defines recording schedule, storage management, NAS configuration, and snapshot. See “Storage” on page 41 for further information on the setup.
6. Event	Defines Basic events motion detection, video tampering, alarm input/output, exception and Smart events Face detection, Intrusion detection, and Cross Line detection. See “Event” on page 48 for further information on the setup.

System

Manage system settings, perform maintenance-related tasks, as well as configure security, and user-related features.

System settings

System settings include an overview of system settings, date & time, and some other options.

Basic Information

This menu displays the hardware and firmware-related information of the device.

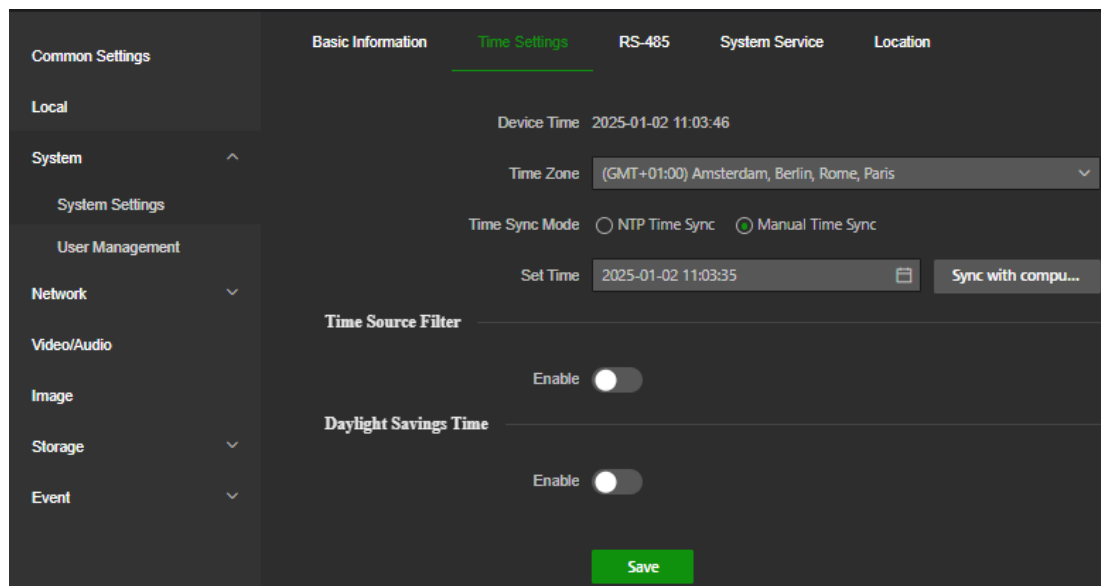
Common Settings	Basic Information	Time Settings	RS-485	System Service	Location
Local	Device Name	IP CAMERA			
System	*Device No.	88			
System Settings	Device Model	TVPA-S02-1201-360-G			
User Management	Serial No.	TVPA-S02-1201-360-G20240513AAWRFE1850527			
Network	Firmware Version	V30.1.2 Upgrade			
Video/Audio	Encoding Version	V7.3 build 230727			
Image	Web Version	V5.1.0.51_R0101 build 240920			
Storage	Number of Channels	4			
Event	Number of HDDs	0			
	Number of Alarm Inputs	2			
	Number of Alarm Outputs	2			
	Firmware Version Property	C-R-G7-0			
	Save				

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 shows the 'Time Settings' tab in a configuration interface. On the left is a sidebar with categories: Common Settings, Local, System, System Settings, User Management, Network, Video/Audio, Image, Storage, and Event. The main area displays 'Device Time' as 2025-01-02 11:03:46. Below this is a 'Time Zone' dropdown menu currently set to '(GMT+01:00) Amsterdam, Berlin, Rome, Paris'. The 'Time Sync Mode' has two radio buttons: 'NTP Time Sync' (unselected) and 'Manual Time Sync' (selected). A 'Set Time' field shows '2025-01-02 11:03:35' with a calendar icon and a 'Sync with compu...' button. There are two sections: 'Time Source Filter' with an 'Enable' toggle (currently off) and 'Daylight Savings Time' with an 'Enable' toggle (currently off). A green '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. Select one of the options for setting the time and date:

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

— OR —

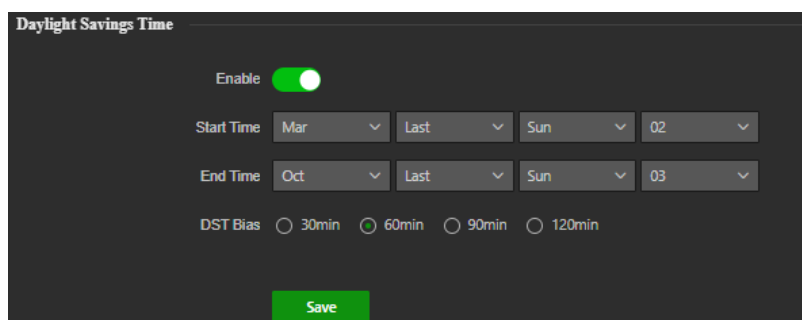
Set manually: Enable the **Manual Time Sync** function and then click  to set the system time from the pop-up calendar.

Note: You can also hit the **Sync with computer time** button to instantly synchronize the time of the camera with the time of your computer.

Time Source Filter:

Enabling the **Time Source Filter** allows you to create a block or allow list with time sync servers.

To define Daylight Saving Time (DST):

The screenshot shows the 'Daylight Savings Time' configuration window. It has an 'Enable' toggle switch which is turned on. Below this are two rows of dropdown menus for 'Start Time' and 'End Time'. The 'Start Time' row is set to 'Mar', 'Last', 'Sun', '02'. The 'End Time' row is set to 'Oct', 'Last', 'Sun', '03'. At the bottom, there are four radio buttons for 'DST Bias': '30min', '60min' (selected), '90min', and '120min'. A green 'Save' button is at the bottom.

1. Switch on **Enable** to enable the DST (Daylight Savings Time) function and set the dates of the DST period.
2. Click **Save** to save changes.

RS-485

RS-485 protocol and communication parameters can be set in this menu.

System Service

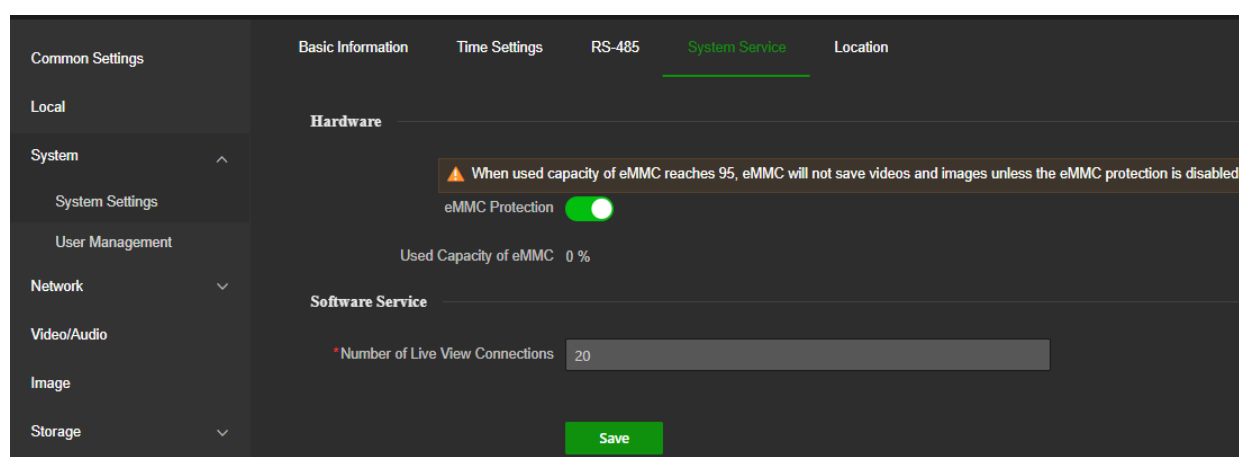
Hardware

eMMC Protection will automatically stop the use of eMMC as a storage media when its health status is poor.

eMMC, which stands for embedded Multimedia Card, is an embedded non-volatile memory system. It is able to store the captured images or videos of the device.

The device monitors the eMMC health status and turns off the eMMC when its status is poor.

Note: using a worn-out eMMC may lead to device boot failure.



Software Service

The **Number of Live View Connection** defines the maximum number of connections the camera allows. Supported values are from 1 to 20.

Location

Location displays and uploads the longitude and latitude of the device.

Check **Enable** and set **Location Upload Interval**. Enter the longitude and latitude of the device and click **Save**.

The device will upload the set location at the set interval.

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 the permissions and password of each user. See Figure 3 below.

Figure 3: User management menu

No.	User Name	User Type	User Status	Operation
1	admin	Administrator	Activate	
2	user01	Operator	Not Activated	
3	user02	User	Not Activated	

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

Note: Keep the admin password in a safe place. If you forget it, please use the Reset Password feature in TruVision Device Manager and contact Technical Support or reset the camera using the camera hardware reset button. Please be aware that by doing so, you will lose all configurations.

Types of users

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

- **Admin:** This is the system administrator. The administrator can configure all settings. Only the administrator can create and delete user accounts. The Admin user account cannot be deleted.
- **Operator:** This user can only change the configuration of his/her account. An operator cannot create or delete other users.
- **User:** This user has permission for 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 *Add user* window.

Add User

User Name *

User Type

Operator

Admin Password *

New Password *

Password Confirm *

Permission Configuration

- ☒ Select All
- ☐ Remote: Parameters Settings
- ☒ Remote: Log Search / Interro...
- ☐ Remote: Upgrade / Format
- ☒ Remote: Two-Way Audio
- ☐ Remote: Shutdown/Reboot
- ☐ Remote: Notify Alarm Recipie...
- ☐ Remote: Video Output Control
- ☐ Remote: Serial Port Control
- ☒ Remote: Live View
- ☒ Remote: Manual Record
- ☒ Remote: PTZ Control

OK Cancel

3. Enter a username.
4. Select the type of user from the **Level** drop-down list. The options are User and Operator.

5. Enter the Admin Password
6. In the Password and Confirmation field, enter a password for the new user

The passwords must meet the following requirements:

- Minimum 8 characters and Maximum 16 characters
- Minimum 1 capital letter
- Minimum 1 small letter
- Minimum 1 special character among _ : - , . * & @ / \$? Space

We 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.

7. Assign permissions to the user. Select from these options:

Remote: Parameters Settings	Remote: Live View
Remote: Log Search/Interrogate Working Status	Remote: Manual Record
Remote: Upgrade/Format	Remote: PTZ Control
Remote: Bi-directional Audio	Remote: Playback/Download
Remote: Shutdown / Reboot	Remote: Set VCA
Remote: Notify Alarm Recipient /Trigger Alarm Output	
Remote: Video Output Control	
Remote: Serial Port Control	

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

To delete a user:

1. From the menu toolbar, click **Configuration > System > User Management**
2. Select the desired user.
3. Click the **Delete** button. A message box appears asking if you want to delete this user. Click **OK**.

Note: Only the administrator can delete a user.

4. Enter the Admin password. Click **OK**.

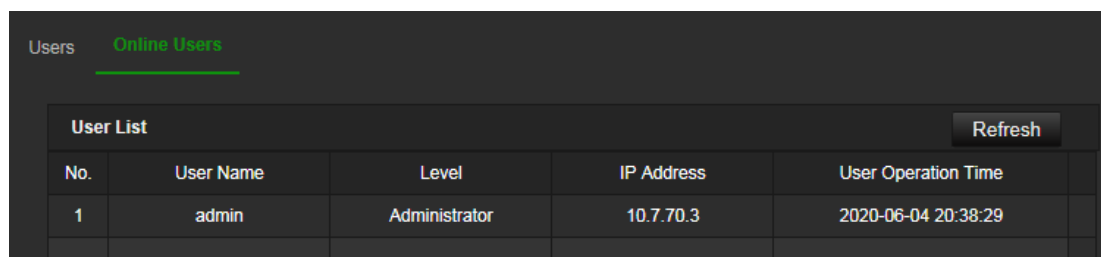
To modify user information:

1. From the menu toolbar, click **Configuration > System > User Management**
2. Select the desired user.
3. Click the **Modify** button. The *Modify user* window appears.
4. Change the information required and enter the admin password. Click **OK**.

Note: Only the admin user can modify users.

Online users

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



The screenshot shows a web interface with a dark theme. At the top, there's a header with 'Users' and 'Online Users' (the latter is highlighted in green). Below this is a 'User List' table with a 'Refresh' button in the top right corner. The table has five columns: 'No.', 'User Name', 'Level', 'IP Address', and 'User Operation Time'. One user is listed: '1', 'admin', 'Administrator', '10.7.70.3', and '2020-06-04 20:38:29'.

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

Network

Use the Network menu to set the desired network parameters.

Network Settings

Menu Network Settings allows you to configure network addresses and other parameters related to connectivity.

TCP/IP

You can set up the following TCP/IP parameters:

Function	Description
NIC Type	Enter the NIC type. Default is Auto. Other options include: 10M Half-dup, 10M Full-dup, 100M Half-dup, and 100M Full-dup
DHCP	Enable the parameter 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 Mask	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 MTU value. The supported value is between 1280 and 1500. Default value is 1500.
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 primary and secondary DNS servers 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 > Network Settings > TCP/IP**.

The screenshot shows the TCP/IP configuration interface. At the top, there are tabs for different network settings: TCP/IP (selected), DDNS, PPPoE, SNMP, 802.1X, and QoS. Below the tabs, the configuration is organized into several sections:

- NIC Type:** A dropdown menu set to "Auto".
- DHCP:** A toggle switch that is currently turned off.
- IPv4 Settings:**
 - *Device IPv4 Address:** 192.168.1.18 (with a "Test" button next to it).
 - *IPv4 Subnet Mask:** 255.255.255.0
 - IPv4 Default Gateway:** 192.168.1.1
- IPv6 Mode:** Three radio buttons: Manual, DHCP, and Route Advertisement (which is selected). There is a "View" link next to the selected option.
- IPv6 Settings:**
 - Device IPv6 Address:** 2a02:1810:cc22:b700:9ef6:1aff:feb9:cb71
 - IPv6 Subnet Mask:** 64
 - IPv6 Default Gateway:** ::
- MAC Address:** 9c:f6:1a:ba:cb:71
- *MTU:** 1500
- Enable Multicast Discovery:** A toggle switch that is turned on.
- DNS Server Configuration:**
 - Preferred DNS Server:** (empty text field)
 - Alternate DNS Server:** (empty text field)
- Host Name Configuration:**
 - Enable Dynamic Domain Name:** A toggle switch that is turned off.
 - Register DNS name:** (empty text field)

A green "Save" button is located at the bottom center of the form.

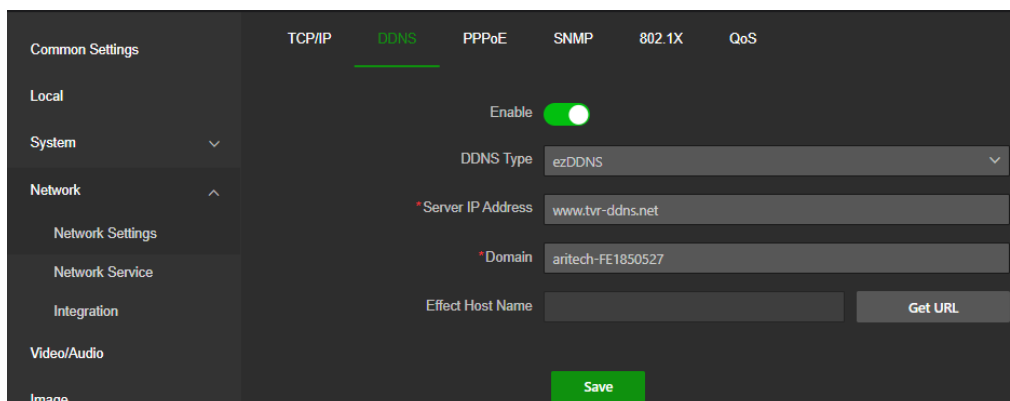
2. Configure the NIC settings, including the NIC Type, IPv4 settings, IPv6 settings, and MTU settings.
3. If the DHCP server is available, select **DHCP**.
4. If the DNS server settings are required for some applications (e.g., sending email), you should configure the **Preferred DNS Server** or **Alternate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

DDNS

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 > Network 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 website. Then enter your username 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 hostname. It will automatically register it online. You can define a hostname 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 hostname field, enter the host obtained from the NO-IP website. Then enter the user name and password that are registered with the No-IP network.

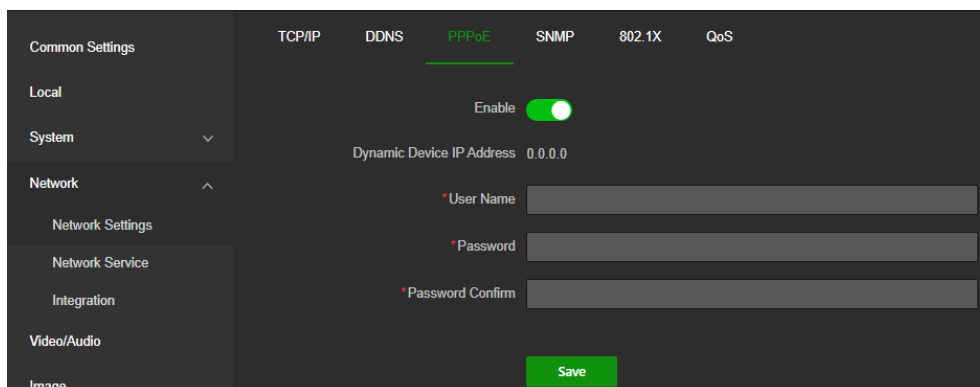
4. Click **Save** to save changes.
5. Reboot the device for the changes to take effect.

PPPoE

This allows you to retrieve a dynamic IP address.

To set up the PPPoE parameters:

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

The screenshot shows a web-based configuration interface for a device. On the left is a sidebar menu with categories: Common Settings, Local, System (with a dropdown arrow), Network (with an up arrow), Network Settings, Network Service, Integration, Video/Audio, and Image. The main area has tabs for TCP/IP, DDNS, PPPoE (which is selected and highlighted with a green underline), SNMP, 802.1X, and QoS. In the PPPoE section, there is an 'Enable' toggle switch that is turned on (green). Below it, the 'Dynamic Device IP Address' is set to '0.0.0.0'. There are three input fields: '* User Name', '* Password', and '* Password Confirm', each with a red asterisk indicating a required field. At the bottom right of the main area is a green 'Save' button.

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.

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 > Network Settings > SNMP**.

TCP/IP DDNS PPPoE **SNMP** 802.1X QoS

SNMP v1/v2

Enable SNMPv1 ☐

Enable SNMPv2c ☐

SNMP v3

Enable ☒

*Read User Name

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 SNMPv1, SNMP v2c, or SNMPv3.
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.

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 > Network Settings > 802.1X**.

The screenshot shows the '802.1X' configuration page. On the left is a sidebar with a menu: 'Common Settings', 'Local', 'System' (with a dropdown arrow), 'Network' (with an up arrow), 'Network Settings', 'Network Service', 'Integration', 'Video/Audio', and 'Image'. The main area has tabs: 'TCP/IP', 'DDNS', 'PPPoE', 'SNMP', '802.1X' (highlighted with a green underline), and 'QoS'. The '802.1X' settings include: 'Enable' (a green toggle switch), 'Protocol' (a dropdown menu showing 'EAP-TLS'), '*Identity' (a text input field), 'EAPOL Version' (a dropdown menu showing '1'), 'Client Certificate' (a dropdown menu showing 'No certificate'), and 'CA Certificate' (a dropdown menu showing 'No certificate'). At the bottom right is a green 'Save' button.

2. Select **Enable IEEE 802.1X** to enable the feature.
3. Configure the 802.1X settings, including the EAPOL version, username, and password. The EAPOL version must be identical to 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 username and password for 802.1X on the server.

QoS

QoS (Quality of Service) can help solve 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 > Network Settings > QoS**.

The screenshot shows the 'QoS' configuration page. It has the same sidebar and tabs as the previous page, with 'QoS' highlighted with a green underline. The settings include: '*Video/Audio DSCP' (a text input field with '0'), '*Alarm DSCP' (a text input field with '0'), and '*Management DSCP' (a text input field with '0'). At the bottom center is a green 'Save' button.

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.

Network Service

In the Network Service menu, you can configure different protocol options and port mappings.

HTTP(S)

Specifies the authentication of the website and its associated web server, which can offer protection against Man-in-the-middle attacks.

To set up the HTTP parameters:

1. Click **Configuration > Network > Network Service > HTTP** and set the port to be used for HTTP communication.

To set up the HTTPS parameters:

1. Click **Configuration > Network > Network Service > HTTPS**.
2. Enable HTTPS and configure port.
3. Select Server Certificate

Enabling option **Force HTTPS Browsing** forces the camera to use HTTPS instead of HTTP.

The screenshot displays the 'Network Service' configuration page. The left sidebar contains a menu with options: Common Settings, Local, System, Network, Network Settings, Network Service, Integration, Video/Audio, Image, Storage, and Event. The main content area has tabs for HTTP(S), Multicast, RTSP, SRTP, Bonjour, WebSocket(s), NAT, and SIP. The 'HTTP(S)' tab is active, showing sections for HTTP, HTTPS, Server Certificate, and WEB Authentication. The HTTP section has an 'HTTP Port' field set to 80. The HTTPS section has an 'Enable' toggle switch turned on, a 'Confirm whether the TLS version used in client is enabled' message with a 'TLS Settings' link, and an 'HTTPS Port' field set to 443. The 'Server Certificate' section has a 'Server Certificate' dropdown menu set to 'default' and a 'Certificate Management' link. The 'WEB Authentication' section has an 'Authentication Mode' dropdown set to 'digest/basic' and a 'Digest Algorithm' dropdown set to 'MD5'. A note at the bottom states: 'WEB authentication and WEB digest algorithm will be effective for HTTP and HTTPS.' A 'Save' button is located at the bottom right.

WEB Authentication

You can secure the stream data of the live view.

To define the web authentication:

1. Select **Authentication Mode: digest/basic** or **digest** in the drop-down list and the desired algorithm MD5, SHA256, or MD5/SHA256.

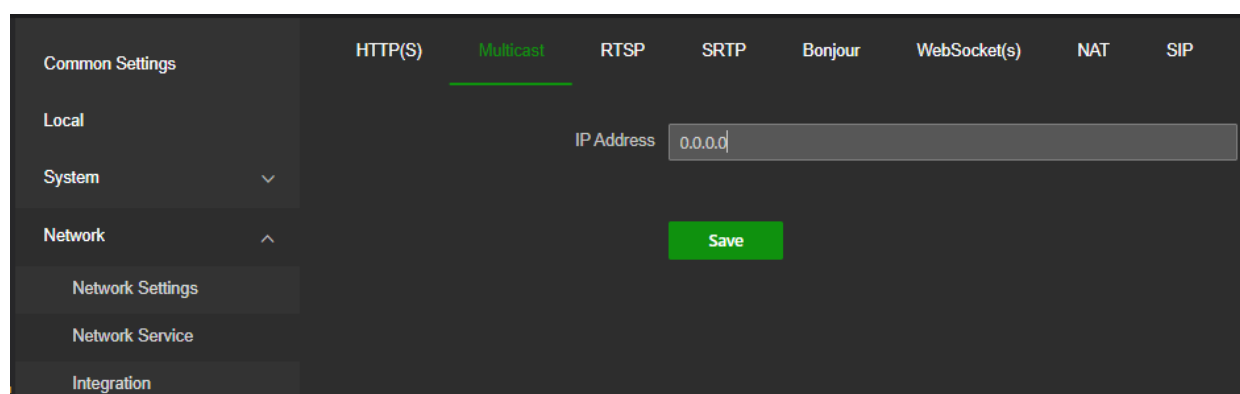
Note: Web authentication is the authentication used between the camera and the web browser.

2. Click **Save** to save the 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 > Network Service > Multicast**.



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 the multicast function in case of a network storm.
3. Click **Save** to save changes.

RTSP

RTSP (Real Time Streaming Protocol) is an application-layer controlling protocol for streaming media.

The screenshot displays the RTSP configuration page. The left sidebar shows the navigation menu with 'Common Settings' selected. The main content area has tabs for different protocols, with 'RTSP' currently active. The configuration fields include selecting a camera stream (1-4), setting a port number (554), choosing a stream type (Main Stream or Substream), and specifying video and audio ports (8860 and 8862). The RTSP Authentication section allows selecting an authentication mode (digest/basic) and a digest algorithm (MD5). A green 'Save' button is located at the bottom right of the configuration area.

To set up the RTSP parameters:

1. Go to **Configuration > Network > Network Service > RTSP**
2. Select camera stream if applicable
3. Enter Port No.
4. Set Multicast parameters.

Stream Type: The stream type as the multicast source.

Video Port: The video port of the selected stream.

Audio Port: The audio port of the selected stream.

5. Set RTSP Authentication.

Authentication

Digest and digest/basic are supported, which means authentication information is needed when RTSP request is sent to the device. If you select digest/basic, it means the device supports digest or basic authentication. If you select digest, the device only supports digest authentication.

Digest Algorithm

MD5, SHA256 and MD5/SHA256 encrypted algorithm in RTSP authentication. If you enable the digest algorithm except for MD5, the third-party platform might not be able to log in to the device or enable live view because of compatibility. The encrypted algorithm with high strength is recommended.

6. Click **Save**.

SRTP

RTSP (Real Time Streaming Protocol) is an application-layer controlling protocol for streaming media.

The screenshot shows the SRTP configuration page. On the left is a sidebar with a 'Common Settings' menu and a list of categories: Local, System, Network, Network Settings, Network Service, Integration, Video/Audio, Image, Storage, and Event. The main area has tabs for HTTP(S), Multicast, RTSP, SRTP (selected), Bonjour, WebSocket(s), NAT, and SIP. Under the SRTP tab, there are four channel selection buttons (1, 2, 3, 4), with '1' selected. Below this is a 'Port No.' field set to 322. The 'Multicast' section includes a 'Stream Type' dropdown with 'Main Stream' selected, and 'Video Port' and 'Audio Port' fields set to 18860 and 18862 respectively. The 'Server Certificate' section has a dropdown set to 'default' and a 'Certificate Management' link. The 'Encrypted Algorithm' section has a dropdown set to 'AES256'. A green 'Save' button is at the bottom.

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

To set up the SRTP parameters:

1. Go to **Configuration > Network > Network Service > SRTP**.
2. Select camera stream if applicable
3. Enter the Port number.
4. Set Multicast parameters.

Stream Type: Click on the stream you want to configure.

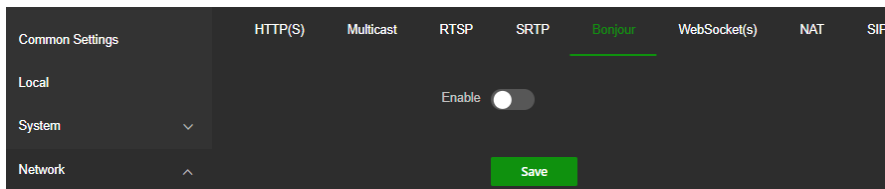
Video Port: The video port of the selected stream.

Audio Port: The audio port of the selected stream.

5. Select Server Certificate.
6. Select Encrypted Algorithm.
7. Click Save.

Bonjour

Bonjour is a general method for applications to discover shared services on a local area network,



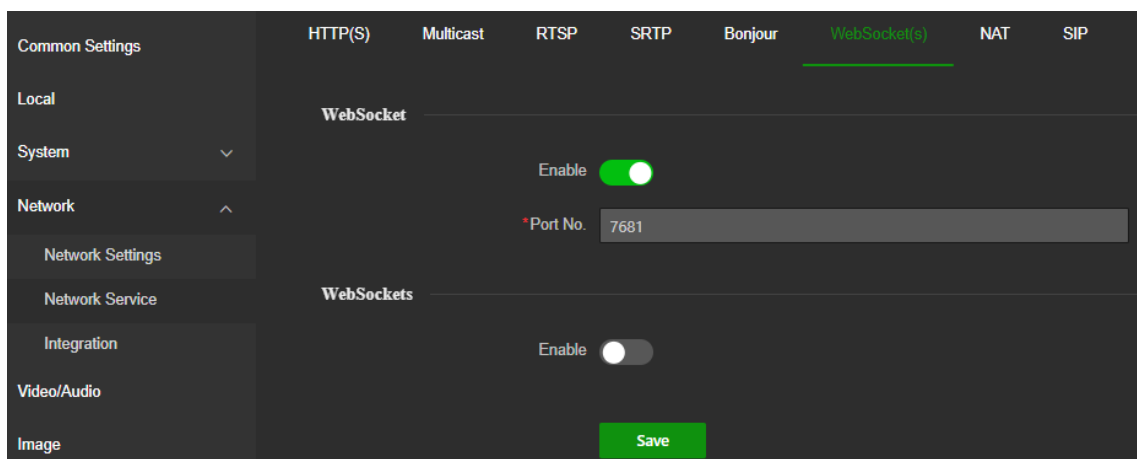
Websocket(s)

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:** TCP-based full-duplex communication protocol port for a plug-in free preview. 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:** TCP-based full-duplex communication protocol port for plug-in free live view. Certificate verification is required to ensure secure access.

To set up the network service parameters:

1. Click **Configuration > Network > Network Service > WebSocket(s)**.



2. **Enable** WebSocket service and enter the port number for live viewing over HTTP protocol without the plug-in.
3. **Enable** WebSockets service for live viewing over HTTPS protocol without the plug-in.
4. Click **Save** to save changes.

NAT

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 > Network Service > NAT**.

Common Settings

Local

System

Network

Network Settings

Network Service

Integration

Video/Audio

Image

Storage

Event

HTTP(S) Multicast RTSP SRTP Bonjour WebSocket(s) **NAT** SIP

Enable UPnP™ ☒

*Friendly Name TruVision TVPA-S02-1201-360-G - FE1850527

Port Mapping Mode Auto

Port Mapping List

Port Type	External Port	External IP Address	Internal Port	Status
HTTP	80	0.0.0.0	80	Invalid
HTTPS	443	0.0.0.0	443	Invalid
RTSP	554	0.0.0.0	554	Invalid
SDK Service Port	8000	0.0.0.0	8000	Invalid
Enhanced SDK Se...	8443	0.0.0.0	8443	Invalid
Websocket	7681	0.0.0.0	7681	Invalid
Websockets	7682	0.0.0.0	7682	Invalid
SSH Port	22	0.0.0.0	22	Invalid

Save

2. **Enable UPnP™** 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.

SIP

The Session Initiating Protocol (SIP) is a signaling protocol used for initiating maintaining, and terminating real-time communication sessions that can include voice, video and messaging applications.

Enable this function and set the parameters. Click Save to save the settings and register device on the SIP server. Refresh the window and check whether the device has been registered or not.

Common Settings

Local

System

Network

Network Settings

Network Service

Integration

Video/Audio

Image

Storage

Event

HTTP(S)

Multicast

RTSP

SRTSP

Bonjour

WebSocket(s)

NAT

SIP

Enable

Allowlist

Edit

Registration Status

*User Name

*SIP User Name

*SIP Authentication ID

*SIP Authentication Password

*SIP Server Address

*SIP Server Port

*Proxy Server Address

*Proxy Server Port

*Local SIP Port

*SIP Expiration

Stream Type

Alarm List

+ Add

ID Card

Phone No.

Remark

Operation

No Data

Save

Integration

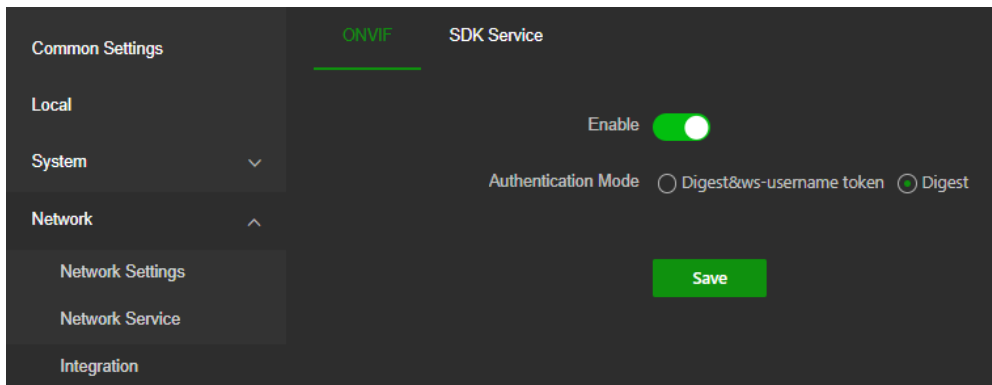
Use this menu to enable third party integration based on ONVIF or SDK.

ONVIF

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:

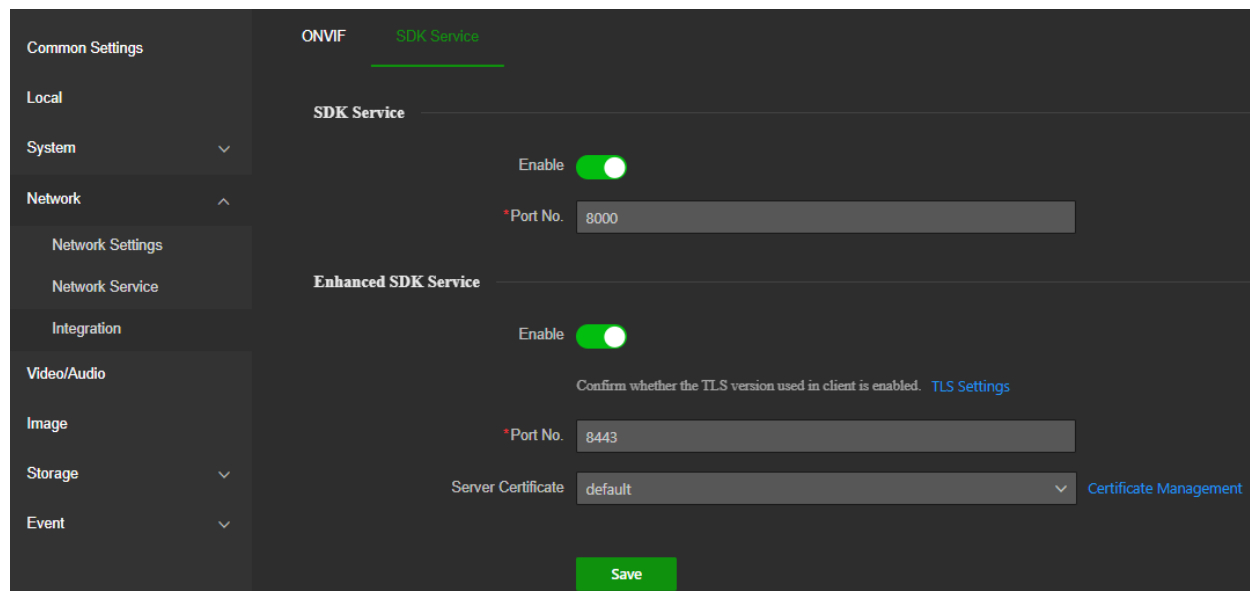
1. Click **Configuration > Network > Integration > ONVIF**.



2. **Enable** ONVIF to enable the ONVIF protocol.
3. Select the desired ONVIF authentication method.
4. Click **Save** to save changes.

SDK Service

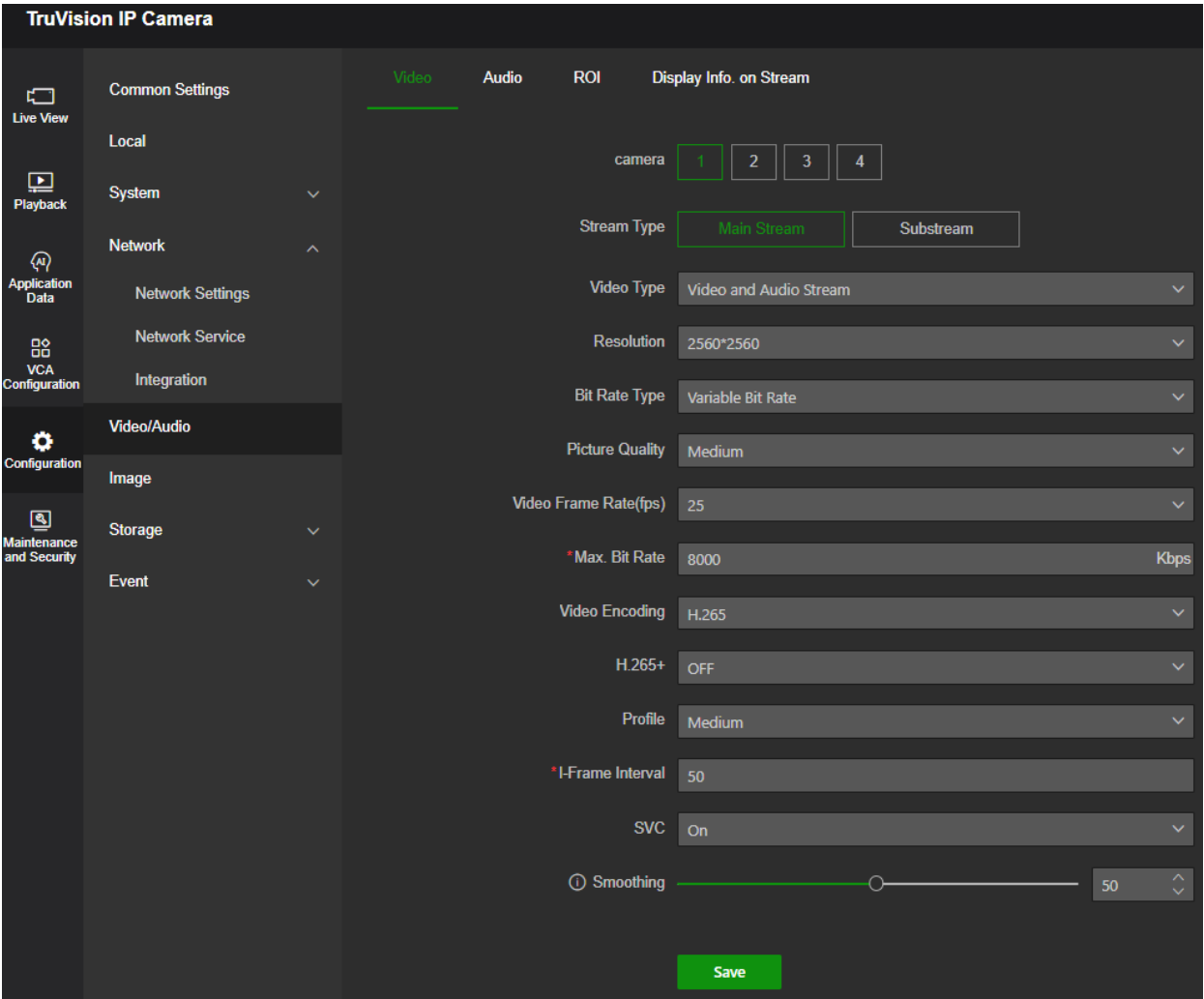
Enable these functions to be able to use the device with a VMS (like TruVision Navigator or a third-party software using the SDK). **SDK Service** uses the SDK protocol. **Enhanced SDK Service** uses SDK over TLS (Transport Layer Security).



Video/Audio

You can adjust the video and audio recording parameters to obtain the image quality best suited to your needs. Figure 4 below lists the video and audio recording options you can configure for the camera.

Figure 4: Video/Audio Settings menu (Video tab shown)

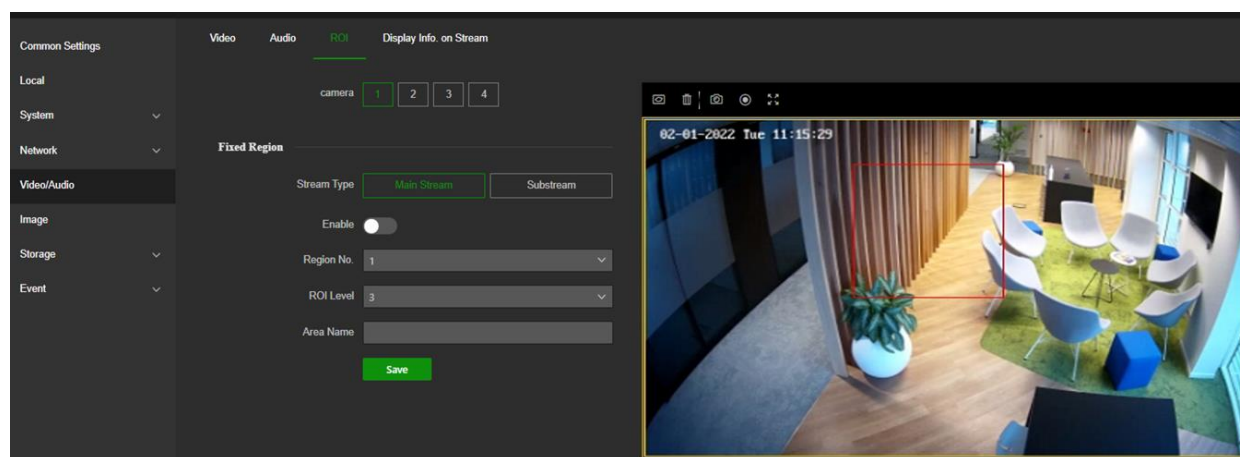


Tab	Parameter descriptions
1. Video	<p>Stream Type: Shows the available streams with its parameters. Options include Main, Stream and Substream.</p> <p>Video Type: Specifies the stream information you wish to record. Select Video Stream to record video stream only. Select Video and Audio stream to record both video and audio streams.</p> <p>Note: Video&Audio is only available for those camera models that support audio.</p> <p>Resolution: Specifies the recording resolution. A higher image resolution provides a higher image quality but also requires a higher bit rate. The resolution options listed depend on the type of camera and on whether the main, sub, third, fourth, or fifth stream is being used.</p> <p>Note: Resolutions can vary depending on the camera model.</p> <p>Bit Rate Type: Specifies whether a variable or fixed bit rate is used. Variable produces higher quality results suitable for video downloads and streaming. Default is Constant.</p>

Tab	Parameter descriptions
	<p>Picture Quality: Specifies the quality level of the video. It can be set when a variable bit rate is selected. Options include Lowest, Lower, Low, Medium, Higher, and Highest.</p> <p>Video Frame Rate (fps): Specifies the frame rate for the selected resolution. The frame rate is the number of video frames that are shown or sent per second.</p> <p>Note: The maximum frame rate depends on the camera model and selected resolution. Please check the camera specifications in its datasheet.</p> <p>Max. Bit Rate: Specifies the maximum bandwidth the camera will be able to use.</p> <p>Video Encoding: Specifies the video encoding used. You can choose between H.264 and H.265.</p> <p>H.264+/H.265+: Depending on the selected Video Encoding, this parameter allows you to activate smart codecs H.264+ or H.265+ by switching it to ON. Leaving this parameter OFF will make the camera use standard H.264 or H.265 video encoding.</p> <p>When switching to H.265+/H.264+, parameters such as SVC Profile and I-Frame Interval will not be supported.</p> <p>Profile: Different profile indicates different tools and technologies used in compression. Options for H.264 include Basic Profile, Main Profile, and High Profile.</p> <p>I-Frame Interval: A video compression method. It is strongly recommended not to change the default value 50.</p> <p>SVC: Scalable Video Coding is an extension of the H.264/AVC standard. Select OFF / ON to disable / enable the SVC function. Select Auto and the device will automatically extract frames from the original video when the network bandwidth is insufficient. SVC is not available when H.264+ or H.265+ video encoding is used.</p> <p>Smoothing: Adjust the smoothness of the stream. Smoothing is not available when H.264+ or H.265+ video encoding is used.</p>
2. Audio (only available if the hardware supports it)	<p>Audio Encoding: G.722.1, G.711ulaw, G.711alaw, MP2L2, G.726, AAC, PCM, and MP3 are supported.</p> <p>Audio Input: Mic In and Line In are selectable for the connected microphone and pickup, respectively.</p> <p>Note: Options can vary depending on the camera model.</p> <p>Input Volume: Specifies the microphone volume from 0 to 100.</p> <p>Audio Output: Specifies how audio will be routed. To the Built-in speaker or Line output.</p> <p>Output volume: Specifies the audio output volume</p> <p>Environmental Noise Filter: Enabling this function will filter out background noise picked up by the microphone.</p>
3. ROI	<p>Enable assigning more encoding resources to the region of interest (ROI) to increase the quality of the ROI whereas the background information is less focused.</p>
4. Display Info on Stream	<p>Enable Dual-VCA to add additional VCA object information such as person/vehicle to the video stream.</p>

To configure ROI settings:

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



2. Draw the region of interest in the image.
3. Choose the stream type to be used for the ROI encoding.
4. **Enable** to manually configure the area.

Region No.: You can configure one fixed ROI region.

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

Area Name: Set the desired name for the selected region.

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

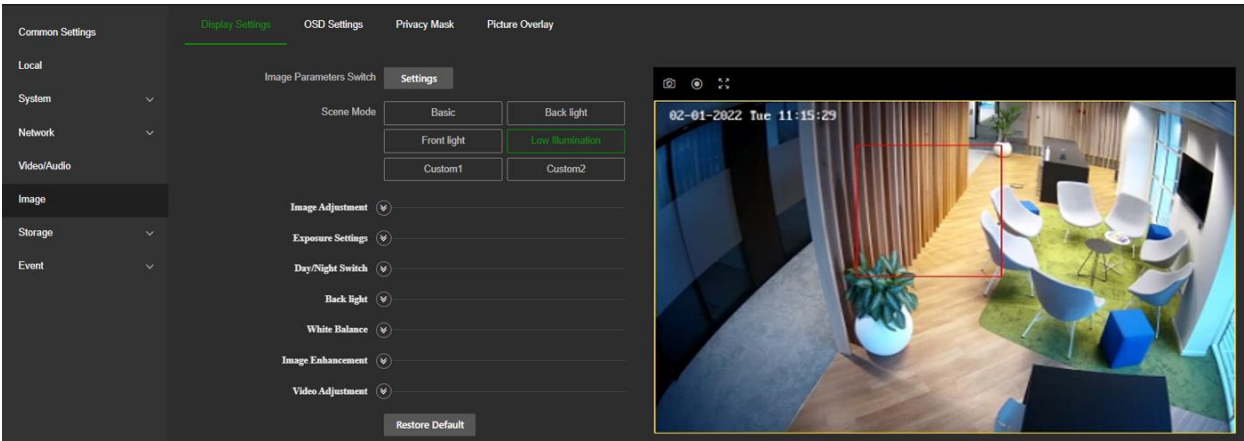
Image

You may need to adjust the camera image depending on the camera model or location background to get the best image quality. See Figure 5 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. Available settings can vary slightly depending on the camera model.

Figure 5: Display Settings menu



The parameters displayed on the right and part of this menu depend on the **Scene** selected from the drop-down list. Select the scene best suited to the environment: Normal, Backlight, Front light, Low Illumination, Custom1, and Custom2.

Parameter	Description
1. Image Adjustment	
Brightness, Contrast, Saturation, Sharpness	Modify the different elements of picture quality by adjusting the values for each parameter. These options can also be modified from the General control panel in Live View.
2. Exposure Settings	
Exposure Mode	Iris Mode: The value cannot be changed as the camera has a fixed iris. Exposure Time: Adjust this value manually to change the light sensitivity of the camera. The higher the value, the slower the shutter speed. It ensures full exposure in underexposed conditions.
3. Day/Night Switch	
Day/Night Switch	Defines whether the camera is in day or night mode. The day (color) option could be used, for example, if the camera is located indoors where light levels are always good. Select one of the following options: Day: Camera is always in day mode. Night: Camera is always in night mode. Auto: The camera automatically detects which mode to use depending on the amount of light captured by the camera. Scheduled switch: The camera switches between day and night modes according to the configured period.
Sensitivity	Only available when <i>Auto D/N switch</i> mode is selected. It defines the sensitivity of the switch between day and night. Set it between 1 and 7.
Filtering Time	This is the time interval between the day/night switch. You can set it from 5 s to 120 s. When the environment changes from bright to dark and the duration of the dark state is equal to or exceeds the filtering time set, the camera will switch to night mode, and vice versa. If the duration of the environmental brightness change is less than the filtering time, the mode will not change.

Parameter	Description
Smart Supplement Light	When enabled, it can avoid over-exposure problems by decreasing the amount of white-light illumination for objects closer to the camera
Supplement Light Mode	IR Supplement Light: The IR LEDs are ON when the camera changes to night mode. OFF: The IR LEDs remain OFF when the camera changes to night mode
Light Brightness Control	Auto: The intensity of the white light will be set automatically according to environmental light. Manual: In manual mode, the white-light intensity can be set to a desired fixed value using the white-light slider.

4. Backlight Settings

BLC	This function improves image quality when the background illumination is high. It prevents the object in the center of the image from appearing too dark. Select OFF, Up, Down, Left, Right, Center, or Auto.
WDR	When enabled, wide dynamic range (WDR) provides clear images when there is a 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. This option can also be enabled/disabled from the General control panel in Live View.
Wide Dynamic Level	The WDR level can be fine-tuned by changing its value between 0 and 100
HLC	Use the highlight compensation (HLC) function when there are strong sources of light in the scene that affects the image quality. This option can also be enabled/disabled from the General control panel in Live View.

5. 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 below:

MWB: Manually adjust the color temperature to meet your requirements.

AWB1: Automatically adjust the camera's white balance between 2500 to 9500K for environments where the lighting is always stable.

AWB2: Automatically adjust the camera's white balance within a narrower range than that of AWB1. This adjustment is more accurate.

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 where there are incandescent lamps installed near the camera.

Warm light lamp: For use in situations where an external warm light is present near the camera.

Natural light: For use, where the camera is installed in a natural light environment.

6. Image Enhancement

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

Parameter	Description
Defog Mode	You can enable the defog function when the environment is foggy, and the image is misty. It enhances the subtle details so that the image appears clearer. Default is OFF.
Gray Scale	You can choose the range of the Gray Scale as [0-255] or [16-235]
7. Video Adjustment	
Video Standard	Select PAL (50 Hz) or NTSC (60 Hz). Select the value depending on the video standards.

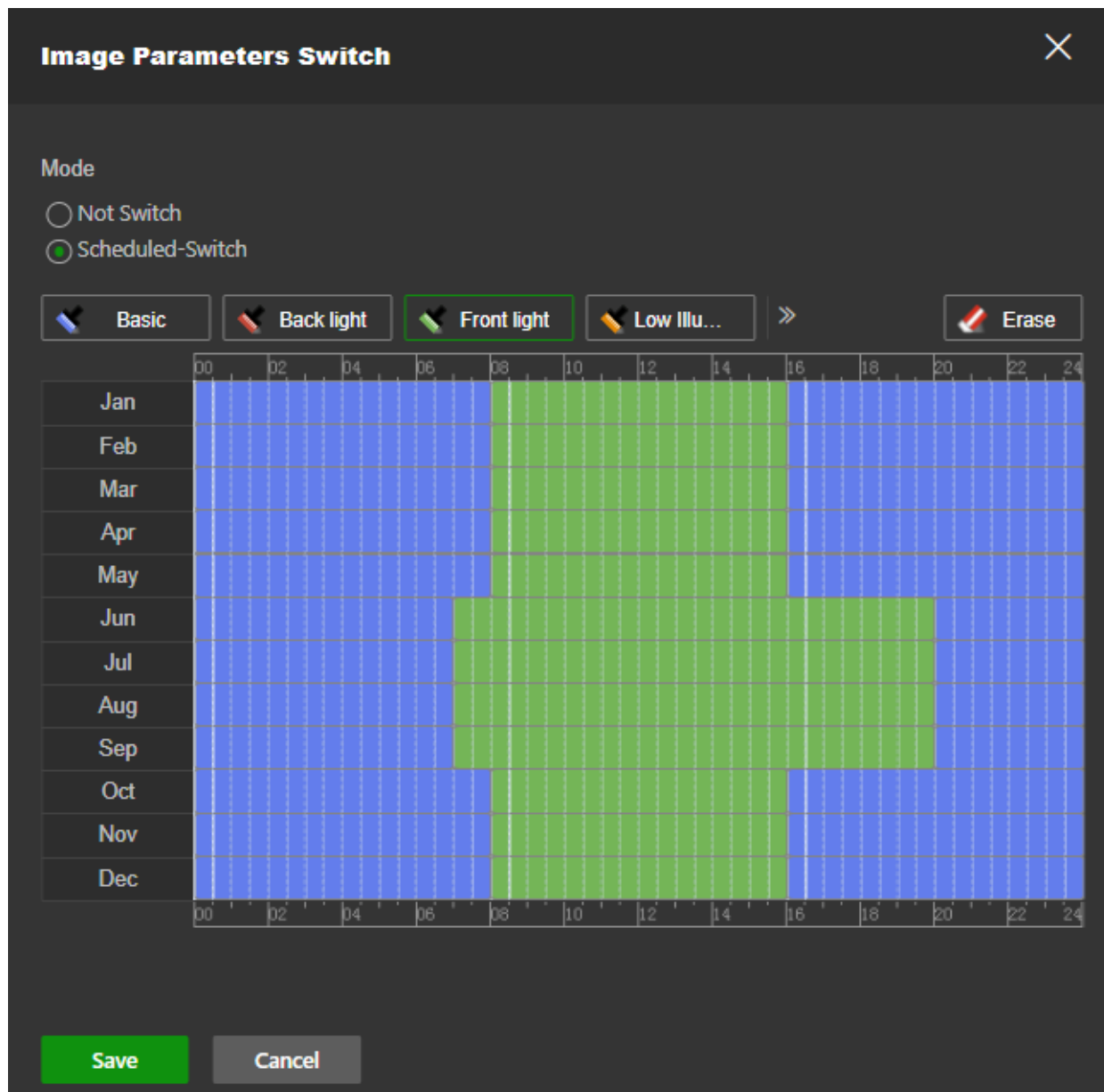
Note: Click the **Restore Default** button to default all the image settings.

Image Parameters Switch

You can link different lighting scenes to a D/N month schedule, such as low illumination or backlight. Before linking the lighting scenes to the D/N schedule, define the parameters for each scene under the *Display Settings* menu (see “Display Settings” on page 34 for further information). You can link up to four lighting scenes to the scheduled D/N.

To set up an image parameter switch:

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



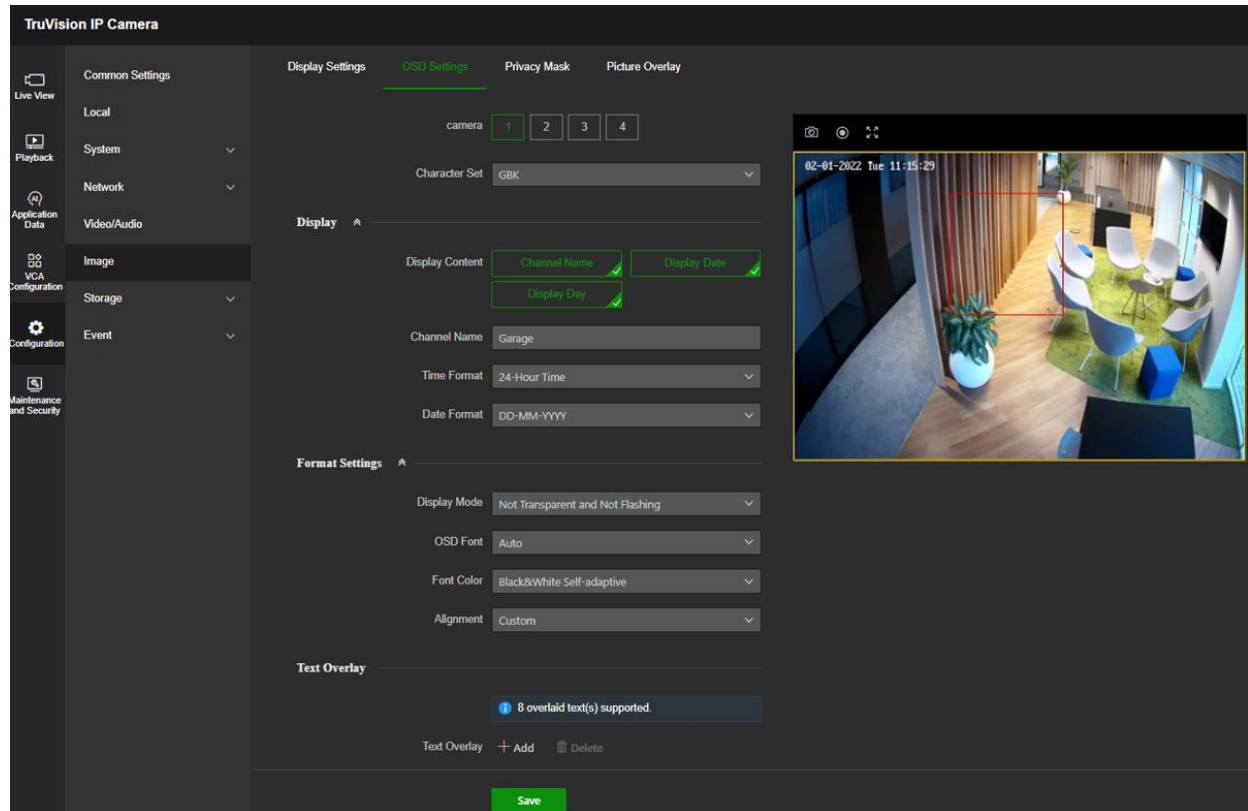
2. Select the **Scheduled-Switch mode** to activate this function.
3. Select from the buttons at the top of the table the desired lighting scene you want to use and then drag the mouse along the timeline bar of the desired day to draw a period for which this scene should be activated. You can schedule up to eight time periods in a day.
 To change a lighting scene, click the Erase button and draw over the time period you want to delete. Click then again on the desired scene mode and draw the time period again. Click **Save** to save the changes.
4. Repeat the above step by selecting another lighting scene from the drop-down list, if required. When the periods/scenes are defined, you can click on a period and manually type in the start/end time to fine-tune the period.
5. Click **Save** to save changes.

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.

To set up the OSD text:

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



2. Select the camera stream if applicable
3. Check 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**.
4. Check the **Display Date** check box to display the date/time on screen.
5. Check the **Display Day** check box to include the day of the week in the on-screen display.
6. In the **Channel Name** box, enter the camera name.
7. Select the time and date formats from the **Time format** and **Date format** drop-down list boxes.
8. 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.

9. Select the desired **OSD Font** size.

10. Select the desired **Font Color**.

11. Select the desired **Alignment** (Custom, Align Left, or Align Right).

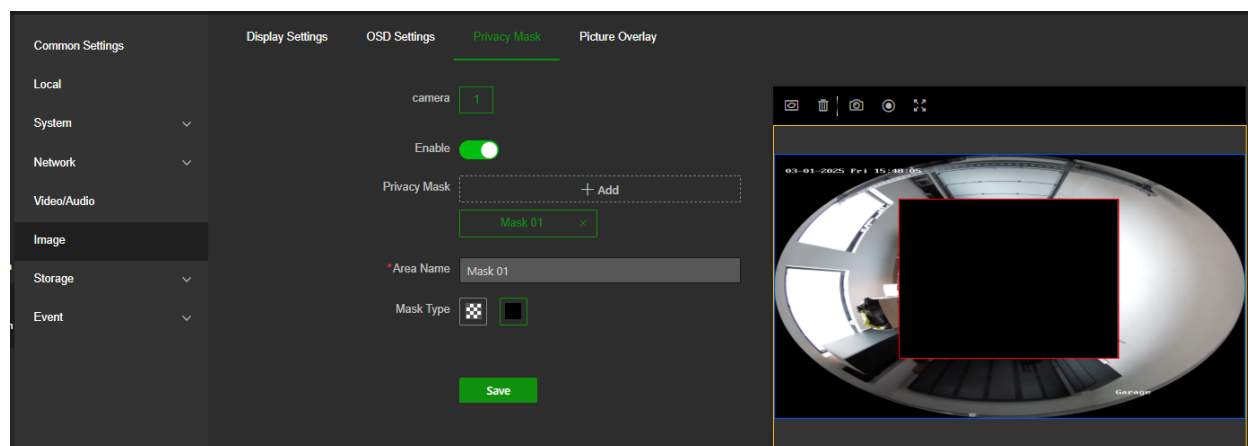
12. Click **Save** to save changes.

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

Eight additional custom *Text Overlays* can be created and positioned across the camera image by dragging the text overlay to the desired position on the image. You can also add and position text overlays when in live view mode under the *General* menu.

Privacy Mask

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 or mosaic area on screen. You can only create one privacy mask area per camera.



To add a privacy mask area:

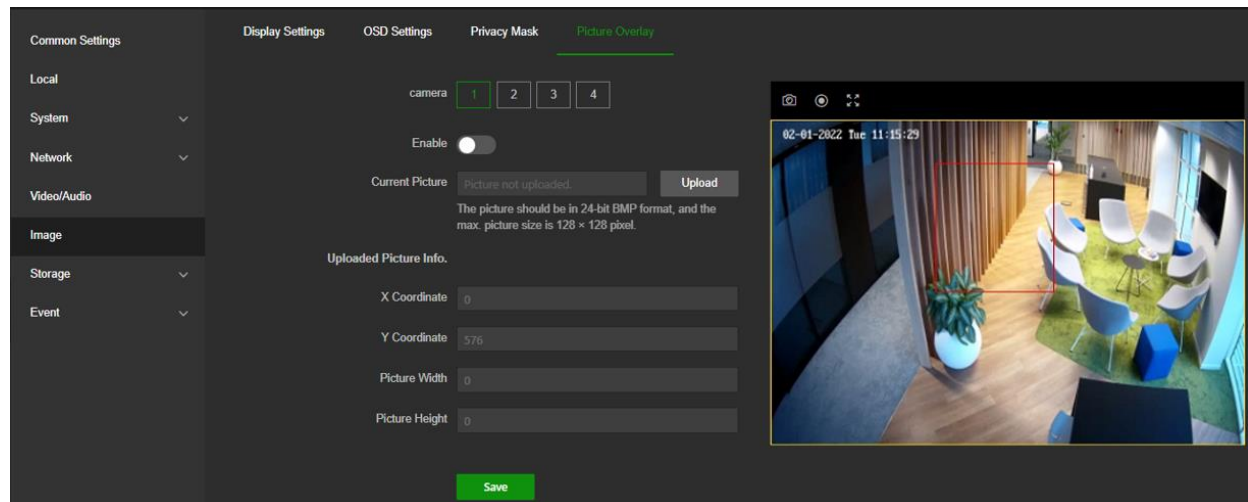
1. Click **Configuration > Image > Privacy Mask**.
2. **Enable** Privacy Mask to activate the function.
3. Click the **Draw Area** button and draw the mask area.
4. Enter an Area Name for the mask and select mask type Black or Mosaic.
5. Click **Save** to save changes.
6. Repeat steps 3 to 5 to create additional masking areas.

Note: Existing privacy mask areas can be deleted by clicking the “x” icon in the button with the name of the corresponding privacy mask.

Picture Overlay

This feature is used to overlay a customized picture on the camera live view stream.

Note: The picture to overlay must be in BMP format with 24-bit, and the maximum picture size is 128 × 128 pixel.



To add an overlay picture:

1. Click **Configuration > Image > Picture Overlay**.
2. Enable
3. Click Upload to browse for a picture and select it for upload.

The picture with a red rectangle will appear in live view after successful upload.

4. Drag the red rectangle to position the picture to a desired position in the image.
5. Click Save.

Storage

Camera streams can be recorded on an optional recording device, NAS, or SD card inserted into the camera.

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 otherwise the device will not function properly.

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

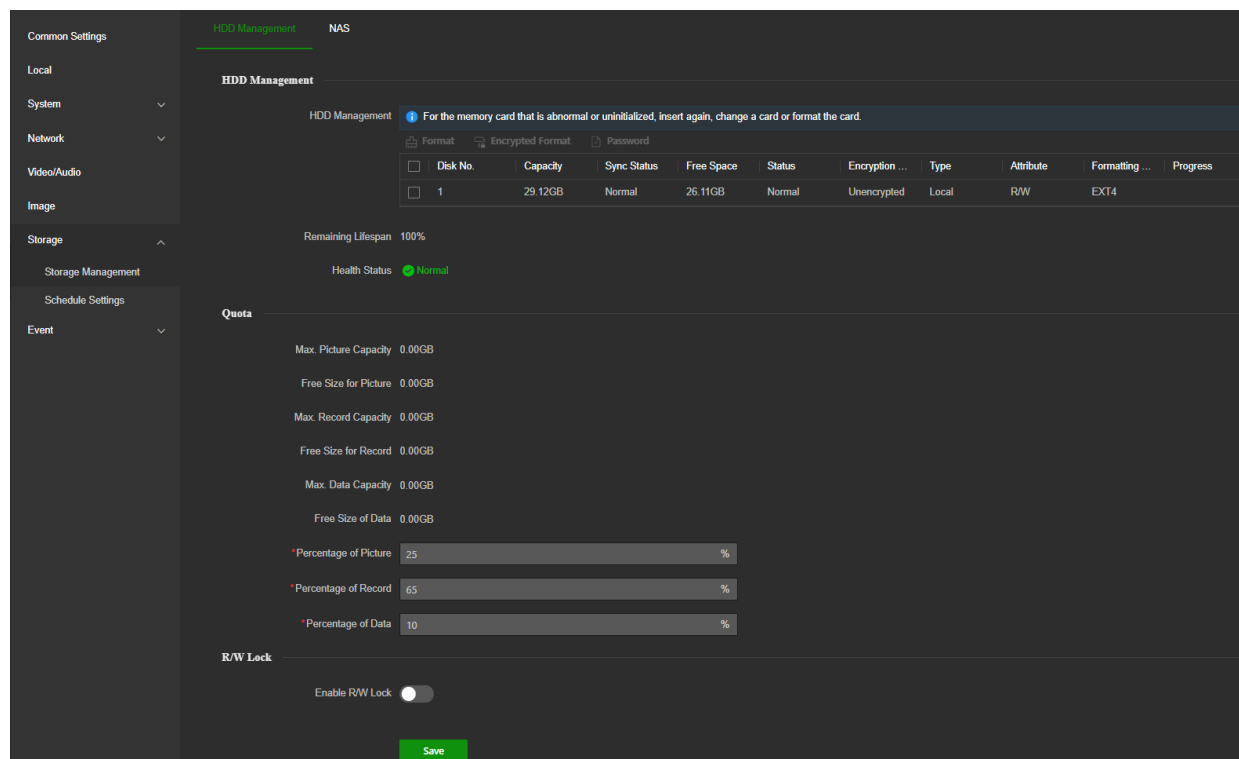
To ensure efficient use of the storage space available on HDDs, you can control the camera's storage capacity using HDD quota management. This function lets you

allocate different storage capacities for main stream/substream recordings and snapshots.

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

To format the storage devices:

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



2. Select the in the table the disk you want to format.
3. If needed, click the **Encrypted format** button. A window appears for you to select your formatting permission. Some SD cards can support **Encrypted formatting** that provides extra encryption for the data stored on the SD card. You can also decide to do a regular formatting by clicking the **Format** button.
4. Click **OK** and enter the admin password to start the formatting process.
5. After the HDD is formatted, its status should show normal.

Notes:

- If the status of the SD card shows Verification Failed, click Password, and enter the password for verification. If the verification is successful, the status becomes Encrypted and data on the card can be accessed again. In case you don't remember the encryption password anymore, the card must be formatted to be used again.
- SD card estimated **Remaining Lifespan** and **Health Status** indicate the overall health of the storage card.

To set the quota storage for recordings and snapshots:

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

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

To set R/W lock:

1. Click **Configuration > Storage > Storage Management > HDD Management**.
2. Activate Enable R/W lock and choose a password to allow only recordings from this camera on the SD card. If the card were placed in another camera, this new camera would not be able to write data onto the SD card unless the R/W lock feature on this camera would also be enabled using the same password that was used on the original camera.
3. Click **Save**

NAS

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

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

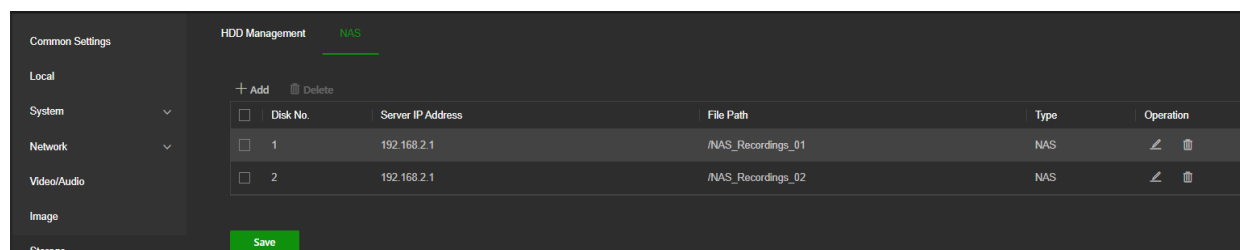
The NAS disk should be available within the network and correctly configured to store the recorded files, log files, etc.

Notes:

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

To set up a NAS system:

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

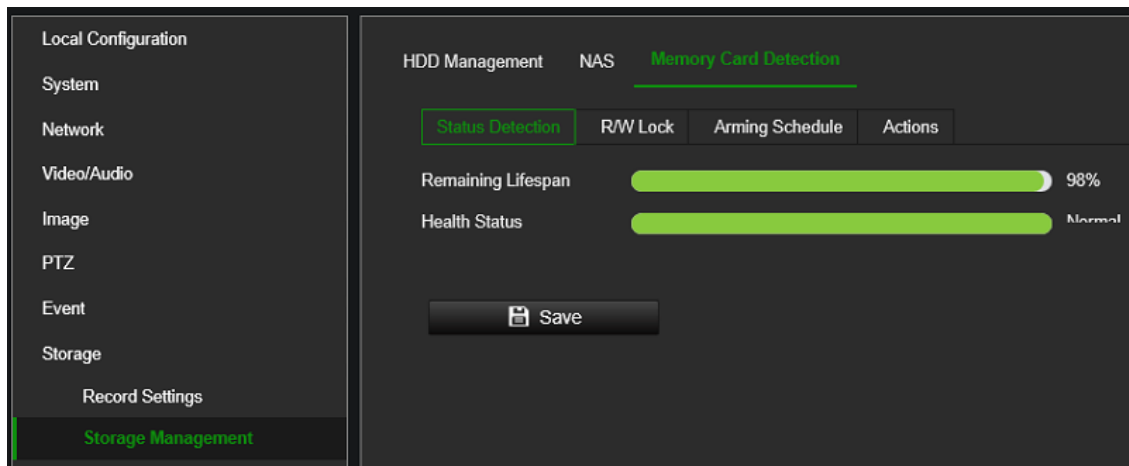


2. Enter the IP address of the network disk(s) and the NAS folder path(s).
3. Click **Save** to save changes.

To check the SD card status:

1. Click **Configuration > Storage > Storage Management > Memory Card Detection**.

The health status and estimated lifespan of the SD Card are displayed.



Schedule Settings

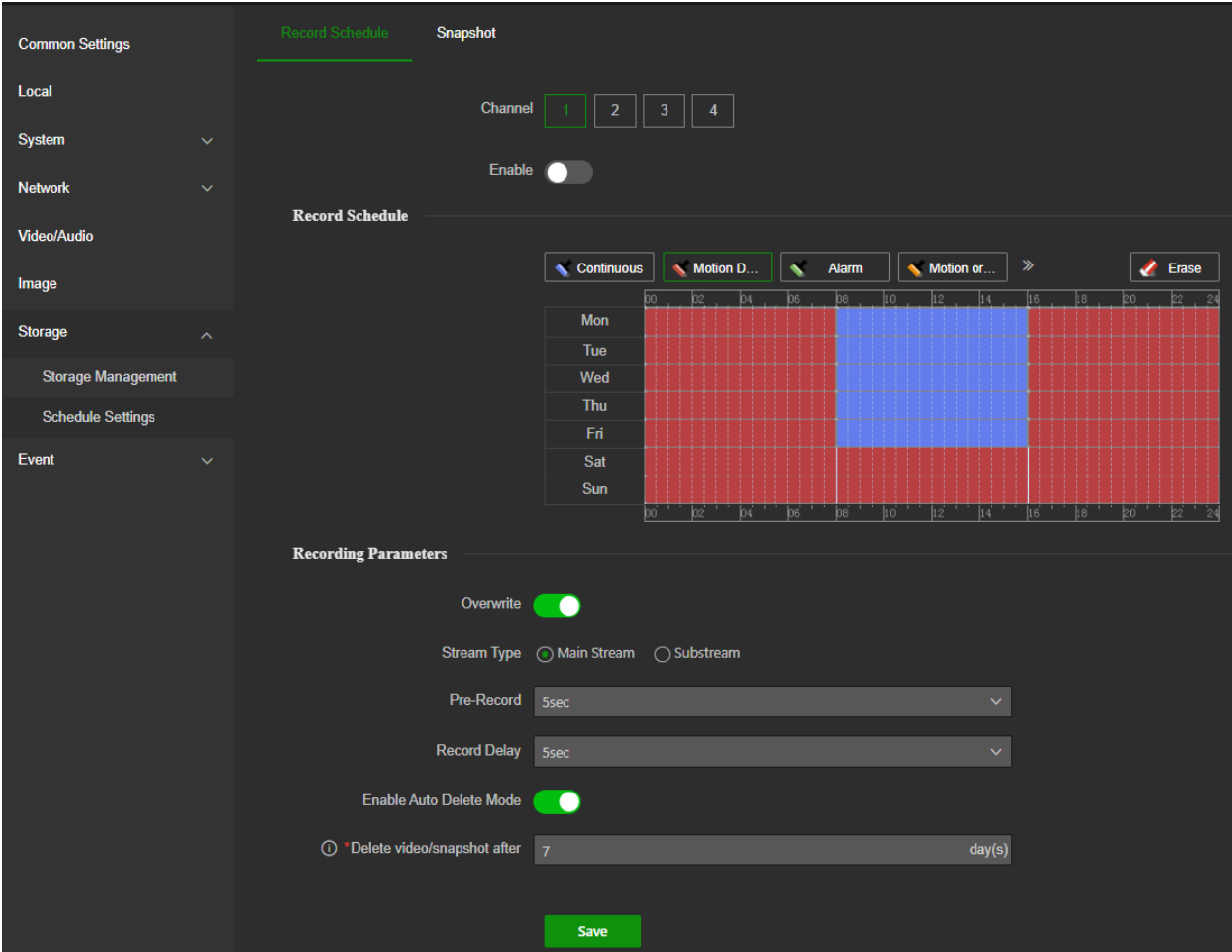
Configure recording and snapshot parameters in this menu.

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

Different recording modes can be defined in the schedule.

Recording Parameters allow you to set pre-record and post-record times, the stream type, and auto-delete mode. When **Auto Delete Mode** is enabled, you can set the number of days after which recordings are automatically deleted.

Figure 6: Record schedule

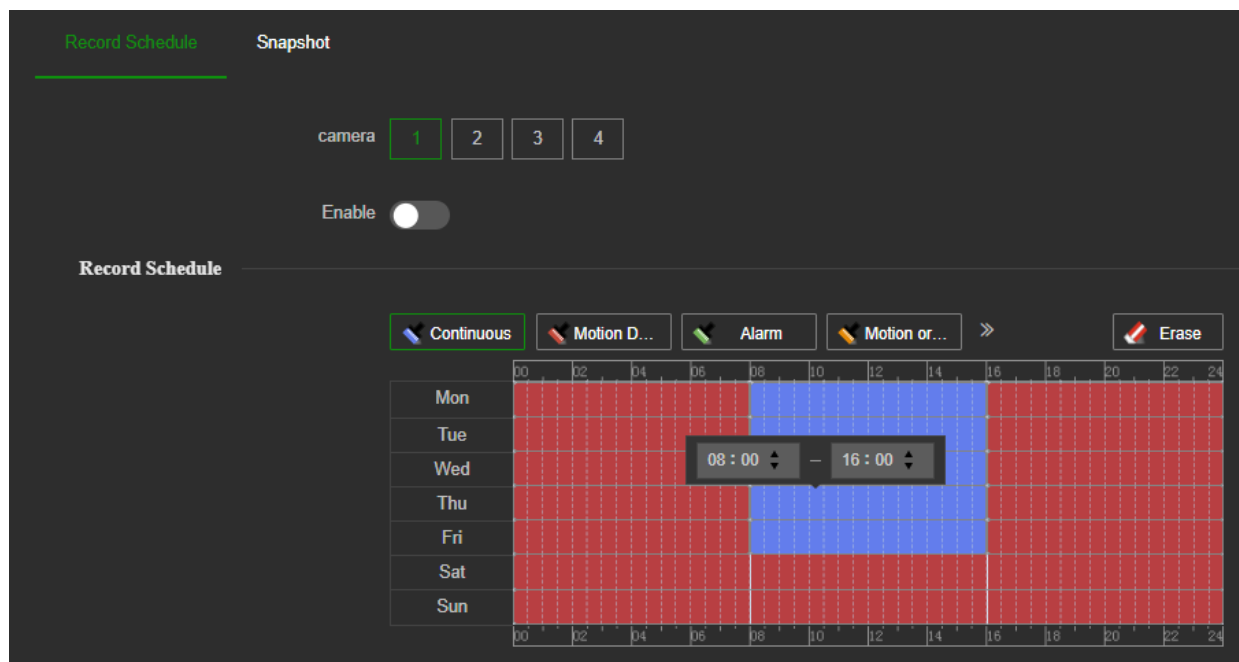


Pre-record time	The pre-record time is set to start recording before the scheduled time or event. For example, if an alarm-triggered recording at 10:00, and the pre-record time is set to 5 seconds, the camera starts to record at 9:59:55. The pre-record time can be configured as No Pre-record, 5 s, 10 s, 15 s, 20 s, 25 s, 30 s, or Not Limited.
Post-record time	The post-record time is set to stop recording after the scheduled time or the event. For example, if an alarm-triggered recording ends at 11:00, and the post-record time is set to 5 seconds, the camera records until 11:00:05. The post-record time can be configured as 5 s, 10 s, 30 s, 1 min, 2 min, 5 min, or 10 min.
Stream type	You can select to record main stream or substream
Enable Auto Delete Mode	When enabled, a recorded video older than the number of days defined by “Delete after” will be automatically deleted, even if the full storage capacity has not been reached.

To set up a recording schedule:

1. From the menu toolbar, click **Configuration > Storage > Schedule Settings > Record Schedule**.
2. Switch on **Enable** to enable recording.
3. Configure the recording schedule.

From the buttons above the schedule, click on the desired type of recording. Then drag the mouse along the timeline of a day of the week to mark the period of the recording. Click the recording timeline to fine-tune recording timings if needed:



4. Enter the exact start and end times of the recording. If required, you can also change the type of recording.
 - **Continuous:** This is continuous recording.
 - **Motion Detection:** Video is recorded when motion is detected.
 - **Alarm:** Video is recorded when an alarm is triggered via the external alarm input channels. Besides configuring the recording schedule, you must also set the alarm type and enable the *Trigger Channel* check box in the *Linkage Method of Alarm Input Settings* interface. For detailed information, please refer to the section on alarm inputs on page 53.
 - **Motion or Alarm:** Video will be recorded when an external alarm is triggered, or motion is detected. Besides configuring the recording schedule, you must also configure the settings on the *Motion Detection* and *Alarm Input Settings* interfaces.
 - **Motion and Alarm:** Video will be recorded when Motion and Alarm are triggered at the same time. Besides configuring the recording schedule, you must also configure the settings on the *Motion Detection* and *Alarm Input Settings* interfaces.
 - **Audio Exception:** Video will be recorded when an audio exception is triggered. You must also configure Audio Exception for this.
 - **Line Crossing Detection:** Video will be recorded when a Line Crossing Detection event is triggered. You must also configure Line Crossing Detection for this.
 - **Intrusion Detection:** Video will be recorded when an Intrusion Detection event is triggered. You must also configure Intrusion Detection for this.

- **Scene Change Detection:** Video will be recorded when a scene detection event is triggered. You must also configure Scene Detection for this.
- **Region Entry Detection:** Video will be recorded when a Region Entry Detection event is triggered. You must also configure Region Entry Detection for this.
- **Region Exit Detection:** Video will be recorded when a Region Exit Detection event is triggered. You must also configure Region Exit Detection for this.
- **Unattended Baggage Detection:** Video will be recorded when an Unattended Baggage event is triggered. You must also configure Unattended Baggage Detection for this.
- **Object Removal Detection:** Video will be recorded when an Object Removal event is triggered. You must also configure Object Removal Detection for this.
- **Event:** Video will be recorded when a VCA event is triggered. Besides configuring the recording schedule, you must configure the settings of the selected VCA event type: Audio Exception Detection, Defocus Detection, Scene Change Detection, Face Detection, Intrusion Detection, Cross Line Detection, Region Entrance Detection, Region Exit Detection, Unattended Baggage Detection, and Object Removal Detection.

Note: Up to eight record types can be selected in a single day.

5. Set the recording periods for the other days of the week if required.
6. Set the desired pre- and post-record times stream type and auto-delete mode.
7. Click **Save** to save changes.

Snapshot (Scheduled snapshots)

You can configure scheduled snapshots and event-triggered snapshots. The captured snapshots can be stored on the SD card (if installed) or a 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.

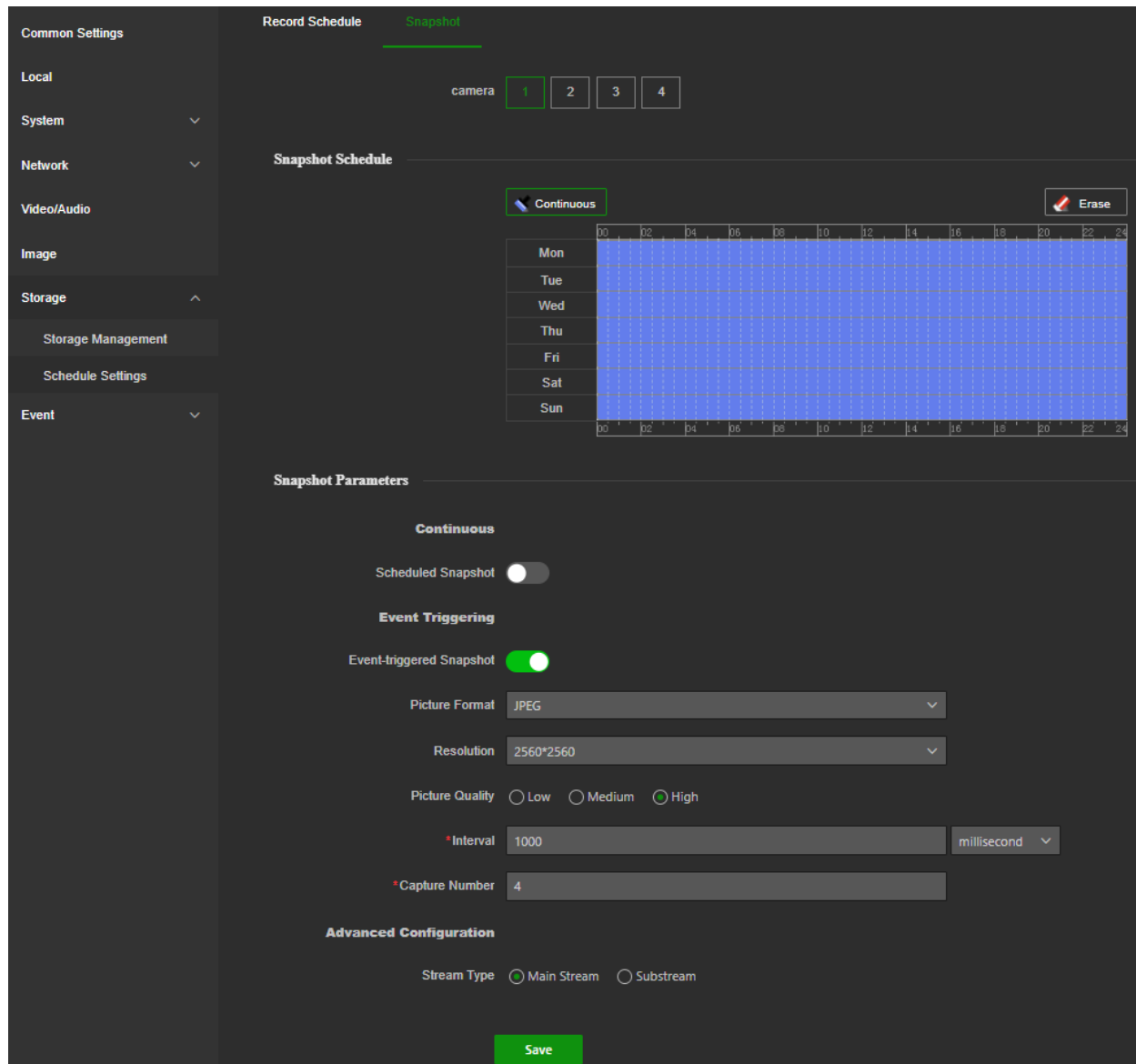
You must enable the option **Scheduled Snapshot** if you want snapshots to be uploaded with a fixed interval to the FTP server. If you have configured the FTP settings, the snapshots will not be uploaded to the FTP if the **Scheduled Snapshot** option is disabled.

You must enable the option **Enable Event-Triggered Snapshot** if you want snapshots to be uploaded to the FTP and NAS when motion detection, VCA event, or an alarm input is triggered. If you have configured the FTP settings, the snapshots will be uploaded to the FTP server.

To set up continuous and event-triggered snapshots:

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

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



2. Click and drag the mouse on the timeline bar of the desired days to set the capture schedule.
3. Enable **Scheduled Snapshot** or **Event-Triggered Snapshot**
4. Configure the snapshot related parameters like resolution, picture quality, etc..
5. Select with Stream Type whether snapshots will be taken in main or substream format.
6. Click **Save** to save changes.

Event

Events can be used to trigger actions whenever the camera is triggered by a physical input or, for example, a VCA event.

Event and Detection

Refer to below event types for the supported events in this category.

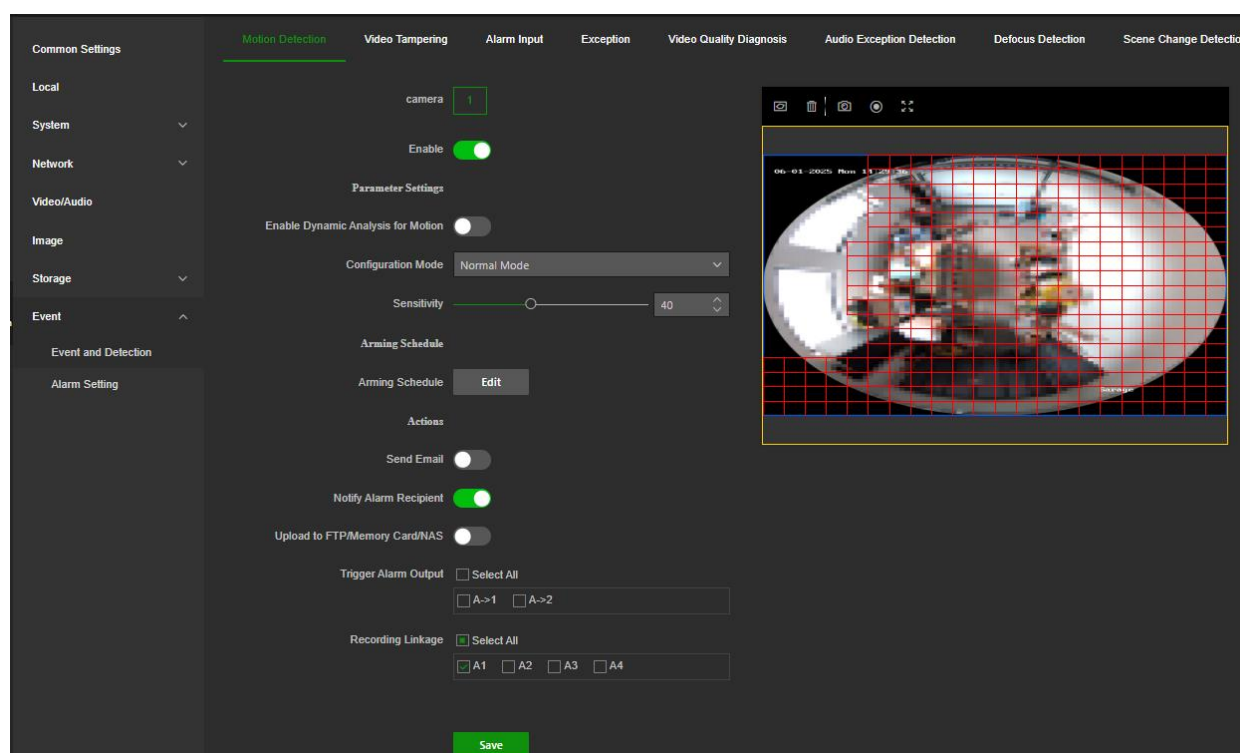
Motion Detection

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

You can draw an area on the screen where you want to detect motion and set the motion sensitivity level, the schedule when the camera is supposed to check for motion as well as which methods are used to alert you to a motion detection alarm.

You can also enable dynamic analysis for motion to verify sensitivity in real time. When there is motion, the area will be highlighted.

Figure 7: Motion detection window



Defining a motion detection alarm requires the following tasks:

1. **Area settings:** Draw an area grid on the image where you want the camera to generate motion detection alarm and set the detection sensitivity level.
2. **Arming schedule:** Click on **Edit** to define the schedule during which the system will be able to detect motion and can trigger actions.
3. **Actions:** Specify the actions triggered by the motion event.
4. **Configuration Mode:** Normal configuration allows you to set the sensitivity level of the motion detection (see Figure 7 above, item 4). Expert configuration gives you additional configuration options. It allows you to define up to eight separate motion areas with different sensitivity and scene parameters.

To set up motion detection in normal mode:

1. Click **Configuration > Event > Event and Detection > Motion Detection**.

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

2. **Enable** Motion Detection. Also, select the **Enable Dynamic Analysis for Motion** option if you want to see real-time motion events.
3. Under Configuration, select **Normal** mode from the drop-down list.
4. Click the **Draw Area icon at the left top above the image preview**. Then click the mouse to set the start point of the area where you want to detect motion. While keeping the mouse button pressed, move to another position and release the mouse button to establish the first detection area. Repeat this step to extend the detection area.

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

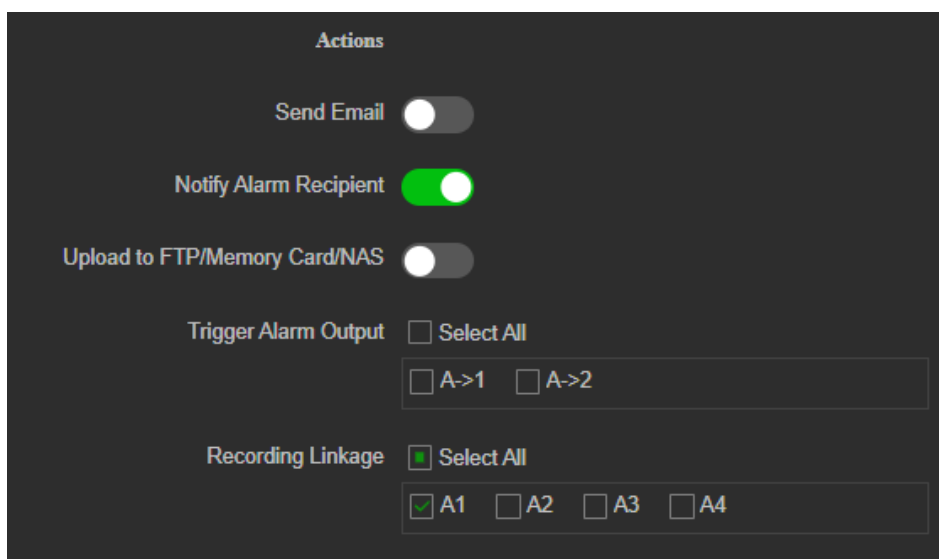
5. Click the **Clear All** icon above the image preview to delete all areas marked and restart drawing.
6. Move the **Sensitivity** slider to set the sensitivity of the detection. All areas will have the same sensitivity level.

- **Set up the arming schedule:**

7. Click the **Edit** button to open the schedule and then drag and click the timeline bar to edit the arming schedule. In the pop-up box, enter the start and end times (hours and minutes).

- **Set up an action for the motion detection alarm:**

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



The screenshot shows the 'Actions' configuration window with the following settings:

- Send Email:** ☐ (disabled)
- Notify Alarm Recipient:** ☒ (enabled)
- Upload to FTP/Memory Card/NAS:** ☐ (disabled)
- Trigger Alarm Output:** ☐ Select All
☐ A->1 ☐ A->2
- Recording Linkage:** ☒ Select All
☒ A1 ☐ A2 ☐ A3 ☐ A4

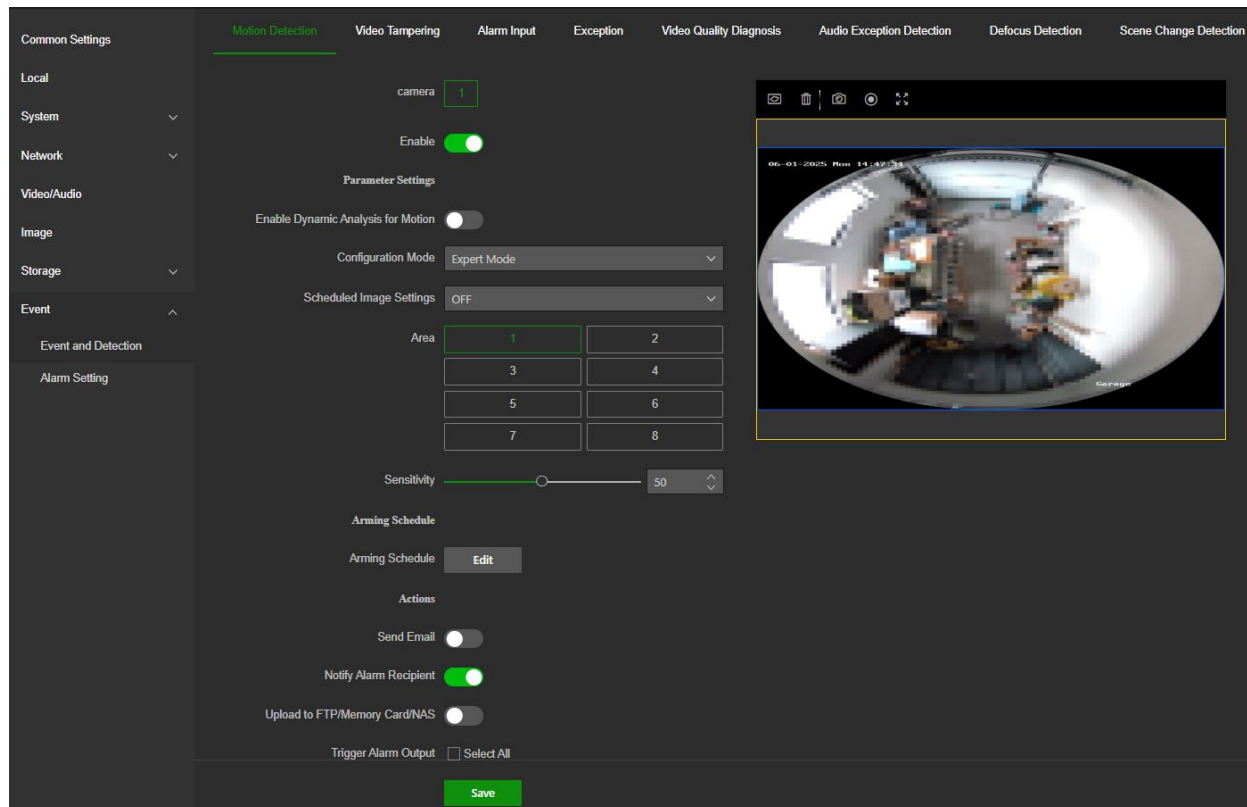
Send Email	<p>Send an email to a specified address when there is a motion detection alarm.</p> <p>Note: You must configure email settings before enabling this option. See “To set up the email parameters” on page 60 for further information. If you want to send the event snapshot together with the email, check the Attached Snapshot option.</p>
Notify Alarm Recipient	<p>Send an exception or alarm signal to remote management software when an event occurs.</p>
Upload to FTP/Memory Card/NAS	<p>Capture the image when an alarm is triggered and upload the picture to NAS, Memory Card, or FTP server.</p> <p>Note: To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS” on page 43 for further information.</p> <p>To upload the snapshot to an FTP, you must first configure the FTP settings. See “To define the FTP parameters” on page 30 for further information. Enable the Upload Type option.</p> <p>To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also select Enable Event-triggered Snapshot under the snapshot parameters. See “Storage” on page 41” for further information.</p>
Trigger Alarm Output	<p>Trigger external alarm outputs when an event occurs. Select “Select All” or each alarm output.</p> <p>Note: This option is only available for cameras that support alarm output.</p>
Recording Linkage	<p>Triggers the recording to start in the camera.</p>

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

Note: some of the above-mentioned actions might not be available on some camera models. They will only appear when supported by the hardware.

To set up advanced motion detection:

1. Click **Configuration > Event > Event and Detection > Motion Detection**.
- **Set up the motion detection area:**
2. **Enable** Motion Detection. Also, select **Enable Dynamic Analysis for Motion** if you want to see where motion occurs in real time.
3. Under Configuration, select **Expert** mode from the drop-down list.



4. Under **Scheduled Image Settings**, select OFF, Auto-Switch, or Scheduled Switch. Default is OFF.

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

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

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

6. Move the **Sensitivity** slider to set the sensitivity of the detection for the selected area.

7. Click **Save** to finish drawing of the first area. Click **Clear All** to delete all areas marked and restart drawing.

Note: Repeat the above 3 steps to draw additional motion detection areas.

8. Click **Save** to save the changes for that area.

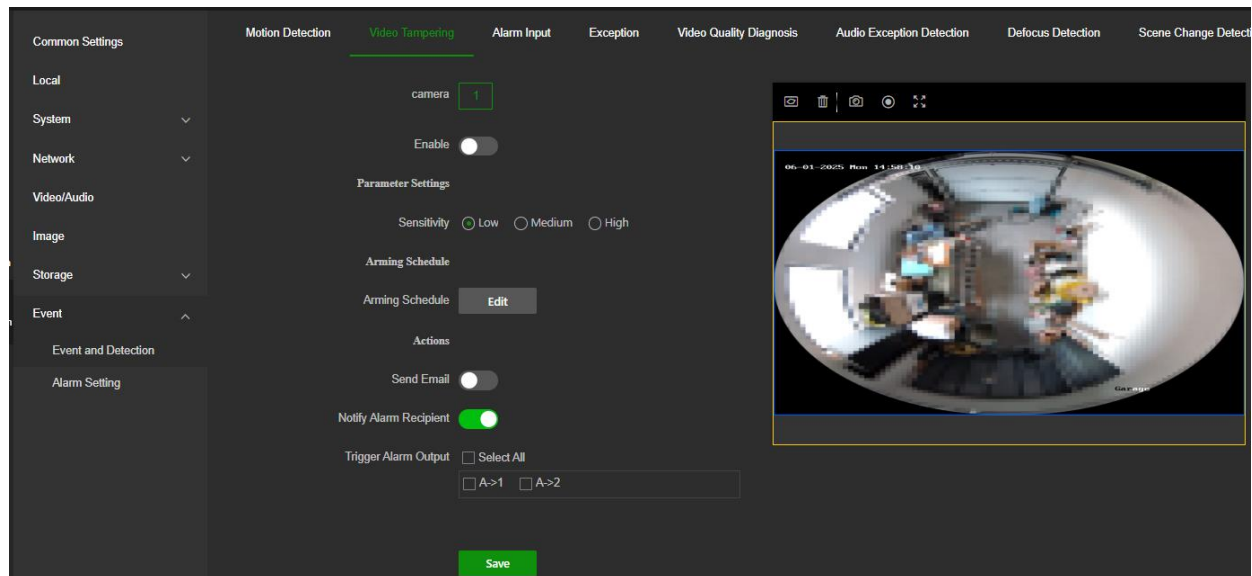
Note: Schedule definition and actions can be configured in the same way as described above for Normal motion detection.

Video Tampering

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

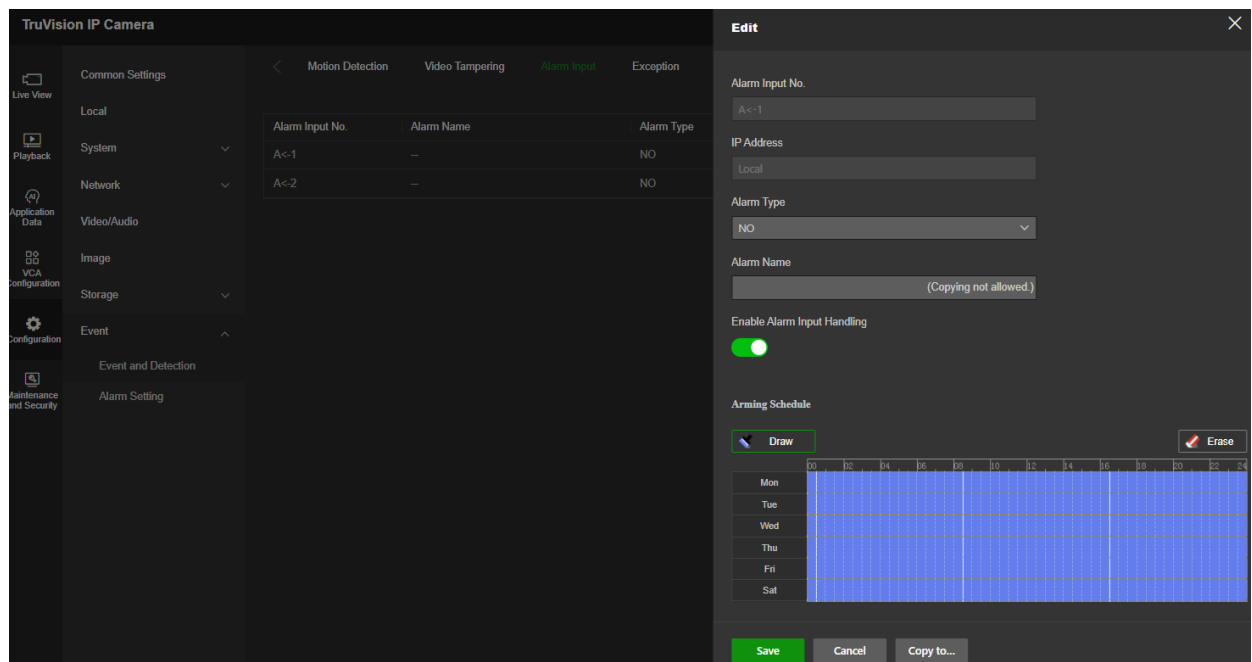
To set up tamper-proof alarms:

1. From the menu toolbar, click **Configuration > Event and Detection > Video Tampering**.



2. **Enable** Video Tampering.
3. Select low, medium, or high detection sensitivity.
4. Edit the arming schedule for video tampering. The arming schedule configuration is the same as that for motion detection.
5. Specify the actions when an event occurs.
6. Click **Save** to save changes.

Alarm Input



To set up the external alarm input:

1. Click **Configuration > Event > Event and Detection > Alarm Input**.
2. In the table, click on the pencil icon to edit the desired alarm input. The alarm type can be NO (Normally Open) and NC (Normally Closed). Enter a name for the alarm input.

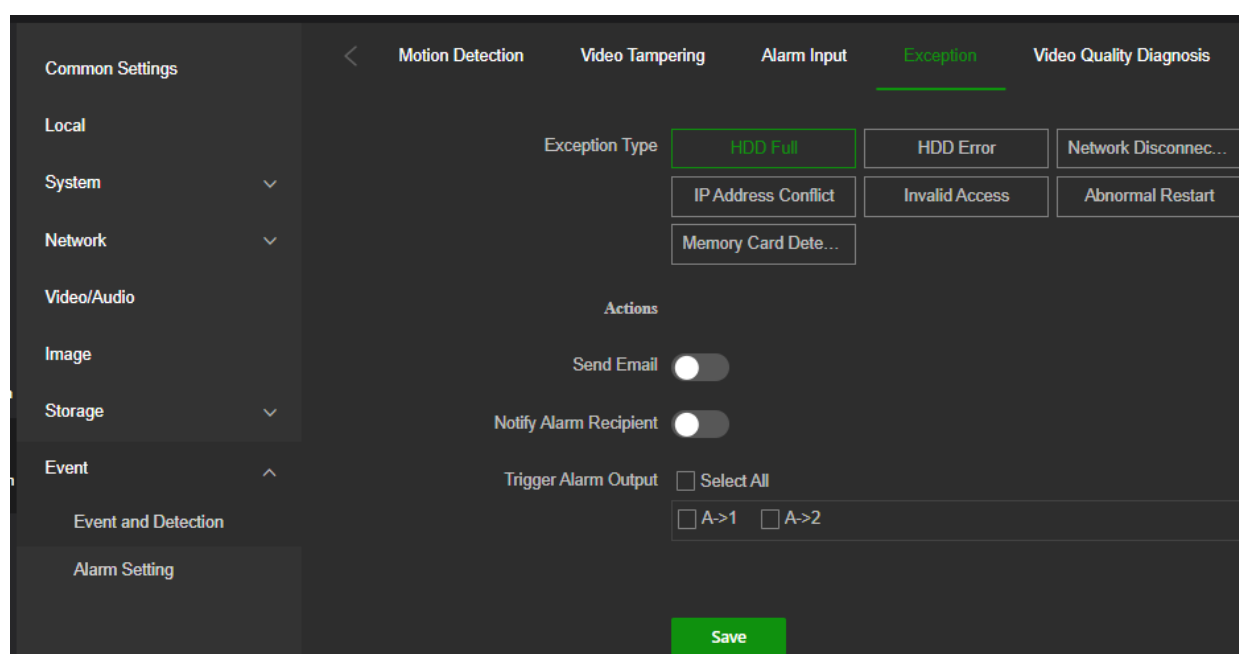
3. Define also an arming schedule for the alarm input.
4. Enable Actions to happen when the alarm input is triggered.

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 Conflict:** Conflict in IP address setting.
- **Invalid Access:** Wrong user ID or password login attempt to the cameras.
- **Abnormal Restart:** The device restarts abnormally.
- **Memory Card Detection:** Issue with overall status of installed SD card.

Figure 8: Exception window



To set up exception alarms:

1. Click **Configuration > Event > Event and Detection > Exception**.
2. Under **Exception Type**, select an exception type.
3. Specify the actions when an event occurs. Select one or more actions when an exception alarm is triggered.

- Click **Save** to save changes.

Video Quality Diagnosis

You can set up the camera to notify you when the image quality decreases. The camera will try to analyze the root cause and report the appropriate event.

Note that this new event type isn't fully recognized by all versions of TruVision Navigator.

The screenshot shows the 'Video Quality Diagnosis' configuration page. On the left is a sidebar with a menu: 'Common Settings' (expanded), 'Local', 'System', 'Network', 'Video/Audio', 'Image', 'Storage', 'Event', 'Event and Detection', and 'Alarm Setting'. The main area has tabs for 'Motion Detection', 'Video Tampering', 'Alarm Input', 'Exception', 'Video Quality Diagnosis' (active), and 'Audio'. Under 'Video Quality Diagnosis', there are four camera selection buttons (1, 2, 3, 4), with '1' highlighted. Below these are sliders for 'Alarm Detection Interval' (set to 5), 'Sensitivity' (set to 5), and 'Alarm Delay Times' (set to 1). A 'Diagnosis Type' dropdown is set to 'Brightness Exception'. Below this is a 'Brightness Exception' toggle switch that is turned on. Further down is an 'Arming Schedule' section with an 'Arming Schedule' label and an 'Edit' button. Below that is an 'Actions' section with a 'Notify Alarm Recipient' toggle switch (turned on) and a 'Trigger Alarm Output' section with checkboxes for 'Select All', 'A->1', and 'A->2'. At the bottom right is a green 'Save' button.

- Select the **Diagnosis Type**. Depending on the camera model, there's multiple Diagnosis types available.
- Activate per selected diagnosis type you want to use the slider button.
- Define per selected also the Sensitivity and Alarm Delay Times
- Click **Save** to save changes
- Repeat steps 2 and 4 to configure additional Video Quality Diagnose types.
- Set the corresponding parameters.

Alarm Detection Interval: Range [5 to 300] determines the minimum time between reporting the same event.

Sensitivity: Range [1 to 9]. The higher the value is, the more easily the exception can be detected.

Alarm Delay Times: Range [0 to 100]. The device uploads the alarm when the alarm occurs for the set number of times.

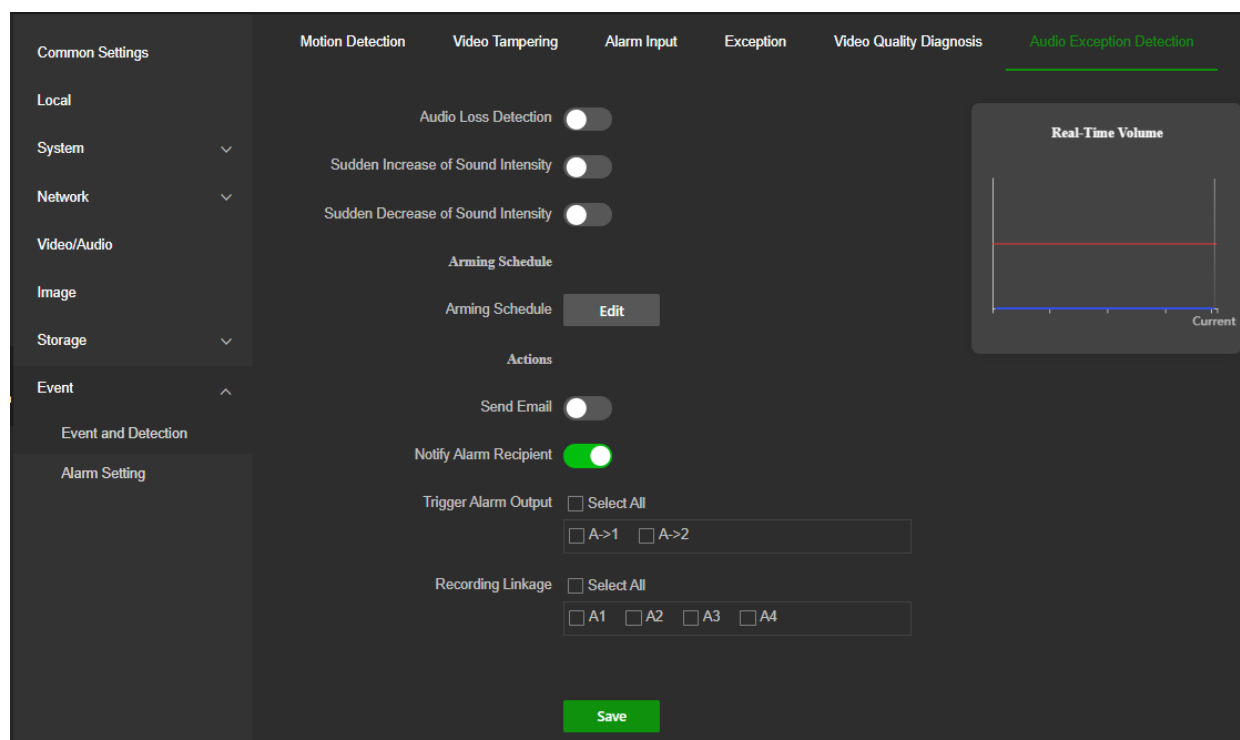
- Click **Edit** Arming Schedule to set the arming schedule.
- Go to Actions to select the linkage methods.
- Click **Save** to save changes.

Audio Exception Detection

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

To set up audio exception detection:

- Click **Configuration > Event > Event and Detection > Audio Exception Detection**.



- Enable **Audio Loss Exception** to activate the audio loss detection function.
- Enable the **Sudden Increase of Sound Intensity Detection** option to detect the steep rise in sound in the surveillance scene. You can set the detection sensitivity and threshold for steep rise in sound.
- Enable the **Sudden Decrease of Sound Intensity Detection** option to detect the steep drop in sound in the surveillance scene. You can set the detection sensitivity and threshold for steep drop in sound.

Notes:

Sensitivity: Range [1-100]. The smaller the value, the greater the change required to trigger detection.

Sound Intensity Threshold: Range [1-100]. It filters the sound in the environment. The louder the environment sounds, the higher the value required. You can adjust it according to the real environment.

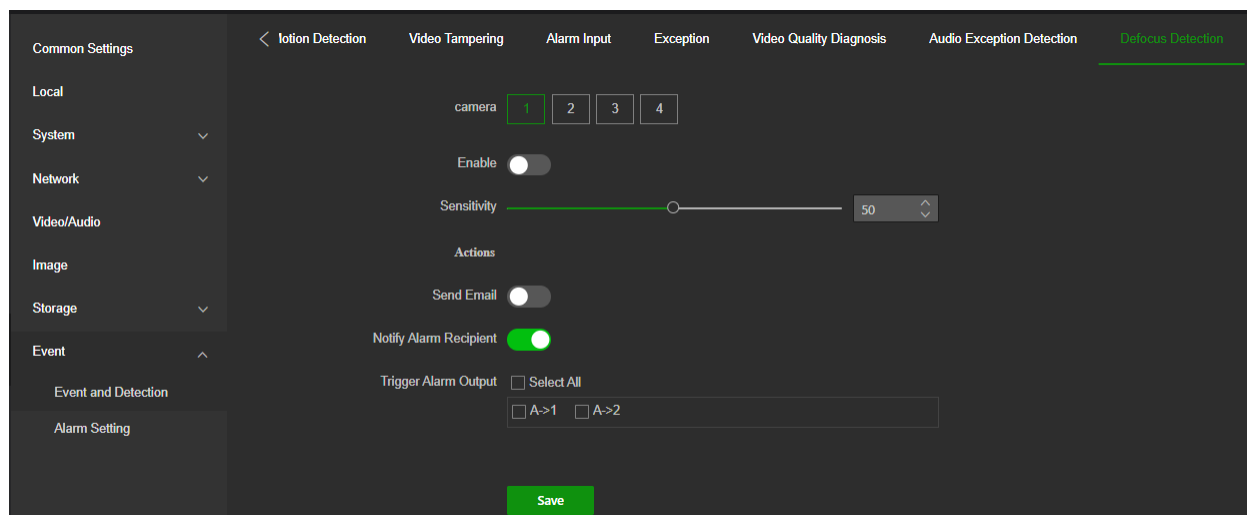
You can view the real-time sound volume on the interface.

5. Click **Edit** to configure the arming schedule.
6. Select recording and/or output **Actions** to be executed in case of audio exception.
7. Click **Save** to save the settings.

Defocus Detection

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

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



To set up defocus detection:

1. Click **Configuration > Event > Event and Detection > Defocus Detection**.
2. **Enable** the function.

Sensitivity: The range is between 1 and 100. The higher the sensitivity level, the faster the defocus event will be triggered.

3. Specify the actions when an event occurs.
4. Click **Save** to save changes.

Scene Change Detection

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

To set up scene change detection:

1. Click **Configuration > Event > Event and Detection > Scene Change Detection**.
2. **Enable** the function.
3. Configure the sensitivity ranging from 1 to 100. The higher the sensitivity, the easier it is to detect a change of scene and trigger the alarm.
4. Click the **Edit** to set the arming schedule.

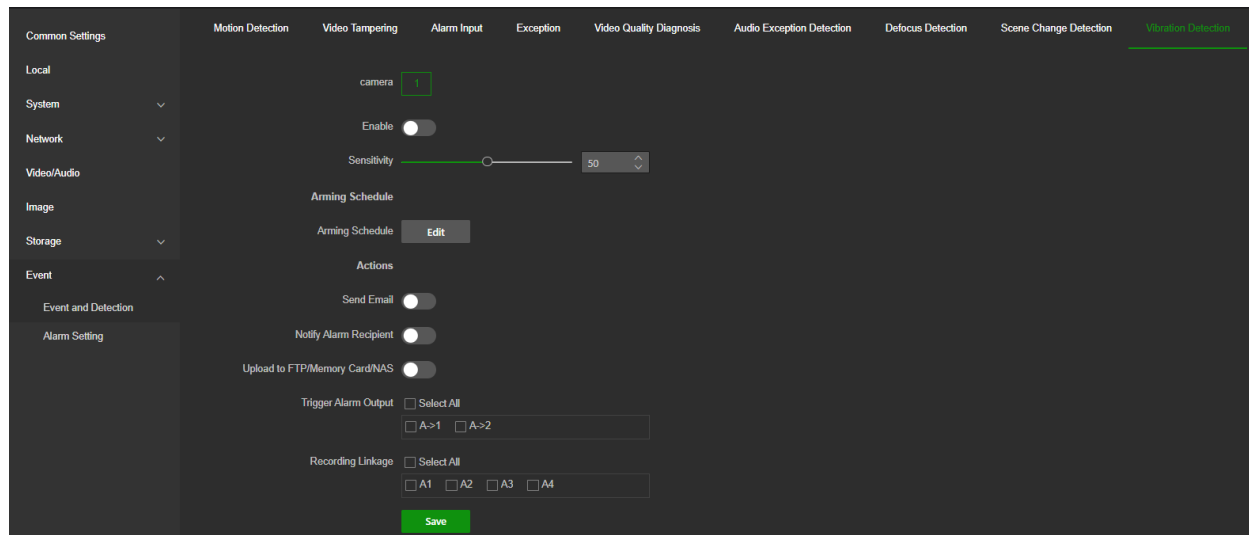
The screenshot shows the 'Scene Change Detection' configuration page. On the left is a sidebar with a menu: 'Common Settings' (expanded), 'Local', 'System', 'Network', 'Video/Audio', 'Image', 'Storage', 'Event' (expanded), 'Event and Detection', and 'Alarm Setting'. The main area has tabs: 'Motion Detection', 'Video Tampering', 'Alarm Input', 'Exception', 'Video Quality Diagnosis', and 'Audio'. Under 'Motion Detection', there are four camera selection buttons (1, 2, 3, 4), with '1' selected. Below is an 'Enable' toggle switch, which is turned on. A 'Sensitivity' slider is set to 50. The 'Arming Schedule' section has an 'Arming Schedule' label and an 'Edit' button. The 'Actions' section includes 'Send Email' (off), 'Notify Alarm Recipient' (on), and 'Upload to FTP/Memory Card/NAS' (off). The 'Trigger Alarm Output' section has a 'Select All' checkbox and two options: 'A->1' and 'A->2'. The 'Recording Linkage' section has a 'Select All' checkbox and four options: 'A1', 'A2', 'A3', and 'A4'. A green 'Save' button is at the bottom right.

5. Set **Actions** to be executed when an event occurs.
6. Click **Save** to save changes.

Vibration Detection

You can set up the camera to notify you when vibration is detected by the camera.

Note that this new event type isn't recognized by all versions of TruVision Navigator.



1. **Enable** Vibration Detection
2. Set sensitivity level. The higher the value, the more sensitive the camera will be to vibrations.
3. Click **Edit** to set the arming schedule.
4. Set the desired **Actions** to be executed when the vibration event occurs.
5. Click **Save** to save the settings.

Alarm Setting

This menu allows you to communicate parameters related to alarm reporting.

FTP

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

To set up the FTP parameters:

1. Click **Configuration > Event > Alarm Setting > FTP**.

The screenshot shows the 'FTP' configuration page within the 'Alarm Setting' section. The left sidebar contains a menu with 'Common Settings', 'Local', 'System', 'Network', 'Video/Audio', 'Image', 'Storage', 'Event', 'Event and Detection', and 'Alarm Setting'. The 'FTP' tab is selected at the top. The main area contains the following settings:

- FTP Protocol:** A dropdown menu set to 'FTP'.
- *Server IP Address:** A text field containing '0.0.0.0'.
- *Port No.:** A text field containing '21'.
- Anonymous Login:** A toggle switch that is currently turned off.
- *User Name:** A text field.
- *Password:** A text field with a password icon.
- Directory Structure:** A dropdown menu set to 'Save in the root directory'.
- Upload Picture:** A toggle switch that is currently turned off.
- Enable Automatic Network Replenishment:** A toggle switch that is currently turned off.
- Test:** A button to test the FTP connection.
- Save:** A green button to save the configuration.

2. Configure the FTP settings, including server address, port, user name, password, directory, and upload type.

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

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

Upload Picture: To enable snapshots to be uploaded to the FTP server.

Enable Automatic Network Replenishment: To upload buffered events from the camera after restoring from a network disconnect.

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

Note: The test button can be used to test FTP server connectivity after connection details have been entered and saved.

Email

Configure the email addresses to which messages are sent when an alarm event occurs.

To set up the email parameters:

1. Click **Configuration > Event > Alarm Setting > Email**.

The screenshot displays the 'Email' configuration page. The sidebar on the left includes 'Common Settings' and 'Event' (expanded to show 'Event and Detection' and 'Alarm Setting'). The main content area has tabs for 'FTP', 'Email' (selected), 'Alarm Output', 'HTTP Listening', and 'Alarm Host'. Under the 'Email' tab, there are input fields for 'Sender', '*Sender's Address', '*SMTP Server', and '*SMTP Port' (set to 25). There is a dropdown for 'E-mail Encryption' (set to TLS) and toggle switches for 'Enable STARTTLS', 'Authentication', and 'Attach picture'. Below these is a 'Recipient' section with '+ Add', 'Delete', and 'Test' buttons. A table with columns 'No.', 'Recipient Name', 'Recipient Add...', and 'Operation' is shown, currently containing 'No data.'. A green 'Save' button is at the bottom right.

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 hostname.

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

Email Encryption: Encrypt via SSL, TLS. TLS is default.

Enable STARTTLS: Emails are sent after encrypted by STARTTLS, and the SMTP Port should be set as 25.

Authentication: If your email server requires authentication, activate this option to use authentication to log in to this server. Enter the login username and password..

Attached Picture: Enable this feature if you want to send emails with attached alarm snapshots.

Interval: This is the time between two actions of sending attached images. Available options are 2, 3, 4, or 5 sec.

Click the **+ Add** button to add email recipients.

Recipient Name: The name of the first user to be notified.

Recipient Address: The email address of the user to be notified.

3. Click **Test** to test the email recipient set up.

Note: Some email clients block the test message that is sent when using the **Test** button. If you believe the settings are correct, then test the email feature by triggering a real video event.

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

Alarm Output

Configure name, schedule, and timing for the available alarm outputs. These alarm outputs can be triggered by other events in the camera.

To configure the alarm output parameters:

1. Click **Configuration > Event > Alarm Setting > Alarm Output**.

Alarm Output No.	Alarm Name	Alarm Status	Activation time (Sec)
A->1		OFF	5
A->2		OFF	5

2. Click the pencil icon to open the edit window of the desired output.
3. Enter an **Alarm Name** for the alarm output.
4. Set the **Activation Time** for the alarm output.
5. Draw the **Arming Schedule** for the alarm output.
6. Click **Save** to save changes.

Note: The button **Manual Alarm** allows you to manually activate/Deactivate the alarm output from this menu.

HTTP listening

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

To set up the HTTP listening parameters:

1. Click **Configuration > Event > Alarm Setting > HTTP Listening**.

The screenshot shows the 'TruVision IP Camera' configuration interface. On the left is a sidebar with icons for Live View, Playback, Application Data, VCA Configuration, Configuration, and Maintenance and Security. The main area has tabs for FTP, Email, Alarm Output, HTTP Listening (selected), and Alarm Host. Below the tabs is a table with columns 'Destination IP...' and 'URL'. A green '+ Add' button is above the table. On the right, an 'Add' dialog box is open, containing fields for 'Destination IP or Host Name' (0.0.0.0), 'URL' (/), 'Protocol' (HTTP), and 'Port No.' (80). There is a toggle for 'ANR' which is turned on. At the bottom of the dialog are 'OK', 'Cancel', and 'Test' buttons.

2. Enter the destination IP or hostname, URL, protocol type, and port number.
 3. Click the **Test** button to test if the service is available.
- Note:** the IP address or hostname 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.
 6. Repeat the above steps to create additional alarm hosts.

Alarm Host

Alarm host needs to be configured in most cases when the camera needs to report events to another device or platform.

The screenshot shows the 'TruVision IP Camera' configuration interface with the 'Alarm Host' tab selected. The left sidebar is the same. The main area has tabs for FTP, Email, Alarm Output, HTTP Listening, and Alarm Host (selected). Below the tabs are two input fields: '* Alarm Host IP' with the value 0.0.0.0 and '* Alarm Host Port' with the value 5001. A green 'Save' button is at the bottom right.

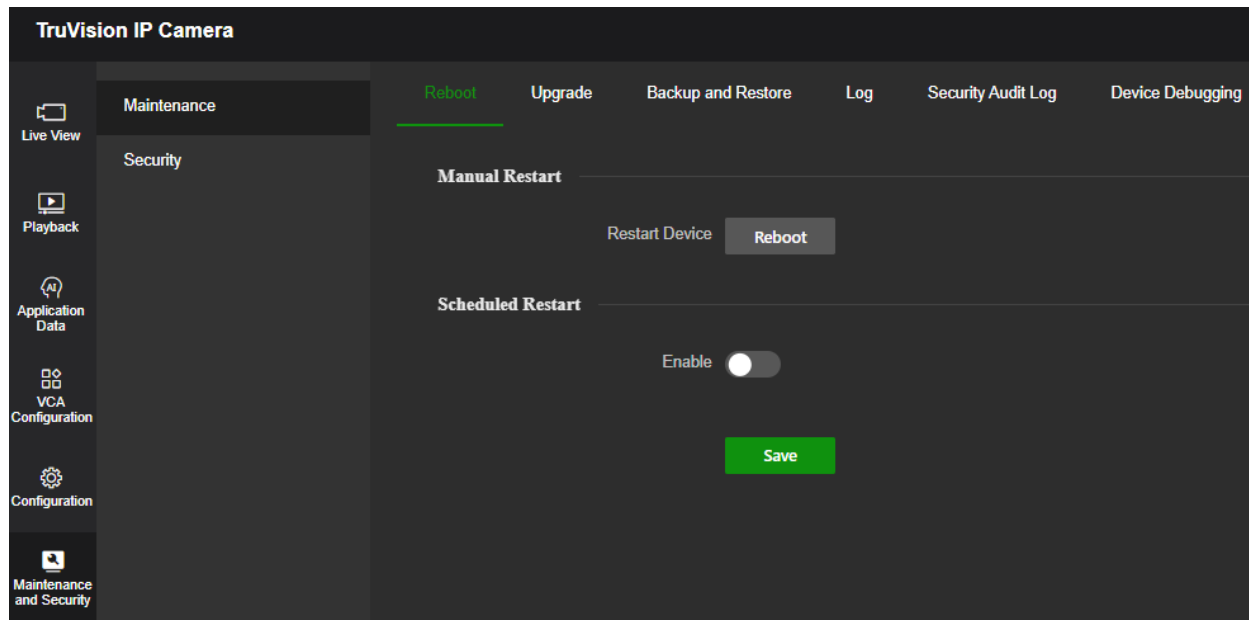
Maintenance and Security

Maintenance tasks and some security related settings can be managed in this menu.

Maintenance

In this menu you can reboot the camera, import/export configuration, debug, and consult the security audit log.

Reboot



Manual Restart

Click **Reboot** to restart the camera.

Scheduled Restart

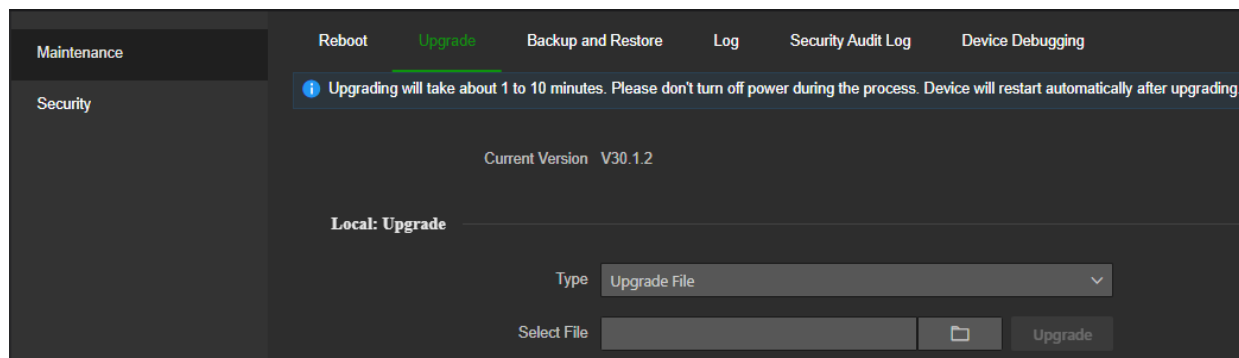
Enable this option if you want to schedule a weekly reboot of the camera. In addition to the day, the exact time for reboot can also be configured.

Note: During reboot, the camera won't be able to do any recordings and it will also lose its connection to other devices and software too.

Upgrade

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 the upgrade. Always refer to the FW release note when upgrading.

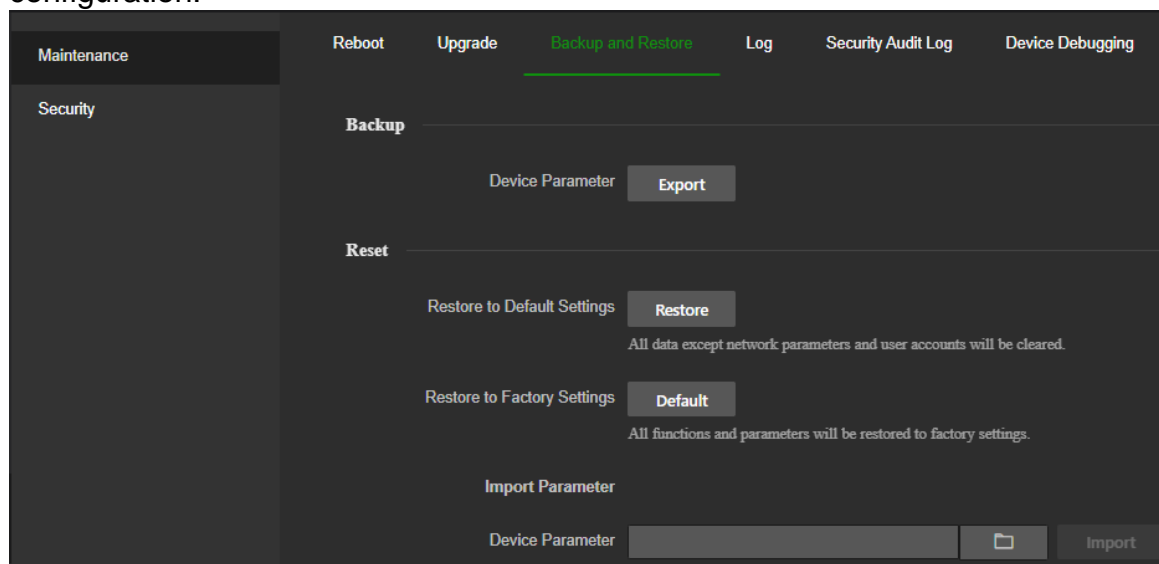


To upgrade the firmware version:

1. Download on to your computer the latest firmware from our website at:
www.firesecurityproducts.com
2. When the zipped firmware file is downloaded to your computer, extract it to the desired destination.
3. From the menu toolbar, click **Maintenance and Security > Maintenance > Upgrade**. Select the **Firmware** or **Firmware Directory** option. Then click the Browse button to locate the 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 and a progress bar indicating the upgrade process followed by a reboot of the camera.
5. When the upgrade is finished, the device will reboot automatically. The browser will also be refreshed.

Backup and Restore

In this menu you can restore camera settings and backup or restore camera configuration.



Click the **Restore** or **Default** button to restore the 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/export a configuration file.

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

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

To import a configuration file:

1. From the menu toolbar, go to **Maintenance and Security > Backup and Restore**
2. Click the **Browse** button to select a configuration file stored on your local PC or network and then click Import to start importing this file. Depending on the selected file, a password might be needed to import the configuration file.

To export a configuration file:

1. To export camera settings, click **Export** and set a password for the exported configuration file. Choose any password you want and make sure to remember it when importing the file.

Device Auto Maintenance

The camera can be scheduled to restart once a week. To do this, enable the option **Enable Auto Maintenance** and select the day and time when the camera needs to be restarted. We do not recommend using this option since it will always interrupt normal camera operation during the rebooting process.

Log

For some camera models it might be needed to configure a NAS or install an 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 depends on the capacity of the storage devices. When this capacity is reached, the system will start overwriting older logs.

Maintenance

Security

Reboot

Upgrade

Backup and Restore

Log

Security Audit Log

Device Debugging

Primary Type

Minor Type

Select Time

All Types

All Types

2025-01-07 00:00:00 - 2025-01-07 23:59:59

Search

Export TXT File

Export CSV

No.	Time	Primary Type	Minor Type	Channel No.	Local/Remote User	Remote Host IP Addr...
1	2025-01-07 09:22:23	Operation	Remote: Get Status	—	admin	192.168.1.115
2	2025-01-07 09:22:20	Operation	Remote: PTZ Control	—	admin	192.168.1.115
3	2025-01-07 09:22:20	Operation	Remote: Get Param...	—	admin	192.168.1.115
4	2025-01-07 09:22:20	Operation	Remote: Get Param...	—	admin	192.168.1.115
5	2025-01-07 09:22:19	Operation	Remote: Get Param...	—	admin	192.168.1.115
6	2025-01-07 09:22:19	Operation	Remote: PTZ Control	—	admin	192.168.1.115
7	2025-01-07 09:22:19	Operation	Remote: Get Param...	—	admin	192.168.1.115
8	2025-01-07 09:22:19	Operation	Remote: Get Param...	—	admin	192.168.1.115
9	2025-01-07 09:22:19	Operation	Remote: Get Param...	—	admin	192.168.1.115
10	2025-01-07 09:22:19	Operation	Remote: Get Param...	—	admin	192.168.1.115
11	2025-01-07 09:22:19	Operation	Remote: Get Param...	—	admin	192.168.1.115
12	2025-01-07 09:22:19	Operation	Remote: Get Param...	—	admin	192.168.1.115
13	2025-01-07 09:22:19	Operation	Remote: Get Param...	—	admin	192.168.1.115
14	2025-01-07 09:22:19	Operation	Remote: Get Param...	—	admin	192.168.1.115
15	2025-01-07 09:22:19	Operation	Remote: Get Param...	—	admin	192.168.1.115
16	2025-01-07 09:22:19	Operation	Remote: Get Param...	—	admin	192.168.1.115
17	2025-01-07 09:22:19	Operation	Remote: Get Param...	—	admin	192.168.1.115
18	2025-01-07 09:22:19	Operation	Remote: Get Param...	—	admin	192.168.1.115
19	2025-01-07 09:22:19	Operation	Remote: Get Param...	—	admin	192.168.1.115

Total 789

20 / page

< 1 2 3 4 5 6 ... 40 >

1 / 40 Go

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

Primary Type: There are four types of logs: Alarm, Exception, and Operation. You can also search All. See Table 1 below for their descriptions.

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

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

Table 1: Types of logs

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

To search logs:

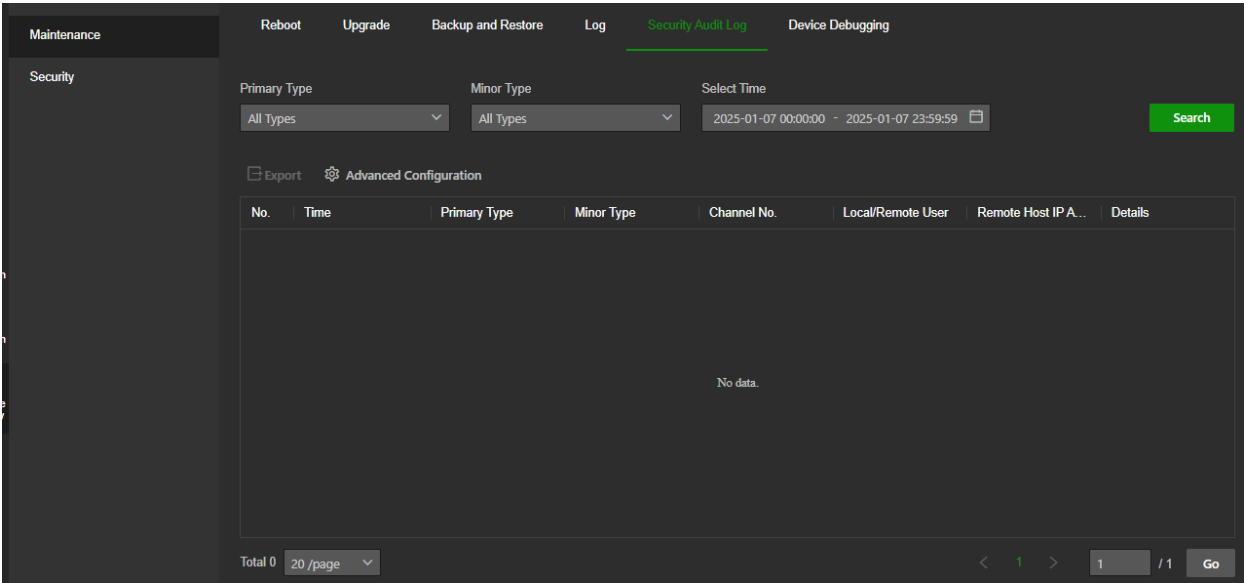
1. From the menu toolbar, go to **Maintenance and Security > Log**.
2. In the **Primary Type** and **Minor Type** drop-down list, select the desired options.
3. Set the start and end date & time for search.
4. Click **Search** to start the search operation. The results appear in the table below.

Note: If needed, you can also export the log files to your local computer in .txt or .csv format.

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's flash memory every 30 minutes.

Due to limited storage in the flash memory, you can save the logs on a log server.



To search the security audit log:

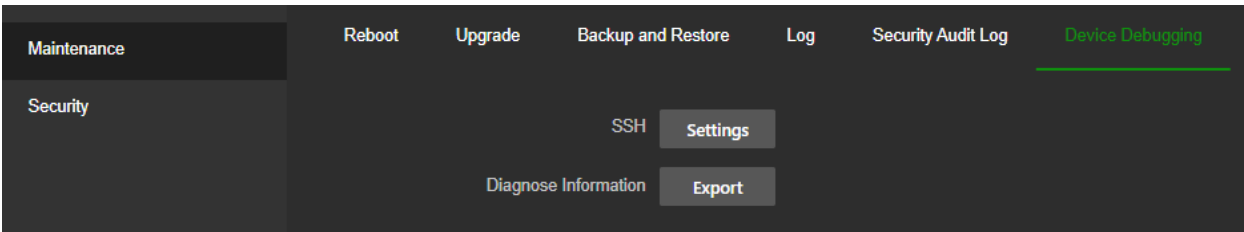
1. From the menu toolbar, go to **Maintenance and Security > Security Audit Log**.
2. In the **Primary Type** and **Minor Type** drop-down list, select the desired options.
3. Set the start and end date&time for search.
4. Click **Search** to start the search operation. The results appear in the table below.

Notes:

- If needed, you can also export the log files to your local computer in .txt or .csv format.
- Via **Advanced Configuration** you can define a log upload server that can be used to send security log info to.

Device Debugging

This menu can be used for troubleshooting or debugging tasks.



Click the **Settings** button to enable SSH.

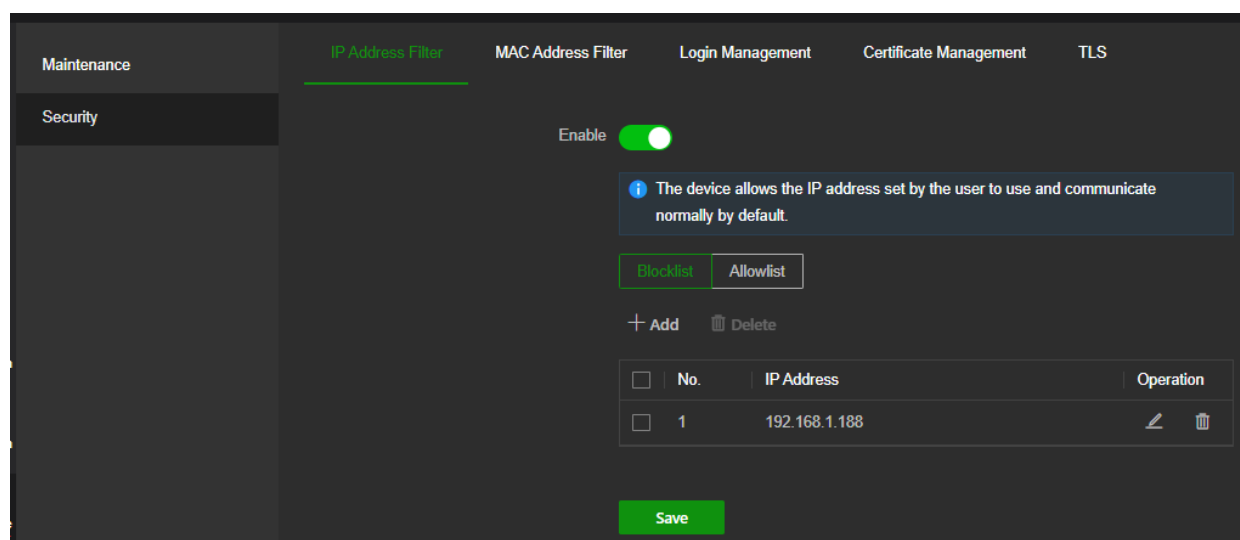
Click the **Export** button to export diagnostic device information.

Security

Security-related parameters, such as IP and MAC address filter, can be managed in this menu.

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.

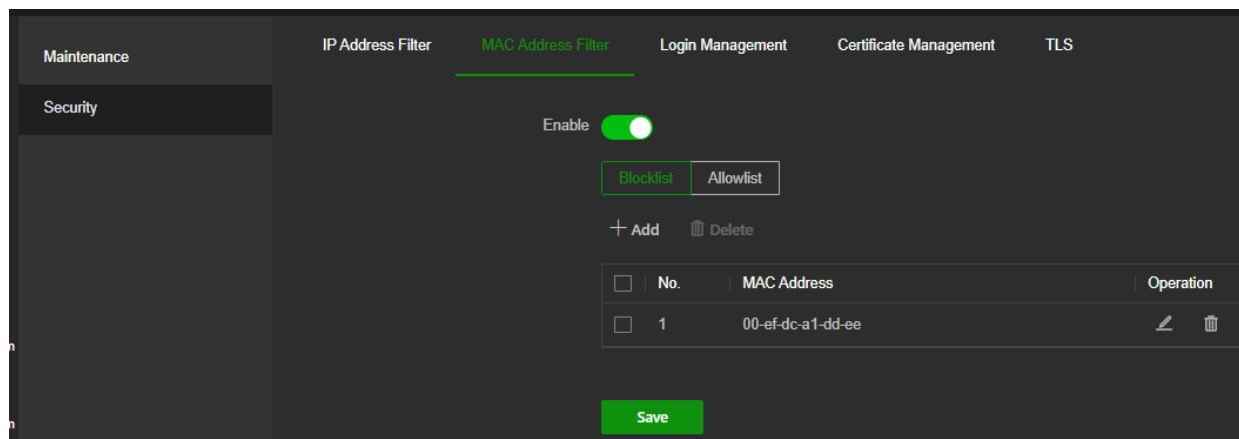


To define the IP address filter:

1. From the menu toolbar, click **Maintenance and Security > Security > IP Address Filter**.
2. **Enable** the filter.
3. Select the type of IP Address Filter in the drop-down list: Blocklist or Allowlist.
4. Click **Add** to add an IP address and enter the address.
5. Click the pencil or delete icon in the table to modify or delete a listed IP address.
6. Click **Save** to save the changes.

MAC address filter

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



To define the MAC address filter:

1. From the menu toolbar, click **Maintenance and Security > Security > Mac Address Filter**.
2. **Enable** the function.
- 3 Select the type of MAC Address Filter in the drop-down list: Blocklist or Allowlist.
4. Click **Add** to add a Mac address and enter the address. The MAC address format needs to be xx-xx-xx-xx-xx-xx
5. Click the pencil or delete icon in the table to modify or delete a listed MAC address.
- 6 Click **Save** to save the changes.

Login Management

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

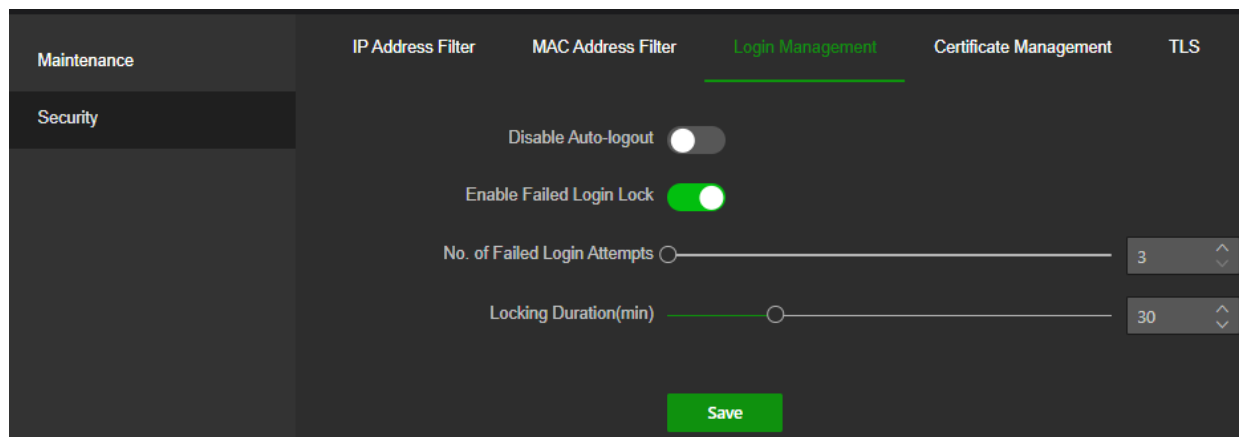
Disable Auto-logout: By default, when logged into the live view webpage or smart display webpage and there is no activity for at least five minutes, the system will automatically log out. Select this function to disable automatic log-out.

Enable 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 a user performs seven failed username/password attempts.
- If the IP address is locked, you can log into the device after the **Locking Duration** time has expired.

To enable the failed login lock:

1. Click **Maintenance and Security > Security > Login Management**.



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

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

Notes:

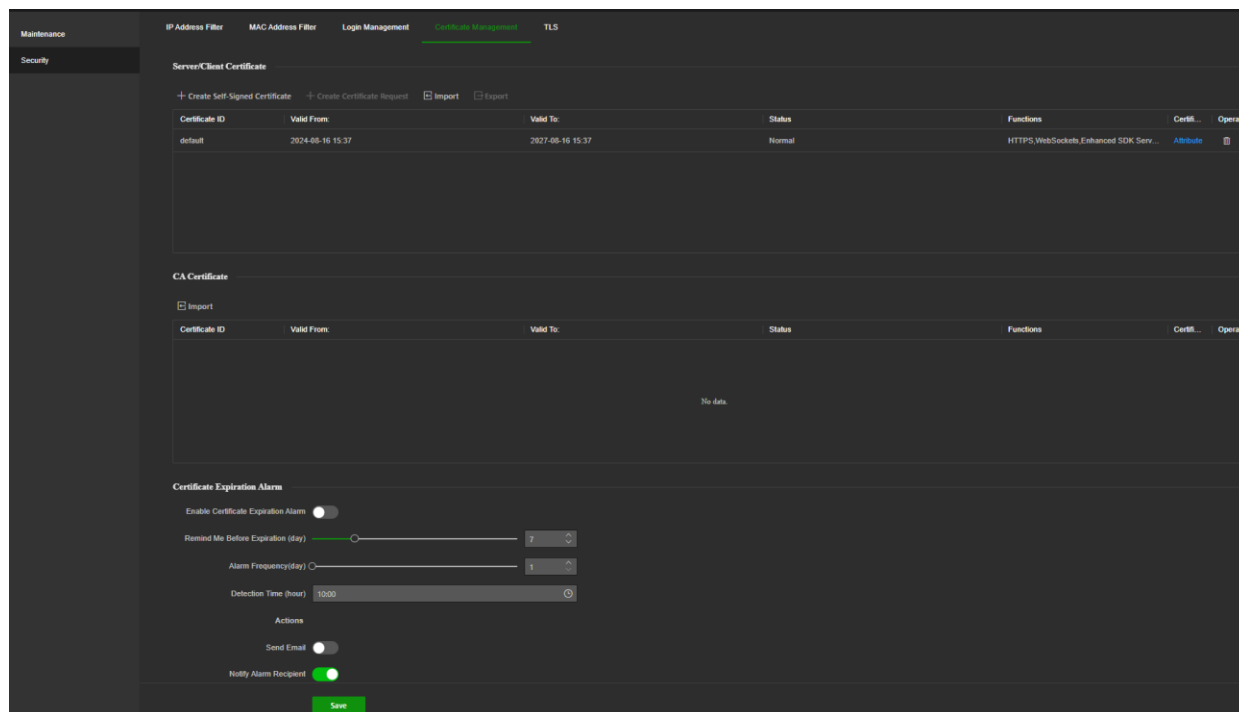
- A. The IP address will be blocked when the number of failed login attempts from a user reaches the number of failed username/password attempts configured in the camera (there is no difference in the number of attempts for the admin/operator/user).
- B. If the IP address is blocked, log in to the device again after 30 minutes.

Certificate Management

It helps manage the server/client certificates and CA certificate and sends an alarm if the certificates will expire or are expired/abnormal.

To manage certificates:

1. Click **Maintenance and Security > Security > Certificate Management**.



To create a self-signed certificate:

1. Click **Create Self-signed Certificate**.
2. Enter certificate ID, country, Domain/IP, validity, and other information. The certificate ID should be numbers or letters of less than 64 characters.

Create Self-Signed Certificate

Certificate ID *

Public Key Length

2048

Country *

Domain/IP *

Validity Period *

day(s)

Password

Province/State

Locality

Save

Cancel

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

4. (Optional) After selecting a certificate, click **Export** to export the certificate, click **Delete** to delete the certificate.

To create a certificate request:

1. Select a saved self-signed certificate.
2. Click **Create Certificate Request**.
3. Enter the related information before saving the request. Otherwise, it cannot be saved.

Create Certificate Request [X]

Certificate ID *
default

Country *
[Empty field with red border]
The item cannot be empty.

Domain/IP *
914fc5761be00faf9ac3b9c9ab87892f

Province/State
[Empty field]

Locality
[Empty field]

Organization
[Empty field]

Organizational Unit
[Empty field]

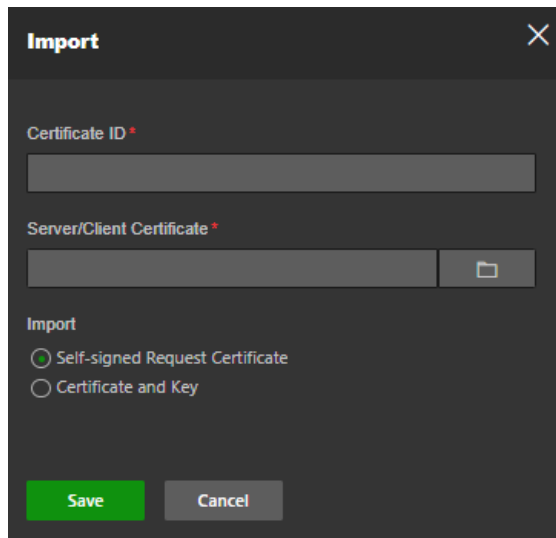
Email
[Empty field]

[Save] [Cancel]

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

To import a certificate:

1. Click **Import**
2. Enter the certificate ID, click the Browse button to select the desired server/client certificate, select the desired import method, and enter the required information.
3. Click **Save** to save the changes.



The image shows a dark-themed 'Import' dialog box with a close button (X) in the top right corner. It contains two text input fields: 'Certificate ID *' and 'Server/Client Certificate *'. The 'Server/Client Certificate' field has a folder icon to its right. Below these fields, there is a section titled 'Import' with two radio button options: 'Self-signed Request Certificate' (which is selected) and 'Certificate and Key'. At the bottom, there are two buttons: a green 'Save' button and a grey 'Cancel' button.

Note:

- Up to 16 certificates are allowed.
- If certain functions are using the certificate, it cannot be deleted.
- You can view the functions that are using the certificate in the Functions column.
- You cannot create a certificate that has the same ID as that of the existing certificate, nor import a certificate that has the same content as that of the existing certificate.

To manage CA certificate:

1. Click **Import**
2. Enter certificate ID, click Browser to select the desired server/client certificate, select the import method, and enter the required information.
3. Click **OK** to save the changes.

Note: Up to 16 certificates are allowed.

To enable certificate expiration alarm:

1. Check **Enable Certificate Expiration Alarm**. If enabled, notification messages that certificates will soon expire, have expired, or are abnormal, will be sent to the saved email address or alarm recipient.

2. Select the **Remind Me Before Expiration (day)**, **Alarm Frequency (day)**, and **Detection Time (hour)** periods.

Note:

- If you set the reminder day before expiration to 1, then the camera will remind you the day before the expiration day. You can select between 1 to 30 days. Seven days is the default reminder days.
- If you set the reminder day before expiration to 1, and the detection time to 10:00, and the certificate will expire at 9:00 the next day, the camera will remind you at 10:00 the first day.

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

TLS

The Transport Layer Security (TLS) protocol aims primarily to provide privacy and data integrity between two or more communicating applications. TLS settings are effective for HTTP(S) and enhanced SDK service.

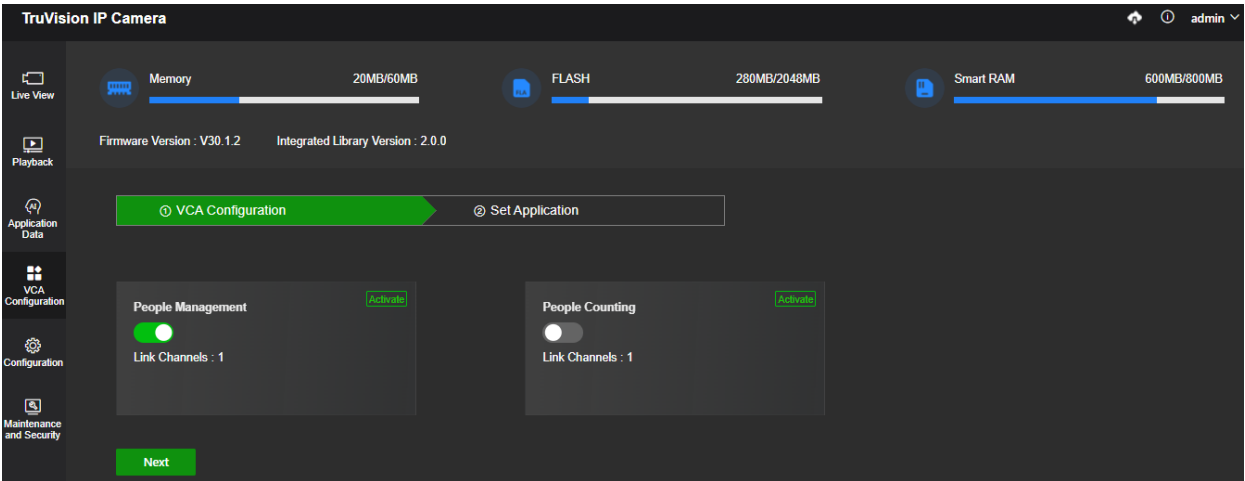
To configure TLS:

1. Go to **Maintenance and Security > Security > TLS** and enable the desired TLS protocol.
2. Click **Save**.

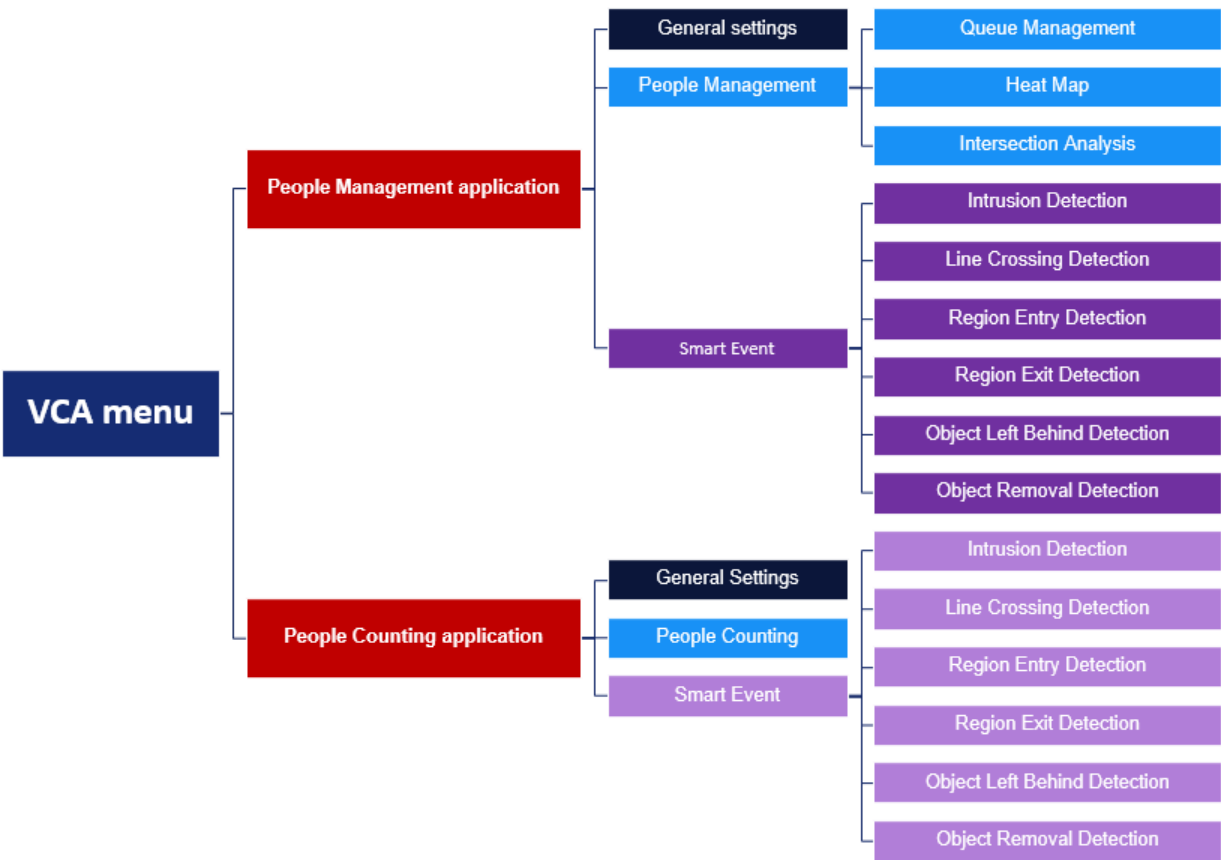
VCA Configuration

Use this menu to configure smart event configuration features such as Cross Line Detection, Intrusion Detection, Face Capture, and others.

Some of these features are only available in specific VCA applications.



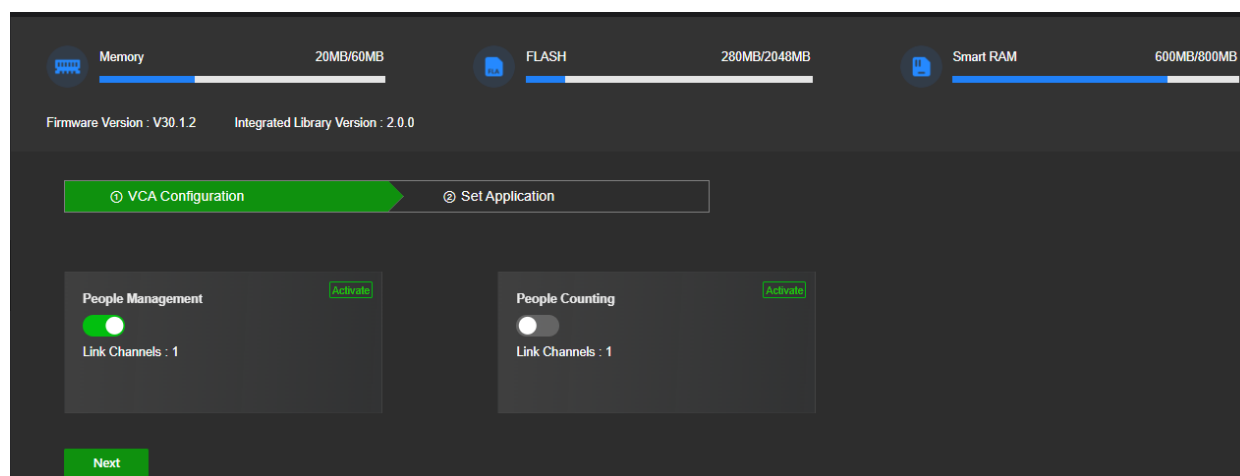
In menu VCA Configuration we can see the available device memory and can enable VCA applications. In case of this camera, there are two main VCA applications **People Management** and **People Counting**. Both applications support a series of features which are outlined below.



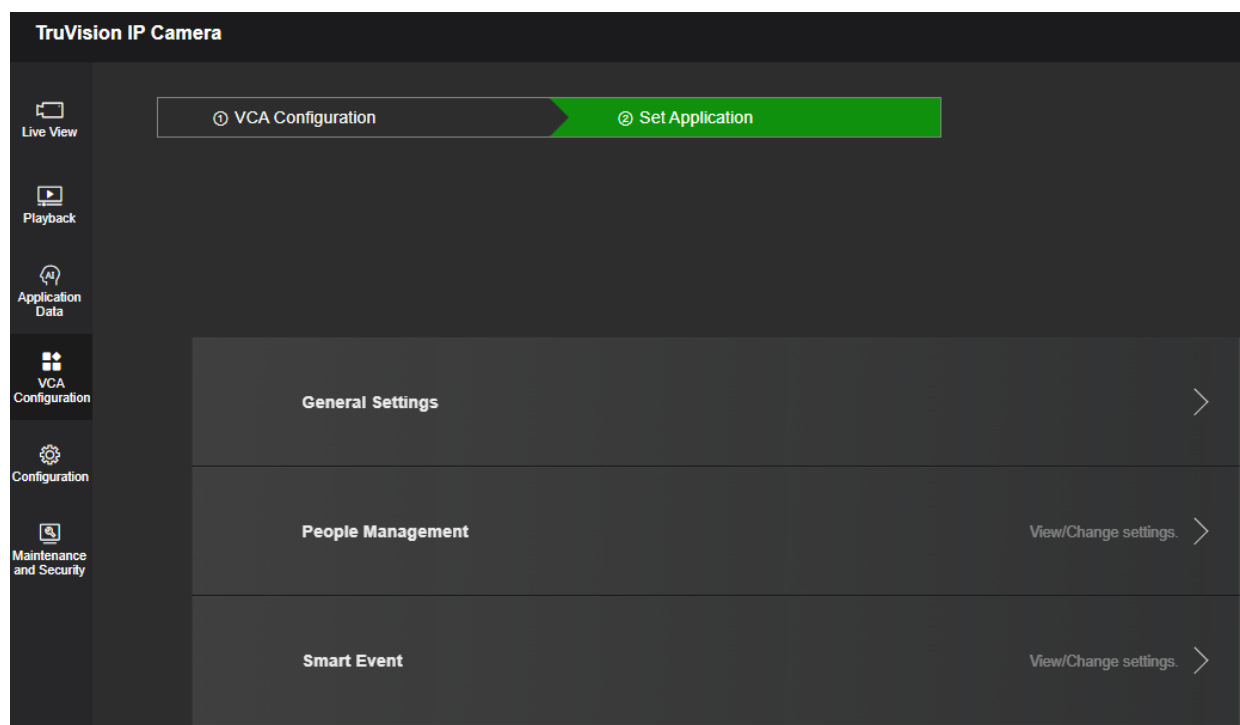
People Management

In people management mode, the camera supports besides Queue Management, Heat Map, and Intersection Analysis also the most common VCA smart event we have in other TruVision IP cameras.

Go to VCA Configuration where you can enable the People Management application.



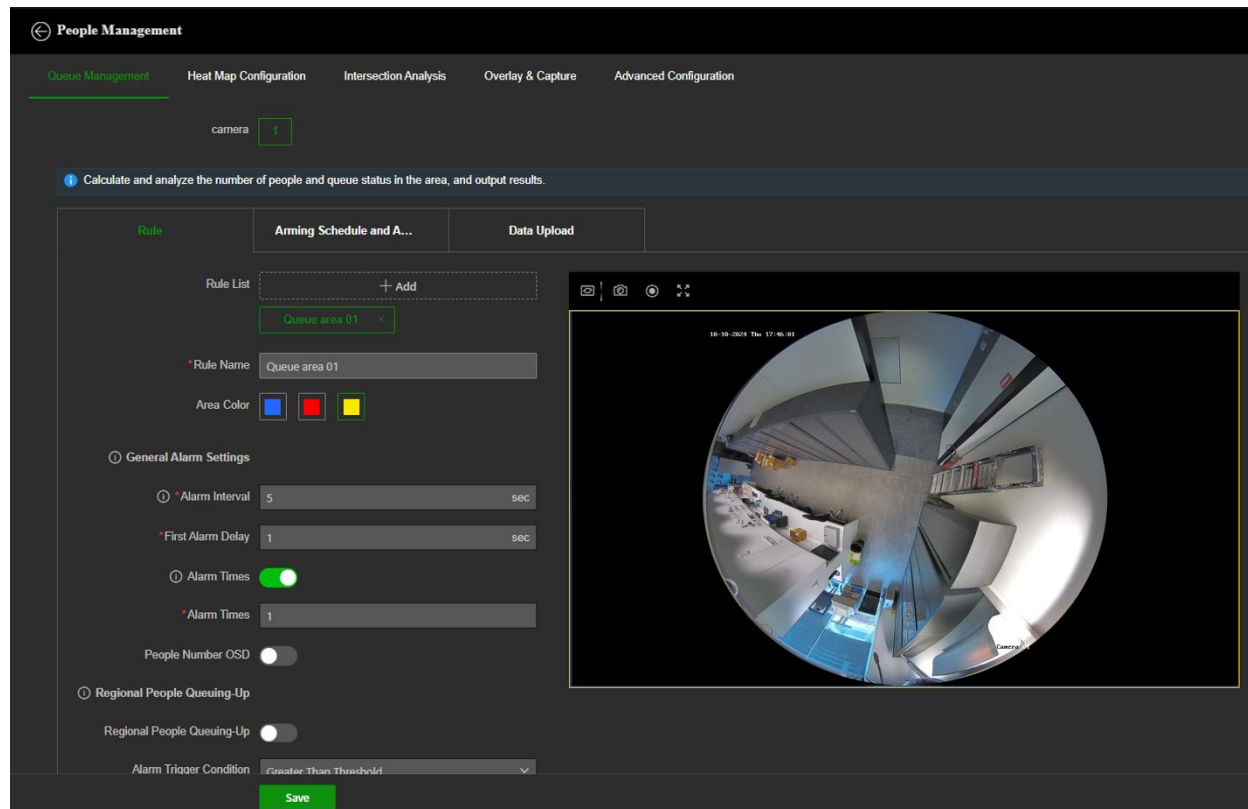
Click **Next** to go to the People Management related parameters and VCA features.



General Settings contains event reporting related parameters such as Camera Info, FTP, Email, Alarm Output, and HTTP listening. Each of these features are described in earlier sections in this manual. Click on People Management to configure the three People Management related features.

Queue Management

This feature is used to count the number of people queuing up in a defined area with their waiting time.



Refer to *Set Regional People Queuing-Up* to set regional people queuing-up detection.

Refer to *Set Waiting Time Detection* to set waiting time detection.

Refer to *Queue Management Statistics* to set and view queue management statistics.

Set Regional People Queuing-Up

It is used to count people queuing-up in defined areas. Alarms are triggered when the alarm threshold condition and the alarm trigger are both met.

How to configure:

1. Go to **VCA Configuration > Set Application > People Management > Queue Management > Rule**.
2. Click Add and enter a name for the rule you want to create.
3. Select an area color and click the drawing icon above the image to draw a rule area. After drawing the last line of the area, right-click the mouse to finish drawing.

Note:

Up to 8 areas can be set at the same time.

Try not to overlap the areas.

4. Set rule parameters.

Alarm Interval: During the set alarm interval, alarms of the same type only trigger one notification.

People Number OSD: It displays the number of people in the live view window.

Ignore Situation of No People: The device will not trigger an alarm when there are no people in the scene. This function can filter the potential alarm condition under which the value is less than the set alarm threshold and no people present in the scene.

5. Select **Regional People Queuing-Up** and set **Alarm Trigger Condition** and **Alarm Threshold**. When the people number in the set area reaches alarm threshold and triggering condition, an alarm will be triggered.

6. Click **Save**.

Note: You can set the parameters of multiple areas by repeating the above steps.

7. For the **Arming Schedule and Actions**, follow the same procedure as described in earlier event related sections of this manual.

Note: Select the rule in the rule list and click **Copy to...** to copy the related arming schedule and action settings to other rules.

Optional: Click Data Upload to set data uploading. Both real-time uploading and scheduled uploading are supported. Click Save after finishing the settings.

Real-Time Uploading: Check Real-Time Upload and the device uploads the detected target ID, waiting duration, and regional people number in real-time.

Scheduled Uploading: The device uploads the people number whose waiting duration is equal to or larger than the Min. Duration of Stay at the integral point.

For example, if the min. duration of stay is set as 10 sec and two areas are covered, the device, at the integral point, will upload the people number when the duration of stay is equal to or longer than 10 sec in two areas respectively.

Optional: Set overlay and capture parameters via the **Advanced Configuration** tab.

Go to **Application Data > Queue Management Statistics** to view detailed Queue Management data analysis.

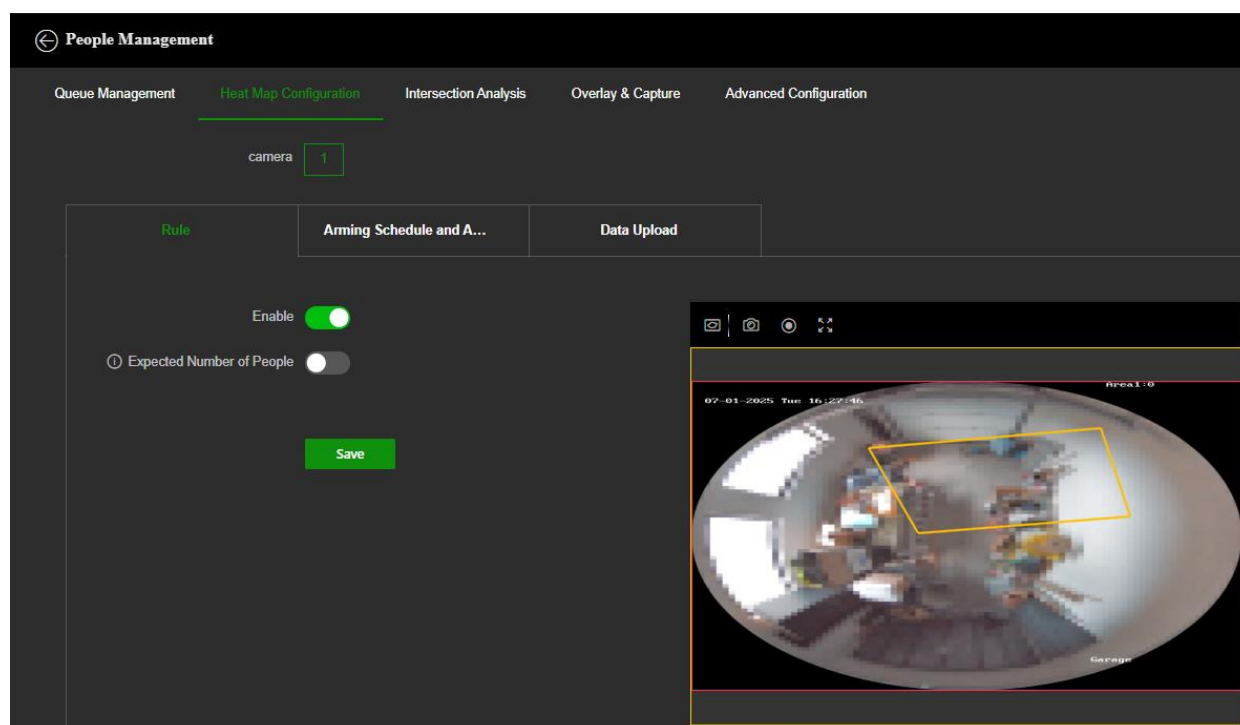
Heat Map Configuration

Heat map is a graphical representation of data represented in colors. The heat map function of the camera is used to analyze the visiting times and dwelling time of customers in a configured area.

Notes:

- The function is only supported in the software decoding mode, or the display mode of fisheye view in the hardware decoding mode.

- Make sure to enable the application on the VCA page first. Make sure you have enough memory, RAM, and FLASH to enable the application, otherwise, you need to disable other applications first.



To configure Heat Map:

1. Go to VCA Configuration and enable the People Management application.
2. Go to **VCA Configuration > Set Application > People Management > Heat Map Configuration**.
3. Check **Enable** to enable the function.
4. Draw a detection area by clicking the draw button at the top left above the camera image draw area. Right-click to complete drawing.
5. Configure the **Expected Number of People** for the area. It refers to the max. expected number of people for heat map counting.
 ON: It refers to that the camera will compare the max. number of the people in the actual scene with the set expected number of people and take the larger one as the max. number of people for heat map.
 OFF: It refers to that the camera will take the actual number of people as the max. value of heat map.
6. Click **Save**.
7. For the Arming Schedule and Actions, follow the same procedure as described in earlier event related sections of this manual.

Optional: Click **Data Upload** to set the data uploading information. Click **Save** to save the settings.

Uploading Data Type

Dwell Time: It refers to the target's dwelling time in the detection area.

Dwell Time and Number of People: It refers to the target's dwelling time in the detection area and the people number in the detection area.

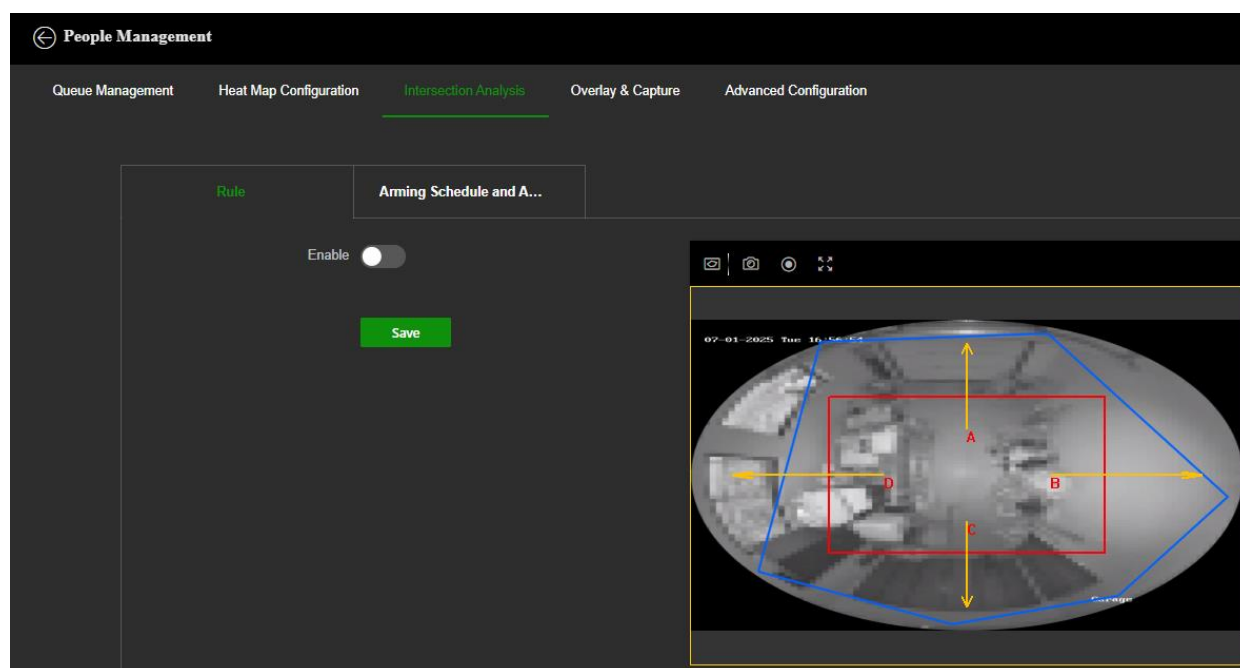
Optional: Set overlay and capture parameters via the **Advanced Configuration** tab.

2. Optional: View version and set filtering condition. For detailed settings, refer to Advanced Settings.

Go to **Application Data > Heat Map** to check Heat Map statistics.

Intersection Analysis

Intersection analysis is used to detect the flow of people in an intersection-like scene. To use this feature, go to **VCA Configuration** and **Enable** the People Management application. Then click Next to enable the function.



To configure Intersection Analysis Map:

1. Go to **VCA Configuration > Set Application > People Management > Intersection Analysis > Rule**.
2. Check **Enable** to enable the function.
3. Click the draw icon at the top left above the image to draw a rule area. Left click the endpoints in the live view window to define the boundary of the set rule area, and right-click to finish drawing.
4. Adjust as desired the arrow direction on each edge of the area. The arrow stands for the direction that the flow leaves the intersection.
5. Go to **Arming Schedule** and **Actions** to set the arming schedule and select the actions.
6. Click **Save**.

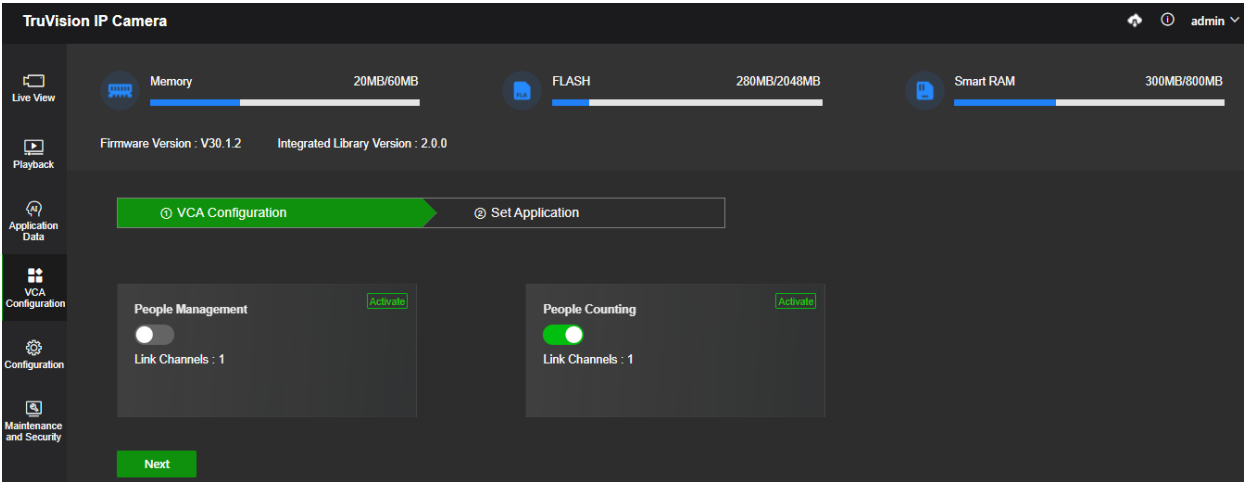
Go to **Application Data > Intersection Analysis** to view detailed data analysis.

People Counting

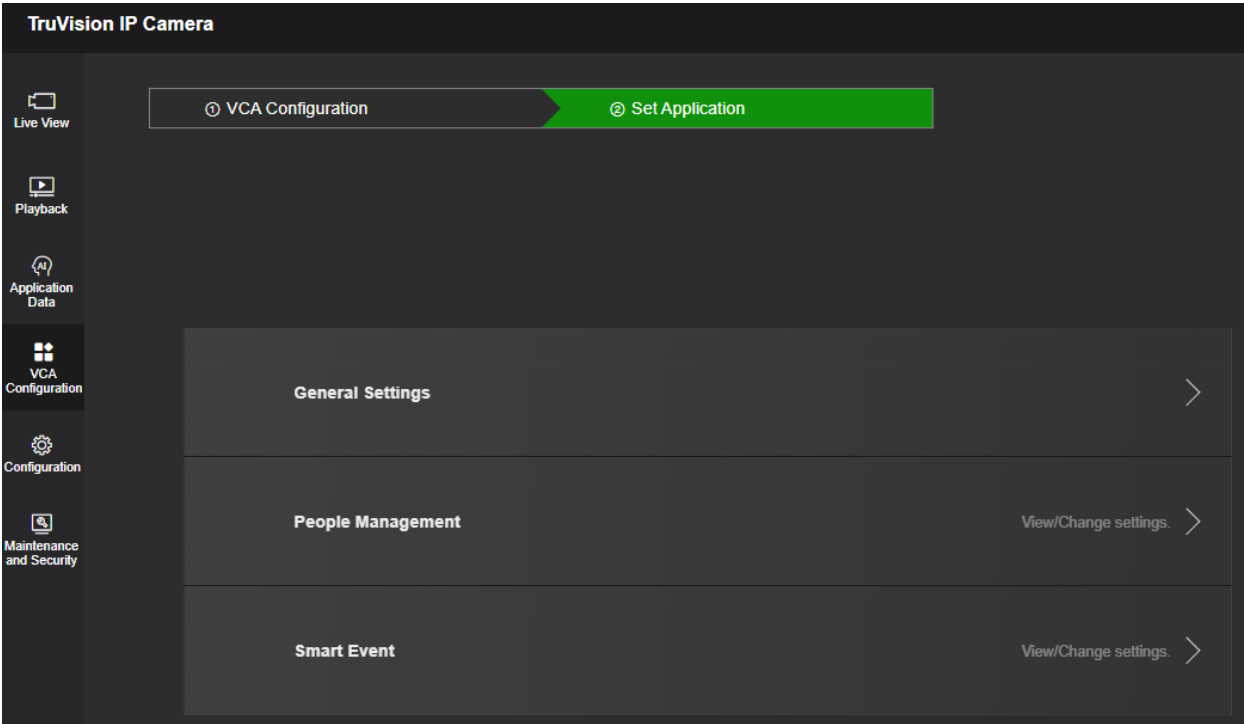
In people counting mode, the camera supports besides People Counting also the most common VCA smart event we have in other TruVision IP cameras.

People Counting

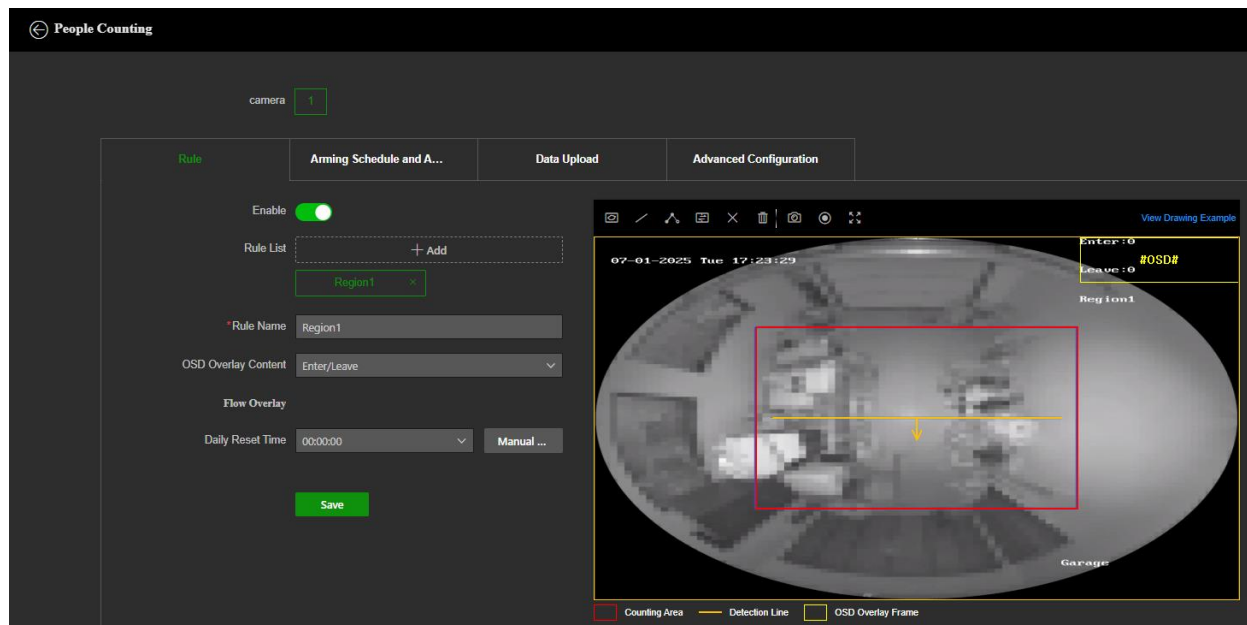
Go to VCA Configuration where you can enable the People Counting application.



Click **Next** to go to the People Counting related parameters and VCA features.



General Settings contains event reporting related parameters such as Camera Info, FTP, Email, Alarm Output, and HTTP listening. Each of these features are described in earlier sections in this manual. Click on People Counting to configure the specific People Counting related features.



To configure People Counting:

1. Go to **VCA Configuration > Set Application > People Counting > Rule**.
2. Check **Enable** to enable the function.
3. Click **Add** to add a detection area.
4. Click the draw icon at the top left above the image to draw the polygon detection area (count area). Left-click end-points in the live view window, and right-click to finish the drawing.
5. Use the second or third icon above the image to draw a detection line. The arrow shows entering direction, you can click on the left/right arrow icon to change the direction.

Notes:

- When the detection area only supports one-way direction, it is recommended to draw a straight detection line.
 - When the detection area supports multiple directions, or there are walls and obstacles in the detection area, it is recommended to click to draw a polyline.
 - Detection lines can be deleted using the Clear Selected or Clear All icons positioned above the preview image.
 - To improve the counting accuracy, please draw the detection area according to the following rules.
 - The detection area needs to cover the people entering and exiting access.
 - The detection line must be completely contained within the red detection area and perpendicular to the path of the person passing through.
6. Repeat the above steps to draw up to 3 detection areas and corresponding detection lines.
 7. Set people counting parameters.

OSD Overlay Content: Select the counting data type to be displayed in the live view image from the drop-down list and adjust the display position of people counting data in the live view image.

Daily Reset Time: The device clears by default the data at midnight each day. You can select another reset time from the drop-down list or manually reset the counter by clicking the Manual button.

8. Click Save.

9. Set Arming Schedule and Actions.

10. Click Save.

11. Optional: Set people counting data uploading parameters.

Go to the Data Upload tab to configure following settings:

Real-Time Data Uploading: Send the real-time data to the platform.

Upload Data Periodically: Set the Data Statistics Cycle, and the person counting data will be uploaded to the platform at intervals according to the Data Statistics Cycle.

12. Optional: Set people counting advanced parameters.

Go to the **Advanced Configuration** tab to configure following settings:

Display VCA Info. on Stream: Display smart information on stream, including the target and rules information.

Clear Storage Data: Clear all people counting data stored in the device. This function must be used with caution.

Smart Event

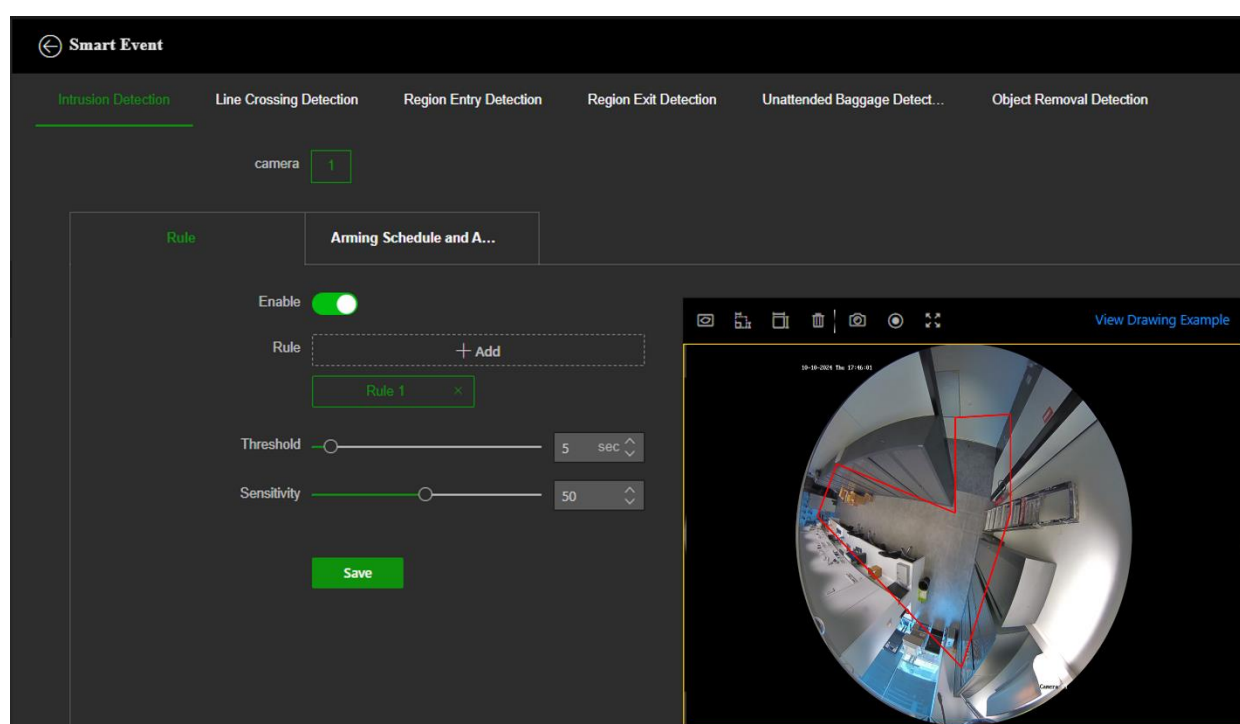
The smart events are available in both People Management and People Counting application mode. See menu structure in section VCA Configuration.

Intrusion Detection

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

To set up intrusion detection:

1. From the menu toolbar, click **VCA Configuration > Next > Smart Event > Intrusion Detection**.



2. **Enable** the function.
3. Click the **Add** button to create a detection rule.
4. Set the **Max. Size** and **Min. Size** to determine valid targets. Targets smaller or larger than the valid target size is not able to trigger detection. Min. and max. size are the second and third drawing button at the left above the image preview.
Max. Size: The maximum size of a valid target. Targets with larger sizes would not trigger detection.
Min. Size: The minimum size of a valid target. Targets with smaller sizes would not trigger detection.
5. Click the first button at the left above the image preview to draw a polygon area on the live video viewer where you want the camera to check for intrusion events.

When you draw the polygon, all lines should connect end-to-end to each other. Click the Clear All button (trash icon) to clear the area you have drawn.

6. Additional options to set up are:

Threshold: This is the time threshold that the object remains in the region. If you set the value as 0 s, the alarm is triggered immediately after the object enters the region. The range is between 0 and 60 seconds.

Sensitivity: The detection sensitivity value defines how fast the camera will react to a moving object in the intrusion zone. The range is between 1 and 100. A higher value will make the camera react faster.

7. Click the **Arming Schedule and Actions** tab and set the arming schedule and actions for the events following the same procedure as described in earlier event related sections of this manual.

Note: Additional actions like *Audible Warning* or *Flashing Alarm* may be available depending on the camera model.

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

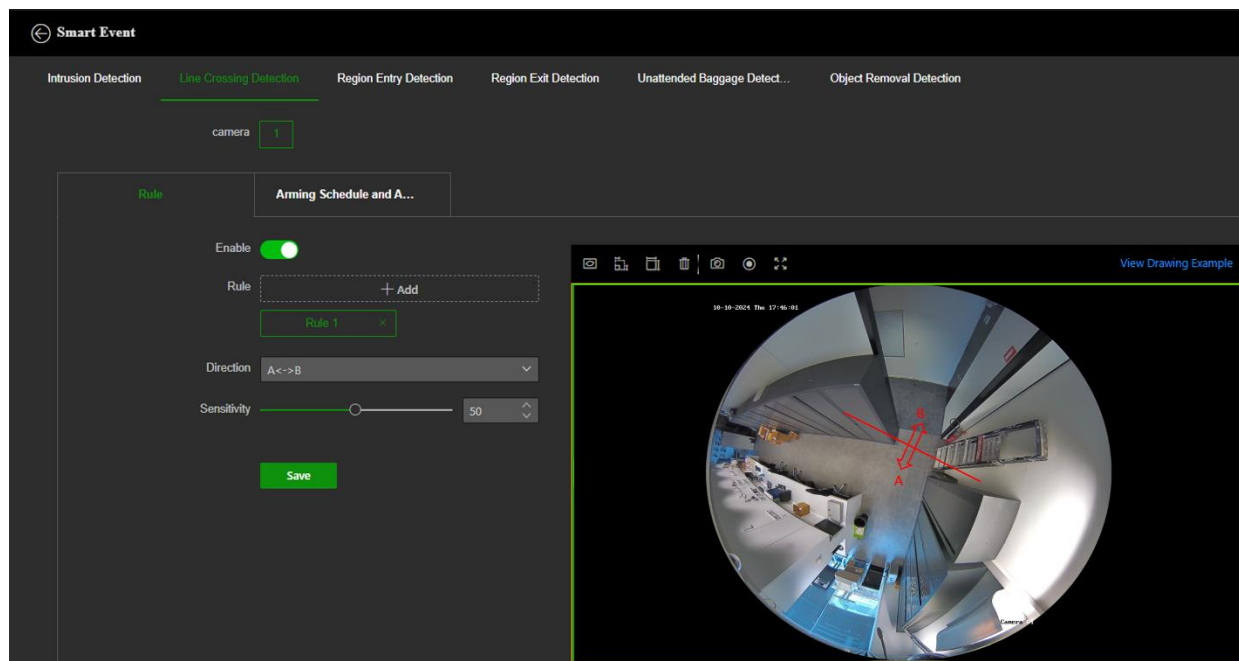
Cross Line Detection

Use this function to detect objects crossing a pre-defined line. Up to four cross lines are supported. The cross line direction can be set as unidirectional or bidirectional. Unidirectional is crossing the line from left to right or from right to left. Bidirectional is crossing the line from both directions.

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

To set up cross line detection:

1. From the menu toolbar, click **VCA Configuration > Next > Smart Event > Line Crossing Detection**.



2. **Enable** line crossing.
3. Click the **Add** button to create a cross line rule.
3. Use the first icon at the left above the image preview to draw the cross line.
3. Position the line on its proper place in the image by grabbing one of the end-points of the line and moving them to the desired position.
4. Set the **Max. Size** and **Min. Size** to determine valid targets. Targets smaller or larger than the valid target size are not able to trigger detection. Min. and max. size are the second and third drawing button at the left above the image preview.
Max. Size: The maximum size of a valid target. Targets with larger sizes would not trigger detection.
Min. Size: The minimum size of a valid target. Targets with smaller sizes would not trigger detection.
5. . Select one of the **Direction** options from the drop-down list:
A<->B: Arrows are displayed on both A and B ends. When an object crosses the line in any direction, it can be detected and trigger an alarm.
A->B: Only an object crossing the line in the A to the B direction can be detected and trigger an alarm.
B->A: Only an object crossing the line in the B to the A direction can be detected and trigger an alarm.
6. Set the **Sensitivity** level between 1 and 100. The higher the value, the more easily the line crossing action can be detected.
7. If desired, add another rule and line by repeating the above steps. Up to four cross lines can be configured.
8. Click the **Arming Schedule and Actions** tab and set the arming schedule and actions for the events following the same procedure as described in earlier event related sections of this manual.

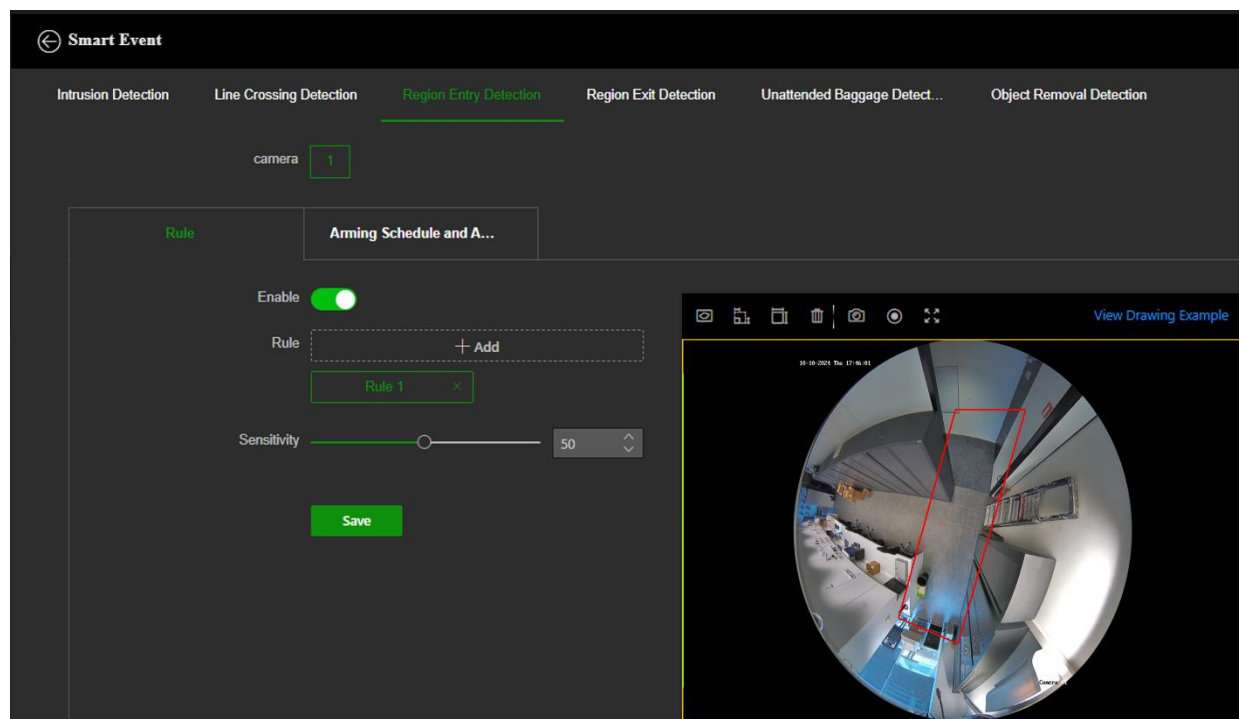
9. Click **Save** to save changes.

Region Entry Detection

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

To define region entry detection:

1. From the menu toolbar, click **VCA Configuration > Next > Smart Event > Region Entry Detection**.



2. **Enable** the function.
3. Click the **Add** button to create a detection rule.
4. Use the first icon at the left above the image preview to draw the detection region by using the mouse and left button to draw the lines of the region. Right-click the mouse after drawing the last line of the area to complete drawing of the region.
5. Set the **Max. Size** and **Min. Size** to determine valid targets by using the second and third icon above the image preview. Targets smaller or larger than the valid target size is not able to trigger detection when entering the area.
Max. Size: The maximum size of a valid target. Targets with larger sizes would not trigger detection.
Min. Size: The minimum size of a valid target. Targets with smaller sizes would not trigger detection.
6. Set the detection sensitivity level. Drag the slider to the desired value.
Sensitivity: Range [1-100]. This is the percentage of the target versus the entire detection area.

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

S1 stands for how much the target occupies the detection area. ST stands for the whole detection area.

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

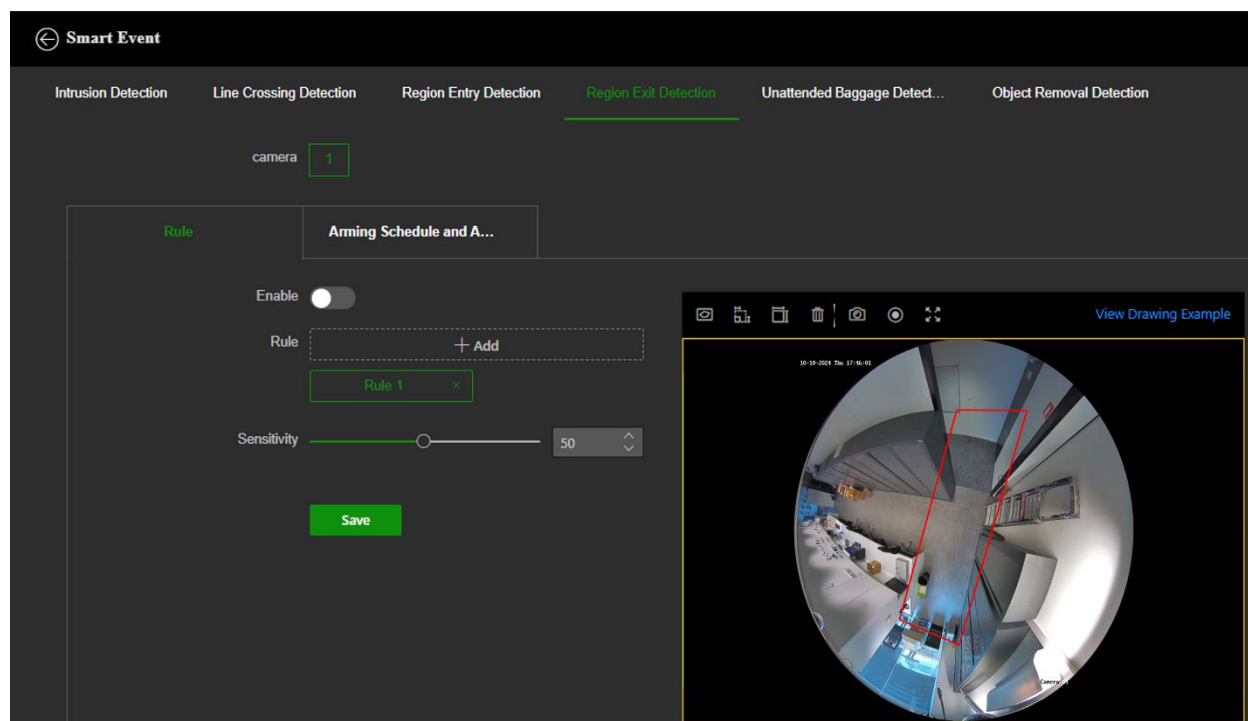
7. Repeat above steps to configure additional regions. Up to four regions can be set. You can click on the “x” in the Rule buttons to delete created regions.
8. Click the Arming Schedule and Actions tab and set the arming schedule and actions for the events following the same procedure as described in earlier event related sections of this manual.
9. Click **Save** to save the settings.

Region Exit Detection

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

To define region exit detection:

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



2. **Enable** the function.
3. Click the **Add** button to create a detection rule.
4. Use the first icon at the left above the image preview to draw the detection region by using the mouse and left button to draw the lines of the region. Right-click the mouse after drawing the last line of the area to complete drawing of the region.

5. Set the **Max. Size** and **Min. Size** to determine valid targets by using the second and third icon above the image preview. Targets smaller or larger than the valid target size is not able to trigger detection when leaving the area.

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

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

6. Set the detection sensitivity level. Drag the slider to the desired value.

Sensitivity: Range [1-100]. This is the percentage of the target versus the entire detection area.

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

S1 stands for how much the target occupies the detection area. ST stands for the whole detection area.

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

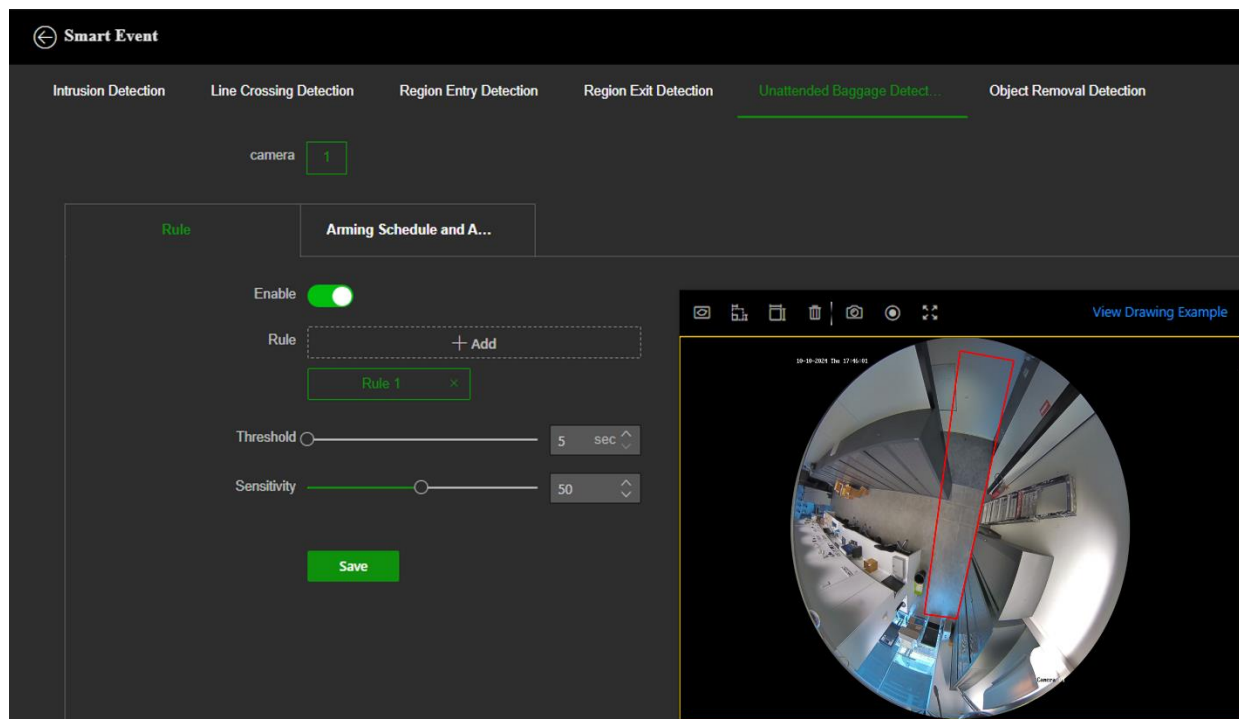
7. Repeat above steps to configure additional regions. Up to four regions can be set. You can click on the “x” in the Rule buttons to delete created regions.
8. Click the Arming Schedule and Actions tab and set the arming schedule and actions for the events following the same procedure as described in earlier event related sections of this manual.
9. Click **Save** to save the settings.

Unattended baggage detection

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

To set up unattended baggage detection:

1. From the menu toolbar, click **VCA Configuration > Next > Smart event > Unattended baggage detection.**



2. **Enable** the function.
3. Click the **Add** button to create a detection rule.
4. Use the first icon at the left above the image preview to draw the detection area by using the mouse and left button to draw the lines of the region. Right-click the mouse after drawing the last line of the area to complete drawing of the region.
5. Define the maximum and minimum sizes of valid objects by using the second and third icon above the image preview. Objects that are smaller or larger than the valid target size cannot trigger detection.
- Max. Size:** The maximum size of a valid object. Objects with larger sizes would not trigger detection.
- Min. Size:** The minimum size of a valid object. Objects with smaller sizes would not trigger detection.
6. Set the time threshold and detection sensitivity for unattended baggage detection. Threshold: Range [1-100]. The threshold for the time of the objects left over in the region. If you set the value as 10, alarm is triggered after the object has appeared in the region for 10s.
7. Drag the slider to set the sensitivity value.

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

$\text{Sensitivity} = 100 - \frac{S1}{ST} \times 100$ S1 stands for the target body part that enters the pre-defined region ST stands for the complete target body. Example: if you set the value as 60, a target is possible to be counted as an unattended baggage only when 40 percent body part of the target enters the region.

Threshold: Stands for the time of an object left in the region. An alarm is triggered after the object is left and stays in the region for the set time.

8. Repeat the above steps to configure other regions. Up to four regions can be set. You can click the Clear button to clear all pre-defined regions.
9. Click the **Arming Schedule and Actions** tab and set the arming schedule and actions for the events following the same procedure as described in earlier event related sections of this manual.
10. Click **Save** to save the settings.

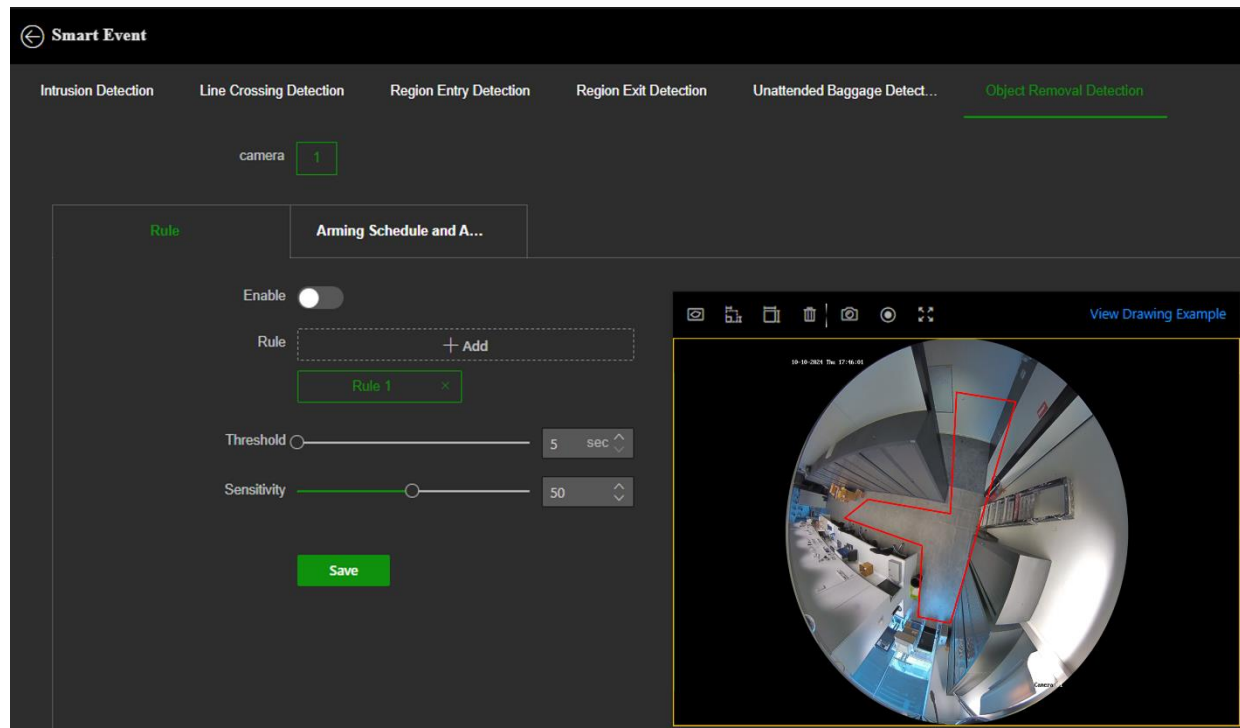
Important: Please note that this feature works best for objects left behind on less complex backgrounds. Complex backgrounds make it more difficult for the camera to detect unattended objects. A significant contrast between background and object on the other hand, makes it easier for the camera to detect.

Object Removal Detection

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

To set up object removal detection:

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



2. **Enable** the function.
3. Click the **Add** button to create a detection rule.

4. Use the first icon at the left above the image preview to draw the detection area by using the mouse and left button to draw the lines of the region. Right-click the mouse after drawing the last line of the area to complete drawing of the region.
5. Define the maximum and minimum sizes of valid objects by using the second and third icon above the image preview. Objects that are smaller or larger than the valid target size cannot trigger detection.

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

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

6. Set the time threshold and detection sensitivity for left behind object detection. Threshold: Range [1-100]. The threshold for the time of the objects removed from the region. If you set the value as 10, alarm is triggered after the object has no longer been seen in the region for 10s.

7. Drag the slider to set the sensitivity value.

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

Sensitivity stands for the percentage of the body part of an acceptable target that enters the predefined region. $\text{Sensitivity} = 100 - S1/ST \times 100$. S1 stands for the target body part that goes across the predefined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

Threshold: The threshold for the time of the objects removed from the region. If you set the value as 10, alarm is triggered after the object disappears from the region for 10s.

8. Repeat the above steps to configure other regions. Up to four regions can be set. You can click the Clear button to clear all pre-defined regions.
9. Click the **Arming Schedule and Actions** tab and set the arming schedule and actions for the events following the same procedure as described in earlier event related sections of this manual.
10. Click **Save** to save the settings.

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 at the top right of the camera web interface. You will be asked each time to enter your user name and password when logging in.

Note: When an incorrect username 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 leave this setting to default, but login settings can be changed under **Maintenance and Security > Security > Login Management**.

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

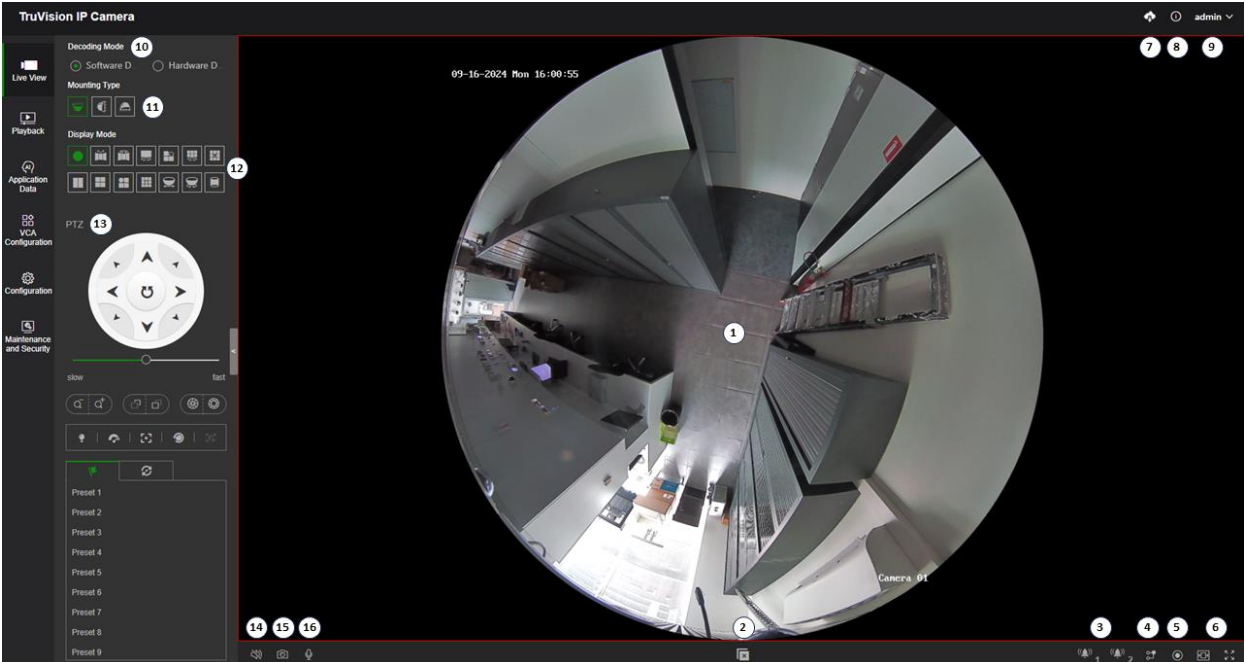
Figure 9: Login dialog box



Live view

Once logged in, click “Live View” on the left vertical menu toolbar to access live view mode.

Figure 10: Live view window



	Name	Description
1.	Live view screen	Camera live stream
2.	Start/stop video	Click to start or stop viewing live video
3.	Alarm outputs	Manual alarm output control buttons
4.	Stream type	Click to select main, sub or third stream
5.	Live recording	Click to manually start/stop recording. The recording is stored in the directory you have configured.
6.	Display options	Change aspect ratio or switch window size between 4:3, 16:9, original window size, original ratio, or self-adapt window size.
7.	Plugin	Click to download and install the web plugin recommended for plugin-free browsers. This button only appears in non-Internet Explorer browsers. PC internet connection is required.
		Click to view captured images of certain smart functions. The Smart Display menu only appears when Face Capture in VCA Resource mode is enabled See “Live view” on page 95 for further information.
		View live video. Time, date, and camera name are displayed here.
8.	Help and Open Source	Click to view Help or Open Source software information
9.	Admin	Displays current user logged on. Change password and logout option available.
10.	Decoding Mode	Choose between software or hardware decoding. Software decoding will require more PC client resources.
11.	Mounting type	Click to select one of the three mounting options. Reboot will be required.

	Name	Description
12.	Display Mode	Choose the desired display mode for live viewing. Options change depending on Decoding mode and Mounting type.
13.	PTZ	The PTZ panel lets you control the movement or view of the camera (see below) as well as call up pre-existing presets. The user will need permission to use the PTZ control panel.
14.	Silent	Click to mute audio.
15.	Take snapshot	Click to take a snapshot of the live video
16.	Start two-way audio	Click to activate audio. This can only work when enabled in video encoding configuration.

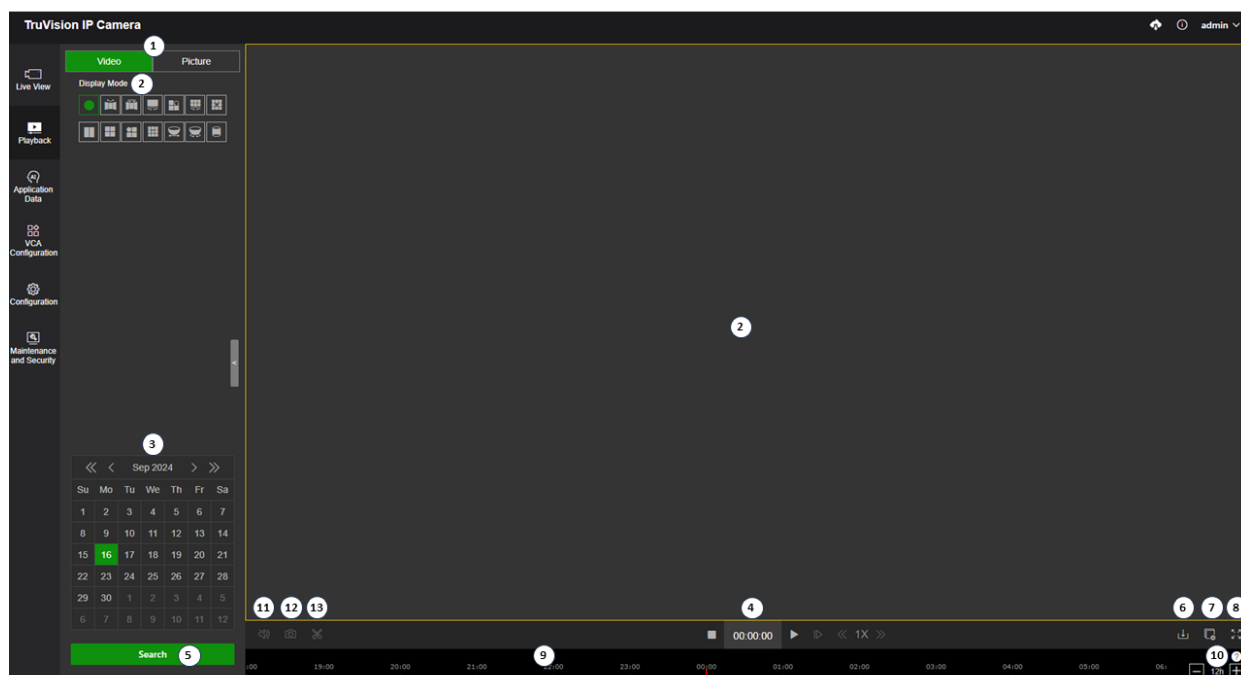
Playback

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.

Figure 11: Playback window



Name	Description
1. Video/Snapshot	Select whether to search for recorded video or snapshots
2. Display Mode	Select the display mode for playback
3. Calendar	Select the date to search for recorded data


Name	Description
4. Search time and playback control	After selecting a date in the calendar, you can refine your search by entering a specific time. With the other buttons next to the time, you can control the playback.
5. Search	Click this button to search
6. Archive	Click this button to open the “Download by Date” and “Download by File” archive menu.
7. Stop all Playback	Click to stop video playback.
8. Full Screen	Click this button to view playback video in full screen mode. Hit the Escape button on your keyboard to return to normal playback view.
9. Timeline bar	The timeline bar displays the 24-hour period of the day being played back. It moves from 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 playback.
10. Timeline information and zoom	Use the +/- buttons to zoom in/out on the timeline. Hovering the “?” explains the recording type associated with the different colors on the timeline.
11. Audio	Enable/disable audio during playback
12. Take snapshot	Click to take a snapshot of the playback video
13. Create video clip	During video playback, you can select and export a certain video clip. The first click defines the start of the export clip and the second click the end. After that, you will be asked to export the video clip to your local PC.

To play back recorded video


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

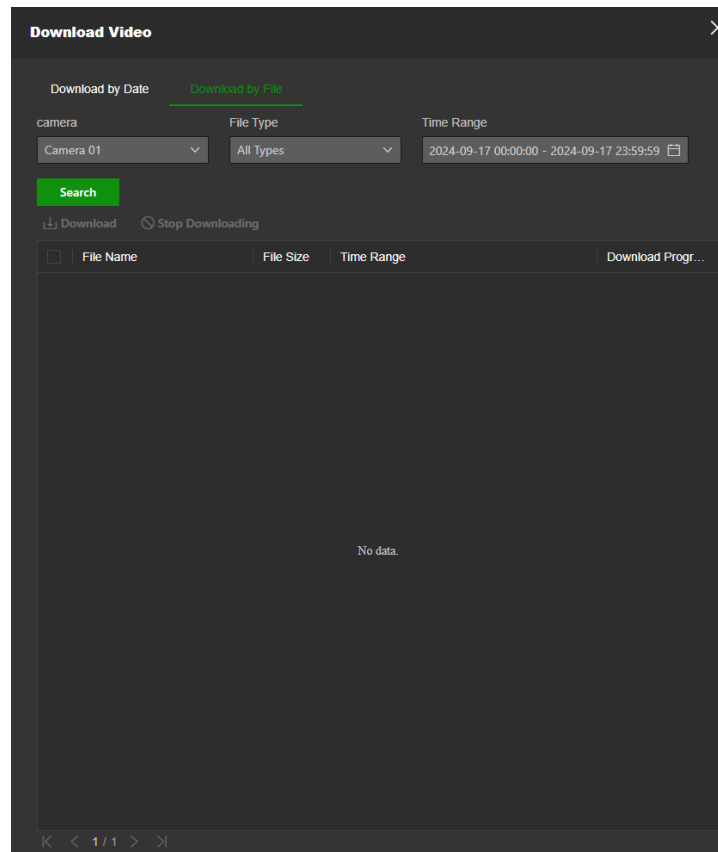
Note: You must have playback permission to play back recorded images. See “Assign permissions to the user” to permit playback of recorded video files.

To archive a recorded video clip during playback:

1. While playing back a recorded file, click  to define the start point of the video clip. Click it again to define the end of the clip. A video clip is created.
2. Repeat step 2 to create additional clips. The video clips are saved on your computer.

To archive recorded video files:

1. Click  to open the Download Video search window.

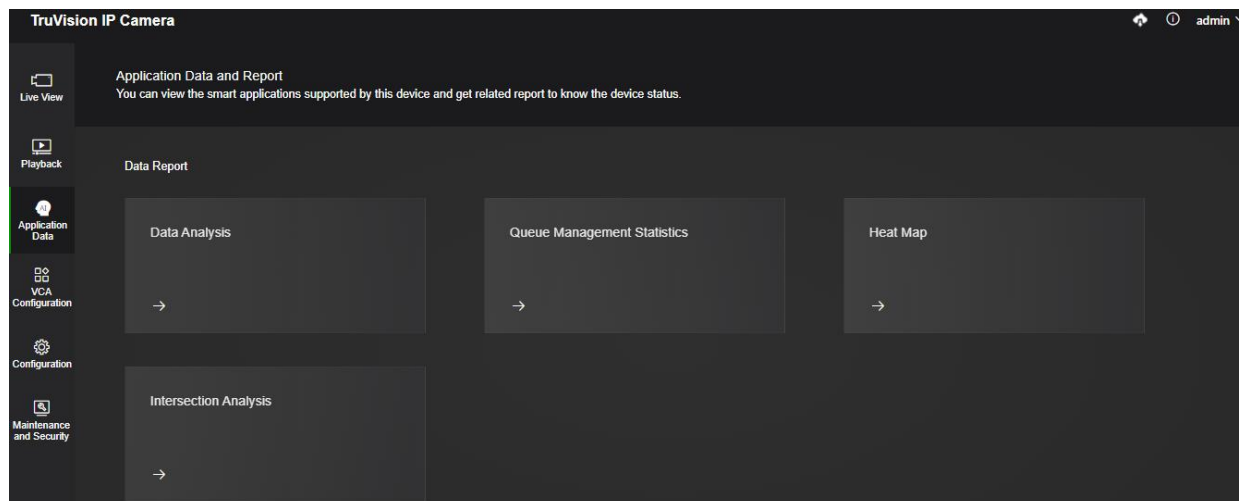


2. Select Download by Date or Download by File.
3. After you selected desired file type and/or time range, click **Search** to search for the recorded video files.
4. Select the desired video files and click **Download** to download them. Downloading files from a NAS or SD card can take some time. A progress bar will be displayed to indicate the download progress.

Application Data

In this menu you can analyze certain system data and data from certain VCA applications supported by the camera.

This menu can be accessed by clicking **Application Data** in the left main menu.



Data Analysis

The data analysis function is used to search and export the data of the restart, arming and capture alarm statistics.

1. Go to **Application Data** → **Data Analysis**.
2. Define the search condition by using following criteria:
 - Statistics Type: Restarting Records or Arming
 - Based on one of the above two criteria a number of refined options will become available under Restarting Type or Arming Type.
3. Set start and end date and then click **Search**.
Data information matching the selected conditions will be displayed.
4. Optional: Click Export to save the data information to your local device.

Queue Management Statistics

Queue management displays data related to the queue management configuration of the camera.

Before using this function:

- Select Queuing-Up Time Analysis and Multi-Area Comparison to compare queuing-up people number of different areas.
- Select Queuing-Up Time Analysis and Multi-Level Comparison to compare queuing-up people number of different waiting time levels.
- Select Queue Status Analysis and Multi-Area Comparison to compare the time and duration that a queue stays at a certain length in different areas.
- Select Queue Status Analysis and Multi-Level Comparison to compare the time and duration of the queue at different queue length levels.

1. Go to **Application Data** → **Queue Management Statistics**.
2. Select Report Type: Daily, weekly, Monthly, or Custom.

3. Select Statistics Content:

Queuing-Up Time Analysis: Queuing-up time analysis calculates people number of different waiting time levels.

Queue Status Analysis: Queue status analysis calculates the time and duration that a queue stays a certain length.

4. Select Statistics Dimension:

Multi-Area Comparison: Multiple areas and one level can be selected for analysis, and an analysis chart can be drawn.

Multi-Level Comparison: Multiple levels and areas can be selected for analysis, and one analysis chart is drawn for each area.

5. Check one or more areas.

6. Set Waiting Time Level.

7. Click the green button at the bottom of the page to generate the report.

8. Optional: Click Export to export the data.

Heat Map

Heat map can observe and calculate the people presence in a predefined area and display these statistics in graphical form. It can be applied to scenes with large people flow such as malls, supermarkets, and museums.

1. Go to **Application Data** → **Heat Map**.

2. Select Report Type. Daily, weekly, monthly, or Annual Report.

3. Select Heat Map Type: Spatial heat map and time heat map are selectable.

Spatial Heat Map: Performs a statistical analysis on the cumulative dwelling of people in different areas in the entire image. Different heat values correspond to different colors, among which red (255, 0, 0) represents the highest heat, and blue (0, 0, 255) represents the lowest heat. The highest heat value and lowest heat value are divided into N levels, corresponding to different colors.

Time Heat Map: Performs a statistical analysis on the total dwelling time of all people in the entire image. The time heat map is presented in a line chart, and you can click Export to export the data in an excel file.

4. Select **Statistics Type**: By Dwell Time or By People Number.

5. Select **Statistics Time**.

6. Click **Search** to generate and visualize the data. After the calculating, you can visualize the data in the spatial and time heat map.

Intersection Analysis

After enabling the intersection analysis function, you can view the intersection analysis data. The picture will overlay the entrance directions and the number of people that followed each of the directions. The number of people flowing into a certain entrance and out of all other entrances will be calculated.

1. Go to **Application Data > Intersection Analysis**.
2. Select one direction as the **Entrance**
3. Set Report Type and Start Time.
4. Click **Search** to visualize the data.

The data matching your search conditions will be displayed.

People Counting

People counting data stored in the device can be displayed as a table, bar chart and line chart.

1. Go to **Application Data > People Counting**
2. Set **Report Type**: Daily, Weekly, Monthly or Annual Report,
3. **Statistics Type**: Enter/Leave, People Entered, People Exited, or Enter/Leave/Pass By.
4. Select Region(s).
5. Set **Start Time**.
6. Click **Search** to display the people counting data.
7. You can select Table, Bar Chart and Line Chart to view the data, and you can export this data through Excel.

Index

8

- 802.1x parameters
 - set up, 22

A

- Alarm inputs, 53
- Alarm outputs, 53
- Archive files, 98, 99
- Audio parameters, 31
- Auto delete mode, 45

C

- Camera image
 - set up, 34
- Camera name
 - display, 39
- Configuration file
 - import/export, 66
- Configuration menu
 - overview, 11
- Cross line detection, 87

D

- D/N schedule
 - link to lighting scenes, 37
- Date format set up, 39
- Day/night switch setup, 35
- DDNS parameters
 - set up, 20
- Default settings
 - restore, 66
- Detection
 - audio exception, 56
 - defocus, 57
 - scene change, 58
- Display information
 - set up, 39

E

- Email parameters
 - set up, 60, 62
- Events
 - search logs, 66
- Exception alarm, 54, 55

F

- Face capture, 91, 93
- Failed login lock, 71
- Filtering time, 35
- Firmware upgrade, 64
- FTP parameters
 - set up, 59

H

- Hard drive
 - capacity, 41
 - formatting, 41
- HTTP listening parameters
 - set up, 62
- HTTPS parameters
 - set up, 24

I

- Image parameters switch, 37
- Integration protocol parameters
 - set up, 30
- Intrusion detection, 86

L

- Language
 - change, 95
- Live view auto logout, 71
- Local configuration menu
 - overview, 9
- Log on/off, 95
- Logs
 - information type, 67
 - search, 66
 - security audit log, 76
 - viewing, 66

M

- Motion detection
 - advanced mode, 51
 - normal mode, 50
- Motion detection, 49
- Multicast parameters
 - set up, 25

N

- NAS management, 43
- NAT parameters
 - set up, 28
- Network service parameters
 - set up, 66
- NTP synchronization, 12

P

- Password activation, 3
- Playback
 - play back recorded files, 98
 - screen, 97, 99
 - searching recorded video, 97, 99
- Plugin-free browsers, 5
- Post-record times, 45
- PPPoE parameters

- set up, 21
- Pre-record times, 45
- Privacy masks, 40

Q

- QoS parameters
 - set up, 23

R

- Reboot camera, 64
- Recording
 - parameters, 31
 - playback, 97, 99
 - set up schedule, 44
- Region entry detection, 89
- Region exit detection, 90
- Region of interest
 - set up, 34
- Restart
 - schedule, 66

S

- SD card
 - capacity, 41
- SDHC card
 - format, 41
- Search
 - events, 66
 - logs, 66
- Security audit log, 76
- Snapshots
 - archive, 99
 - event-triggered snapshots, 47
 - scheduled snapshots, 47
- SNMP parameters
 - set up, 21

- Storage management, 41
- System time
 - set up, 12

T

- Tamper-proof alarms, 52
- TCP/IP parameters
 - set up, 18
- Time format set up, 39

U

- User management
 - add users, 16
 - delete users, 17
 - modify users, 17
 - online users, 18

V

- VCA configuration, 77
 - cross line detection, 87
 - face capture, 91, 93
 - intrusion detection, 86
 - region entry detection, 89
 - region exit detection, 90
- Video clips
 - archive, 98
- Video parameters, 31
- Video quality, 34

W

- Web browser
 - interface overview, 7
- Web browser security level, 2
- White balance, 36