

A large, bold, black square icon with a white square cutout in the center, positioned to the left of the title text.

TruVision M Series Full Color IP Camera Configuration Manual

Copyright

© 2023 Carrier. All rights reserved. Specifications are subject to change without prior notice.

This document may not be copied in whole or in part or otherwise reproduced without prior written consent from Carrier, except where specifically permitted under US and international copyright law.

Trademarks and patents

TruVision and associated names and logos are a product brand of Aritech, a part of Carrier.

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

Manufacturer

PLACED ON THE MARKET BY:
Carrier Fire & Security Americas Corporation Inc.
13995 Pasteur Blvd, Palm Beach Gardens, FL 33418, USA

AUTHORIZED EU REPRESENTATIVE:
Carrier Fire & Security B.V.
Kelvinstraat 7, 6003 DH Weert, Netherlands

Certification



Product warnings and disclaimers



THESE PRODUCTS ARE INTENDED FOR SALE TO AND INSTALLATION BY QUALIFIED PROFESSIONALS. CARRIER FIRE & SECURITY CANNOT PROVIDE ANY ASSURANCE THAT ANY PERSON OR ENTITY BUYING ITS PRODUCTS, INCLUDING ANY "AUTHORIZED DEALER" OR "AUTHORIZED RESELLER", IS PROPERLY TRAINED OR EXPERIENCED TO CORRECTLY INSTALL FIRE AND SECURITY RELATED PRODUCTS.

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

Contact information

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

Product documentation



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

Content

Important information ii

Limitation of liability ii

Product warnings ii

Warranty disclaimers iii

Intended use iv

Advisory messages iv

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 configuration 8

Local configuration 8

Configuration menu overview 9

System 10

Certificate Management 18

Network 25

Video/Audio 38

Image 41

Event 48

VCA Configuration 59

Storage 73

Camera operation 82

Login and Logout 82

Live view mode 82

Play back recorded video 85

Snapshot 87

Smart Display 88

Log 89

Index 91

Important information

Limitation of liability

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

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

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

Product warnings

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

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

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

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

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

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

DO NOT CONNECT TO A RECEPTACLE CONTROLLED BY A SWITCH.

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

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

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

Warranty disclaimers

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

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

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

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

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

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

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

Intended use

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

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

Advisory messages

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

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

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

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

Introduction

Product overview

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

TVFC-M01-0401-BUL-G: TruVision 4MP, Full color IP Fixed Lens Mini Bullet Camera

TVFC-M01-0401-DOM-G: TruVision 4MP, Full color IP Fixed Lens Dome Camera

TVFC-M01-0401-TUR-G: TruVision 4MP, Full color IP Fixed Lens Turret Camera

TVFC-M01-0401-WED-G: TruVision 4MP, Full color IP Fixed Lens Wedge Camera

TVFC-M01-0402-BUL-G: TruVision 4MP, Full color IP Fixed Lens Bullet Camera

TVFC-M01-0402-DOM-G: TruVision 4MP, Full color IP Fixed Lens Dome Camera

TVFC-M01-0402-TUR-G: TruVision 4MP, Full color IP Fixed Lens Turret Camera

TVFC-M01-0403-BUL-G: TruVision 4MP, Full color IP Varifocal Bullet Camera

TVFC-M01-0403-DOM-G: TruVision 4MP, Full color IP Varifocal Dome Camera

TVFC-M01-0802-BUL-G: TruVision 4K/8MP, Full color IP Fixed Lens Bullet Camera,

TVFC-M01-0802-TUR-G: TruVision 4K/8MP, Full color IP Fixed Lens Turret Camera

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

- TruVision M Series Full Color IP Camera Installation Guides
- TruVision M Series Full Color IP 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:	firesecurityproducts.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

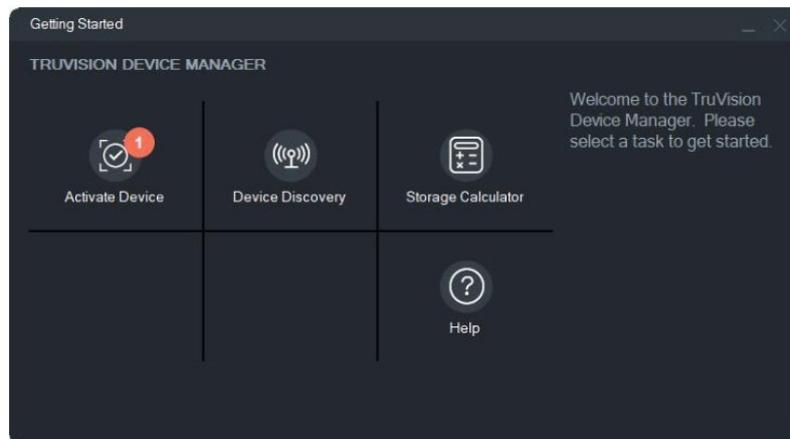
- At least 1 uppercase letter
- At least 1 of the following special characters `_ : - , . * & @ / $? Space`.

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 9.1SP2* 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.

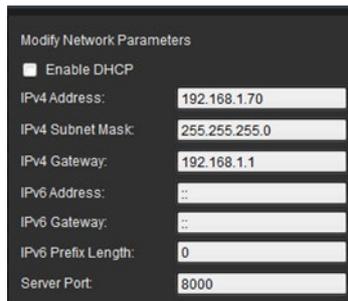
Note: A valid password range must meet the following conditions:

- 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.



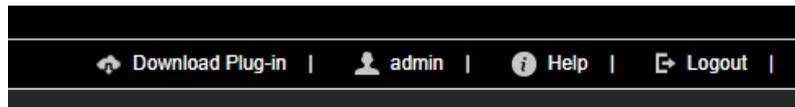
The screenshot shows a dark-themed configuration window titled "Modify Network Parameters". It contains several settings:

- Enable DHCP
- IPv4 Address: 192.168.1.70
- IPv4 Subnet Mask: 255.255.255.0
- IPv4 Gateway: 192.168.1.1
- IPv6 Address: ::
- IPv6 Gateway: ::
- IPv6 Prefix Length: 0
- Server Port: 8000

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

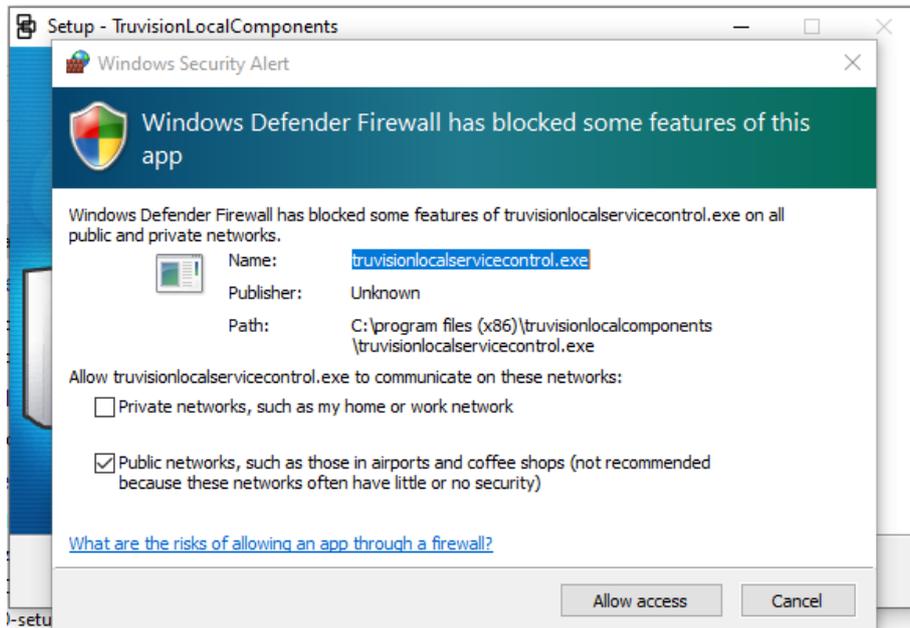
Plugin-free browsers such as Google Chrome, Mozilla Firefox, Microsoft Edge, and Apple Safari have limitations compared to Internet Explorer which uses ActiveX plugins. To solve this, an additional plugin can be downloaded through the camera live view web page. Please note that an internet connection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

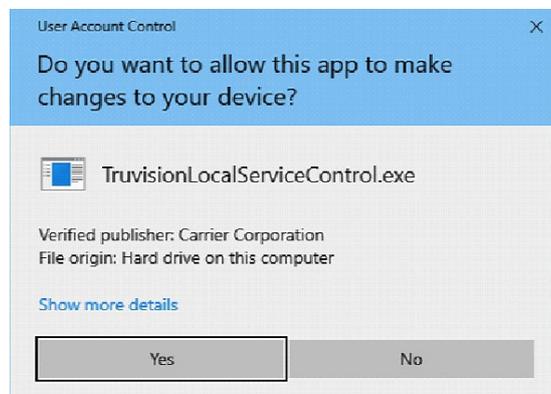


Close the browser and install the downloaded plugin *TruVisionLocalComponents.exe* on your PC. Once the plugin is installed, you can reopen the browser to view and configure the camera.

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 8 for an example.

Camera configuration

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

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

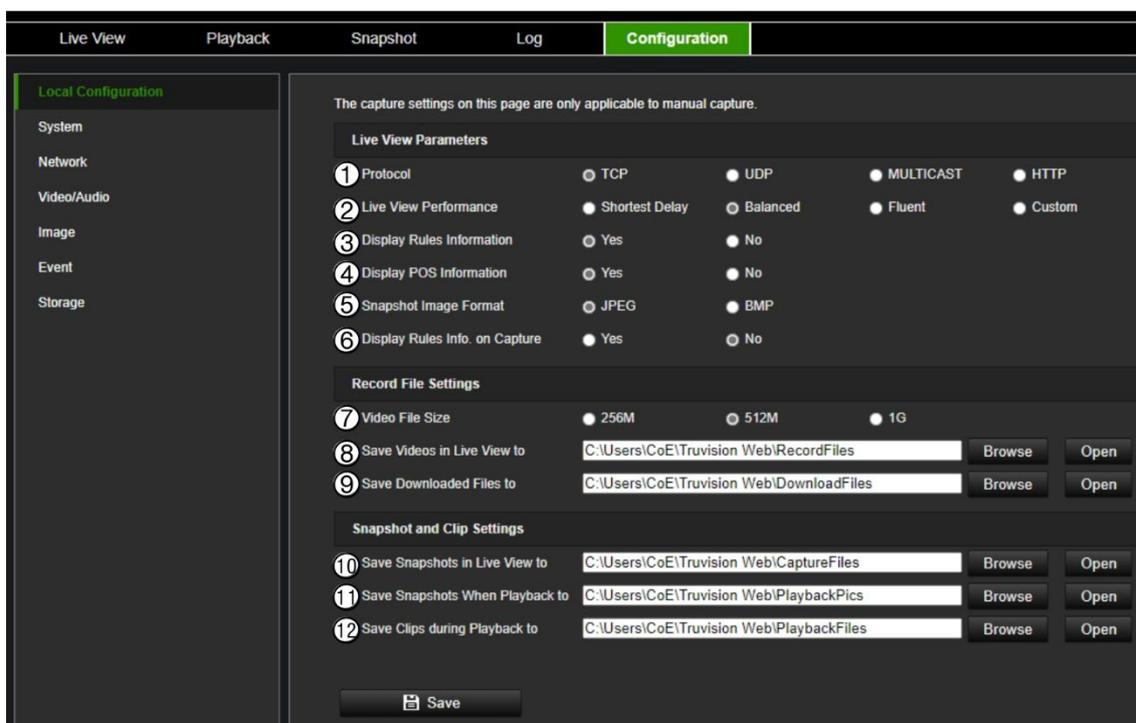
There are two main folders in the configuration panel:

- Local configuration
- Configuration

Local configuration

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

Figure 1: Example of the Local configuration window



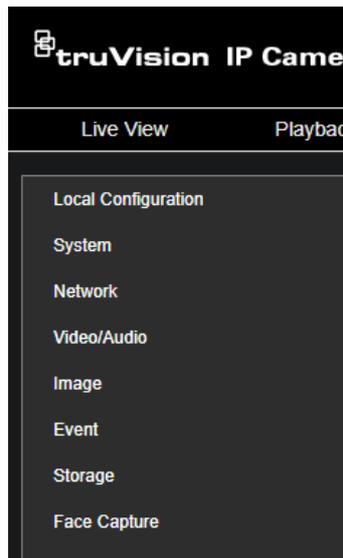
Parameters	Description
Live View Parameters	
1. Protocol	Specify the network protocol used. Options include TCP, UDP, MULTICAST, and HTTP.

Parameters	Description
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. Meta Data Overlay	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 a face is detected, the face will be marked with a green rectangle in live view.
4. Display POS Information	Enable external data to be displayed as text overlay on camera image (currently not used)
5. Snapshot Image Format	Choose snapshot image format: JPEG or BMP.
6. Display Rules Info. on Capture	Enable to display the rules information on a captured image.
Record File Settings	
7. Video File 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. Save Snapshots in Live View To	Specify the directory for saving snapshots in live view mode.
11. Save Snapshots when Playback To	Specify the directory for saving snapshots in playback mode.
12. Save Clips during Playback to	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 25 for further information on the setup.
3. Video/Audio	Defines recording parameters. See “Video/Audio” on page 38 for further information.
4. Image	Defines the image parameters, OSD settings, overlay text, and privacy mask. See “Image” on page 41 for further information on the setup.
5. 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.
6. Storage	Defines recording schedule, storage management, NAS configuration, and snapshot. See “Storage” on page 73 for further information on the setup.
7. Face Capture	Defines face capture parameters. This menu option will only appear when the VCA resource mode “Face Capture” is enabled. See “VCA Resource” on page 13 on how to enable Face Capture.

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 VCA-related options.

Basic Information

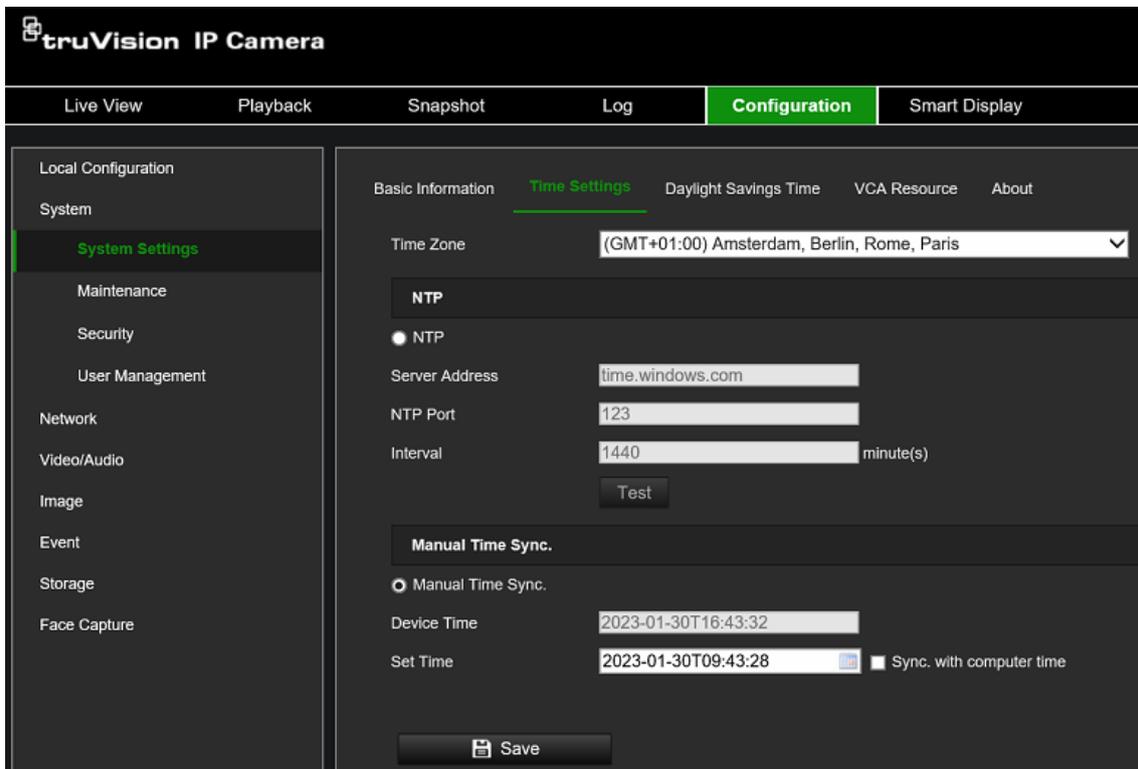
This menu displays the hardware and firmware-related information of the device.

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**.



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:

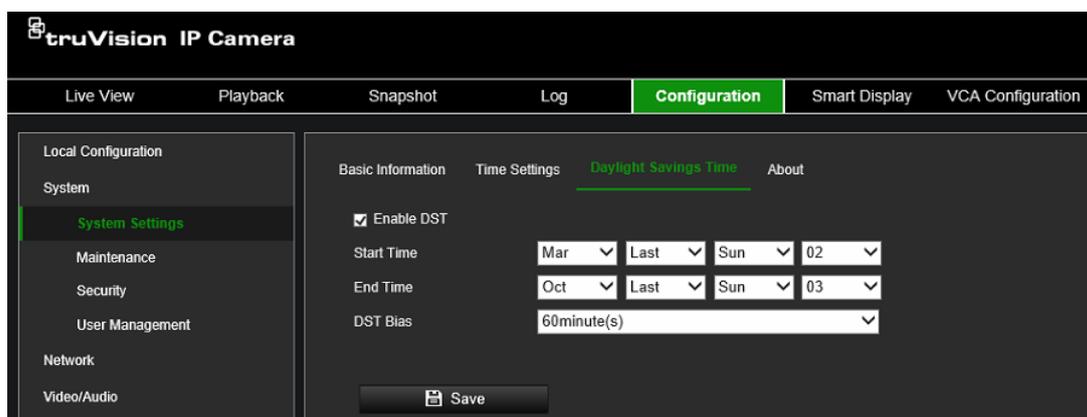
Synchronize with an NTP server: Select the **NTP** enable box and enter the server NTP address. The time interval can be set from 1 to 10080 minutes.

— 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 select the **Sync with computer time** check box to instantly synchronize the time of the camera with the time of your computer.

To define Daylight Saving Time (DST):

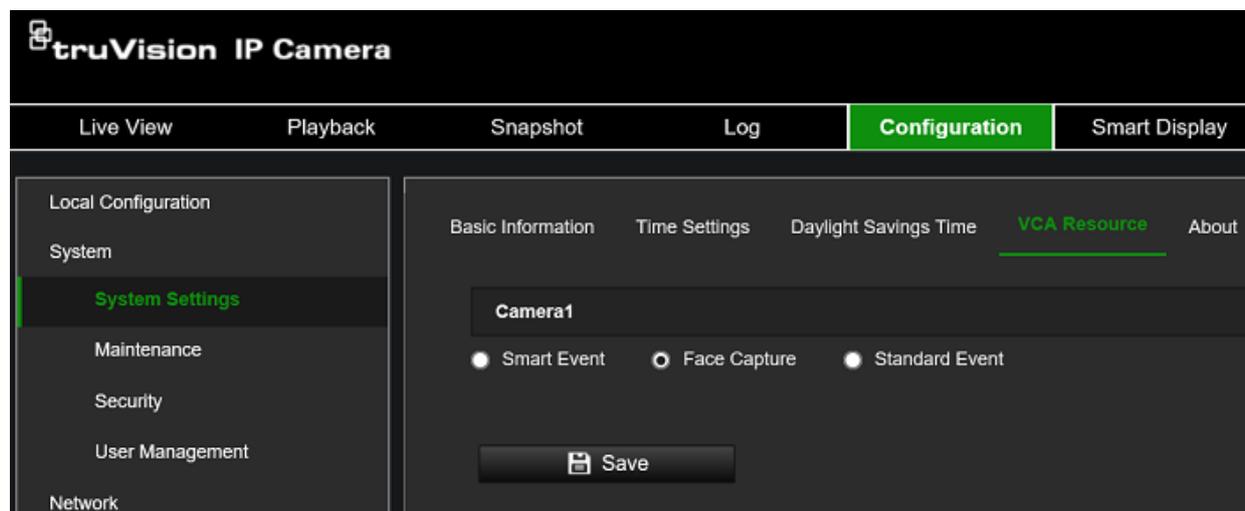


1. Select **Enable DST** to enable the DST (Daylight Savings Time) function and set the dates of the DST period.

2. Click **Save** to save changes.

VCA Resource

There are three different VCA resource options available, each enabling and disabling certain camera features. Please refer to the table below to see which camera features are available in each of the different VCA Resource modes.



Feature	Smart Event (Default mode)	Face Capture	Standard Event
Motion (Normal + Expert)	Yes	Yes	Yes
Cross Line Detection	Yes	No	No
Intrusion Detection	Yes	No	No
Region Entry Detection	Yes	No	No
Region Exit Detection	Yes	No	No
Video Tampering	Yes	Yes	Yes
Scene Change Detection	Yes	Yes	Yes
Face Capture	No	Yes	No
Third Stream	No	No	Yes

Note:

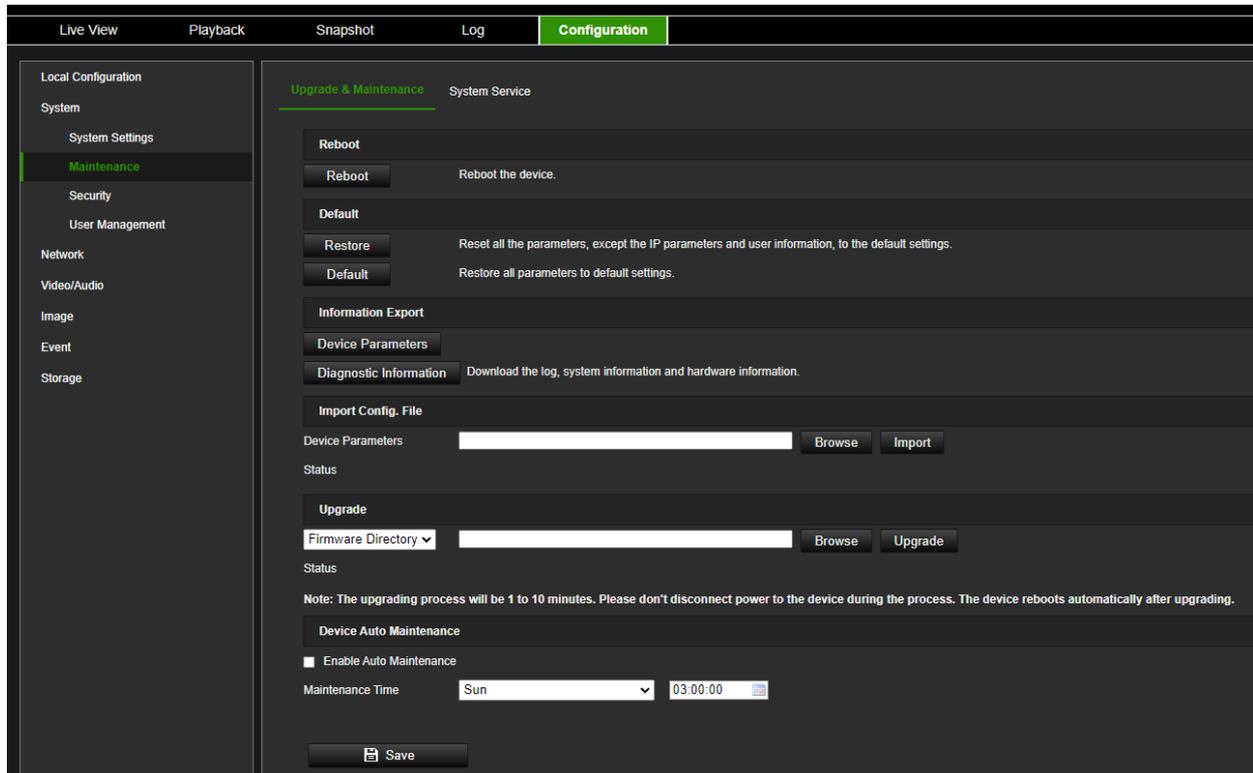
- Switching between VCA resource options will require the camera to reboot for changes to take effect.
- Some older TruVision recorders do not support the configuration of person/vehicle event options. For these recorders, you first configure all your event options from the recorder UI and then activate the desired person/vehicle options via the camera web interface.

About

The open-source software licenses used by the camera are listed here.

Maintenance

Maintenance tasks such as importing/exporting configurations and firmware upgrades can be managed in this menu, *Upgrade and Maintenance*.



Reboot camera

Click **Reboot** to restart the camera.

Restore default settings

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/export configuration file:

1. From the menu toolbar, go to **Configuration > System > Maintenance > Information Export**.
2. Click **Browse** to select the local configuration file and then click **Import** to start importing a configuration file. Depending on the selected file, a password might be needed to import the configuration file.

3. To export camera settings, click **Device Parameters** and set the saving path to save the configuration file. The camera will ask to encrypt the exported file with a password. Choose any password you want and make sure to remember it when importing the file.
4. To export three categories of diagnostic information, click the **Export Diagnostic Info** button.

Upgrade firmware

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

You need to upgrade firmware when it has become outdated. When you upgrade the firmware, all existing settings are unchanged. Only the new features are added with their default settings. In some cases, a factory default might be required after 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.
Note: Do not save the file on your desktop.
3. From the menu toolbar, click **Configuration > Camera Configuration > System > Maintenance**. 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 asking you to reboot the camera.
5. When the upgrade is finished, the device will reboot automatically. The browser will also be refreshed.

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.

Security

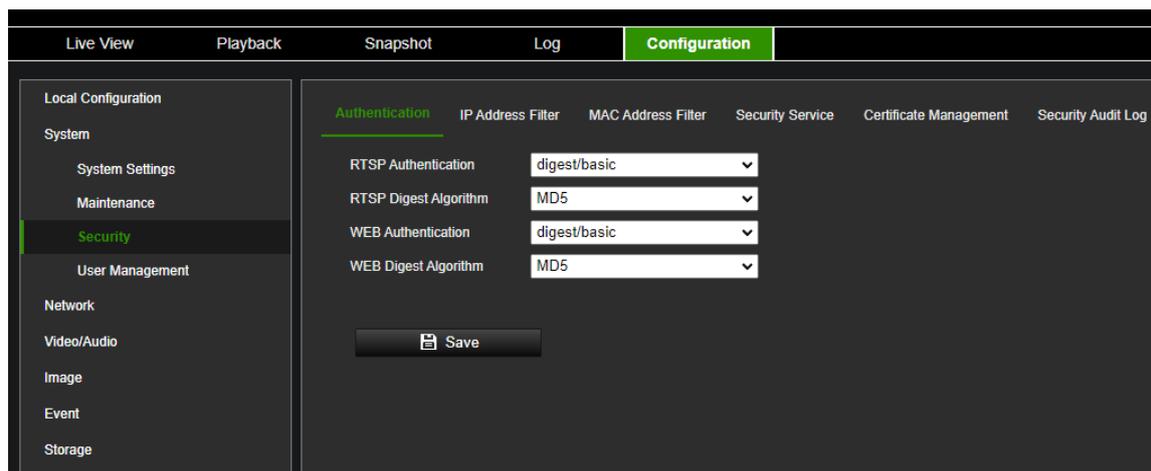
Security-related parameters, such as user accounts and the IP address filter, can be managed via the camera menu **System > Security**.

Authentication

You can secure the stream data of the live view.

To define the RTSP and web authentication:

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



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

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

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

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

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

IP address filter

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

To define the IP address filter:

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

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 **Configuration > System > Security > Mac Address Filter**.
2. Select the **Enable MAC Address Filter** check box.
3. Select the type of MAC Address Filter in the drop-down list: Forbidden or Allowed.
3. Click **Add** to add a Mac address and enter the address. The MAC address format needs to be xx-xx-xx-xx-xx-xx
4. Click **Modify** or **Delete** to modify or delete the selected MAC address.
6. Click **Save** to save the changes.

Security service

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

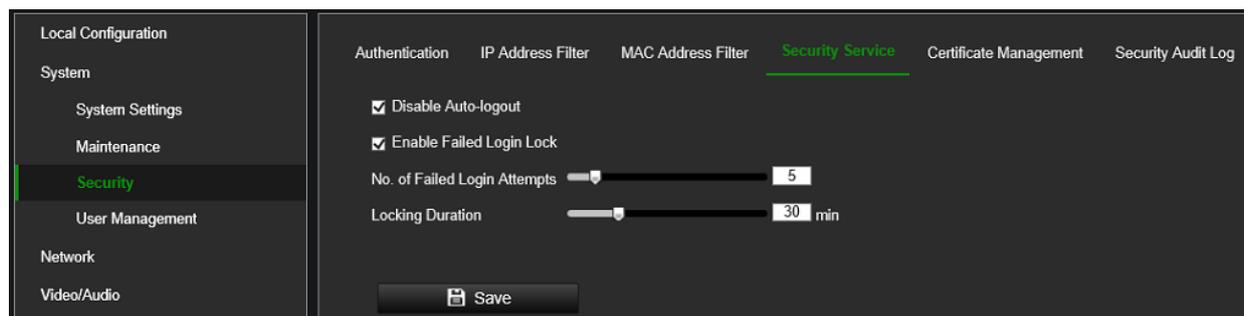
Disable Auto-logout: By default, when logged into the live view webpage or smart display webpage and there is no activity for at least five minutes, the system will automatically log out. Select this function to disable automatic log-out.

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 30 minutes.

To enable the failed login lock:

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



2. Select the **Disable Auto-logout** check box to disable auto-logout when staying at the live view or smart display webpage.
3. Select the **Enable Failed Login Lock** check box 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:

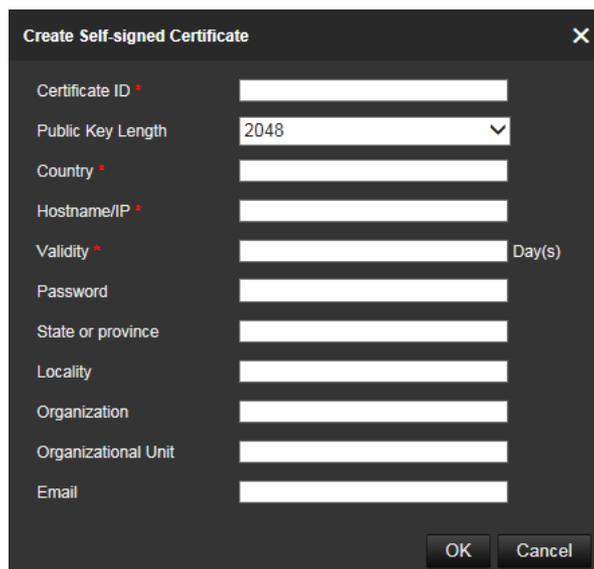
1. Click **Configuration > System > Security > Certificate Management**.

The screenshot shows the 'Configuration' tab of a device's web interface. The left sidebar lists various configuration categories, with 'Security' highlighted. The main content area is titled 'Certificate Management' and contains two sections: 'Server/Client Certificate' and 'CA Certificate'. The 'Server/Client Certificate' section has a table with one entry: 'default' with a 'Valid From' date of 2022-11-23 13:16 and a 'Valid To' date of 2025-11-22 13:16. The 'CA Certificate' section is currently empty. Below these sections is the 'Certificate Expiration Alarm' configuration area, which includes a checkbox to 'Enable Certificate Expiration Alarm', three sliders for 'Remind Me Before Expiration' (set to 7), 'Alarm Frequency(day)' (set to 1), and 'Detection Time (hour)' (set to 10). There are also checkboxes for 'Normal Linkage', 'Send Email', and 'Notify Alarm Recipient' (which is checked).

To create a self-signed certificate:

1. Click **Create Self-signed Certificate**.

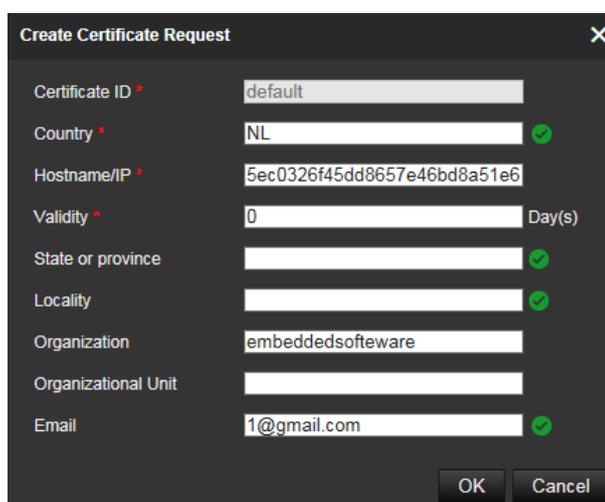
2. Enter certificate ID, country, hostname/IP, validity, and other information. The certificate ID should be numbers or letters less than 64 characters.



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

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.

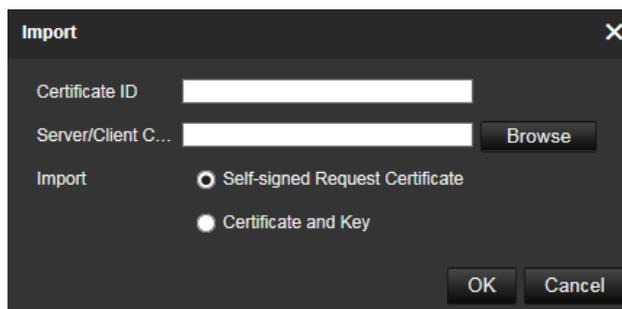


4. Click **OK** to save the changes.

To import a certificate:

1. Click **Import**

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



Note:

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

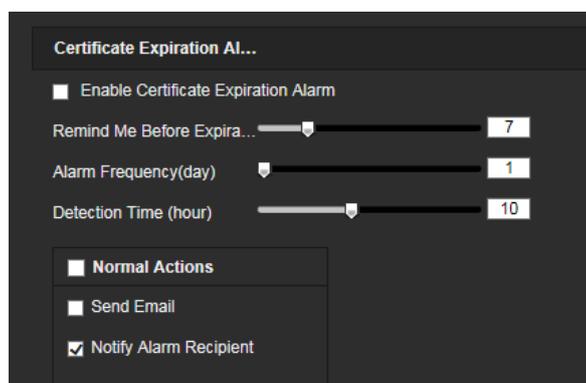
To manage CA certificate:

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 box or alarm recipient.



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

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 reminded days.
- If you set the reminding 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.

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. Configure the server settings under **Advanced Settings**.

User Management

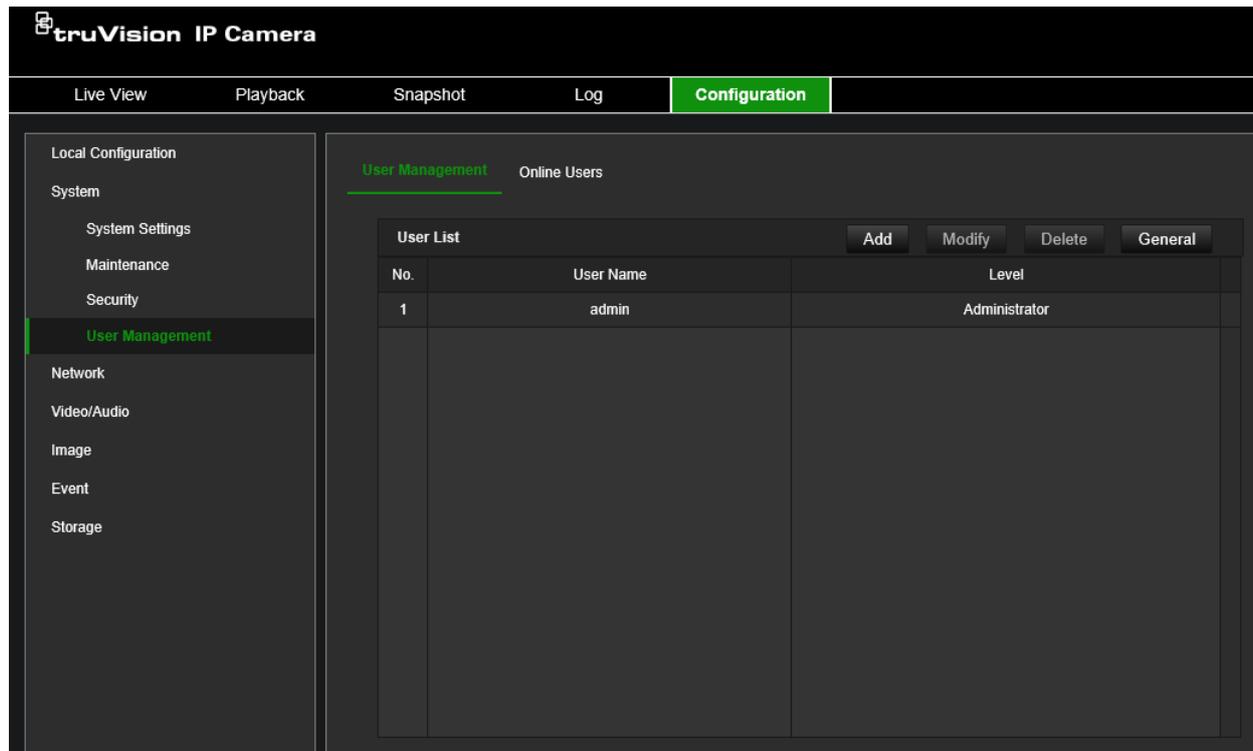
This section describes how to manage users. You can:

- 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 window



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 will 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 [X]

User Name:

Level: ▼

Admin Password:

Password:

Confirm:

Password length must be between 8 and 16 characters and contain upper case letters, lower case letters, numbers, and special characters (_ - , . * & @ / \$? Space).

Select All
 Remote: Parameters Settings
 Remote: Log Search / Interrogate Working Status
 Remote: Upgrade / Format
 Remote: Bi-directional Audio
 Remote: Shutdown / Reboot
 Remote: Notify Surveillance Center / ...
 Remote: Video Output Control
 Remote: Serial Port Control
 Remote: Live View
 Remote: Manual Record
 Remote: PTZ Control
 Remote: Playback

OK Cancel

3. Enter a username.
4. Select the type of user from the **Level** drop-down list. The options are User and Operator.
4. Enter the Admin Password
5. 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.

6. 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
Remote: Shutdown / Reboot	
Remote: Notify Surveillance Center/Trigger Alarm Output	
Remote: Video Output Control	
Remote: Serial Port Control	

7. 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**.

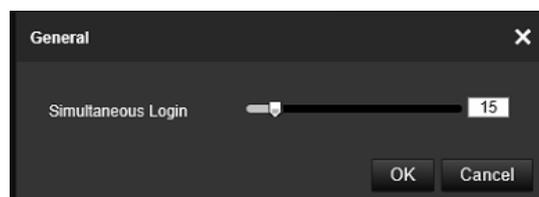
To modify user information:

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.

To define the maximum number of simultaneous logins:

1. From the menu toolbar, click **Configuration > System > User Management**
2. Click the **General** button and use the slider to define the maximum number of simultaneous logins allowed for the camera.



Online users

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

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

Network

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

TCP/IP

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 Prefix Length	Enter the IPv6 subnet prefix length value of the camera.
IPv6 Default Gateway	Enter the IPv6 default gateway value of the camera.
MAC Address	Shows the MAC address of the devices.
MTU	Enter the 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 > Basic Settings > TCP/IP**.

The screenshot displays the TCP/IP configuration page with the following settings:

- TCP/IP** (selected tab), DDNS, PPPoE, Port, NAT, Multicast
- NIC Type: Auto
- DHCP
- IPv4 Address: 10.7.70.4 (Test button)
- IPv4 Subnet Mask: 255.255.255.0
- IPv4 Default Gateway: 10.7.70.254
- IPv6 Mode: Route Advertisement (View Route Advertisement button)
- IPv6 Address: [Empty]
- IPv6 Subnet Mask: [Empty]
- IPv6 Default Gateway: ::
- Mac Address: 84:9a:40:b1:a9:7d
- MTU: 1500
- Enable Multicast Discovery

DNS Server

- Preferred DNS Server: 10.1.7.97
- Alternate DNS Server: 10.1.7.98

Domain Name Settings

- Enable Dynamic Domain Name
- Register Domain Name: [Empty]

Save button

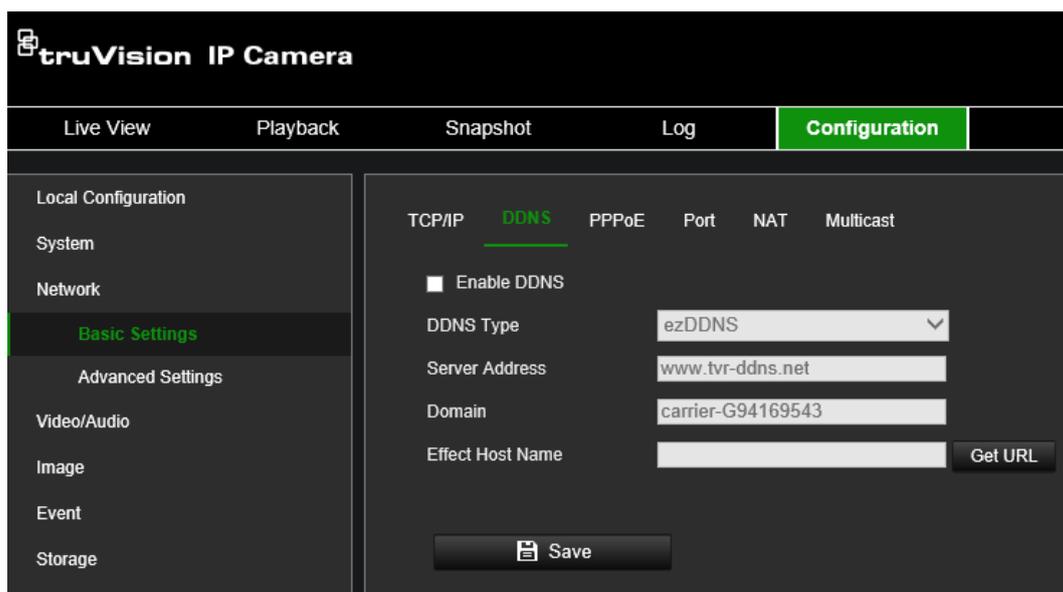
2. Configure the NIC settings, including the NIC Type, IPv4 settings, IPv6 settings, and MTU settings.
3. If the DHCP server is available, select **DHCP**.
4. If the DNS server settings are required for some applications (e.g., sending email), you should configure the **Preferred DNS Server** or **Alternate 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 > Basic Settings > DDNS**.



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

DynDNS: Select **DynDNS** and enter the server address for DynDNS. In the recorder domain name field, enter the domain name obtained from the DynDNS 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.

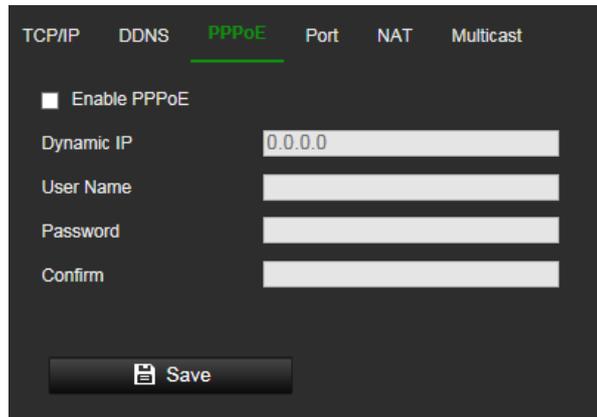
4. Click **Save** to save changes.
5. Reboot the device for the changes to take effect.

PPPoE

This allows you to retrieve a dynamic IP address.

To set up the PPPoE parameters:

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



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

Port

You can set up several ports:

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

RTSP Port: The default port is 554 and it can be changed to any port number from 1 to 65535.

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

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

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

WebSocket Port: The default port is 7681. It can be changed to any port number ranging from 1 to 65535.

WebSockets Port: The default server port is 7682. It can be changed to any port number from 1 to 65535.

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

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

To set up the port parameters:

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

TCP/IP	DDNS	PPPoE	Port	NAT	Multicast
HTTP Port			80		
RTSP Port			554		
HTTPS Port			443		
Server Port			8000		
Enhanced SDK Service Port			8443		
WebSocket Port			7681		
WebSockets Port			7682		
Alarm Host IP			0.0.0.0		
Alarm Host Port			5001		

Save

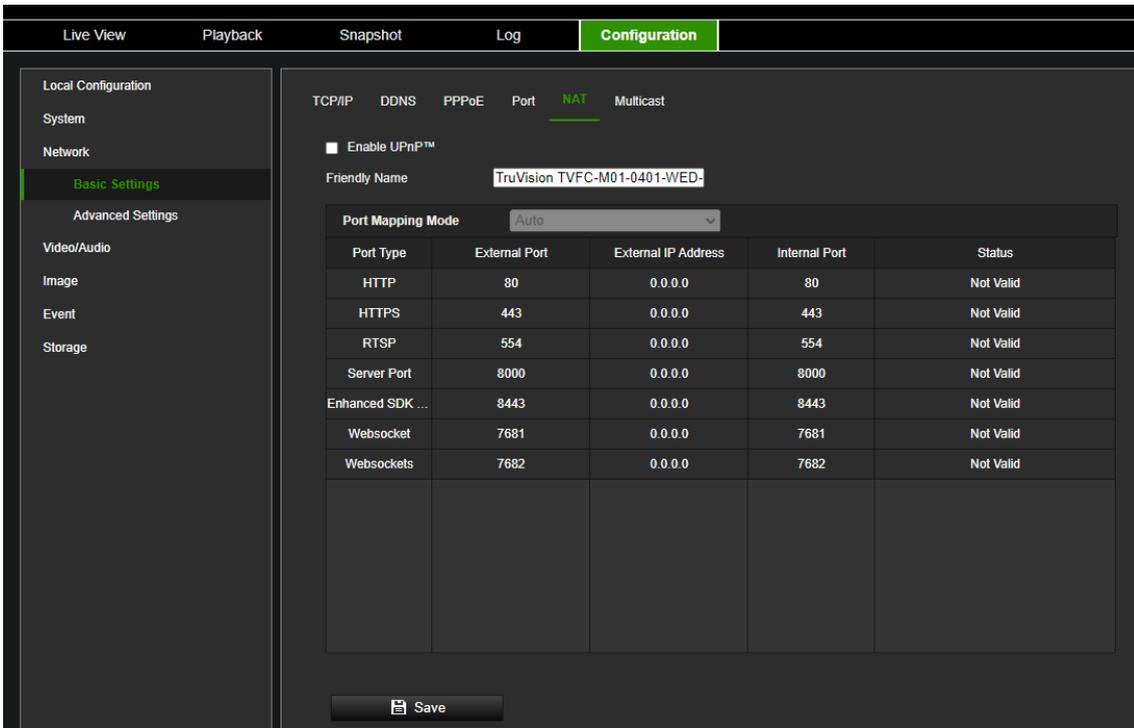
2. Set the HTTP port, RTSP port, HTTPS port, and Server port of the camera.
3. Enter the IP address and port if you want to upload the alarm information to the remote alarm host. Also, select the **Notify Alarm Recipient** option in the normal Linkage of each event page.
4. Click **Save** to save changes.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

NAT

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

To set up the NAT parameters:

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



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

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

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

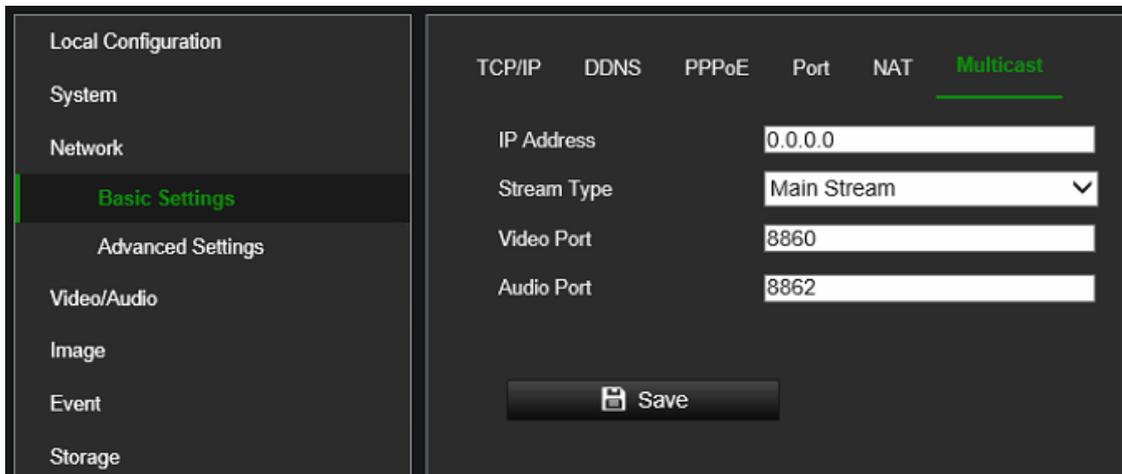
4. Click **Save** to save changes.

Multicast

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

To set up the Multicast parameters:

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



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. Configure the main stream and substream video and audio ports.
4. Click **Save** to save changes.

SNMP

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

To set up the SNMP parameters:

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

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.

FTP

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

To set up the FTP parameters:

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

The screenshot displays the 'FTP' configuration page. The left sidebar is titled 'Local Configuration' and includes sections for System, Network, Basic Settings, Advanced Settings (highlighted), Video/Audio, Image, Event, and Storage. The main content area has tabs for SNMP, FTP (selected), Email, HTTPS, QoS, 802.1x, Integration Protocol, Network Service, and HTTP Listening. The FTP configuration fields are as follows:

- Server Address: 0.0.0.0
- Port: 21
- User Name: [Empty field]
- Password: [Empty field]
- Confirm: [Empty field]
- Anonymous:
- Directory Structure: Save in the root directory (dropdown)
- Snapshot Archiving Interval: OFF (dropdown) Day(s)
- Snapshot Name: Default (dropdown)
- Upload Picture:
- Enable Automatic Network Replenishment:
- Test: [Test button]
- Save: [Save button]

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.

Email

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

To set up the email parameters:

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

No.	Receiver	Receiver's Address	Test
1			Test
2			Test
3			Test

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. NONE is default.

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

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

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

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

Password: Enter the password.

Confirm: Confirm the password.

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

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

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

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

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

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

3. Click **Test** to test the email parameters 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.

HTTPS

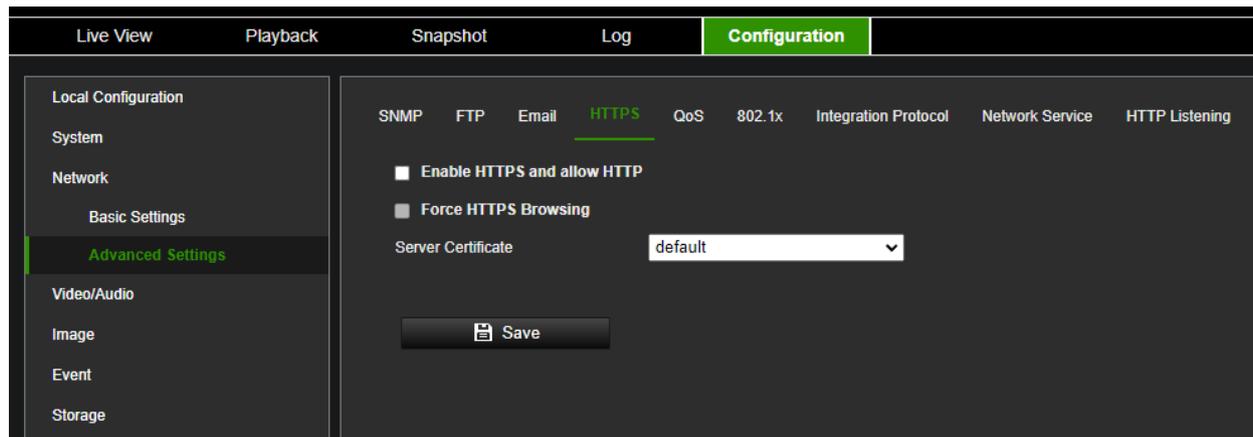
Specifies the authentication of the website and its associated web server, which protects against Man-in-the-middle attacks.

To set up the HTTPS parameters:

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

Select **Enable HTTPS and allow HTTP** to allow connections.

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



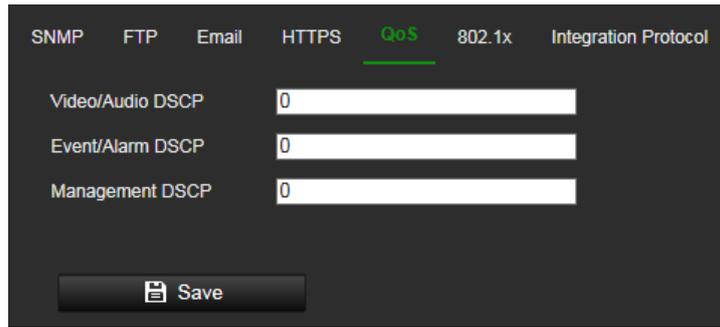
QoS

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 > Advanced Settings > QoS**.



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

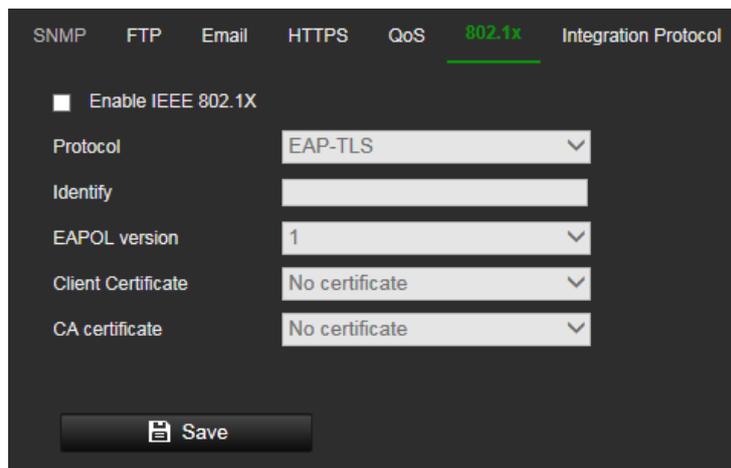
2. Configure the QoS settings, including Video / Audio DSCP, Event / Alarm DSCP, and Management DSCP. The valid value range of the DSCP is 0-63. The bigger the DSCP value is, the higher the priority is.
3. Click **Save** to save changes.

802.1x

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

To set up the 802.1x parameters:

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



The screenshot shows the '802.1x' configuration page. At the top, there are tabs for 'SNMP', 'FTP', 'Email', 'HTTPS', 'QoS', '802.1x' (which is selected and highlighted in green), and 'Integration Protocol'. Below the tabs, there is a checkbox labeled 'Enable IEEE 802.1X' which is currently unchecked. Below the checkbox, there are several configuration options: 'Protocol' is set to 'EAP-TLS' (dropdown menu), 'Identify' is an empty text input field, 'EAPOL version' is set to '1' (dropdown menu), 'Client Certificate' is set to 'No certificate' (dropdown menu), and 'CA certificate' is set to 'No certificate' (dropdown menu). At the bottom of the page, there is a '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.

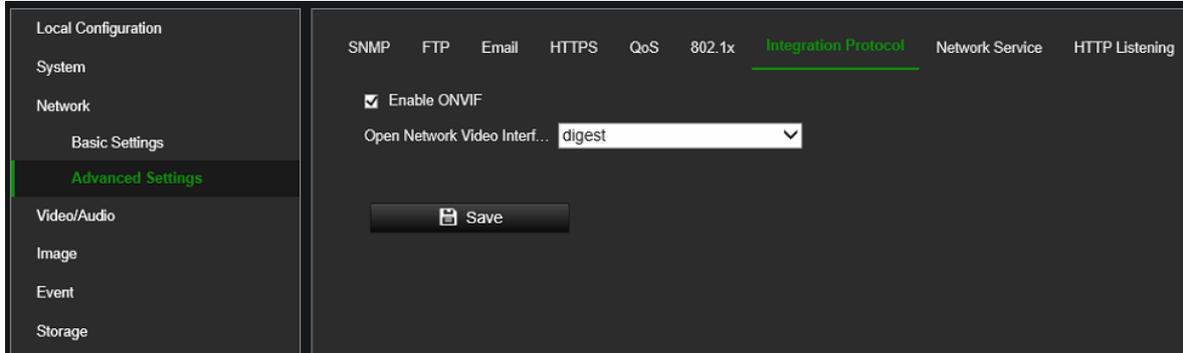
Note: The switch or router to which the camera is connected must also support the IEEE 802.1X standard. A server must also be configured. Please apply and register a username and password for 802.1X on the server.

Integration protocol

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

To set up the integration protocol parameters:

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



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

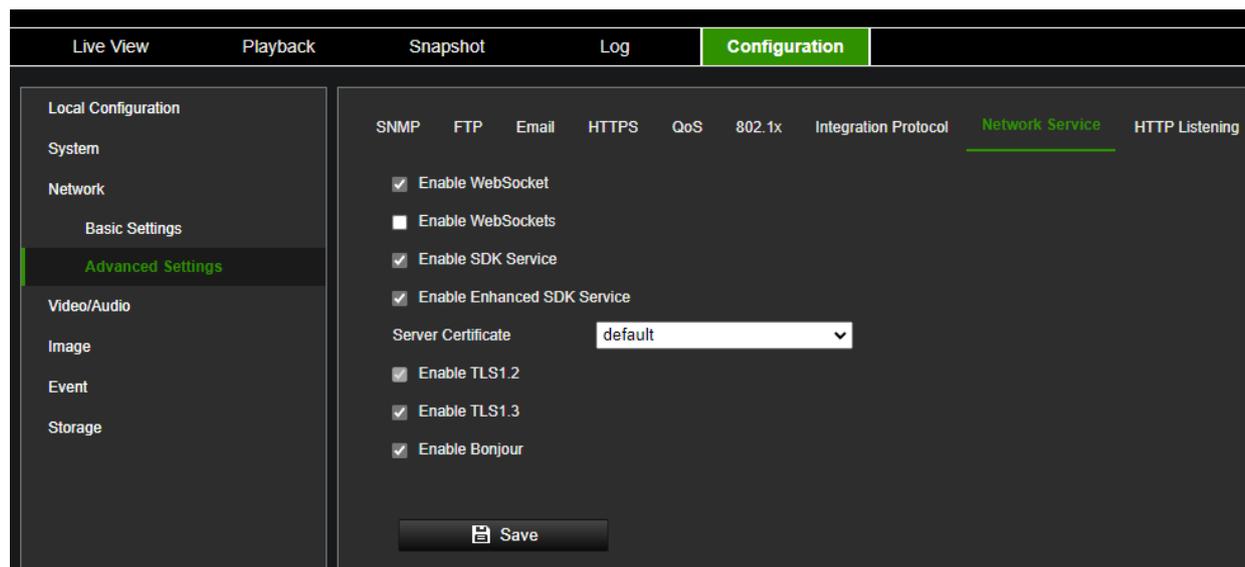
Network service

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

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

To set up the network service parameters:

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



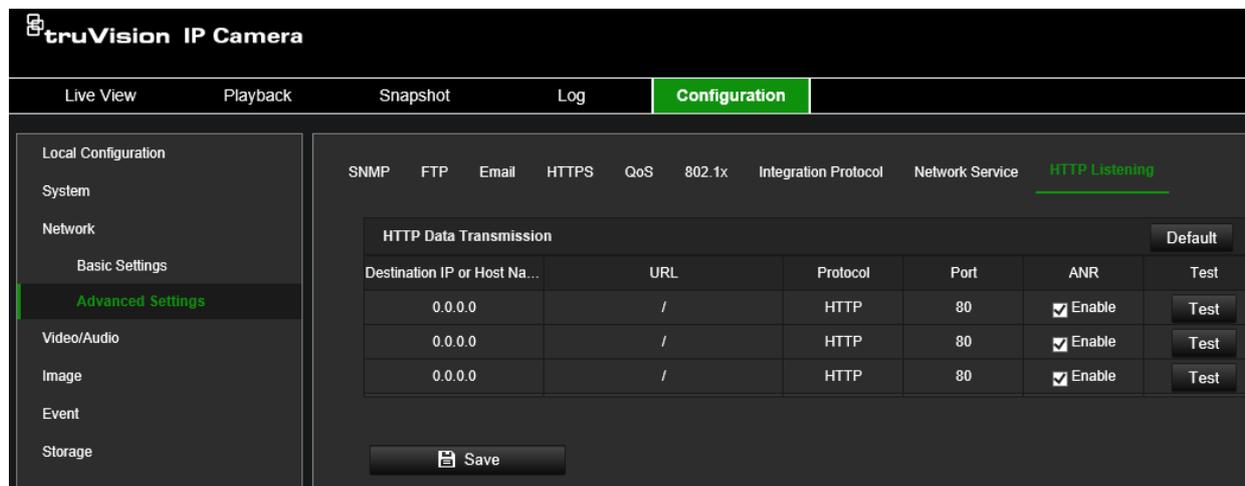
2. Select the **Enable WebSocket** check box to enable WebSocket service for live viewing over HTTP protocol without the plug-in.
3. Select the **Enable WebSockets** check box to enable WebSockets service for live viewing over HTTPS protocol without the plug-in.
4. Select the **Enable SDK Service** check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

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 > Network > Advanced Settings > HTTP**.



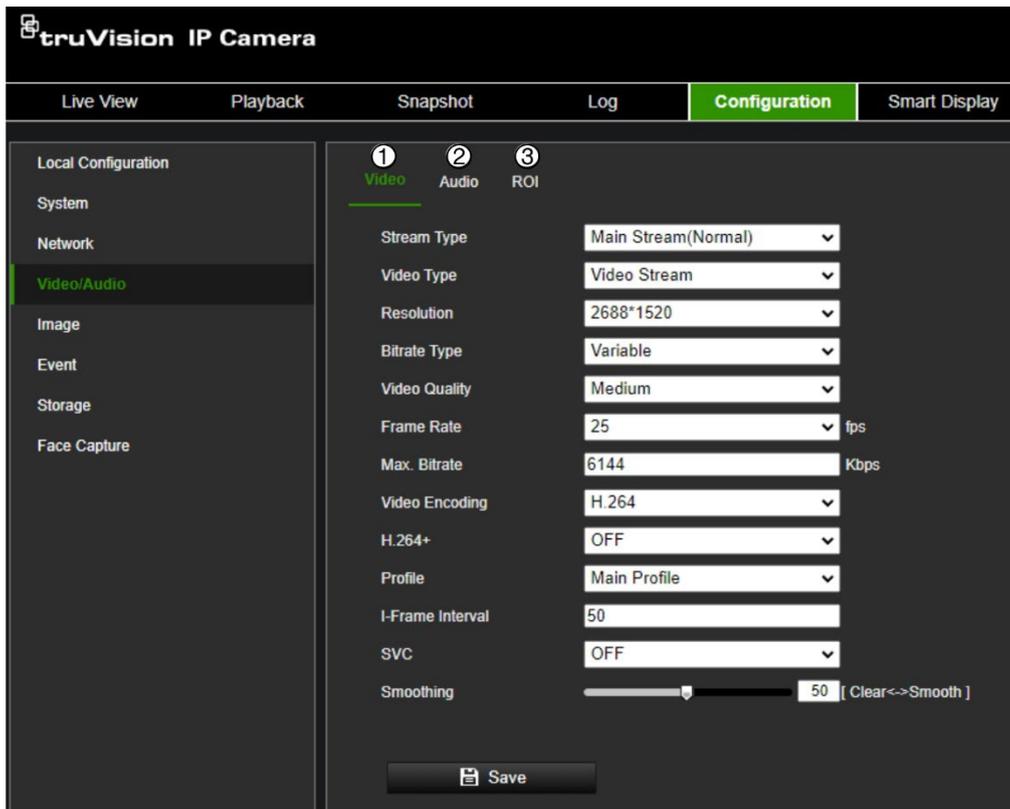
2. Enter the destination IP or hostname, URL, protocol type, and port number.
3. Click the **Test** button to test if the service is available.

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.

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)

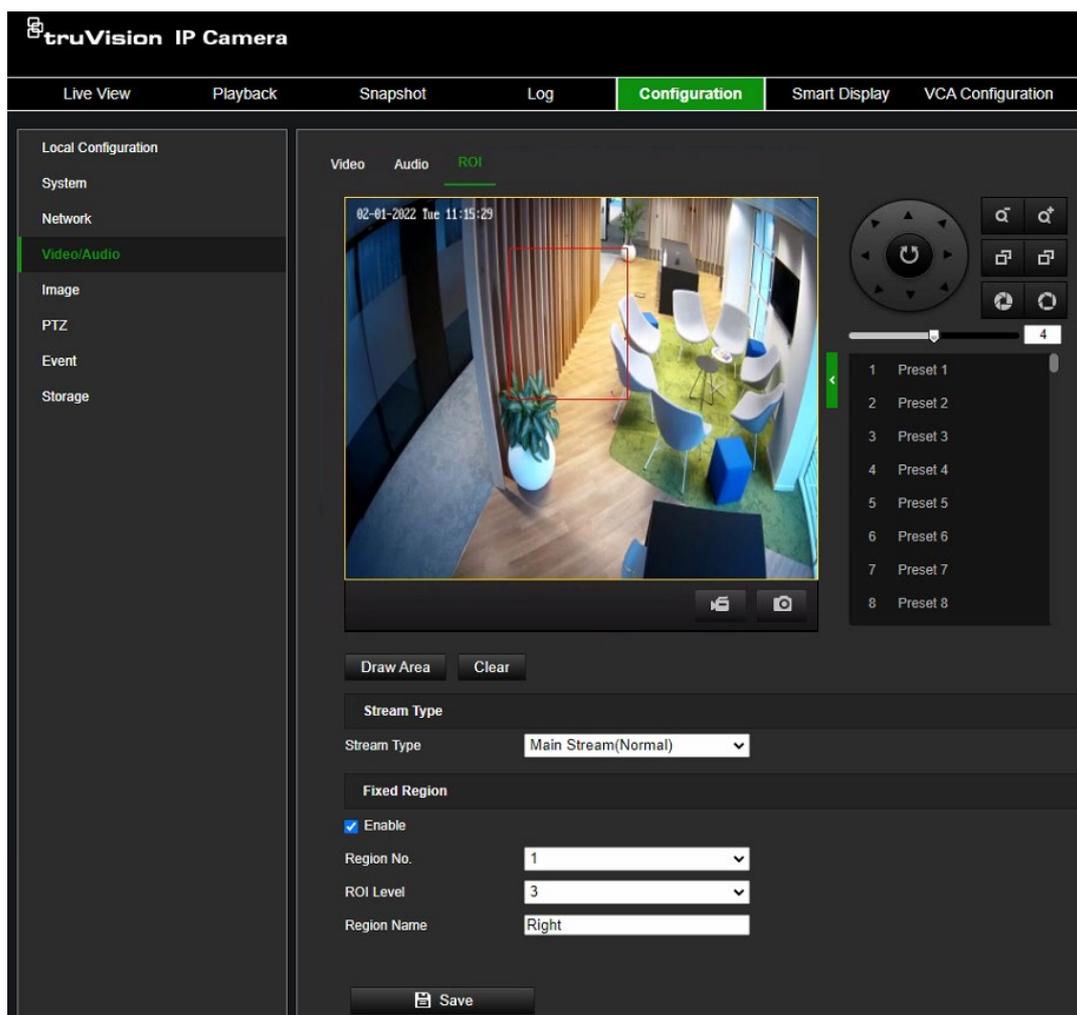


Tab	Parameter descriptions
1. Video	<p>Stream Type: Specifies the streaming method used. Options include Main, Stream, Substream, and Third Stream. Note that Third Stream is only available in Standard Event Mode (menu System > VCA Resource)</p> <p>Video Type: Specifies the stream information you wish to record. Select Video Stream to record video stream only. Select Video&Audio to record both video and audio streams.</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> <p>Video Quality: Specifies the quality level of the image. It can be set when a variable bit rate is selected. Options include Lowest, Lower, Low, Medium, Higher, and Highest.</p> <p>Frame Rate: Specifies the frame rate for the selected resolution. The frame rate is the number of video frames that are shown or sent per second.</p> <p>Note: The maximum frame rate depends on the camera model and selected resolution. Please check the camera specifications in its datasheet.</p> <p>Video Encoding: Specifies the video encoding used. You can choose between H.264 and H.265.</p>

Tab	Parameter descriptions
	<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>Note: H.264+ and H.265+ can only be in Standard Event mode. When switching to H.265+/H.264+, parameters such as SVC Profile and I-Frame Interval will not be supported.</p> <hr/> <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> <hr/> <p>I-Frame Interval: A video compression method. It is strongly recommended not to change the default value 50.</p> <hr/> <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> <hr/> <p>Smoothing: Adjust the smoothness of the stream. Smoothing is not available when H.264+ or H.265+ video encoding is used.</p>
<p>2. Audio (only available if the hardware supports it)</p>	<p>Audio Encoding: G.722.1, G.711ulaw, G.711alaw, MP2L2, G.726, and PCM are supported.</p> <hr/> <p>Audio Input: Mic In and Line In are selectable for the connected microphone and pickup, respectively. Note: Options can vary depending on the camera model.</p> <hr/> <p>Input Volume: Specifies the microphone volume from 0 to 100.</p> <hr/> <p>Output volume: Specifies the audio output volume</p> <hr/> <p>Environmental Noise Filter: Set it as OFF or ON. When you set the function On, the noise detected can be filtered.</p>
<p>3. ROI</p>	<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>

To configure ROI settings:

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



2. Draw the region of interest on the image.
3. Choose the stream type to be used for the ROI encoding.
4. Under the *Fixed Region* section, select **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.

Region Name: Set the desired region name.

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

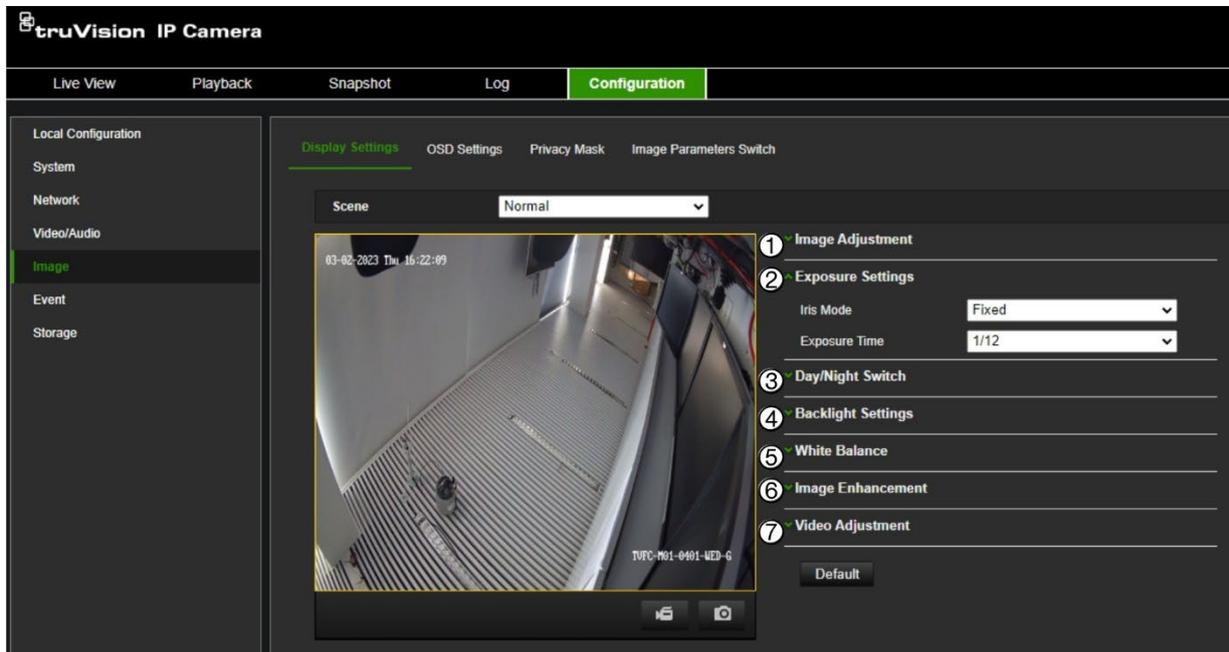
Image

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.

Parameter	Description
3. Day/Night Switch	
Day/Night Switch	<p>Defines whether the camera is in day or night mode. The day (color) option could be used, for example, if the camera is located indoors where light levels are always good.</p> <p>Select one of the following options:</p> <p>Day: Camera is always in day mode.</p> <p>Night: Camera is always in night mode.</p> <p>Auto: The camera automatically detects which mode to use depending on the amount of light captured by the camera.</p> <p>Scheduled switch: The camera switches between day and night modes according to the configured period.</p>
Sensitivity	<p>Only available when <i>Auto D/N switch</i> mode is selected. It defines the sensitivity of the switch between day and night.</p> <p>Set it between 1 and 7.</p>
Filtering Time	<p>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.</p>
Smart Supplement Light	<p>When enabled, it can avoid over-exposure problems by decreasing the amount of white-light illumination for objects closer to the camera</p>
Supplement Light Mode	<p>White Supplement Light: The white-light LEDs are ON when the camera changes to night mode.</p> <p>OFF: The white-light LEDs remain OFF when the camera changes to night mode</p>
Light Brightness Control	<p>Auto: The intensity of the white light will be set automatically according to environmental light.</p> <p>Manual: In manual mode, the white-light intensity can be set to a desired fixed value using the white-light slider.</p>
4. Backlight Settings	
BLC	<p>This function improves image quality when the background illumination is high. It prevents the object in the center of the image from appearing too dark.</p> <p>Select OFF, Up, Down, Left, Right, Center, or Auto.</p>
WDR	<p>When enabled, wide dynamic range (WDR) provides clear images when there is high contrast between light and dark areas in the field of view of the camera. Both bright and dark areas can be displayed in the frame.</p> <p>This option can also be enabled/disabled from the General control panel in Live View.</p>
Wide Dynamic Level	<p>The WDR level can be fine-tuned by changing its value between 0 and 100</p>
HLC	<p>Use the highlight compensation (HLC) function when there are strong sources of light in the scene that affects the image quality.</p> <p>This option can also be enabled/disabled from the General control panel in Live View.</p>

Parameter	Description
5. White Balance	
	<p>White balance (WB) tells the camera what the color white looks like. Based on this information, the camera will then continue to display all colors correctly even when the color temperature of the scene changes such as from daylight to fluorescent lighting, for example. Select one of the options below:</p> <p>MWB: Manually adjust the color temperature to meet your requirements.</p> <p>AWB1: Automatically adjust the camera's white balance between 2500 to 9500K for environments where the lighting is always stable.</p> <p>AWB2: Automatically adjust the camera's white balance within a narrower range than that of AWB1. This adjustment is more accurate.</p> <p>Locked WB: Locks the WB to the current environment color temperature.</p> <p>Fluorescent Lamp: For use where there are fluorescent lamps installed near the camera.</p> <p>Incandescent Lamp: For use where there are incandescent lamps installed near the camera.</p> <p>Warm light lamp: For use in situations where an external warm light is present near the camera.</p> <p>Natural light: For use where the camera is installed in a natural light environment.</p>
6. Image Enhancement	
Digital Noise Reduction	<p>Digital noise reduction (DNR) reduces noise, especially in low light conditions, to improve image performance.</p> <p>Select Normal Mode, OFF, or Advanced. Default is Normal.</p>
Defog Mode	<p>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.</p>
EIS	<p>Electrical Image Stabilizer (EIS) reduces the effects of vibration in a video. Default is OFF. Using EIS will decrease the camera's field of view.</p>
7. Video Adjustment	
Mirror	<p>It mirrors the image so you can see it inversed.</p> <p>Select Center or OFF. Default is OFF.</p>
Video Standard	<p>Select PAL (50 Hz) or NTSC (60 Hz).</p> <p>Select the value depending on the video standards.</p>

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

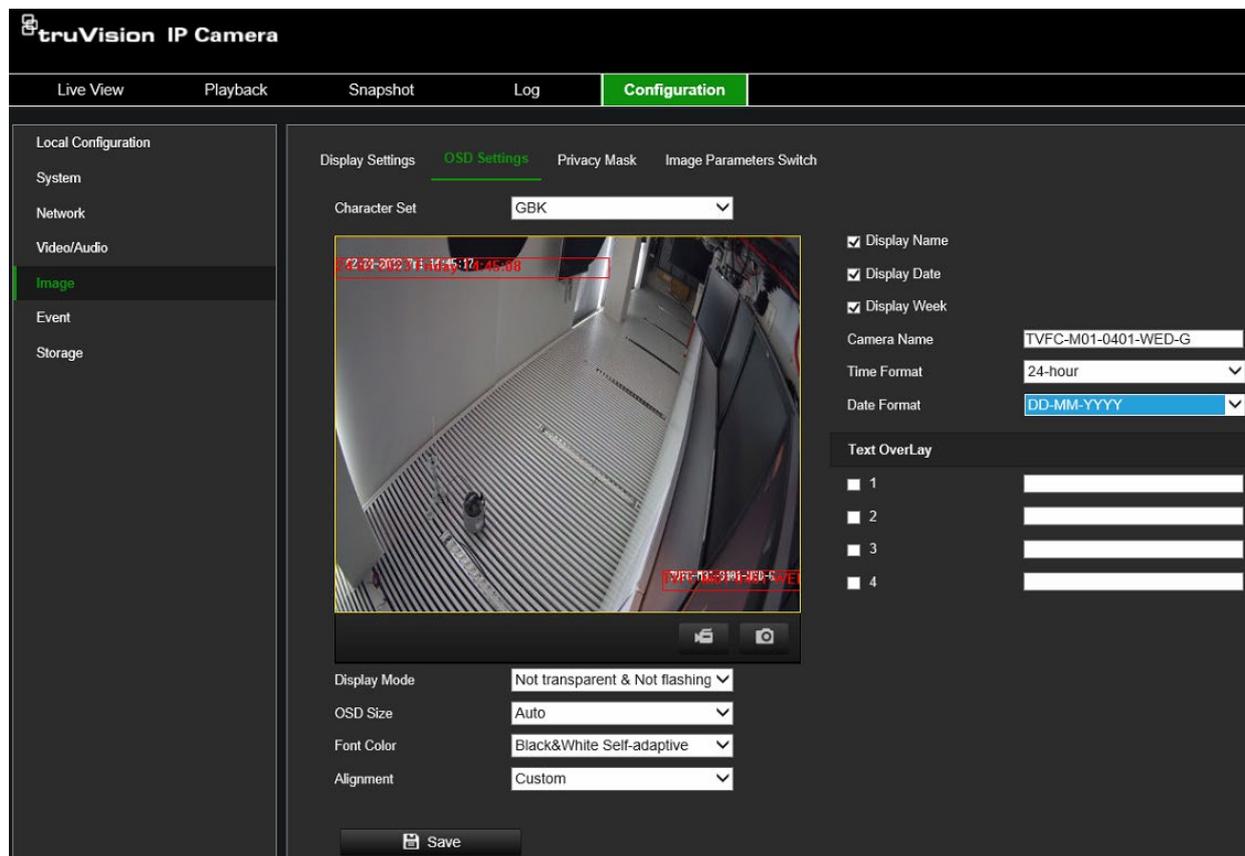
OSD Settings (On Screen Display)

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

You can also set up the OSD settings from the *Live View General* control panel. Go to **Live View > General > OSD Settings** and select the desired options.

To set up the OSD text:

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



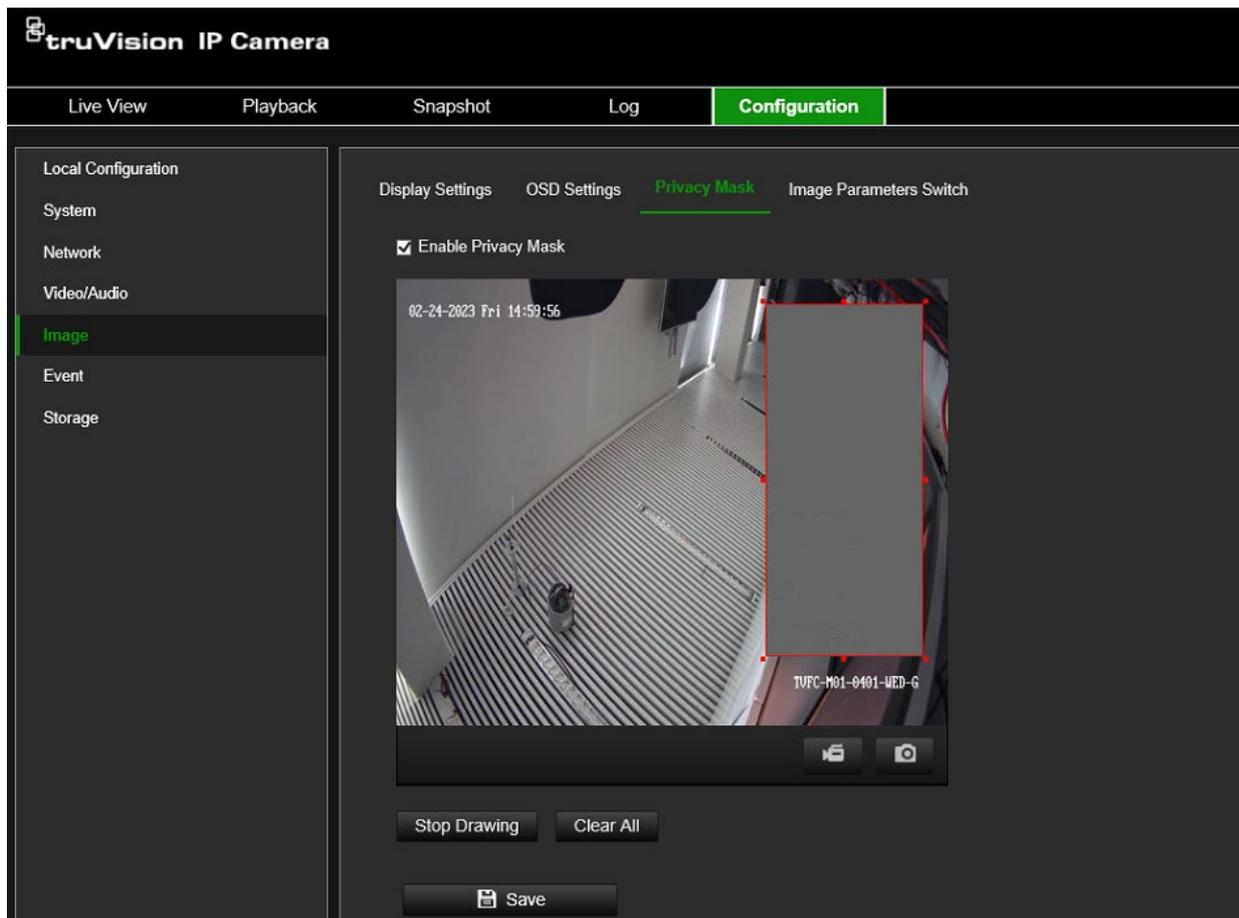
2. Select the **Display Name** box to display the camera's name on screen. You can modify the default name in the text box of **Camera Name**.
3. Select the **Display Date** check box to display the date/time on screen.
4. Select the **Display Week** check box to include the day of the week in the on-screen display.
5. In the **Camera Name** box, enter the camera name.
6. Select the time and date formats from the **Time format** and **Date format** drop-down list boxes.
7. Select a display mode for the camera from the **Display Mode** drop-down list box. Display modes include:
 - **Transparent & Not flashing.** The image appears through the text.
 - **Transparent & Flashing.** The image appears through the text. The text flashes on and off.
 - **Not transparent & Not flashing.** The image is behind the text. This is default.
 - **Not transparent & Flashing.** The image is behind the text. The text flashes on and off.
8. Select the desired OSD size.
9. Select the desired font color.
10. Select the desired alignment (Custom, Align Left, or Align Right).
11. Click **Save** to save changes.

Note: If the display mode is set as transparent, the text varies, according to the background. With some backgrounds, the text may be not 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 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. Select the **Enable Privacy Mask** check box to enable the function
3. Click the **Draw Area** button and draw the mask area.
4. Delete an existing privacy mask area by clicking the **Clear All** button.
5. Click **Save** to save changes.

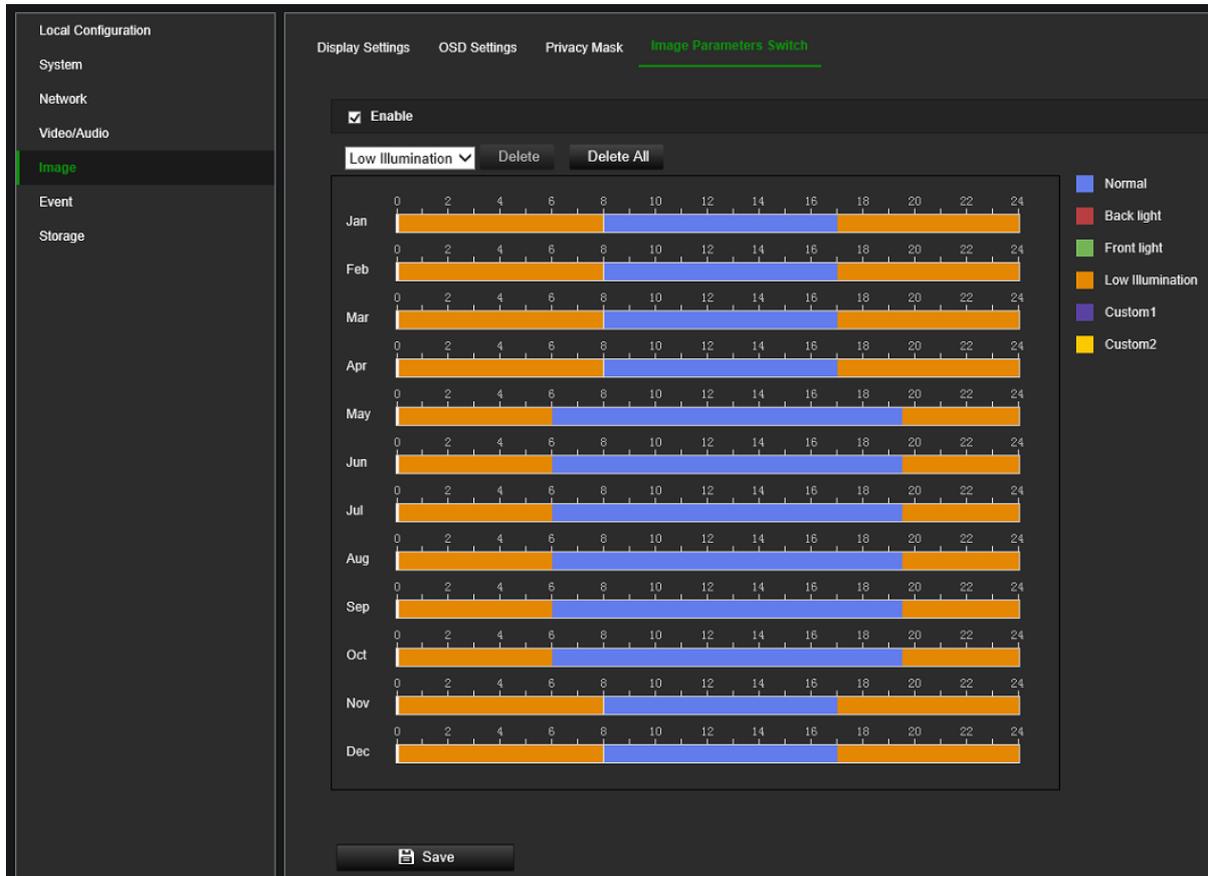
Image Parameters Switch

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 42 for further information). You can link up to four lighting scenes to the scheduled D/N.

To set up an image parameter switch:

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



2. Select the **Enable** check box to activate this function.
3. Select from the drop-down list 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 when the alarm can be recorded. You can schedule up to eight time periods in a day.
 To change a lighting scene, double-click it and make your changes in the pop-up box that appears. 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 for one month, you can click on a period and manually type in the start/end time to fine-tune the period.
5. When you hover the mouse above a timeline bar a small green copy button appears at the end of the bar that allows you to easily copy the selected month configuration to another month.
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. There are two categories, Basic and Smart Event.

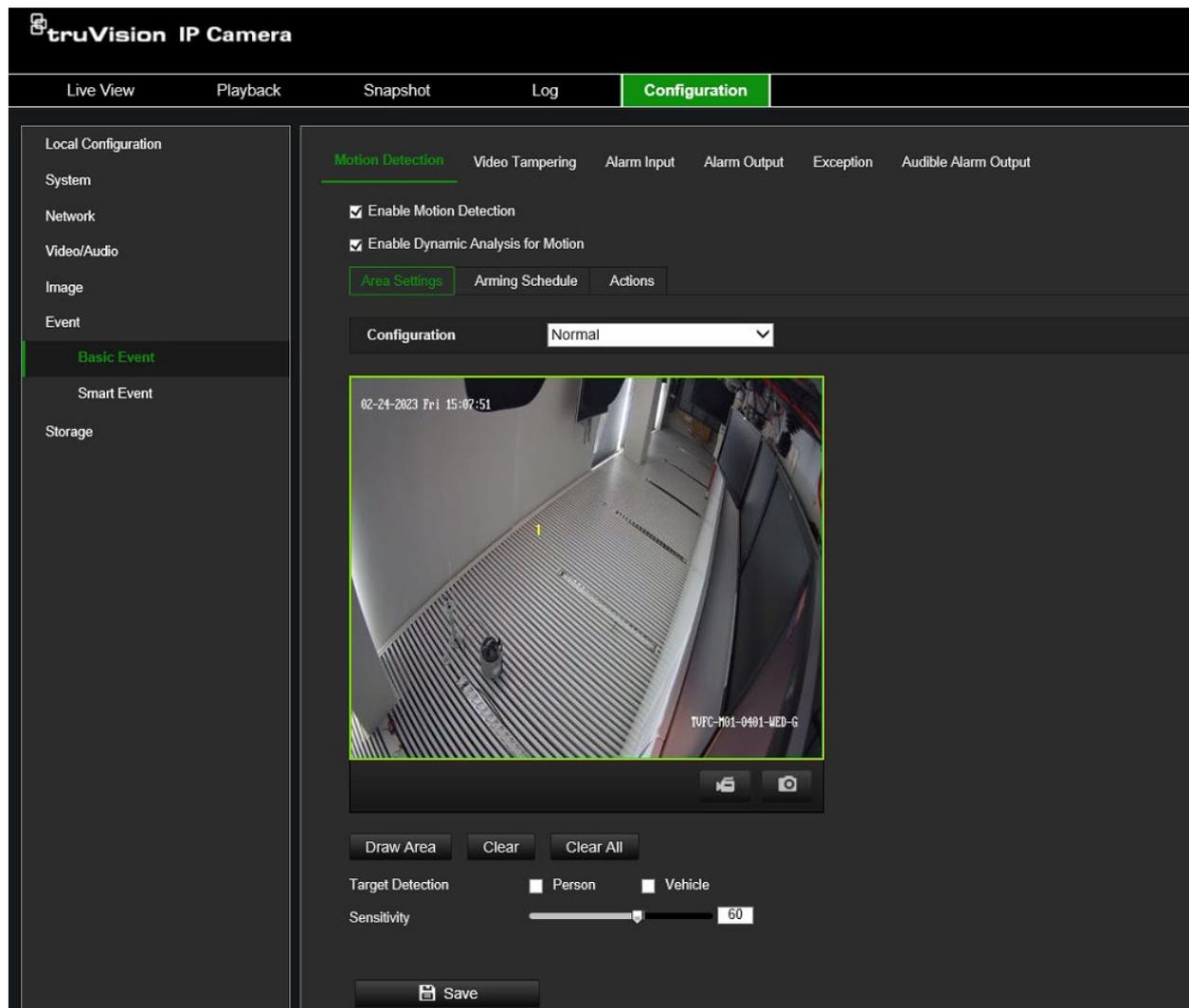
Motion Detection

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 as green. See Figure 6 below.

Figure 6: Motion detection window



Defining a motion detection alarm requires the following tasks:

1. **Area settings:** Draw a polygon area on the image where you want the camera to generate motion detection alarm and set the detection sensitivity level (see Figure 6 on page 48, item 1).
2. **Arming schedule:** Define the schedule during which the system detects motion (see Figure 6 on page 48, item 2).
3. **Recording schedule:** Define the schedule during which motion detection can be recorded (when using an SD card or NAS). See “Recording schedule” on page 75 for further information.
4. **Actions:** Specify the actions triggered by the motion event (see Figure 6 on page 48, item 3).
5. **Normal and advanced configuration:** Normal configuration allows you to set the sensitivity level of the motion detection (see Figure 6 on page 48, item 4). Advanced configuration gives you additional configuration options. It allows you to define up to eight separate motion areas with different sensitivity and scene parameters. Target options for person/vehicle are not available in *Advanced Motion Detection* mode.

To set up motion detection in normal mode:

1. Click **Configuration > Event > Basic Event > Motion Detection**.
- **Set up the motion detection area:**
2. Select the **Enable Motion Detection** check box. Also, select the **Enable Dynamic Analysis for Motion** check box if you want to see real-time motion events.

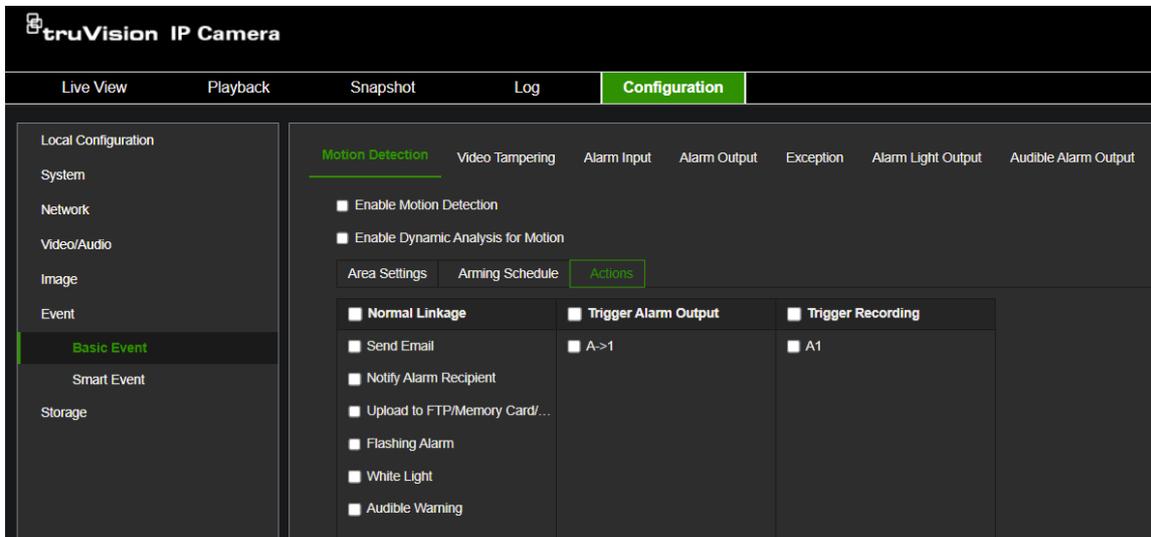
Note: If you do not want the detected object to be marked with the green frame, select **Disable** from **Configuration > Local Configuration > Live View Parameters > Enable Meta Data Overlay**.

3. Under Configuration, select **Normal** mode from the drop-down list.
4. Click **Draw Area**. Click the mouse to set the start point of the area where you want to detect motion. Then move to another position and click the mouse to define the first side of the detection area. Repeat this step to draw additional lines and ultimately close the detection area. A detection area can be a polygon with a maximum of 10 sides. After the last side of the polygon is drawn, right-click the mouse to close the polygon and stop drawing.

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

5. Click **Clear All** to delete all areas marked and restart drawing.
6. Select Target Detection **Person** and/or **Vehicle** in case you want the camera to generate motion only on these targets.
7. Move the **Sensitivity** slider to set the sensitivity of the detection. All areas will have the same sensitivity level.

- **Set up the arming schedule:**
8. 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).
 9. Click  to copy the schedule to other days or the whole week.
- **Set up a linking method to the motion detection alarm:**
10. 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:



<p>Send Email</p>	<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 33 for further information. If you want to send the event snapshot together with the email, check the Attached Snapshot option.</p>
<p>Notify Alarm Recipient</p>	<p>Send an exception or alarm signal to remote management software when an event occurs.</p>
<p>Upload to FTP/Memory Card/NAS</p>	<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 79 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 32 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 73” for further information.</p>
<p>Flashing Alarm</p>	<p>A flashing white alarm light will activate when an event occurs. Configure more settings related to this action in the menu Configuration > Event > Basic Event > Alarm Light Output.</p>
<p>White Light</p>	<p>Trigger the white light when an event occurs. When enabled, you can also set a duration between 0 and 90 s.</p>

Audible Warning	An audio message can be triggered when an event occurs. For camera models with built-in speakers, the audio can be heard through the speaker. For models without a speaker, the audio is only available via the audio line out output. Configure more settings related to this action in the menu Configuration > Event > Basic Event > Audible Alarm Output.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Select “Select All” or each alarm output. Note: This option is only available for cameras that support alarm output.
Trigger Recording	Triggers the recording to start in the camera.

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

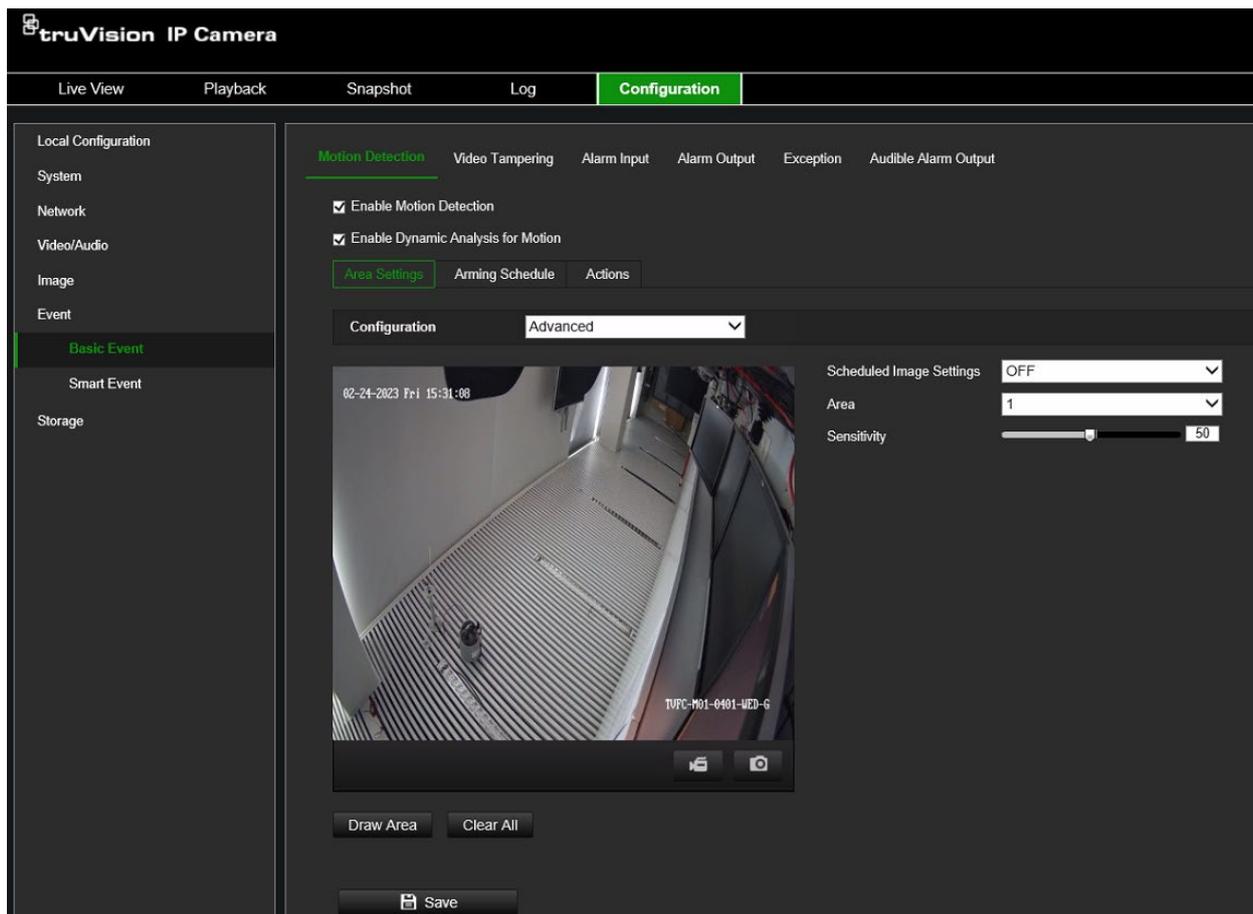
Note: some of the above-mentioned actions might not be available on some camera models. They will only appear when supported by the hardware.

To set up advanced motion detection:

1. Click **Configuration > Event > Basic Event > Motion Detection**.
- **Set up the motion detection area:**
2. Select the **Enable Motion Detection** box. Also, select **Enable Dynamic Analysis for Motion** if you want to see where motion occurs in real time.

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

3. Under Configuration, select **Advanced** mode from the drop-down list.



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

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

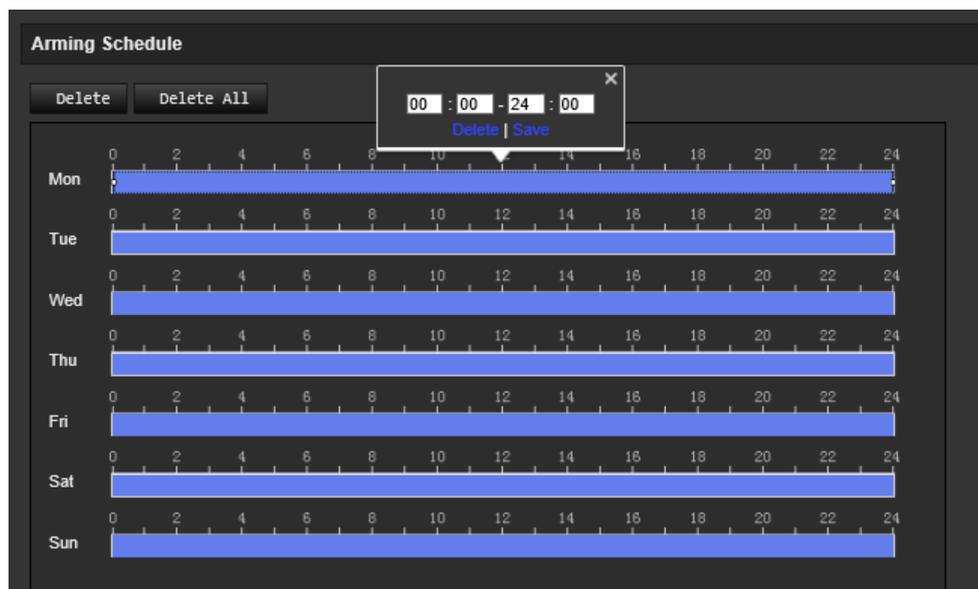
5. Select **Area No.** and click **Draw Area**. Click and drag the mouse on the live video image to draw an area sensitive to motion detection.

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

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

- **Set up the arming schedule:**

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



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



3. Click **OK** to save changes.

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

4. Click **Actions** to specify when an event action occurs. Select one or more response methods for the system when a motion detection alarm is triggered. Refer to “Set up a linking method to the motion detection alarm” on page 50 for more details on motion detection actions.

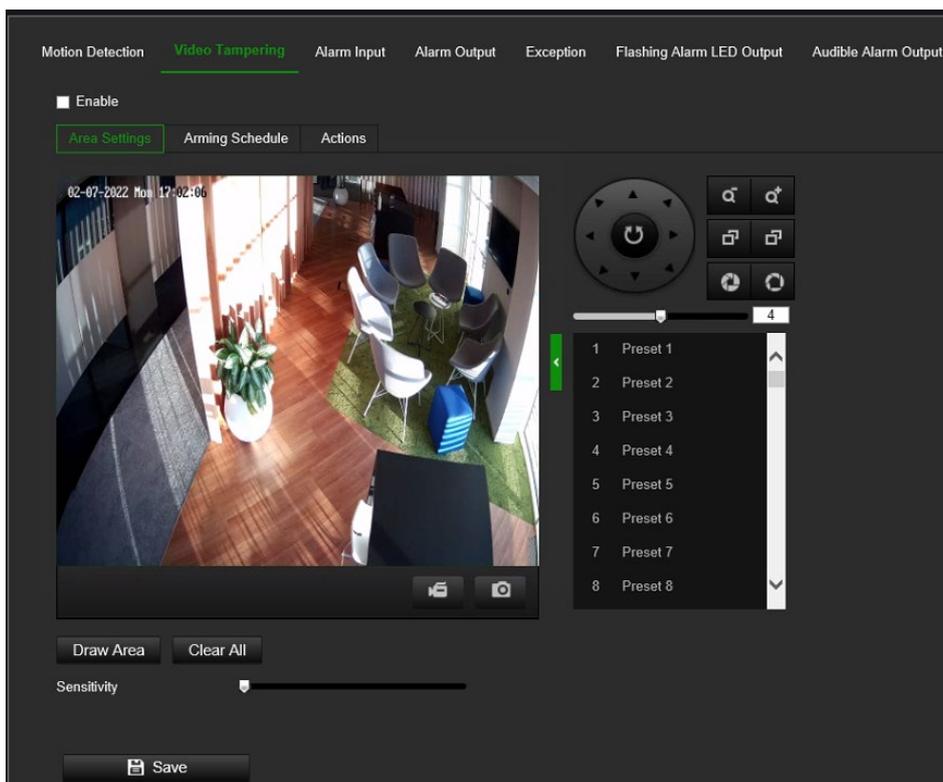
5. Click **Save** to save changes.

Video Tampering

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

To set up tamper-proof alarms:

1. From the menu toolbar, click **Configuration > Camera Configuration > Alarm Event > Video Tampering**.



2. Select the **Enable** option to activate *Video Tampering*.

3. Move the **Sensitivity** slider to set the detection sensitivity.

- Edit the arming schedule for video tampering. The arming schedule configuration is the same as that for motion detection. See “To set up motion detection” on page 49 for more information.
- Specify the linkage method when an event occurs. Select one or more response methods for the system when video tampering is triggered.

Send Email	Send an email to a specified address when there is a motion detection alarm. Note: You must configure email settings before enabling this option. See “To set up the email parameters” on page 33 for further information. If you want to send the event snapshot together with the email, select the Attached Snapshot option.
Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Select “Select All” or each alarm output. Note: This option is only available for cameras that support alarm output.

- Click **Save** to save changes.

Alarm Inputs and Outputs

To set up the external alarm input:

- Click **Configuration > Event > Basic Event > Alarm Input**.
- Choose the **Alarm Input No.** and the **Alarm Type**. The alarm type can be NO (Normally Open) and NC (Normally Closed). Enter a name for the alarm input.
- Set the arming schedule for the alarm input. See “To set up motion detection” on page 49 for more information.
- Select the check box to select the actions.

Send Email	Send an email to a specified address when there is a motion detection alarm. Note: You must configure email settings before enabling this option. See “To set up the email parameters” on page 33 for further information. If you want to send the event snapshot together with the email, check the Attached Snapshot option.
Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.

Upload to FTP/Memory Card/NAS	<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 79 for further information. To upload the snapshot to an FTP, you must first configure the FTP settings. See “To define the FTP parameters” on page 32 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 73” for further information.</p>
Flashing Alarm	<p>A flashing white alarm light will activate when an event occurs. Configure more settings related to this action in the menu Configuration > Event > Basic Event > Alarm Light Output.</p>
White Light	<p>Trigger the white light when an event occurs. When enabled, you can also set a duration between 0 and 90 s.</p>
Audible Warning	<p>An audio message can be triggered when an event occurs. For camera models with built-in speakers, the audio can be heard through the speaker. For models without a speaker, the audio is only available via the audio line out output. Configure more settings related to this action in the menu Configuration > Event > Basic Event > Audible Alarm Output.</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>
Trigger Recording	<p>Triggers the recording to start in the camera.</p>

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

To set up an alarm output:

1. Click **Configuration > Event > Basic Event > Alarm Output**.
2. Select one alarm output channel from the **Alarm Output** drop-down list. You can also set a name for the alarm output.
3. Set the delay time to 5 s, 10 s, 30 s, 1 min, 2 min, 5 min, 10 min, or manual. The delay time refers to the time duration that the alarm output remains in effect after the alarm occurs.
4. Set the arming schedule for the alarm input. See “To set up motion detection” on page 49 for more information.
5. Click **Save** to save changes.

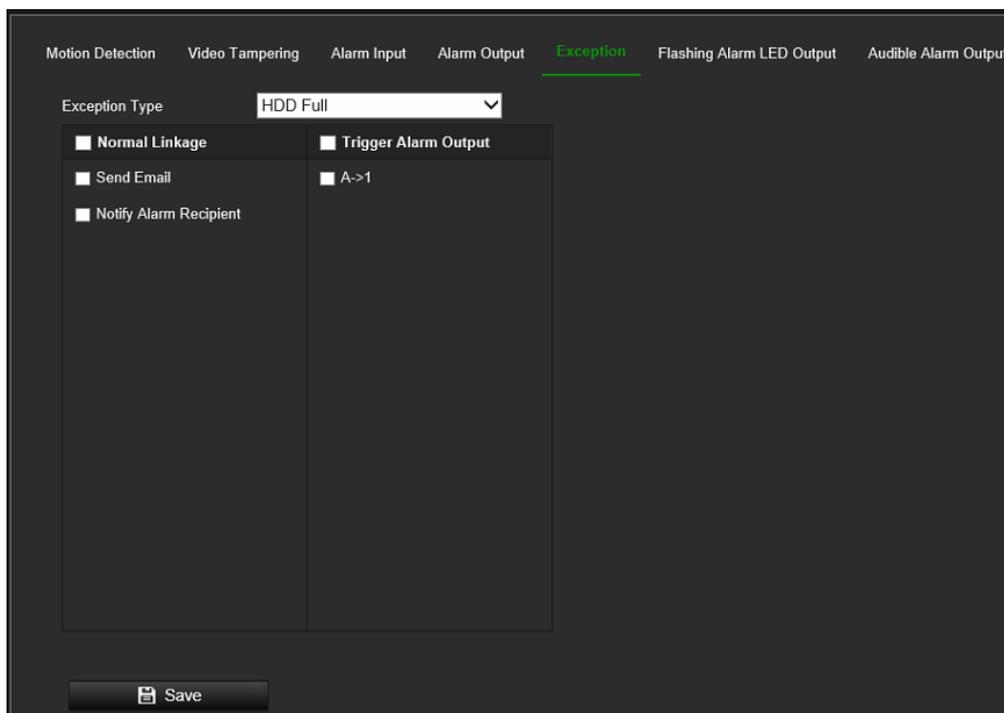
Exception

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

- **HDD Full:** All recording space of NAS is full.
- **HDD Error:** Errors occurred while files were being written to the storage, no storage or storage had failed to initialize.

- **Network Disconnected:** Disconnected network cable.
- **IP Address Conflicted:** Conflict in IP address setting.
- **Invalid Login:** Wrong user ID or password login attempt to the cameras.

Figure 7: Exception window



To set up exception alarms:

1. Click **Configuration > Event > Basic Event > Exception**.
2. Under **Exception Type**, select an exception type from the drop-down list.
3. Specify the actions when an event occurs. Select one or more response actions when an exception alarm is triggered.

Send Email	Send an email to a specified address when there is a motion detection alarm. Note: You must configure email settings before enabling this option. See “To set up the email parameters” on page 33 for further information. If you want to send the event snapshot together with the email, check the Attached Snapshot option.
Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Select “Select All” or each alarm output. Note: This option is only available for cameras that support alarm output.

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

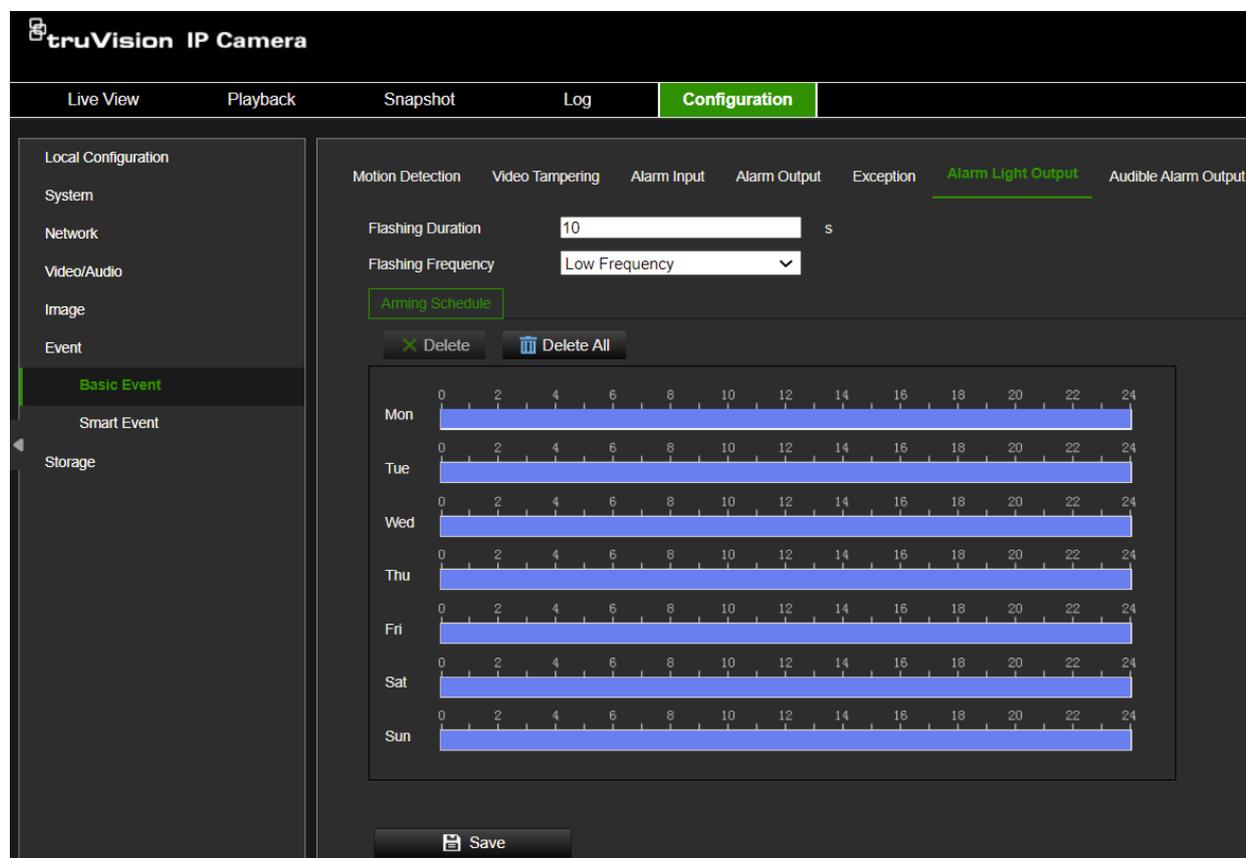
Alarm Light Output

Depending on the camera model a white alarm light may be supported.

The *Flashing Duration* determines how long the alarm light will be activated after an event. Supported duration is between 1 and 300 seconds.

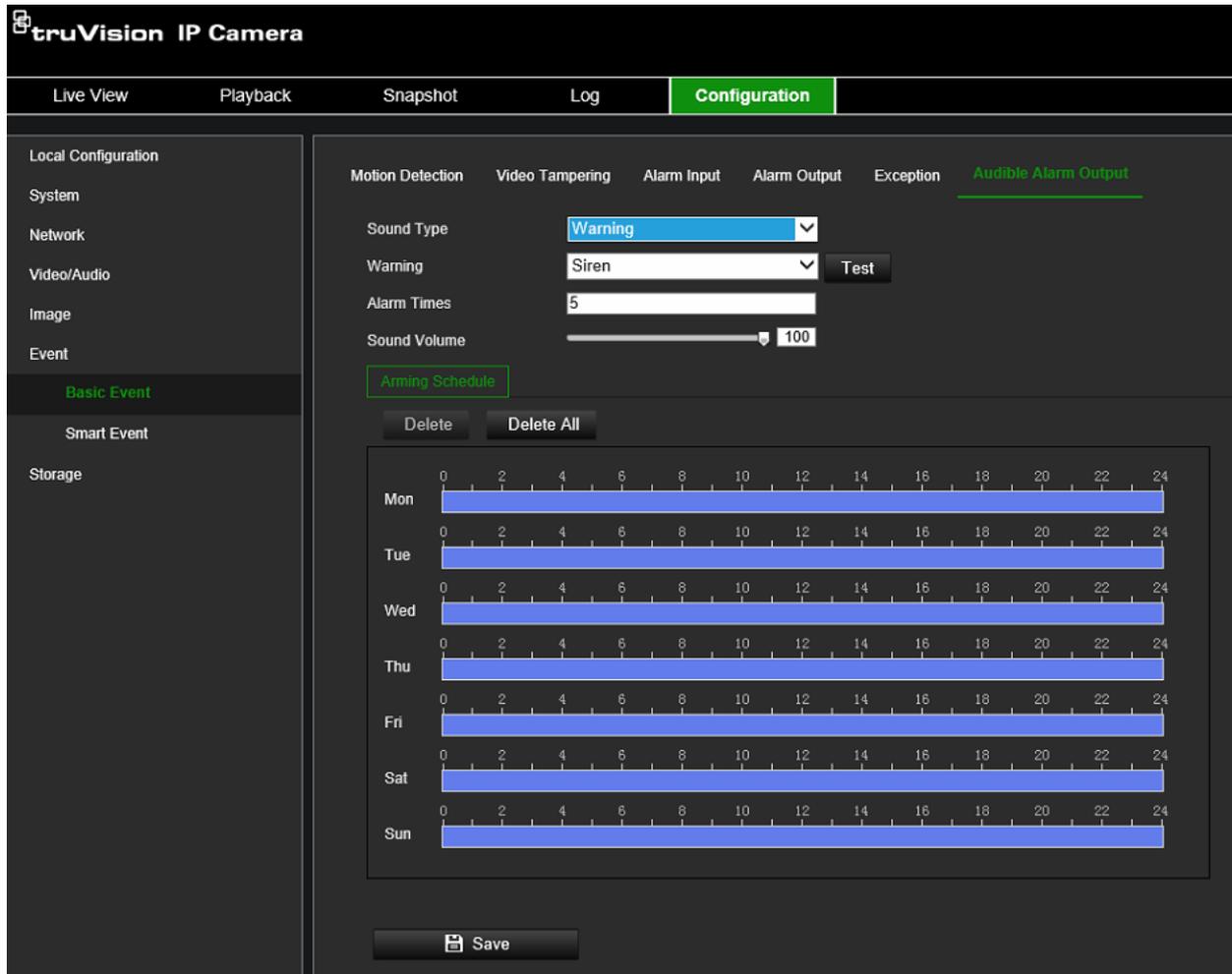
The *Flashing Frequency* determines the flashing interval when the light is active. Available values are High/Medium/Low Frequency or Normally On.

Like other event features, an arming schedule can be defined to determine when the alarm LED can be triggered.



Audible Alarm Output

The camera can trigger a pre-defined or custom audio alert when an event occurs. To use this feature, the camera needs to support an audio output or a built-in speaker.



To set up the audible alarm output:

1. Click **Configuration > Event > Basic Event > Audible Alarm Output**.
2. Choose the desired **Sound Type**. You can choose between **Warning**, **Prompt**, or **Custom Audio**.
3. With **Custom Audio** you can upload a .wav audio file max 512 kB recorded at 8 kHz into the camera.
4. Click the **Test** button to check the audio Set the arming schedule for the alarm input. See “To set up motion detection” on page 49 for more information.
5. Set the **Sound Duration** to define the duration of the audio alarm
6. Select the check box to select the actions.
7. Adjust the **Sound Volume** slider to the desired level
8. Configure the **Arming Schedule** to define when audio can be triggered
9. Click **Save** to save changes.

VCA Configuration

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

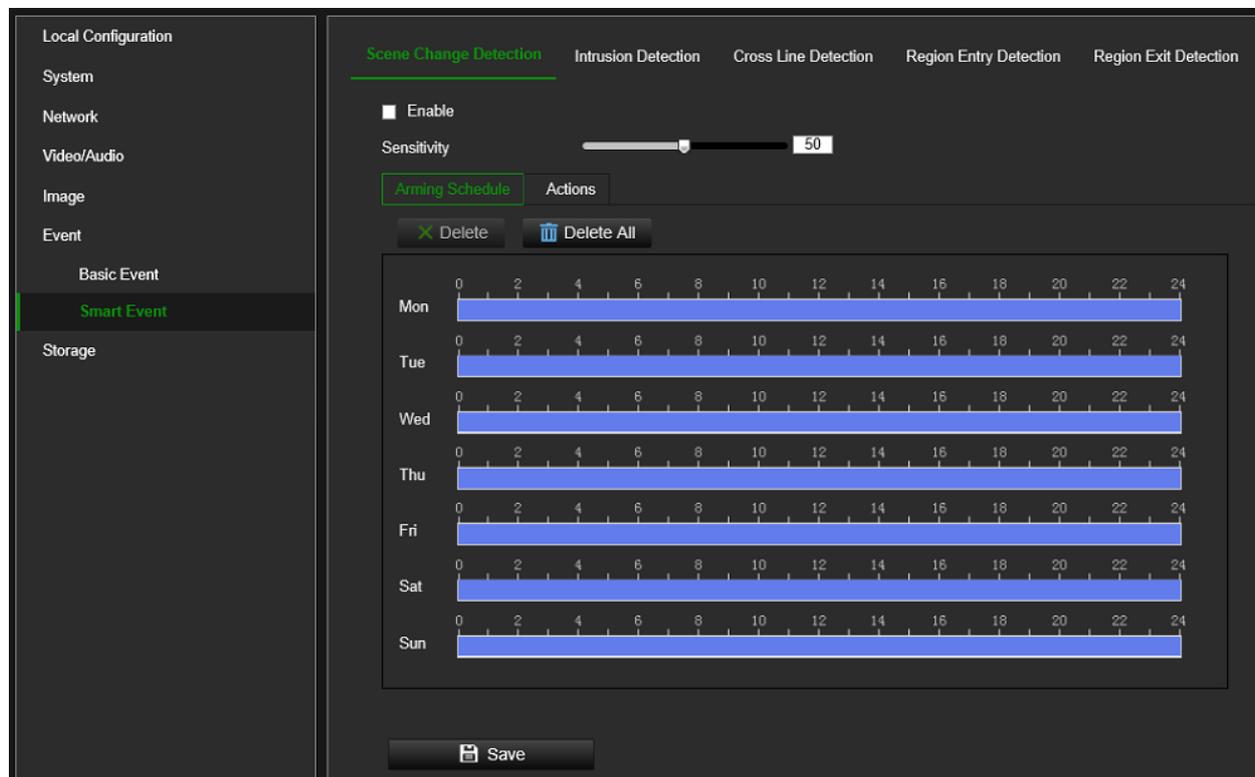
Some of these features are only available in a specific VCA Resource mode. See VCA Resource on page 13 for more information.

Scene Change Detection

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

To set up scene change detection:

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



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

Normal Actions	This is a group selection. It automatically selects “Send Email” and “Notify Alarm Recipient”.
-----------------------	--

Send Email	Sends an email to a specified address when there is a motion detection alarm. Note: You must configure email settings before enabling this option. See “Email” on page 33 for further information. If you want to send the event snapshot together with the email, select the Attached Snapshot option.
Notify Alarm Recipient	Send an exception or alarm signal to the remote management software when an event occurs.
Upload to FTP/Memory Card/NAS	Capture the image when an alarm is triggered and upload the picture to NAS, Memory Card, or FTP server. Note: To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS” on page 79 for further information. To upload the snapshot to an FTP, you must first configure the FTP settings. See “To define the FTP parameters” on page 32 for further information. Enable the Upload Type option. To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also select Enable Event-triggered Snapshot under the snapshot parameters. See “Storage” on page 73” for further information.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Select “Select All” or each alarm output. Note: This option is only supported by cameras that feature an alarm output.
A->1	Trigger the alarm input A->1.
A1	Triggers the recording to start in the camera.

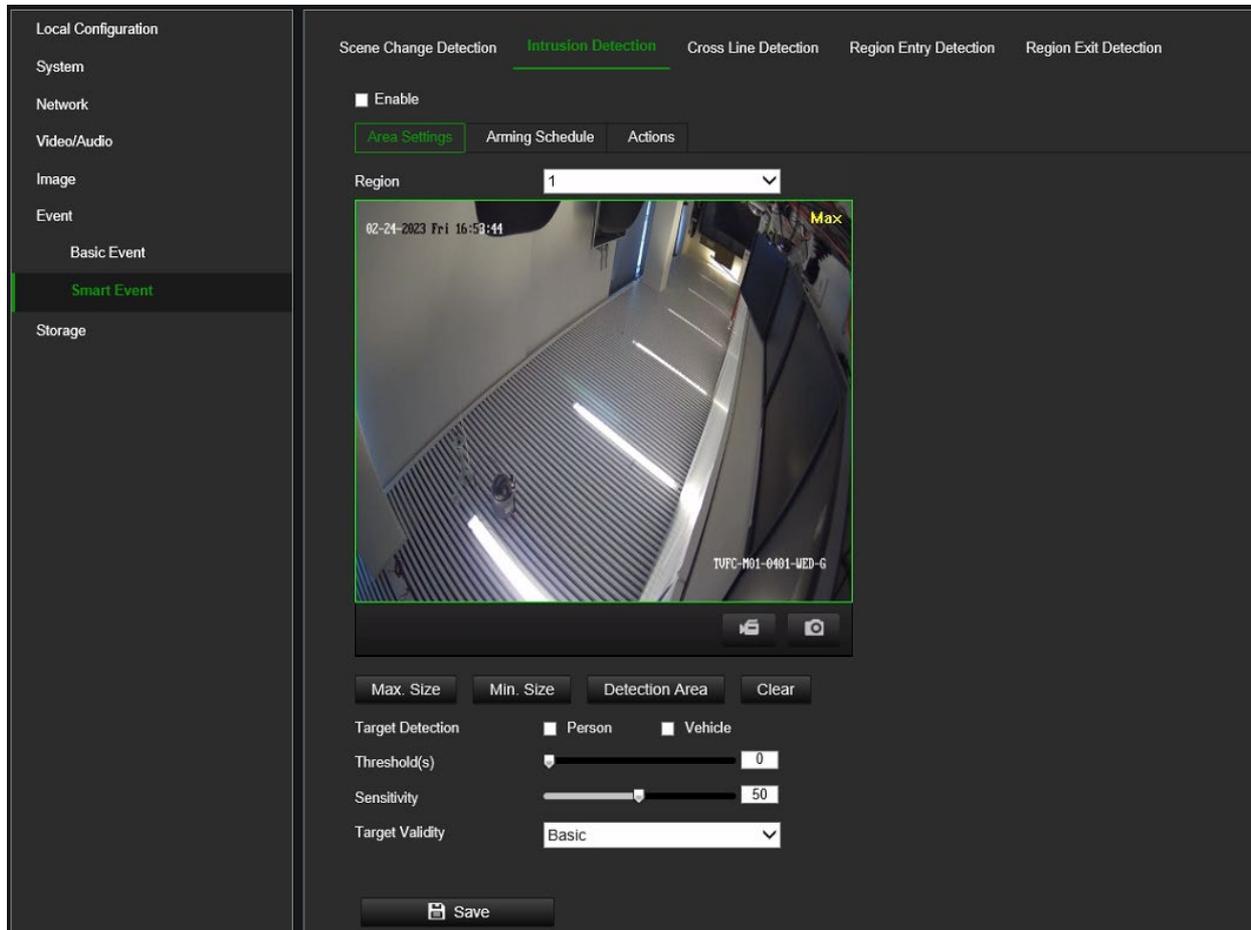
6. Click **Save** to save changes.

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 > Smart Event > Intrusion Detection**.



2. Select the **Enable** check box to enable the function.
3. 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.

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.
4. Click **Detection Area** and 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 **Clear** to clear the area you have drawn.
5. Enable the options **Person and/or Vehicle** to have the camera react to people or vehicles. Selecting the person/vehicle options will result in fewer false intrusion detection events and will also exclude, for example, animals. If neither option is selected, the camera will react to all types of objects.
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 10 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** tab and set the arming schedule for the alarm input. See “To set up motion detection” on page 49 for more information.
8. Click the **Actions** tab and specify the actions when an event occurs. Select one or more response actions when an intrusion detection alarm is triggered.

Send Email	<p>Send an email to a specified address when there is a motion detection alarm.</p> <p>Note: You must configure email settings before enabling this option. See “To set up the email parameters” on page 33 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 79 for further information. To upload the snapshot to an FTP, you must first configure the FTP settings. See “To define the FTP parameters” on page 32 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 73” for further information.</p>
Flashing Alarm	<p>A flashing white alarm light will activate when an event occurs. Configure more settings related to this action in the menu Configuration > Event > Basic Event > Alarm Light Output.</p>
White Light	<p>Trigger the white light when an event occurs. When enabled, you can also set a duration between 0 and 90 s.</p>
Audible Warning	<p>An audio message can be triggered when an event occurs. For camera models with built-in speakers, the audio can be heard through the speaker. For models without a speaker, the audio is only available via the audio line out output. Configure more settings related to this action in the menu Configuration > Event > Basic Event > Audible Alarm Output.</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>
Trigger Recording	<p>Triggers the recording to start in the camera.</p>

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

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

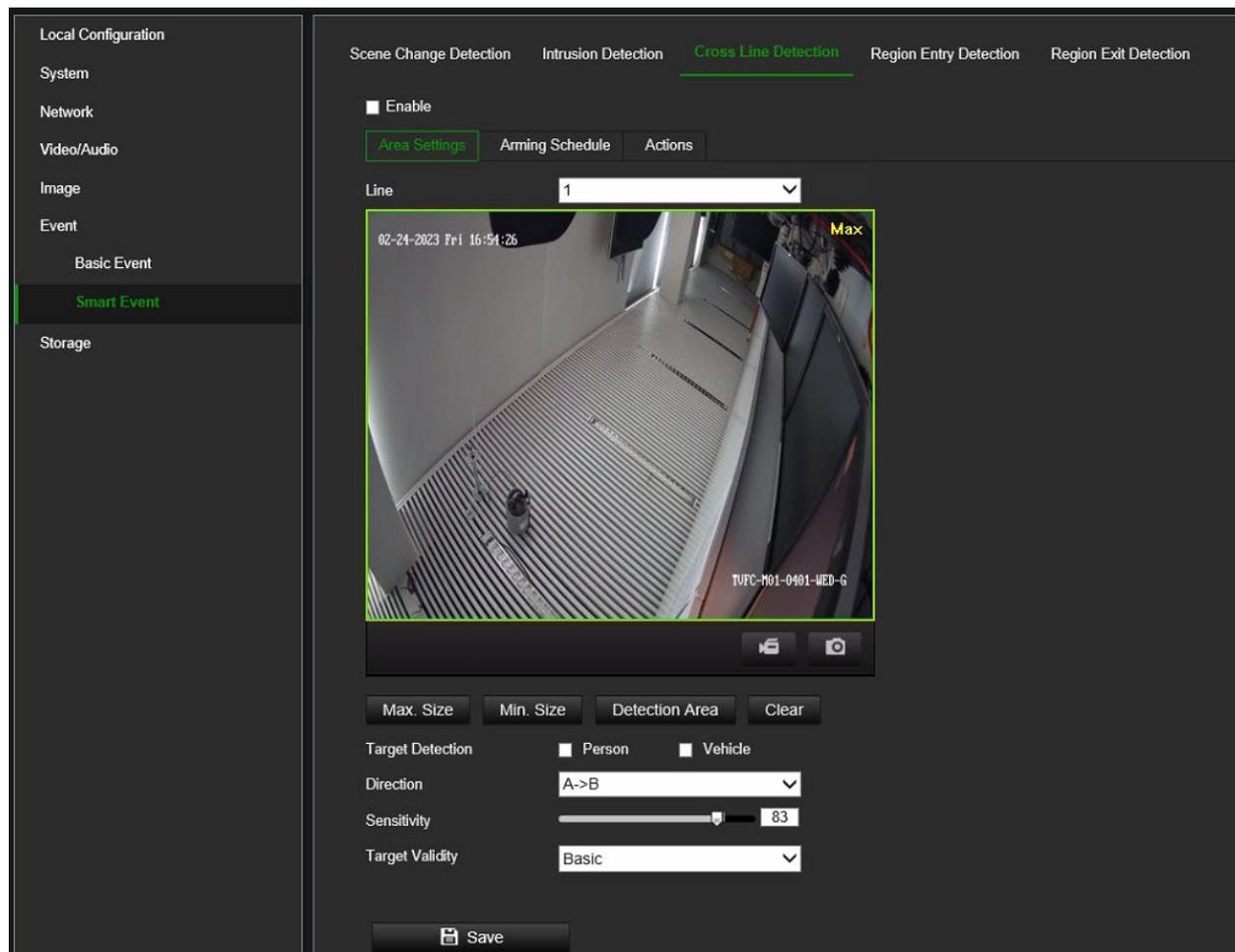
Cross Line Detection

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

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

To set up cross line detection:

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



2. Select the **Enable** check box to enable the function.
3. Click the **Area Settings** tab.
3. Under **Line**, select the desired line from the drop-down list for detection settings.
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.

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 **Detection Area** to have a cross line on the live video viewer. Click the starting point of the line on the live video viewer and drag it to the desired end position. 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. Enable the options **Person and/or Vehicle** to have the camera react to people or vehicles. Selecting the person/vehicle options will result in fewer false intrusion detection events and will also exclude, for example, animals. If neither option is selected, the camera will react to all types of objects.
7. Set the **Sensitivity** level between 1 and 100. The higher the value, the more easily the line crossing action can be detected.
8. If desired, select another line crossing area to configure from the **Line** dropdown menu. Up to four cross lines can be configured.
9. Set the arming schedule for the alarm input. See “To set up motion detection” on page 49 for more information.
10. Specify the linkage method when an event occurs. Select one or more response methods for the system when a line cross detection alarm is triggered.

Send Email	Send an email to a specified address when there is a motion detection alarm. Note: You must configure email settings before enabling this option. See “To set up the email parameters” on page 33 for further information. If you want to send the event snapshot together with the email, check the Attached Snapshot option.
Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.
Upload to FTP/Memory Card/NAS	Capture the image when an alarm is triggered and upload the picture to NAS, Memory Card, or FTP server. Note: To upload the snapshot to NAS, you must first configure the NAS settings. See “NAS” on page 79 for further information. To upload the snapshot to an FTP, you must first configure the FTP settings. See “To define the FTP parameters” on page 32 for further information. Enable the Upload Type option. To upload the snapshot to FTP and NAS when motion detection or an alarm input is triggered, you must also select Enable Event-triggered Snapshot under the snapshot parameters. See “Storage” on page 73” for further information.
Flashing Alarm	A flashing white alarm light will activate when an event occurs. Configure more settings related to this action in the menu Configuration > Event > Basic Event > Alarm Light Output.
White Light	Trigger the white light when an event occurs. When enabled, you can also set a duration between 0 and 90 s.

Audible Warning	An audio message can be triggered when an event occurs. For camera models with built-in speakers, the audio can be heard through the speaker. For models without a speaker, the audio is only available via the audio line out output. Configure more settings related to this action in the menu Configuration > Event > Basic Event > Audible Alarm Output.
Trigger Alarm Output	Trigger external alarm outputs when an event occurs. Select “Select All” or each alarm output. Note: This option is only available for cameras that support alarm output.
Trigger Recording	Triggers the recording to start in the camera.

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

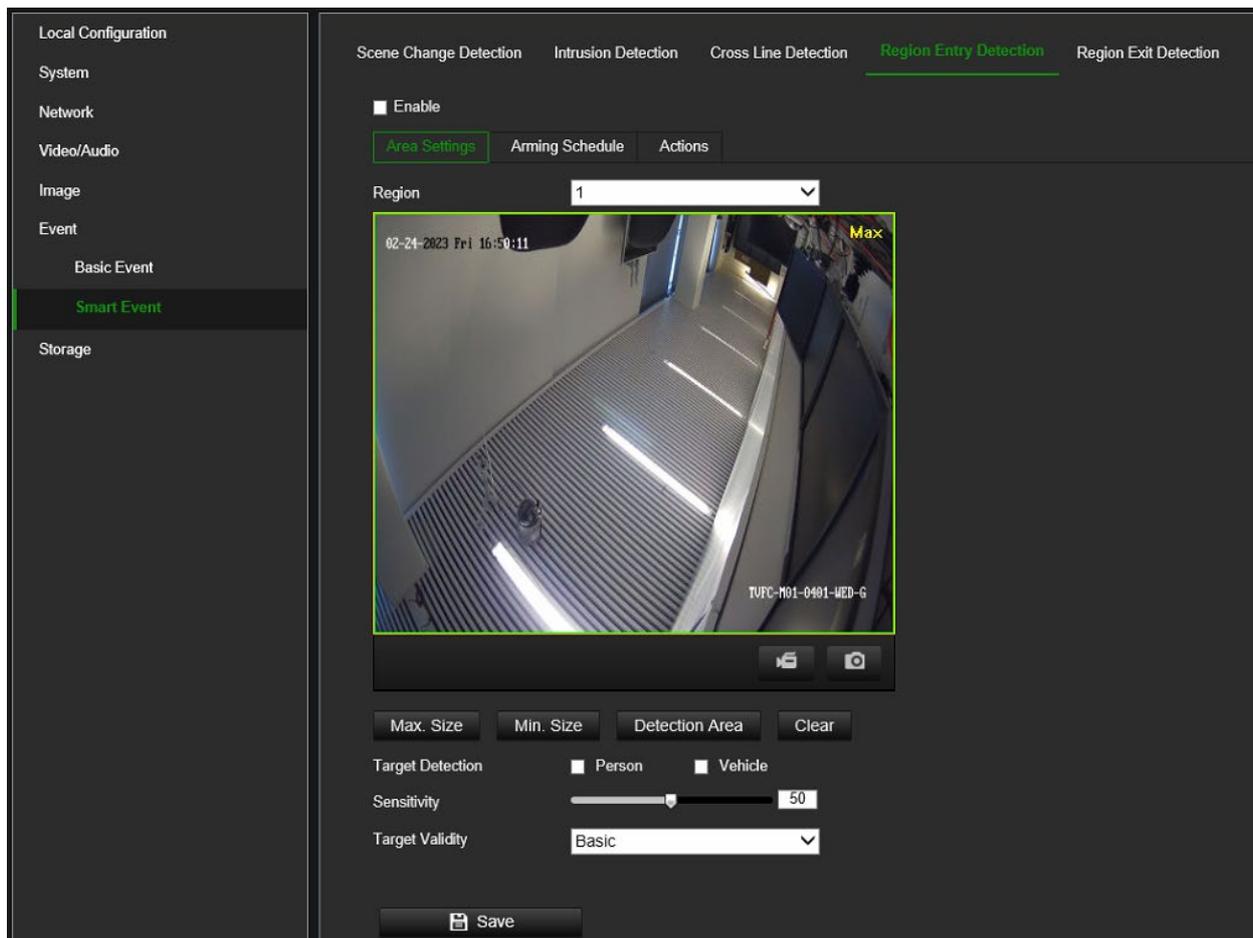
11. Click **Save** to save changes.

Region Entry Detection

This function detects people, vehicles, or other 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 > Smart Event > Region Entry Detection**.



2. Select the **Enable** check box to enable the function.
3. Click the **Area Settings** tab.
4. Under **Region**, select the desired region from the drop-down list for detection settings.
5. Click the **Detection Area** button to draw a detection area.
6. Click the live video viewer to specify the four vertexes of the detection region and release the mouse to complete drawing.
7. 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.

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.

8. Enable the options **Person and/or Vehicle** to have the camera react to people or vehicles. Selecting the person/vehicle options will result in fewer false intrusion detection events and will also exclude, for example, animals. If neither option is selected, the camera will react to all types of objects.
9. 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.

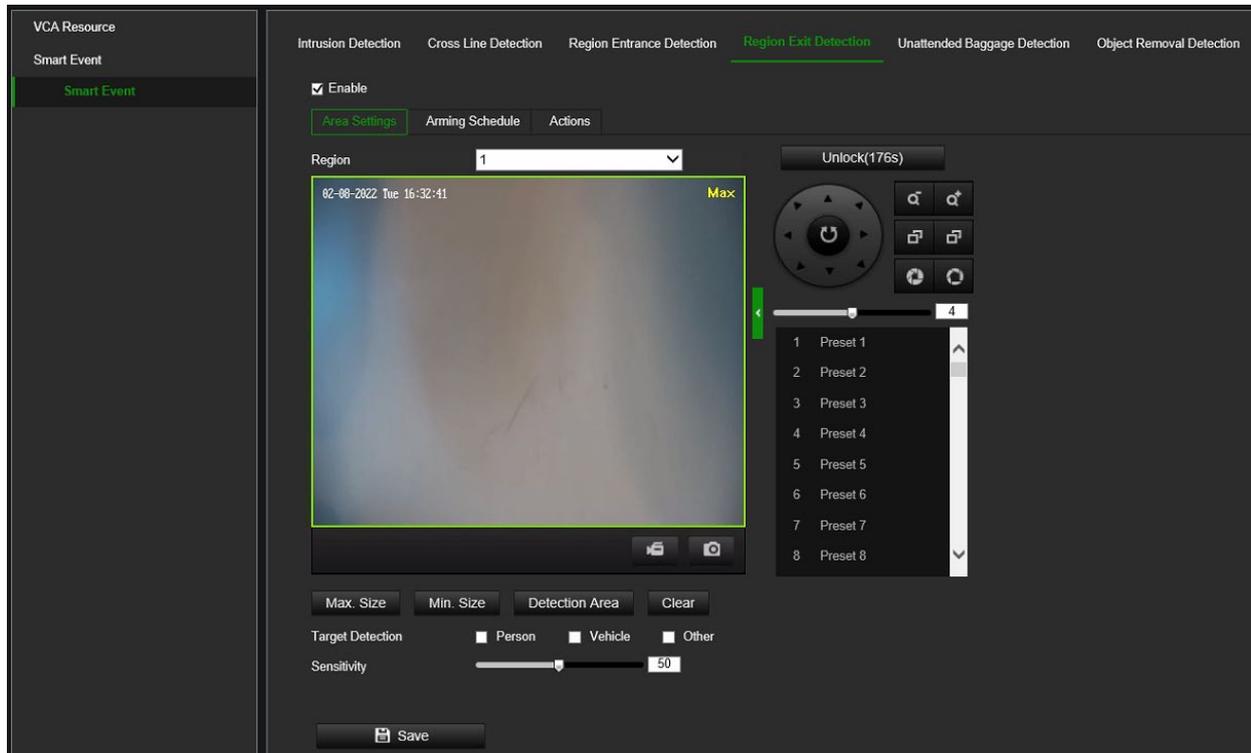
10. Repeat steps 4 to 9 to configure other regions. Up to four regions can be set. You can click the **Clear** button to clear all pre-defined regions.
11. Click the **Arming Schedule** tab to set the arming schedule.
12. Click the **Actions** tab to select the linkage methods.
13. Click **Save** to save the settings.

Region Exit Detection

This function detects people, vehicles, or 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 > Smart Event > Region Exiting Detection**.



2. Select the **Enable** check box to enable the function.
3. Click the **Area Settings** tab.
4. Under **Region**, select the desired region from the drop-down list for detection settings.
5. Click the **Detection Area** button to draw a detection area.
6. Click the live video viewer to draw the four vertexes of the detection region. Release the mouse to complete drawing.
7. 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.

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.
8. Enable the options **Person and/or Vehicle** to have the camera react to people or vehicles. Selecting the person/vehicle options will result in fewer false intrusion detection events and will also exclude, for example, animals. If neither option is selected, the camera will react to all types of objects.
9. 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-exiting action only when 40 percent of the target part enters the region.

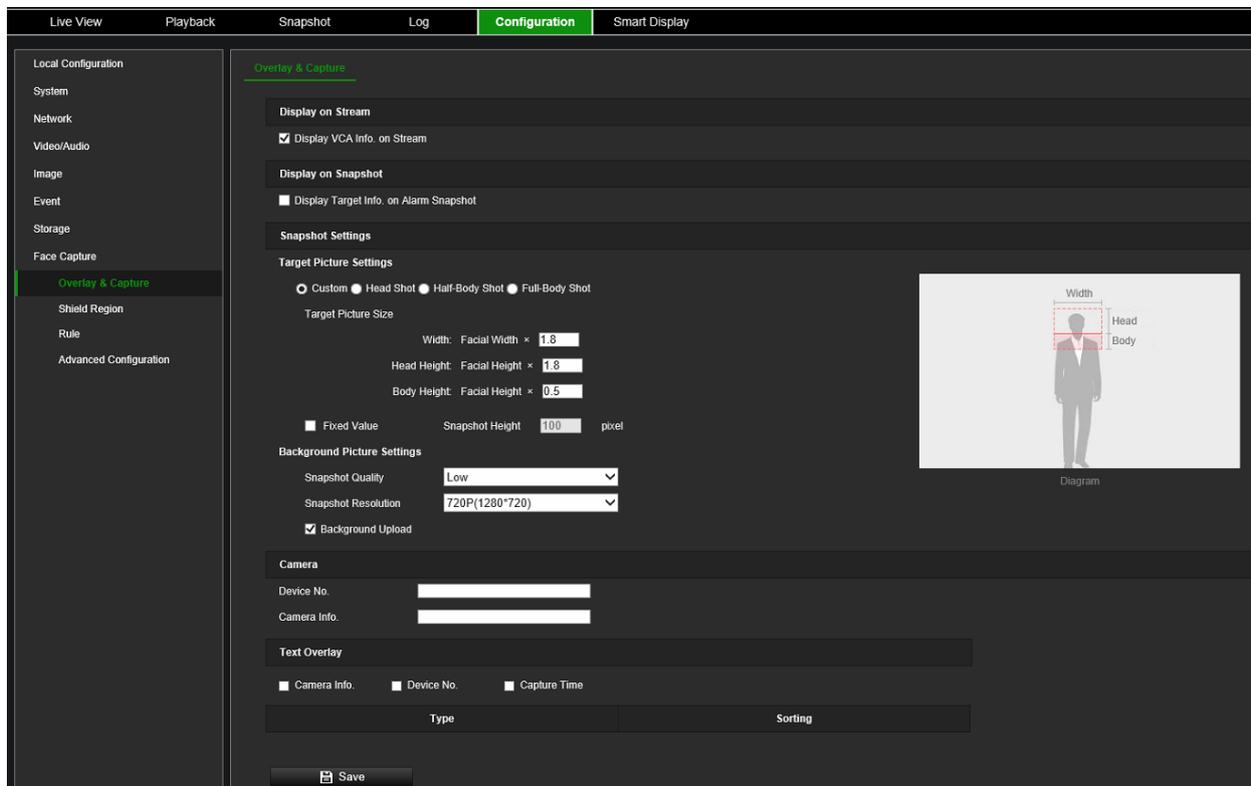
10. Repeat steps 4 to 9 to configure other regions. Up to four regions can be set. You can click the **Clear** button to clear all pre-defined regions.
11. Click the **Arming Schedule** tab to set the arming schedule.
12. Click the **Actions** tab to select the linkage methods.
13. Click **Save** to save the settings.

Face Capture

The face capture function can detect and capture faces in surveillance scenes. The face detection algorithm in the camera detects faces and can trigger actions such as storing snapshots, trigger recording, and other actions. A face capture rule must be set up to use this feature.

To set up Face Capture:

1. From the menu toolbar, click **Configuration > Face Capture**.



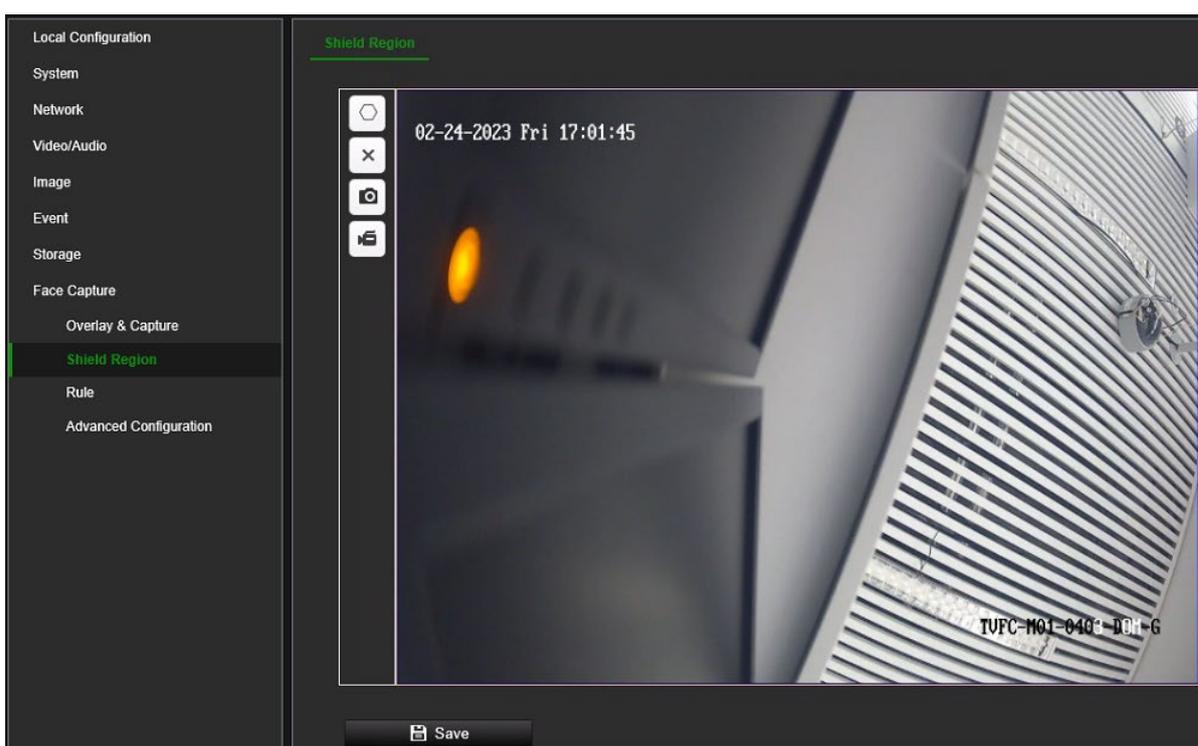
2. Select **Display VCA Info on Stream** and **Display Target Info on Alarm Snapshot** to add additional target and rules information to a stream or face capture snapshot.
3. Under **Target Picture Settings** set the face snapshot type by selecting **Custom**, **Head Shot**, **Half-Body Shot**, or **Full-Body Shot**. If you select *Custom*, you can define the desired snapshot width and height. If the captured snapshots always have the same snapshot height, enable **Fixed Value**, and enter the desired snapshot height.

4. Under **Background Picture Settings** set the background snapshot quality and resolution. If the background image needs to notify the alarm host, check **Background Upload**.
5. Under **Text Overlay** set how you want to display Device No., Camera Info. and Capture Time text on snapshots.
6. Click **Save** to save changes.

To set up a Shield Region:

1. A shield region can be used when you want to prevent the camera from taking face snapshots in a certain area in the camera field of view. When a shield area is defined, this area can still be viewed and recorded but no faces will be captured in that area.

From the menu toolbar, click **Configuration > Face Capture >Shield Region**.

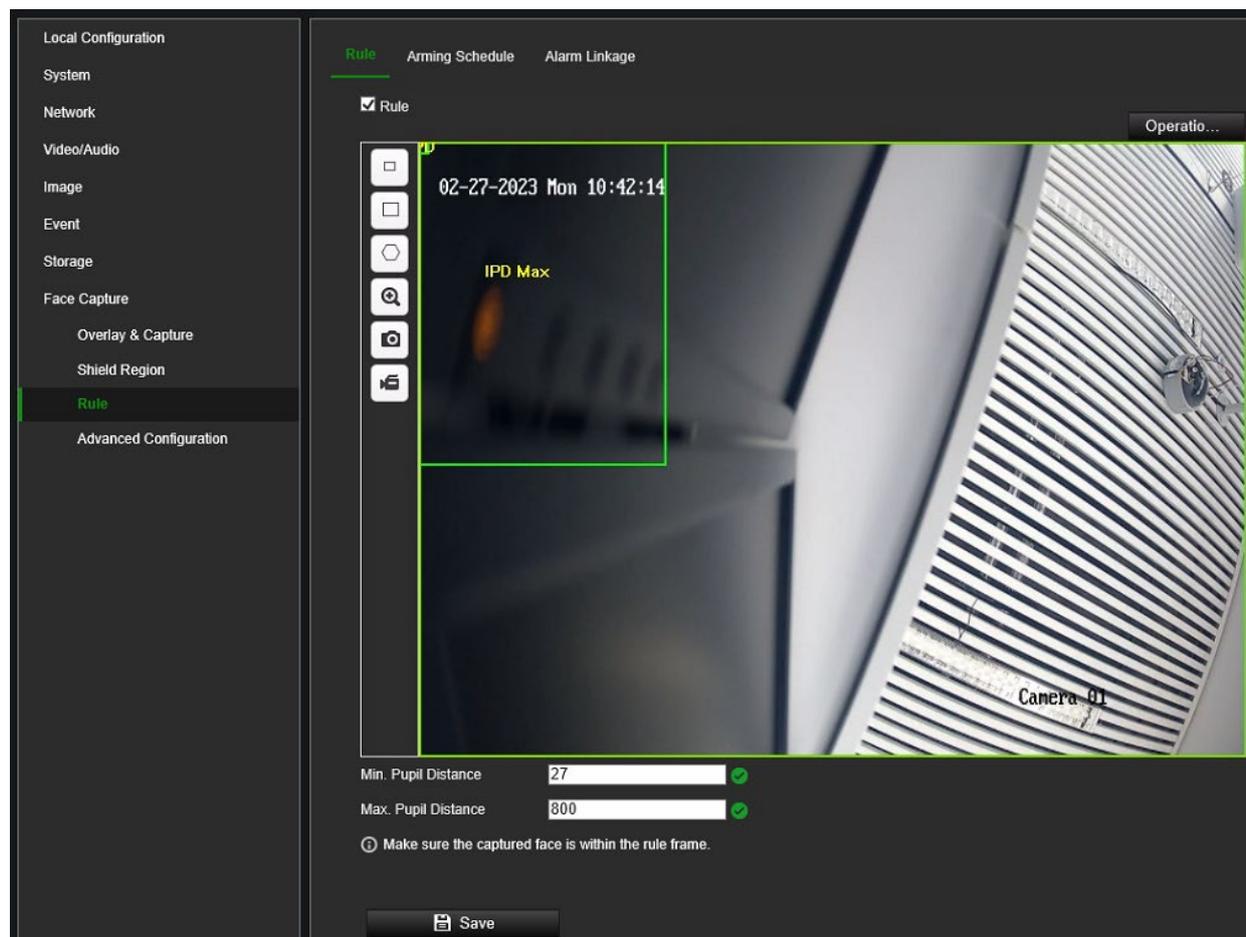


Button	Description
	Click the button and draw a polygon shield region in the image
	Click this button to delete an existing shield region
	Click this button to take a snapshot on your local PC
	Click this button to start live view recording on your local PC

2. Click **Save** to save changes.

To set up a Face Capture Rule:

Use the Face Capture Rule menu to define the area in which face snapshots can be taken (detection scene) and what actions are triggered when the event occurs.



1. From the menu toolbar, click **Configuration > Face Capture > Rule**.
2. Select the **Rule** check box to enable Face Capture
3. Set the minimum and maximum pupil distance. The closer people are to the camera, the larger the pupil distance between the eyes. You can test this by standing in front of the camera and measuring the pixels using the pixel counter on the live view webpage.

Minimum Pupil Distance: Enter a value between 27 and 806.

Maximum Pupil Distance: Enter a value between 27 and 16804.

5. Click the **Arming Schedule** tab and set up when you want Face Capture to be active.
6. Click the **Actions** tab to define the method by which you want the camera to notify you of events:

Normal Linkage

This is a group selection. It automatically selects “Send Email”, “Notify Alarm Recipient” and “Upload to FTP/NAS”.

Notify Alarm Recipient	Send an exception or alarm signal to remote management software when an event occurs.
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 79 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 32 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 73 for further information.</p>
Trigger Alarm Output	<p>Trigger the camera alarm output when an event occurs.</p> <p>Note: This option is only supported by cameras that support alarm output.</p>

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

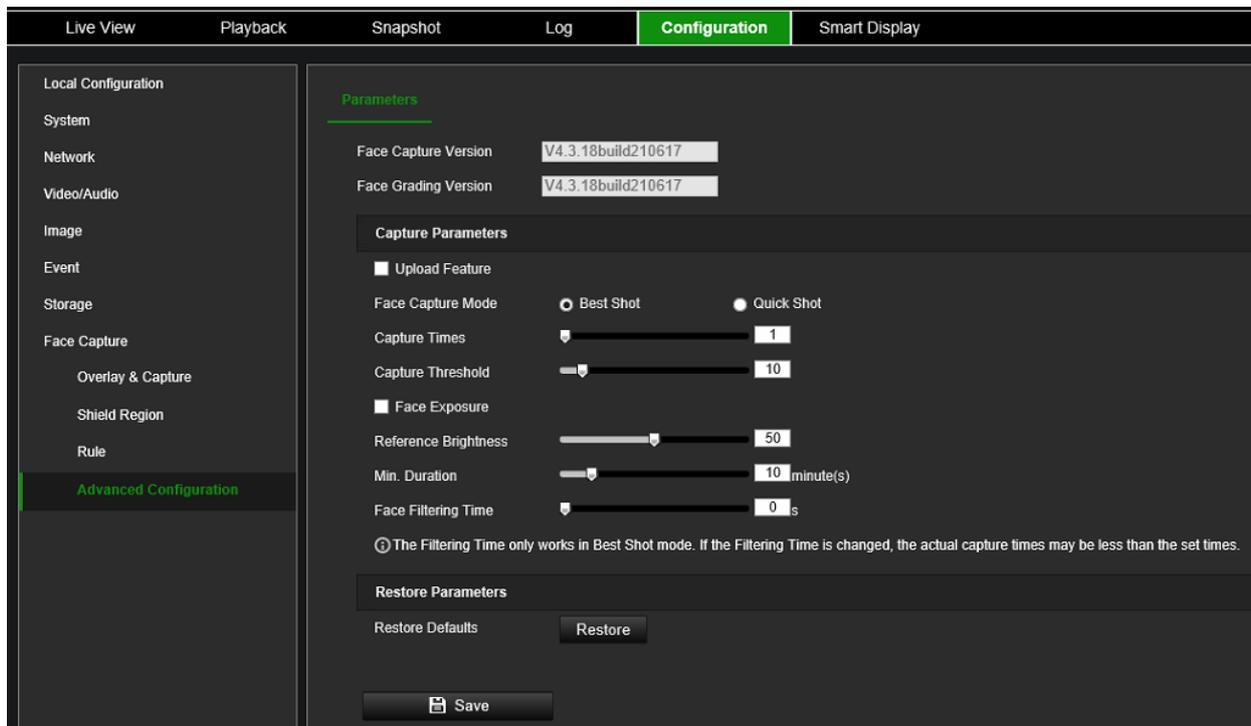
To set up Advanced Configuration:

This function is used to set up and optimize the parameters of the face capture algorithm. The parameters displayed will depend on which Face Capture Mode has been selected: Best Shot or Quick Shot.

Best Shot: The camera captures the target snapshot with the highest algorithm score after setting the parameters.

Quick Shot: The camera captures the target snapshot when the score of the captured face exceeds the *Quick Shot Threshold* during the *Max. Capture Interval*. If the score does not exceed the Quick Shot Threshold, the camera selects and uploads the snapshot with the highest score during the Max. Capture Interval.

1. From the menu toolbar, click **Configuration > Face Capture > Advanced Configuration**.
2. The **Face Capture Version** shows the current algorithm version in use.
3. Under **Face Capture Mode**, select **Best Shot**. and then select the desired capture parameters:



Capture Times	This is how often a face will be captured while in the detection area.
Capture Threshold	The level of face quality that triggers a face capture. A higher value means better face visibility is required to capture the face.
Similarity Threshold for Duplicate Removal	This is the similarity between the newly captured face snapshot and the snapshots in the duplicate removing library. When the similarity is higher than the value you set, the captured snapshot is regarded as a duplicated face and will be removed.
Reference Brightness	This is the reference brightness of a face in the face exposure mode. When a face is detected, the camera adjusts the face brightness according to the value that is set. The higher the value, the brighter the face will be.
Min. Duration	The minimum duration of the camera exposures the face. Note: When face exposure is enabled, the WDR function must be disabled.
Face Filtering Time	This is the time interval between the camera detecting a face and taking a capture action. If the detected face stays in the scene for less than the set filtering time, capture will not be triggered. For example, if the face filtering time is set as 5 seconds, the camera will capture the detected face when the face stays in the scene for 5 seconds. Note: The Filtering Time only works in Best Shot mode. When the filtering is changed, the actual Capture Times may be less than the value defined.

- Or -

Under **Face Capture Mode**, select **Quick Shot**. and then select the desired capture parameters.

Quick Shot Threshold	This is the level of the face quality that triggers a face capture. A higher value means better face visibility is required to capture the face.
Max. Capture Interval	This is the maximum time a person must be in the detection area for one quick shot of the face. Time is measured in seconds.
Capture Times	This is how often a face will be captured while in the detection area.

4. Select **Face Exposure** so that the camera automatically adjusts the exposure level when a face appears in the scene.
5. Adjust the **Reference Brightness** scale as required. This is the brightness of a face in face exposure mode. If a face in the actual scene is brighter than the set reference brightness, the device will lower the exposure level. If a face in the actual scene is darker than the set reference, the device will increase the exposure level.
6. Adjust the **Minimum Duration** scale as required. The extra time the device keeps the face exposure level after the face disappears from the scene.
7. Adjust the **Face Filtering Time** scale as required. This is the time interval between the camera detecting a face and taking a capture action. If the detected face stays in the scene for less than the set filtering time, capture will not be triggered. For example, if the face filtering time is set to 5 seconds, the camera will capture the detected face only when it stays in the scene for at least 5 seconds.
8. At any time during setup, you can restore all the Face Capture Advanced Configuration settings to factory default by clicking the **Restore** button.
9. Click **Save** to save changes.

Storage

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

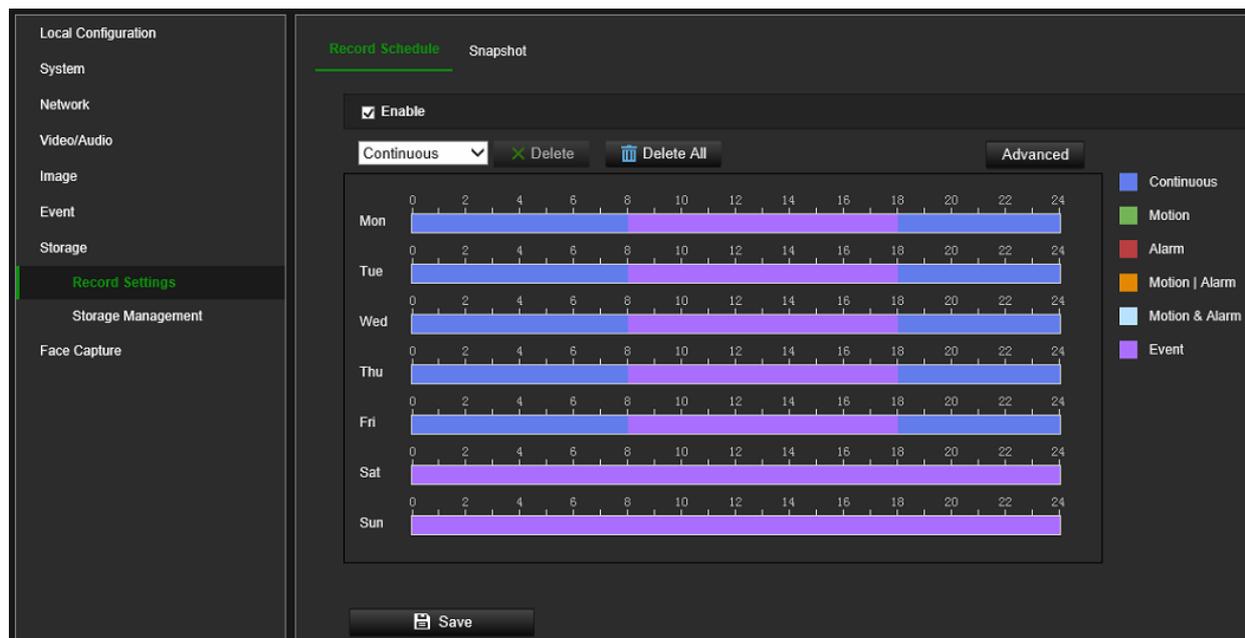
Record Settings

Configure recording and snapshot parameters in this menu.

You can define a recording schedule for the camera in the “Record Schedule” window (see Figure 8 on page 74). 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.

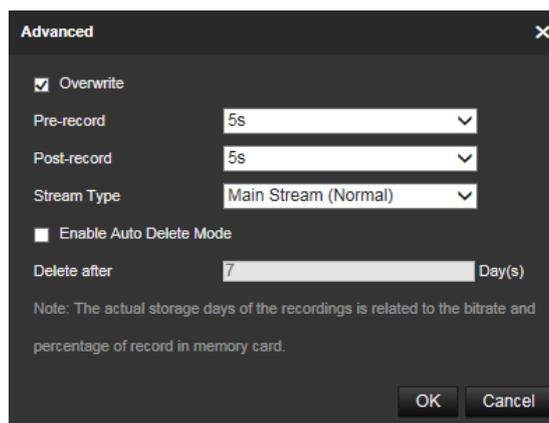
Different recording modes can be defined in the schedule.

Figure 8: Record schedule window



Click the **Advanced** button to open additional recording settings that 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 9: Record schedule - Advanced window



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.

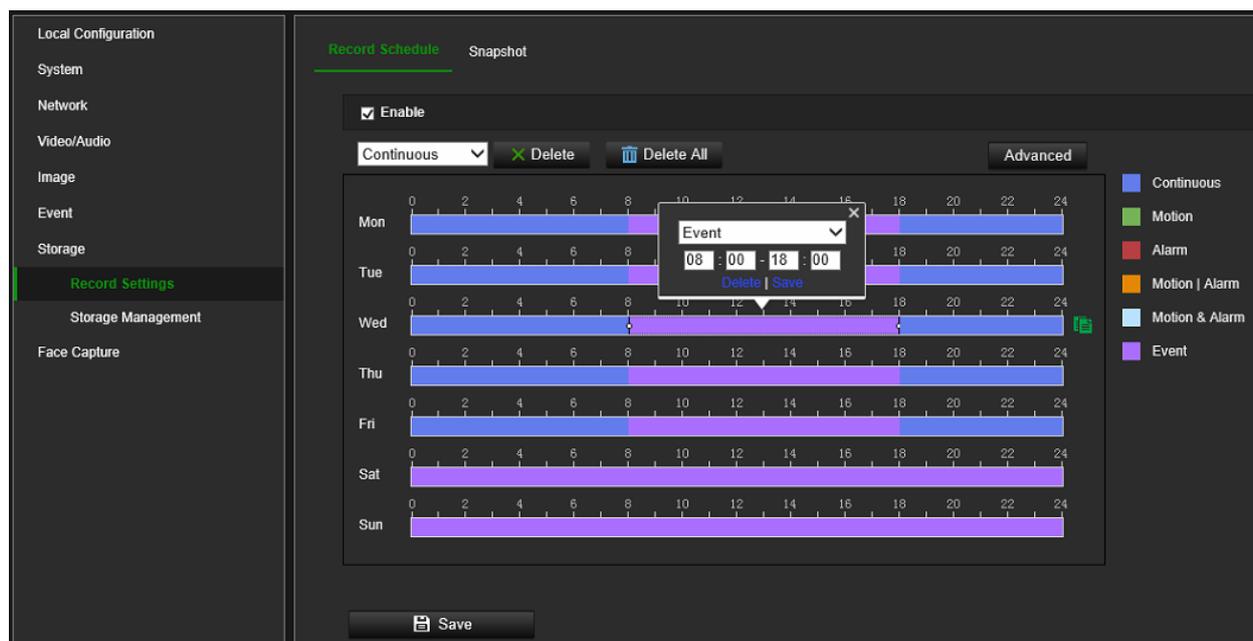
Enable Auto Delete Mode

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 > Record Settings > Record Schedule**.
2. Select the **Enable** check box to enable recording.
Note: To disable recording, disable the option.
3. Configure the recording schedule.

From the drop-down list, select 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 get the following pop-up window:



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:** 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 54.
 - **Motion | 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. For detailed information, please refer to the section on alarm inputs on page 54.

- **Motion & 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. For detailed information, please refer to the section on alarm inputs on page 54.
- **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. Click **OK**.

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

6. Click the **Advanced** button and set the desired pre- and post-record times stream type and auto-delete mode. Click **Save to save the changes** and return to the main recording schedule menu.
7. Click **Save** to save changes.

Note: If you set the record type to “Motion detection” or “Alarm”, you must define the arming schedule to trigger motion detection or alarm input recording. Some recording types such as motion might not be available depending on the selected VCA resource mode.

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.

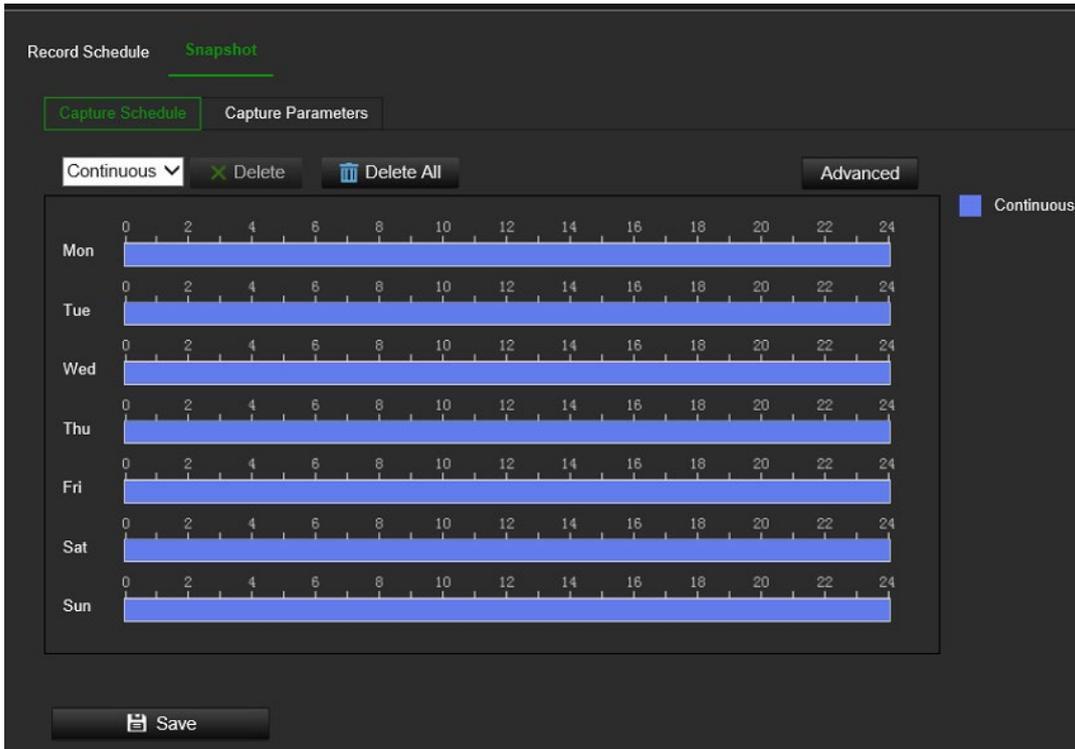
You must enable the option **Enable Timing Snapshot** if you want snapshots to be uploaded with a fixed interval to the FTP server. If you have configured the FTP settings and enabled **Upload Type** in the **Network > Advanced Settings > FTP** tab, the snapshots will not be uploaded to the FTP if the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

You must enable the option **Enable Event-Triggered Snapshot** if you want snapshots to be uploaded to the FTP and NAS when motion detection, VCA event, or an alarm input is triggered. If you have configured the FTP settings in **Network > Advanced Settings > FTP** and selected the action **Upload to FTP/Memory Card/NAS** for motion detection, VCA, or alarm input, the snapshots will be uploaded to the FTP server.

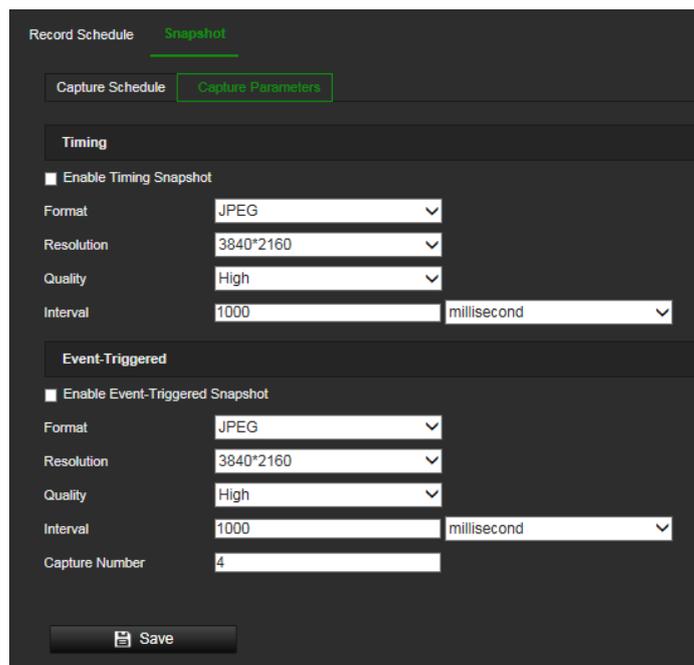
To set up continuous and event-triggered snapshots:

1. From the menu toolbar, click **Configuration > Storage > Record Settings > Snapshot > Capture 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. Click **Advanced** to select the stream type.
4. Select the **Capture Parameters** tab to configure the captured snapshot parameters.



5. In the *Timing* section, select the parameters for continuous snapshots:
 - a) Select the **Enable Timing Snapshot** check box.
 - b) Select the desired format of the snapshot. Default is JPEG.

- c) Select the desired resolution and quality of the snapshot.
- d) Enter the time interval between two snapshots. Select the unit of time from the drop-down list: milliseconds, seconds, minutes, hours, or days.

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

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

6. Under **Capture Number**, enter the total number of snapshots that can be taken.

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

Storage Management

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

HDD Management

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

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

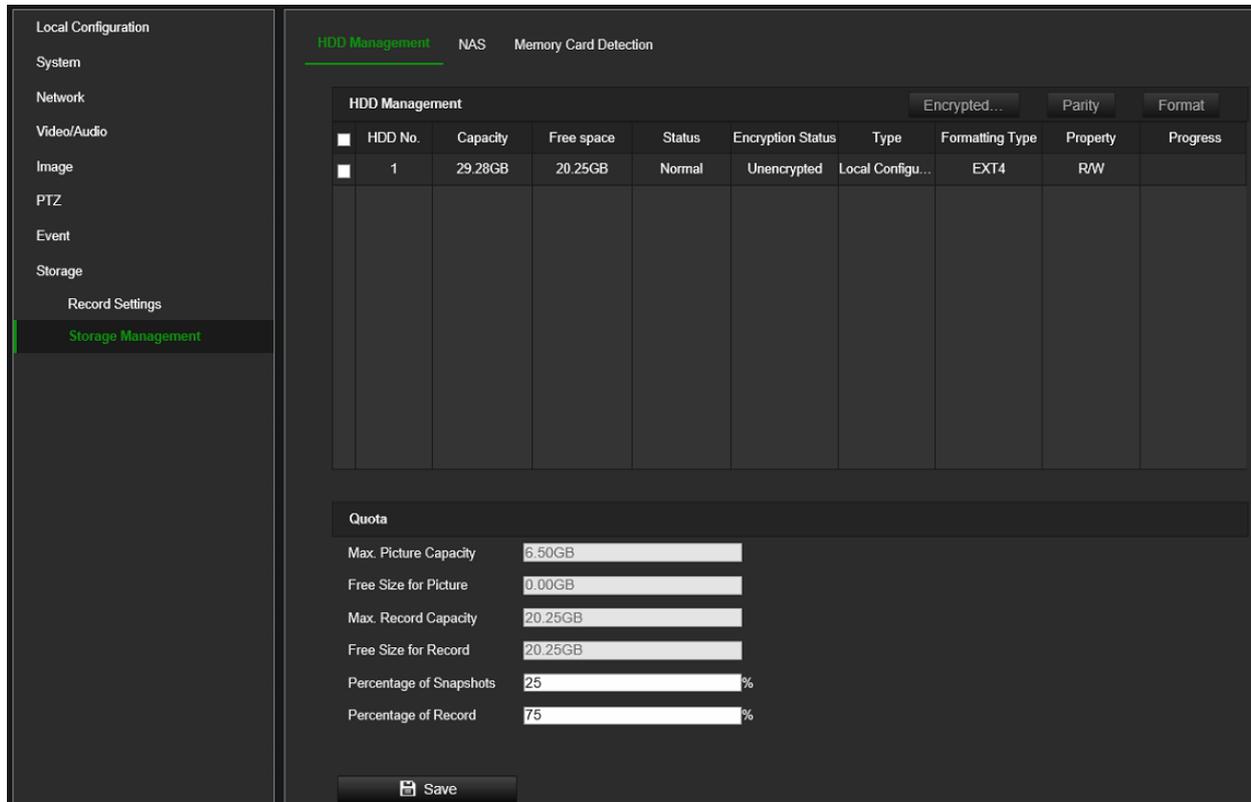
If overwrite is enabled, the oldest files are overwritten when the storage becomes full.

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

To set the quota storage for recordings and snapshots:

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

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.

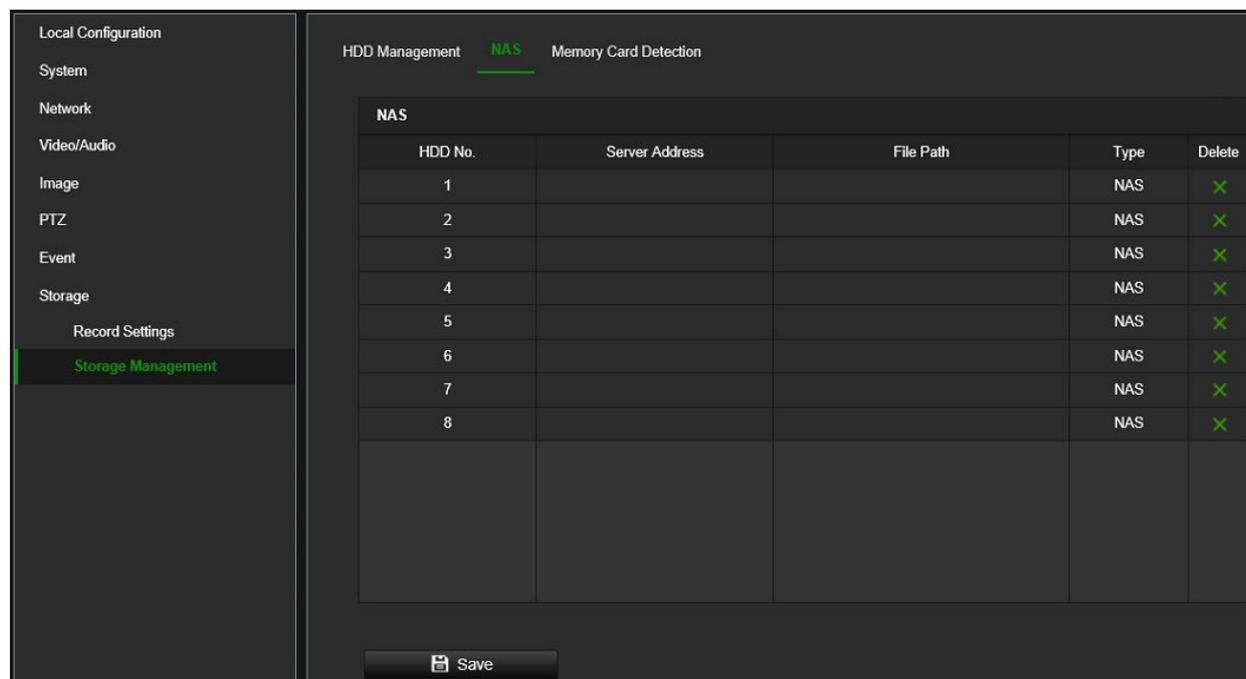
The NAS disk should be available within the network and correctly configured to store the recorded files, log files, etc.

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**.

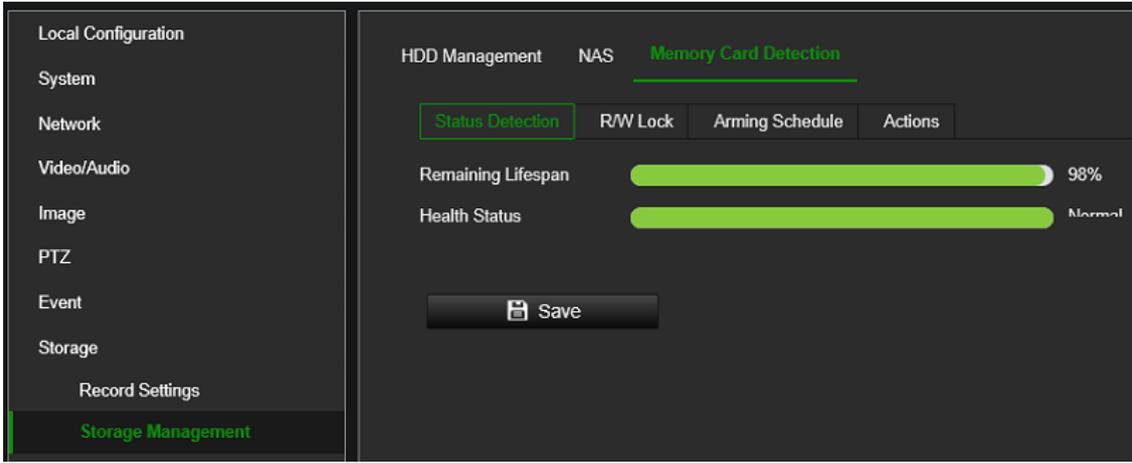


2. Enter the IP address of the network disk and the NAS folder path.
3. Click **Save** to save changes.

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.



Camera operation

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

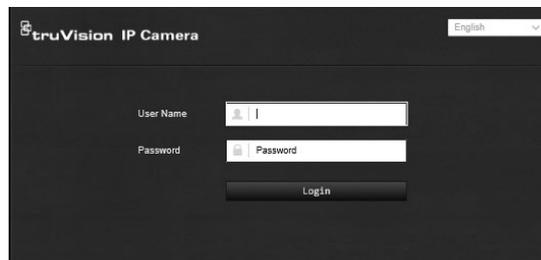
Login and Logout

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

Note: When an incorrect 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 **Configuration > System > Security > Security Service**.

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

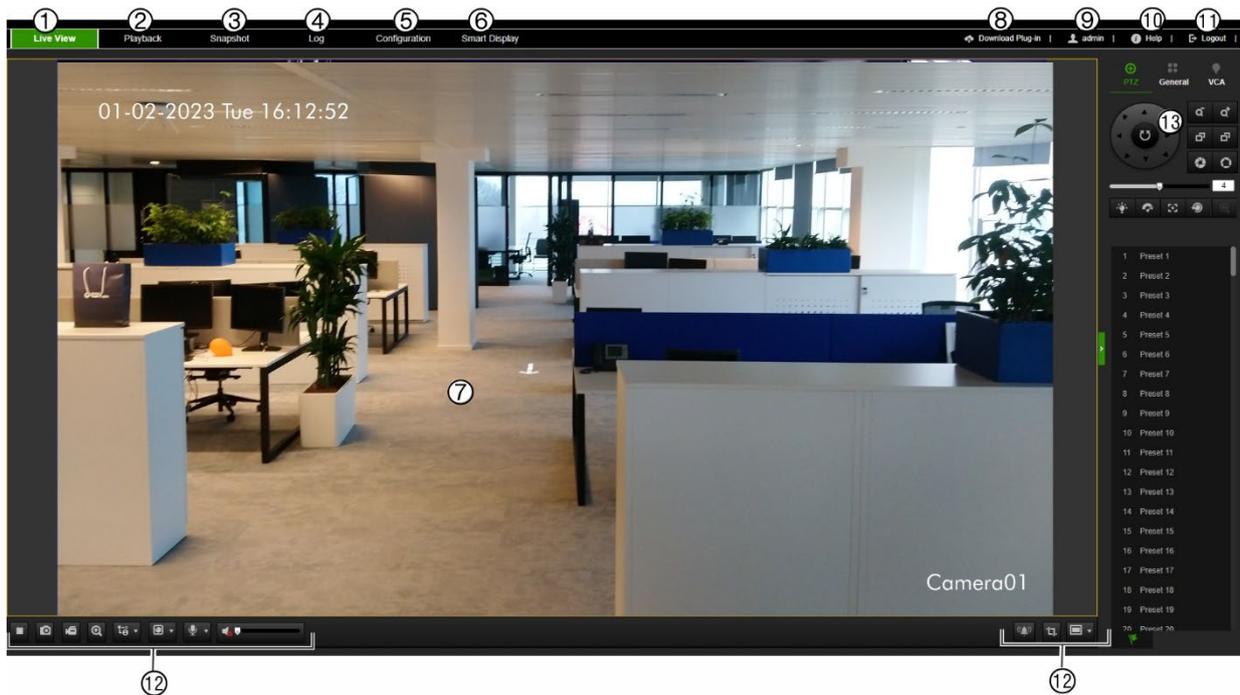
Figure 10: Login dialog box



Live view mode

Once logged in, click “Live View” on the menu toolbar to access live view mode. See Figure 11 on page 83 for the description of the interface.

Figure 11: Live view window



Name	Description
1. Live view	Click to view live video.
2. Playback	Click to play back video. See “Play back recorded video” on page 85 for more information.
3. Snapshot	Click to search snapshots . See “Snapshot” on page 87 for more information.
4. Log	Click to search for event logs. There are three main types: Alarm, Exception, and Operation. See “Log” on page 89 for more information.
5. Configuration	Click to display the configuration window for setting up the camera.
6. Smart Display	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 “Smart Display” on page 88 for further information.
7. Viewer	View live video. Time, date, and camera name are displayed here.
8. Download Plug-in	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.
9. Admin	Displays current user logged on.
10. Help	Click to find the function.
11. Logout	Click to log out from the system. This can be done at any time.
12. Live view toolbar	<p> Click to start/stop live view.</p> <p> Click to manually capture a snapshot.</p> <p> Click to manually start/stop recording. The recording is stored in the directory you have configured.</p> <p> Click to start/stop the digital zoom function.</p> <p> Live view with main stream, substream, or third stream.</p>

Name	Description
	Click to select the third-party plug-in. Not supported by all browsers.
	Turn on/off the microphone.
	Audio on/off and adjust volume/mute.
	Manual alarm
	Pixel counter
	Aspect ratio. Switch window size between 4:3, 16:9, original window size, original ratio, or self-adapt window size.

13. PTZ / General

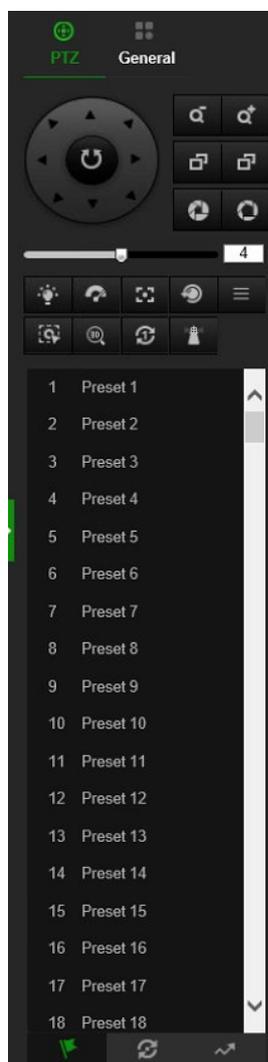
Configuration options for PTZ and General control panels. These options can be changed from the live view menu. See a description of the control panels below.

The PTZ panel lets you control the movement of the camera (see below) as well as call up pre-existing presets.

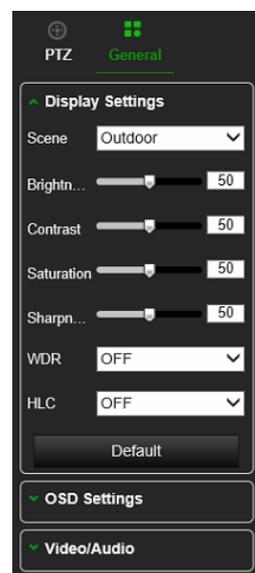
The user will need permission to use the PTZ control panel (see page 23).

Although you can modify the display, OSD, and video/audio settings from the General Control panel, you have greater control of these settings from the Configuration > Image menu.

PTZ control panel



General control panel



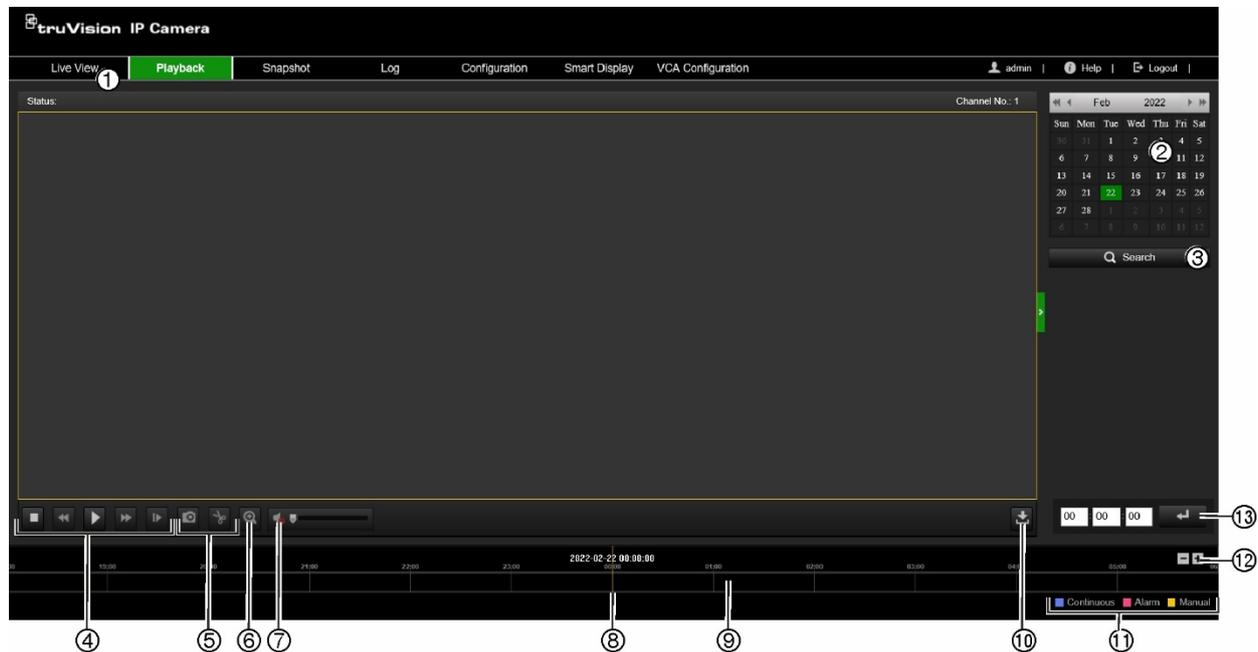
Play back recorded video

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

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

To search recorded video stored on the camera's storage device for playback, click **Playback** on the menu toolbar. The Playback window appears. See Figure 12 below.

Figure 12: Playback window



Name	Description
1. Playback button	Click to open the Playback window.
2. Search calendar	Click the day required to search.
3. Search	Start search.
4. Control playback	Click to control how the selected file is played back: play, stop, slow, and fast forward playback.
5. Archive functions	Click these buttons for the following archive actions:  Capture a snapshot image of the playback video.  Start/stop the video clip during playback. Sections of a recording are saved to a local computer folder.
6. Digital zoom	Zoom in and out of the selected camera image.
7. Audio control	Modify the audio level.
8. Timeline	The timeline moves from left (oldest video) to right (newest video). It shows where you are in the playback recording. The current time and date are also displayed.
9. Timeline bar	The timeline bar displays the 24-hour period of the day being played back. It moves from left (oldest) to right (newest). The bar is color-coded to display the type of recording.

Name	Description
10. Download functions	 Download video files.
11. Recording type	<p>The color code displays the recording type. Recording types are schedule recording, alarm recording, and manual recording.</p> <p>The recording type name is also displayed in the current status window.</p>
12. Zoom in/out	Click to zoom in or out of the timeline bar.
13. Jump start	Enter a precise time in the box and click  to jump start the playback from this selected time.

To play back recorded video

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

Note: You must have playback permission to play back recorded images. See “Assign permissions to the user” on page 23 to permit playback of recorded video files.

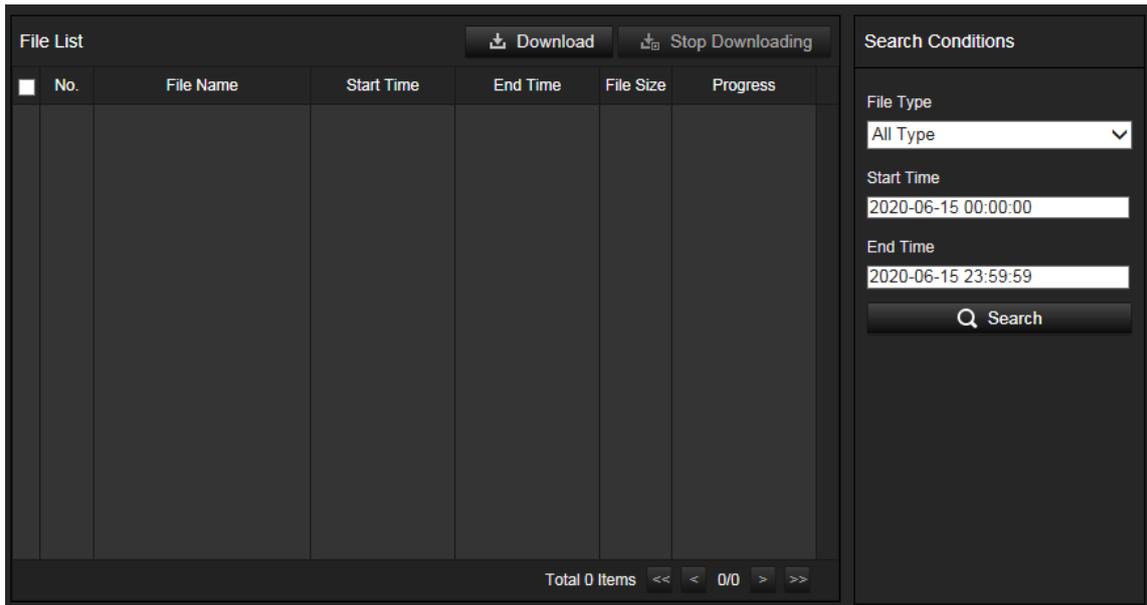
4. Select the date and click the **Search** button to search for the required recorded file.
5. Click **Search** to search the video file.
6. In the pop-up window, select the box of the video file and click  to download the video files.

To archive a recorded video segment during playback:

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

To archive recorded video files:

1. Click  to open the recorded file search window.



2. Select the file type and set the start and end times.
3. Click **Search** to search for the recorded video files.
4. Select the desired video files and click **Download** to download them. Downloading files from a NAS or SD card can take some time. A progress bar will be displayed to indicate the download progress.

Snapshot

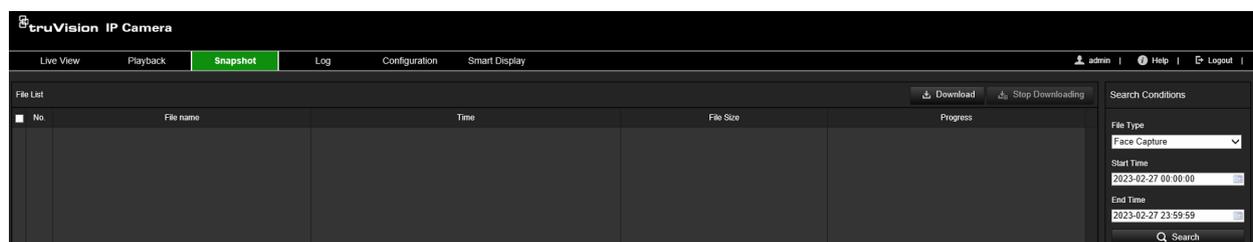
Click **Snapshot** on the menu toolbar to enter the window to search for snapshots. You can search, view, and download the snapshots stored in the NAS or memory card storage.

Notes:

- Make sure the HDD, NAS, or memory card is correctly configured before you process the snapshot search.
- To store snapshots, a capture schedule needs to be configured or the camera needs to be set up for Face Capture.

To search recorded snapshots:

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

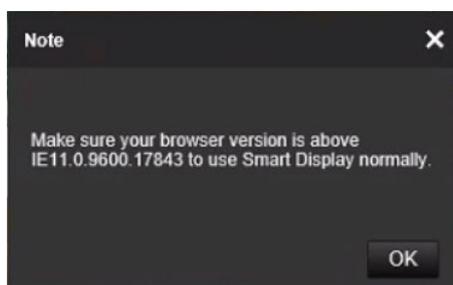


2. From the **File Type** drop-down list, select the file type for which you want to search: Continuous, Motion, Alarm, Face Capture, Cross Line Detection, Intrusion Detection, etc.
3. Select the start and end times.
4. Click **Search** to find the matching files.
5. In the list of snapshots, select the check box of the files you need and click **Download**.

Smart Display

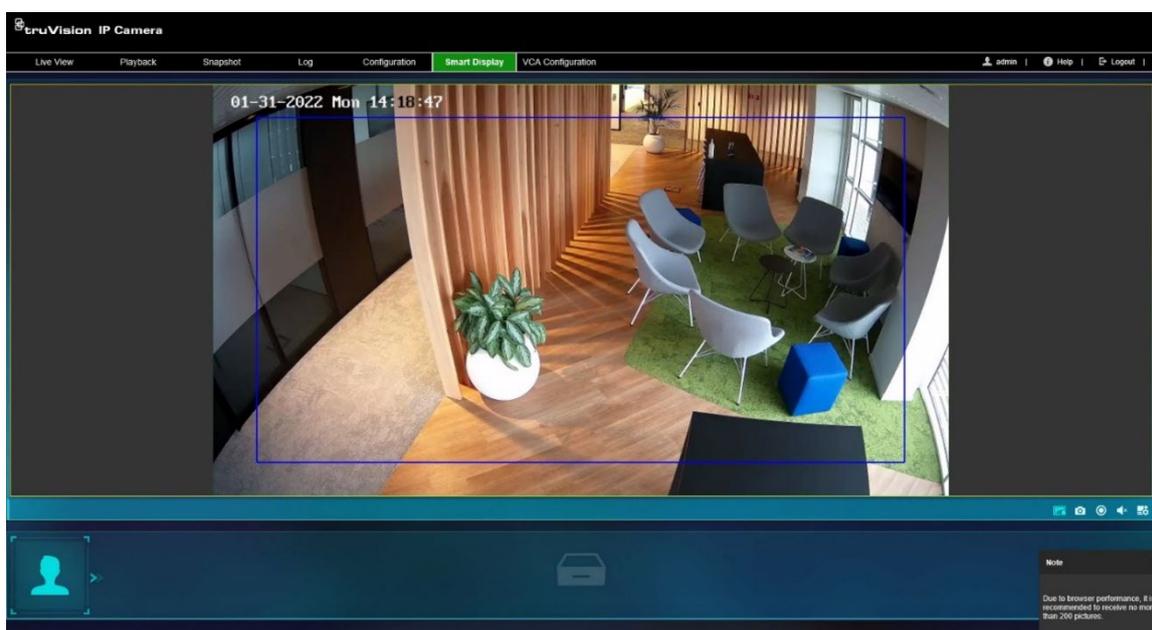
Use this menu to display captured snapshots (faces) in real time. The Smart Display menu only appears when Face Capture in VCA resource mode is enabled. See “VCA Resource” on page 13 on how to enable Face Capture.

This page works only in Internet Explorer version 11.0.9600.17843 and above. Each time you open Smart Display, a pop-up warning will appear to inform the user about the browser compatibility required for this feature.



To receive face snapshots in real-time:

1. From the menu toolbar, click **Smart Display**.



2. On the bottom right of the screen there are a set of buttons:

	Start/Stop saving face capture snapshots in the browser cache.
	Click to manually take a snapshot of the full image.
	Start/stop recording live stream on local PC.
	Mute audio.
	Configure the Smart Display layout.

3. Click the **Start/Stop**  button to send live captured face snapshots to the browser cache. When using this button, the browser will inform the user that, for browser performance reasons, a maximum of 200 snapshots can be sent to the browser cache.
4. Click  again to stop the real-time saving of snapshots to the browser cache and automatically download the captured snapshots from the browser cache to your local PC.
5. Use additional buttons for extra features, as required (see the table in step 2 above).

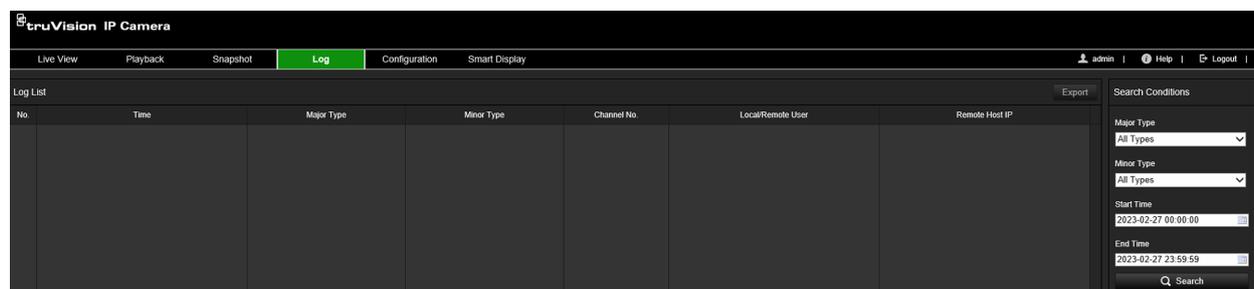
Log

You must configure 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 on a NAS or SD card depends on the capacity of the storage devices. When this capacity is reached, the system will start overwriting older logs. To view log events stored on storage devices, click **Log** on the menu toolbar to open the log menu.

Note: The user must have viewing log access rights to search and view logs. See “Assign permissions to the user” under “User Management” on page 23 to permit the user to search and view logs.

Figure 13: Log window



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

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

Minor Type: Each major type has some minor types which can help to refine your search. See Table 1 below for their descriptions.

Start Time and End Time: Set the 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, click **Log**.
2. In the **Major Type** and **Minor Type** drop-down list, select the desired options.
3. Set the start and end times of the log.
4. Click **Search** to start the search operation. The results appear in the left window.

Index

8

802.1x parameters
set up, 35

A

Alarm inputs, 54
set up, 57, 58
Alarm outputs
set up, 57, 58
Alarm outputs, 54
Archive files, 86, 87
Audio parameters, 38
Auto delete mode, 75

C

Camera image
set up, 41
Camera name
display, 44
Configuration file
import/export, 14
Configuration menu
overview, 9
Cross line detection, 63

D

D/N schedule
link to lighting scenes, 46
Date format set up, 44
Day/night switch setup, 43
DDNS parameters
set up, 26
Default settings
restore, 14
Detection
scene change, 59
Display information
set up, 44

E

Email parameters
set up, 33
Events
search logs, 89
Exception alarm, 55

F

Face capture, 13, 68
define rule, 70
optimize capture algorithm, 71
shield region, 69
Failed login lock, 17
Filtering time, 43

Firmware upgrade, 15
FTP parameters
set up, 32

H

Hard drive
capacity, 78
formatting, 78
HTTP listening parameters
set up, 37
HTTPS parameters
set up, 34

I

Image parameters switch, 46
Integration protocol parameters
set up, 36
Intrusion detection, 60

L

Language
change, 82
Live view auto logout, 17
Local configuration menu
overview, 8
Log on/off, 82
Logs
information type, 89
search, 89
security audit log, 21
viewing, 89

M

Motion detection
advanced mode, 51
normal mode, 49
Motion detection, 48
Multicast parameters
set up, 30

N

NAS management, 79
NAT parameters
set up, 29
Network service parameters
set up, 36
NTP synchronization, 11

P

Password activation, 3
Playback
play back recorded files, 86
screen, 85
searching recorded video, 85

- Plugin-free browsers, 5
- Port parameters
 - set up, 28
- Post-record times, 74
- PPPoE parameters
 - set up, 28
- Pre-record times, 74
- Privacy masks, 46

Q

- QoS parameters
 - set up, 34

R

- Reboot camera, 14
- Recording
 - parameters, 38
 - playback, 85
 - set up schedule, 73
- Region entry detection, 65
- Region exit detection, 66
- Region of interest
 - set up, 41
- Restart
 - schedule, 15

S

- SD card
 - capacity, 78
- SDHC card
 - format, 78
- Search
 - events, 89
 - logs, 89
- Security audit log, 21
- Shield region
 - block face snapshots, 69
- Smart display
 - face snapshots, 88
- Smart event, 13
- Snapshots
 - archive, 87
 - event-triggered snapshots, 76

- scheduled snapshots, 76
- search, 87
- SNMP parameters
 - set up, 31
- Standard event, 13
- Storage management, 78
- System time
 - set up, 11

T

- Tamper-proof alarms, 53
- TCP/IP parameters
 - set up, 25
- Time format set up, 44

U

- User management
 - add users, 22
 - delete users, 24
 - modify users, 24
 - online users, 24

V

- VCA configuration, 59
 - cross line detection, 63
 - face capture, 68
 - intrusion detection, 60
 - region entry detection, 65
 - region exit detection, 66
- VCA resources, 13
- Video clips
 - archive, 86
- Video parameters, 38
- Video quality, 41

W

- Web browser
 - interface overview, 7
- Web browser security level, 2
- White balance, 44