User Guide

Roughneck® AI V2000D-PTZ

Outdoor Vandal PTZ Dome Camera

XX320-01-02

Vicon Industries Inc.
Tel: 631-952-2288) Fax: 631-951-2288
Toll Free: 800-645-9116
24-Hour Technical Support: 800-34-VICON (800-348-4266)
UK: 44/(0) 1489-566300
www.vicon-security.com

Table of Content

Connection 1
Live View 3
Playback 6
Configuration 8
1. Encode 8
2. Image 11
3. Video 16
4. Network 20
5. System 31
6. Account 37
7. Event Source 40
8. Video Analytics: V2002D-PTZ Only 49
9. Video Analytics: V2005D-PTZ Only 62
10. Event Setting 72
11. PTZ Settings 80
Appendix 1: Continuous Recording to an SD Card 90
Vicon Standard Equipment Warranty 94

Connection

Accessing the Camera

The camera can be accessed directly from its web page or using Vicon's PRONTO Device Manager, which can be found on Vicon's website. Note that when accessing the camera for the first time, a message will display to reset the password.

Since this is a network-based camera, an IP address must be assigned. The camera's default IP address is obtained automatically through a DHCP server in your network; be sure to enable DHCP in "Network Settings." If DHCP is not available, the camera will use APIPA (link-local address); IPv4 link-local addresses are assigned from address block 169.254.0.0/16 (169.254.0.0 through 169.254.255.255).

Connecting from a Computer

Connecting from a Computer

Make sure the camera and your computer are in the same subnet.

Check whether the network available between the camera and the computer by executing ping the default IP address. To do this, simply start a command prompt (Windows: from the "Start Menu", select "Program". Then select "Accessories" and choose "Command Prompt"), and type "Ping and then type your IP address. If the message "Reply from..." appears, it means the connection is available.

Start a browser, e.g., Chrome, and enter IP address. A login window as shown below should pop up. In the window, enter the default user name: ADMIN; it is required to change the password when you login for the first time for added security, which requires at least 8 characters including 1 uppercase letter, 1 special character, alphanumeric characters to log in.

Further administration on the unit can be found in "Configuration."

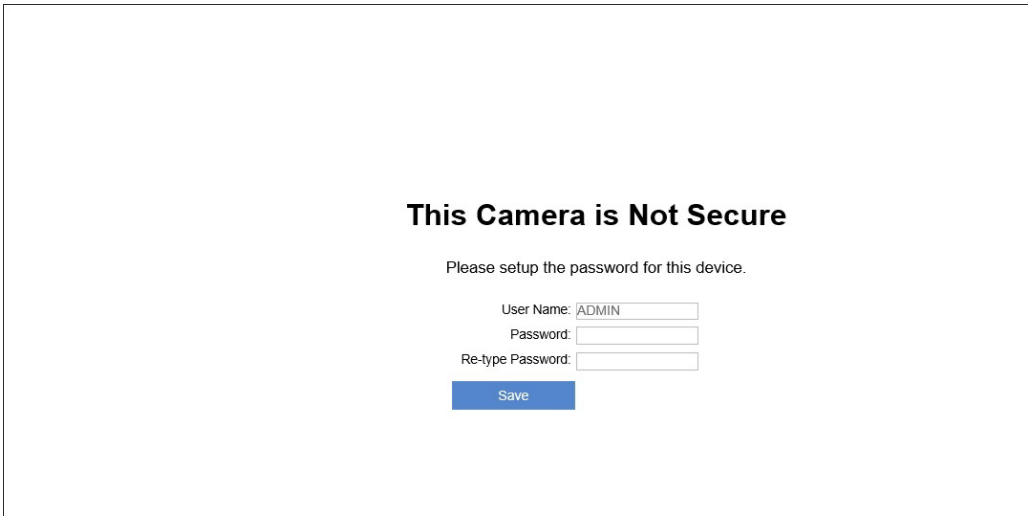


Figure: Login Window

PRONTO Device Manager

PRONTO is Vicon's device manager (Discovery tool) that can be used to discover all Vicon cameras on a system.

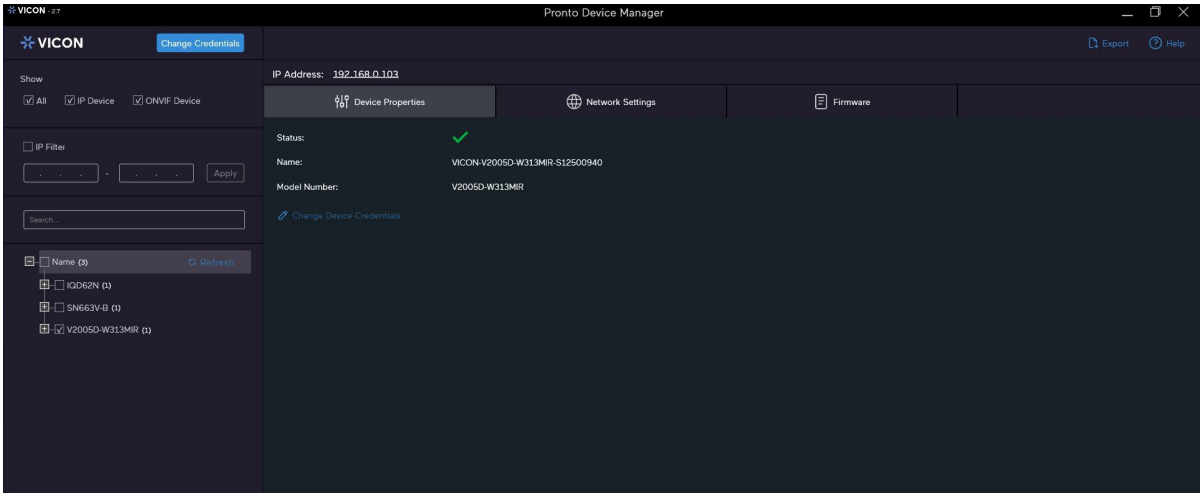


Figure: PRONTO Interface

- Upon startup of the PRONTO Device Manager, the tool's auto-discovery function generates a list of the discovered cameras on the network in a resource list.
- There are a variety of filtering options, including filter by All Devices/IP Device/ONVIF Device; IP range or text.
- There are tabs for Device Properties, Network Settings and Firmware.

Live View

After accessing and logging in to the IP address of the camera, there are 3 main options on the upper left side: "**Live View**," "**Playback**" and "**Configuration**." The upper right corner indicates the current user level and has the "Logout" option, which allows user to log out by clicking it. In addition, the dropdown menu beside the Configuration is used for changing the UI language. This chapter mainly focuses on Live View; later chapters will detail Playback and Configuration.

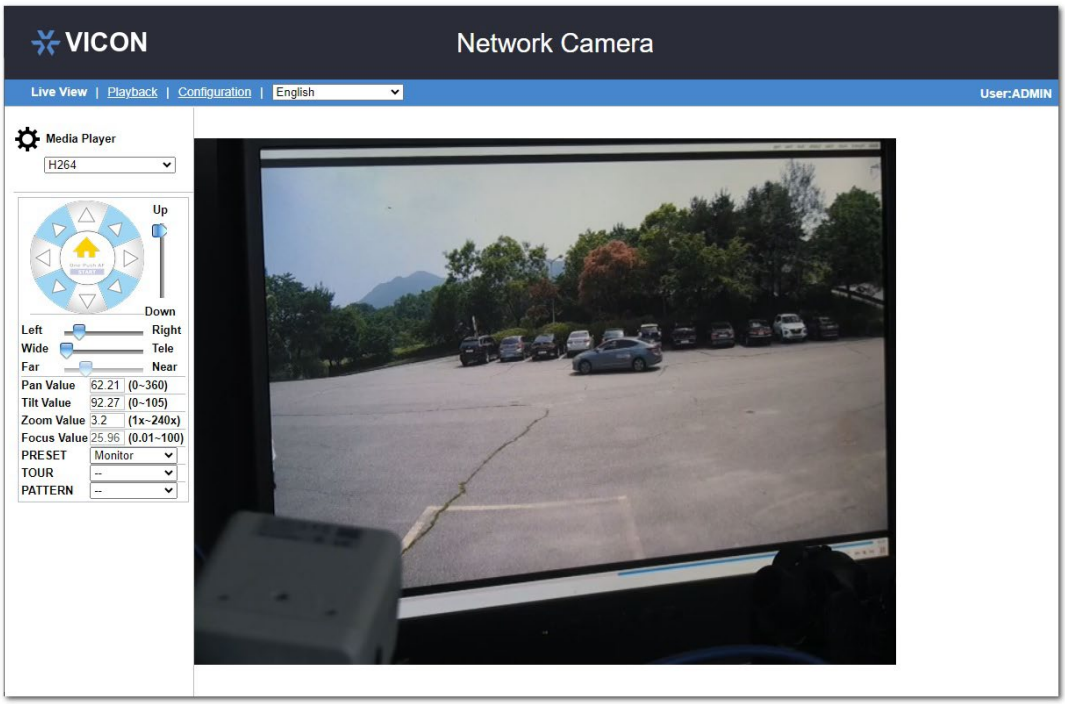


Figure: Live View (without analytics)

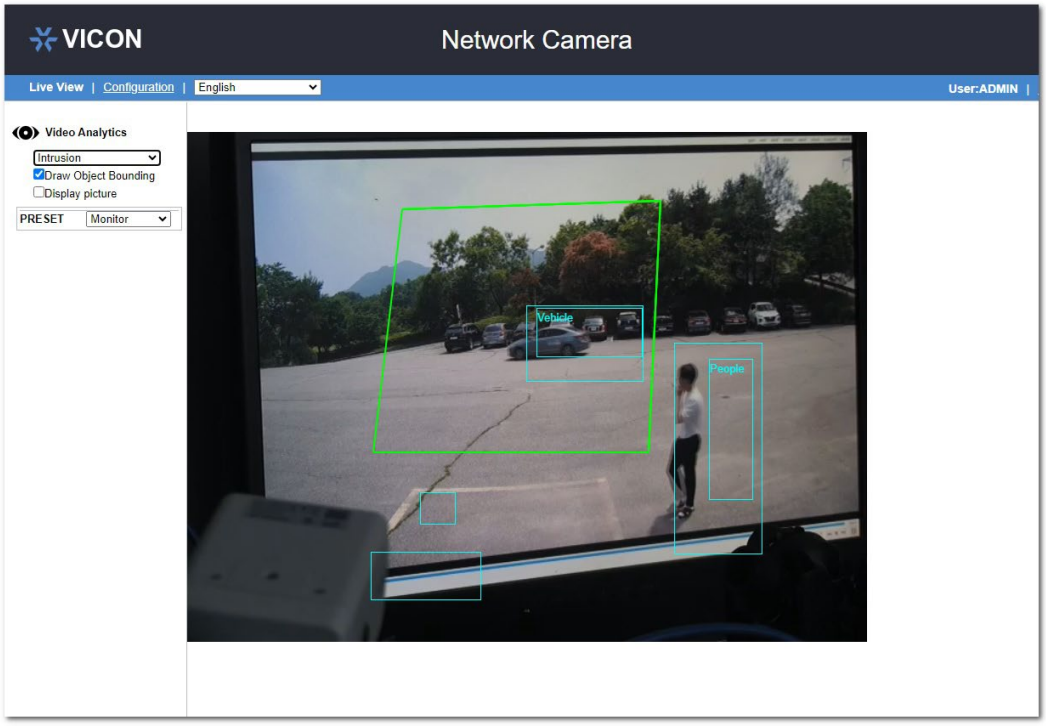


Figure: Live View (with analytics)

In "**Live View**" page, user will have access to real-time Live View display.

The drop-down menu under "**Media Player**" title consists of 2 options for display: **JPEG** and **H.264**. JPEG offers a broad range of browser options, including Chrome, Opera, etc., but has lower frame rate display. Additionally, in JPEG mode a Snapshot button is provided for users to take a still picture and save it in a predefined folder.

Video Analytics

- Select a Video Analytics (VA) function from the dropdown menu. Make sure that the selected VA function is enabled in "Video Analytics" section. When "Off" is selected, the camera is not performing any VA function.
- Draw Object Bounding: Check this box to allow camera to activate motion detection and draw an area around the detected object. This function can be used only when a VA function is activated.
- Display Picture: When an object enters the area, an easily identifiable icon of a person or vehicle (rather than text) displays, showing its movement until it exits the area.

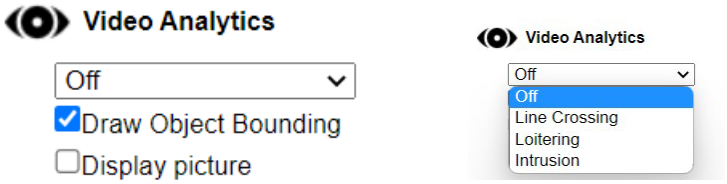


Figure: Video Analytics Panel

PTZ Control Panel

Whether in Live View or Configuration, user can always see the PTZ Control Panel on the lower-left side of window. The PTZ Control Panel allows quick access for execution of Pan, Tilt, Zoom and Focus movements, as well as Preset, Patrol and Pattern actions.

Note	• Refer to "*11.4 Preset*", "*11.5 Patrol*" and "*11.6 Pattern*" for details on Preset, Patrol and Pattern.

Figure: Pan/Tilt Control

Use the Pan/Tilt Control to pan and/or tilt camera in up/down/left/right/up right/up left/down right/down left directions to adjust camera view. Click once to perform the movement once. Clicking and holding allows continuous movement. Click the center part of Pan/Tilt Control to go to home view.

In addition, the user can adjust camera view using the options listed below.

Item	Option/Range	Description
Up - Down	0 ~ 105	Click and drag to tilt camera view.
Left - Right	1 ~ 360	Click and drag to pan camera view
Wide - Tele	1x ~ 120x (up to 240x based on Digital Zoom Limit)	Click and drag to zoom in/out camera view
Far - Near	1 ~ 100	Click and drag to adjust focus of camera view
Pan Value	1 ~ 360	Enter a value for pan angle
Tilt Value	0 ~ 105	Enter a value for tilt angle
Zoom Value	1x ~ 120x (up to 240x based on Digital Zoom Limit)	Enter a value for zoom depth
Focus Value	1 ~ 100	Enter a value for focus depth
Preset	1 ~ 128	Select a preset action
Patrol	1 ~ 4	Select patrol action
Pattern	1 ~ 4	Select pattern action

Playback

The camera provides a method to play video stored on micro SD card.

Due to compatibility issues related to video and audio formats; when playing video stored on micro SD Card, it is highly recommended to use Chrome or Safari browser along with H.264 codec, since these browsers support H.264 format. Remember that both camera and browser must support same format; therefore, it is possible to use any other browser along with H.265 codec, as long as both camera and browser support H.265 format.

After clicking on the playback function on the upper left side next to Live View, the page displays.

Storage device: SD Card

This camera supports a micro SD card storage device.

Event Type: Network Loss/Schedule/Tamper/Motion/Alarm/Audio

After selecting the edge storage, videos can be searched based on type of events that triggered video recording, and date and time recording was stored. Check the boxes to select the type of events that might trigger the video you are searching for.

Date & Time

User can select the exact date and time segment to search for recorded video, by clicking on a date on the calendar and entering time, respectively. The selected date will turn into a blue background on the calendar. The current date has a light brown background. Finally click the search button to start searching for videos on timeline area, according to the parameters chosen.

Timeline: 0.5 ~ 6 (hours)

Interval is used for adjusting the time range of timeline area in terms of hours; each step from timeline changes half hour in timeline area. Timeline helps user to get more details and a larger scale view of timeline area for easier search. 6 hours allows search in larger scale while 0.5 hour allows more details.

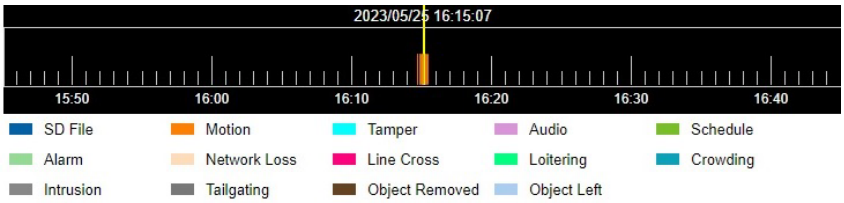


Figure: Timeline Area

User can click, and then drag left or right to see other parts of the timeline area. Based on the search configuration, if there is a video list on micro SD card, it will be shown on timeline area in different colors, sizes and times based on type, duration and time recorded, respectively. Refer to the illustration below timeline area to know the relation between type and color.

Selected types will be shown in timeline area according to their respective color bars, while types that are not selected will be shown in dark blue bars represented as "SD File."

Current or filtered date and time are shown at the upper center of timeline, where there is a vertical yellow line that represents the center of timeline area.

Display/Playback Toolbar

Figure: Display and Playback Toolbar

- To play a video, simply hover over a color bar on timeline area until a hover box displays; then click on the color bar for the recorded video to automatically start playing on the display.
- While the video is playing, user can hover over the displaying video to activate playback toolbar.

Configuration

After clicking "**Configuration,**" the screen will display as below, with several menu options on the left side for users to configure. These will be explained one by one in the following chapters.

1. Encode

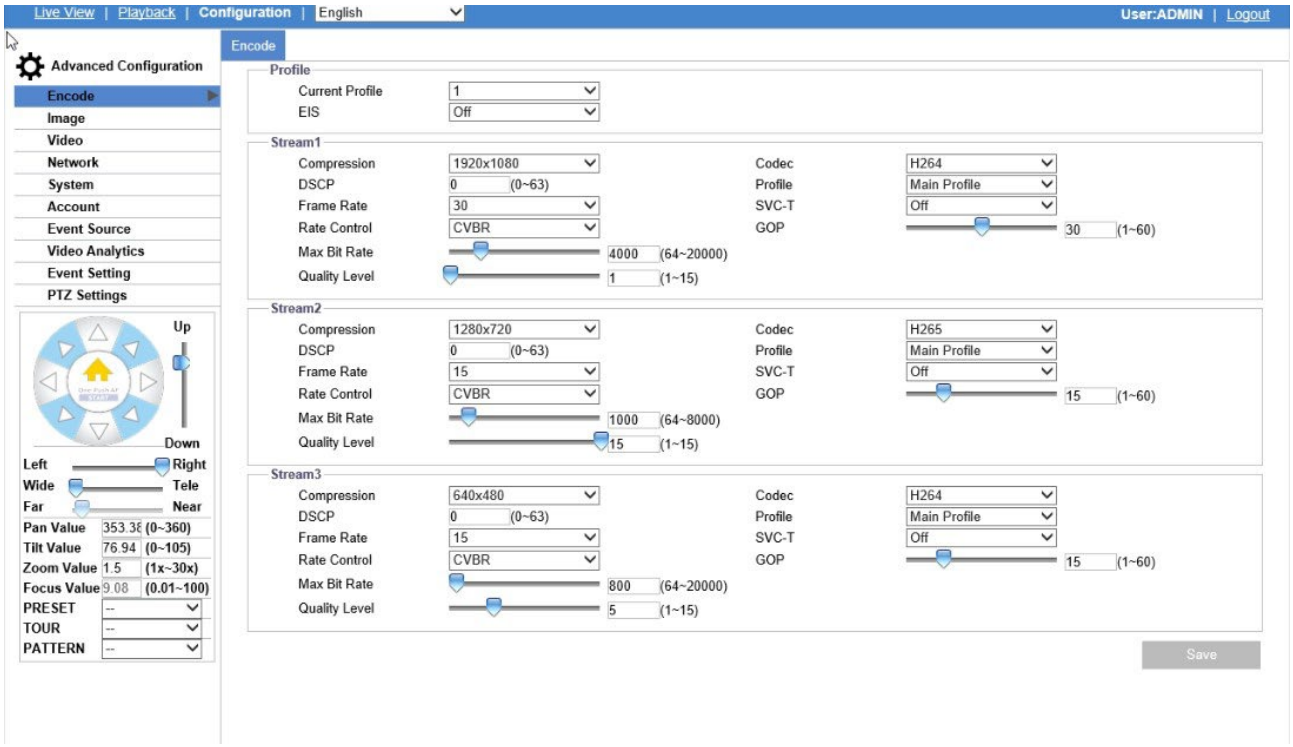


Figure: Encode Settings

Profile and Streams

Current Profile: 1/2/3

It is strongly recommended to define different settings under each stream to maintain better video transmission for varied network environments and applications. By default, there are 3 profiles, and each profile contains 3 streams for individual configuration. The detailed configurations for each stream are described in detail below.

EIS: On/ Off

When EIS is turned on, if shaking of the camera is detected, the software can compensate by adjusting the image from blurring, fine-tuning some functions, such as shutter time.

Stream

Compression

As an example, compression options for the 2 MP models are 1920x1080, 1280x960, 1280x720, 800x600, 640x480, 640x360, 320x240. Higher resolution values are model dependent and frame rates correspond to the resolution, streams and codec selected.

Note	•	Refer to the datasheet for the camera model for details.

DSCP: 0 ~ 63

To classify and manage network traffic and provide quality of service (QoS) on modern IP networks, Differentiated Services Code Point (DSCP) is a computer networking architecture that specifies a resource allocation to each device on a priority-based pattern for ideal bandwidth management. The bigger the value, the higher priority it will be.

Frame Rate: 30 ~ 1

Choose desired frames per second from the dropdown menu.

Rate Control: CBR/VBR/CVBR

Choose one of the Rate Control modes depending on different situations. Higher bit rate value will result in better image quality with bigger file size and therefore consume more network bandwidth, while lower bit rate value has less loading on network bandwidth due to smaller file size but with inferior image quality.

CBR Bit Rate/Max Bit Rate: 64 ~ 20000 (for H.264 codec); 64 ~ 8000 (for H.265 codec)

The default bit rate synchronizes with the maximum resolution. It is recommended to use the default bit rate, as it provides a better balance between image quality and network bandwidth.

When bit rate value lower than default bit rate is selected, the image quality may deteriorate.

When selecting bit rate higher than default bit rate, there is a correlation between resolution and selected bit rate. Higher maximum resolution cameras are better suited to selection of bit rate higher than default bit rate than lower maximum resolution cameras.

Note	• CBR Bit Rate and Max Bit Rate options are available only when H.264 or H.265 codec is selected.

Quality Level: VBR: 1 ~ 10; MJPEG: Low/Mid/High

Select the Quality Level number from 1 to 10 for H.264/H.265 Codec with VBR Rate Control selected, or Quality Level Low/Mid/High for MJPEG Codec. "High" or "larger value" produces the highest image quality but increases the file size. By contrast, "low" or "smaller value," produces the lowest image quality with decreased file size and network bandwidth consumption. For CVBR, select the limitation on the bit rate.

Note	• Quality Level option is available only when VBR Rate Control is selected or when MJPEG Codec is selected.

Codec: MJPEG/H.264/H.265

- MJPEG: Each video frame is individually compressed as single jpeg image with full-scale contents and can be retouched easily. However, this results in larger file size and therefore tends to lose frames under limited network bandwidth.
- H.264: This widespread video compression format adopts intelligent technology to record variations in each frame rather than record each full frame. As a result, less network bandwidth is required, and file size tends to be smaller compared with the MJPEG codec.
- H.265: Also known as HEVC (High Efficiency Video Coding), H.265, the latest video compression standard, provides almost double the compression ratio at the same level of video quality compared with H.264. It efficiently reduces the redundant areas among different frames by using pattern comparison, enhanced difference-coding areas and variable-block-size segmentation.

Note	• Rate Control, Max Bit Rate, CBR Bit Rate Profile, SVC-T, and GOP options are NOT available when MJPEG Codec is selected.

Profile: High Profile/Main Profile

There are 2 different kinds of profiles for H.264 codec and 1 profile for H.265 codec compression ratios, where the protocol for each type varies. H.264 Codec supports Main Profile and High Profile profiles. H.265 Codec supports Main Profile only. Users can select the preferred one for their applications or contact IT personnel for more information.

SVC-T: On/Off

SVC-T supports the FPS adjustment on the client side, for example, users can adjust the FPS to 7.5, 15, 30, etc. Select Off or adjustment; it is recommended to select Off .

GOP: 1 ~ 60/ 1 ~ 50

Group of Picture (GOP) length. Select the GOP length number from 1 to 60 for 60Hz camera type or 1 to 50 for 50Hz camera type. Smaller number means the distance between 2 I-frames is smaller, which needs more network bandwidth while having better image quality. By contrast, larger number consumes less bandwidth but in an unstable network connection, video display may not be smooth. The available length number options of GOP will vary based on frame rate settings.

.

2. Image

2.1 Exposure

This section allows user to control the settings pertaining to exposure mode and day night modes. Note that the PTZ incorporates Smart IR and Adaptive IR automatically based on zoom level.

Basic Settings

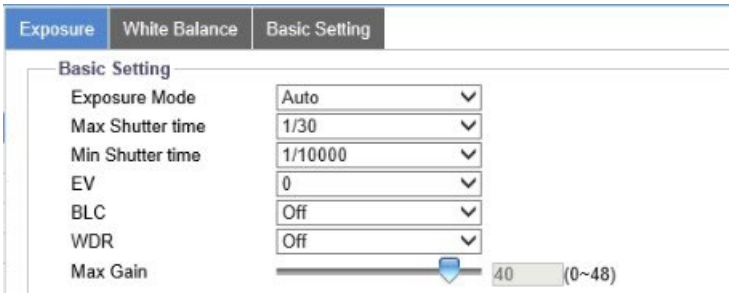


Figure: Exposure Basic Settings

Exposure Mode: Auto/Flickerless/Shutter Priority/Iris Priority/Manual

There are 5 modes to select from, which are described below. Note that the choices on Basic Setting change depending on what mode is selected.

- Auto: With certain pre-settings, before taking videos, the camera automatically determines the correct exposure for pictures without user input settings.
- Flickerless: This mode allows the camera to override the shutter speed, which helps to avoid interference of fluorescent lights in some environments.
- Shutter Priority: Enables user to select a specific shutter speed for adjustment of aperture, ensuring a correct and proper exposure.
- Iris Priority: When more control is needed for the iris, for example if more depth-of-field is needed, which requires a smaller iris, iris priority mode (also known as aperture priority) can be used to set the iris. The iris value takes priority, and the camera will auto adjust the shutter and gain values for the selected iris. Select the F number from the dropdown list.
- Manual: A mode that allows user to manually control both gain value and shutter speed. It is recommended that only an experienced administrator use this mode.

Max Shutter Time: 1/8000 ~ 1

Select the maximum shutter time from the dropdown menus.

Note	•	Max Shutter Time function is available only in "Auto" exposure mode.

Min Shutter Time: 1/10000 ~ 1/120

Select the minimum shutter time from the dropdown menus.

Note	•	Min Shutter Time function is available only in "Auto" exposure mode.

EV : -2 ~ 2

This is the exposure compensation that makes the scenes either darker or brighter. Positive number provides the brighter image, while negative number provides the darker image.

Note	•	EV function is NOT available in "Manual" exposure mode.

BLC Off/Upper/Lower/Central (1/3rd)/Central (1/6th)/Left/Right

Set an area for Backlight Compensation. Backlight Compensation is a function that sets the brightness of a selected area to optimal image level. This function is necessary when an autoiris lens closes quickly due to an intense light behind the object in the area being viewed, resulting in a display that is too dark and difficult to see. In this case, users can set the area corresponding to the area of the scene being viewed. The area size illustrations are as follows.

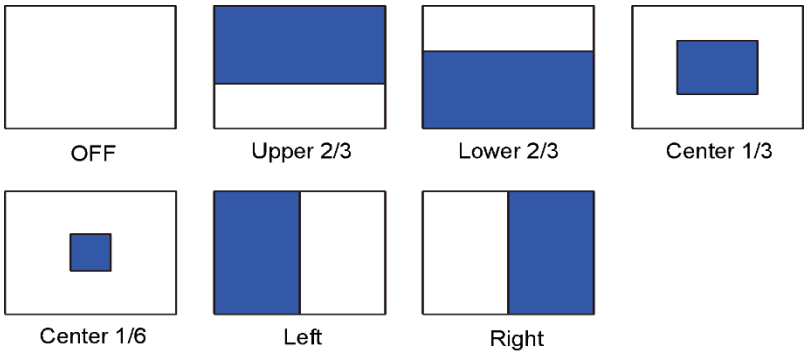


Figure: BLC Settings Illustrations

Note	•	BLC function is available only in "Auto" exposure mode.

WDR: Off/On

Wide Dynamic Range (WDR) technology is intended to provide clear image even under backlight circumstances where intensity of illumination can vary excessively, for example, when both extreme bright and dark areas exist simultaneously in field of view. WDR is a sensor-based technology that achieves proper exposure levels by capturing short and long exposures individually and combining them into a single frame to render a superior detail of image quality. Note that when WDR is enabled, the maximum frame rate will be forcibly decreased to 30fps if it was selected above 30fps.

Note	•	WDR function is available only in "Auto" exposure mode.

Max Gain: 0 ~ 48

This is used to set the max gain in auto exposure mode.

Frequency: 50 Hz/60 Hz

In some cases, the indoor lighting causes flickering; adjust the frequency to the power line frequency.

Note	•	Frequency is only available when exposure mode "Flickerless" is selected.

Iris: F1.6/ ~ F6.7

Iris, with built-in stepper motor, assists camera to precisely regulate the iris position in volatile lighting conditions, optimizing the result of crisp images with better depth-of-field. Iris position will be kept within the selected level. Smaller iris value means fully open iris, whereas "Closed" means completely closed iris. Select the Iris from the dropdown list.

Note	•	Iris is only available when exposure mode is "Iris Priority" or "Manual".

Shutter Speed: 1/10000 ~ 1/7.5

Select a shutter speed from the dropdown menu. Selecting 1/10000 provides the fastest shutter speed. Values available are dependent on selections made.

Note	•	Shutter Speed is only available when exposure mode is "Shutter Priority" or "Manual".

Gain 0 ~ 48:

The larger the value, the more intensity of light comes into the camera and vice versa.

Note	•	Gain is only available when exposure mode "Manual" is selected. Otherwise, a Max Gain slider is provided, 0 ~ 48.

Day Night Setting

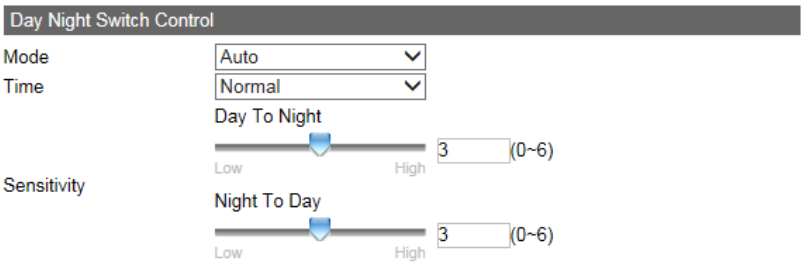


Figure: Day Night Switch Control Settings

Day Night Switch Control – Mode: Auto/Color/B/W

When Color mode is selected, the camera is forced to stay in Color mode permanently. Similarly, the camera stays in black-and-white mode when B/W is selected. Auto lets the camera switch between the two modes automatically, based on the light intensity.

Note	•	Only Color and B/W options are available when exposure mode "Manual" is selected.

Day Night Switch Control – Sensitivity: Day to Night (0 ~ 6)/Night to Day (0 ~ 6)

This determines the sensitivity of the day/night mode switching mechanism. A larger the value (High) means camera can auto switch from day to night or night to day mode based on minor light intensity changes. A smaller value (Low) indicates camera is going to switch from day to night or night to day mode based on major changes of surrounding light intensity.

Note	•	Day Night Switch Control – Sensitivity is NOT available when exposure mode is "Manual"

IR Control

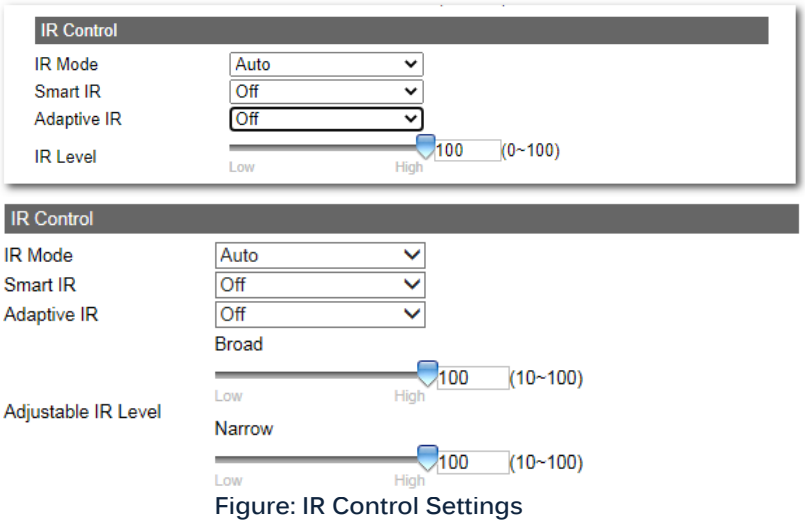


Figure: IR Control Settings

IR Mode: Auto/On/Off

Select "On" to enable IR LED permanently and select "Auto" to let camera switch IR LED on or off based on light intensity of different applications. Choose "Off" to turn off IR LED.

Smart IR: On/Off

Smart IR technology was developed via an intelligent algorithm to keep close objects from overexposure effect under low-light environment. Turn "On" Smart IR function to have camera dynamically adjust the shutter speed as well as the sensor gain to prevent overexposure.

Adaptive IR: On/Off

Adaptive IR, via built-in multiple groups of IR LEDs that are able to cover different angles from diversified field-of-views, is a cutting-edge technology practical for cameras with a motorized lens that generally have a common problem of uneven IR intensity in variable focal length. Select "On" to let camera adjust adaptive IR intensity automatically, whereas choosing "Off" will make the IR level adjustable bar display below.

IR Level: Low/High (0~100)

Depending on selections made, a user can click and drag to adjust the IR intensity level from "Low" to "High" level or also enter an exact value into the field for a specific IR intensity.

2.2 White Balance

This section allows user to set the white balance values to meet ambient conditions for best color rendition.

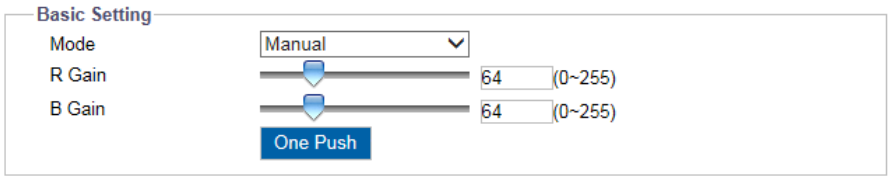


Figure: White Balance Settings

Basic Setting

Mode: Auto/ATW/Manual

- Auto: Continuously adjusts the camera color balance in accordance with any change in color temperature simultaneously.
- ATW: "Auto Tracing White Balance" automatically controls color temperature ranging from 2500°K to 10000°K.
- Manual - R Gain/B Gain: 0~511/One Push

R Gain/B Gain 0~511:
Allows users to adjust red color and blue color in the image.
One Push:
Click this button to make the camera rapidly adjust to the proper gain values depending on the ambient environment.

- Indoor: Uses color temperature of 3200°K, which is suitable for indoor scene.
- Outdoor: Uses color temperature of 5800°K, which is suitable for outdoor scene.

2.3 Basic Setting

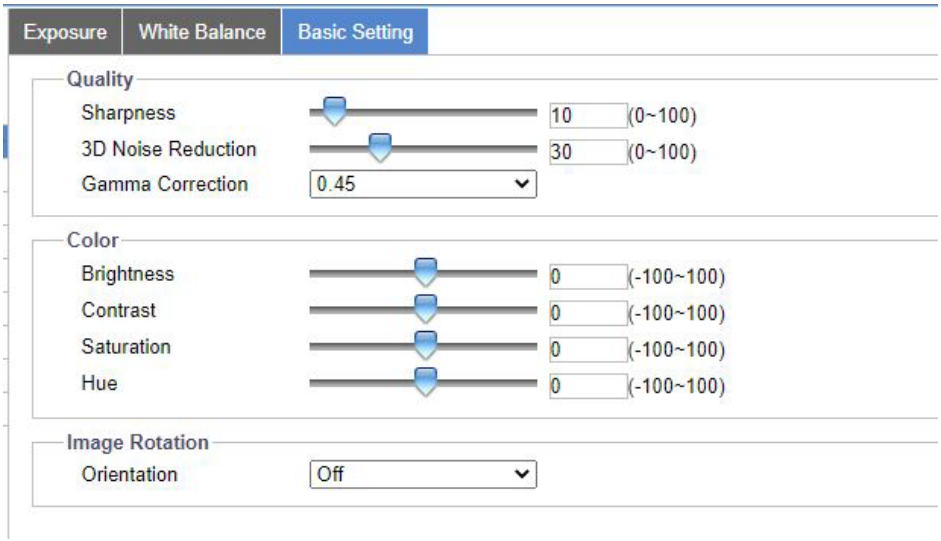


Figure: Basic Settings

Quality

Sharpness: 0 ~ 100

Increasing the sharpness value will define the edges and small feature of viewing images. If the edges appear too smooth or blurred, increase the sharpness. Selecting higher value provides the sharper image.

3D Noise Reduction: 0 ~ 100

This is the process of removing noises from a signal and can be set to decrease noise on the screen. Selecting higher value provides higher effect of noise reduction.

Gamma Correction: 1/0.45

Set gamma correction from the dropdown list, which is important for an image to display accurately when it is being viewed on different monitor screens. Set gamma correction between 1 and 0.45 for better rendition in varied screens.

Color

Item	Option/Range	Description
Brightness	Use slider or enter a number -100 - 100	Selecting higher value provides brighter image.
Contrast	Use slider or enter a number -100 - 100	Selecting higher value provides higher contrast image.
Saturation	Use slider or enter a number -100 - 100	Decreasing saturation brings the image closer to a grayscale (monochrome/BW) image. Selecting higher values provide higher image saturation.
Hue	Use slider or enter a number -100 - 100	Selecting higher value provides deeper hue effect.

Image Rotation

The image can be rotated 180 or 270 degrees when selected from the dropdown.

Orientation: Off/Flip

- Off: Disable video orientation function.
- Flip: Vertically change the orientation of the video display.

3. Video

3.1 Privacy Zone

Basic Setting

Privacy Zone enables user to block out a specific portion of the view with a solid color mask for privacy concerns. It must apply on all streams, TV output, and Live View; and it should not affect the motion detection behavior. There are up to 8 privacy zones for users to define on the view. After setting up a privacy zone, the live view image will appear with a frame in the area; the color, size and position of the privacy zone can be customized by user's preference.

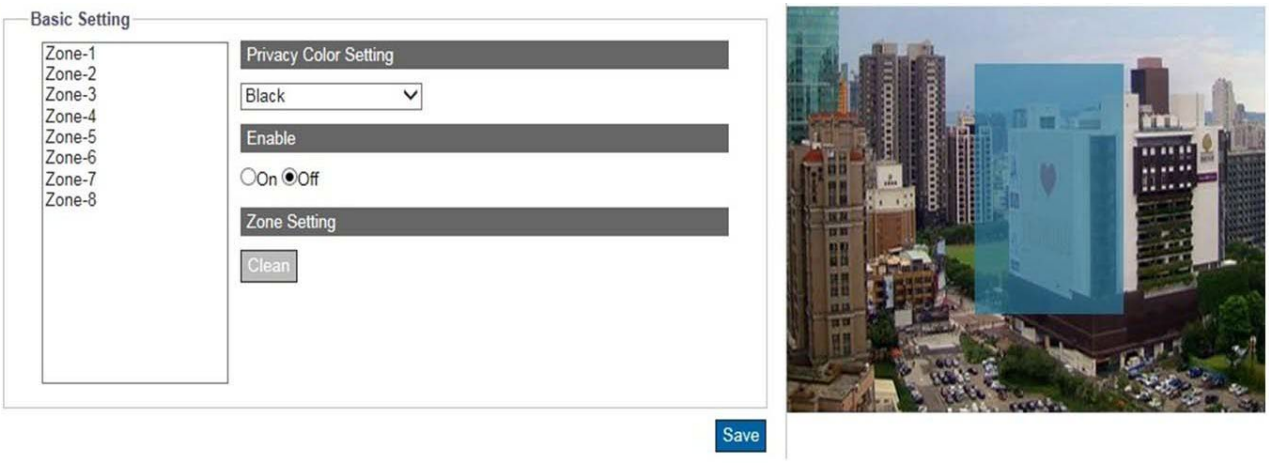


Figure: Privacy Zone Setting

- Privacy Color Setting

Click the dropdown menu to select color (Black, Gray or White) for privacy zone. Selected color will be applied to all the privacy zones collectively. Click "Save" for the action to take effect.

- Enable

Select "On" or "Off" to enable or disable Privacy Zone, respectively. Click "Save" for the action to take effect. After saving the changes, when Enable is "On," if any privacy zone was previously setup in the current view it will show on the view. Enabling or disabling privacy zone will be applied to privacy collectively.

- Zone Setting

To set up privacy zone, user first needs to Enable the function; then, select a zone from Basic Setting list to define a view.

Click "Setup" and a transparent blue block will appear in the middle of the view.

Define the size and shape of the transparent blue block by either left clicking on any point of the view or left clicking on any point of the view and dragging to outline a desired transparent blue block.
Finally, click "Save" for the action to take effect; the transparent blue block will turn into solid color block, which represents the privacy zone.

Once a Privacy zone is set up, "View" and "Clean" options will become available.

For zones already setup, click "View" to go to the scene where privacy zone was defined. If privacy zone is enabled, solid color block will be seen on the view; however, if privacy zone is disabled, no solid color block will be seen on the view.

For zones already setup, click "Clean" to delete the solid color block. This action will cancel privacy zone setup and make "View" unavailable for specific zone.

Notes	• Set the privacy zone slightly larger than the actual area to ensure privacy concern. • The maximum size of the privacy zone can reach full resolution. • Privacy zone must be kept after changing resolution and codec format.

3.2 Enhanced Codec

Enhanced codec is a method to keep low bitrate when H.264 or H.265 is selected. The implementation of enhanced codec depends upon 2 key ideas.

Dynamic ROI: This is used for the camera to dynamically adjust compression based on what it judges is of interest in the scene. For example, the camera would be able to detect objects and identify which objects require higher or lower compression levels. The function is designed to reduce the bandwidth by decreasing the image quality on the static or irrelevant area within the whole scene.

Dynamic GOP: Adaptive GOP size. Comparing the average-sampling of current standard fixed GOP structure with dynamic GOP, the camera has great freedom in I-, P- and B-frame selection.. The dynamic GOP structure keeps temporal important information of frames in the encoded video, which helps in the decision for adapting to bandwidth decrease and temporal-SNR quality tradeoff. It also helps in storing more information with restricted resources, resulting in increasing code efficiency and better user perception.

The Enhanced Codec technology features both the iZone and iStream technologies to not only economically exert leverage between different regions and compression levels, but also effectively reduce the average bit rate to level down the overall bandwidth usage as the following explains.

Basic Setting

iZone

iZone is a feature that utilizes the intelligent algorithm to place diverse compression levels upon different areas while retaining the target bitrate. By enabling this feature, user can designate a customized zone, which will be compressed less to enhance the clear image quality within the zone, while the undefined zone, being less important, will be sacrificed for image quality by higher compression ratio.

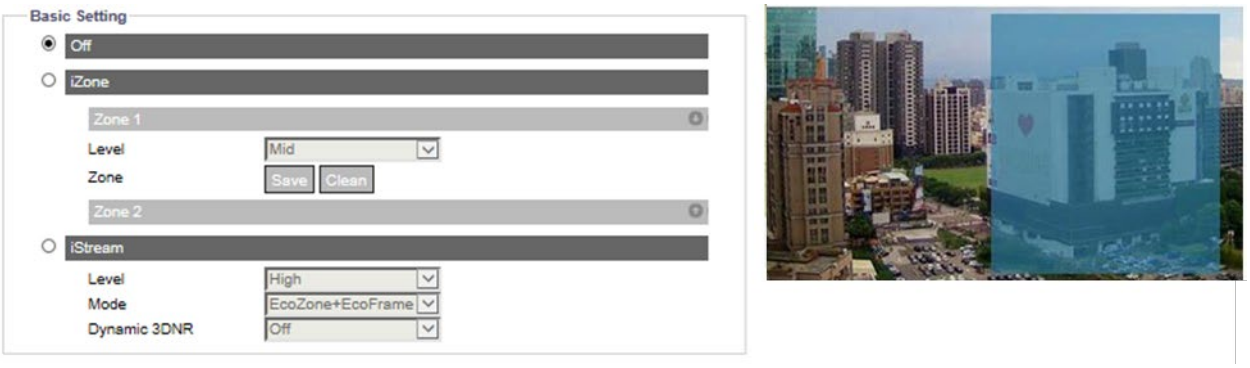


Figure: iZone Settings

First, click iZone to turn on one or both Zones. On the preview image, the cursor changes to a cross icon; left click and drag to outline a desired zone. User can select a level for each Zone. High level means higher image quality and lower compression in the Zone. Press "Save" to make settings take effect. To delete settings, click "Clean" to wipe out the selected Zone settings.

iStream

This is a groundbreaking technology that helps save network bandwidth efficiently while maintaining the clear image quality for critical image details based on the 2 cutting-edge features. Click iStreams to enable the features as follows:

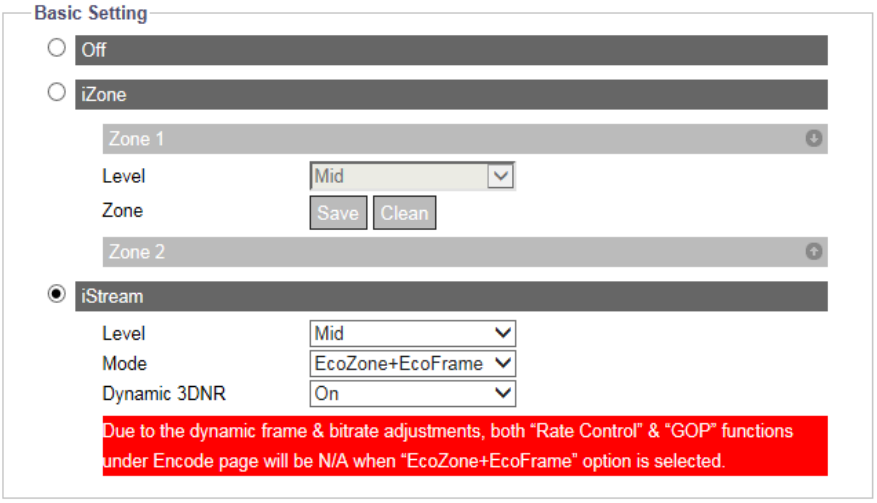


Figure: iStream Settings

- Level

Select Low, Mid or High to determine the level of bandwidth usage.

- Mode
  - EcoZone

As opposed to iZone, the "EcoZone" can swiftly identify dynamic motions that occurred within a scene and retain its details with clear quality, whereas the rest of the areas, e.g., static background, will have a higher compression level, resulting in economically decreasing bandwidth on less important areas but keeping the dynamic motion details for future forensic purpose. The intensity for EcoZone can be defined by the "Level" dropdown menu. High level means higher image quality and lower compression in the Zone.

  - EcoZone + EcoFrame

Under Mode, select EcoZone + EcoFrame. By enabling the proprietary EcoFrame function, the overall bitrate, i.e., bandwidth utilization, will be reduced even further. When less motion occurs within a scene, e.g., storeroom, I-frame number, which is needed when motion is in a scene, will be drastically reduced by EcoFrame activation. Based on complexity of scenes and motions occurred, a large amount of bandwidth saving can be achieved to deliver a compact yet valuable performance on bandwidth utilization. Note that it is necessary to enable both EcoZone & EcoFrame functions simultaneously by selecting the option "EcoZone + EcoFrame," since EcoFrame is an enhancing technology that is based on EcoZone to promote the overall large-scale efficiency. The intensity for EcoZone + EcoFrame can be defined by the "Level" dropdown menu; High level means higher image quality and lower compression in the Zone.

Notes	• Due to the attribute of dynamic bitrate management, "Rate Control" options (CBR, CVBR, and VBR) under Encode page are NOT available when "EcoZone" function is activated. • Due to the dynamic frame & bitrate adjustments, both "Rate Control" & "GOP" options under Encode page are NOT available when "EcoZone + EcoFrame" function is enabled.

- Dynamic 3DNR

While 3DNR allows user to adjust noise reduction level manually, dynamic 3DNR dynamically and automatically adjusts to the best noise reduction level according to the amount of noise on the image. Lux level change is what triggers changes in noise reduction level for dynamic 3DNR. Higher lux activates smaller noise reduction level.

Be aware that using Dynamic 3DNR in a scene that contains motion may result in blurred image. When Dynamic 3DNR function is "ON" the 3DNR function under Image will become unavailable.

4. Network

4.1 General

This section is for the user to set detailed settings related to wired network condition for the camera.

Basic Setting

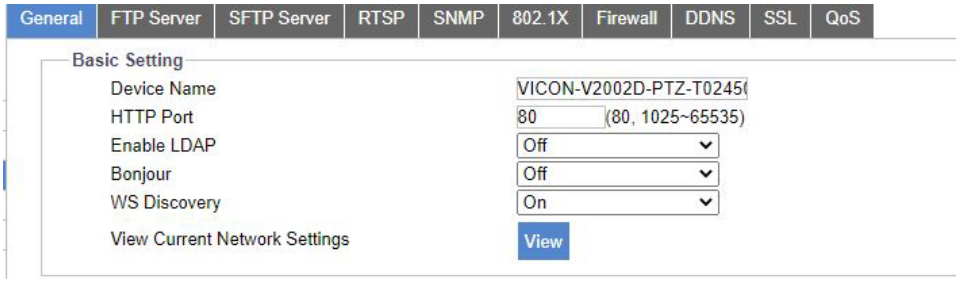


Figure: Network Basic Setting

Device Name

Enter a device name.

HTTP Port: 80, 1025 ~ 65535

This protocol allows for TCP protocol quality without having to open specific ports for streaming. User using a firewall can utilize this protocol to allow data to stream through it. It is recommended to use the default port number 80; however, if it is required to change the port number, contact your system administrator.

Enable LDAP: On/Off

For accessing and maintaining distributed directory information services over an Internet Protocol network, the Lightweight Directory Access Protocol (LDAP), an open, vendor-neutral, industry standard application protocol, has a major role in both intranet and internet applications to facilitate information sharing between devices.

Bonjour: On/Off

Bonjour is a specific protocol introduced by Apple Inc. to make IP devices, including IP cameras, easily found by software like Safari within local network on the basis of zero configuration.

WS Discovery: On/Off

WS Discovery (Web Services Dynamic Discovery) is a mechanism that supports probing a network to find ONVIF capable devices.

View Current Network Settings: View

Click "View" to see your current network related settings.

IP Settings

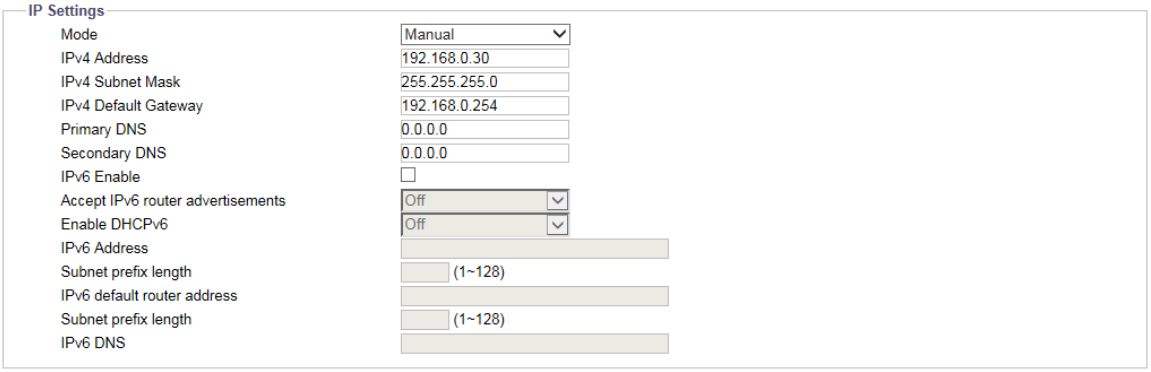


Figure: Network IP Settings

Item	Option/ Range	Description
Mode	Manual	User can manually input IP address and the related settings.
	PPPoE	This is a point-to-point-based protocol that offers authentication, encryption and compression. It predominantly authenticates user with the predefined username and password.
	DHCP	The camera will automatically obtain an available dynamic IP address from the DHCP server each time it connects to the LAN.
APIPA	On/Off	APIPA (Automatic Private IP Addressing) helps reserve a certain address block for link-local addressing, which is very practical for assigning an IP address automatically for cameras when DHCP is not available within the connected internet environment.
IPv4 Address		Manually set an IP address under IPv4.
IPv4 Subnet Mask		Use default address: 255.255.255.0. If subnet mask is not properly configured, the unit may not be able to communicate with other devices.
IPv4 Default Gateway		Leave blank as default setting. No Default Gateway address required if not used. Ask your network administrator for further information.
Primary DNS		Same as above.
Secondary DNS		Same as above.
IPv6 Enable	Enable/Disable	Enable/ Disable IPv6 protocol.
Accept IPv6 router advertisements	On/Off	Check the box to activate RA (Router Advertisement) corresponding to RS (Router Solicitation) for IPv6 address designation.
Enable DHCPv6	On/ Off	If enabled, the camera will automatically obtain an available dynamic IP address under IPv6 protocol from the DHCP server each time it connects to the LAN.
IPv6 Address		Manually set an IP address under IPv6 protocol.
Subnet prefix length	1 ~ 128	Set prefix length for subnet.
IPv6 default router address		Manually set a default router address under IPv6 protocol.
Subnet prefix length	1 ~ 128	Set prefix length for subnet.
IPv6 DNS		Set a DNS (Domain Name Server) under IPv6 protocol.

Wired Setting

Speed & Duplex: Auto/10 or 100 Half Duplex/10 or 100 Full Duplex

Due to the collision issue, Half Duplex can only send or receive information at one time, while Full Duplex can receive and transmit in full line rate simultaneously without the issue of collision. For the Mbps number, the larger the number, the faster the results; the smaller the number, the slower the results. "Auto" allows the camera to decide which mode to use.

UPnP

Enable UPnP: On/Off

When UPnP (Universal Plug & Play) is "On," a device can be detected automatically by any computer in the LAN to skip the installation of the IP Toolbox utility.

Mode: IP and Device Name/Device Name/User Input

When the camera connects with the LAN, select one of the modes below for identification:

- IP and Device Name: The device name and IP address will be shown simultaneously.
- Device Name: Only device name will be shown.
- User Input: User can input a customized name for the camera.

SSL

Enable SSL: On/Off

Turn Secure Sockets Layer (SSL) on to enable both HTTP and HTTPS communications. Turning SSL "Off" will allow only HTTP communication. Select the option "Https Only" to enable only HTTPS communication, which automatically disables web port (port 80).

Note	• Before enabling SSL (on/Https Only), refer to "*4.9 SSL*" section to install or generate SSL certificate

HTTPS Port: (443, 1025~65535)

HTTPS enables a secure video transmission from network camera. It is recommended to use the default port number 443; however, if it is required to change the port number, contact your system administrator. This field is only available if SSL has been turned on and configured.

4.2 FTP Server

FTP (File Transfer Protocol), transferring files via TCP-based network like the Internet, is a standard protocol that is adopted to transmit computer files from one host to another.

The camera can act as both FTP Server and FTP Client. This section describes how to use the camera as FTP Server while 7. Event Source section (Handlers → Snapshot: Store to Edge/Store to FTP) describes how to use the camera as FTP Client.

Basic Setting

Figure: FTP Settings

Enable: On/Off

User can enable or disable FTP server by selecting On or Off from the dropdown.

Port: 21/1025 ~ 65535

Input a value of 21 by default into the port field to activate the FTP server function.

The login ID and password are shared with the user account, which can be changed by modifying the username and password of the user account.

- SD card access:

If the FTP Server is enabled, a user on a remote client can access files (video/image recording) stored on the camera's SD card via FTP Client.

4.3 SFTP Server

SFTP (Secure File Transfer Protocol), used for transferring files via a more secure channel than FTP, is a network protocol that offers multiple file access, transfer and management over reliable data stream.

Figure: SFTP Settings

Enable: On/Off

User can enable or disable SFTP server by selecting On or Off from the dropdown.

Port: 1025 ~ 65535

Input a value into the port field to activate the SFTP server function.

- SD card access:

If the SFTP Server is enabled, user on a remote client can access files (video/image recording) stored on the camera's SD card via SFTP Client.

4.4 RTSP

RTSP is a standard protocol for connecting a client to establish and control streaming data over the web. If you want to allow third-party devices or software to access video/audio streams from the IP camera over the network, you must configure the RTSP ports. The major difference between Unicast and Multicast is how client and server communicate packets with each other. Specifically, Unicast transmits packets in a 1 to 1 device method, while multicast transmits 1 to multiple devices. Therefore, Unicast requires large network bandwidth and uses more resources of server but is more stable because of its simple structure; by contrast, Multicast needs less bandwidth with resources and is more practical for multiple devices broadcast, with the condition that all relevant peripheral devices, like switch or router, support the multicast protocol. Select a method based on your network applications for best efficiency. For each RTSP session, there are 3 kinds of real-time data that can be configured, including video, audio and meta data. When codec related information is changed, the RTSP server will be restarted.

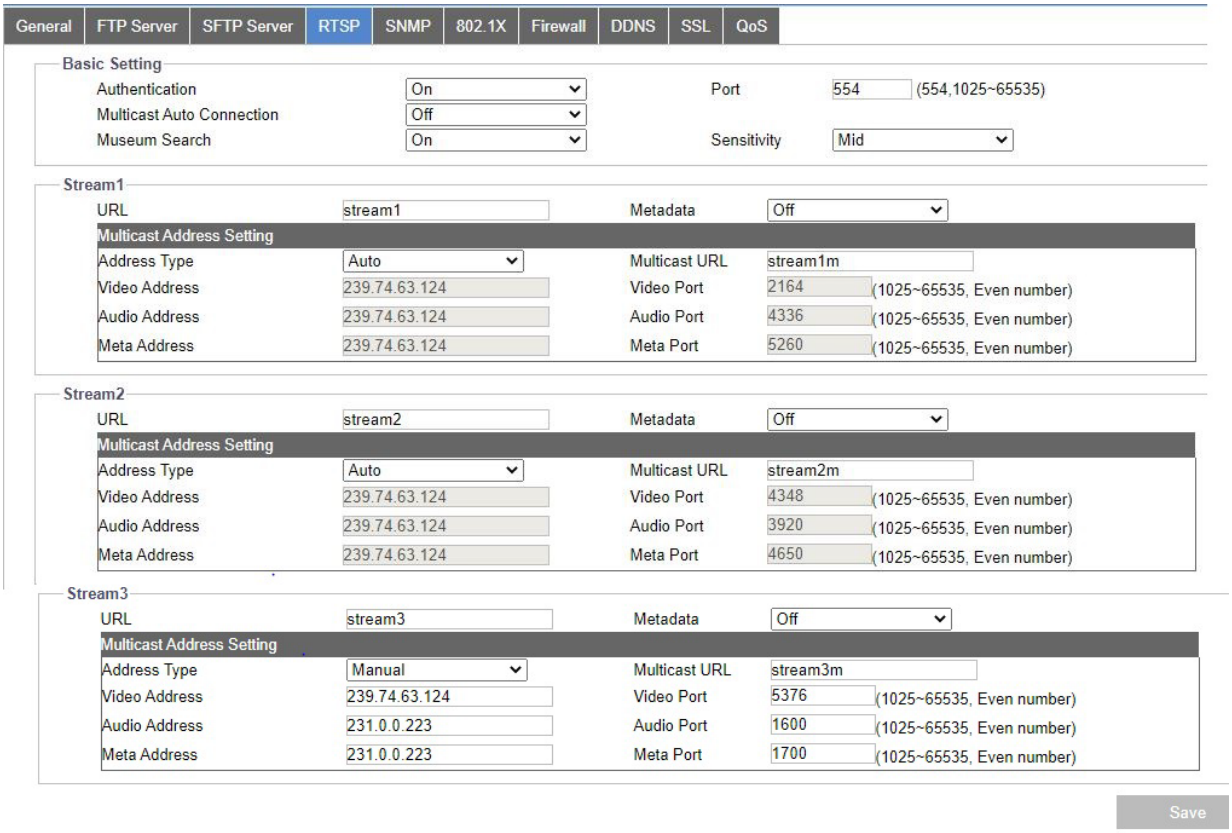


Figure: RTSP Settings

Basic Settings & Authentication

Enabling the authentication (On) will improve the verifying mechanism and make the RTSP connection process more secure and much safer. To verify the RTSP, simply enter the Login ID, Password and Port (554 by default) with Authentication turned On.

Turning Multicast Auto Connection "On" will enable auto connection. Note that it is not required to enable authentication before proceeding with RTSP. Museum Search can be turned On to enable (On by default). It is recommended to leave Museum Search set to On; if Museum Search is turned off, access to certain analytics features is also turned off, such as bounding boxes. Sensitivity of Museum Search can be set to Low, Mid High to control the number of search results (high will yield more results).

Museum Search: On/Off

Museum Search is used to find video where a defined amount of change in a region of interest is detected. The amount of change in a scene's region of interest that will be searched for is defined using the Sensitivity.

Sensitivity: High/Mid/Low

The level of change that will determine detection.

Stream1/2/3

URL

Input a preferred name for each RTSP Stream URL. This refers to Multicast URL protocol which transmits data via one host to a single host, consuming more network bandwidth but with a direct and simple transmission method. For unicast, user can change port and url stream. After defining preferred URL name for each stream, via 3rd party software, enter the address like the following examples for RTSP URL streaming.

- rtsp://(camera IP address)/(URL stream 1)
- rtsp://(camera IP address)/(URL stream 2)
- rtsp://(camera IP address)/(URL stream 3)

For example: rtsp://192.168.0.30/URL stream1

Metadata: On/Off

Turn Metadata ON from the dropdown to enable information about data, which means the data information will be allocated systematically, keeping similar data together by certain criteria and distinguishing dissimilar data organizationally to effectively transmit data information.

Multicast URL

Differing from URL, Multicast URL can transmit data from one host to a single host or to all hosts, consuming less network bandwidth with more flexibility. However, it is required to make sure that the peripherals connected to the camera are all compatible with Multicast in advance. For multicast, user can change address, port and url stream. The address for Multicast is roughly the same as the previous URL. Refer to the samples below:

- rtsp://(camera IP address)/(Multicast URL stream 1)
- rtsp://(camera IP address)/(Multicast URL stream 2)
- rtsp://(camera IP address)/(Multicast URL stream 3)

For example: rtsp://192.168.0.30/Multicast URL stream1

Address Type: Auto/Manual

By selecting "Manual," user can enter the Video, Audio and Meta settings below; selecting "Auto" keeps the original settings by the camera.

Video, Audio and Meta Address/Port

Complex in its transmitting procedure and layer structure, Multicast streaming requires more specific settings containing Video Address/Port, Audio Address/Port and Meta Address/Port, all of which have a certain IP address range (224.0.1.1 – 239.255.255.254) for user to define individually.

4.5 SNMP

SNMP (Simple Network Management Protocol) is an Internet standard protocol used for monitoring and managing the status of devices connected to IP networks.

Three versions of SNMP have been developed, namely, SNMPv1, SNMPv2c and SNMPv3, with the newest version featuring improvements in performance, flexibility and security.

When SNMP is "On," upon request of SNMP server, network-attached devices display their status to SNMP server, which activates remote modifications if necessary.

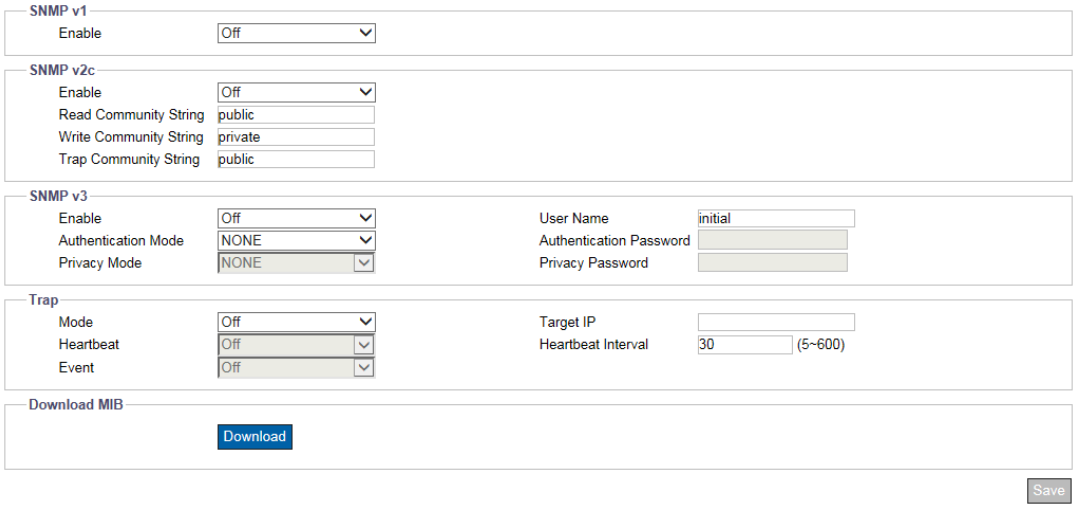


Figure: SNMP Settings

SNMP v1

Enable: On/Off

Select "On" or "Off" to enable or disable.

SNMP v2c

Enable: On/Off

Select "On" or "Off" to enable or disable. The community name can be specified as a password for read, write or trap access to all supported SNMP objects; check the community string from SNMP server and input to the corresponding field in camera.

SNMP v3

Enable: On Off

SNMP V3 provides more security features than SNMP v1/SNMP v2. Select "On" in the dropdown to enable the function. Input User Name for SNMP v3 first. Then select desired modes for "Authentication" with "Privacy" and enter passwords paired with both protocols individually.

Trap

Mode: V1/V2C/V3/Off

Trap under SNMP allows a network-attached device to notify the SNMP server of significant events via unsolicited and irregular notification. Select which SNMP mode (v1, v2c or v3) to be enabled with Trap.

Target IP:

Input the IP address of SNMP server in "Target IP" field.

Heartbeat: On/Off

To ensure a network free from delayed notifications, "Heartbeat" communications protocol sends notifications at the selected interval. Select "On" or "Off" " when a Mode is selected to enable or disable heartbeat function.

Heartbeat Interval: 5 ~ 600

Input desired values in seconds for Heartbeat Interval (when a Mode is selected).

Event: On/Off

Specifically designed for event occurrence, this option, when turned ON, will automatically record the log file of events that occurred for review afterwards.

Download MIB

Click "Download" to get specifics of MIB (Management Information Base). MIBs describe the structure of the management data of a device subsystem' which uses a hierarchical namespace containing object identifiers (OID). Each OID identifies a variable that can be read or set via SNMP.

4.6 802.1X

802.1X is an IEEE Standard for port-based network access control and defines the encapsulation of the Extensible Authentication Protocol (EAP) over IEEE 802, which is known as EAP over LAN. Simply select a desired EAP protocol type from the dropdown menu and then input its required subfields to complete setup. Inner authentication mode can support CHAP, EAP-MSCHAPV2, MD5, MSCHAP, MSCHAPV2 and PAP.

Basic Setting

Protocol: None/EAP-MD5/EAP-TTLS/EAP-PEAP

- None: None of the protocols is selected by user.
- EAP-MD5: It is the only IETF Standards Track based EAP method and offers the minimal security.
- EAP-TTLS: Tunneled Transport Layer Security (TTLS) is an EAP protocol and is well-supported among wireless vendors. It further extends TLS protocol and is widely supported across a variety of platforms.
- EAP-PEAP: The Protected Extensible Authentication Protocol (PEAP) was jointly developed by Cisco Systems, Microsoft, and RSA Security and provides unique security for users.

4.7 Firewall

Under this menu, a user can manually define several IP addresses to be allowed or denied access to the camera.

Figure: Firewall Settings

Basic Setting

Mode: Allow/Deny/Off

- Allow: Select this option to give inputted IP addresses access IP camera.
- Deny: Select this option to not allow inputted IP addresses to access IP camera.
- Off: Select this option, no actions will be made for inputted IP addresses.

IP Address 1 ~ 10

Manually input IP addresses in each of the fields to be allowed or denied access. After entering the address, check the box in front of each address to activate the filters of allow or deny.

4.8 DDNS

Dynamic Domain Name Server (DDNS) is the system that can automatically upgrade DSN records without further manual editing in real time, resulting in web address directing faster and smoother.

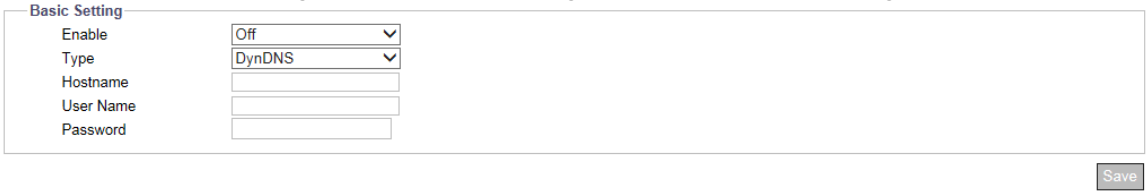


Figure 3 - 22: DDNS Settings

Basic Setting

Enable: On/Off

Type: DynDNS/No-IP/Two-DNS/FreeDNS

There are 4 types of DDNS for selection, explained as follows.

- DynDNS: One of the DDNS providers offering service with fee.
- No-IP: A DDNS provider offering free service. You must register before enabling this type.
- Two-DNS: A DDNS provider offering free service. You must register before enabling this type.
- FreeDNS: A DDNS provider offering free service. You must register before enabling this type.

Item	Description
Hostname	Define a specific hostname for DDNS.
User Name	Configure a privileged username for accessing to DDNS.
Password	Input the password associated with the privileged username.
Hash	It is required to set up the value when selecting FreeDNS type.

4.9 SSL

Method: None/Self Signed/Upload Certificate

Secure Sockets Layer (SSL), the standard security technology for establishing encryption, allows sensitive information such as login credentials to be transmitted securely. Select the method from the dropdown.

- Self Signed: Self-signed certificate is a privately owned key that has no connection to a person or organization that performs an authorized certificate signing procedure. For self-signed certificate, user can create CSR (Certificate Signing Request) by filling in the following information: Country, Province, City, Common Name, Organization, Organization Unit and Email. For an installed certificate user can view Common Name, Organization, Location, Country, Issuer, Start Date and End Date. Select it and input the required fields below to display information of a self-signed certificate.

Notes	• The certificate can be removed. • HTTPS will not work correctly if SSL is not enabled.

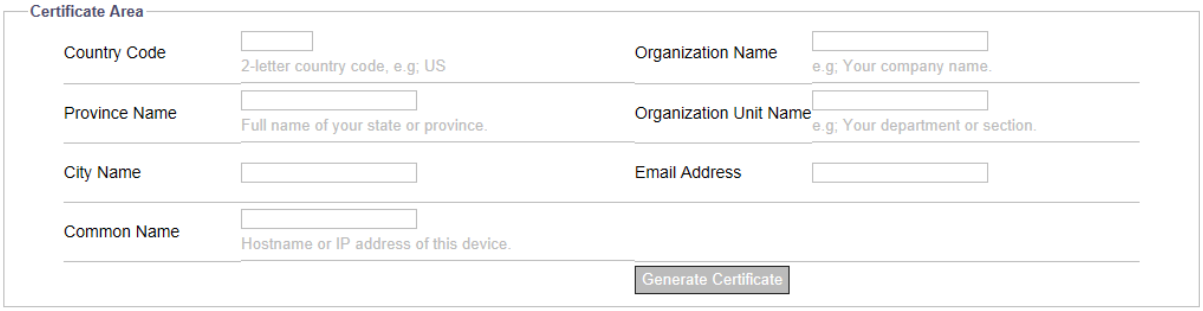


Figure: Self Signed & Request Settings

- Request

Similar to the settings of Self-Signed, by clicking the "Generate Certificate" after inputting the required fields, Request will provide user, in addition to showing the information like self signed, with a download option of created certificate for future utilization.

- Upload Certificate

After downloading the certificate from Request page, user can upload it to the camera via clicking "Upload" to locate the created certificate for "Upload Certificate." In addition, it is required to browse and upload the other CA (Certificate Authority), which is issued by an authorized person or organization, followed by clicking the "Upload" to complete the SSL procedure.

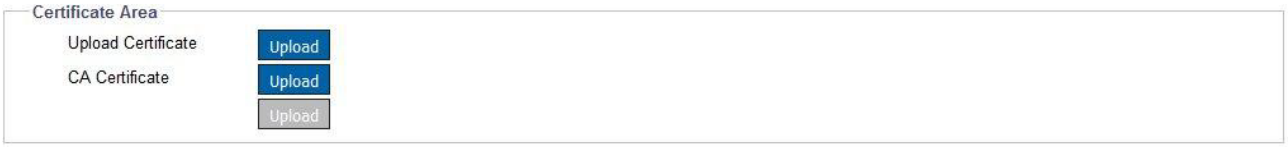


Figure: Upload Certificate

4.10 QoS

QoS (Quality of Service) refers, specifically, to both resource control and traffic prioritization mechanisms to provide different priorities to different applications or users in an attempt of maintaining a certain level of performance on data flow. It is especially efficient when transport of traffic has additional requirements.

Figure: QoS Settings

Item	Option/Range	Description
Enable		Check this box to enable the QoS function.
IPv4 Address		Input an IPv4 address for the fields of Priority 1 and 2 individually.
Netmask Bit	0 ~ 32	Enter a value into the fields for netmask bit in response to the IPv4 address assigned respectively.

5. System

5.1 Date & Time

Figure: Date & Time Settings

Basic Setting

Current Server Time

The current date/time is displayed here.

Synchronization Mode: Manually/PC/NTP Server

- Manually: Enter information to set date and time manually and individually.
- Synchronize with PC: Select this option to synchronize date and time of the camera to be consistent with date and time of connected computer.
- Synchronize with NTP Server: Select this option to synchronize date and time of the camera with date and time of the assigned NTP server.

NTP Setting

Enable: Manual/From DHCP Server

Enable NTP by selecting "Manual," which allows user to input desired NTP server address, or "From DHCP Server," which obtains a NTP address assigned by DHCP Server.

Server Address

Input desired NTP server address in the field.

Synchronization Period: 1 ~ 24 (hour)

Set the synchronization period using the slider or enter the number in the field, 1-24 hours.

Time Zone Setting

First choose one of the regions from the left dropdown menu and then select the corresponding city, based on your location country/area, from the right dropdown menu.

5.2 Audio

Equipped with audio input/output ports, the camera is able to connect with external audio devices for audio input and output individually. See the settings page and descriptions below for more details.

Figure: Audio Settings

Audio In Setting

Source: Line In

Select which audio source will be connected from the 2 options in the dropdown menu.

- Line In: via audio line in source.

Enable: On/Off

Set "On" to activate audio input/output functions when audio input/output devices are connected.

Encoding: G.711 A-law/G.711 μ-law

There are 2 audio codecs, G.711 a-law and G.711 μ-law, that can be selected for audio input encoding. G.711 μ-law is primarily used in North America and G.711 a-law is used by most other countries in the rest of the world.

Level: High/Mid/Low

Three audio levels, Low/Mid/High, are selectable for audio input and output individually.

Notes	• The audio output performance is not influenced by the codec combination. • The camera only supports one user to use audio out. Once the audio out is in use, others cannot use this function on live view. • The encoding of audio output is determined by the transmitter (NVR) rather than the camera; the current supported formats are G.711a-law and G.711u-law.

5.3 Firmware

Information about camera firmware is displayed on this page. User can manually upgrade System Firmware if upgrade is available. All motion of camera will be stopped during the firmware upgrade. Be sure to close any other screens before firmware upgrade. Never disconnect power or LAN cable during the upgrading process. It takes approximately 3 minutes for the unit to reboot after firmware upgrade process. Click "Choose File" to locate the firmware file and click "Upgrade" to proceed or use Vicon's PRONTO Device Manager; refer to the Connection section of this manual.

Figure: Firmware Settings

Note	• Power should not be turned off when upgrading firmware; this will cause the upgrade to fail and technical support may, therefore, be required.

5.4 Initialization

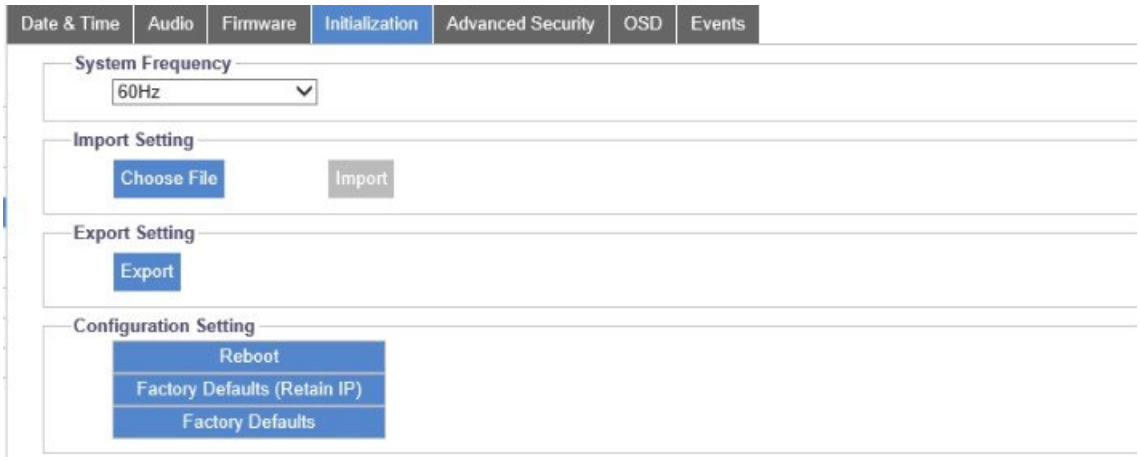


Figure: Initialize Settings

System Frequency: 60Hz/50Hz

Select "60Hz" or "50Hz" in accordance with requirements. Once set to the correct frequency, flickering by fluorescent light can be reduced.

Import Setting

Click "Choose File" to locate a file and then click "Import" to upload configuration settings from local computer to the camera.

Export Setting

Press "Export" to download configuration settings to local computer.

Configuration Setting

Reboot

Click "Reboot" to simply reboot the camera.

Factory Defaults (Retain IP)

Click to reset all configuration settings back to factory defaults excluding network settings.

Factory Defaults

Click to reset all configuration settings back to factory defaults.

5.5 Advanced Security

Advanced Secure functionality is used to turn off the access and connection to cameras completely or partially, making the IP camera even safer.

Activating any of the protocols or services under Active Prevention or Passive Protection will override any related settings done elsewhere in the camera UI. For instance, when UPnP service is "On" under both Active Prevention and *6.1 General*, no device under the same LAN will be able to discover the camera through UPnP, as Active Prevention setting overrides *6.1 General* setting.

Active Prevention has priority over Passive Protection. Therefore, if SSH is set "On" within both Active Prevention and Passive Prevention, no device under the same LAN will be able to access the camera through SSH, as Active Prevention setting overrides Passive Prevention setting.

Click Save at the bottom of the page after changing configurations for the settings take effect.

Active Prevention

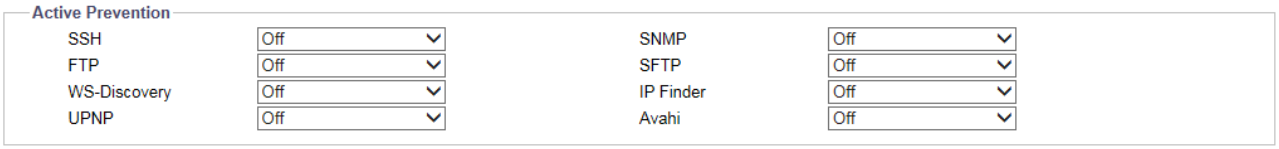


Figure: Active Prevention

SSH/SNMP/FTP/SFTP/WS-Discovery/IP Toolbox/UPNP/Avahi: On/Off

For each protocol and service under Active Prevention, set "On" to activate Active Prevention mode and stop access or connection to IP camera through the specific protocol or service.

Passive Protection

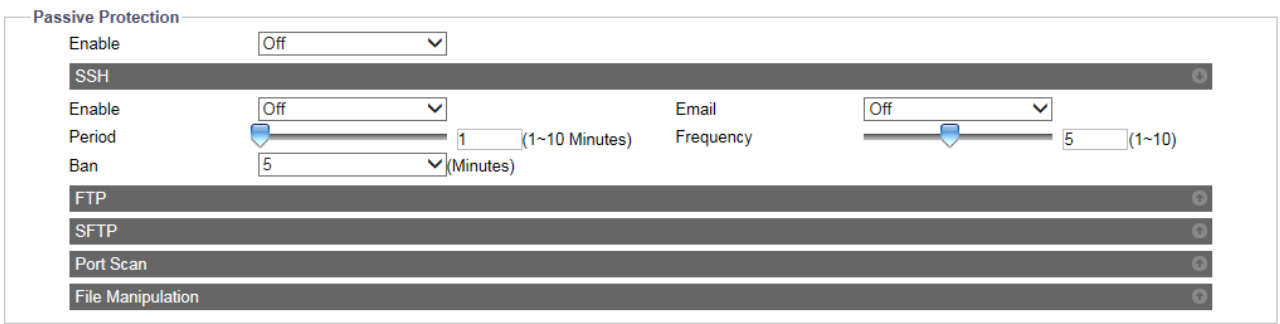


Figure: Passive Protection

Enable: On/Off

While Active Prevention simply blocks the access and connection to the camera, Passive Protection, bans IP addresses that try and fail to access or connect to the IP camera through the specific protocol or service within a defined period of time and with certain frequency; an email is then sent to a predefined user as notification.

Set "On" to activate Passive Protection mode. Further configurations are still needed to activate or deactivate specific protocols or services.

When enable is set to "Off," Passive Protection is disabled no matter how specific protocols or services are configured.

SSH/FTP/SFTP/Port Scan/File Manipulation

Enable: On/Off

Set "On" to activate Passive Protection mode for a specific protocol or service.

Email: On/Off

Set "On" to enable an email to be sent to a predefined user when an IP address has been banned.

Period: 1 ~ 10

Set an amount of time, in minutes, in which an IP address is allowed to try and fail to access or connect to camera.

Frequency: 1 ~ 10

Set a frequency within a period in which an IP address is allowed to try and fail to access or connect to camera.

Ban: Infinite/1/3/5/10/30/60

Set a time, in minutes, in which an IP address will be banned for trying and failing to access the camera with a certain frequency within a period. Or set period to infinite to never allow IP address to access or connect to IP camera.

Note	•	Only "Enable" and "Email" are available in File Manipulation.

Email

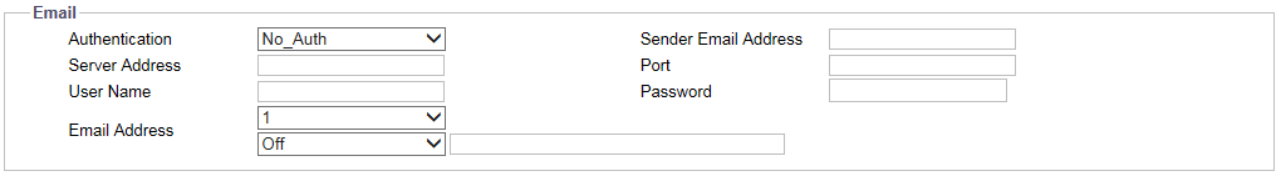


Figure: Email

In this section user can configure settings for both email sender and receivers. The Email configuration is jointly used by all protocols and services under Passive Protection.

Refer to "*9.3 Email*" section for details about Authentication, Server Address, User Name, Sender Email Address, Port and Password functions.

Email Address: 1 ~10/On/Off

Email can be sent to up to 10 users with privilege to access server. Choose a specific user number, and then set to "On" to allow email to be sent to the user. Next, separately, enter the user email address for each user.

Banned IP List

Figure: Banned IP List

Whenever an IP address is banned, it will be shown on the Banned IP List, including the time it was banned.

Select an IP address or select all IP addresses; then click reset to remove it or them from the banned list at your convenience.

5.6 OSD

This section allows user to enable OSD (On Screen Display) settings. In addition, it extends the OSD function to the occurrence of events.

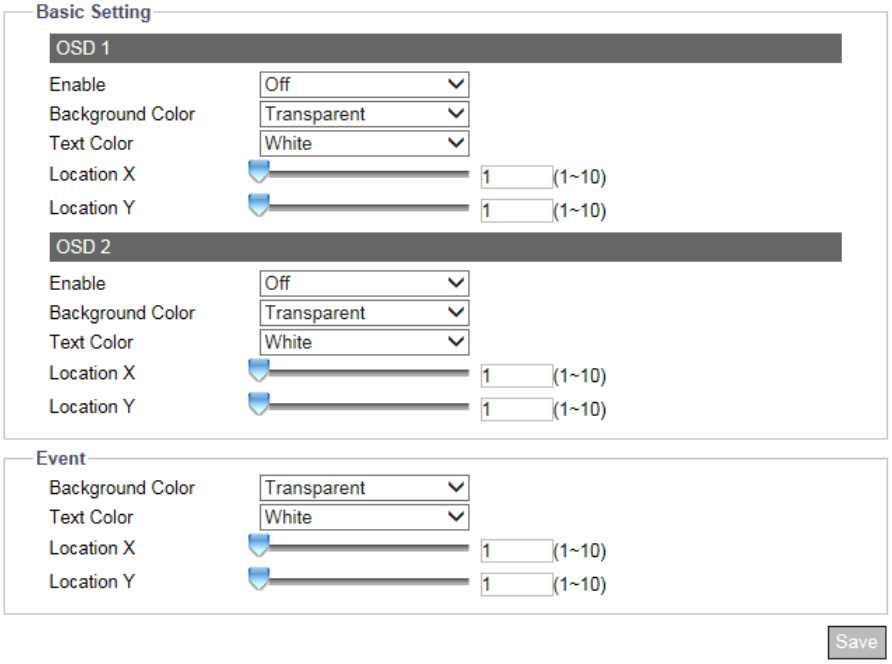


Figure: OSD Settings

Basic Setting

There are up to 2 sets of OSD settings that can be enabled concurrently, as shown on the following table.

Function	Option/Range	Remark
Enable	Device Name/Date/Text//Off	
Background Color	Black/Transparent	
Text Color	White/Black	Not supported for event.
Text Input		Not supported for event.
Location X	1~10	
Location Y	1~10	

Event

When an event is triggered, OSD can be displayed on screen to notify user.

6. Account

6.1 Account Management

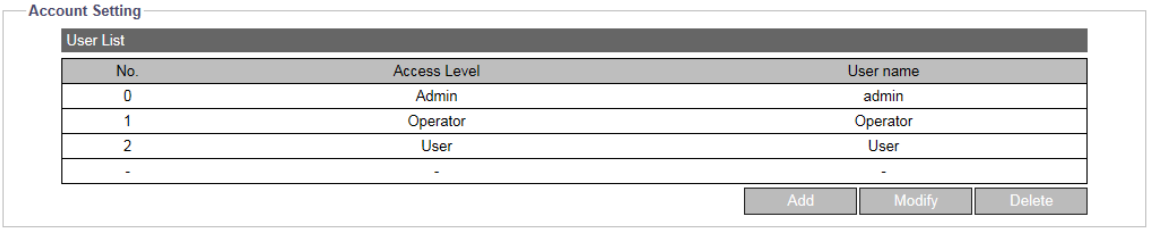


Figure: Account Settings

Account Setting

Access Level: Admin/Operator/User

- Admin: "Admin" level has the highest privilege control for accessing camera, allowing handling of both live view and all the configuration settings. The default username is ADMIN and password for Admin depends on user's initial setting.
- Operator: Operator level can only access camera for live view, storage and remote lens control functions.
- User: User level can only access camera for live view function.

Add Users

Figure: Add Admin/ Operator/ User

- Add: Place the mouse cursor over the blank row/column and click the "Add" button. A prompt window will display to enter a customized username and password for new user; the level (Admin, Operator or User) of user is also selected here.

Note	•	Up to 10 users are available.

Modify & Delete Users

- Delete: Choose one of the users from the list and then click "Delete" to remove it immediately. (The default Admin is not available to be deleted.)
- Modify: Choose one of the users from the list and enter updated information if necessary. Click "Save" for changes to take effect.

Caution	•	The login Username and Password must be 4 to16 characters long with the valid alphanumeric value only including '0' to '9', 'a' to 'z', 'A' to 'Z', '.','-','+','_'and '@'.
	•	The username cannot be the same as any currently existing username, included "admin".
	•	A user may reset the Account Management system to the camera's default settings.

6.2 LDAP

For accessing and maintaining distributed directory information services over an Internet Protocol network, the Lightweight Directory Access Protocol (LDAP), an open, vendor-neutral, industry standard application protocol, has a major role in both intranet and internet applications to facilitate information sharing between devices.

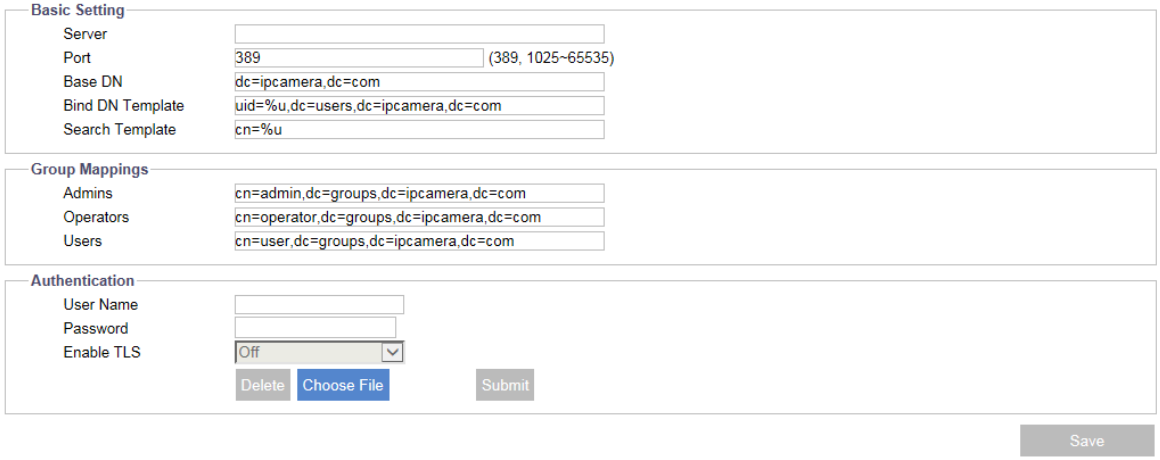


Figure: LDAP Settings

Basic Setting

Server

Input a server for LDAP.

Port: 389/1025 ~ 65535

It is recommended to use the default port number 389; however, if it is required to change the port number, contact your system administrator.

Base DN/Bind DN Template/Search Template

The strings within Base DN (Distinguish Name), Bind DN Template (sublevel of Base DN) and Search Template fields are updated by the LDAP server to be accessed. Refer to the fields here for later/further configuration.

Group Mappings

Admins/Operators/ Users

- Admins: Relates to the LDAP admin privileges, which are full access to Live View functionalities.
- Operators: Relates to the LDAP operator privileges, which are watching Live View and operating snapshot, manual recording and full screen.
- Users: Relates to the LDAP user privileges, which is only watching Live View.

The strings within Admins, Operators and Users fields are updated by the LDAP server to be accessed. Refer to the fields here for later/further configuration.

Authentication

User Name

Enter a designated username for authentication to the accessed LDAP.

Password

Enter the password corresponding to the entered username for correct authentication.

Enable TLS: On/Off

User can enable LDAP over TLS after uploading certificate. When TLS is enabled, the data transmission will be done through TLS mode, using encryption for the protection of data communication. (TLS is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet, which encrypts internet traffic of all types, making secure internet communication, and therefore internet commerce, possible.)

To turn TLS "On", first click "Choose File" button, then select and upload the desired CA file. Finally, click "Submit Query" button, then finally turn TLS "On".

"Delete" button is used for deleting submitted CA file from the settings.

After successfully completing all the required steps to enable LDAP over TLS, a user will be able to login using username and password according to the settings in the LDAP server.

Note

- Before enabling TLS, refer to "*4.9 SSL*" section to install or generate SSL certificate.
- Before starting using LDAP, a user must enable LDAP. Refer to *"4.1 General"* section for more details.

7. Event Source

Event source configurations consist of Event Specific, Handler and Arming Schedule. The table below gives an overview of event source configurations and relevant remarks.

Type	Settings			Remark
	Event Specific	Handler	Arming Schedule	
Alarm	NO/NC	V	V	
Audio	Sound Intensity	V	V	
Motion	Enable. Set object size/sensitivity in PTZ section	V	V	
Network	Wired Network Loss/ Wired Network Conflict	V	-	Does not support HTTP Generic Event.
Schedule	Regular/Persist trigger event action (without event source as premise)	V	V	Does not support HTTP Generic Event.
Tamper	Sensitivity	V	V	
mSD Healthiness	Free space/Mount failure	V	-	

Handlers

Alarm Out

Alarm output function will be enabled when an event occurs. Check the box to enable.

Audio

- Enable: Audio output function will be enabled when an event occurs. Check the box to enable.
- Sound: 1~10

  10 sound types are available from the dropdown menu for audio output. Be sure to set up the sound file beforehand. Refer to the "*9.7 Sound*" section for details.

Snapshot: Store to Edge/Store to FTP

- Store to Edge: Check the box to save snapshot to the SD card when event occurs; be sure a customer-supplied SD card is inserted in the slot to use this option.
- Store to FTP: Check the box to save snapshot to the FTP remote device when event occurs. Note that under Handler, the camera acts as FTP client, while the remote device acts as FTP server, and the FTP server path should be properly configured in advance in "*9.3 FTP*" section.

Recording

- Edge Record: Check the box to save the recorded video to the SD card when event occurs; be sure a customer-supplied SD card is inserted in the slot to use this option.

Email

- Enable: Check the box to enable an email to be sent to a predefined user when event occurs.
- Subject: Preset the subject of the email to be sent.
- Message: Preset message contents of the email to be sent.

OSD

- Enable: Check the box to enable the OSD function when an event occurs.
- Text: Input desired text manually to display when event occurs.

HTTP Generic Event

- Enable: Check the box to enable the function when event occurs.
- Method: 1~10

10 method types are available from the dropdown menu for message notification. After user sets the type of method, refer to "*9.8 HTTP Generic Event*" section for details about method setting.

Arming Schedule Setting: Monday ~ Sunday (24H)

Under this section, the user can set up a custom schedule for recording video when alarm input signal occurs. The following table includes 7 days a week from Monday to Sunday, 24 hours group from 0 to 24 hours. Click the "Edit" button at the upper-left corner to enter the setting page.

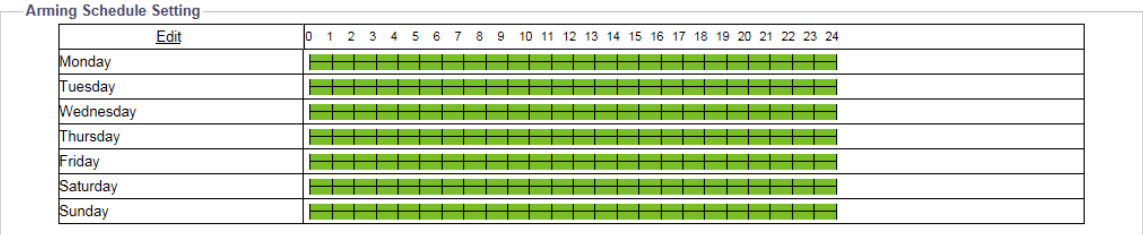
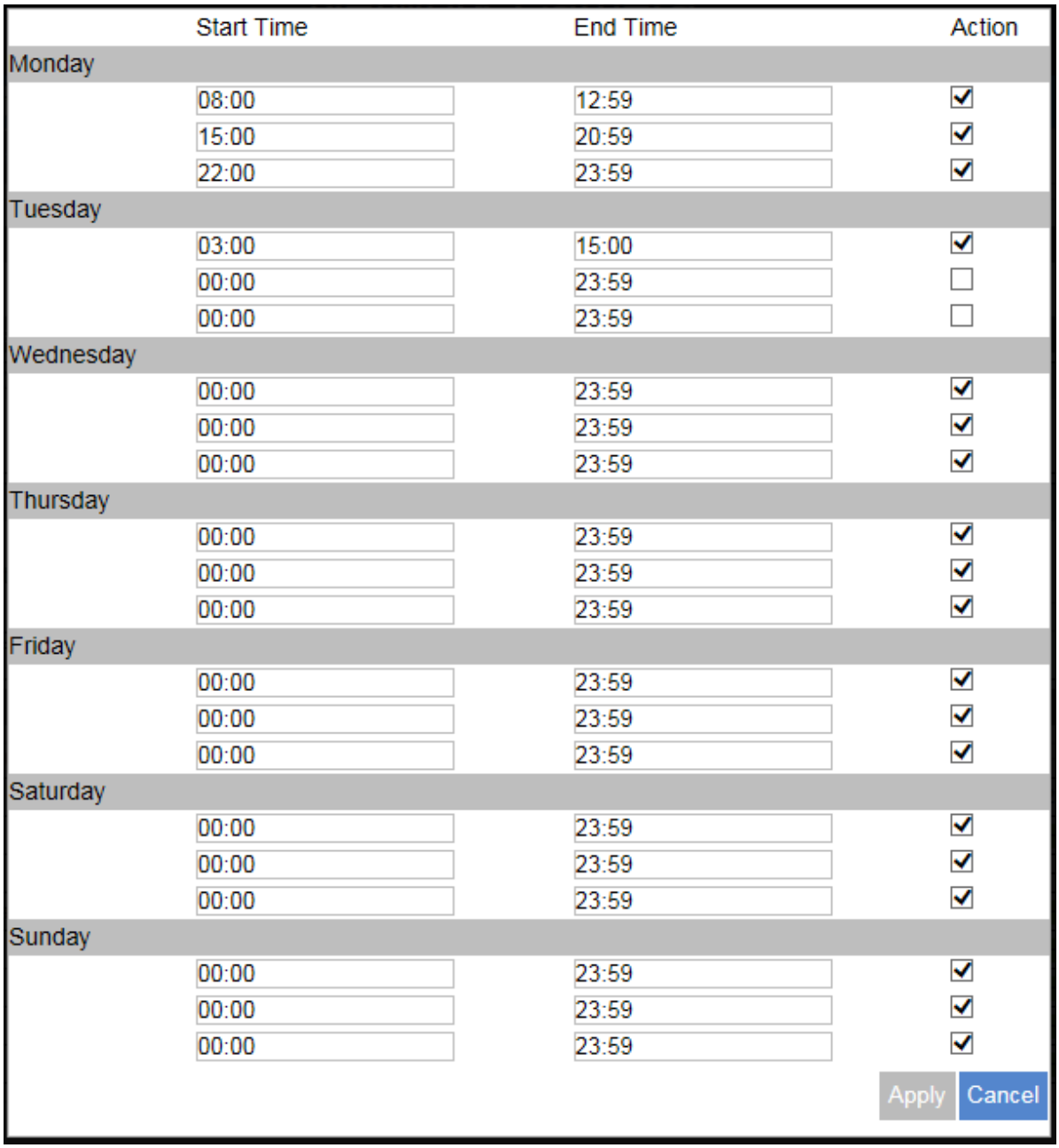


Figure: Arming Schedule Setting

After clicking "Edit," the prompt setting page will display as below. By default, the boxes are all checked 24/7. User can individually establish up to 3 sets of time ranges for each day, where start and end time can be separately defined. Check the box on the right side to enable the defined time range, followed by clicking "Apply" for it to take effect.

The screenshot above shows that the defined time ranges are highlighted with bright green color to indicate any alarm input signal within the green time ranges will be recorded properly. . The screenshot below shows that the 2 time ranges, Monday (08:00 – 24:00) and Tuesday (03:00 – 15:00), are properly defined and checked; the other days remain set for 24/7.



	Start Time	End Time	Action
Monday			
	08:00	12:59	☑
	15:00	20:59	☑
	22:00	23:59	☑
Tuesday			
	03:00	15:00	☑
	00:00	23:59	☐
	00:00	23:59	☐
Wednesday			
	00:00	23:59	☑
	00:00	23:59	☑
	00:00	23:59	☑
Thursday			
	00:00	23:59	☑
	00:00	23:59	☑
	00:00	23:59	☑
Friday			
	00:00	23:59	☑
	00:00	23:59	☑
	00:00	23:59	☑
Saturday			
	00:00	23:59	☑
	00:00	23:59	☑
	00:00	23:59	☑
Sunday			
	00:00	23:59	☑
	00:00	23:59	☑
	00:00	23:59	☑

Apply Cancel

Figure: Arming Schedule Setting

7.1 Alarm

Connecting an alarm input device with the camera can expand alert functions. For example, when an infrared detector connected to the camera detects motion based on heat emission, an alarm input message will be sent to the camera. Additionally, by connecting to an alarm output device such as siren, the camera will send a signal to notify the siren and activate it when receiving an alarm signal either from alarm input device or other detection settings. This page is designed to establish related actions when the camera receives alarm input signal.

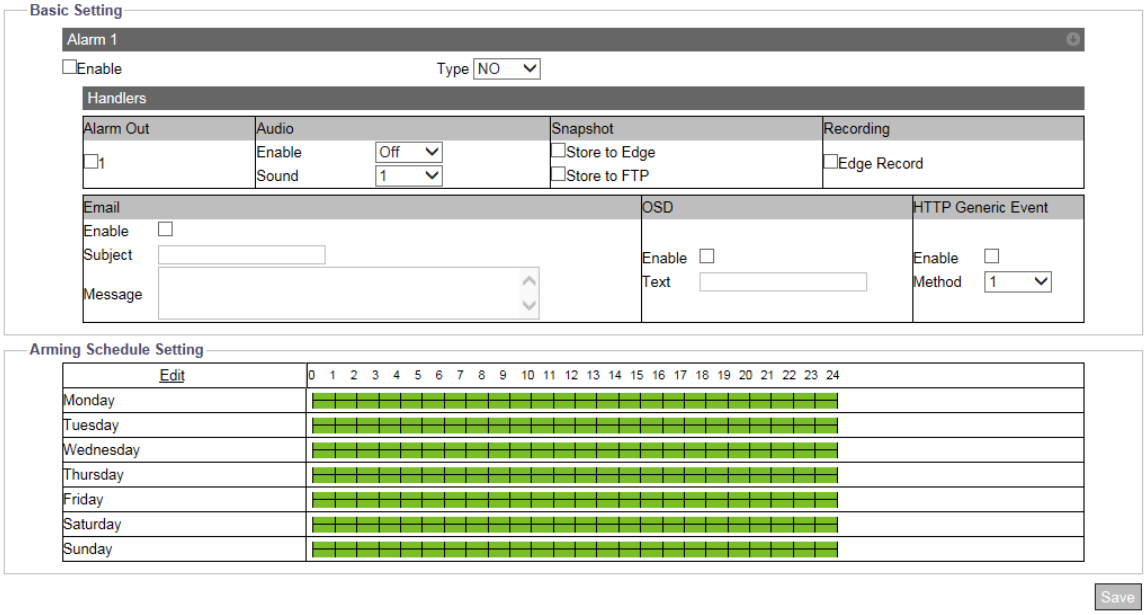


Figure: Alarm Event Settings

Basic Setting

Enable: Check the box to enable the alarm input function.

Type: NO/NC

NO (Normally Opened): An alarm will be triggered when the external contact closes.
NC (Normally Closed): An alarm will be triggered when the external contact opens.

7.2 Audio

By connecting to an audio input device, e.g., microphone, the camera can receive an audio input signal from the microphone and react with the certain responses that are preset under this section. Review the information below for details.

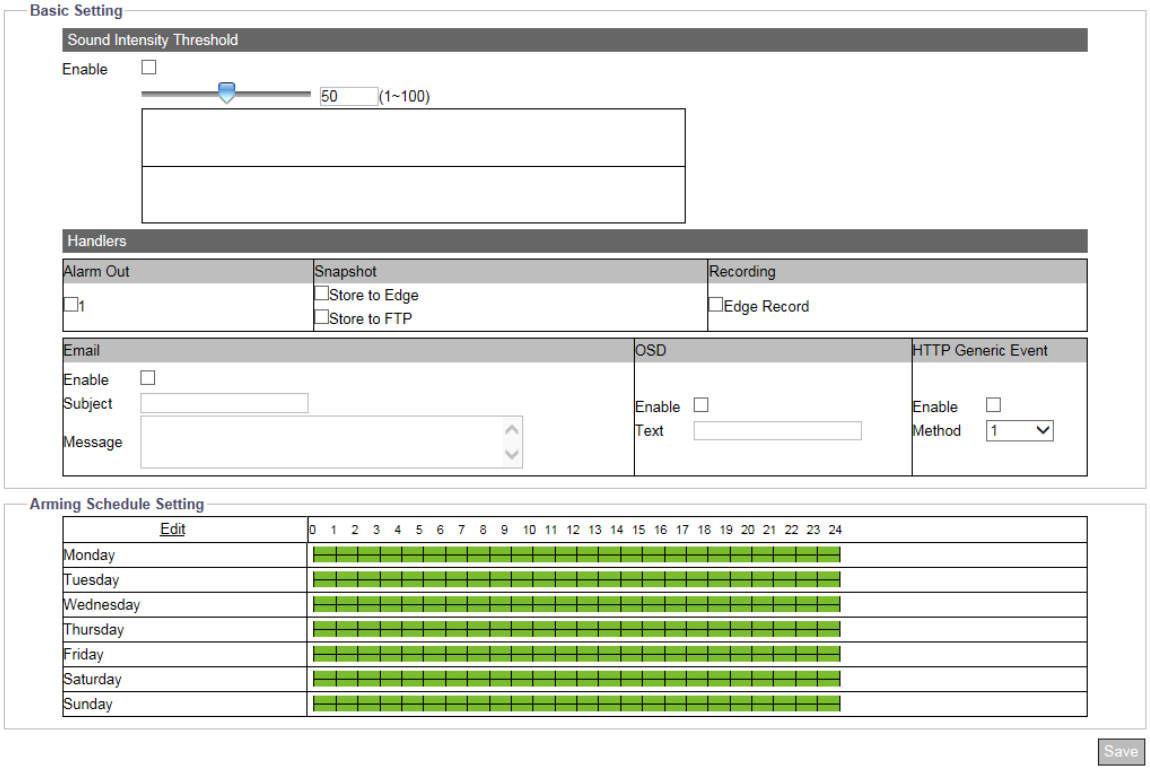


Figure: Audio Event Settings

Basic Setting

Enable: Check the box to enable the audio input event function.

Sound Intensity Threshold: 1 ~ 100

Define an exact sound intensity threshold to trigger the actions when the camera receives audio signal from the connected input device. Select 100 for the highest sound intensity threshold.

7.3 Motion

This function is designed to establish related actions when the camera detects motion issues. Motion detection areas are setup from the PTZ Settings, Preset screen, but the function must be Enabled from this screen first. See below and Section 10.4 of this manual for details.

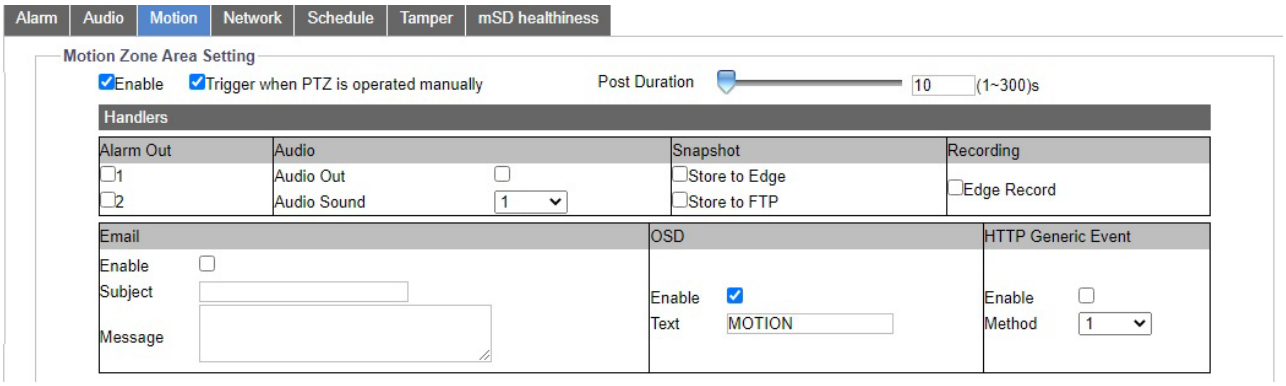


Figure: Motion Detection Settings

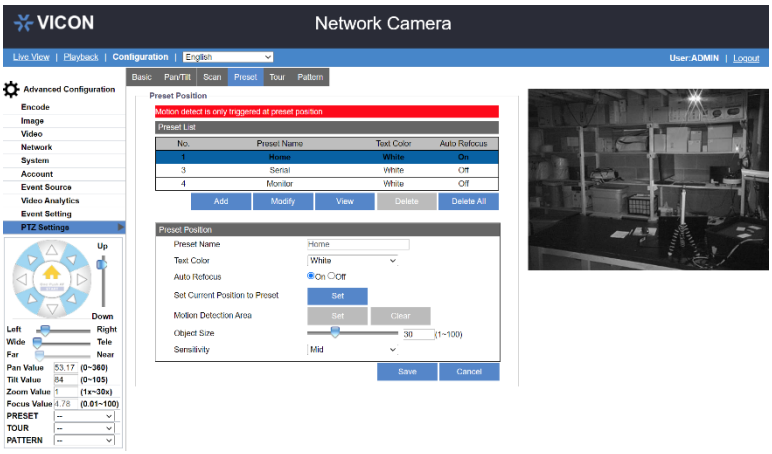
Motion Zone Area Setting

Enable

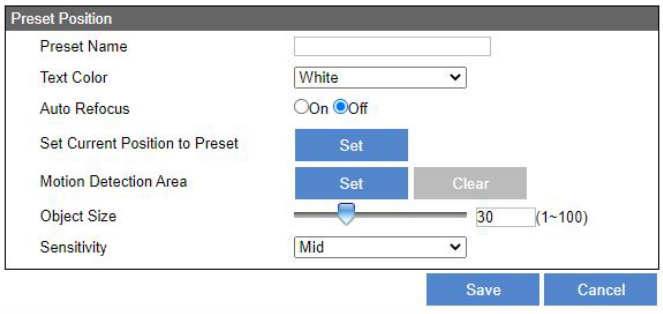
Check the Enable box. Configure the event source (Handlers) and required actions from the arming schedule and click "Save" to have the settings take effect.

Setting the Motion Detection Area

Go to PTZ Settings, Preset. Select a preset from the list and click Modify or click Add to create a new preset.



The popup below displays. Click the Set button for Set Current Position to Preset (if this is a new preset, position the camera and click Save). After the Set button for Set Current Position to Preset is clicked, the Set button for Motion Detection Area turns blue. In the Motion Detection Area, click the Set button. Using the cursor, draw the area in which motion is to be detected. A colored box will overlay on the video; optimize object size and sensitivity as needed. Click Save. A small red icon will appear to the left of the preview image.



7.4 Network

This function is designed to configure related actions when the camera is subject to network conflict or network lost events.

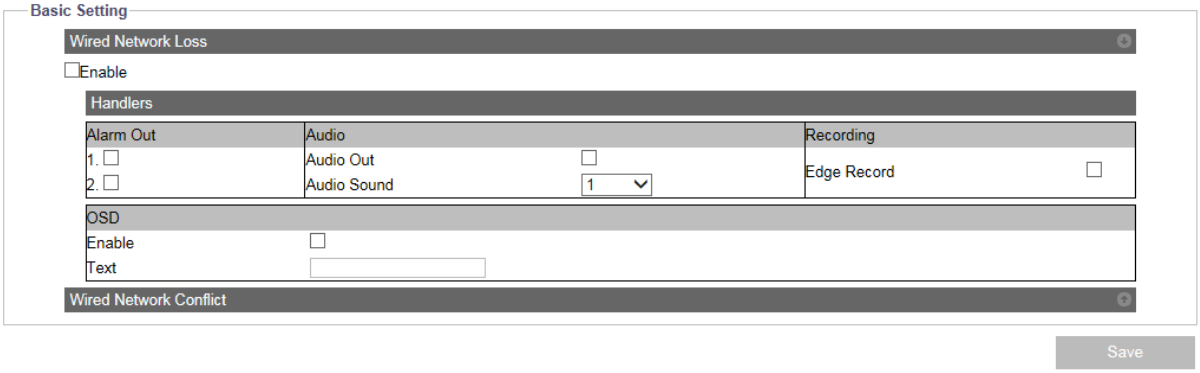


Figure: Network Event Settings

Basic Setting

Wired Network Loss

Check the box to enable the detection of network loss. When the camera loses internet access, the network loss event will be detected and recorded.

Wired Network Conflict

Check the box to enable the detection of network conflict. When there is another IP address conflicting with the camera, the network conflict event will be detected and recorded.

Note	• Press the arrow buttons at the upper-right corner to expand or collapse the setting pages of Network Lost and Network Conflict.

7.5 Schedule

This function is designed to establish related actions for recording schedule, independent of any event.

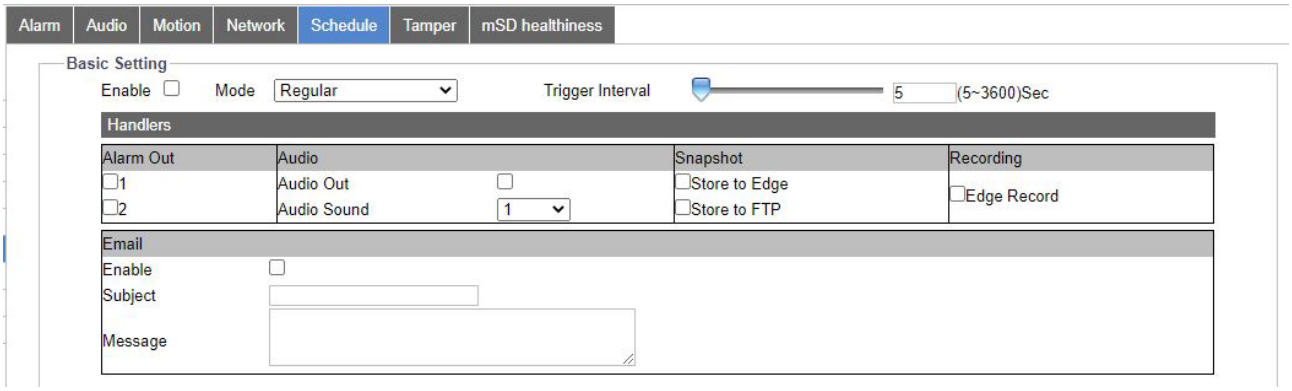


Figure: Recoding Schedule Settings

Basic Setting

Enable: Check the box to enable recording schedule function.

Mode: Regular/Persist

- Regular: When enabled, the recording schedule will progress on a regular basis on the trigger interval settings.
- Persist: When enabled, regardless of interval, the recording schedule will progress continuously.

Trigger Interval: 5 ~ 3600 (sec)

The trigger interval is the time between two alarms when in Regular mode. The interval time starts when the previous finishes through when the next alarm is triggered. For example, if "60", schedule under Regular mode triggers on 60 seconds per time, so if an alarm is triggered during 12:00:00, 12:00:10 (alarm duration of 10 seconds), the following alarm will not be triggered until 12:01:00 with a defined interval time of 60 seconds.

7.6 Tamper

This function is designed to establish related actions when the camera is subject to tamper events.

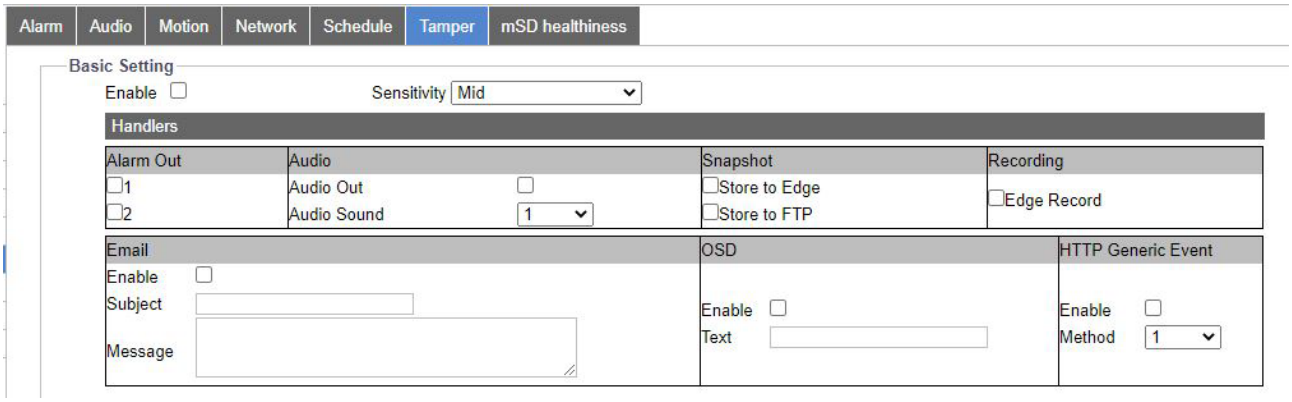


Figure: Tamper Detection Settings

Basic Setting

Enable: Check the box to enable tamper detection.

Sensitivity: High/Mid/Low

Set the sensitivity for tamper detection. High means that camera can be triggered with a minor tamper issue, while Low means that camera is triggered with only a major tamper issue.

Note	• It is recommended to use Tamper function only when no PTZ operation is being performed, that is when the camera view does not change

7.7 mSD Healthiness

This function is designed to establish related actions when the inserted micro SD card has unexpected failed events or is running out of sufficient storage space.

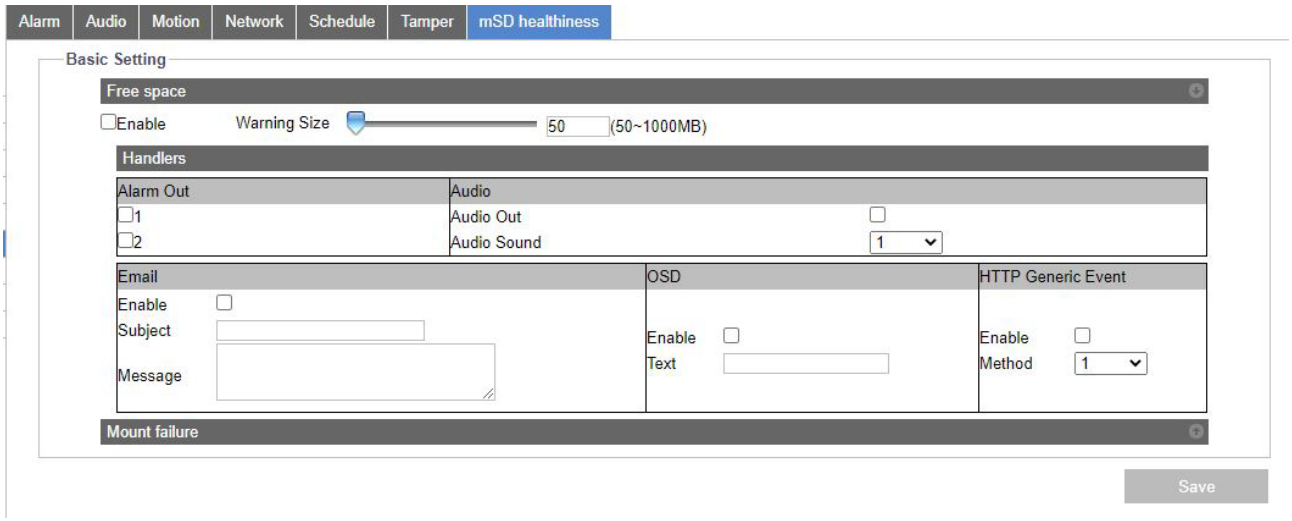


Figure: mSD Healthiness Settings

Micro SD Card Events

Free space

Check the box to enable the detection of insufficient space of the inserted micro SD card. When there is insufficient space on the inserted micro SD card, the selected handlers will be activated. Slide the "Warning Size" bar to define a space threshold for trigger.

Mount failure

Check the box to enable the detection of failure of the inserted micro SD card. When any failure issue occurs on SD card, the selected handlers will be activated.

Note	• Press the arrow buttons at the upper-right corner to expand or collapse the setting pages of "Free space" and "Mount failed."

8. Video Analytics: V2002D-PTZ Only

Video Analytics (VA) comprises the proprietary algorithm to perform intelligent video analysis, e.g., to detect intrusion or loitering within defined zone from suspicious objects or to count people and traffic flow by designated line deployment. It is especially practical to monitor certain alert areas or key zones; this relieves administrator from constantly staying in front of the monitor by recording only critical scenes where events happen, facilitating interoperability and reducing required recording storage for surveillance camera.

Video Analytics configurations consist of Video Analytic specific settings, Handler and Arming Schedule. The Table below presents an overview of event source configuration and dependency.

Type	Settings			Remark
	VA Specific	Handler	Arming Schedule	
General	Motion sensitivity and object size.	-	-	
Line Counting	Set line 1~3 and direction.	V	V	
Line Cross	Set line 1~3 and direction.	V	V	
Loitering	Set area and trigger interval.	V	V	
Area Counting	Set area.	V	V	
Intrusion	Set area.	V	V	
Object Removed	Set object and trigger interval.	V	V	
Wrong Direction	Set line and angle.	V	V	
Object Left	Set area and trigger interval.	V	V	

Note

- When camera executes PTZ related commands, the VA functions should disable automatically.

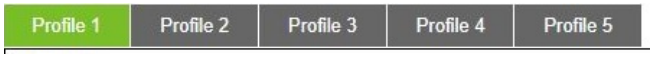
8.1 Setup Guidelines

There are five (5) profiles that can be setup for video analytics. Each profile can be associated with an analytic and a preset position. Only one (1) analytic can be assigned to each preset. The same type of analytic can be associated with multiple different presets. However, Line Crossing can be paired with Line Counting and Intrusion can be paired with Area Counting using the referenced analytic in the pair.

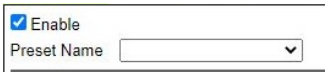
Follow the steps below to setup each analytic. The specifics for each type of analytic will follow in each section.

1. Select the analytic from the tabs at the top.

2. Select a profile.



3. Enable the analytic and then select a preset name from the dropdown list. Go to the preset in the PTZ pane.

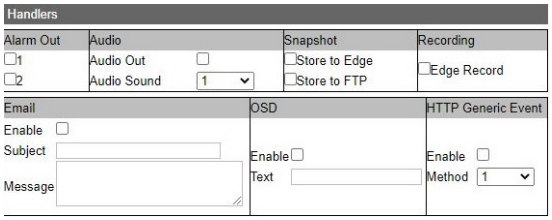


4. For additional profiles, it is important to select the profile number first and then select the desired analytic and a different preset. Only one (1) analytic can be assigned to a preset.

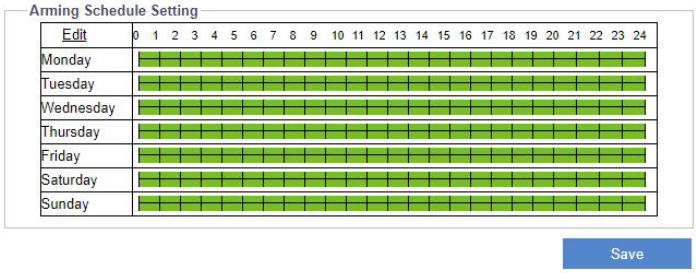
Caution: If, for example, profile 1 was programmed for Intrusion, and then Line Crossing was selected before profile 2 is selected, profile 1 could potentially be reprogrammed with a different

analytic. A warning will be sent if a preset is set to be used again.

5. Each analytic has a Handler section. Handler is used to define how to deal with the video analytics result (e.g., audio out, alarm out, recording, etc.).



6. Each analytic has an Arming Schedule Setting: Arming schedule is used to decide when to enable the video analytics function. Click the "Edit" button at the upper-left corner to enter the setting page. After clicking "Edit," the prompt setting page will display. User can individually establish up to 3 sets of time ranges for each day, where start and end time can be separately defined. Check the box at the right side to enable the defined time range, followed by clicking "Apply" for it to take effect.



The unique steps to set up each individual analytic follow.

8.3 General

This page contains general settings shared by all VA functions. Prior to setting up each VA function, it is fundamental to define the settings here before advancing to other function settings.

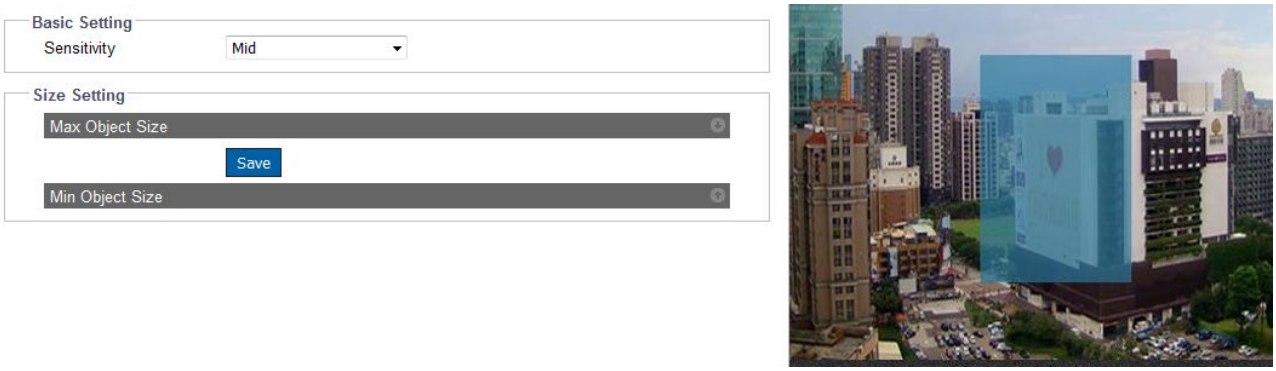


Figure: Video Analytics: General Settings

Basic Setting

Sensitivity: High/Mid high/Mid/Mid Low/Low

Choose a sensitivity level from the dropdown menu to define a clear threshold for triggering all VA functions. High represents VA functions will be triggered easily by slight events, while Low triggering occurs only when major events occur.

Size Settings

Max Object Size

Draw a desired maximum object size in the right-side preview window and then click "Save" to enable the settings. Any object larger than the maximum size defined here will neither be detected, nor triggered.

Min Object Size

Draw a desired minimum object size in the right-side preview window and then click "Save" to enable the settings. Any object smaller than the minimum size defined here will neither be detected, nor triggered.

Note	• Press the arrow buttons at the upper-right corner to expand or collapse the setting pages of "Max Object Size" and "Min Object Size" individually. • It is strongly recommended to define a fitting size range in accordance with desired objects to be detected. This will increase the accuracy of VA functions.

8.4 Line Counting

This function is designed to count the moving objects that passed through the designated line defined by users. Appropriate applications for this function, for instance, can be an entrance of a shopping mall or exit of a department store. Also, it can be applied to count the traffic flow of an intersection.

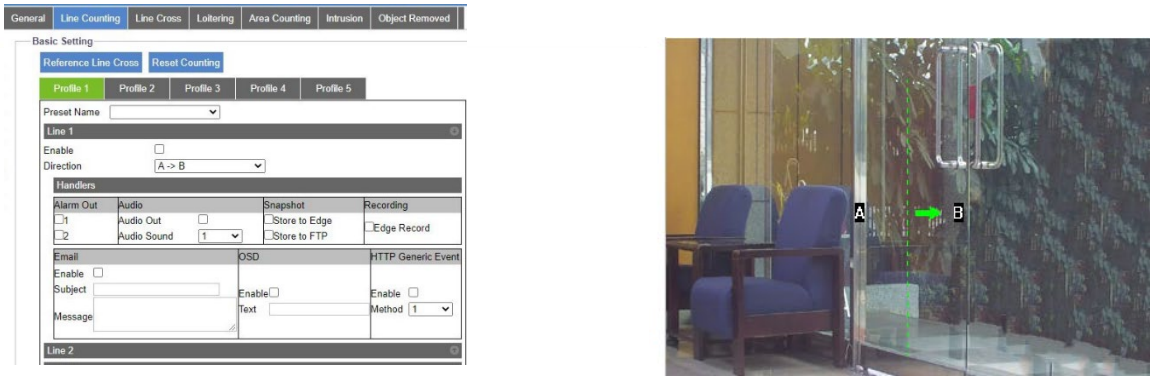


Figure: Line Counting Settings

Line Setting

Reference Line Cross

Pressing this button will allow user to apply the identical line deployment settings referred from Line Cross function, an easy way to prompt setup and implement.

Reset Counting

Pressing the button will erase the accumulated counting records.

Line 1 ~ 3

Check the box to enable each line setting. Press the arrow buttons at the upper-right corner to expand or collapse the setting page of Line 1 to Line 3 individually. The options from Direction dropdown menu (A to B, B to A) helps user to define the exact direction to be counted.

Method

Press and hold cursor on the right-side preview image to draw a line on the selected area and then click the "Save" button to have the settings take effect. Up to 3 lines can be assigned concurrently.

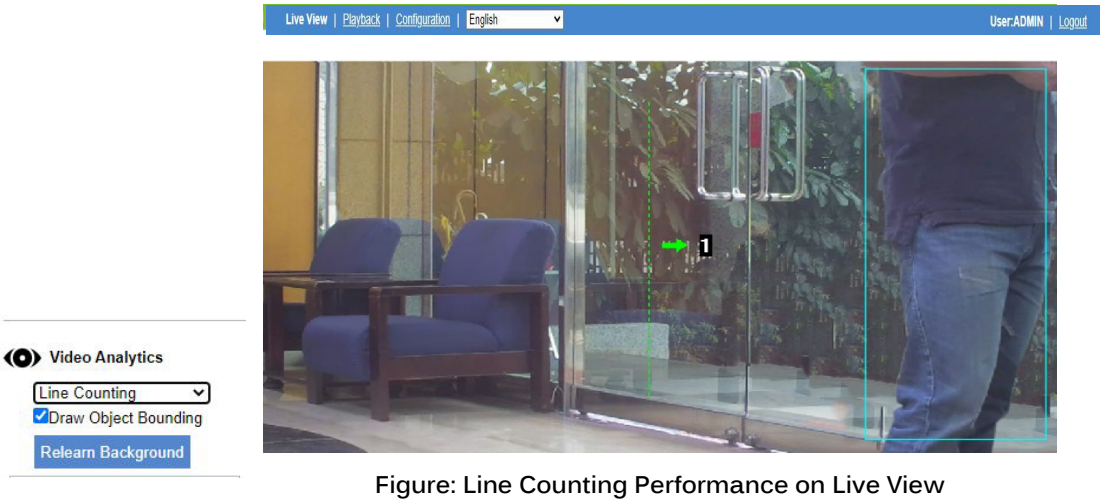


Figure: Line Counting Performance on Live View

Performance

Switch to the Live View page and select "Line Counting" from the lower-left VA dropdown menu. When there is a moving object traveling through the designated line as in the above image, the number coming along with the arrow and line will increase ("1" shown in the image). Additionally, any moving object within the Live view will be framed by a blue rectangle for clear identification.

8.5 Line Cross

This function is designed to establish borderlines to guard certain alerted zones within the camera coverage. For example, administrator can assign multiple lines bordering the area where a valuable object is located to efficiently monitor any suspicious person crossing those borderlines deployed.

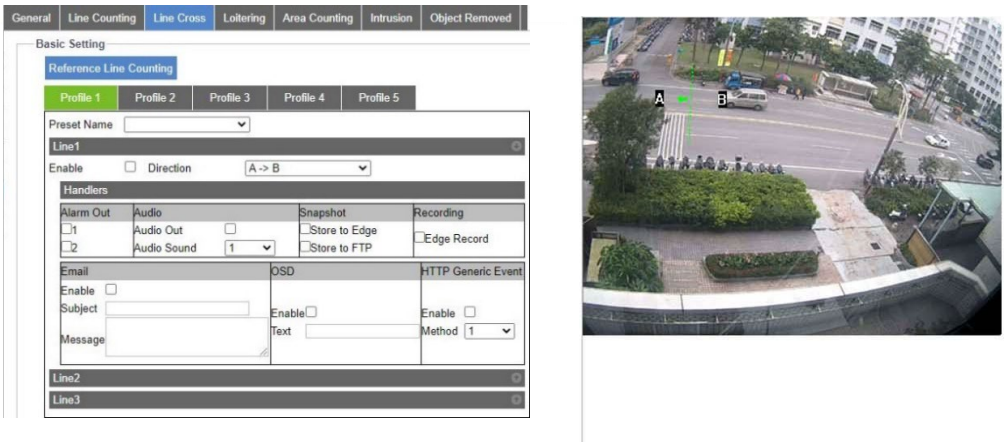


Figure: Line Cross Settings

Basic Setting

Reference Line Counting

Pressing this button will allow user to apply the identical line deployment settings referred from Line Counting function, an easy way to prompt setup and implement.

Line 1 ~ 3

Check the box to enable each line setting. Press the arrow buttons at the upper-right corner to expand or collapse the setting page of Line 1 to Line 3 individually. The options from Direction dropdown menu (A to B, B to A) helps user to define the exact direction to be counted.

Method

Press and hold the cursor on the right-side preview image to draw a line on the desired area and then click the "Save" button to have the settings take effect. Up to 3 lines can be assigned concurrently.

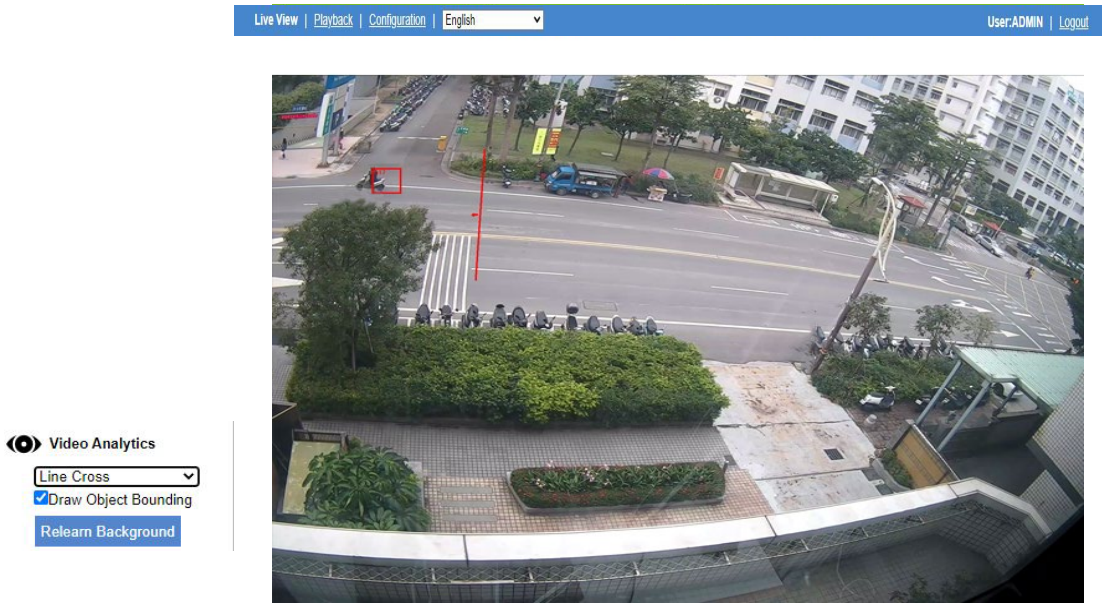


Figure: Line Cross Performance on Live View

Performance

Switch to the Live View page and select "Line Cross" from the lower-left VA dropdown menu. When there is a moving object crossing the designated line as in the above image, both the crossed borderline and the rectangular frame enclosing the moving object are highlighted with red color for distinctive identification. Any moving object within the Live view will be framed by a blue rectangle for clear recognition.

8.6 Loitering

This function is designed to intelligently observe suspicious objects that enter and linger for a designated period within the alert area defined by administrator. This is a practical way to monitor key zones without wasting human resources to keep vigil in front of monitor 24/7.

Figure: Loitering Settings

Basic Setting

Enable: Check the box to enable the loitering detecting function.

Trigger Interval: 5 ~ 300

Define a value for the threshold period to trigger loitering alarm by any suspicious object/person that enters and lingers in the zone over that value.

Method

Draw a desired shape (octagon at the maximum) covering the key zone for loitering detection and then click "Save" to have the settings take effect.

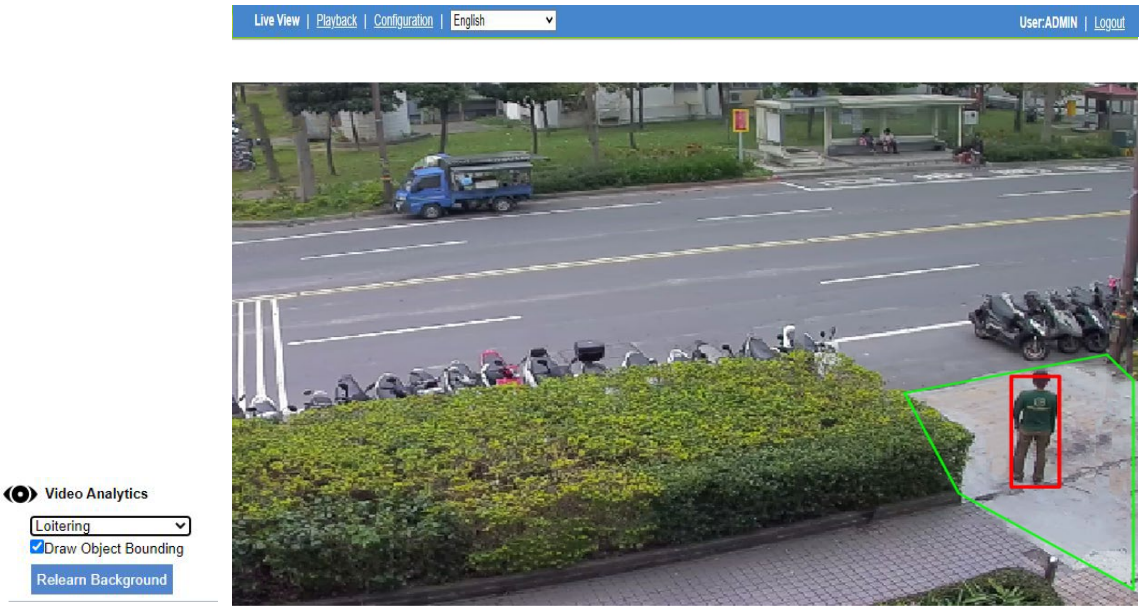


Figure: Loitering Performance on Live View

Performance

Switch to the Live View page and select "Loitering" from the lower-left VA dropdown menu. When there is a moving object/person traveling into and lingering within the designated zone over a designated period of time defined by administrator, as in the above image, the rectangular frame enclosing the suspicious object/person is highlighted with red color for distinctive identification. Any moving object within the Live view will be framed by a blue rectangle for clear recognition.

8.7 Area Counting

In some locations, e.g., parking lot, administrator may have the need to compile statistics on objects that get into or move off the location. By implementing the Area Counting function, administrator can easily gather statistics by intelligent surveillance camera.

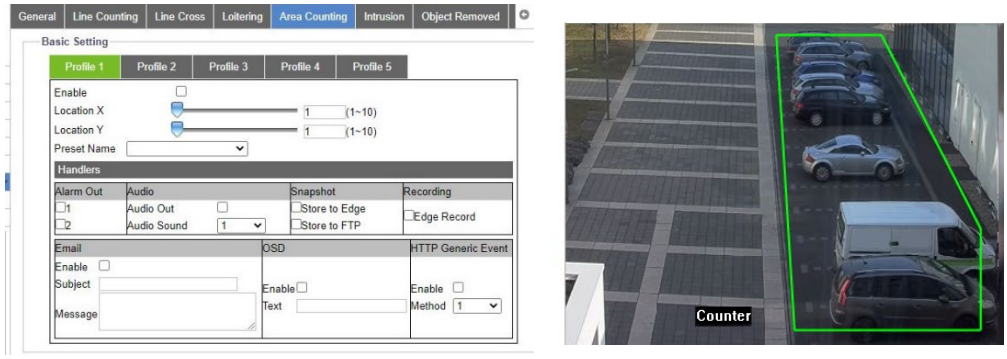


Figure: Area Counting Settings

Basic Setting

Enable: Check the box to enable the area counting function.

Location X & Location Y: 1 ~ 10

Input a value or simply slide the bar to define the exact location for the OSD counter, which records numbers accumulated by both exit and entry of the defined zone.

Method

Draw a desired shape (octagon at the maximum) covering the desired zone for area counting and define a location for OSD counter; then "Save" to have the settings take effect.

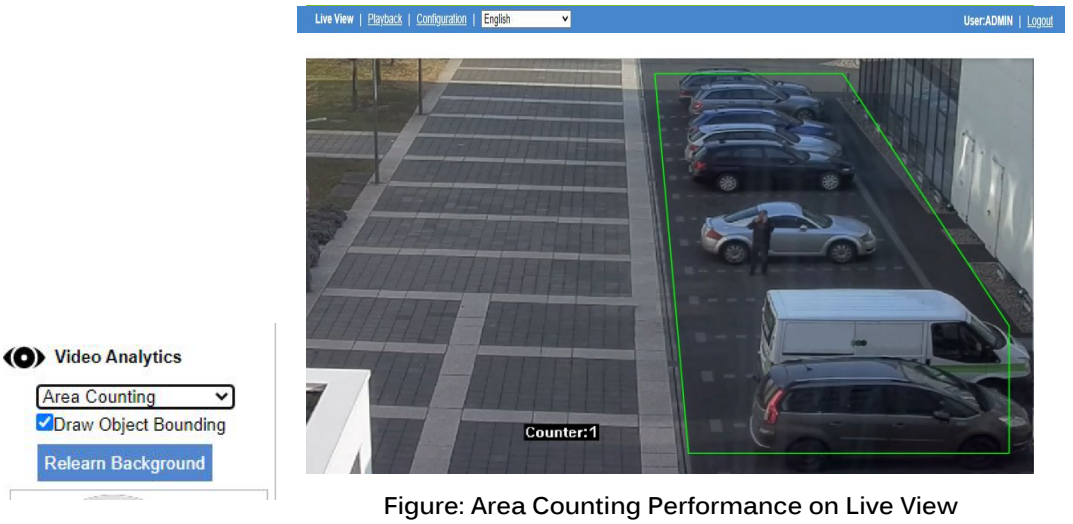


Figure: Area Counting Performance on Live View

Performance

Switch to the Live View page and select "Area Counting" from the lower-left VA dropdown menu. When there is a moving object entering into or moving off the designated area defined by administrator, as in the above image, the OSD counter will show the digit that represents the accumulated number from objects entering and leaving the designated area. Additionally, any moving object within the Live view will be framed by a blue rectangle for clear recognition.

8.8 Intrusion

Intrusion is a function where administrator can define an irregular shaped an area (octagonal at the maximum) to watch if any suspicious object enters the area. Using Intrusion, administrator can effortlessly have command of a critical zone and receive a prompt warning if any object trespasses the defined critical zone in real-time.

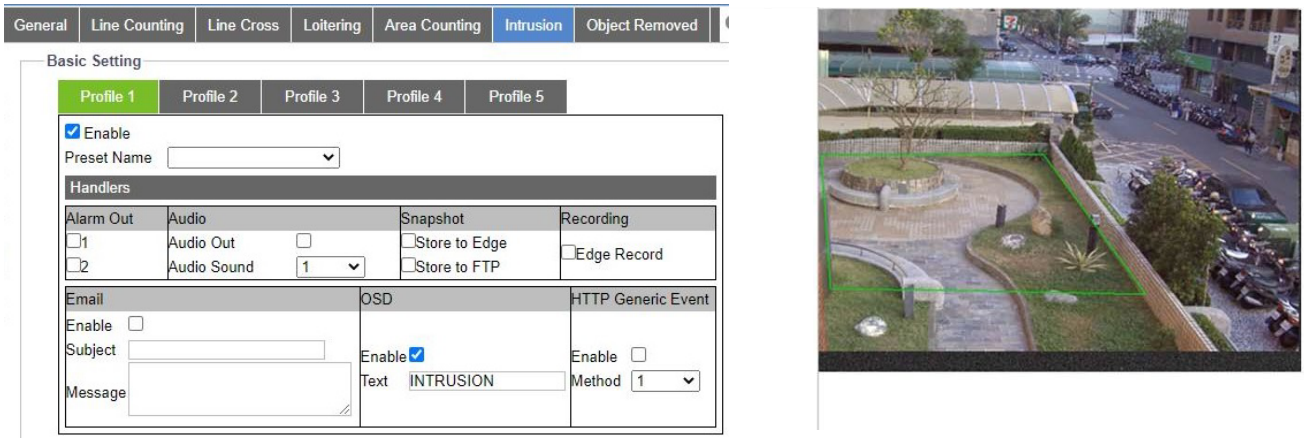


Figure: Intrusion Settings

Basic Setting

Enable: Check the box to enable the intrusion detecting function.

Method

Draw a and then click "Save" to have the settings take effect.

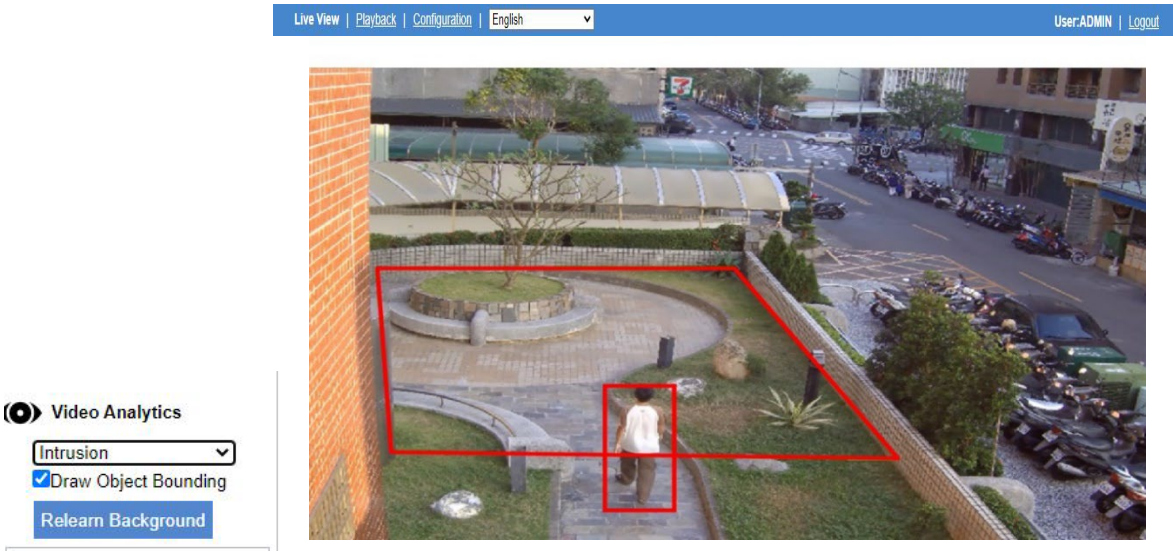


Figure: Intrusion Performance on Live View

Performance

Switch to the Live View page and select "Intrusion" from the lower-left VA dropdown menu. When there is a moving object trespassing into the designated critical zone defined by administrator, as in the above image, both the rectangular frame enclosing the suspicious object and the defined zone are highlighted with red color for distinctive identification. Additionally, any moving object within the Live view will be framed by a blue rectangle for clear recognition.

8.9 Object Removed

Object Removed detection was developed with the objective to guarantee that selected valuable objects are properly monitored and safeguarded. For example, the owner of a jewelry store would want to secure that each piece of jewelry is protected.

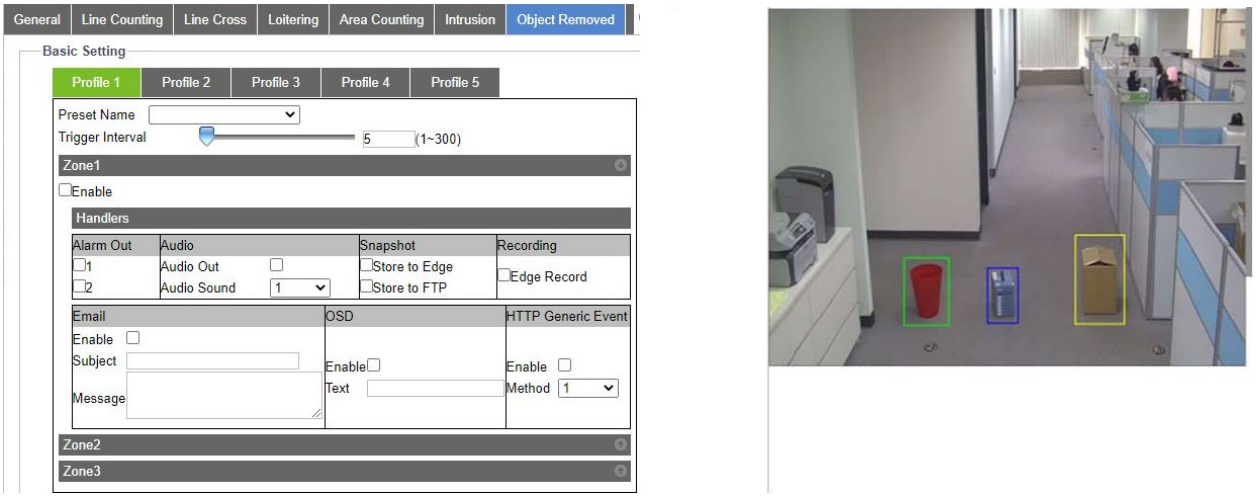


Figure: Object Removed Settings

Basic Setting

Trigger Interval

Define an exact threshold of time to trigger Object Removed detection. Either use the slider or enter an exact number in the field.

Zone 1 ~ 3

Check the box to enable each zone setting. Press the arrow buttons at the upper-right corner to expand or collapse the setting page of Zone 1 to Zone 3 individually.

Method

Draw a desired rectangular zone covering the critical item for Object Removed detection and then click "Save" to have the settings take effect. Up to 3 zones can be set up having varied color indications.

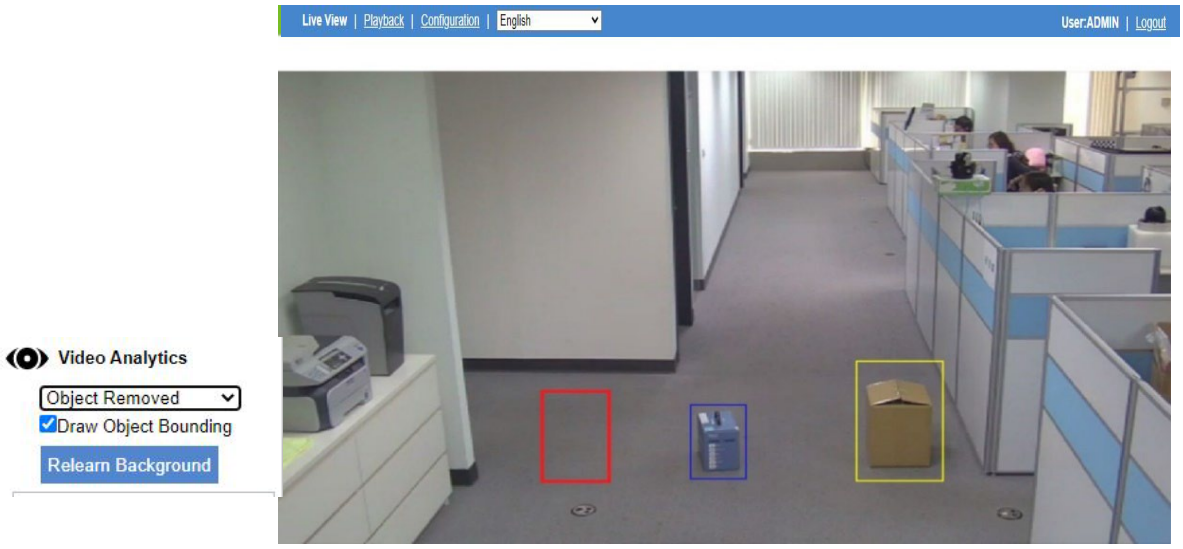


Figure: Object Removed Performance on Live View

Performance

Switch to the Live View page and select "Object Removed" from the lower-left VA dropdown menu. When any of the items marked by colored zones is taken away, as in the above image, the zone will be highlighted with red color to indicate the original item was taken away. Additionally, any moving object within the Live view will be framed by a blue rectangle for clear recognition.

8.10 Wrong Direction

The Wrong Direction function can be used to track vehicles or people that move in a direction that is not permitted. It can help control vehicles that may violate regulations for one-way street or people entering through an exit.

Figure: Wrong Direction Settings

Basic Setting

Enable: Check the box to enable the wrong direction detecting function.

Method

Press and hold the mouse to draw a green line on targeted area; the blue included angle in the proximity of the green line, appears to indicate the permitted range for vehicles passing. By contrast, the areas out of the boundary of included angle are the sensitive zones to trigger Wrong Direction detection once any vehicle enters. The blue included angle can be enlarged up to 180° and shrunk to the lowest 15° for flexible applications. Also, direction of included angle can be adjusted by simply press and hold to move the middle arrow.

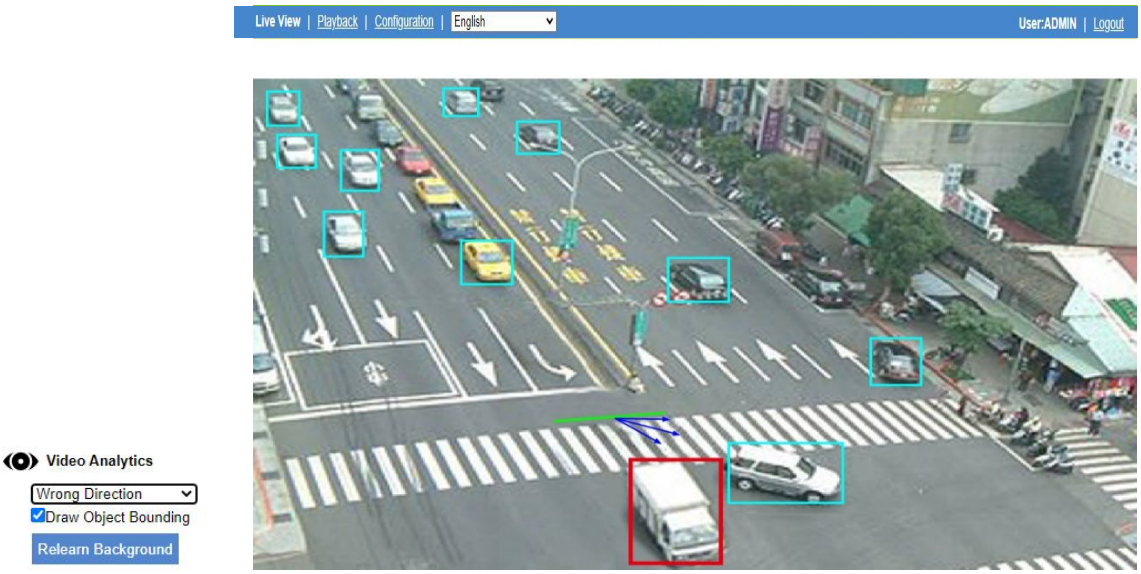


Figure: Wrong Direction Performance on Live View

Performance

Switch to the Live View page and select "Wrong Direction" from the lower-left VA dropdown menu. When there is a moving vehicle crossing the green line but toward a direction away from the permitted range, i.e., blue included angle, the rectangular frame enclosing the detected vehicle is highlighted by red color for distinctive identification, as in the above image. Additionally, any moving object within the Live view will be framed by a blue rectangle for clear recognition.

8.11 Object Left

The detection function "Object Left" is specifically designed to prevent an object from being intentionally deposited in a critical place, e.g., entrance of building or subway station. If a person deliberately leaves an object, such as a backpack, it can be intelligently detected and determined a suspicious abandoned object.

Figure: Object Left Settings

Basic Setting

Enable: Check the box to enable the Object Left detecting function.

Trigger Interval: 5 ~ 300

Define a value for the threshold period to trigger Object Left alarm for any suspicious object that was left within the zone over the value.

Method

Draw a desired shape (octagon at the maximum) covering the key zone for Object Left detection and then click "Save" to have the settings take effect.

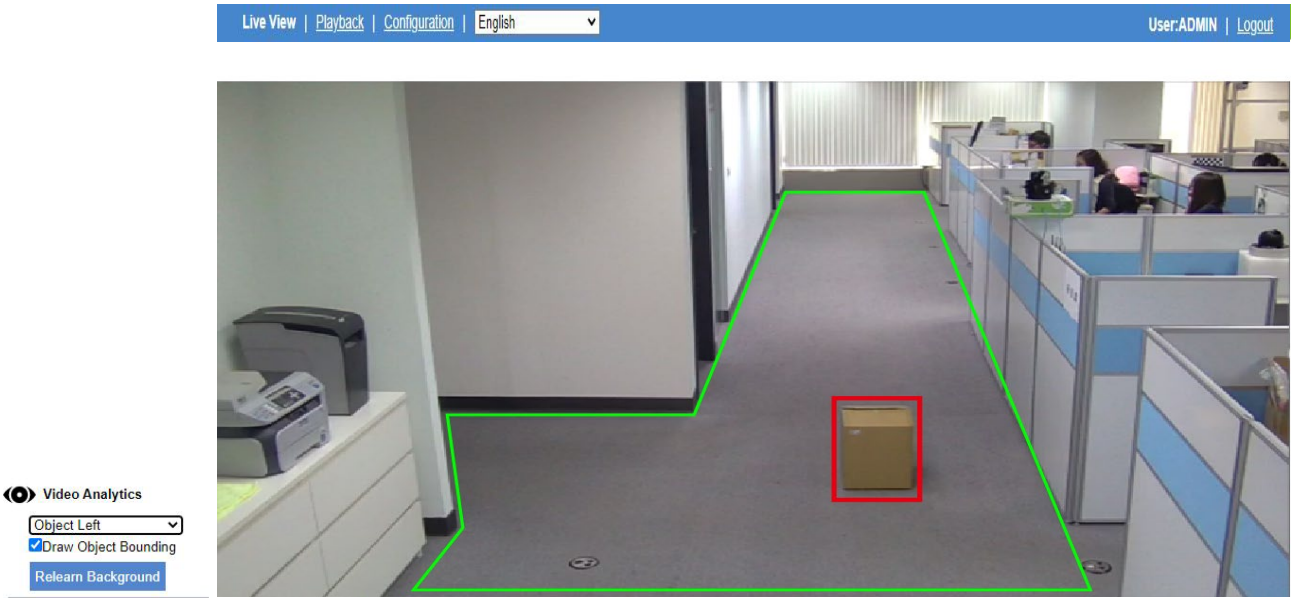


Figure: Object Left Performance on Live View

Performance

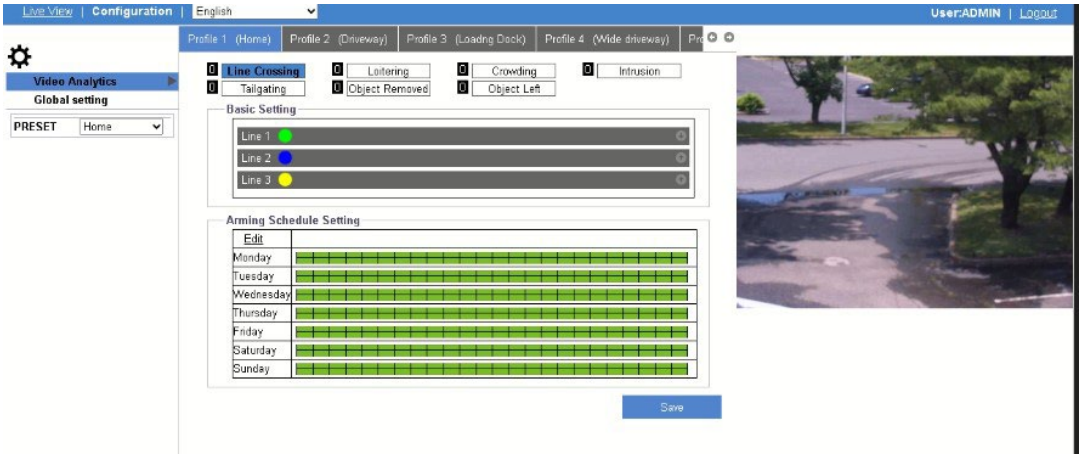
Switch to the Live View page and select "Object Left" from the lower-left VA dropdown menu. When there is a suspicious object left within the designated zone over a certain period of time defined by administrator, as in the above image, the rectangular frame enclosing the suspicious object is highlighted with red color for distinctive identification. Additionally, any moving object within the Live view will be framed by a blue rectangle for clear recognition.

9. Video Analytics: V2005D-PTZ Only

Video Analytics with object classification technology processes digital video using a special AI algorithm to perform security related functions. Using these analytics provides a practical solution to reviewing hours of surveillance video to identify incidents that have been configured, increasing efficiency of security monitoring.

From the Configuration tab, select Advanced Analytics from the list on the left side. A new tab opens, and the left list now lists Video Analytics and Global setting. Each of these will be explained below.

The screen below displays, showing the Video Analytics available, Line Crossing (includes Line Counting), Loitering, Crowding, Intrusion, Tailgating, Object Removed and Object Left. Select the analytic to configure.



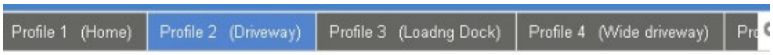
Video Analytics configurations are VA specific for Handler and Arming Schedule. The table below gives an overview of event source configuration and dependency.

Type	Settings		
	VA Specific	Handler	Arming Schedule
Line Cross (includes Counting)	Set line 1~3 and direction.	✓	✓
Loitering	Set area 1~3 and trigger interval.	✓	✓
Crowding	Set area 1~3.	✓	✓
Intrusion	Set area 1~3.	✓	✓
Tailgating	Set line 1~3, direction and trigger interval.	✓	✓
Object Removed	Set area 1~3 and trigger interval.	✓	✓
Object Left	Set area 1~3 and trigger interval.	✓	✓

9.1 Setup Guidelines

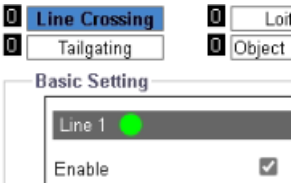
Before analytics can be configured, presets must be configured as explained in the PTZ section of this manual. There are five (5) profiles (relating to presets) that can be setup for video analytics. Each profile can be associated with analytics and a preset position. The same type of analytic can be associated with multiple different presets.
Follow the steps below to setup each analytic. The specifics for each type of analytic will follow in each section.

1. Select a profile.



2. Select the analytic from the tabs at the top.

3. Enable the analytic.



4. Follow the directions that follow for setting up each type of analytic. Be sure to save each one for the configuration to take effect.

9.2 Line Crossing

Line Crossing is designed to establish borders to outline certain zones within the camera coverage. For example, these lines can outline an entry way or the perimeter of a property. This feature also does line counting and these values are presented in the analytics Live page; the line count is the number of times the line is crossed, based on the parameters configured for the analytic. Up to 3 lines can be configured, each noted by a different color, green, blue or yellow.

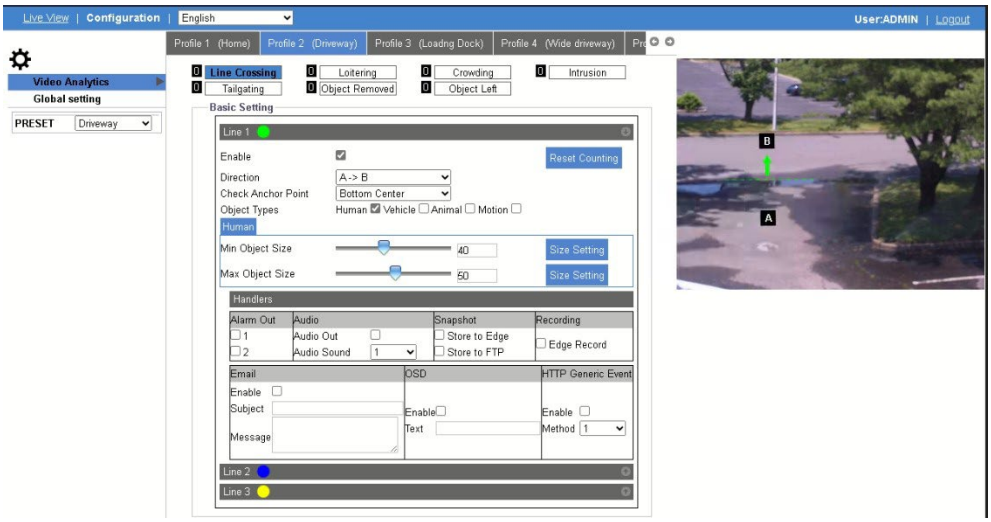


Figure: Line Crossing Settings

Basic Setting

Click the arrow on Line 1 to open the screen above. Click the arrows on Lines 2 and 3 as needed.

Enable: Check the box to allow configuring this function.

Direction

Select the line direction for crossing, A to B, B to A or in both directions, to help define the exact direction the line is crossed.

Anchor Points

Set the anchor point (Bottom Center/Right/Left, Top Center/Right/Left, Center Center) to designate where the object triggers the alarm, noting exactly where an object crosses the line. See Note on anchor points below.

Object Types

To further refine the event, check the type of object to detect crossing the line, human, vehicle, animal or any motion regardless of classification.

Min/Max Object Size

Use the slider to define the min/max object size or enter the exact number in the field provided (object size as a percentage of the image, 0-100%); select the Size Setting button to display a sample proportional graphic of the size being selected.

Method

Using the cursor, draw the line on the selected area of the preview picture. Click Save to have these lines take effect.

Performance

After saving the setting, on the Live page the Preset Profile can be selected from the Video Analytics dropdown. When an object moves across the designated line, the event will be highlighted on the screen. The bounding boxes that will display on Live and Playback video will be green for a person, blue for a vehicle and yellow for an animal.

9.3 Loitering

Loitering is designed to watch for suspect people/objects that enter and linger within a defined area for a defined period of time. Up to three areas can be defined for loitering, each with a different color, green, blue or yellow.

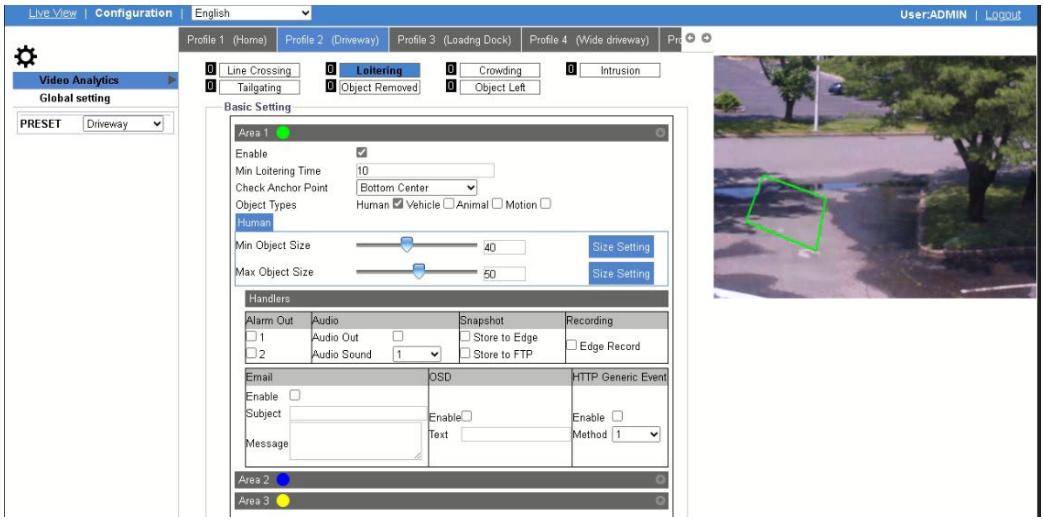


Figure: Loitering Settings

Basic Setting

Click the arrow on Area 1 to open the screen above. Click the arrows on Areas 2 and 3 as needed.

Enable: Check the box to allow configuring this function.

Min Loitering Time

Enter the time in the field provided (in seconds) to define how long the object has to remain in the area to be considered loitering.

Anchor Points

Set the anchor point (Bottom Center/Right/Left, Top Center/Right/Left, Center Center) to designate where the object triggers the alarm, so if an object stays in the area for longer than the defined time, the exact point of entry is available. See Note on anchor points below.

Object Types

To further refine the event, check the type of object to detect lingering in the area, human, vehicle, animal or any motion regardless of classification.

Min/Max Object Size

Use the slider to define the min/max object size or enter the exact number in the field provided (object size as a percentage of the image, 0-100%); select the Size Setting button to display a sample proportional graphic of the size being selected.

Method

Configure the Handlers section and Arming Schedule Setting according to the User Guide.
Using the cursor, define the area to be monitored for loitering; right click to close the ends of the outline of the area. Click Save to have these areas take effect.

Performance

After saving the setting, on the Live page Loitering can be selected from the Video Analytics dropdown. When an object stays in this area for longer than the designated time, the event will be highlighted on the screen. The bounding boxes that will display on Live and Playback video will be green for a person, blue for a vehicle and yellow for an animal.

9.4 Crowding

Crowding is designed to keep track of the number of people/objects in a designated area. This can be useful when it is necessary to minimize the number of people/objects in any given area to create an alarm when there is congestion in the defined area. Up to three areas can be defined for crowding, each with a different color, green, blue or yellow.

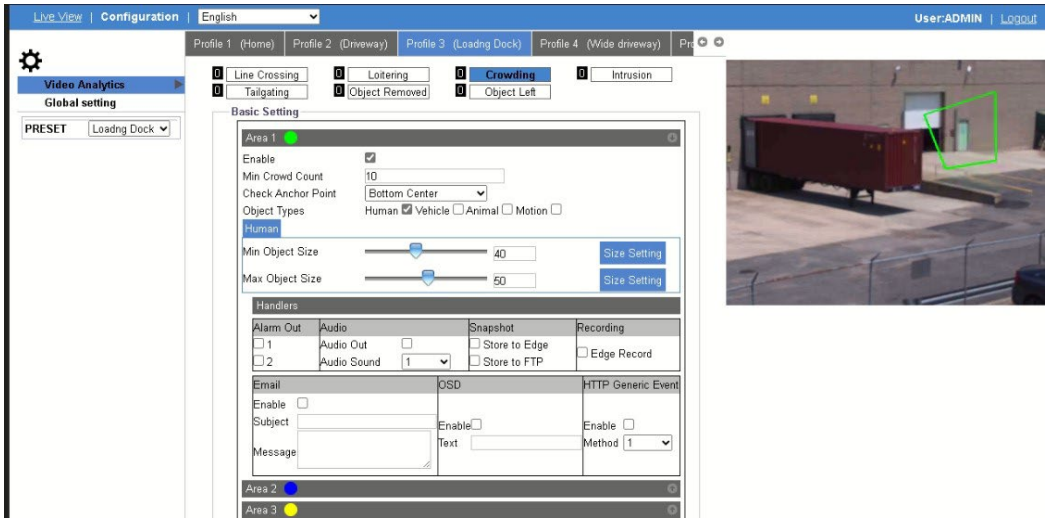


Figure: Crowding Settings

Basic Setting

Click the arrow on Area 1 to open the screen above. Click the arrows on Areas 2 and 3 as needed.

Enable: Check the box to allow configuring this function.

Min Crowd Count

Enter the number of objects in the field provided to define how many objects are to be considered a crowd.

Anchor Points

Set the anchor point (Bottom Center/Right/Left, Top Center/Right/Left, Center Center) to designate where the object triggers the alarm, so if more than the defined number of objects allowed enters the area, the exact point of entry is available. See Note on anchor points below.

Object Types

To further refine the event, check the type of object to detect what is gathering in the area, human, vehicle, animal or any motion regardless of classification.

Min/Max Object Size

Use the slider to define the min/max object size or enter the exact number in the field provided (object size as a percentage of the image, 0-100%); select the Size Setting button to display a sample proportional graphic of the size being selected.

Method

Configure the Handlers section and Arming Schedule Setting according to the User Guide.
Using the cursor, define the area to be monitored for crowding; right click to close the ends of the outline of the area. Click Save to have these areas take effect.

Performance

After saving the setting, on the Live page Crowding can be selected from the Video Analytics dropdown. When more than the designated number of objects enters this area, the event will be highlighted on the screen. The bounding boxes that will display on Live and Playback video will be green for a person, blue for a vehicle and yellow for an animal.

9.5 Intrusion

Intrusion can define an area to watch for any suspicious or unauthorized person/object that enters the specified area. This way a critical area can be monitored for any trespassing. Up to three areas can be defined for intrusion, each with a different color, green, blue or yellow.

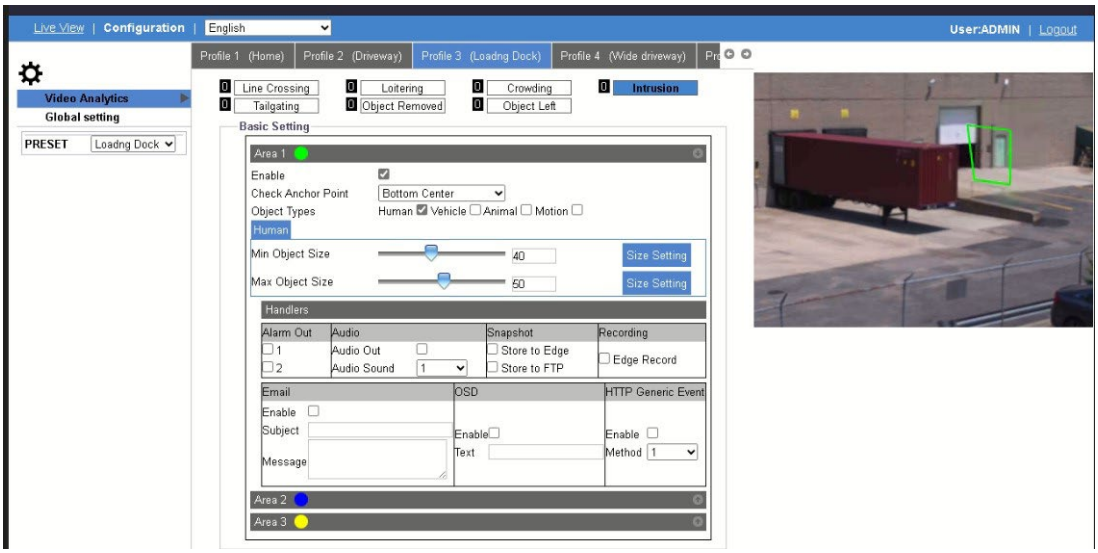


Figure: Intrusion Settings

Basic Setting

Click the arrow on Area 1 to open the screen above. Click the arrows on Areas 2 and 3 as needed.

Enable: Check the box to enable the intrusion detecting function.

Anchor Points

Set the anchor point (Bottom Center/Right/Left, Top Center/Right/Left, Center Center) to designate where the object triggers the alarm, to capture the exact point of entry. See Note on anchor points below.

Object Types

To further refine the event, check the type of object to detect entering in the area, human, vehicle, animal or any motion regardless of classification.

Min/Max Object Size

Use the slider to define the min/max object size or enter the exact number in the field provided (object size as a percentage of the image, 0-100%); select the Size Setting button to display a sample proportional graphic of the size being selected.

Method

Configure the Handlers section and Arming Schedule Setting according to the User Guide.
Using the cursor, define the area to be monitored for intrusion; right click to close the ends of the outline of the area. Click Save to have these areas take effect.

Performance

After saving the setting, on the Live page Intrusion can be selected from the Video Analytics dropdown. When an object enters this area, the event will be highlighted on the screen. The bounding boxes that will display on Live and Playback video will be green for a person, blue for a vehicle and yellow for an animal.

9.6 Tailgating

Tailgating is designed to control access to a sensitive area and detect if more than one person/vehicle enters an area too close to the previous entry. Up to 3 lines can be configured, each noted by a different color, green, blue or yellow line.

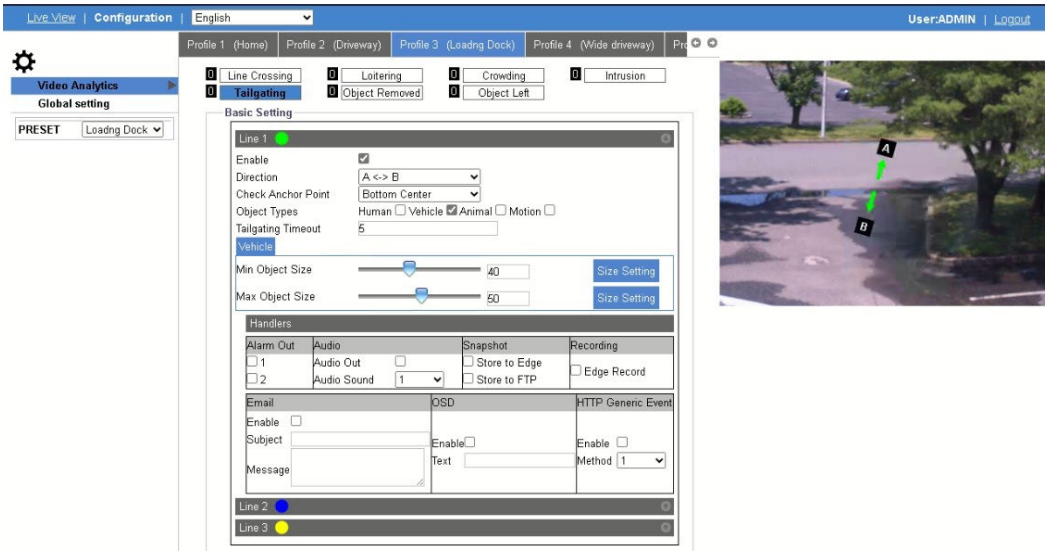


Figure: Tailgating Settings

Basic Setting

Click the arrow on Line 1 to open the screen above. Click the arrows on Lines 2 and 3 as needed.

Enable: Check the box to enable the intrusion detecting function.

Direction

Select the line direction for crossing, A to B, B to A or in both directions, to help define the exact direction the line is crossed too closely to the previous crossing.

Anchor Points

Set the anchor point (Bottom Center/Right/Left, Top Center/Right/Left, Center Center) to designate where the object triggers the alarm, the specific point where the object crosses the line too closely to the previous entry. See Note on anchor points below.

Object Types

To further refine the event, check the type of object that entered the area too closely to the previous entrance, human, vehicle, animal or any motion regardless of classification.

Tailgating Timeout

Define how much time (seconds) has to pass for another object to pass the line.

Min/Max Object Size

Use the slider to define the min/max object size or enter the exact number in the field provided (object size as a percentage of the image, 0-100%); select the Size Setting button to display a sample proportional graphic of the size being selected.

Method

Configure the Handlers section and Arming Schedule Setting according to the User Guide.
Using the cursor, draw the line on the selected area of the preview picture. Click Save to have these lines take effect.

Performance

After saving the setting, on the Live page Tailgating can be selected from the Video Analytics dropdown. When an object moves across the designated line too quickly after the previous, the event will be highlighted on the screen. The bounding boxes that will display on Live and Playback video will be green for a person, blue for a vehicle and yellow for an animal.

9.7 Object Removed

Object Removed detection was developed to guarantee that valuable or important objects are safeguarded in their location. Up to three areas can be defined for object removed, each with a different color, green, blue or yellow.

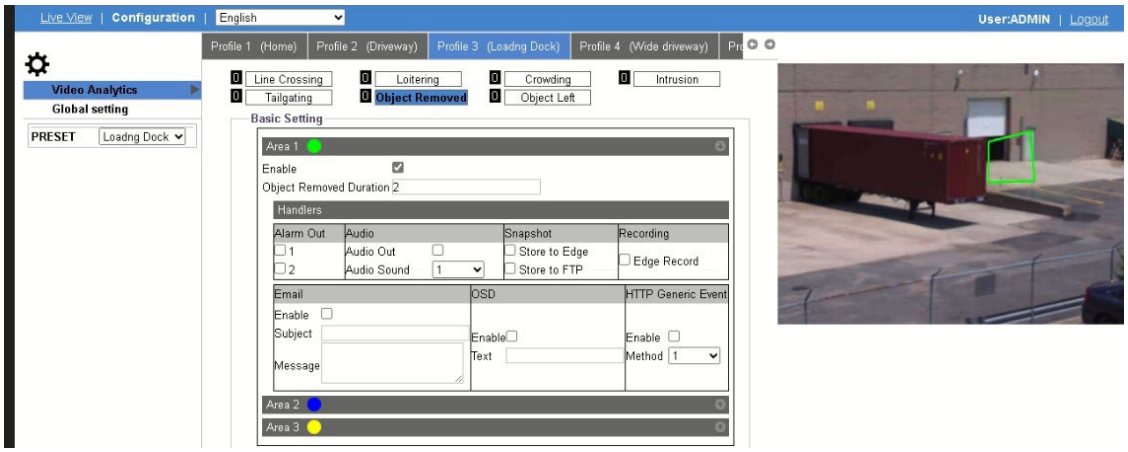


Figure: Object Removed Settings

Basic Setting

Click the arrow on Area 1 to open the screen above. Click the arrows on Areas 2 and 3 as needed.

Enable: Check the box to allow configuring this function.

Object Removed Duration

Enter a number to define how long a time (seconds) before it is considered removed.

Method

Configure the Handlers section and Arming Schedule Setting according to the User Guide.
Using the cursor, define the area to be monitored for observing object removal; right click to close the ends of the outline of the area. Click Save to have these lines take effect.

Performance

After saving the setting, on the Live page Object Removed can be selected from the Video Analytics dropdown. When an object is removed from this area, the event will be highlighted on the screen. The bounding boxes that will display on Live and Playback video will be green for a person, blue for a vehicle and yellow for an animal.

9.8 Object Left

Object Left is designed to prevent an object from being intentionally deposited in a critical place. If an object is left in a defined area, it can quickly be determined if it is suspicious. Up to three areas can be defined for object left, each with a different color (green, blue or yellow).

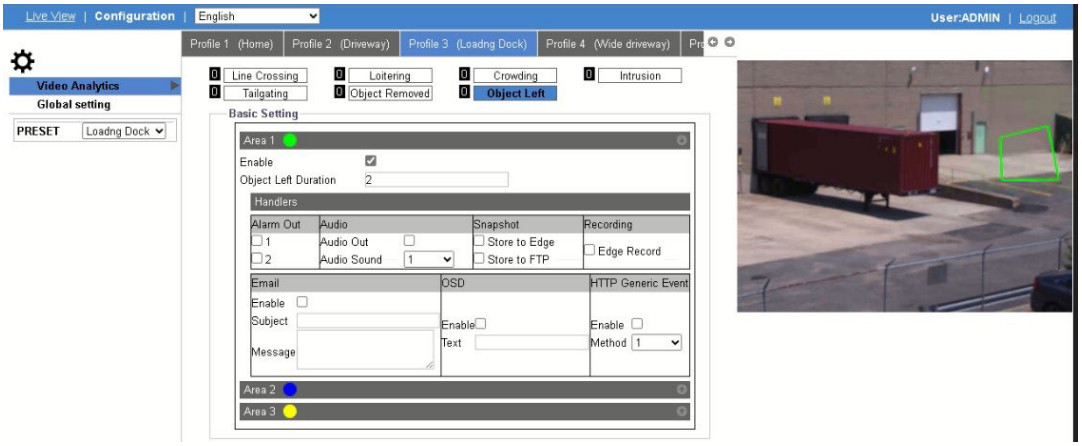


Figure: Object Left Settings

Basic Setting

Click the arrow on Area 1 to open the screen above. Click the arrows on Areas 2 and 3 as needed.

Enable: Check the box to allow configuring this function.

Object Left Duration

Enter a number to define how long (seconds) the object has to remain in the area before it is considered left.

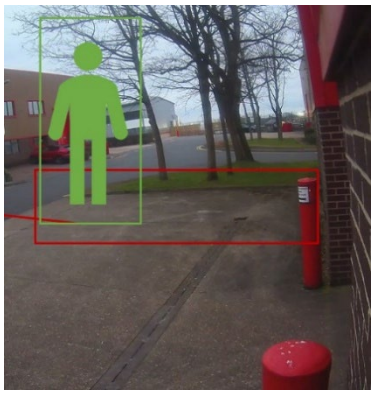
Method

Configure the Handlers section and Arming Schedule Setting according to the User Guide.
Using the cursor, define the area to be monitored for observing object being left; right click to close the ends of the outline of the area. Click Save to have these lines take effect.

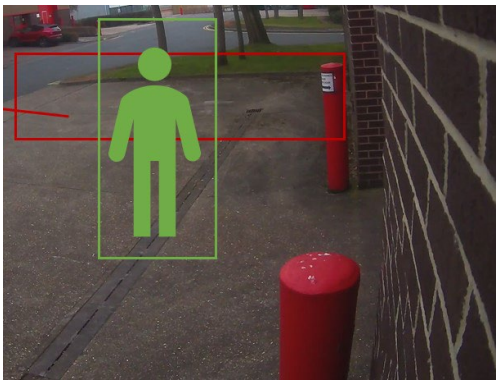
Performance

After saving the setting, on the Live page Object Removed can be selected from the Video Analytics dropdown. When an object is left in this area, the event will be highlighted on the screen. The bounding boxes that will display on Live and Playback video will be green for a person, blue for a vehicle and yellow for an animal.

Notes on Anchor Point: Setting the anchor point adds another dimension to fine-tune how an event is triggered. Since objects are represented as a bounding box, this pinpoints exactly where in that box the trigger occurs. By selecting the specific place in the bounding box (Bottom Center/Right/Left, Top Center/Right/Left, or Center Center) that the object triggers the alarm, each analytic event can be customized for different scenarios. When defining an area for Intrusion, Loitering, Crowding or Object Left/Removed, it would matter whether the object is approaching the area from the foreground, when it would be more likely to trigger at the top of the box, or from the background, when it is more likely to trigger at the bottom of the box. For line cross and tailgating, it would usually be preferential to select a bottom area, where the feet of a person or front of a vehicle would cross the line first and eliminate some random momentary line crosses.



Entering from background. Feet enter area first; anchor point Bottom Center.



Entering from foreground. Head enters area first; anchor point Top Center.

Crossing from background. Feet cross line first; anchor point Bottom Center.

9.8 Global setting

The Global setting area provides for general settings for all the Video Analytics.

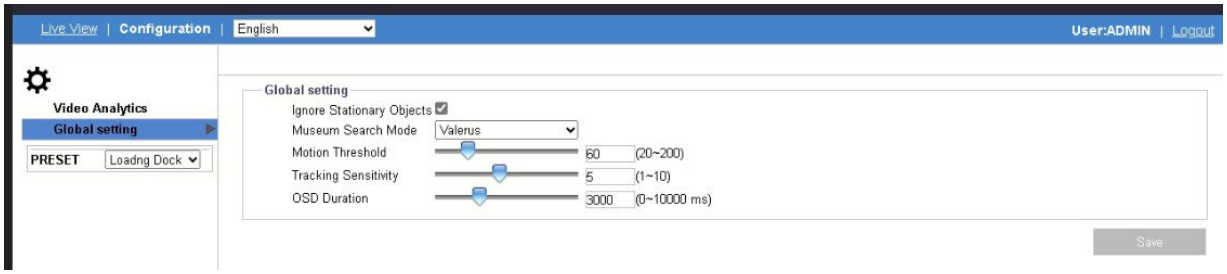


Figure: Global Settings

Use the checkbox to Ignore Stationary Objects when setting up analytics, for example to disregard a parked car even if the car is detected.

From Museum Search, select Valerus or ViconNet. If Valerus is selected, when this camera is used in the Valerus VMS, the advanced Museum Search will be functional by default, improving the ease and accuracy of doing museum searches. If ViconNet is selected, the feature is not supported in the VMS. Use the slider or enter an exact number in the field to set Motion Threshold and Tracking Sensitivity. This determines how often alarms will be alerted; the smaller the number, the more alarms will be set off.

OSD Duration determines how long the OSD text displays on the screen when an alarm occurs, if the OSD has been set up in the configuration of these analytics.

10. Event Setting

10.1 Alarm Out

This section is designed to set up detailed settings for alarm output(s) when events occur. Make sure you have enabled alarm output in each event section to activate this function.

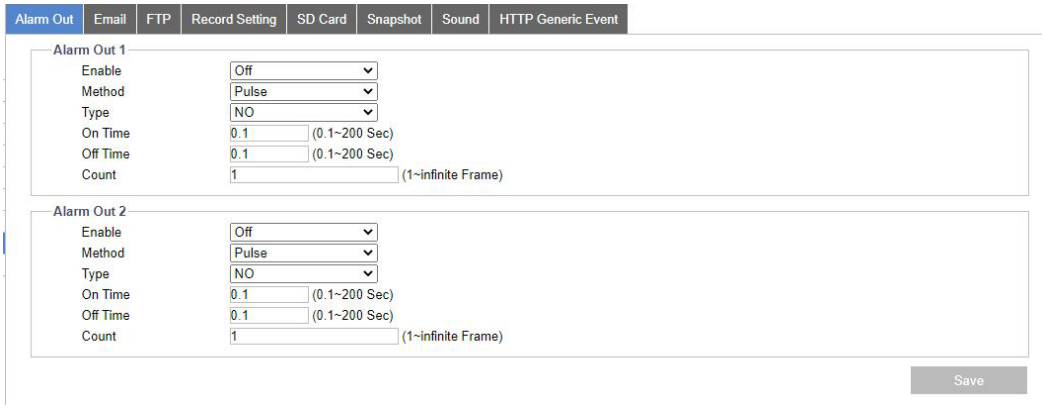


Figure: Alarm Output Settings

Alarm Out

Enable: Select "On" from the dropdown to activate this function.

Method: Pulse/Normal

There are 2 methods to proceed with alarm output. The fields available change according to method.

- Normal: The standard method to execute alarm output function, where user can define a duration from options in Post Duration dropdown menu.

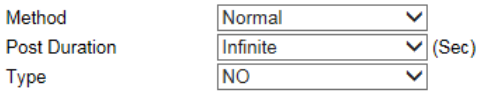


Figure: Normal Method Settings

- Pulse: Selecting this method, user can specifically define both the duration and interval time individually for alarm output. Additionally, counts for alarm output can also be customized.

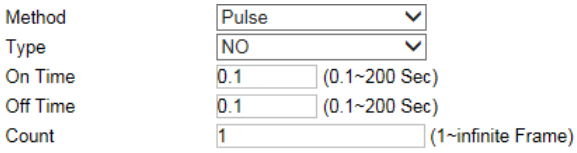


Figure: Pulse Method Settings

For Normal Method:

Post Duration: Infinite/5/10/15/30 (sec)

Set a period of duration for alarm output under Normal method. Infinite means unlimited and continuous triggering for alarm output.

For Pulse Method:

Type: NO/NC

Define which type to use for triggering alarm output.

- NO (Normally Opened): An alarm will be triggered when the external contact closes.

- NC (Normally Closed): An alarm will be triggered when the external contact opens.

On Time: 0.1 ~ 200 (sec)
Define a specific duration for alarm output.

Off Time: 0.1 ~ 200 (sec)
Define a specific interval for each alarm output triggering.

Count: 1 ~ Infinite Frame
Define how many frames will be counted for alarm output.

10.2 Email

This section is designed to set up detailed settings for email notification when events occur. Make sure you have enabled email sending in each event section to activate this function.

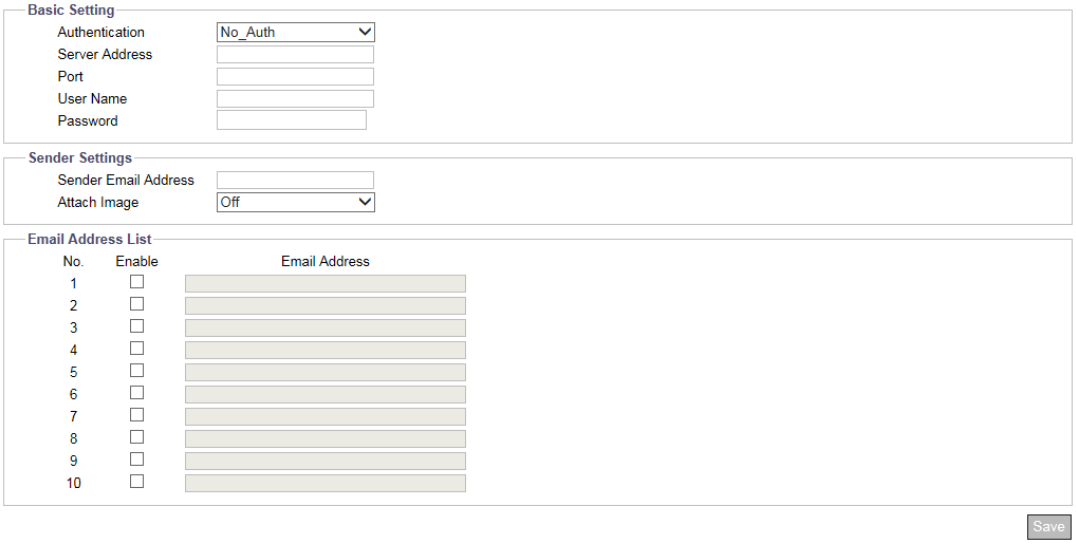


Figure: Email Settings

Basic Setting

Authentication: No_Auth/SMTP_Plain/Login/TLS-TTLS
Select an authentication type; a detailed description for each follows:

- No_Auth: No restriction.
- SMTP_Plain: PLAIN is the name of a registered SASL authentication mechanism, which serves as a parameter to the AUTH command. The PLAIN authentication mechanism is described in RFC 2595. Plain is the least secure of all the SASL authentication mechanisms, since the password is sent unencrypted across the network.
- Login: The Login mechanism is supported by Microsoft's Outlook Express and by some other clients.
- TLS_TTLS: TLS is usually implemented on top of any of the Transport Layer protocols encapsulating the application-specific protocols such as HTTP, FTP, SMTP, NNTP and XMPP. The TLS protocol allows client-server applications to communicate across a network in a way designed to prevent eavesdropping and tampering. TLS can also be used to tunnel an entire network stack to create a VPN, as is the case with OpenVPN.

Server Address

Input a designated server address for email notification.

Port

Set "25" as default or change to dedicated number. Discuss with your IT administrator for details if necessary.

User Name

Input a username with privileges to access the server.

Password

Input the password associated with the username.

Sender Settings

Sender Email Address

Enter the sender email address into the field.

Attach Image: On/Off

Select "On" from the dropdown to enable attaching the detected image of events to the email being sent.

E-mail Address List:

This function is designed to notify multiple users via email when events occur.

Figure: Email Address List

- Check "Enable" to send email to the selected address.
- Email Address: Input an email address to which events will be sent. A maximum of 10 email addresses can be defined.

10.3 FTP

This section is designed to set up detailed settings for FTP image storing when events occur. Make sure you have enabled FTP function in each event section to activate this function.

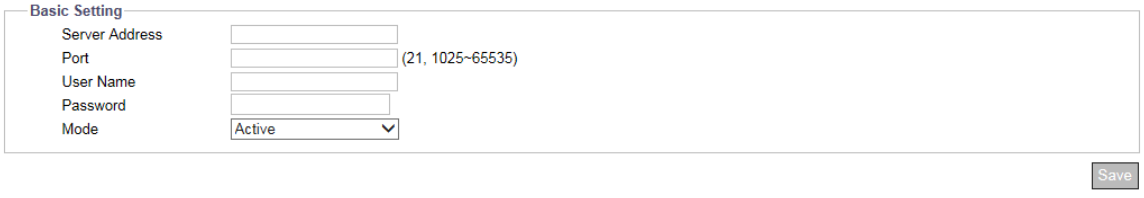


Figure: FTP Settings

Basic Setting

Server Address

Input an FTP server address.

Port: 21/1025 ~ 65535

Set "21" as default or change to dedicated number. Discuss with your IT administrator for details if necessary.

Username

Input a user name with privileges to access the server.

Password

Input the password associated with the username.

Mode: Active/Passive

Select the connection mode to be utilized; detailed descriptions follow:

- Active: Selecting this option, the camera will keep reconnecting with the designated FTP site, which uses more network bandwidth but delivers instant response to FTP.
- Passive: By selecting this option, the camera will only connect with the designated FTP site when necessary, which greatly helps to save the network bandwidth.

10.4 Record Setting

This section is designed to set up detailed settings for video recording. Make sure you have enabled recording function in each event section to activate this function.

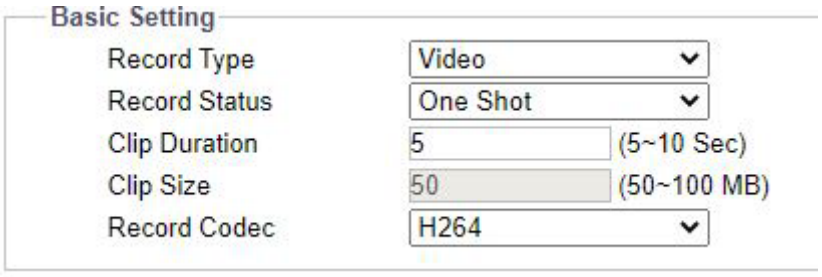


Figure: Record Settings

Basic Setting

Record Type: Audio and Video/Video

Choose which record type to use:

- Audio And Video: Both video and audio will be recorded.
- Video: Only video will be recorded.

Record Status: One Shot/Continuous

Define the method of recording.

- One Shot: Camera records video with designated duration and file size.
- Continuous: Camera keeps recording video continuously.

Clip Duration: 5 ~ 10 (sec)

Set the length limit for recording file.

Clip Size: 50 ~ 100 (MB)

Define the file size for recording file.

Record Codec: H.264/H.265

Choose type of video codec.

- H.264: Camera records video with H.264 video file format.
- H.265: Camera records video with H.265 video file format.

10.5 SD Card

This section is designed to set up detailed settings for Edge Recording when events occur. the SD card is mounted, installed and formatted and the Edge Record function has been enabled in each e vent section to activate this function. The display will change according to the selections made.

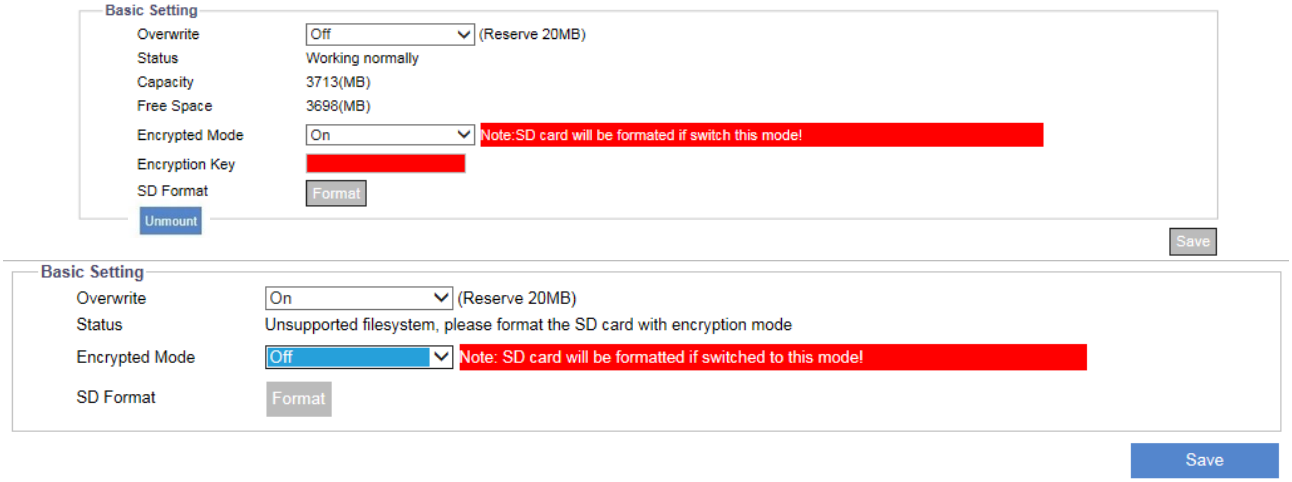


Figure: SD Card Settings

Basic Setting

Overwrite: On/Off

This means that recorded files will be overwritten when SD card is at full capacity. The recording program will erase the earliest file (FIFO) and store another new file when the remaining capacity of mounted SD card is below 20 MB. Select On to enable this function.

Status

Shows status if SD card is inserted and mounted correctly or if an SD card is not inserted in the slot. There are three possible status listed below. When Status is shown to be Working normally, Capacity and Free Space fields will display.

- SD Card not inserted.
- Working normally.
- Unsupported filesystem, please format the SD card to ext4.

Note	• Due to compatibility issues related to filesystem, the camera only supports ext4 format, which not only is recommended due to its resilience against data loss if the card is ejected or if there is abrupt power loss, but also allows the use of SD card with capacity greater than 32GB.

Capacity

Capacity only displays when the Status is "Working normally;" it shows the capacity of the inserted SD card.

Free Space

Free Space only displays when the Status is "Working normally;" it shows the amount of free space on the inserted SD card.

Encrypted Mode: On/Off

Encryption Mode allows user to decide whether the data on the SD card is encrypted or not. When "On," all data that will be saved on the SD card is encrypted. When "Off," all data that will be saved on the SD card is NOT encrypted.

Encryption Key

Available when Encryption Mode is "On," Encryption Key allows user to enter a password, which will be used for decrypting and accessing the video file on the SD card.

SD Format

Click "Format" to start formatting the mounted SD card.

Note	• Formatting the SD card will always delete any data in the SD card, no matter if Encryption Mode is "On" or "Off." • To access data stored on the SD card from Windows OS or Mac OS, a third party ext4 driver or application is required.

10.6 Snapshot

This section is designed to set up detailed settings for snapshot capture when events occur. Make sure you have enabled Snapshot function in each event section to activate this function.

Figure: Snapshot Settings

Basic Setting

Pre Event Capture Count: 1 ~ 10 (Frame)

Set the number of frames to be captured prior to an event.

Event Capture Interval: 1 ~ 10 (sec)

Set a time interval ranging from 1 to 10 seconds between each snapshot capture.

Post Event Capture Count: 1 ~ infinite (Frame)

Set the number of frames to be captured after an event occurs.

10.7 Sound

This section is designed to set up detailed settings for audio output sounds when events occur. Make sure you have enabled Audio Out function in each event section to activate this function.

Figure: Sound Settings

Basic Setting

Mode: One Shot/Infinite

- One Shot: The sound of audio out will be played only 1 time.
- Infinite: "Infinite" keeps the sound playing continuously.

No.

The numerical order list of each sound file.

File Status

The current status of each sound file is clearly shown here.

Select File

Click the "Choose File" button to open the window for selecting a desired sound file from your local computer.

Delete File

Simply click "Delete" to remove the sound file from the list.

10.8 HTTP Generic Event

HTTP Generic Event can help a user send messages and commands directly to Network Video Recorder (NVR), which supports CGI commands function. User can customize the messages and commands as needed.

Figure: HTTP Generic Event Settings

Basic Setting

Method

Select one of the events that can be communicated to the VMS/NVR, which supports HTTP generic event, for the trigger event.

Title

Preset the title of messages.

URL

Input the web address of the NVR. Refer to the user manual for NVR for the details on finding the web address.

Option: Get/Post

Select the mode of notification transmission as needed.

- Get: The Get method is a simple and fast method to transmit messages, but it is less secure than Post.
- Post: The Post method is a more complex way to transmit messages, but it is also safer than Get.

User Name

Enter a designated username for authentication to the accessed NVR.

Password

Enter the password corresponding to the entered username for correct authentication.

- Active Message: Camera will send an active message to NVR when the trigger event occurs.
- Inactive Message: Camera will send an inactive message to NVR when the trigger event ends.

11. PTZ Settings

In this chapter, the user will be guided through setup steps for various types of PTZ operations, including PTZ movements (pan, tilt, zoom and focus); and actions (Scan, Preset, Patrol (Tour) and Pattern). In addition, Basic PTZ settings and PTZ Control Panel settings are also explained.

Note	• Click "Save" button after changing configurations in any of the "PTZ Settings" for the settings take effect. • A few of the configurations will not require clicking "Save" for settings to take effect (e.g., Start/Stop).

11.1 Basic

Basic Setting

Figure: Basic Setting

Power on Action: NONE/Home/Auto Scan/Frame Scan/Auto Patrol 1~4/Pattern 1~4

The camera can execute a PTZ action when the system is powered on or rebooted. These actions are listed below:

- NONE: Camera will have no action when powered on.
- Home: Camera will automatically move to its home position.
- Auto Scan: Camera will perform scanning automatically.
- Frame Scan: Camera will perform frame scanning automatically.
- Auto Patrol 1 ~ 4: Camera will perform patrol action based on selected patrol.
- Pattern 1 ~ 4: Camera will perform pattern action based on selected pattern.

Auto Return: NONE/Home/Auto Scan/Frame Scan/Auto Patrol 1~4/Pattern 1~4

The camera can execute certain PTZ actions when no PTZ action or PTZ movement occurs in the user defined timeout period. The actions are the same as the options for "Power on Action."

Auto Return Timeout (min): 1/2/3/5/10/20/30/60

Set a timeout in minutes to activate Auto Return.

Lens Stabilization: On/Off

Lens-based stabilization that counteracts horizontal and vertical vibrations. Set this function "On" to minimize image blur and jitter resulting from camera shaking.

Zoom Setting

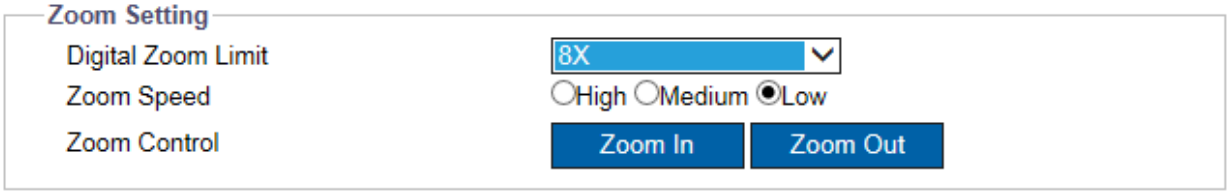


Figure: Zoom Setting

Digital Zoom Limit: 1X/2X/4X/8X

This function allows user to use digital zoom on the view to enlarge the view at 1x, 2x, 4x, and 8x,

Zoom Speed: High/Medium/Low

Allows the user to define the speed at which the camera changes from one zoom depth to another. High is a faster speed.

Zoom Control: Zoom In/Zoom Out

Click the buttons for zooming in and out.

Focus Setting

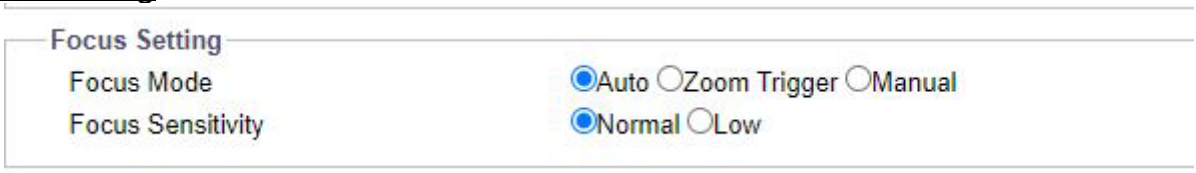


Figure: Focus Setting

Focus Mode: Auto/Zoom Trigger/Manual

- Auto: Camera can automatically focus whenever user performs PTZ operation. Focus Sensitivity can be set in this mode.
- Zoom Trigger: Camera can automatically focus whenever user operates Zoom functions.
- Manual: Allows user to manually set camera focus by pressing "Focus Near, "Focus Far" or One-Push (using Focus Control) and to adjust focus speed (using Focus Speed).

Focus Sensitivity: Normal/Low

Set the sensitivity of lens focus as "Normal" or "Low" when in Auto mode. Normal means lens will automatically refocus easily when there's minor alteration in the camera coverage; selecting Low will ignore minor alterations and lens will only automatically refocus for major changes in the camera coverage.

Focus Speed: High/Medium/Low

Allows the user to define the speed at which the camera changes from one focus level to another. High means faster speed. Available in Manual mode.

Preset/Patrol Setting

Figure: Preset/Patrol Setting

Preset/Patrol Move Speed: 1 ~ 500

Use the slider to select Preset and Patrol speed. Higher value means the Preset and Patrol movement speed will be faster.

Note	• Refer to sections "*11.4 Preset*" and "*11.5 Patrol* sections for details on Preset and Patrol actions.

Show Preset Name on Screen: On/Off

Select "On" to show Preset name on the screen.

Calibration

This is used to calibrate the lens as needed.

11.2 Pan/Tilt

Pan/Tilt section is where user can configure Pan and Tilt actions. Changes in this section will affect the behavior of PTZ control panel.

Pan/ Tilt Setting

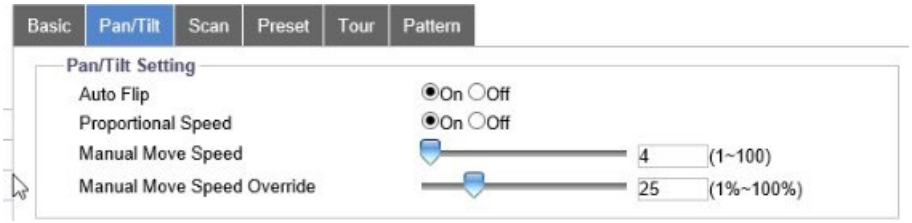


Figure: Pan/Tilt Setting

Auto Flip: On/Off

The Auto Flip function is useful for following a person who passes directly beneath the camera; the camera will pan 180° and reposition itself for uninterrupted viewing of any subjects that pass directly beneath the camera, as long user holds the down cursor of the Control Panel.

Proportional Speed: On/Off

Set Proportional Speed "On" for the camera to automatically decrease or increase the Pan and Tilt speeds in proportion to the amount of zoom. At tele zoom settings, the Pan and Tilt speeds will be slower.

Manual Move Speed: 1 ~ 100

Allows the user to define Pan and Tilt movement speed. Higher values mean faster speed.

Manual Move Speed Override: 1% ~ 100%

The percentage value that is multiplied by the Manual Move Speed. It is used for more precise adjustment of the movement speed.
The actual PTZ movement is a product of both the Manual Move Speed and the Manual Move Speed Override values.

Pan/Tilt Limit

Depending on where the camera is installed, as the camera view changes based on PTZ operation, situations can arise where the view covered by the camera is not relevant (e.g., the camera view is facing a wall, where nothing will happen). To avoid this situation, user can specify limits on Pan and Tilt operations and let the camera focus only on important scenes. For instance, instead of setting the camera to cover from 0° to 200° for scan action; user can set scan limit from 0° to 150° that covers the

region of interest where activity usually would occur, while 151˚ and above is ignored, as this region may have an object blocking the scene.

Figure: Pan/Tilt Limit

Note	• Refer to the figure above and table below to go through the steps for setting up limits for Pan, Tilt and Scan operations.

Item	Option/ Range	Description
Enable Limit	On/Off (Pan/Tilt/Scan)	Enable limit by selecting "On"
Left Limit **Right Limit**	0 ~ 360 (Pan/Scan)	Drag and adjust the bar or enter a value for setting left/right limit
Up Limit **Down Limit**	0 ~ 105 (Tilt)	Drag and adjust the bar or enter a value for setting up/down limit
Set Current Position to Limit	Left/Right (Pan/Scan) Up/Down (Tilt)	Set current position to Left/Right or Up/Down limit
Go to Limit	Left/Right (Pan/Scan) Up/Down (Tilt)	Go to Left/Right or Up/Down Limit
Clear Limit	Left/Right (Pan/Scan) Up/Down (Tilt)	Clear Left/Right or Up/Down Limit

Table: Pan/Tilt/Scan Limit

11.3 Scan

Scan action allows the camera to automatically pan back and forth regularly within a specified limit, at a constant speed and with predefined and constant tilt, zoom and focus values. In Scan action, the entire scene (sequence of views) is being monitored repeatedly, so it is suitable for touring the scene without losing focus at any time and keeping the covered scene defined correctly.

Scan Setting

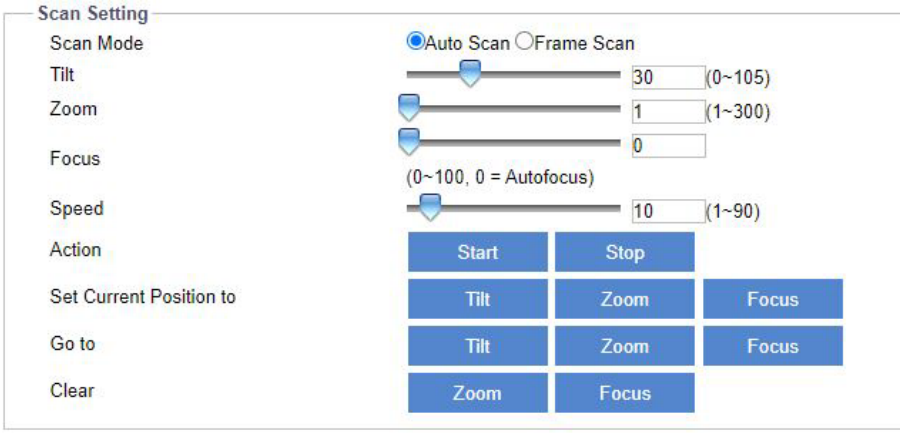


Figure: Scan Setting

Scan Mode: Auto Scan/Frame Scan

Auto Scan: Camera pans back and forth regularly with predefined tilt, zoom and focus.
Frame Scan: Camera pans back and forth regularly with predefined tilt, zoom and focus, but during the scan the camera will stop 8 times and stay at a view depending on the Scan Left/Right Limit.

Tilt: 0 ~ 105

Drag and adjust the bar or enter a value for setting tilt angle for Scan action.

Zoom: 1 ~ 300

Drag and adjust the bar or enter a value for setting zoom depth for Scan action.

Focus: 0 ~ 100, 0 = Auto Focus

Drag and adjust the bar or enter a value for setting focus depth for Scan action.

Speed: 1 ~ 90

Allows the user to define pan speed for Scan action. Higher value is faster speed.

Action: Start/Stop

Click "Start" to begin Scan action and "Stop" to cease Scan action.

Set Current Position to: Tilt/Zoom/Focus

Set current position to tilt, zoom or focus for the Scan action by dragging and adjusting the tilt, zoom or focus bar or entering a value for setting tilt, zoom or focus on the PTZ Settings control panel and then saving by clicking "Save". Click "Tilt", "Zoom" or "Focus" of "Set current position to" function for the action to take effect.

Go to: Tilt/Zoom/Focus

Go to a previously setup tilt, zoom and focus for Scan action, by dragging and adjusting the tilt, zoom or focus bar or entering a value for setting tilt, zoom or focus on the PTZ control panel and then saving by clicking "Save". Click "Tilt", "Zoom" or "Focus" of "Go to" function for the action to take effect.

Clear: Zoom/Focus

Clear current zoom and focus for Scan action by dragging and adjusting the zoom or focus bar or entering a value for setting zoom or focus on the PTZ control panel and then saving by clicking "Save". Click "Zoom" or "Focus" of "Clear" function for the action to take effect.

Scan Limit

User can specify limits on Scan operation and let the camera focus only on important scenes. To limit the scan position, select On to Enable the limit settings. Click Save to save the limit settings.

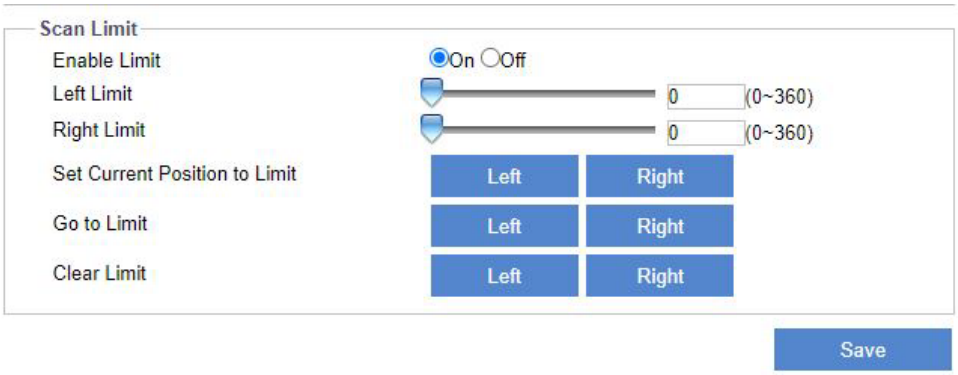


Figure: Scan Limit Setting

Note	• Refer to "Table: Preset/Patrol/Pattern Limit" in"*11.2 Pan/Tilt*" section for details.

11.4 Preset

Preset action allows the creation of up to 128 predefined camera views called Preset. User must manually call a Preset and when a Preset is called, the camera will automatically move to the predefined view and stay there until another PTZ operation is triggered. Basically, calling a Preset is telling the camera to go to a specific view and stay there. At a Preset the view is focused correctly based on settings, but while the camera is moving to a Preset the view may not be well defined. A Preset is usually used when user wants to quickly access a key monitoring area and then monitor the area for undetermined time.

Presets can be added, modified, viewed and deleted.

Additionally, Preset Name and Text Color, Auto Refocus and Motion Area are values that add to the ease of use of Presets.

Preset Position

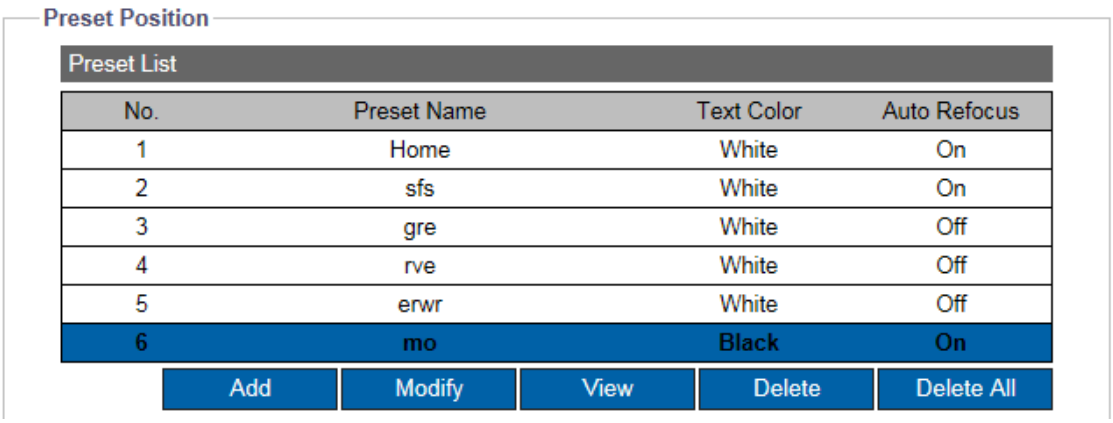


Figure: Preset List

Preset List

- Preset Name: Displays the selected Preset Name on screen
- Text Color: Displays the selected color of Preset Name on screen
- Auto Refocus: Displays the selected option for Auto Refocus, On/Off.
- Delete All: Allows user to delete all the existing Presets at once.
- View: Allows user to view the selected Preset.

Note	• Refer to "*Table: Preset/Patrol/Pattern List*" below for more details on Preset List. • The table below has combined details relevant to Preset List (for this section), and Patrol and Pattern Lists (for the 2 following sections).

Item	Description
Add	Allows user to create a new Preset/Patrol/Pattern to the list
Modify	Allow user to change a selected Preset/Patrol/Pattern already defined on the list
Delete	Allows user to remove a selected Preset/Patrol/Pattern already defined on the list
No.	Displays the numerical order of Preset/Patrol/Patterns on the list.
Preset/Patrol/Pattern Name	Displays the name or ID of each Preset/Patrol/Pattern
Action	Displays "Play" when Play/Stop is clicked in Patrol or Pattern, and the Patrol/Pattern is playing. Also, displays "Recording" when Start Record is clicked in Pattern and the Pattern is being recorded.

Table: Preset/Patrol/Pattern List

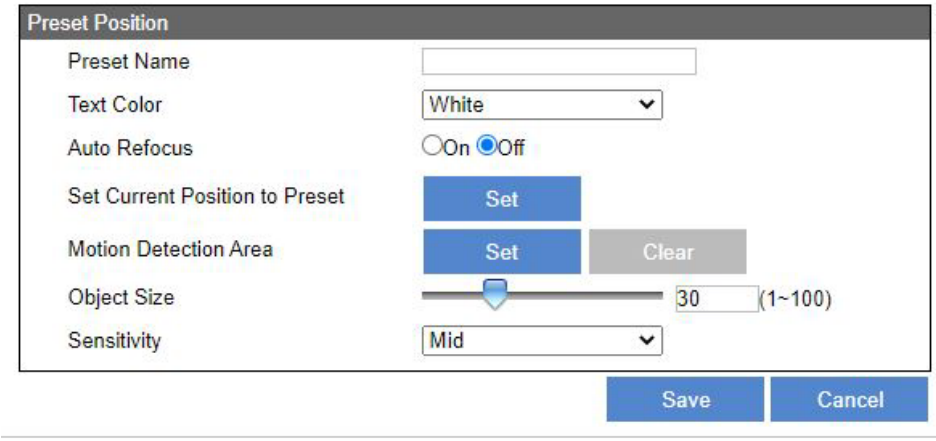


Figure: Add Preset Position

Preset Position

- Text Color: Select the color for the name of Preset displayed on screen. Two options are available, "White" and "Black."
- Auto Refocus: Set "On" to allow the camera auto refocus when viewing a Preset. Setting "Off" disables this function.
- Set Current Position to Preset: Click "Set" to make current view a Preset.
- Motion Detection Area: Click "Set" in motion area; then, on the view, click and drag to draw the motion area, used for motion detection purposes. Click Clear to delete the current motion area. Note that Motion Detection must be Enabled from the Event Source, Motion (section7.3) screen.
- Object Size 1 ~ 100: The lower the value, the smaller the object that can be detected, and vice-versa.
- Sensitivity: Set the sensitivity for motion detection. High means that camera tends to be triggered with slight motion or light change within the live view, while Low means that camera is triggered only when major change in motion or light occurs.

Note	• Refer to "**Table: Preset Position and Patrol/Pattern Setting**" (below) for more details on Preset Position. • The table below has combined details relevant to Preset Position (for this section), as well as Patrol and Pattern Settings (the 2 following sections).

Item	Description
Save	Click "Save" button for the Preset/Patrol/Pattern settings to take effect.
Cancel	Click "Cancel" to discard the Preset/Patrol/Pattern Settings.
Preset/Patrol/Pattern Name	Allows user to enter the name or ID of each Preset/Patrol/Pattern.

Table: Preset Position and Patrol/Pattern Setting

11.5 Patrol

Patrol action configures a sequence of presets and dwell time for each preset for the camera automatically and regularly repeated action. User can set up to 4 Patrols and add a maximum of 128 Presets in each Patrol; a Preset can be repeated. Patrol is suitable for situations where user has a set of key areas to monitor following a convenient monitoring sequence and dwell time.

A Patrol can be added, modified, played, stopped and deleted.

Patrol Setting

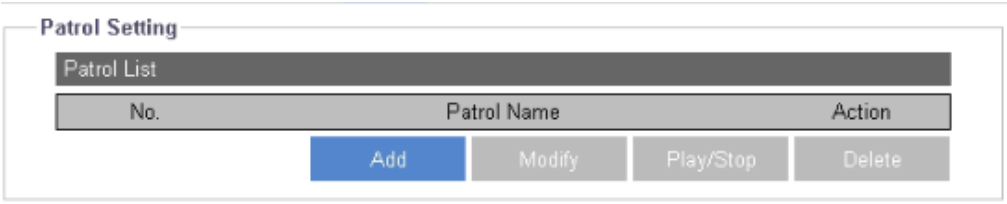


Figure: Patrol List

Patrol List

- Play/Stop: Select a Patrol from Patrol List, then click "Play/Stop" to start or stop playing the selected Patrol r action.

Note	• Refer to "Table: Preset/Patrol/Pattern List" in"*11.4 Preset*" section for more details.

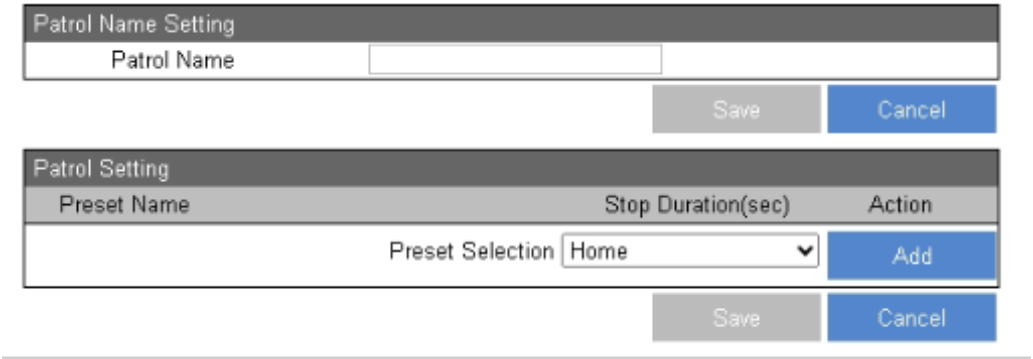


Figure: Add Patrol Setting

Patrol Setting

- Preset Name: Display the name of all Presets added to the Patrol.
- Stop Duration (3/5/7/10/15/30/60): To set stop duration time in seconds for each Preset.
- Preset Select: To select a Preset from the dropdown menu and add it to the current Patrol.
- Action (Delete/Add): Click "Delete" to delete the related Preset from the current Patrol. Click "Add" to add another Preset to current Patrol.

Note	• Refer to "Table: Preset Position and Patrol/Pattern Setting" in"*11.4 Preset*" section for more details.

11.6 Pattern

Pattern action memorizes camera series of up to 128 pan, tilt, zoom and presets operations to be automatically and regularly repeated when the Pattern is activated. By default, the focus and iris are in auto status during the time the pattern is being memorized. Pattern is suitable when user wants to use the camera for touring a scene (sequence of views) while having more flexibility on adjustment of pan/tilt speed and angle, zoom depth and presets selection. During a Pattern action, values of pan/tilt speed and angle, zoom depth and presets selection can change.

A Pattern can be added, modified, deleted, played, recorded and stopped.

Pattern Setting

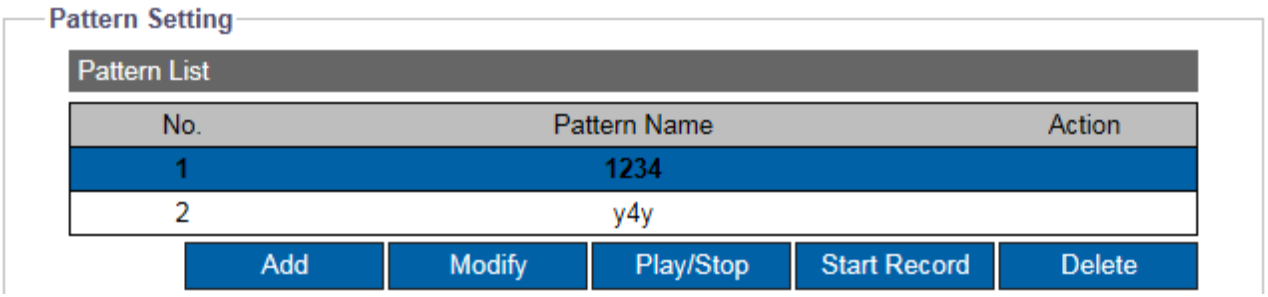


Figure: Pattern List

Pattern List

- Play/Stop: Select a Pattern from Pattern List, then click "Play/Stop" to start or stop playing the selected Pattern action.
- Start Record: Select a Pattern from Pattern List, then click "Start Record" to begin recording a Pattern action. Then use the Control Pane, for the operations to be memorized on the current Pattern. Pattern recording only memorizes the movements generated from pan, tilt, zoom and Preset.
- Stop: Click "Stop" to stop Pattern recording process.

Note	• Refer to "Table: Preset/Patrol/Pattern List" in"*11.4 Preset*" section for more detail.

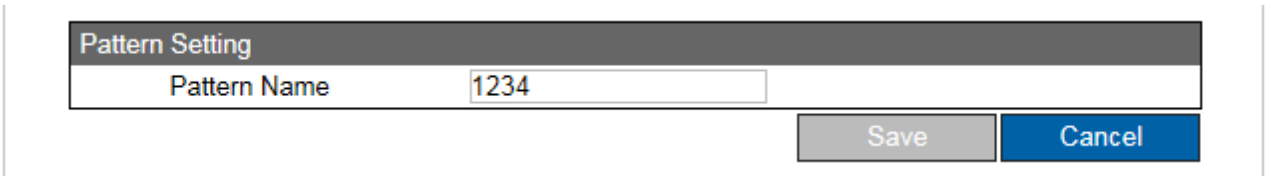


Figure: Pattern Setting

Pattern Setting

Note	• Refer to "Table: Preset Position and Patro /Pattern Setting" in"*11.4 Preset*" section for more details.

Appendix 1: Continuous Recording to an SD Card

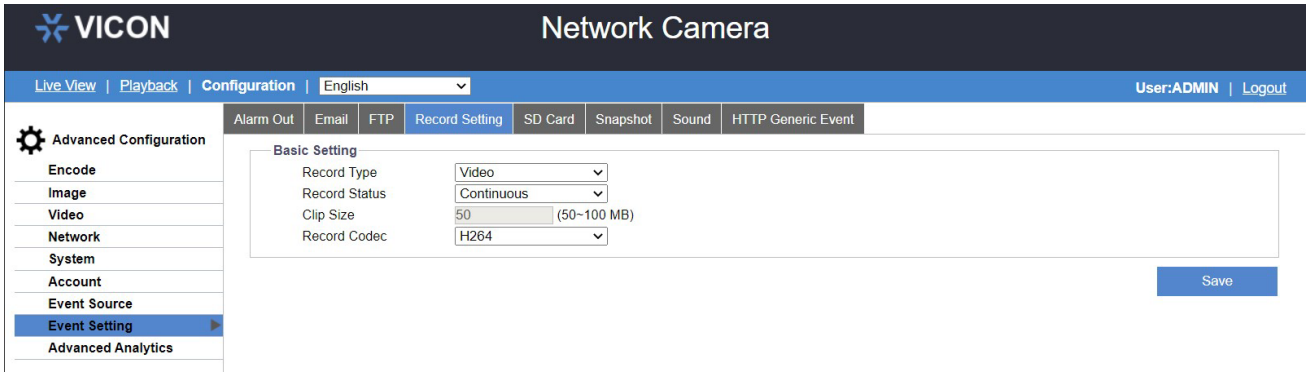
There are two options for continuous recording to the uSD card, Regular and Persist.

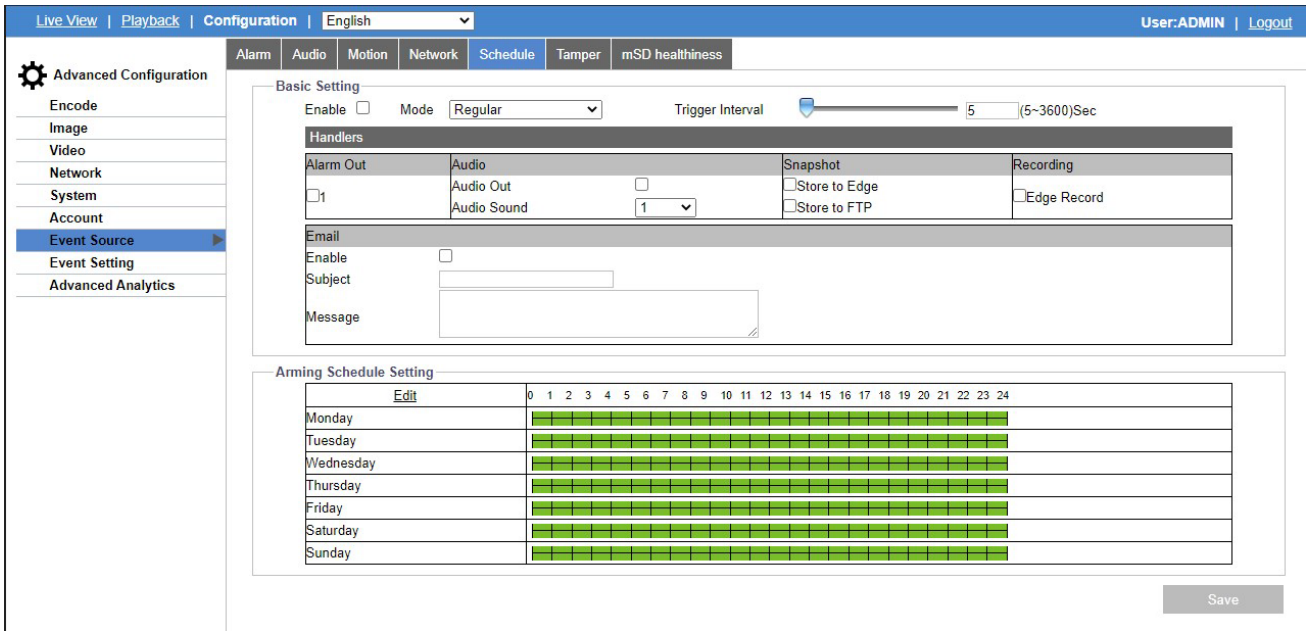
Regular uses pre-defined intervals. The date/time must be set properly to record the clips, preferably with time synched to an NTP server.

1. **If user wants to record video continuously:**

   If a user wants to record continuously (24/7) and wants the timeline on playback able to be updated, it is suggested to use the following setting. The recommended duration is 120 seconds to 300 seconds (2 to 5 minutes file sizes).

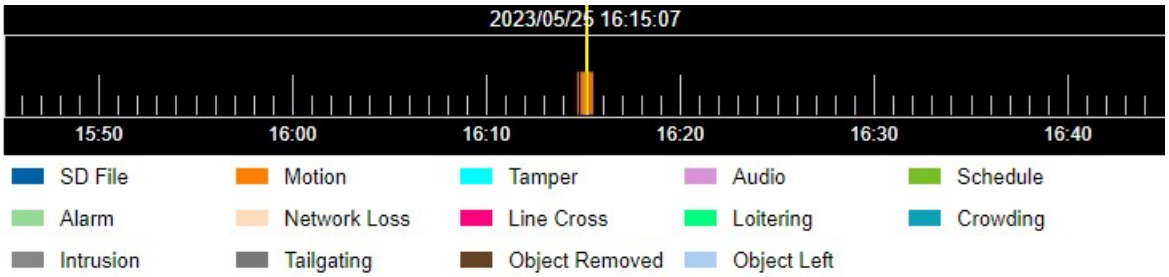
Regular (5 to 3600 sec)	Continuous	Records continuously and, when pressing Search button on playback page, updates timeline with the latest file with the pre-programmed duration.





Playback:

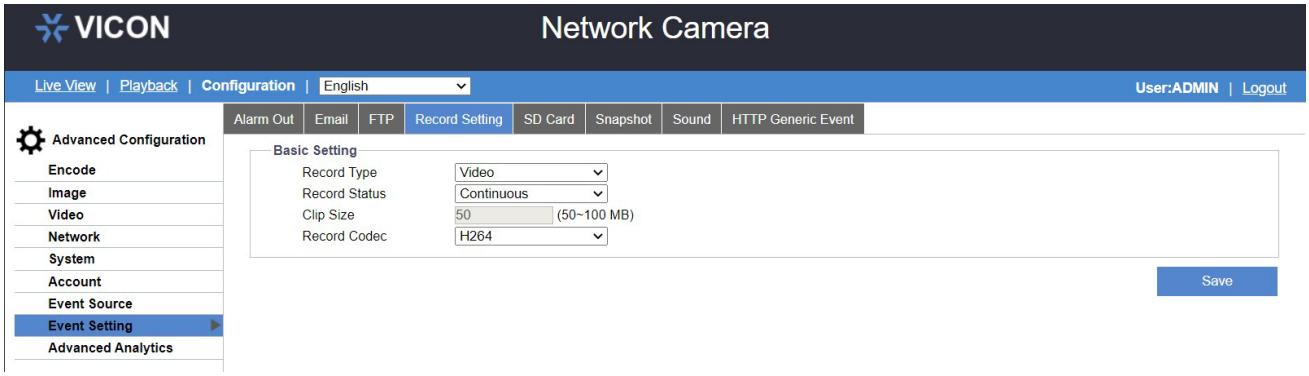
Press Search to update the timeline.

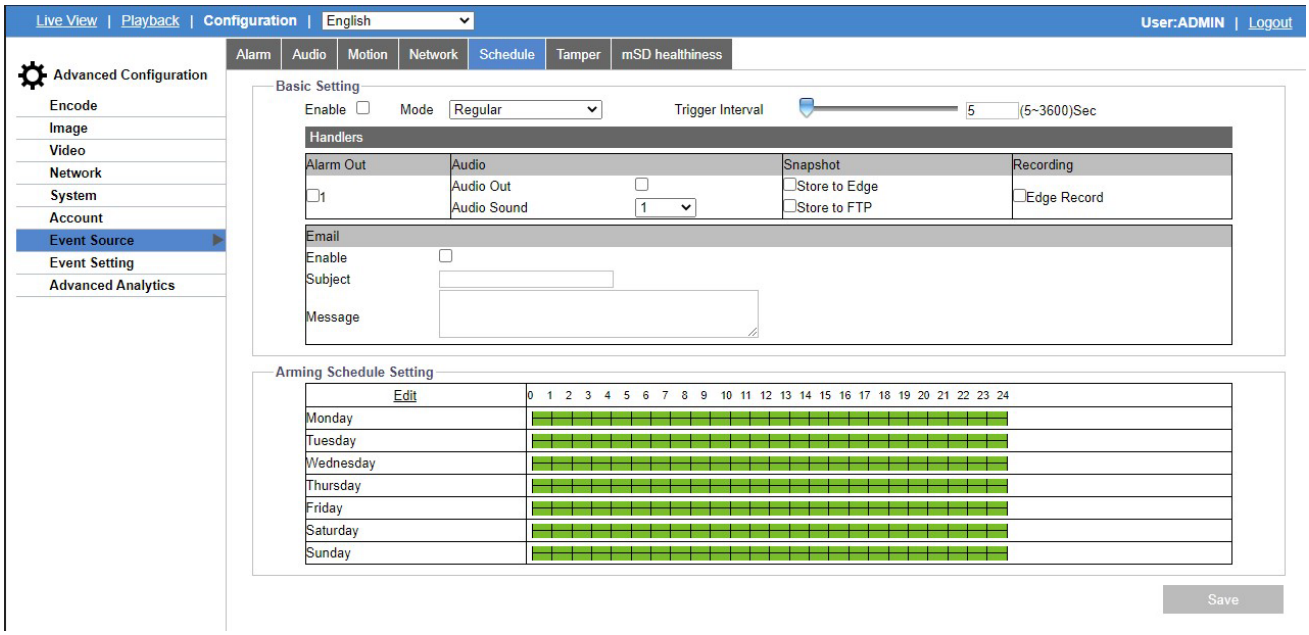


The selected clip will play, and the playback will stop at the end of the clip. Click on the next clip to play it back.

2. If user wants to use Persist mode and see the timeline updated:

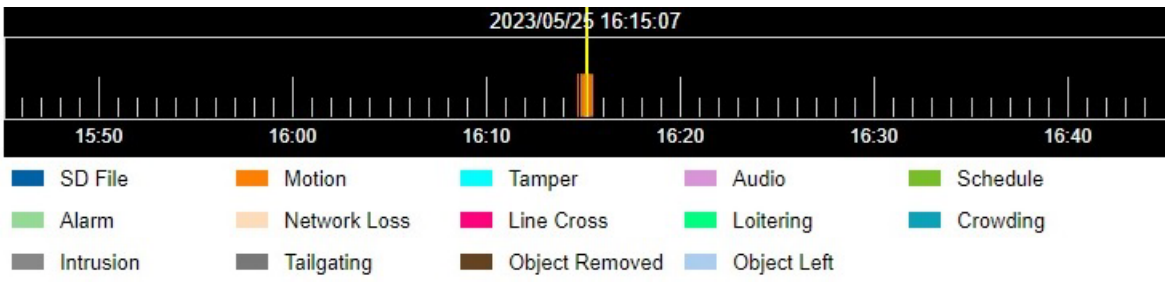
If the event has not ended yet, you can see the blue color on the timeline after 50 MB file is generated. However, if the event is finished, then the green color will be blended with the blue timeline.





Playback:

Press Search to update the timeline.



The selected clip will play, and the playback will stop at the end of the clip. Click on the next clip to play it back.

Vicon Standard Equipment Warranty

Vicon Industries Inc. (the "Company") warrants your equipment to be free from defects in material and workmanship under Normal Use from the date of original retail purchase for a period of three years, with the following exceptions:

1. Valerus/VAX Shadow Elite Servers, Recorders and Client Workstations: Five years from original retail purchase.
2. Vicon IP Cameras: Five years from original retail purchase.
3. Access Control System Components: Some readers and credentials have a lifetime warranty; refer to VAX warranty document for details.
4. Thermal Sensor VTR-3XXX/VTR-6XXX: One year from date of original retail purchase.
5. For PTZ cameras, "Normal Use" excludes prolonged use of lens and pan-and-tilt motors, gear heads, and gears due to continuous use of "autopan" or "tour" modes of operation. Such continuous operation is outside the scope of this warranty.
6. Any product sold as "special" or not listed in Vicon's commercial price list: One year from date of original retail purchase.

Date of retail purchase is the date original end-user takes possession of the equipment, or, at the sole discretion of the Company, the date the equipment first becomes operational by the original end-user.

The sole remedy under this Warranty is that defective equipment be repaired or (at the Company's option) replaced, at Company repair centers, provided the equipment has been authorized for return by the Company, and the return shipment is prepaid in accordance with policy. Repaired or replacement hardware will be warranted for the remainder of the original Warranty Period or ninety (90) days, whichever is longer. When a product or part is exchanged the replacement hardware becomes the property of the original purchaser and all hardware or part thereof that is replaced shall become the property of Vicon.

The warranty does not apply (a) to faulty and improper installation, maintenance, service, repair and/or alteration in any way that is not contemplated in the documentation for the product or carried out with Vicon consent in writing, operation adjustments covered in the operating manual for the product or normal maintenance, (b) to cosmetic damages, (c) if the product is modified or tampered with, (d) if the product is damaged by acts of God, misuse, abuse, negligence, accident, normal wear and tear and deterioration, improper environmental conditions (including, but not limited to, electrical surges, water damage, chemical exposure, an/or heat/cold exposure) or lack of responsible care, (e) if the product has had the model or serial number altered, defaced or removed, (f) to consumables (such as storage media or batteries) (g) to products that have been purchased "as is" and Vicon the seller or the liquidator expressly disclaim their warranty obligation pertaining to the product, (h) to any non-Vicon hardware product or any software (irrespective of packaged or sold with Vicon hardware product) and Vicon products purchased from an unauthorized distributor/reseller, (i) to damage that occurs in shipment or (j) to damages by any other causes not related to defective design, workmanship and/or materials.

The warranty for the products shall run from Vicon to End User customers only (including product purchased through authorized partners and resellers). Vicon is not obligated under any circumstances to honor warranties on product(s) purchases from internet auction sites including eBay, uBid or from any other unauthorized resellers. Except as explicitly provided herein, Vicon disclaims all other warranties, including the implied warranties of fitness for a particular purpose and merchantability.

Software supplied either separately or in hardware is furnished on an "As Is" basis. Vicon does not warrant that such software shall be error (bug) free. Software support via telephone, if provided at no cost, may be discontinued at any time without notice at Vicon's sole discretion. Vicon reserves the right to make changes to its software in any of its products at any time and without notice.

The Warranty and remedies provided above are exclusive and in lieu of all other express or implied warranties including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. Certain jurisdictions do not allow the exclusion of implied warranties. If laws under such jurisdictions apply, then all express and implied warranties are limited to the warranty period identified above. Unless provided herein, any statements or representations made by any other person or firm are void. Except as provided in this written warranty and to the extent permitted by law, neither Vicon nor any affiliated shall be liable for any loss, (including loss of data and information), inconvenience, or damage, including, but not limited to, direct, special, incidental or consequential damages, resulting from the use or inability to use the Vicon product, whether resulting from breach of warranty or any other legal theory. Notwithstanding the foregoing, Vicon total liability for all claims under this warranty shall not exceed the price paid for the product. These limitations on potential liabilities have been an essential condition in setting the product.

No one is authorized to assume any liability on behalf of the Company, or impose any obligations on it in connection with the sale of any Goods, other than that which is specified above. In no event will the Company be liable for indirect, special, incidental, consequential, or other damages, whether arising from interrupted equipment operation, loss of data, replacement of equipment or software, costs or repairs undertaken by the Purchaser, or other causes.

This warranty applies to all sales made by the Company or its dealers and shall be governed by the laws of New York State without regard to its conflict of laws principles. This Warranty shall be enforceable against the Company only in the courts located in the State of New York.

The form of this Warranty is effective March 2023.

THE TERMS OF THIS WARRANTY APPLY ONLY TO SALES MADE WHILE THIS WARRANTY IS IN EFFECT. THIS WARRANTY SHALL BE OF NO EFFECT IF AT THE TIME OF SALE A DIFFERENT WARRANTY IS POSTED ON THE COMPANY'S WEBSITE, *WWW.VICON-SECURITY.COM*. IN THAT EVENT, THE TERMS OF THE POSTED WARRANTY SHALL APPLY EXCLUSIVELY.

VICON INDUSTRIES INC.

For office locations, visit the website: vicon-security.com