



User's Manual

A214, A426, A711, A826, A952, A953, Q83

2026/08/27



ACTi
Connecting Vision

Copyright

Copyright 2024. All rights reserved. No part of this manual may be copied, reproduced, translated, or distributed in any form or by any means without prior consent in writing from our company.

Trademark Acknowledgement

The manufacturer's trademarks and logos are the property of the manufacturer. Other trademarks, company names and product names contained in this manual are the property of their respective owners.

Disclaimer



CAUTION: The default password is used for your first login. To ensure account security, please change the password after your first login. You are recommended to set a strong password.

To the maximum extent permitted by applicable law, the product described, with its hardware, software, firmware and documents, is provided on an "as is" basis.

Best effort has been made to verify the integrity and correctness of the contents in this manual, but no statement, information, or recommendation in this manual shall constitute formal guarantee of any kind, expressed or implied. We shall not be held responsible for any technical or typographical errors in this manual. The contents of this manual are subject to change without prior notice. Update will be added to the new version of this manual.

Use of this manual and the subsequent result shall be entirely on the user's own responsibility. In no event shall we be liable to you for any special, consequential, incidental, or indirect damages, including, among others, damages for loss of business profits, business interruption, or loss of data or documentation in connection with the use of this product.

Video and audio surveillance can be regulated by laws that vary from country to country. Check the law in your local region before using this product for surveillance purposes. We shall not be held responsible for any consequences resulting from illegal operations of the device.

The illustrations in this manual are for reference only and may vary depending on the version or model. The screenshots in this manual may have been customized to meet specific requirements and user preferences. As a result, some of the examples and functions featured may differ from those displayed on your monitor.

This manual is a guide for multiple product models and so it is not intended for any specific

product.

Due to uncertainties such as physical environment, discrepancy may exist between the actual values and reference values provided in this manual. The ultimate right to interpretation resides in our company.

Environmental Protection

This product has been designed to comply with the requirements on environmental protection. For the proper storage, use and disposal of this product, national laws and regulations must be observed.

Symbols

The symbols in the following table may be found in this manual. Carefully follow the instructions indicated by the symbols to avoid hazardous situations and use the product properly.

Symbol	Description
WARNING	Indicates a hazardous situation which, if not avoided, could result in bodily injury or death.
CAUTION	Indicates a situation which, if not avoided, could result in damage, data loss or malfunction to product.
NOTE	Indicates useful or supplemental information about the use of product.

Table of Contents

Copyright.....	2
Trademark Acknowledgement.....	2
Disclaimer	2
Environmental Protection	3
Overview	7
Key Features	7
Installation	8
Recommendation for Camera Installation.....	8
Scene Requirement.....	9
Home Page	11
Main Menu	12
Functions on the Home Page	13
System Settings	18
System	18
Security	19
User	19
HTTPS	21
IP Filter	22
IEEE 802.1X	23
Network	24
Basic	24
QoS	26
VLAN	26
UPnP	28
DDNS	28
Mail	28
FTP	29
HTTP	29
Events (Alarm Settings).....	30
Application	30
Motion Detection	32

Network Failure Detection	36
Tampering	37
Periodical Event	39
Manual Trigger	40
Audio Detection	42
Video Analytics Standard Setting	44
Storage Management	49
SD Card	49
Network Share (NAS)	50
Recording	52
Schedule	53
File Location (Snapshots and Web Recording)	54

Built-in Video Analytics 55

Abandoned Object (Unattended Object Detection)	56
Installation Requirement	56
Scene Requirement	56
Configuration	57
Intrusion Detection	59
Installation Requirement	59
Scene Requirement	59
Configuration	60
Camera Sabotage	61
Installation Requirement	61
Scene Requirement	61
Configuration	61
Wrong Direction	62
Installation and Configuration Requirements	62
Scene Requirement	62
Configuration	62
Loitering Detection	63
Installation and Configuration Requirements	63
Scene Requirement	63
Configuration	64
Object Counting	65
Installation and Configuration Requirement	65
Scene Requirement	65
Configuration	66
Object Removal	67
Installation and Configuration Requirement	67
Scene Requirement	67

Configuration 68

Stopped Vehicle 69

 Installation and Configuration Requirement 69

 Scene Requirement 69

 Configuration 69

Automatic License Plate Recognition (ALPR) 72

Overview

Video Analytics (VA) provides an intelligent detection system for network surveillance cameras. With advanced image processing algorithms, especially for people or vehicle counting, it is an optimal solution for a variety of applications, such as moving object recognition and tracking. Besides, the diversity of VA functions offers thorough monitoring almost in any kind of circumstances or environment.

Key Features

- Abandoned Object
- Intrusion Detection
- Camera Sabotage
- Wrong Direction
- Loitering Detection
- Object Counting
- Object Removal
- Stopped Vehicle
- Face Detection
- Face Recognition
- License Plate Recognition

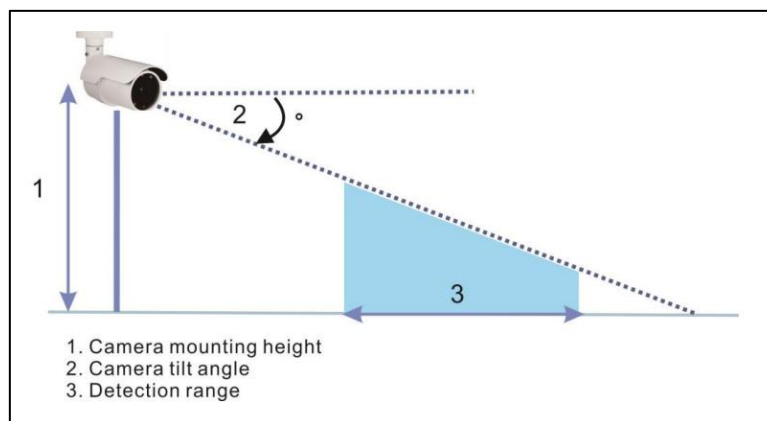
Availability of these features vary depending on the camera model.

Installation

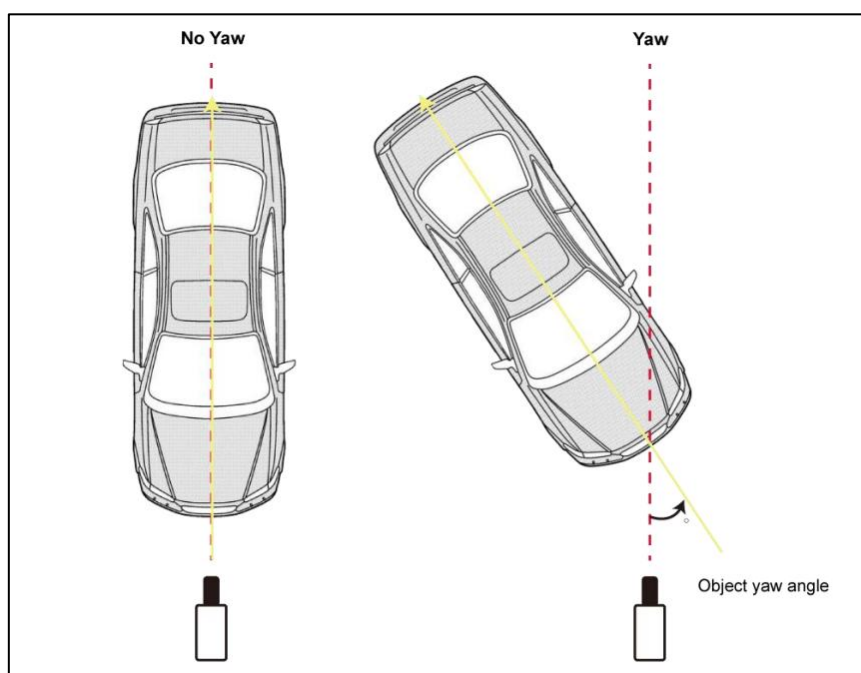
Recommendation for Camera Installation

Below are the following factors that must be considered when installing the camera to be used for video analytics.

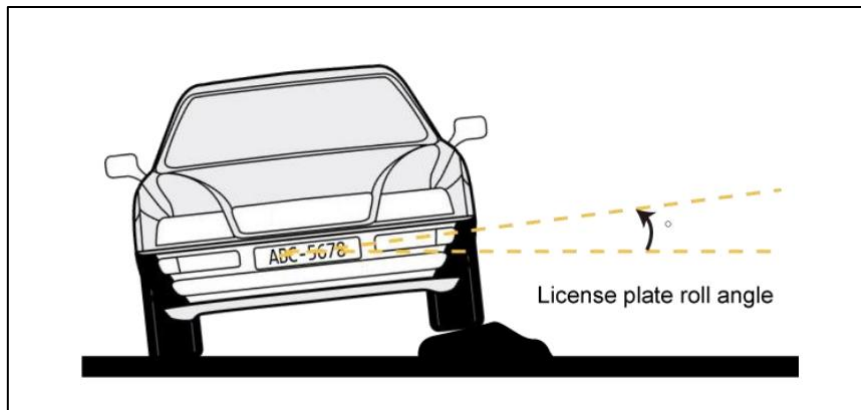
- **Target Size:** The suggested target size that can be detected
- **Effective field of view:** Due to the possibility of lens distortion, it is suggested to set the detection zone within the FOV
- **Camera mounting height:** The suggested mounting height for camera
- **Detection range:** The detectable distance range between camera and target object
- **Camera tilt angle:** The included angle between camera and ceiling



- **Object yaw angle:** The angle between the camera direction and the direction where the object is facing.



Roll angle: Rotation angle of the object



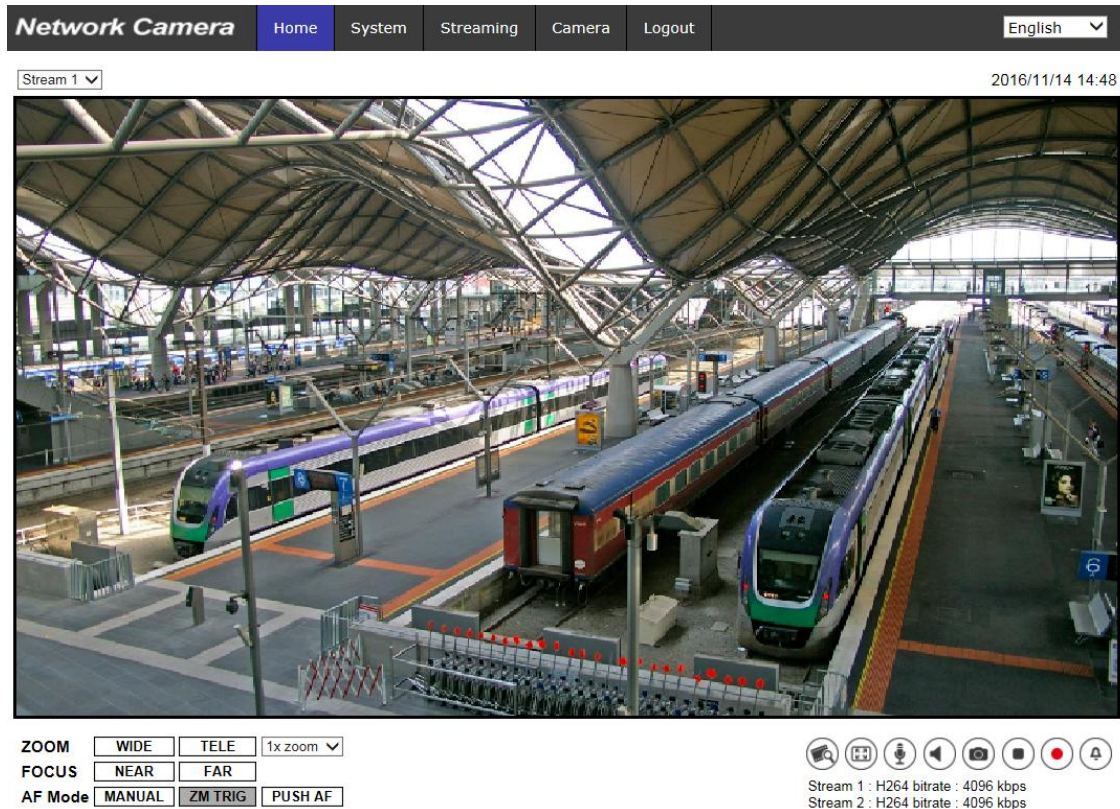
Scene Requirement

- Keep the camera lens clean and free from rain and water drops. Protect the camera from condensation.
- Position the camera in a place where the scene will not cause any reflection.
- To eliminate camera shake, the camera must be placed and installed in a sturdy and secured location, e.g., on a pole. Incorrect camera installation may cause poor camera performance.
- The distinction of the target object from the background must be clear and obvious, e.g., color and texture. The color and texture of the target object must not be similar to the background.
- Good video analytics performance requires steady and sufficient illumination.
- With the installation of external illuminators, low light conditions can be avoided, and the target object can be distinguished under both natural and artificial lighting conditions. Note that the effect of shadow should be considered when planning the illumination. For the best performance, white light mode is preferable compared to IR mode.
- Avoid backlight scenes and unexpected light sources (e.g., from vehicles, streetlights) projecting in the detection zone.
- Make sure that the target object can be seen clearly, and there are no obstructions, e.g., trees, pillars, buildings and furniture.
- Poor camera performance may occur if there are clouds, fog or other moving objects with similar appearance to the target object in the detection zone.
- Bad weather conditions, e.g. heavy rain, fog or snow, might affect and reduce detection range and accuracy.
- It is suggested to turn on WDR function in high dynamic range scene for sufficient image details.
- To improve the camera performance, turn on noise reduction to prevent the image from flickering noise and artifacts.
- As long as the target object does not move fast, the following functions of PTZ cameras that can work properly when the camera is moving (pan/ tilt) are LPR, Face Detection and

Face Recognition. Once the PTZ camera moves (pan/tilt), the configuration of the detection zone in the original scene might not be applicable to the new scene. The configuration of the detection zone in the new scene should be reconfigured.

Home Page

Click the **Home** tab to access the **Home** page. The available functions are described in the following sections.



NOTE: The function buttons on the Home page will vary according to different camera models.

Below is an example of the Function Buttons on the Home page of A951 model.



Main Menu

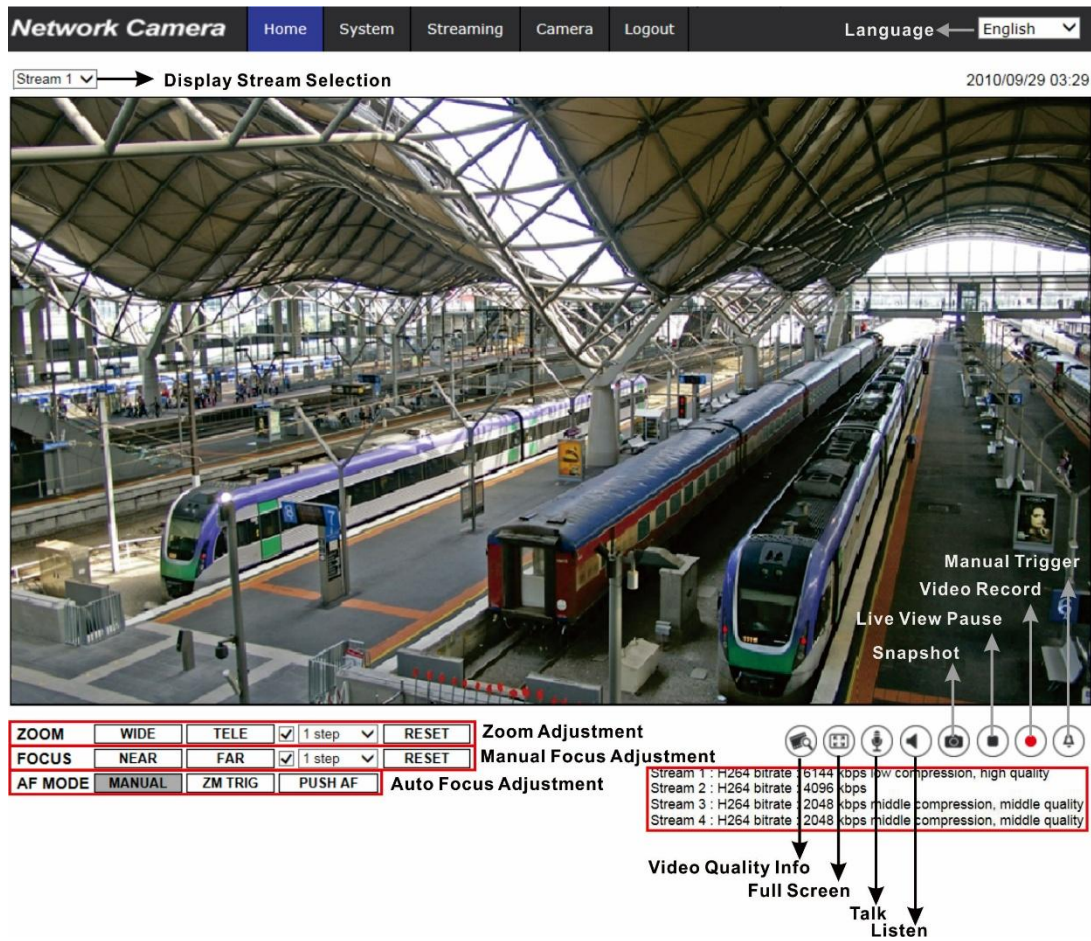
The **Main Menu** is the primary navigation area of the camera's web interface. It provides access to the camera's main functions and configuration settings. Depending on the user account and camera model, the available menu options may vary.

The main menu includes the following sections:

- **Home:** View and monitor the camera's live video.
- **System Setting:** Configure system-related settings such as the host name, date and time, password, network, and other system parameters.
- **Streaming Setting:** Configure video and audio streaming parameters, including video format, compression, frame rate, and related protocols.
- **Camera Setting:** Adjust image and camera parameters such as exposure, white balance, sharpness, noise reduction, digital zoom, WDR, and other image-related functions.
- **Pan Tilt Setting:** Configure preset points, sequence lines, and pan/tilt-related functions for supported cameras.
- **Logout:** Log out of the current user account and return to the login page.

NOTE: The functions and menu items displayed may differ depending on the camera model, firmware version, and user privileges.

Functions on the Home Page



Zoom Adjustment	
ZOOM	WIDE TELE ☒ 1 step RESET
Manual Focus Adjustment	
FOCUS	NEAR FAR ☒ 1 step RESET
Auto Focus Adjustment	
AF MODE	MANUAL ZM TRIG PUSH AF

Video Quality Info	
Stream 1 : H264 bitrate	6144 kbps low compression, high quality
Stream 2 : H264 bitrate	4096 kbps
Stream 3 : H264 bitrate	2048 kbps middle compression, middle quality
Stream 4 : H264 bitrate	2048 kbps middle compression, middle quality

Full Screen
Talk
Listen

Multiple Languages Support

The web interface supports multiple languages, including German, English, Spanish, French, Italian, Japanese, Portuguese, Russian, Simplified Chinese and Traditional Chinese for the viewer window interface.

Display Stream Selection

Select the desired stream from the drop-down menu.

Camera Info

Double-click the **Live View** pane to open the **Camera Info** window and view basic camera information, such as the **IP address**, **network status**, and **video format**.

Digital Zoom Control

In **full-screen mode**, scroll the mouse wheel to **zoom in or out**. Click and drag the mouse to move the viewing area.

PTZ Controls

Click to show / hide the PTZ control panel.

Video Quality

Click to show/hide the video quality information including bitrate and compression.

Full Screen

Click to adjust image display to full screen. Alternatively, click on the Live Video pane and select **Fullscreen** to resize to full screen. To exit full screen mode, press **Esc** on the keyboard, or double-click on the Live Video pane or right-click on the Live Video pane and select **Normal view**.

Talk

The **Talk** function enables communication from the local site to the remote site. Click the **Talk** button to turn the function **On** or **Off**. To enable the Talk function, users must first select the appropriate transmission mode under **Streaming > Audio**

Listen

Click **Listen** to mute or unmute the audio. Select the appropriate **Transmission Mode** under **Streaming > Audio** to enable this function.

NOTE: **Talk** and **Listen** are available only to users with the required privileges. See **Security > Add User > Talk/Listen** for details.

Snapshot

Click the **Snapshot** button to save a JPEG snapshot to the designated location. The default save location is **C:**. To change the location, see **File Location** for more details.

NOTE: On Windows, run Internet Explorer as an administrator to use the Snapshot function. Right-click the IE icon and select **Run as administrator**.

Live View Pause / Restart

Click **Pause** to stop video streaming. The live video will appear black. Click **Restart** to resume live video.

Web Recording

Click **Record** to record the Live View to the local hard drive. The default save location is **C:**. To change the location, see **File Location** for details.

NOTE: On Windows, run Internet Explorer as an administrator to use Web Recording. Right-click the IE icon and select **Run as administrator**.

Manual Trigger

Click **Manual Trigger** to turn the manual trigger **On** or **Off**. For details, see **Manual Trigger** in the next chapter.

Wiper (Available on select models only)

Click **Wiper** to manually swipe the wiper on the lens glass.

Seamline (Available on select models only)

Click **Seamline** to reset the camera's stitching line.

NOTE: The minimum stitching distance is **450 cm**. Avoid placing objects too close to the camera or across the stitching line.

Zoom Adjustment

- **Wide / Tele** (Zoom lens only)
Press and hold **WIDE / TELE** to continuously adjust the zoom. You can also use the mouse wheel over the Live View to zoom in or out in **Normal View** mode.
- **Wide / Tele Step** ☒ 1 step 
Select a **Wide / Tele** step value from the drop-down menu to adjust the zoom by the selected increment.
- **Reset Button**
Click **Reset** to calibrate the zoom lens to the maximum wide-angle position.

Manual Focus Adjustment

- **Near / Far**
Press and hold **Near / Far** to continuously adjust the focus.
- **Near / Far Steps (Available on select models only)**
Select a **Tele / Wide** step value from the drop-down menu to adjust the focus by the selected increment.
- **Reset (Available on select models only)**
Click **Reset** to reset the focus to the maximum near position, then automatically calibrate it for the monitoring environment.

- **Lock (Available on select models only)**
Click **Lock** to lock the ABF function after autofocus is adjusted. Click again to unlock it and allow focus adjustment.
- **Precise AF** ☒ **Precise AF** (Available on select models only)
Enable **Precise AF** for precise focus adjustment and to help prevent the camera from going out of focus. Enable this option before clicking **PUSH AF**.

Lock ABF Function (Available on select models only)

Use **Lock ABF** to prevent the camera from losing focus after being moved or accidentally adjusted locally or remotely via an NVR.

Follow these steps to achieve optimal focus:

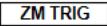
Step 1: After powering on the camera, click **Reset**.

Step 2: Manually adjust the lens to the desired zoom and approximate focus position.

Step 3: Select **Precise AF** and click **Push AF**.

Step 4: Click **Lock** to lock the current focus position.

Auto Focus (AF) Adjustment (Available on select models only)

- **Manual Button**
Click **Manual** to enable manual focus adjustment using the **<Near / Far>** buttons.
- **Zoom Trigger AF** 
In this mode, autofocus (AF) is activated automatically whenever zoom is adjusted.
- **Push AF Button**
Click **Push AF** to perform a one-push autofocus adjustment.

Fisheye Image Adjustment (For Fisheye camera models only)

Fisheye adjustment icons appear only when **Fisheye Dewarping Type** is set to **Back End Dewarping** under **Camera > Fisheye Setting**.

- **Overview** 
Click **Overview** to view the live video without dewarping.
- **Single ePTZ** 
Click **Single ePTZ** to view dewarped live video and perform virtual pan, tilt, and zoom. Scroll the mouse wheel to zoom in or out, and drag the mouse to change the viewing direction.
- **360° Panoramic** 
Click **360° Panoramic** to view the dewarped live video as two 180° views. Suitable for ceiling-

mounted cameras only.

- **4PTZ (Quad View)**

Click **4PTZ** to view the dewarped live video as four ePTZ views. Suitable for wall-mounted cameras only.

- **180° Panoramic**

Click **180° Panoramic** to view the dewarped live video as a single 180° view. Suitable for wall-mounted cameras only.

- **180° Dual ePTZ**

Click **180° Dual ePTZ** to view the dewarped live video as a single 180° view with two ePTZ views. Scroll the mouse wheel to zoom in or out, and drag the mouse within an ePTZ pane to change the viewing direction. Suitable for wall-mounted cameras only.

System Settings

The System Settings can be accessed through the following path: **System > System**.

System

This page allows the administrator to configure basic system information and time-related settings for the camera.

Host Name

The **Host Name** is used to identify the camera on the network and within the system. If the **Alarm** function is enabled and configured to send alarm notifications via **Mail** or **FTP**, the host name entered here will be included in the alarm message for camera identification.

Time Zone

Select the appropriate **Time Zone** from the drop-down menu according to the camera's physical location. The selected time zone is used to determine the camera's local system time.

Enable Daylight Saving Time

Enable **Daylight Saving Time (DST)** when required by the camera's location. Check the **Enable Daylight Saving Time** option, then specify the **time offset** and **DST duration**.

The time offset must be entered in the following format: **HH:MM:SS**

For example, for a one-hour time offset, enter: **01:00:00**

Time Settings

The **Time Settings** section allows the administrator to configure the camera's date and time display and synchronize the camera clock with a computer or NTP server.

Time Format

Select the desired **Time Format** from the drop-down menu:

- **yyyy/mm/dd**
- **dd/mm/yyyy**

The date and time displayed above the live video window will be shown according to the selected format.

Sync with Computer Time

Select **Sync with Computer Time** to synchronize the camera's date and time with the connected computer's system clock.

NOTE: Users **MUST** click **Save** to apply and confirm the synchronization. Otherwise, the camera time will not be synchronized with the computer.

Manual

Select **Manual** to manually configure the camera's date and time. Enter the values using the format specified in the examples displayed next to the corresponding input fields.

Sync with NTP Server

Network Time Protocol (NTP) allows the camera to automatically synchronize its clock with an NTP server over the network.

To configure NTP synchronization:

1. Enter the address of the desired **NTP Server**.
2. Select the **update interval** from the drop-down menu.
3. Click **Save** to confirm the settings.

The camera will also synchronize its time with the configured NTP server each time the camera **boots up**. For more information about NTP, visit www.ntp.org.

Security

The **Security** settings can be accessed through the following path: **System > Security**

Click **Security** to open the security configuration menu. The following tabs are available:

- **User** – Manage administrator and user account settings, including passwords and access privileges.
- **HTTPS** – Configure secure HTTPS communication for accessing the camera.
- **IP Filter** – Configure IP address filtering to control which devices are permitted or denied access to the camera.
- **IEEE 802.1X** – Configure network access authentication using the IEEE 802.1X standard.

User

The **User** settings can be accessed through: **System > Security > User**

Admin Password

The **Admin Password** setting allows the administrator to change or reset the administrator password.

To change the administrator password:

1. Enter the new password in the **Admin Password** field.
2. Re-enter the same password in the **Confirm Password** field.
3. Click **Save** to apply the changes.

The password can contain a maximum of 14 characters.

NOTE: The following characters are valid for the password: **A–Z, a–z, 0–9, ! # \$ % & ' - . @ ^ _ ~**

After the new password is saved, the web browser will require the administrator to log in to the camera again using the new password.

Add User

Use this item to add a new user account. Enter the username in **User name** and the password in **User password**. The username can contain up to 16 characters, and the password can contain up to 14 characters.

Click **Add** to create the account. The new username will appear in the **User name** drop-down menu under **Manage User**. A maximum of 20 user accounts can be created.

Select the required privileges:

- **I/O access** – Allows the user to view live video from the camera.
- **Camera control** – Allows the user to change camera parameters on the **Camera** and **Pan Tilt** setting pages.
- **Talk/Listen** – Allows the user at the camera site to communicate with a user at the remote site.

Manage User

Delete User

Select the username to delete from the **User name** drop-down menu, then click **Delete**.

Edit User

Select a username from the **User name** drop-down menu and click Edit. In the pop-up window, enter the new password and adjust the user privileges as required. Click <Save> to apply the changes, then click <Close> to exit.

HTTP Authentication Setting

This setting secures communication between the IP camera and the web browser by requiring users to enter a username and password before accessing protected camera settings or live video.

Two authentication methods are available:

- **Basic** – Provides basic authentication but offers less protection because the password may be intercepted.
- **Digest** – Provides stronger protection by transmitting the password in an encrypted format.

Click **Save** to apply the settings.

Streaming Authentication Setting

This setting prevents unauthorized users from accessing live streams through the Real-Time Streaming Protocol (RTSP). When enabled, users must enter a username and password before viewing live streams.

Three authentication modes are available:

- **Disable** – No authentication is required, allowing users to access live streams without a username or password.

- **Basic** – Provides basic protection for live streams, but the password may still be intercepted.
- **Digest** – Provides stronger protection by transmitting the password in an encrypted format.

NOTE: Click **<Save>** to apply the setting.

Enable Account Lockout Function

This function temporarily locks a user account after multiple consecutive failed login attempts. To enable it, select **Enable Account Lockout Function**, then specify the **Threshold** and **Duration**.

- **Threshold** – Specifies the maximum number of consecutive failed login attempts before the account is locked. The range is **5–20 attempts**. The default value is **5 attempts**.
- **Duration** – Specifies how long the account remains locked after the threshold is reached. The range is **1–60 minutes**. The default value is **10 minutes**.

HTTPS

The HTTPS setting can be found under **System > Security > HTTPS**.

HTTPS secures communication between the camera and the web browser using **Secure Socket Layer (SSL)** or **Transport Layer Security (TLS)**. This helps protect camera settings and username/password information from unauthorized access.

An HTTPS certificate is required to use HTTPS. The certificate can be obtained by either requesting one from a **Certificate Authority (CA)** or creating a self-signed certificate.

Enable HTTPS

Select the checkbox to enable HTTPS. Then select one of the following modes:

- **HTTP & HTTPS** – Enables both HTTP and HTTPS connections.
- **HTTPS only** – Allows connections through HTTPS only.

Click **Save** to apply the setting.

Create Self-Signed Certificate

A self-signed certificate can be created and installed before obtaining a CA-issued certificate.

Click **Create** under **Create Self-Signed Certificate**, then enter the required information to create the certificate. For details, see **Provide the Certificate Information** at the end of this section.

NOTE: A self-signed certificate does not provide the same level of security as a CA-issued certificate.

Install Signed Certificate

Click **Create Certificate Request** to generate a certificate request and submit it to a Certificate Authority (CA).

Enter the required information in the dialog box. See **Provide the Certificate Information** for details.

After the request is created, its subject will appear in the **Created Request** field. Click **Properties**, copy the PEM-formatted certificate request, and submit it to the selected CA.

When the CA returns the signed certificate, upload it to install the certificate.

Provide the Certificate Information

Enter the required information to create a self-signed HTTPS certificate or a certificate request for a CA.

	Create Self Signed Certificate	Create Certificate Request
Country	v	v
State or Province	v	v
Locality	v	v
Organization	v	v
Organizational Unit	v	v
Common Name	v	v
Valid Days	v	-

- **Country** – Enter the two-letter country code where the certificate will be used. For example, enter **US** for the United States.
- **State or Province** – Enter the state, province, or other administrative region.
- **Locality** – Enter the city or other geographic location.
- **Organization** – Enter the name of the organization associated with the certificate.
- **Organization Unit** – Enter the name of the department or organizational unit associated with the certificate.
- **Common Name** – Enter the name of the person or entity identified by the certificate, typically the website or domain name.
- **Valid Days** – Enter the certificate validity period in days, from **1** to **9999**.

Click **OK** to save the certificate information.

IP Filter

The IP Filter setting can be found under **System > Security > IP Filter**.

IP Filter allows users to allow or deny specific IPv4 addresses from accessing the camera.

- **Enable IP Filter**

Select the checkbox to enable IP Filter. The IP addresses listed under Filtered IP Addresses will then be either allowed or denied access.

Select Allow or Deny from the drop-down menu, then click Apply.

- **Add IP Address**

Enter an IPv4 address in the field below Filtered IP Address, then click Add. The address will be added to the list. Up to 256 IP addresses can be specified.

To filter a range of IP addresses, enter an IP address followed by a slash and a number from 1 to 31. For example, 192.168.2.81/30 filters the IP addresses 192.168.2.80 to 192.168.2.83.

The number after the slash specifies the number of network bits used to determine the IP address range. A larger number results in a smaller range.

Example: Filtering a Group of IP Addresses

For 192.168.2.81/30:

192.168.2.80 – Filtered

192.168.2.81 – Filtered

192.168.2.82 – Filtered

192.168.2.83 – Filtered

192.168.2.79 – Not filtered

192.168.2.84 – Not filtered

Therefore, entering 192.168.2.81/30 filters four consecutive IP addresses, from 192.168.2.80 to 192.168.2.83.

- **Delete IP Address**

To remove an IP address, select it from the Filtered IP Address list and click Delete.

IEEE 802.1X

The IEEE 802.1X setting can be found under this path: **System> Security> IEEE 802.1X**.

The camera is allowed to access a network protected by 802.1X/EAPOL (Extensible Authentication Protocol over LAN).

Choose **On** to enable the IEEE 802.1X function. Select one among the four protocol types: <EAP-MD5>, <EAP-TLS>, <EAP-TTLS> and <EAP-PEAP>.

Users need to contact the network administrator for gaining certificates, usernames and passwords.

CA Certificate

The CA certificate is created by the Certification Authority for the purpose of validating itself. Upload the certificate for checking the server's identity.

Client Certificate / Private Key

Upload the Client Certificate and Private Key for authenticating the camera itself.

Settings

- **Identity**

Enter the user identity associated with the certificate. Up to 16 characters can be used.

- **Private Key Password**

Enter the password (maximum 16 characters) for user identity.

Save IEEE 802.1X

Click on **Save** to save the IEEE 802.1X/EAP- TLS setting.

Network

The Network setting can be found under System > Network.

Click **Network** to access the following settings:

- **Basic**
- **QoS**
- **SNMP**
- **UPnP**

Basic

The Basic setting can be found under **System > Network > Basic**.

Use this page to configure the camera's IP address and other network parameters, including IPv6 settings when supported by the network.

General

Before configuring the IP address, determine the network type. Contact the network provider if necessary.

NOTE: If the network uses Point-to-Point Protocol over Ethernet (PPPoE), obtain the PPPoE username and password from the network provider.

- **Get IP Address Automatically (DHCP)**

Select **Get IP Address Automatically (DHCP)** and click **Save**. The camera will restart and obtain an IP address from the DHCP server.

After the restart:

1. Record the camera's MAC address from the camera label or packaging for identification.
2. Close the web browser and open **DeviceSearch.exe**.
3. Click **Device Search**. The detected IP devices will be listed.
4. Find the camera using its MAC address.
5. Double-click the camera or right-click it and select **Browse**.
6. Enter the username and password when prompted to access the camera.

- **Use Fixed IP Address**

Select **Use Fixed IP Address** and enter the required network settings.

The camera's IP address must be in the same LAN as the PC. For example:

- **IP Address:** 192.168.7.123
- **Default Gateway:** 192.168.7.254

Click **Save** and then **OK** when prompted to restart the camera. Wait approximately 15 seconds for the camera to restart.

After restarting, the camera's IP address will change, and you must log in again.

To access the camera, enter its IP address in the browser address bar and press **Enter**.

- **Network Parameters**

- **IP Address** – Specifies the camera's network address.
- **Subnet Mask** – Determines whether the destination is on the same subnet. The default value is **255.255.255.0**.
- **Default Gateway** – Specifies the gateway used to communicate with devices on different subnets. An incorrect gateway may prevent communication with external networks.
- **Primary DNS** – Specifies the primary DNS server used to resolve hostnames to IP addresses.
- **Secondary DNS** – Specifies the backup DNS server used if the primary DNS server is unavailable.

- **Use PPPoE**

If the network uses PPPoE, select **Use PPPoE** and enter the PPPoE username and password. Click **Save** to apply the settings.

Advanced

Use this section to configure the camera's **Web Server**, **RTSP**, **MJPEG over HTTP**, and **HTTPS** ports.

- **Web Server Port** – The default port is **80**. When using port 80, enter only the camera's IP address in the browser address bar.
If a different port is configured, enter the IP address followed by a colon and the port number. For example, if the IP address is **192.168.0.100** and the port is **8080**, enter:
<http://192.168.0.100:8080>
- **RTSP Port** – The default port is **554**. The port can be set to **554** or any value from **1024 to 65535**.
- **MJPEG over HTTP Port** – The default port is **8008**. The port can be set to **8008** or any value from **1024 to 65535**.
- **HTTPS Port** – The default port is **443**. The port can be set to **443** or any value from **1024 to 65535**.

NOTE: Use a different port number for each service to prevent network conflicts.

- **RTSP URL**

When viewing live video with an RTSP player, you can configure an access name for each of the four streams. The RTSP URL format is: **rtsp://IP address:RTSP port/access name**

For example, if the camera IP address is **192.168.0.100**, the RTSP port is **554**, and the Stream 1 access name is **liveview.1**, the RTSP URL is: **rtsp://192.168.0.100:554/liveview.1**

The access name can contain up to **32 characters**. Valid characters are **A–Z, a–z, 0–9, and ! # \$ % & ' - . @ ^ _ ~**.

IPv6 Address Configuration

If the network supports IPv6, select **Enable IPv6** and click **Save**. The assigned IPv6 address will appear next to **Address**. Use this address to access the camera.

QoS

The QoS (Quality of Service) setting can be found under this path: **System> Network> QoS**.

QoS allows providing differentiated service levels for different types of traffic packets, which guarantees delivery of priority services especially when network congestion occurs. Adapting the Differentiated Services (DiffServ) model, traffic flows are classified and marked with DSCP (DiffServ Codepoint) values, and thus receive the corresponding forwarding treatment from DiffServ capable routers.

DSCP Settings

The DSCP value range is from 0 to 63. The default DSCP value is 0, which means DSCP is disabled. The camera uses the following QoS Classes: Management, Video and Audio.

- **Management DSCP**

The class consists of HTTP traffic: Web browsing.

- **Stream 1~4 DSCP**

Users can set the Audio/Video DSCP of each stream.

- **Video DSCP**

The class consists of applications such as MJPEG over HTTP, RTP/RTSP and RTSP/HTTP.

- **Audio DSCP**

This setting is only available for the cameras that support audio.

NOTE: To enable this function, please make sure the switches / routers in the network support QoS.

VLAN

The VLAN setting can be found under System > Network > VLAN.

Select Enable VLAN to activate VLAN. Enter a VLAN ID from 1 to 4095. The default value is 20.

CoS

CoS (Class of Service) assigns transmission priority to different types of network traffic. A higher CoS value gives the traffic higher priority. CoS values range from 0 to 7 for each of the following traffic types:

- Live Video – Sets the priority for live video traffic.
- Live Audio – Sets the priority for live audio traffic.
- Management – Sets the priority for management traffic.

SNMP

The SNMP (Simple Network Management Protocol) setting can be found under System > Network > SNMP.

SNMP allows a network management system to remotely monitor and manage the camera.

SNMP v1 / v2

- **Enable SNMP v1 / v2** – Select the checkbox to enable SNMP v1 or v2.
- **Read Community** – Specifies the community name for read-only access to supported SNMP objects. The default value is public.
- **Write Community** – Specifies the community name for read/write access to supported SNMP objects, except read-only objects. The default value is private.

SNMP v3

SNMP v3 provides enhanced security by authenticating users and encrypting SNMP messages between the camera and the network management system.

- **Enable SNMP v3** – Select Enable SNMP v3 to activate SNMP v3.
- **Security Name** – Enter the SNMP security name. The maximum length is **32 characters**. Valid characters are **A–Z, a–z, 0–9, and ! # \$ % & ' - . @ ^ _ ~**.
- **Authentication Type** – Select an authentication method: **MD5** or **SHA**. **SHA** provides stronger security.
- **Authentication Password** – Enter an authentication password of at least **8 characters**. The password is displayed as dots for security. Valid characters are **A–Z, a–z, 0–9, and ! # \$ % & ' - . @ ^ _ ~**.
- **Encryption Type** – Select an encryption method: **DES** or **AES**. **AES** provides stronger security.
- **Encryption Password** – Enter an encryption password from **8 to 512 characters**. The password is displayed as dots for security. This field can be left blank; however, SNMP messages will not be encrypted. Valid characters for the encryption password are **A–Z, a–z, 0–9, and ! # \$ % & ' - . @ ^ _ ~**.

Traps for SNMP v1 / v2 / v3

SNMP traps allow the camera to automatically send notifications to a network management system when important events or status changes occur.

- **Enable Traps** – Select the checkbox to enable trap reporting.
- **Trap Address** – Enter the IP address of the network management server.
- **Trap Community** – Enter the community name used for trap messages.

Trap Option

- **Warm Start** – Sends an SNMP trap when the camera software restarts.

Click **Save** to apply the settings.

UPnP

The UPnP setting can be found under **System > Network > UPnP**.

UPnP Setting

- **Enable UPnP** – Enables the camera to be automatically discovered on the local network. When enabled, the camera appears under **Network** in Windows, allowing direct access.
NOTE: The UPnP component must be installed on the computer. See **Appendix A: Install UPnP Components** for installation instructions.
- **Enable UPnP Port Forwarding** – Allows the camera to automatically open its web server port on a UPnP-enabled router.
NOTE: The router must support UPnP, and UPnP must be enabled.
- **Friendly Name** – Assigns a name to the camera for easy identification.

Click **Save** to apply the settings.

DDNS

The DDNS setting can be found under **System > DDNS**.

Dynamic Domain Name System (DDNS) allows a domain name to remain linked to a camera with a dynamic IP address. This allows users to access the camera using a domain name instead of its changing IP address.

- **Enable DDNS** – Select **Enable DDNS** to activate the function.
- **Provider** – Select the DDNS service provider from the list.
- **Host Name** – Enter the domain name registered with the DDNS provider.
- **Username/E-Mail** – Enter the username or email address required by the DDNS provider.
- **Password/Key** – Enter the password or key required by the DDNS provider.

Mail

The Mail setting can be found under **System > Mail**.

The camera can send email notifications through **Simple Mail Transfer Protocol (SMTP)** when an alarm is triggered.

Up to **two SMTP servers** can be configured. Each configuration includes:

- **SMTP Server** – Enter the SMTP server address. Contact your network or email service provider for the required settings.
- **Account Name** – Enter the SMTP account name.

- **Password** – Enter the SMTP account password.
- **E-Mail Address** – Enter the email address used for sending notifications.

Click **Save** to apply the settings. Then click **Test** to verify the connection between the camera and the specified SMTP server.

FTP

The FTP setting can be found under this path: **System> FTP**.

The administrator can set the camera to send the alarm messages to a specific File Transfer Protocol (FTP) site when an alarm is triggered. Users can assign alarm message to up to two FTP sites. Enter the FTP details, which include server, server port, username, password and remote folder, in the fields.

Click on **Save** when finished. Then, please click on **Test** to check the connection between the camera and the specified FTP server.

HTTP

The HTTP setting can be found under this path: **System> HTTP**.

An HTTP Notification server can listen for the notification messages from the cameras by triggered events. Enter the HTTP details, which include server name (for instance, <http://192.168.0.100/admin.php>), username, and password in the fields. **Alarm** triggered and **Motion Detection** notifications can be sent to the specified HTTP server.

Click on **Save** when finished.

Please refer to [Events> Application> Send HTTP notification](#) for HTTP Notification settings.

Events (Alarm Settings)

The Events setting can be found under this path: **System> Events**.

Click on **Events**, there will be a drop-down menu with tabs including **Application**, **Motion Detection**, **Network Failure Detection**, **Tampering**, **Periodical Event**, **Manual Trigger**, and **Audio Detection**.

Application

The Application setting can be found under this path: **System> Events> Application**.

The camera supports one alarm input and one relay output for cooperation with alarm system to catch event images. Refer to alarm pin definition below to connect alarm devices to the camera if needed.

Alarm Switch

The default setting for the Alarm Switch function is <Off>. Enable the function by selecting <On>. Users can also activate the function according to the schedule previously set in the <Schedule> setting page. Select <By schedule> and click <Please select...> to choose the desired schedule from the drop-down menu.

Alarm Type

Select an alarm type, **Normal close** or **Normal open**, that corresponds with the alarm application.

Triggered Action

The administrator can specify alarm actions that will take when the alarm is triggered. All options are listed as follows.

- **Enable Alarm Output (high/low)**
Select the item to enable alarm relay output.
- **IR Cut Filter**
Select the item and the IR cut filter (ICR) of the camera will be removed (on) or blocked (off) when alarm input is triggered. This function is only available for models with IR cut filter.
NOTE: The IR Function could not be set as **Auto** mode if this triggered action is enabled.
- **Send Message by FTP/E-Mail**
Select whether to send alarm notifications by **FTP**, **E-Mail**, or both when an alarm is triggered.
- **Upload Image by FTP**
Select **Upload Image by FTP** to upload alarm-triggered images to a specified FTP server. At least one video stream **must** be set to **MJPEG**. Otherwise, this function is unavailable.
 - **Pre-trigger Buffer** – Uploads images captured before the alarm was triggered. This helps identify what caused the alarm. The default range is **1–20 frames**, but the available range may change when the MJPEG frame rate is 6 fps or lower.

- **Post-trigger Buffer** – Uploads a specified number of images after the alarm is triggered.
 - **Continue Image Upload** – Continues uploading images after the alarm is triggered. Select one of the following:
 - **Upload for ___ sec** – Uploads images for the specified duration, from **1 to 99999 seconds**.
 - **Upload during the trigger is active** – Continues uploading images until the alarm is released.
 - **Image Frequency** – Sets the image upload rate from **1 to 15 frames per second**.
- NOTE:** Configure the FTP settings before using this function. See **FTP** for details.

- **Upload Image by E-Mail**

Select **Upload Image by E-Mail** to send alarm-triggered images to a specified email address. At least one video stream **must** be set to **MJPEG**. Otherwise, this function is unavailable.

The following settings are available:

- **Pre-trigger Buffer** – Includes images captured before the alarm was triggered. The default range is **1–20 frames**, but the available range may change when the MJPEG frame rate is 6 fps or lower.
 - **Post-trigger Buffer** – Includes a specified number of images captured after the alarm is triggered.
 - **Continue Image Upload** – Continues sending images after the alarm is triggered:
 - **Upload for ___ sec** – Sends images for **1 to 99999 seconds**.
 - **Upload during the trigger is active** – Continues sending images until the alarm is released.
 - **Image Frequency** – Sets the image upload rate from **1 to 15 frames per second**.
- NOTE:** Configure the SMTP settings before using this function. See **Mail** for details.

- **Send HTTP Notification**

Select **Send HTTP Notification** and enter the destination HTTP server address.

When an alarm is triggered, the camera sends an HTTP notification to the specified server.

Custom parameters can be added to the notification.

For example, if the custom parameter is **action=1&group=2** and the server is

<http://192.168.0.100/admin.php>, the notification is sent to:

<http://192.168.0.100/admin.php/action=1&group=2>

- **Record Video Clip**
Select **Record Video Clip** and choose the storage location:
- **SD Card** – Saves alarm-triggered recordings to the camera's SD card.
- **NAS** – Saves recordings to a Network-Attached Storage device.
- **Pre-trigger Buffer** – Records video captured before the alarm is triggered. The available range is **1–3 seconds**.
- **Upload for ___ sec** – Sets the recording duration after the alarm is triggered, from **1 to 99999 seconds**.
- **Upload during the trigger is active** – Continues recording until the alarm is

released.

NOTE: Local recording or NAS recording must be enabled before using this function.

See **Recording** for details.

- **File Name**

Enter a file name, such as **image.jpg**, and select the required naming format.

- **Add Date/Time Suffix** – Adds the date, time, and sequence number to the file name.
Example: **imageYYMMDD_HHNNSS_XX.jpg**
Y = Year, **M** = Month, **D** = Day, **H** = Hour, **N** = Minute, **S** = Second, **X** = Sequence number
- **Add Sequence Number Suffix (No Maximum Value)** – Adds a continuously increasing sequence number.
Example: **imageXXXXXXX.jpg**
- **Add Sequence Number Suffix Up to # and Then Start Over** – Sets a maximum sequence number and restarts from 00 after reaching the limit.
Example: If the limit is **10**, file names cycle from **00 to 10** and then restart at **00**.
- **Overwrite** – Replaces the existing file with the same name on the FTP server.

- **Save**

Click **Save** to apply all settings.

Motion Detection

The Motion Detection setting can be found under **System > Events > Motion Detection**.

Motion Detection detects movement by comparing pixels between consecutive live images. When the detected motion reaches the configured sensitivity threshold, an alarm is triggered.

Up to **four Motion Detection Settings** can be configured. Select a setting from the **Motion Detection** drop-down menu.

Motion Detection

Motion Detection is **Off** by default. Select **On** to enable it.

You can also enable Motion Detection according to a schedule configured in **Schedule**. Select **By Schedule**, then choose the required schedule from the drop-down menu.

Motion Region Setup

The camera divides the detection area into **1,200 grids (40 × 30)**. Select the grids where motion should be detected.

To define the detection area:

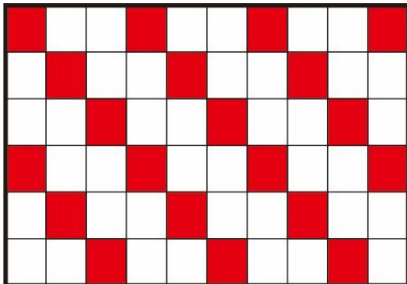
1. Select **Enable Brush**.
2. Select a brush size: **1 × 1**, **3 × 3**, or **5 × 5**.
3. Click and drag the mouse over the grids to select the detection area.
4. To remove a selected area, click and drag over the colored grids.



Motion Detection Settings

Use this section to configure the motion detection parameters.

- **Sampling Pixel Interval [1–10]** – Sets the number of pixels skipped when comparing two consecutive frames. The default value is **1**. For example, a value of **3** checks one pixel for every three pixels in each row and column of the detection area.



- **Detection Level [1–100]** – Sets the amount of pixel difference required to detect motion. A lower value detects smaller changes. The default value is **10**.
- **Sensitivity Level [1–100]** – Sets the percentage of changed sampling pixels required to trigger motion detection. The default value is **80**. At this setting, motion is detected when approximately **20% or more** of the sampling pixels change. A higher value increases sensitivity and lowers the red threshold line in the motion indication window.
- **Time Interval (sec) [0–7200]** – Sets the minimum interval between motion detection events. The default value is **10 seconds**.

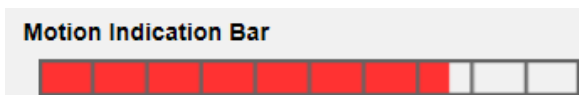
Motion Indication Bar

When Motion Detection is enabled, the Motion Indication Bar displays the detected motion level.

- **Green** – Motion is detected but remains below the configured detection threshold. No alarm is triggered.



- **Red** – Motion exceeds the configured detection threshold. An alarm is triggered.



Triggered Action

Select one or more actions to perform when motion is detected.

- **Enable Alarm Output (High/Low)** – Activates the selected alarm output when motion is detected.
- **Send Alarm Message by FTP/E-Mail** – Sends an alarm notification by FTP, E-Mail, or both.
- **Upload Image by FTP** – Uploads images captured during the motion event to a specified FTP server. At least one video stream **must** be set to **MJPEG**.
 - **Pre-trigger Buffer** – Includes images captured before the motion event. The default range is **1–20 frames**, but the available range may change when the MJPEG frame rate is 6 fps or lower.
 - **Post-trigger Buffer** – Includes images captured after the motion event.
 - **Continue Image Upload** – Continues uploading images after motion is detected:
 - **Upload for ___ sec** – Uploads images for **1 to 99999 seconds**.
 - **Upload during the trigger is active** – Continues uploading until the motion event ends.
 - **Image Frequency** – Sets the upload rate from **1 to 15 frames per second**.

NOTE: Configure the FTP settings before using this function. See **FTP** for details.
- **Upload Image by E-Mail** – Sends images captured during the motion event to a specified email address. At least one video stream **must** be set to **MJPEG**.
 - **Pre-trigger Buffer** – Includes images captured before the motion event. The default range is **1–20 frames**, but the available range may change when the MJPEG frame rate is 6 fps or lower.
 - **Post-trigger Buffer** – Includes images captured after the motion event.
 - **Continue Image Upload** – Continues sending images after motion is detected:
 - **Upload for ___ sec** – Sends images for **1 to 99999 seconds**.
 - **Upload during the trigger is active** – Continues sending images until the motion event ends.
 - **Image Frequency** – Sets the upload rate from **1 to 15 frames per second**.

NOTE: Configure the SMTP settings before using this function. See **Mail** for details.
- **Send HTTP Notification** – Sends an HTTP notification to a specified server when motion is

detected. Custom parameters can be included in the notification.

Example:

HTTP Server: <http://192.168.0.100/admin.php>

Custom Parameter: action=1&group=2

The resulting notification URL is: <http://192.168.0.100/admin.php/action=1&group=2>

- **Record Video Clip** – Records motion-triggered video to an **SD Card** or **NAS**.
 - **Pre-trigger Buffer** – Records video from **1 to 3 seconds** before the motion event.
 - **Upload for ___ sec** – Sets the recording duration after motion is detected, from **1 to 99999 seconds**.
 - **Upload during the trigger is active** – Continues recording until the motion event ends.
- NOTE:** Local recording or NAS recording must be enabled before using this function.
See **Recording** for details.

File Name

Enter a file name, such as **image.jpg**, and select the required naming format.

- **Add Date/Time Suffix** – Adds the date, time, and sequence number to the file name.
Example: **imageYYMMDD_HHNNSS_XX.jpg**
Y = Year, **M** = Month, **D** = Day, **H** = Hour, **N** = Minute, **S** = Second, **X** = Sequence number
- **Add Sequence Number Suffix (No Maximum Value)** – Adds a continuously increasing sequence number.
Example: **imageXXXXXXX.jpg**
- **Add Sequence Number Suffix Up to # and Then Start Over** – Sets a maximum sequence number and restarts from 00 after reaching the limit. For example, with a limit of **10**, the sequence runs from **00 to 10**, then starts again at **00**.
- **Overwrite** – Replaces an existing file with the same name on the FTP server.

Save

Click **Save** to apply the settings.

Network Failure Detection

The Network Failure Detection setting can be found under **System > Events > Network Failure Detection**.

Network Failure Detection periodically checks the connection to a specified IP device, such as an NVR or video server. If the device fails to respond, the camera can trigger an alarm and start backup recording.

The camera can record to an **SD Card** or **NAS** during a network failure, providing backup recording for the surveillance system.

Detection Switch

The function is **Off** by default. Select **On** to enable it.

To enable detection according to a schedule, select **By Schedule** and choose the required schedule from the drop-down menu.

Detection Type

Enter the IP address of the device to monitor and set the ping interval.

The camera sends a ping every **1 to 99 minutes**. If the camera fails to receive a response **three consecutive times**, a network failure alarm is triggered.

Triggered Action

Select one or more actions to perform when a network failure is detected.

- **Enable Alarm Output (High/Low)** – Activates the alarm relay output.
- **Send Alarm Message by FTP/E-Mail** – Sends an alarm notification by FTP, E-Mail, or both.
- **Record Video Clip** – Records video to an **SD Card** or **NAS**.
 - **Pre-trigger Buffer** – Records video from **1 to 3 seconds** before the network failure is detected.
 - **Upload for ____ sec** – Sets the recording duration after the alarm is triggered, from **1 to 99999 seconds**.
 - **Upload during the trigger is active** – Continues recording until the network failure is cleared.

NOTE: Local recording or NAS recording must be enabled before using this function.
See **Recording** for details.

Save

Click **Save** to apply the settings.

Tampering

The Tampering setting can be found under **System > Events > Tampering**.

NOTE: This feature is available only on select models.

Tampering Alarm detects camera tampering, such as camera redirection, obstruction, paint spray, or lens covering. When tampering is detected, the camera can trigger an alarm, send notifications, upload images, or record video.

Tampering Alarm

The function is **Off** by default. Select **On** to enable it.

To enable tampering detection according to a schedule, select **By Schedule** and choose the required schedule.

Tampering Duration

Sets the minimum time required to confirm a tampering event. A longer duration provides a higher detection threshold and helps reduce false alarms.

The setting range is **10–3600 seconds**. The default value is **20 seconds**.

Triggered Action

Select one or more actions to perform when tampering is detected.

- **Enable Alarm Output (High/Low)** – Activates the selected alarm output.
- **Send Message by FTP/E-Mail** – Sends an alarm notification by FTP, E-Mail, or both.
- **Upload Image by FTP** – Uploads tampering event images to a specified FTP server. At least one video stream **must** be set to **MJPEG**.
 - **Pre-trigger Buffer** – Includes images captured before the tampering event. The default range is **1–20 frames**, but the available range may change when the MJPEG frame rate is 6 fps or lower.
 - **Post-trigger Buffer** – Includes images captured after tampering is detected.
 - **Continue Image Upload** – Continues uploading images after tampering is detected:
 - **Upload for ___ sec** – Uploads images for **1 to 99999 seconds**.
 - **Upload during the trigger is active** – Continues uploading until tampering stops.
 - **Image Frequency** – Sets the upload rate from **1 to 15 frames per second**.

NOTE: Configure the FTP settings before using this function. See **FTP** for details.
- **Upload Image by E-Mail** – Sends tampering event images to a specified email address. At least one video stream **must** be set to **MJPEG**.
 - **Pre-trigger Buffer** – Includes images captured before the tampering event. The default range is **1–20 frames**, but the available range may change when the MJPEG frame rate is 6 fps or lower.
 - **Post-trigger Buffer** – Includes images captured after tampering is detected.
 - **Continue Image Upload** – Continues sending images after tampering is detected:
 - **Upload for ___ sec** – Sends images for **1 to 99999 seconds**.
 - **Upload during the trigger is active** – Continues sending images until

tampering stops.

- **Image Frequency** – Sets the upload rate from **1 to 20 frames per second**.

NOTE: Configure the SMTP settings before using this function. See **Mail** for details.

- **Send HTTP Notification** – Sends an HTTP notification to a specified server when tampering is detected. Custom parameters can be included.

Example:

HTTP Server: <http://192.168.0.1/admin.php>

Custom Parameter: action=1&group=2

The notification is sent to: <http://192.168.0.1/admin.php?action=1&group=2>

- **Record Video Clip** – Records tampering-triggered video to an **SD Card** or **NAS**.
 - **Pre-trigger Buffer** – Records video from **1 to 3 seconds** before the tampering event.
 - **Upload for ____ sec** – Sets the recording duration after tampering is detected, from **1 to 99999 seconds**.
 - **Upload during the trigger is active** – Continues recording until tampering stops.

NOTE: Local recording or NAS recording must be enabled before using this function.
See **Recording** for details.

File Name

Enter a file name, such as **image.jpg**, and select the required naming format.

- **Add Date/Time Suffix** – Adds the date, time, and sequence number to the file name.

Example: **imageYYMMDD_HHNNSS_XX.jpg**

Y = Year, **M** = Month, **D** = Day, **H** = Hour, **N** = Minute, **S** = Second, **X** = Sequence number

- **Add Sequence Number Suffix (No Maximum Value)** – Adds a continuously increasing sequence number.

Example: **imageXXXXXXX.jpg**

- **Add Sequence Number Suffix Up to # and Then Start Over** – Sets a maximum sequence number and restarts from 00 after reaching the limit. For example, with a limit of **10**, the sequence runs from **00 to 10**, then starts again at **00**.
- **Overwrite** – Replaces an existing file with the same name on the FTP server.

Save

Click **Save** to apply the settings.

Periodical Event

The Periodical Event setting can be found under **System > Events > Periodical Event**.

Periodical Event allows the camera to capture and upload images at regular intervals to an **FTP server, email address, or SD Card**.

For example, with a time interval of **60 seconds**, the camera uploads images every 60 seconds.

Periodical Event

The function is **Off** by default. Select **On** to enable it.

Time Interval

Sets how often images are captured and uploaded.

The setting range is **60–3600 seconds**. The default value is **60 seconds**.

Triggered Action

Select one or more destinations for the captured images.

- **Upload Image by FTP** – Uploads images periodically to a specified FTP server. At least one video stream **must** be set to **MJPEG**.
 - **Pre-trigger Buffer** – Specifies the number of images captured before the scheduled capture time. The default range is **1–20 frames**, but the available range may change when the MJPEG frame rate is 6 fps or lower.
 - **Post-trigger Buffer** – Specifies the number of images captured after the scheduled capture time.

NOTE: Configure the FTP settings before using this function. See **FTP** for details.
- **Upload Image by E-Mail** – Sends images periodically to a specified email address. At least one video stream **must** be set to **MJPEG**.
 - **Pre-trigger Buffer** – Specifies the number of images captured before the scheduled capture time. The default range is **1–20 frames**, but the available range may change when the MJPEG frame rate is 6 fps or lower.
 - **Post-trigger Buffer** – Specifies the number of images captured after the scheduled capture time.

NOTE: Configure the SMTP settings before using this function. See **Mail** for details.
- **Upload Image to SD Card** – Saves images periodically to the SD Card. At least one video stream **must** be set to **MJPEG**.
 - **Pre-trigger Buffer** – Specifies the number of images captured before the scheduled capture time.
 - **Post-trigger Buffer** – Specifies the number of images captured after the scheduled capture time.

NOTE: Make sure the SD Card is properly installed and detected before using this function. See **Storage Management > SD Card > Device Information** for details.

File Name

Enter a file name, such as **image.jpg**, and select the required naming format.

- **Add Date/Time Suffix** – Adds the date, time, and sequence number to the file name.
Example: **imageYYMMDD_HHNNSS_XX.jpg**
Y = Year, **M** = Month, **D** = Day, **H** = Hour, **N** = Minute, **S** = Second, **X** = Sequence number
- **Add Sequence Number Suffix (No Maximum Value)** – Adds a continuously increasing sequence number.
Example: **imageXXXXXXX.jpg**
- **Add Sequence Number Suffix Up to # and Then Start Over** – Sets a maximum sequence number and restarts from 00 after reaching the limit. For example, with a limit of **10**, the sequence runs from **00 to 10**, then starts again at **00**.
- **Overwrite** – Replaces an existing file with the same name on the FTP server.

Save

Click **Save** to apply the settings.

Manual Trigger

The Manual Trigger setting can be found under **System > Events > Manual Trigger**.

Manual Trigger allows users to manually upload images or video to an FTP server or email address.

When enabled, click the **Manual Trigger** button on the Home page to start uploading. Click it again to stop.

Manual Trigger

The default setting is **Off**. Select **On** to enable the function.

Triggered Action

Select the actions to perform when the Manual Trigger is activated.

- **Enable Alarm Output (High/Low)**
Enables the selected alarm relay output.
- **IR Cut Filter**
Controls the camera's IR cut filter when the trigger is activated. This option is available only on models with an IR cut filter.
NOTE: The IR Function cannot be set to **Auto** when this option is enabled.
- **Send Message by FTP/E-Mail**
Sends an alarm message through FTP, email, or both when the trigger is activated.
- **Upload Image by FTP**
Uploads event images to the specified FTP server. One of the camera streams **must** be set to **MJPEG** to enable this function.
 - **Pre-trigger buffer** specifies the number of images captured before the trigger.
 - **Post-trigger buffer** specifies the number of images captured after the trigger.
The pre-trigger buffer normally ranges from 1 to 20 frames. The available range may vary when the MJPEG frame rate is 6 fps or lower.
Select **Continue image upload** to continue uploading images for a specified duration or until the trigger is released:

- **Upload for __ sec:** Upload images for 1 to 99999 seconds.
 - **Upload during the trigger active:** Continue uploading until the trigger is released.
 - **Image frequency:** Sets the upload rate from 1 to 15 frames per second.
NOTE: Make sure the FTP settings are configured. See the **FTP** section for details.
- **Upload Image by E-Mail**
 Sends event images to the specified email address. One of the camera streams **must** be set to **MJPEG** to enable this function.
 - **Pre-trigger buffer** specifies the number of images captured before the trigger.
 - **Post-trigger buffer** specifies the number of images captured after the trigger.
 The pre-trigger buffer normally ranges from 1 to 20 frames. The available range may vary when the MJPEG frame rate is 6 fps or lower.
 Select **Continue image upload** to continue sending images for a specified duration or until the trigger is released:
 - **Upload for __ sec:** Send images for 1 to 99999 seconds.
 - **Upload during the trigger active:** Continue sending images until the trigger is released.
 - **Image frequency:** Sets the upload rate from 1 to 15 frames per second.
NOTE: Make sure the SMTP settings are configured. See the **Mail** section for details.
 - **Send HTTP Notification**
 Sends an event notification to the specified HTTP server when the trigger is activated. Enter the destination HTTP address and event parameters.
 - **Record Video Clip**
 Records the triggered video to an **SD Card** or **NAS**.
 - **Pre-trigger buffer** records 1 to 3 seconds of video before the trigger.
 - **Upload for __ sec:** Records for 1 to 99999 seconds after the trigger.
 - **Upload during the trigger active:** Continues recording until the trigger is released.
NOTE: Local recording on the SD card or remote recording on the NAS must be enabled. See the **Recording** section for details.

File Name

Enter the file name format for uploaded images, such as image.jpg.

- **Add date/time suffix**
 Format: imageYYMMDD_HHNNSS_XX.jpg
 Y = Year, M = Month, D = Day, H = Hour, N = Minute, S = Second, X = Sequence number.
- **Add sequence number suffix (no maximum value)**
 Format: imageXXXXXXXXX.jpg
 The sequence number continues without a maximum limit.
- **Add sequence number suffix up to # and then start over**
 Format: imageXX.jpg
 The sequence number resets after reaching the specified limit. For example, setting the limit to 10 generates numbers from 00 to 10, then starts again at 00.

- **Overwrite**

Overwrites the existing file on the FTP server with the new image when a fixed file name is used.

Save

Click **Save** to apply all settings.

Audio Detection

The Audio Detection setting can be found under **System > Events > Audio Detection**.

Audio Detection allows the camera to detect sounds that exceed the configured sensitivity level and trigger specified alarm actions.

NOTE: This function is available only on models with Audio I/O support.

Audio Detection

The default setting is **Off**. Select **On** to enable Audio Detection.

Audio Detection Setting

Configure the following parameters:

- **Detection Level [1–100]**
Sets the sound level required to trigger detection. A lower value provides higher sensitivity. The default value is 10.
- **Time Interval (sec) [0–7200]**
Sets the minimum interval between detected audio events. The default value is 10 seconds.

Triggered Action

Select the actions to perform when audio is detected.

- **Enable Alarm Output (High/Low)**
Enables the selected alarm relay output.
- **Send Alarm Message by FTP/E-Mail**
Sends an alarm message through FTP, email, or both when audio is detected.
- **Upload Image by FTP**
Uploads event images to the specified FTP server. One of the camera streams **must** be set to **MJPEG** to enable this function.
 - **Pre-trigger buffer** specifies the number of images captured before the audio event.
 - **Post-trigger buffer** specifies the number of images captured after the event.
The pre-trigger buffer normally ranges from 1 to 20 frames. The available range may vary when the MJPEG frame rate is 6 fps or lower.
Select **Continue image upload** to continue uploading images for a specified duration or until the event ends:
 - **Upload for __ sec:** Upload images for 1 to 99999 seconds.
 - **Upload during the trigger active:** Continue uploading until the event ends.
 - **Image frequency:** Sets the upload rate from 1 to 15 frames per second.

NOTE: Make sure the FTP settings are configured. See the **FTP** section for details.

- **Upload Image by E-Mail**

Sends event images to the specified email address. One of the camera streams **must** be set to **MJPEG** to enable this function.

- **Pre-trigger buffer** specifies the number of images captured before the audio event.
- **Post-trigger buffer** specifies the number of images captured after the event.
Select **Continue image upload** to continue sending images for a specified duration or until the event ends:
- **Upload for __ sec:** Send images for 1 to 99999 seconds.
- **Upload during the trigger active:** Continue sending images until the event ends.
- **Image frequency:** Sets the upload rate from 1 to 15 frames per second.

NOTE: Make sure the SMTP settings are configured. See the **Mail** section for details.

- **Send HTTP Notification**

Sends an event notification to the specified HTTP server when audio is detected. Enter the destination HTTP address and event parameters.

- **Record Video Clip**

Records video to an **SD Card** or **NAS** when audio is detected.

- **Pre-trigger buffer** records 1 to 3 seconds of video before the event.
- **Upload for __ sec:** Records for 1 to 99999 seconds after the event.
- **Upload during the trigger active:** Continues recording until the event ends.

NOTE: Local recording on the SD card or remote recording on the NAS must be enabled. See the **Recording** section for details.

File Name

Enter the file name format for uploaded images, such as image.jpg.

- **Add date/time suffix**

Format: imageYYMMDD_HHNNSS_XX.jpg

Y = Year, M = Month, D = Day, H = Hour, N = Minute, S = Second, X = Sequence number.

- **Add sequence number suffix (no maximum value)**

Format: imageXXXXXXXX.jpg

The sequence number continues without a maximum limit.

- **Add sequence number suffix up to # and then start over**

Format: imageXX.jpg

The sequence number resets after reaching the specified limit. For example, setting the limit to 10 generates numbers from 00 to 10, then starts again at 00.

- **Overwrite**

Overwrites the existing file on the FTP server with the new image when a fixed file name is used.

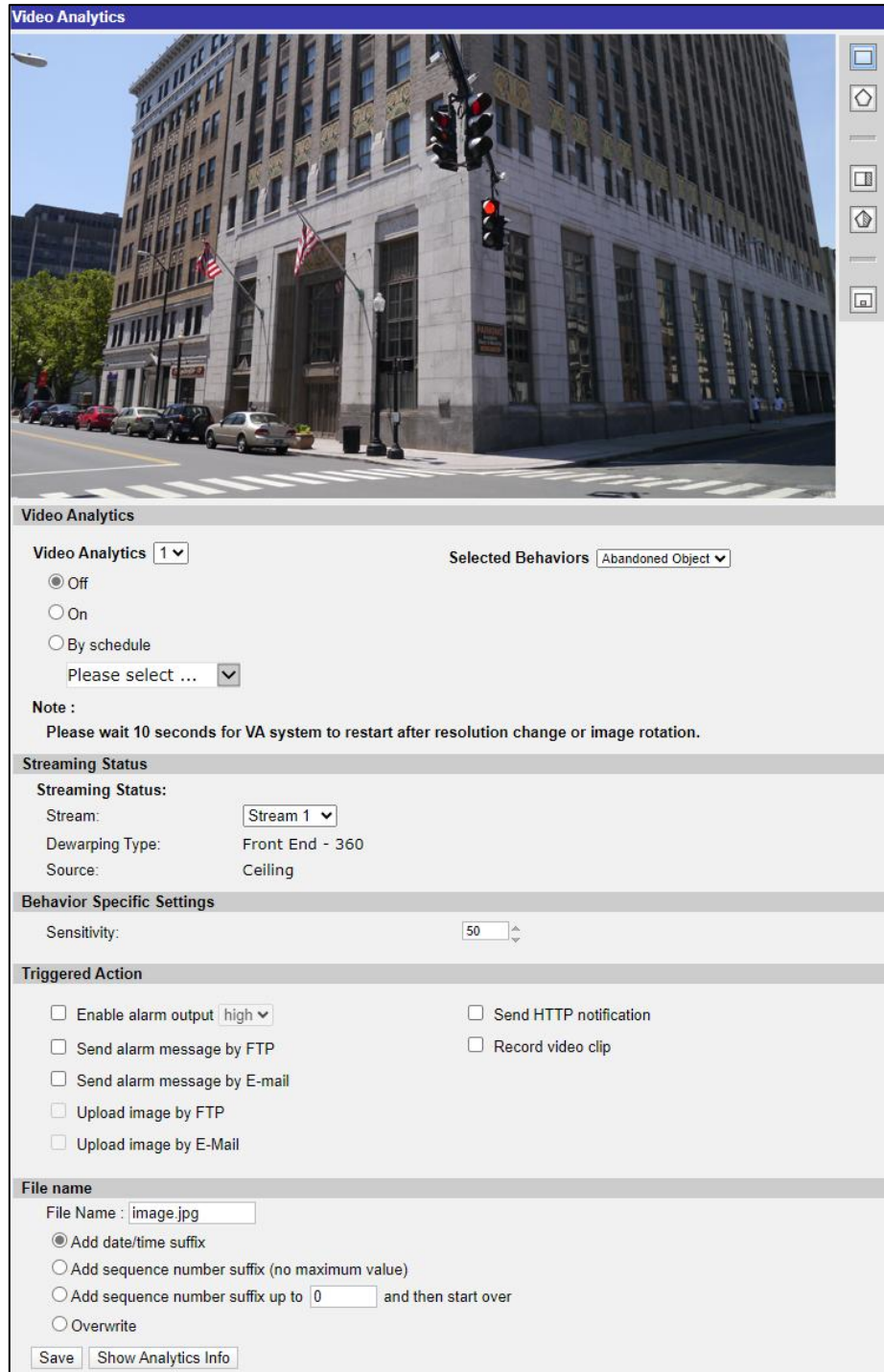
Save

Click **Save** to apply all Audio Detection settings.

Video Analytics Standard Setting

Use this section to configure video analytics functions for cameras that support video analytics.

The standard setting for built-in video analytics includes zone and behavior setting. The availability of the built-in video analytics and its parameters may vary depending on the camera model.



Video Analytics

Video Analytics 1 Selected Behaviors Abandoned Object

☒ Off
☐ On
☐ By schedule
 Please select ... ▼

Note :
Please wait 10 seconds for VA system to restart after resolution change or image rotation.

Streaming Status

Streaming Status:

Stream: Stream 1 ▼

Dewarping Type: Front End - 360

Source: Ceiling

Behavior Specific Settings

Sensitivity: 50 ▲▼

Triggered Action

☐ Enable alarm output high ▼ ☐ Send HTTP notification
☐ Send alarm message by FTP ☐ Record video clip
☐ Send alarm message by E-mail
☐ Upload image by FTP
☐ Upload image by E-Mail

File name

File Name : image.jpg

☒ Add date/time suffix
☐ Add sequence number suffix (no maximum value)
☐ Add sequence number suffix up to 0 and then start over
☐ Overwrite

The video analytics functions that support people/face or vehicle recognition are **Intrusion Detection**, **Wrong Direction**, **Loitering Detection**, **Object Counting**, **Stopped Vehicle**, **Face Detection**, **Face Recognition** and **License Plate Recognition**. See the **Built-in Video Analytics** section for specific details of each function.

Zone

A zone is defined as the region of interest or detection area. This is where users want to monitor and check for any intrusion or abandoned object, etc. A zone can be defined by a polygon or line, among others. Select a drawing tool and click on the video pane to draw the zone.

The definition of each drawing tool is as below:

Item		Description
	Box	Detection zone. Objects in the defined zone will trigger the alarm if the objects move in the same direction or behave as defined.
	Polygon	
	Line	Detection zone. The line is a detection zone. Set lines to trigger the alarm as when objects cross that line or move in the same direction.
	Exclude Zone Box Tool	Set zones in which objects in the zone will be ignored.
	Exclude Polygon Tool	
	Object Size Filter	Set the minimum and maximum size of objects. To prevent incorrect detection setting, the short side of the Max Object Size must be longer than any side of the Min Object Size.

NOTE: Zone drawing tools vary depending on the selected built-in analytics function and its behavior.

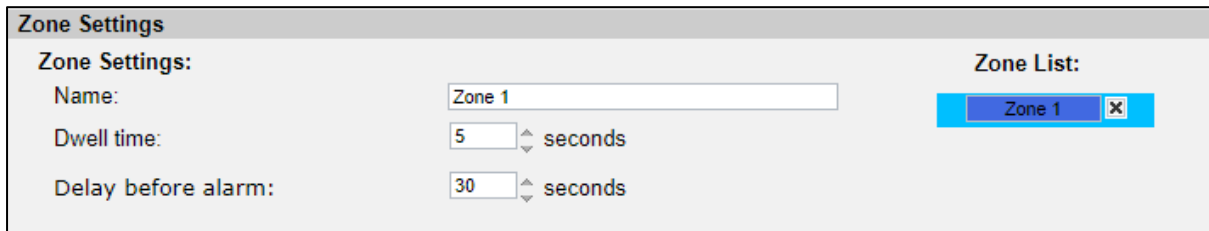
NOTE: The number of detection zones is 8. A warning message window will pop up if the number of zones exceeds 8.

Behavior Setting

After setting the detection zone, configure the behavior or response action to take once the event is triggered. A **Zone Settings** section appears when a detection zone is configured. This allows you to configure the conditions of the event.

NOTE: Zone setting parameters vary depending on the type of analytics being configured.

Zone Settings



Zone Settings

Zone Settings:

Name:

Dwell time: seconds

Delay before alarm: seconds

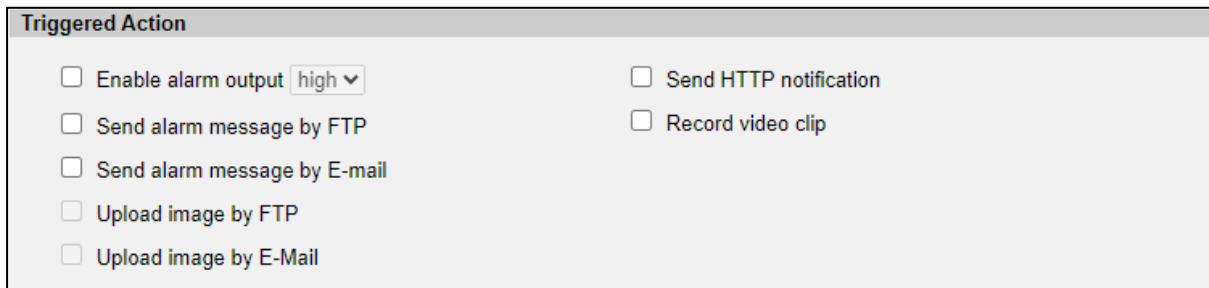
Zone List:

Below are the zone settings parameters commonly available from all the video analytics:

- **Name:** Name of the detection zone
- **Directions:** Set the motion direction that the camera will track. Alarms will only be triggered when the camera detects motion in the specified direction.
- **Dwell time:** Set the amount of time that the alarm will continue to sound when triggered. Dwell time ranges from 1 to 1000 seconds. Default is 5 seconds.
- **Delay before alarm:** Define the amount of time that the defined behavior will last before an alarm is triggered. The time range is 20 to 1800 seconds. Default is 30 seconds.
- **Alarm at:** Set the number of objects to trigger the alarm. When the number of the counted objects reaches that number, the alarm will be triggered
- **Reset counter on alarm:** Check or un-check to reset or keep object counting.

Triggered Action

On this section, select the response or actions to take when the event is triggered. Multiple options can be selected.



Triggered Action

☐ Enable alarm output

☐ Send alarm message by FTP

☐ Send alarm message by E-mail

☐ Upload image by FTP

☐ Upload image by E-Mail

☐ Send HTTP notification

☐ Record video clip

- **Enable Alarm Output:** Select the item to enable alarm relay output.
- **Send Message by FTP:** Select to send an alarm message by FTP.
- **Send Message by E-Mail:** Send an alarm message by E-mail.
- **Upload Image by FTP:** Users can assign an FTP site and configure various parameters. When the alarm is triggered, event images will be uploaded to the appointed FTP site.

- **Upload Image by E-Mail:** Users can assign an E-mail address and configure various parameters. When the alarm input is triggered, event images will be sent to the appointed E-mail address.
- **Send HTTP Notification:** Check this item and select the destination HTTP address. Then specify the parameters for event notifications by <Alarm> triggered. When an alarm is triggered, the HTTP notification will be sent to the specified HTTP server.
- **Record Video Clip:** Check this item and select a video recording storage type, <SD Card> or <NAS> (Network-Attached Storage). The alarm-triggered recording will be saved into the memory card or the NAS.

File Name

On this section, the file format and file name of the images to be uploaded are configured.

File name

File Name :

☒ Add date/time suffix
☐ Add sequence number suffix (no maximum value)
☐ Add sequence number suffix up to and then start over
☐ Overwrite

- **Add date/time suffix**
 File name: imageYYMMDD_HHNNSS_XX.jpg
 Y: Year, M: Month, D: Day
 H: Hour, N: Minute, S: Second
 X: Sequence Number
- **Add sequence number suffix (no maximum value)**
 File name: imageXXXXXXXX.jpg
 X: Sequence Number
- **Add sequence number suffix up to # and then start over**
 File Name: imageXX.jp
 X: Sequence Number
 The file name suffix will end at the number being set. For example, if the setting is up to "10", the file name will start from 00, end at 10, and then start all over again.
- **Overwrite**
 The original image in the FTP site will be overwritten by the new uploaded file with a static filename.

Save

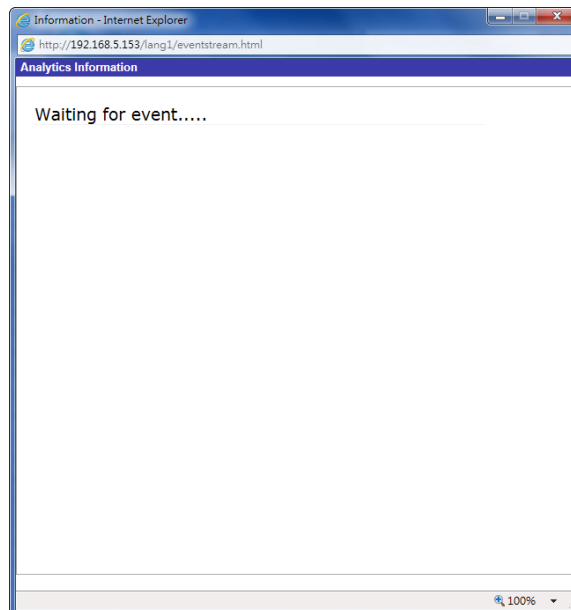
After completing all the settings mentioned above, click **Save** to save all the settings in this page.

Show Analytics Info

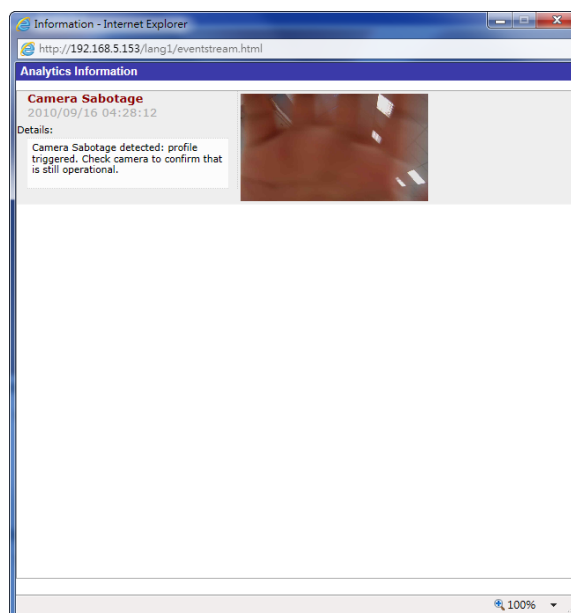
Click **Show Analytics Info** and the “Analytics Information” window will pop up. Whenever an event occurs, “Analytics Information” will update and post the occurring event to notify users.

NOTE: Set at least one Video Stream to MJPEG format to show the snapshot of the occurring event. Go to **Streaming > Video Configuration** and then set at least one Video Stream to **MJPEG** under **Encode Type**.

When no event occurs, the “Analytics Information” window will be shown as below.



When an event occurs, the related information and the snapshot will be updated in this window as shown below.



Storage Management

The Storage Management setting can be found under **System > Storage Management**.

The page includes the following tabs: **SD Card** and **Network Share**.

SD Card

The SD Card setting can be found under **System > Storage Management > SD Card**.

The camera supports local recordings to microSD, SDHC, and SDXC cards up to 128 GB. This page displays card capacity and status, lists recorded files, and provides options to format the card and automatically delete old recordings.

To enable SD card recording, configure the settings under Recording.

NOTE: Format the SD card before using it for the first time. Reformat the card if it is moved from a camera with a different software platform.

NOTE: Continuous 24/7 recording to an SD card is not recommended because long-term continuous read/write operations may reduce card reliability and lifespan. Contact the card manufacturer for recommended usage and service life.

Device Information

Displays information about the inserted SD card, including its capacity and status.

Recording Source

Select the video stream to use for recording. The default is Stream 1. Select the desired stream and click **Save**.

- **Recording Filename Format**
Select the format used for recording file names. The default is Start time only. Select the desired format and click Save.

Device Setting

Click Format to format the SD card. The available file systems are:

- vfat — Default
- ext4 — Recommended for more stable and reliable performance

Disk Cleanup Setting

Enable **Automatic Disk Cleanup** to automatically delete old recordings when specified conditions are met. Configure the following:

- Time: 1–999 days or 1–142 weeks
- Storage limit: 1–99% full

Click **Save** to apply the settings.

Recording List

Enter a date range and click Search to view recorded files. Select Video or JPEG to filter the results. The maximum file size is 60 MB per file.

When **Always** recording is enabled, event-triggered recording takes priority when an event occurs.

After the event recording ends, the camera resumes normal continuous recording.

- **Remove**

Select a file and click Remove to delete it.

- **Sort**

Click Sort to arrange files by name or date.

The first letter of a recording file name indicates the recording type. The available codes are A, M, N, T, S, R, V, and U, as described below.

Initial	Recording Type	Initial	Recording Type
A	Alarm	S	Periodical Event
M	Motion	R	Regular Recording
N	Network Failure	V	Manual Trigger
T	Tampering	U	Audio Detection

- **Download**

Select a video or image file from the Recording List and click **Download**. In the pop-up window, click the **AVI** or **JPEG** file to open it or save it to the desired location.

Network Share (NAS)

The Network Share setting can be found under **System > Storage Management > Network Share**.

The camera can store recordings on a network share folder or **NAS (Network-Attached Storage)**.

This page displays NAS capacity and status, lists recorded files, and provides options to format the NAS and automatically clean up old recordings.

Device Information

Displays the NAS capacity and status when the NAS is successfully connected.

Storage Settings

Enter the NAS connection details:

- **Host:** IP address of the NAS
- **Share:** NAS folder name
- **Username:** NAS account name
- **Password:** NAS account password

Click **Save** to apply the settings.

Storage Tools

Click **Format** to format the NAS.

Recording Source

Select the video stream to use for recording. The default is **Stream 1**. Select the desired stream and click **Save**.

Recording Filename Format

Select the format used for recording file names. The default is **Start time only**. Select the desired format and click **Save**.

Disk Cleanup Setting

Enable **Automatic Disk Cleanup** to automatically delete old recordings.

Configure the following:

- **Time:** 1–999 days or 1–142 weeks
- **Storage limit:** 1–99% full

Click **Save** to apply the settings.

Recording List

All recorded video files stored on the NAS are listed here. The maximum file size is **60 MB per file**.

When **Always** recording is enabled, event-triggered recording takes priority when an event occurs.

After the event recording ends, the camera resumes normal continuous recording.

- **Remove**

Select a file and click **Remove** to delete it.

- **Sort**

Click **Sort** to arrange files by name or date.

The first letter of a recording file name indicates the recording type:

Initial	Recording Type	Initial	Recording Type
A	Alarm	S	Periodical Event
M	Motion	R	Regular Recording
N	Network Failure	V	Manual Trigger
T	Tampering	U	Audio Detection

Download

Select a video file from the Recording List and click **Download**. In the pop-up window, click the **AVI** file to play the video or save it to the desired location.

Recording

The Recording setting can be found under **System > Recording**.

Use this page to configure the camera's recording schedule.

Recording

Recording Storage

☒ SD Card
 ☐ Network Share

Recording Schedule

☐ Disable
 ☐ Always
 ☒ Only during time frame

	Weekday	Start time	Duration
1	☐ - ☐ - ☐ - ☐ - ☐ - ☐ - ☐	00:00	24:00
2	- - - - -	---	---
3	- - - - -	---	---
4	- - - - -	---	---
5	- - - - -	---	---
6	- - - - -	---	---
7	- - - - -	---	---
8	- - - - -	---	---
9	- - - - -	---	---
10	- - - - -	---	---

☒ Sun
 ☐ Mon
 ☐ Tue
 ☐ Wed
 ☐ Thu
 ☐ Fri
 ☒ Sat

Start time :
 Duration :

Recording Storage

Select the recording storage location:

- **SD Card**
- **Network Share**

Enable Recording Schedule

Select one of the following recording modes:

- **Always**
Records continuously to the selected storage.
- **Only during time frame**
Records during a specified schedule. Select the desired days, start time, and recording duration. The duration can be set from **00:00 to 168:59**.

Click **Save** to apply the schedule.

To delete a schedule, select it from the schedule list and click **Delete**.

Disable Recording Schedule

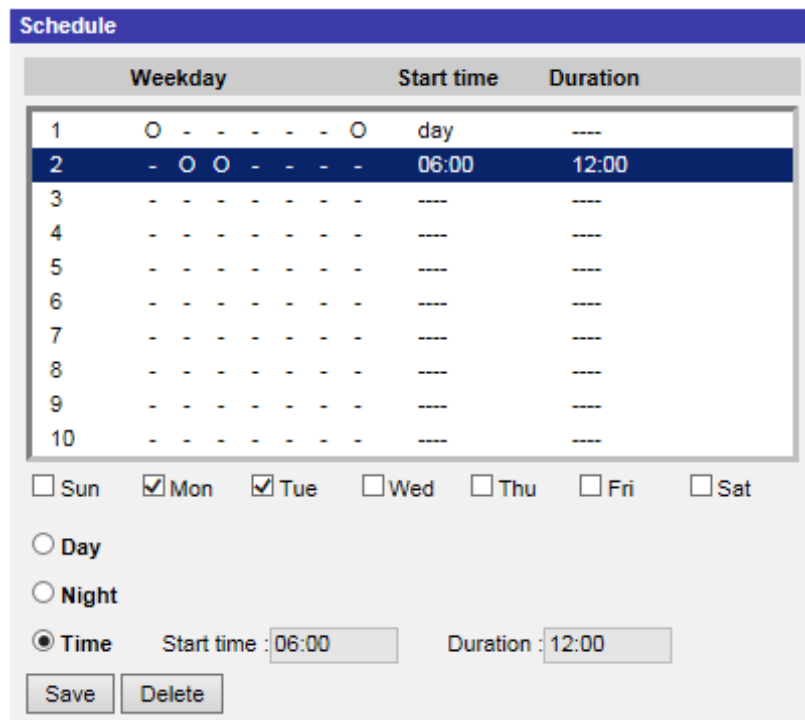
Select **Disable** to stop scheduled recording.

Click **Save** to apply the settings.

Schedule

The Schedule setting can be found under **System > Schedule**.

Use this page to create schedules for features such as **Alarm Switch**, **Motion Detection**, and **Network Failure Detection**. Up to **10 schedules** can be configured.



	Weekday	Start time	Duration
1	☐ - - - - - ☐	day	---
2	- ☐ ☐ - - - - -	06:00	12:00
3	- - - - -	---	---
4	- - - - -	---	---
5	- - - - -	---	---
6	- - - - -	---	---
7	- - - - -	---	---
8	- - - - -	---	---
9	- - - - -	---	---
10	- - - - -	---	---

☐ Sun ☒ Mon ☒ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

☐ Day
☐ Night
☒ Time

Start time : 06:00 Duration : 12:00

Schedule Setup

Step 1: Select a time frame from the list.

Step 2: Select the desired weekdays.

Step 3: Select a time mode: **Day**, **Night**, or **Time**.

- **Day** — Loads the camera profile when the IR cut filter is on.
- **Night** — Loads the camera profile when the IR cut filter is off.
- **Time** — Activates the schedule at a specified start time for the selected duration. The duration can be set from **00:00 to 168:59**.

Step 4: Click **Save** to save the schedule or **Delete** to remove the selected time frame.

NOTE: Select **By schedule** in the corresponding feature settings to activate the schedule.

Time Mode

- **Day:** Loads the camera's Day profile when the IR cut filter is on.
- **Night:** Loads the camera's Night profile when the IR cut filter is off.
- **Time:** Activates the schedule based on the specified start time and duration.

NOTE: Select **By schedule** in the corresponding feature settings to enable the schedule.

File Location (Snapshots and Web Recording)

The File Location setting can be found under **System > File Location**.

Users can choose where snapshots and web recordings are saved on the PC or hard drive. The default location is C:\ drive. Click **Save** to apply the selected location.

NOTE:

- Make sure the file path uses valid characters, such as letters and numbers.
- On Windows, run Internet Explorer as **Administrator** to use the Snapshot and Web Recording functions. Right-click the IE icon and select **Run as Administrator**.

Built-in Video Analytics

There are eleven built-in video analytics for users to implement. These functions include:

- Unattended Object Detection / Abandoned Object
- Forbidden Area Detection / Intrusion Detection
- Tampering Detection / Camera Sabotage
- Vehicle Incorrect Direction / Wrong Direction
- Object Loitering Detection
- Object Counting
- Missing Object Detection / Object Removal
- Stopped Vehicle Detection
- Face Detection
- Face Recognition
- Automatic License Plate Recognition

For general video analytics settings, see the **Video Analytics Standard Setting** section.

Abandoned Object (Unattended Object Detection)

Unattended Object or abandoned object detection detects objects placed within a defined zone and triggers the alarm if the object remains in the zone longer than the user-defined time allows.

Installation Requirement

Consider the following when installing the camera for analytics functions. Once the installation height is determined, zoom in or out the camera lens to meet the following requirements.

Installation Requirements	
Suggested Target Size	50x50 ~ 500 x 500 (@1080p)
Camera Mounting Height	The suggested camera installation height is 2 ~ 3 meters from the ground.
Detection Zone or Region of Interest (ROI)	The detection zone should be greater than the maximum size of the object to be detected.
Maximum Object Size	Should be larger than the object.
Minimum Object Size	Should be smaller than the object
Sensitivity	Adjust according to the on-site environment
Delay before alarm	The alarm trigger is delayed until the set number of seconds passed.

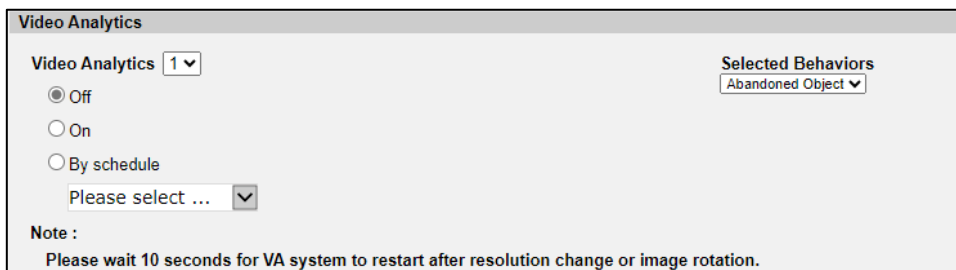
Scene Requirement

- Stationary or slow-moving irrelevant objects should not stay within the scene for a long time.
- The background should be simple and plain.
- If the background is a dynamic scenario, monitoring zones should be placed in a stable area.
- Note that swinging objects, like tall grass, tree leaves, and sliding doors, etc., or any distracting motions cause continuous modification of the images in the zone area, and thus may reduce analytics performance.
- Severe illumination changes, like turning on/off lights) or camera tampering might trigger false alarm.

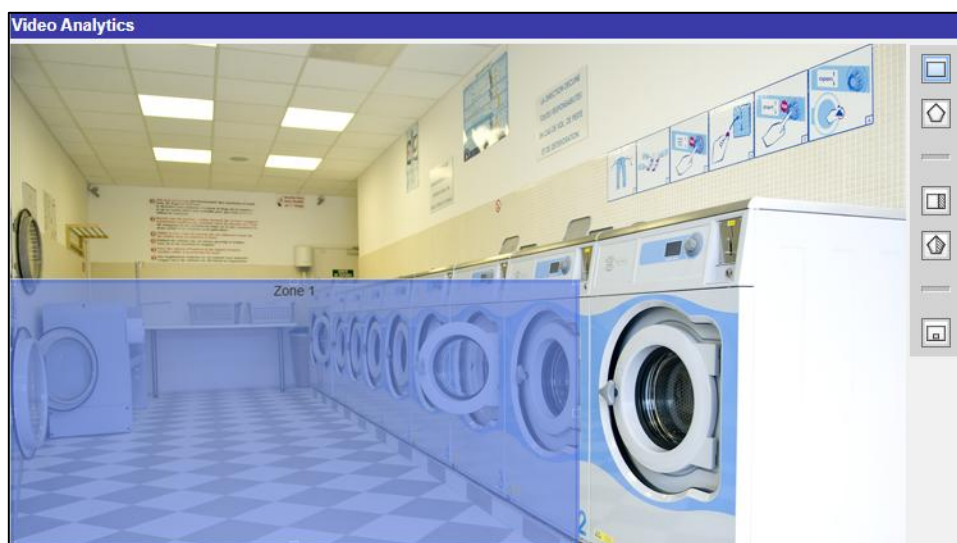
Configuration

When an unknown object is left in the detection zone over a specific period of time, the camera will trigger the alarm and/or send notification to users according to the configured behavior below.

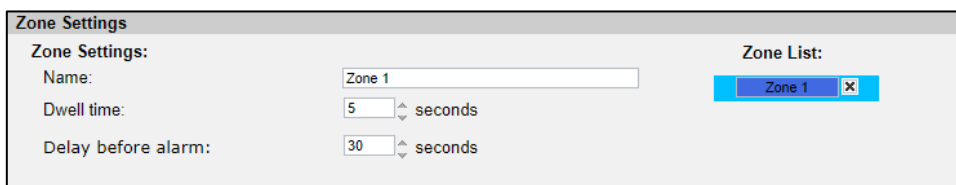
Go to **System > Events > Video Analytics**. Then follow the steps below to configure Unattended Object Detection.



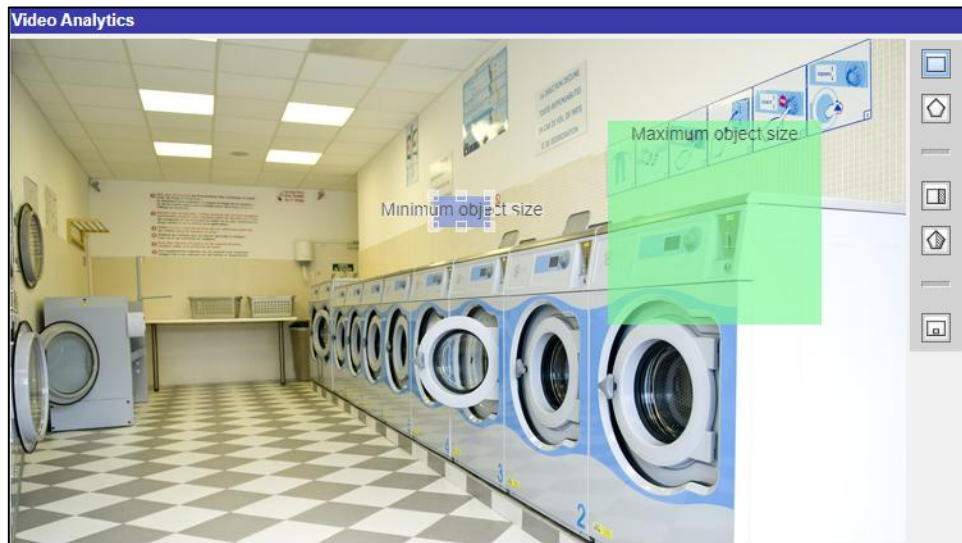
1. On **Video Analytics**, select stream **1** or **2**.
2. On **Selected Behaviors**, select **Abandoned Object**.
3. Click  or  to select a drawing tool and then draw the detection zone on the video panel.



4. Once a detection zone is drawn, the **Zone Settings** section appears. Define the zone and setup **Dwell time** and **Delay before alarm**.



5. Click  and define the minimum and maximum size of objects.



6. If needed, click  or  to draw areas where the objects will be ignored.
7. On the **Triggered Action** and **File Name** sections, configure the actions to take when the event occurs.
8. Click **Save** to apply and save the settings.

Intrusion Detection

Intrusion Detection detects and tracks objects that enter the user-defined zone of a scene, like a forbidden area, which triggers an alarm. It is suitable for both indoors and outdoors to track a few moving objects in broad areas. Note that the behavior will gradually adapt to the change of the monitoring environments like snow, fog, wind, and rain. Refer to the following to configure this function.

Installation Requirement

Consider the following when installing the camera for analytics functions. Once the installation height is determined, zoom in or out the camera lens to meet the following requirements.

Installation Requirements	
Camera Mounting Height	The suggested camera installation height is 2 ~ 3 meters from the ground.
Detection Zone Size or Region of Interest (ROI)	The detection zone size should be greater than the maximum size of the object to be detected.
Maximum Object Size	Should be larger than the object.
Minimum Object Size	Should be smaller than the object
Detectable Items	Human and Vehicle
Detection Direction	Up, down, left, right, top left, bottom left, top right, bottom right, all directions

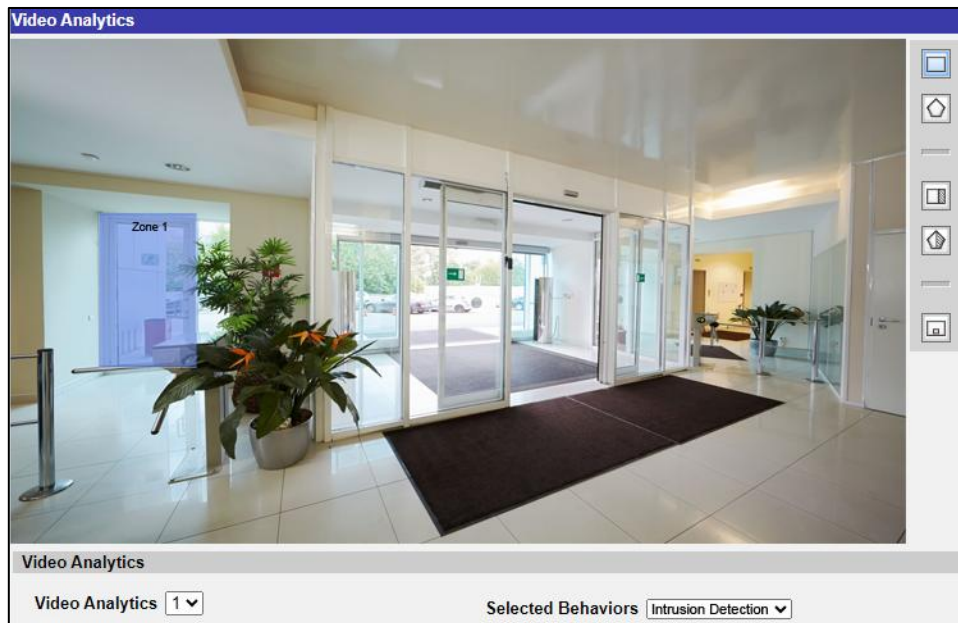
Scene Requirement

- There should be a sufficient distinction between the object and the background in order to make the object stand out from the scene.
- Postures other than upright position (e.g. crawling, crouching) would reduce the accuracy of human detection.
- Avoid overlapping objects in the scene. Otherwise, the object trajectory might be mixed up which will then cause inaccurate results.
- Obstruction on the image being detected will cause inaccurate detection results.

Configuration

When unknown objects enter the detection zone from a specified direction, the camera will trigger the alarm and/or send notifications to users.

To configure the camera configuration settings, go to **System > Events > Video Analytics**. Then follow the steps below to configure Intrusion Detection.



1. On **Video Analytics**, select stream **1** or **2**.
2. On **Selected Behaviors**, choose **Intrusion Detection**.
3. Click  or  and then draw the detection zone on the video panel.
4. Click  and then define the minimum and maximum size of objects.
5. Set the **Direction** from which the object will be coming from to trigger an intrusion.
6. Name the zone and configure **Dwell Time**.
7. On **Triggered Action** and **File Name** sections, select the event response or actions to take when intrusion detection is triggered.
8. Click **Save** to apply the settings.

Camera Sabotage

Camera sabotage detects obvious changes in the field of view, and triggers an alarm if the camera lens is obstructed by spray paint, a cloth, and the likes. Moreover, any unauthorized repositioning of the camera will also trigger an alarm.

Installation Requirement

Consider the following when installing the camera for analytics functions.

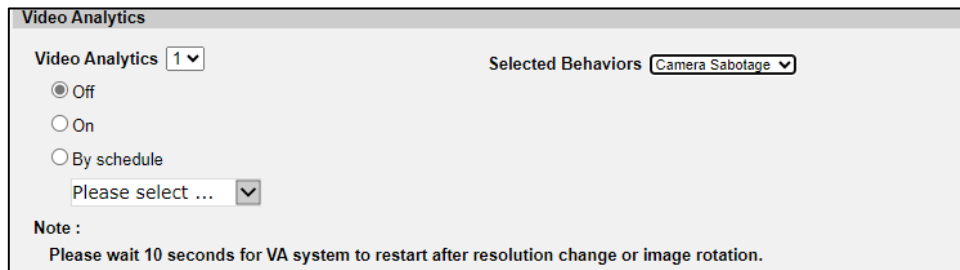
Installation Requirements	
Camera Mounting Height	No required installation height
Detection Zone Size	No required detection zone
Environment Illumination	Minimum environment illumination is 10 lux.

Scene Requirement

- There should be an obvious change before and after the camera is tampered with.
- Sudden illumination changes might trigger a false alarm.
- Constant scene changes might trigger a false alarm.

Configuration

When there is a deliberate attempt to damage the camera lens or something similar, the camera will trigger the alarm according to what behaviors are configured.



1. Go to **System > Events > Video Analytics**.
2. On **Video Analytics**, select stream **1** or **2**.
3. On **Selected Behaviors**, choose **Camera Sabotage**.
4. Set **Sensitivity**, **Dwell Time** and **Delay Before Alarm**.
5. On **Triggered Action** and **File Name** sections, select the event response or actions to take when camera sabotage occurs.
6. Click **Save** to apply the settings.

Wrong Direction

Wrong Detection triggers an event alarm when a person or vehicle moves in a particular direction. The ideal applications include airports, entrance/exit doors, fences, etc.

Installation and Configuration Requirements

Consider the following when installing the camera for analytics functions. Once the installation height is determined, zoom in or out the camera lens to meet the following requirements.

Installation Requirements	
Camera Mounting Height	The suggested camera installation height is 2 ~ 3 meters from the ground.
Detection Zone Size or Region of Interest (ROI)	The detection zone size should be greater than the maximum size of the object to be detected.

Below are the settings that must be configured in order to ensure detection.

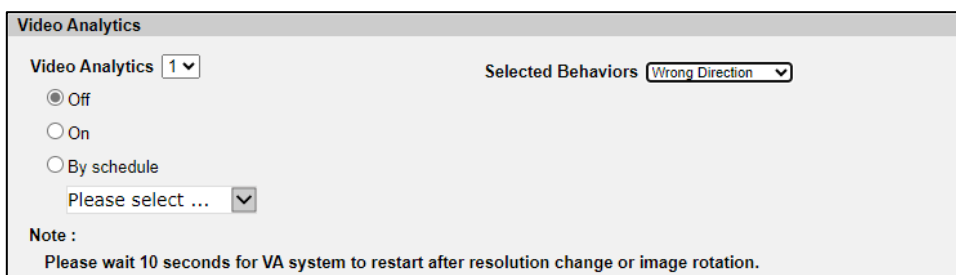
Configuration Requirements	
Detectable Items	Human and Vehicle
Detection Direction	Up, down, left, right, top left, bottom left, top right, bottom right, all directions

Scene Requirement

- There should be an obvious change before and after the camera is tampered.
- Sudden illumination changes might trigger a false alarm.
- Constant scene changes might trigger a false alarm.

Configuration

When there is a deliberate attempt to damage the camera lens or the likes, the camera will trigger the alarm according to what behaviors are configured.



1. Go to **System > Events > Video Analytics**.
2. On **Video Analytics**, select stream **1** or **2**.
3. On **Selected Behaviors**, choose **Wrong Direction**.
4. Click  or  to select a drawing tool and then draw the detection zone.

5. Name the zone and set up **Dwell Time**.
6. On **Zone Settings**, select the direction to forbid entering. Based on the direction selected, once a person goes to that direction, the alarm will be triggered.
5. On **Triggered Action** and **File Name** sections, select the event response or actions to take when this event is triggered.
6. Click **Save** to apply the settings.

Loitering Detection

Loitering detection is an event that identifies people or vehicle that stay or loiter in a defined zone longer than the specified time. This event is effective in real-time notifications of suspicious persons hanging around ATMs, stairwells, and school grounds.

Installation and Configuration Requirements

Consider the following when installing the camera for analytics functions. Once the installation height is determined, zoom in or out the camera lens to meet the requirements and configure the settings as below:

Installation Requirements	
Camera Mounting Height	The suggested camera installation height is 2 ~ 3 meters from the ground.
Detection Zone Size or Region of Interest (ROI)	The detection zone size should be greater than the maximum size of the object to be detected.
Maximum Object Size	Should be larger than the object.
Minimum Object Size	Should be smaller than the object

Below are the settings that must be configured in order to ensure detection.

Configuration Requirements	
Detectable Items	Human and Vehicle
Sensitivity	Adjust settings according to the actual environment
Detection Direction	Up, down, left, right, top left, bottom left, top right, bottom right, all directions
Delay Before Alarm	Set this to trigger the alarm after a specified delay (in seconds)

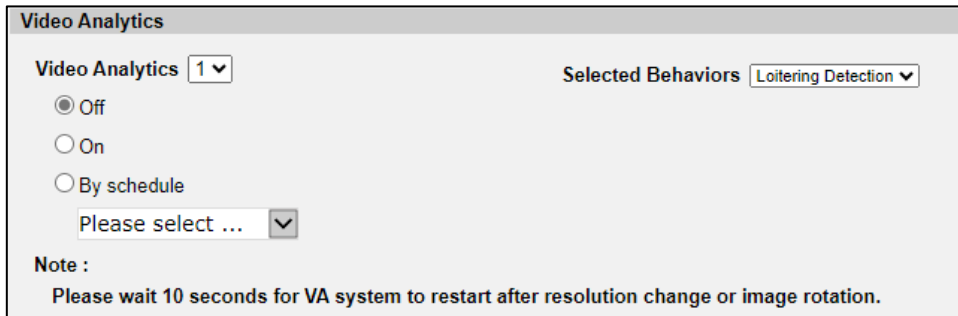
Scene Requirement

- There should be sufficient difference between the object and the background in order to make the object stand out from the scene.
- Postures other than upright position (e.g. crawling, crouching, etc.) would reduce the accuracy of human detection.

- Avoid overlapping of objects. Otherwise, the trajectory might be mixed up which may reduce accuracy.
- Blocked objects may reduce accuracy.

Configuration

When there is a suspicious person or vehicle within the detection zone for longer than the defined time, the camera will trigger the alarm and send a notification according to the configured event response.



1. Go to **System > Events > Video Analytics**.
2. On **Video Analytics**, select stream **1** or **2**.
3. On **Selected Behaviors**, choose **Loitering Detection**.
4. Click  or  to select a drawing tool and then draw the detection zone.
5. Name the zone and set up **Dwell Time** and **Delay before alarm**.
6. Click  and then define the minimum and maximum size of objects.
7. On **Triggered Action** and **File Name** sections, select the event response or actions to take when this event is triggered.
6. Click **Save** to apply the settings.

Object Counting

Object Counting counts the number of objects that enter a user-defined zone. This feature can be used to count people at a store entrance or exit. It is also suitable to monitor vehicle traffic on highways, streets, parking lots, etc. Object counting can detect persons and vehicles.

Installation and Configuration Requirement

Consider the following when installing the camera for analytics functions. Once the installation height is determined, zoom in or out the camera lens to meet the requirements and configure the settings as below:

Installation Requirements	
Camera Mounting Height	The suggested camera installation height is 2 ~ 3 meters from the ground.
Detection Zone Size or Region of Interest (ROI)	The detection zone size should be greater than the maximum size of the object to be detected.
Maximum Object Size	Should be larger than the object.
Minimum Object Size	Should be smaller than the object

Below are the settings that must be configured in order to ensure detection.

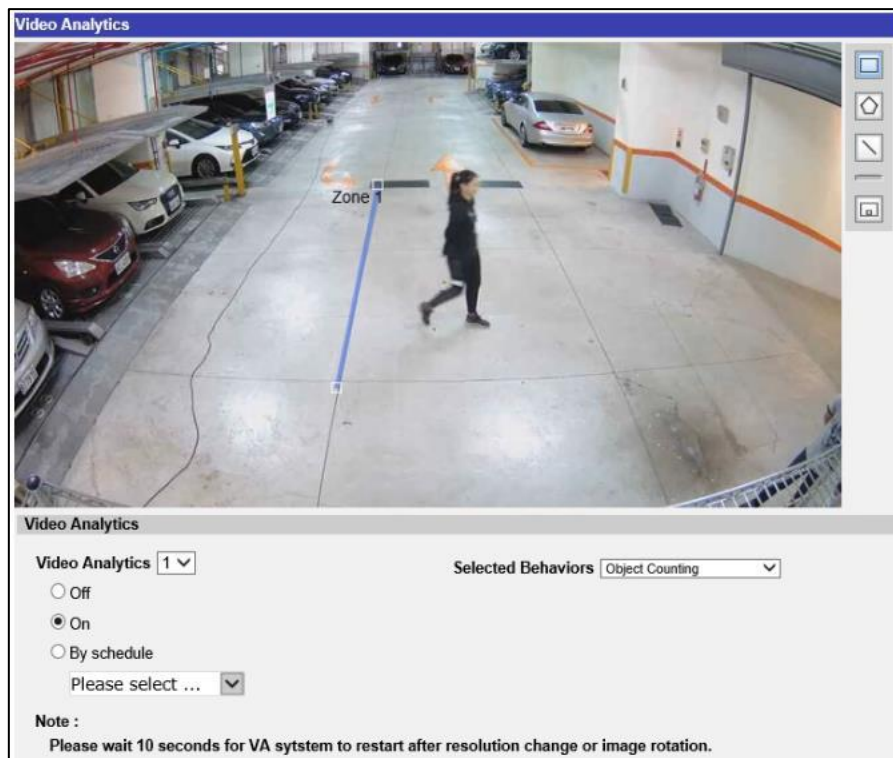
Configuration Requirements	
Detectable Items	Human and Vehicle
Detection Direction	Up, down, left, right, top left, bottom left, top right, bottom right, all directions

Scene Requirement

- There should be a sufficient distinction between the object and the background in order to make the object stand out from the scene.
- Postures other than upright position (e.g. crawling, crouching) would reduce the accuracy of human detection.
- Avoid overlapping objects in the scene. Otherwise, the object trajectory might be mixed up which will then cause inaccurate results.
- Obstruction to the image being detected will cause inaccurate detection results.

Configuration

To configure the camera settings, go to **System > Events > Video Analytics**. Then follow the steps below to configure Object Counting.



1. On **Video Analytics**, select stream **1** or **2**.
2. On **Selected Behaviors**, choose **Object Counting**.
3. Click  or  or  and then draw the detection zone or line on the video panel.
4. Click  and then define the minimum and maximum size of objects (for person).
5. Name the zone.
6. Set the **Direction** from which the object will be coming from to trigger an intrusion.
7. On **Alarm at**, configure the number of objects. When this number is reached, the alarm will be triggered.
8. Configure **Dwell Time**.
9. Check **Reset counter on alarm** to reset the object counting once an alarm is triggered. Or, uncheck this box to disable this function.
7. On **Triggered Action** and **File Name** sections, select the event response or actions to take when the alarm is triggered.
8. Click **Save** to apply the settings.

Object Removal

Object Removal triggers an alarm when a monitored object is removed from a user-defined zone. The ideal size of the object to be monitored should occupy a major proportion of the detection zone, such as a painting from a wall or a statue on a pedestal, etc.

Installation and Configuration Requirement

Consider the following when installing the camera for analytics functions. Once the installation height is determined, zoom in or out the camera lens to meet the requirements and configure the settings as below:

Installation Requirements	
Camera Mounting Height	The suggested camera installation height is 2 ~ 3 meters from the ground.
Detection Zone Size or Region of Interest (ROI)	The detection zone size should be the same or slightly greater than the size of the object to be monitored.

Below are the settings that must be configured in order to ensure detection.

Configuration Requirements	
Detectable Items	Human, Vehicle, Object
Sensitivity	At least 70% (recommended)

Scene Requirement

- Three-dimensional objects are considered better targets for detection compared to flat objects.
- Other objects unrelated to the scene passing in front of the target might trigger false alarm.
- Camera tampering or severe illumination changes might trigger false alarm.

Configuration

To configure the camera settings, go to **System > Events > Video Analytics**. Then follow the steps below to configure Object Removal.



1. On **Video Analytics**, select stream **1** or **2**.
2. On **Selected Behaviors**, choose **Object Removal**.
3. Click  or  and then draw the detection zone on the video panel.
4. Name the zone, set **Dwell Time** and **Delay before alarm**.
5. On **Triggered Action** and **File Name** sections, select the event response or actions to take when the alarm is triggered.
6. Click **Save** to apply the settings.

Stopped Vehicle

Stopped Vehicle detects vehicles which are occupying a specific area, such as a “no parking zone”. When a vehicle stays inside the area for longer than the user-defined period of time, the alarm is triggered. This function is ideal for parking enforcement, identifying suspicious parking, finding traffic lane breakdowns, and spotting vehicles waiting at gates.

Installation and Configuration Requirement

Consider the following when installing the camera for analytics functions. Once the installation height is determined, zoom in or out the camera lens to meet the requirements and configure the settings as below:

Installation Requirements	
Camera Mounting Height	The suggested camera installation height is 2 ~ 3 meters from the ground.
Detection Zone Size or Region of Interest (ROI)	The detection zone size should be the same or slightly greater than the size of the object to be monitored.
Maximum Object Size	Should be larger than the object.
Minimum Object Size	Should be smaller than the object

Below are the settings that must be configured in order to ensure detection.

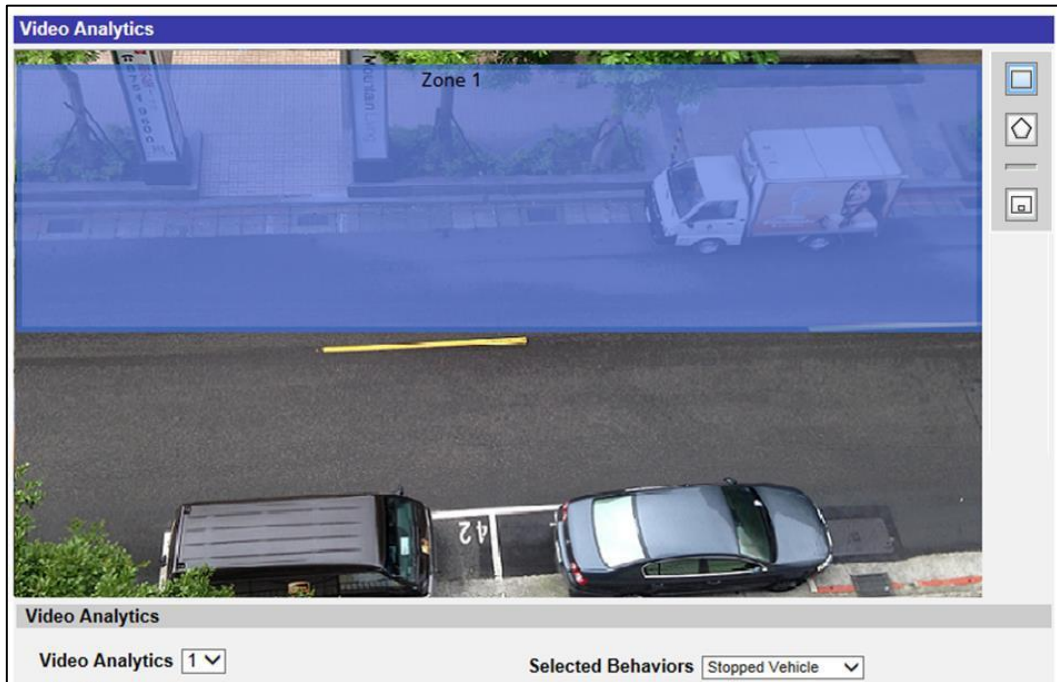
Configuration Requirements	
Detectable Items	Vehicle
Delay Before Alarm	Set this to trigger the alarm after a specified delay (in seconds)

Scene Requirement

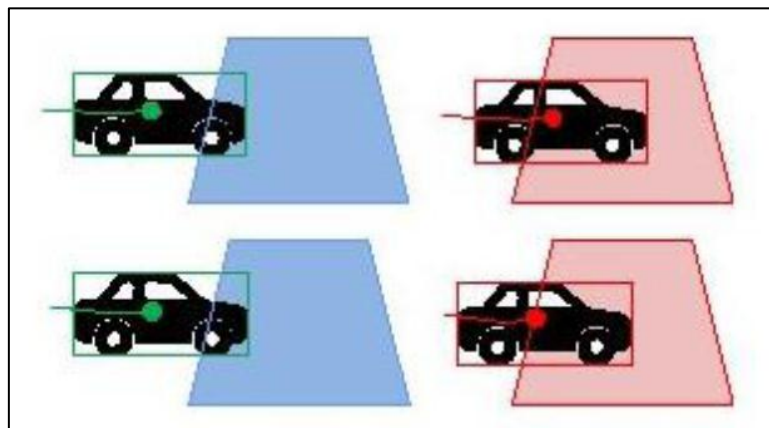
- There should be a sufficient distinction between the object and the background in order to make the object stand out from the scene.
- Avoid overlapping objects in the scene. Otherwise, the object trajectory might be mixed up which will then cause inaccurate results.
- Obstruction to the image being detected will cause inaccurate detection results.

Configuration

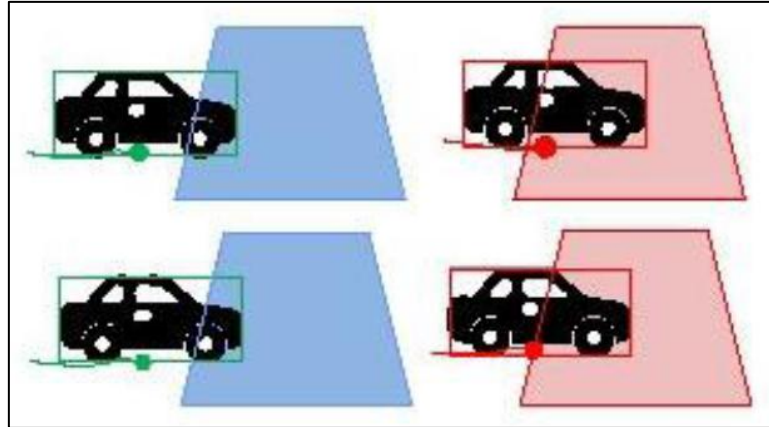
To configure the camera settings, go to **System > Events > Video Analytics**. Then follow the steps below to configure Stopped Vehicle.



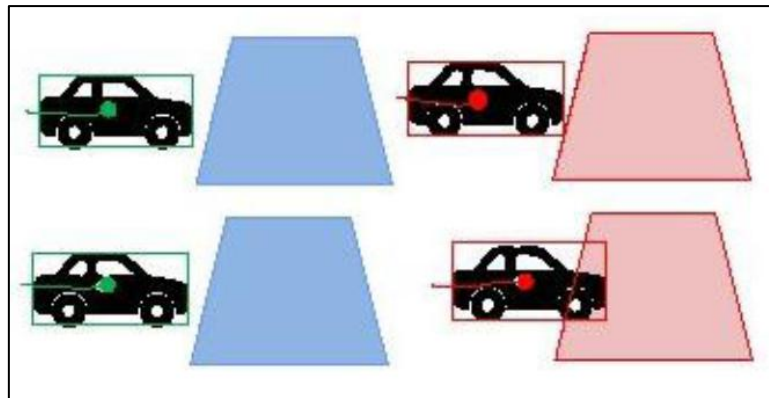
1. On **Video Analytics**, select stream **1** or **2**.
2. On **Selected Behaviors**, choose **Stopped Vehicle**.
3. Click  or  and then draw the detection zone on the video panel.
4. On **Zone Settings** section, name the zone, set **Dwell Time** and **Delay before alarm**.
5. Select one of the five (5) the **Trigger type** options:
 - a. **Center**: The camera will trigger the alarm when the center point of the vehicle touches or goes within the detection zone.



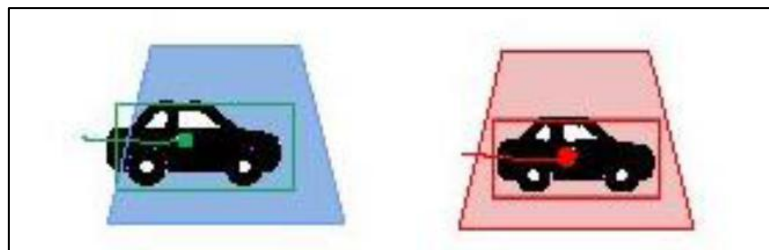
- b. **Bottom center**: The camera will trigger the alarm when the bottom center point of the vehicle touches or goes within the detection zone.



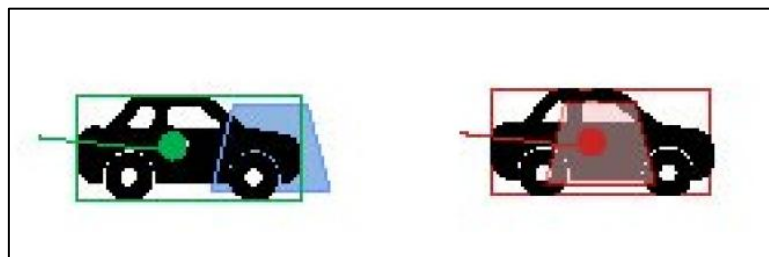
- c. **Edge:** The camera will trigger the alarm when the edge of the vehicle touches or goes within the detection zone.



- d. **Fully inside:** The camera will trigger the alarm when the vehicle goes fully within the detection zone.



- e. **Fully cover:** The camera will trigger the alarm when the vehicle fully covers the detection zone.



6. Click  and then define the minimum and maximum size of objects (for person).
7. On **Triggered Action** and **File Name** sections, select the event response or actions to take when the alarm is triggered.
8. Click **Save** to apply the settings.

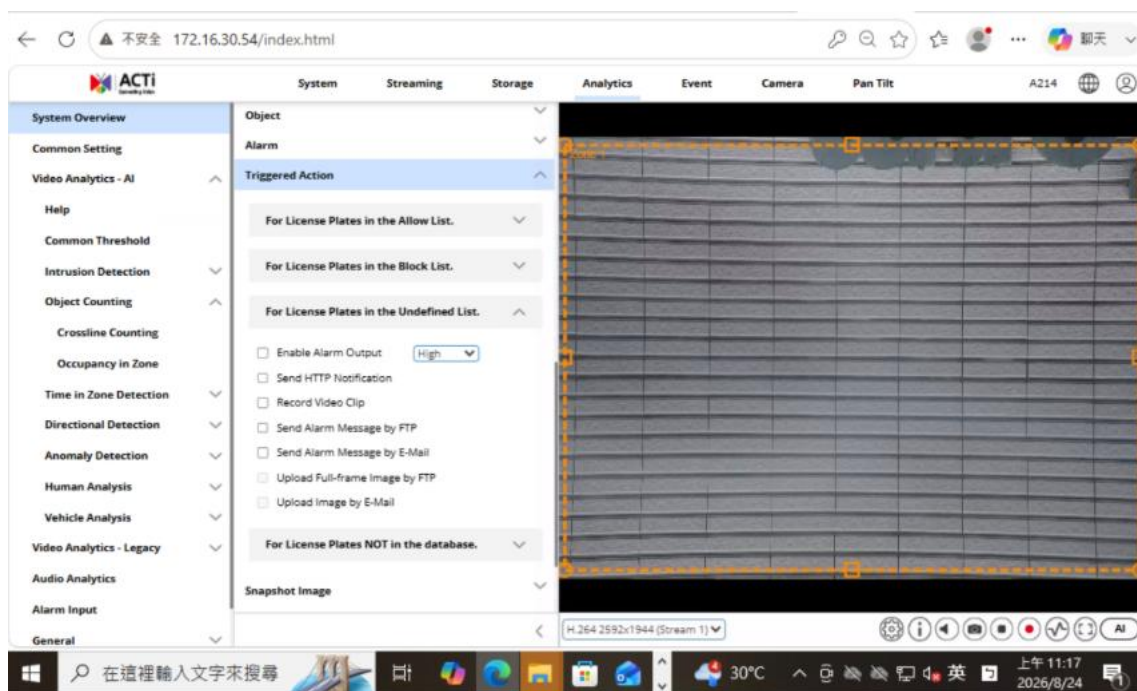
Automatic License Plate Recognition (ALPR)

Cameras with built-on Automatic License Plate Recognition (ALPR) can recognize license plates automatically, so the user does **not** need to pre-enter the plate information.

The database is only required if the user wants to classify plates into **Allow List**, **Block List**, **Undefined List**, or **Groups**.

Different **Triggered Actions** can be configured independently for Allow List, Block List, Undefined List, and license plates **NOT** in the database.

- Available Triggered Actions include:
- Alarm Output
- HTTP Notification
- Record Video Clip
- Alarm Message by FTP
- Alarm Message by E-mail
- Upload Full-frame Image by FTP
- Upload Image by E-mail



If a plate is assigned to a **Group**, the Group information can also be included in the **ONVIF event**.



Copyright © 2020, ACTi Corporation All Rights Reserved

7F, No. 1, Alley 20, Lane 407, Sec. 2, Ti-Ding Blvd., Neihu District, Taipei, Taiwan 114, R.O.C.

TEL : +886-2-2656-2588 FAX : +886-2-2656-2599

Email: sales@acti.com