User's Manual

Network Camera

LPR Series

v02.01.1.2.14216

SN-IPS56/30CDR/ZSD12/11

Table of Content

Connection

Default IP Address

Since this is a network-based camera, an IP address must be assigned at the very first stage. The camera's default IP address is 192.168.0.30 and sub mask is 255.255.255.0. However, if you have a DHCP server in your network, the camera would obtain an IP address automatically from the DHCP server so that you don't need to change the camera's IP address. But be sure to enable DHCP in "Network Settings" first.

Connecting from a Computer & Viewing Preparation

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 192.168.0.30". If the message "Reply from..." appears, it means the connection is available.

Start a browser e.g., Internet Explorer and enter IP address: 192.168.0.30. A login window as shown below should pop up. In the window, enter the default user name: admin and password: 1234 to log in.

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

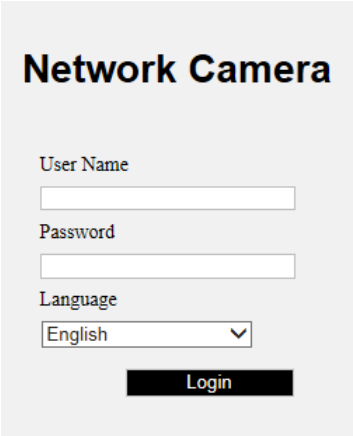


Figure: Login Window

Viewing Preparation

Images of the unit can be viewed through various browsers. Before viewing, follow these steps to enable the display.

Enable Cookies as instructions below.

- In Internet Explorer, click **Internet Options** on the **Tools** menu.
- On the **Privacy** tab, move the settings slider to **Low** or **Accept All Cookies**.
- Click **OK**.

When a proxy server is used, click **Internet Options** on the Tools menus of Internet Explorer, select **Connect** tab, click **LAN** button, and set proxy server.

Change Security in Internet options as instructions below.

- On tool menu, click **Internet Options**.
- Press the **Security** tab.
- If the camera operates inside of the intranet, click the **Intranet** icon.
- If the camera operates outside of the intranet, click the **Internet** icon.
- Click **Custom Level**. This will open the Security Settings – Internet Zone screen.

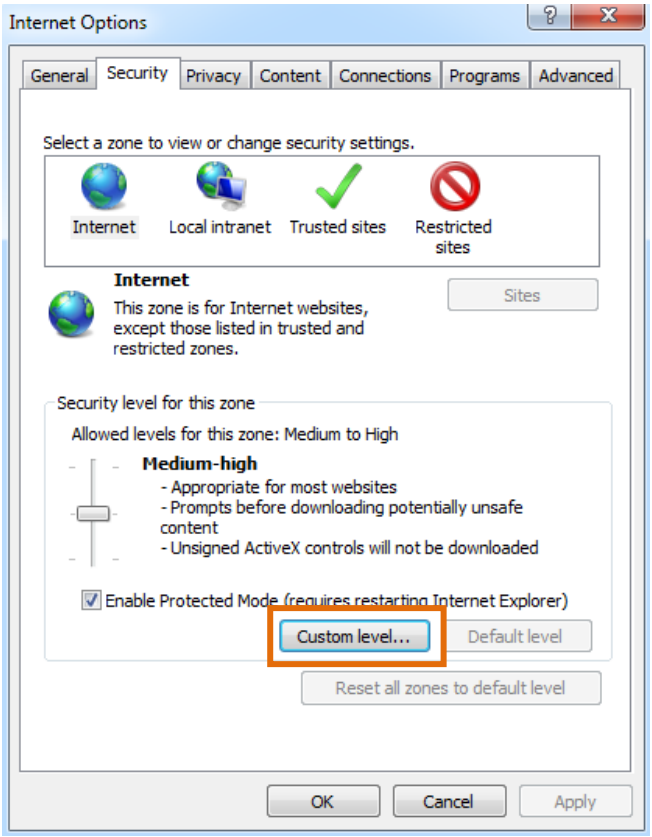


Figure: Security Settings 1/4

- Scroll down to the ActiveX controls and plug-ins radio buttons and set as follows.
- 【Download signed ActiveX controls】→ Prompt (recommended)
- 【Download unsigned ActiveX controls】→ Prompt
- 【Initialize and script ActiveX not marked as safe for scripting】→ Prompt

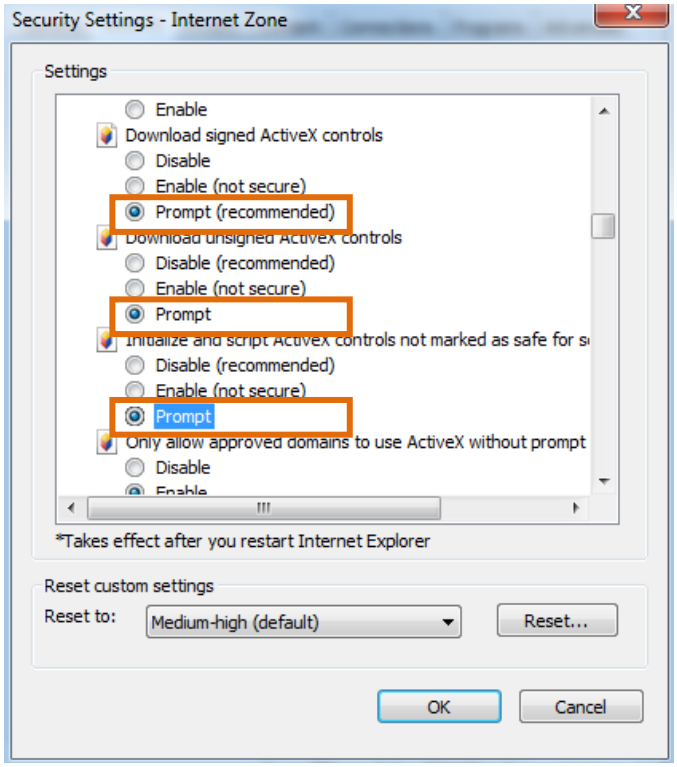


Figure: Security Settings 2/4

- 【Automatic prompting for ActiveX controls】→ **Enable**

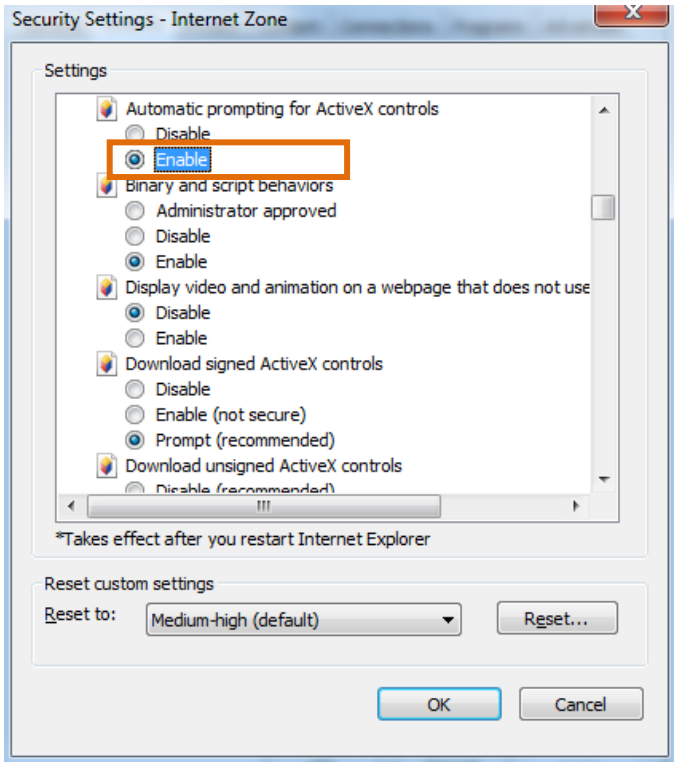


Figure: Security Settings 3/4

- 【Run ActiveX controls and plug-ins】→ Enable
- 【Script ActiveX controls marked safe for scripting*】→ Enable

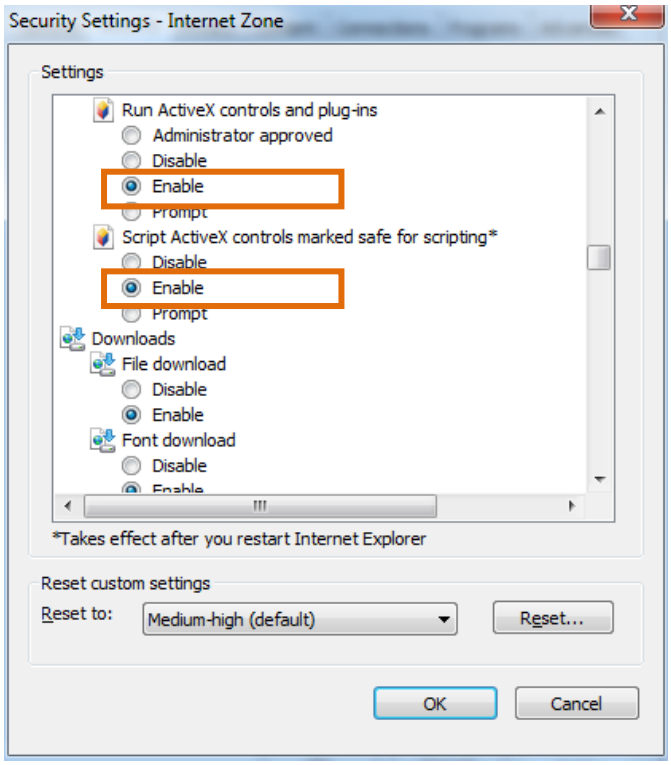


Figure: Security Settings 4/4

- Press **OK** to save the settings.
- Close the all browser windows and restart the browser. This will allow the new settings taking effect.
- Type your setting IP address into the browser.
- Then you should be able to see the camera image screen.

IP Finder

IP Finder is a utility program that helps users to locate the camera(s) in local area network that computer is connected to. Please note that IP Finder works only in Microsoft Windows XP, Microsoft Windows Vista, and Microsoft Windows 7 or above. Steps to get the utility program running are listed below.

1. Download the IP Finder's folder to local computer.
2. Double click on **IPFinder.exe** in the IP Finder's folder, and the IP Finder window should pop out below.

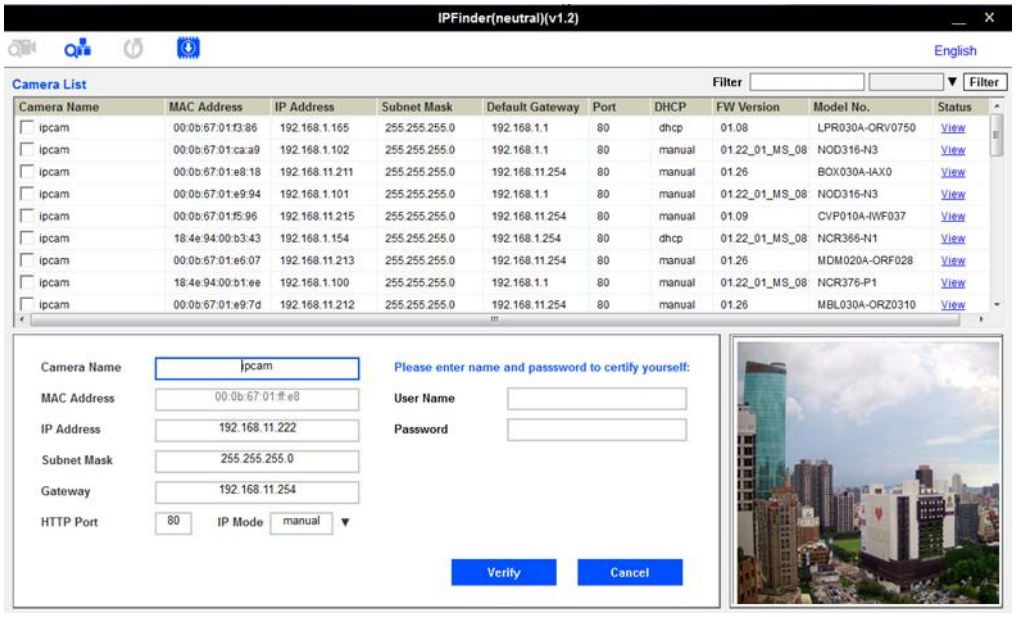


Figure: IP Finder

3. The window would list information of camera(s) in operation at present. Click one of the cameras in the list you want to configure the network settings.
4. Configure the following settings as needed.

- **User Name & Password:** Before performing any operation to any listed camera, please enter username and password for the selected camera, and then click "**Verify**" for authentication purposes.
- **Camera Name:** Enter a descriptive name for the camera.
- **Network Settings:** If you have a DHCP server on your network to assign IP addresses to network devices, enable the "dhcp" option from dropdown menu of **IP MODE**. Otherwise, select "manual" to manually enter the values for **IP Address**, **Subnet Mask**, **Gateway** and **HTTP Port** fields.
- Click **"Save"** to enable the settings. Click "**Cancel**" to discard the settings.

5. Press **"View"** button, the designated browser page of the selected camera will pop out. Please input the corresponding **User Name** & **Password** to log in to the specific page of camera.
6. Press **"Refresh"** button, all the cameras currently connected to the network will appear on the list.
7. Press **"Initialize"** button, there are three options, Software default, Hardware default, and Reboot camera, for user to perform the factory default or reboot the camera. After clicking the preferred item, the warning message will appear. Please confirm again before you perform the

selected function.

8. The "**Filter**" button on the upper-right corner allows user to perform filtering search, which means you can input certain keywords into the field nearby and also narrow down the range by selecting the criteria from the dropdown menu for a target search on cameras connected.

9. Click "**Fw Upgrade**" button to upgrade the firmware of selected camera. A pop up window like the image below will show up.

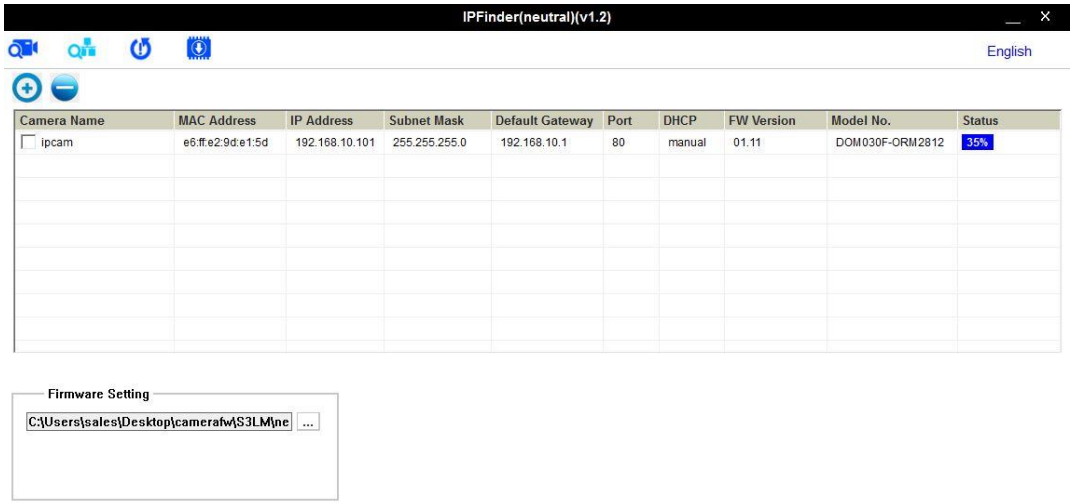


Figure: IP Finder Fw Upgrade

Please, follow the steps below to complete firmware upgrade:

- Click or to add or remove camera to be upgraded (only verified cameras will be shown on this list).
- Select a camera or click "**Select All**" button to select a camera or all the cameras on the firmware upgrade list, respectively.
- Click "**Add**" or "**Cancel**" button to confirm the selected cameras for upgrade or to cancel the selection, respectively.
- Enter the path for the desired firmware .tar or click ... then follow the instructions to find and upload the .tar file
- When the process is complete, click again to return to the list of all cameras located in the local network.

Live View

After accessing and logging 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, on the other hand, 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. We mainly focus on Live View part in this chapter and will detail Playback and Configuration in the later chapters.

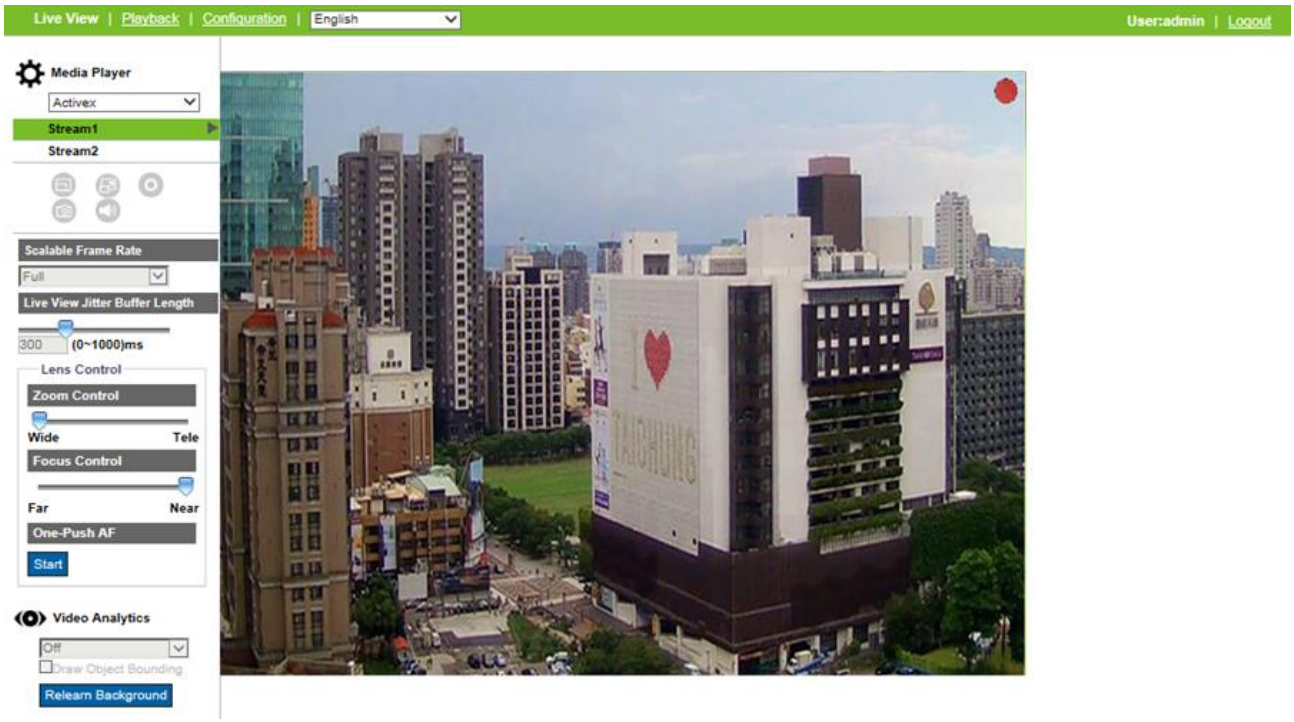


Figure: Live View

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: **ActiveX** and **JPEG**. ActiveX, only available in Internet Explorer, provides full functionality, better image quality and lower bandwidth consumption in Live View page. On the other hand, JPEG trades ActiveX advantage off for broader browser options including Chrome, Opera, etc. but has lower frame rate display.

"Stream1/2/3" are available for user to switch among each stream configuration for better adaptation in varied applications.

Note	• "Stream1/2/3"are available only in ActiveX mode, provided that the streams are enabled in "Encode" section.

Other items and icons under Live View are elaborated in detail next.

Icon	Definition
	The "Snapshot" button is for user to take a snapshot and save it in a user predefined folder.
	The "Full Screen" button is for user to display a full screen display. (ESC to back)
	The "Manual Recording" button is for user to activate recording function.
	The icon on the upper-right corner indicates that live view video is being recorded.
	The "Audio Output" button is for user to toggle on/off the audio output function.
	The "Zoom Control" button is for user to manipulate digital zoom magnification. After clicking the button, place the mouse cursor over the live view screen followed by using the scroll wheel to perform digital zoom in or zoom out functions.

Table: Live View Icons Definition

Note	•	"Full Screen", "Manual Recording", "Audio Out", and "Zoom Control" icons are available only in Activex mode, while "Snapshot" icon is available in both Activex and JPEG modes.

Scalable Frame Rate

Due to multi-browsers support, the performance of live view will vary according to the efficiency of each browser and client device. Consequently, the "Scalable Frame Rate" is introduced to help user dynamically adjust to a desired frame rate per browser applied for smooth video display. The option "Full" indicates a full frame rate display in response to the setting under "Encode" page, whereas "1/2" & "1/4" mean that display frame rate will be reduced to one half and one quarter respectively. Turn "SVC-T" on before using this function. Refer to "***SVC-T***" for further details.

Note	•	Scalable Frame Rate is available only in ActiveX mode.

Live View Jitter Buffer Length

Live View Jitter Buffer Length decides when to transmit media packets for Live View display based on packets it has collected, packets it is still waiting for and the timing required to playback the media.

Dragging the adjustable bar of "Live View Jitter Buffer Length" to higher value lessen the negative effect, namely choppy live video display, caused by transmission delay arising from network congestion. However higher values also increases overall transmission latency.

Note	•	Live View Jitter Buffer Length is available only in ActiveX mode.

Back Focus / Lens Control

The specific Lens Control section under Live View is related to both lens and focus remote manipulations and nearly identical to the chapter "*4.1Back Focus / Lens Control*". Refer to the latter chapter for thorough manipulations.

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, it means that 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 use only when a VA function is activated
- Relearn Background: click this button to save new background that later will be compared to current background for motion detection purpose.

Note	• Keep the zoom level of used browser as 100% to display a normal live view. • While using a browser that does not support ActiveX, e.g., Chrome, some of the above sections will NOT be available.

Playback

Our cameras provide 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.

The key point to remember is 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 that appears will look like the image below.

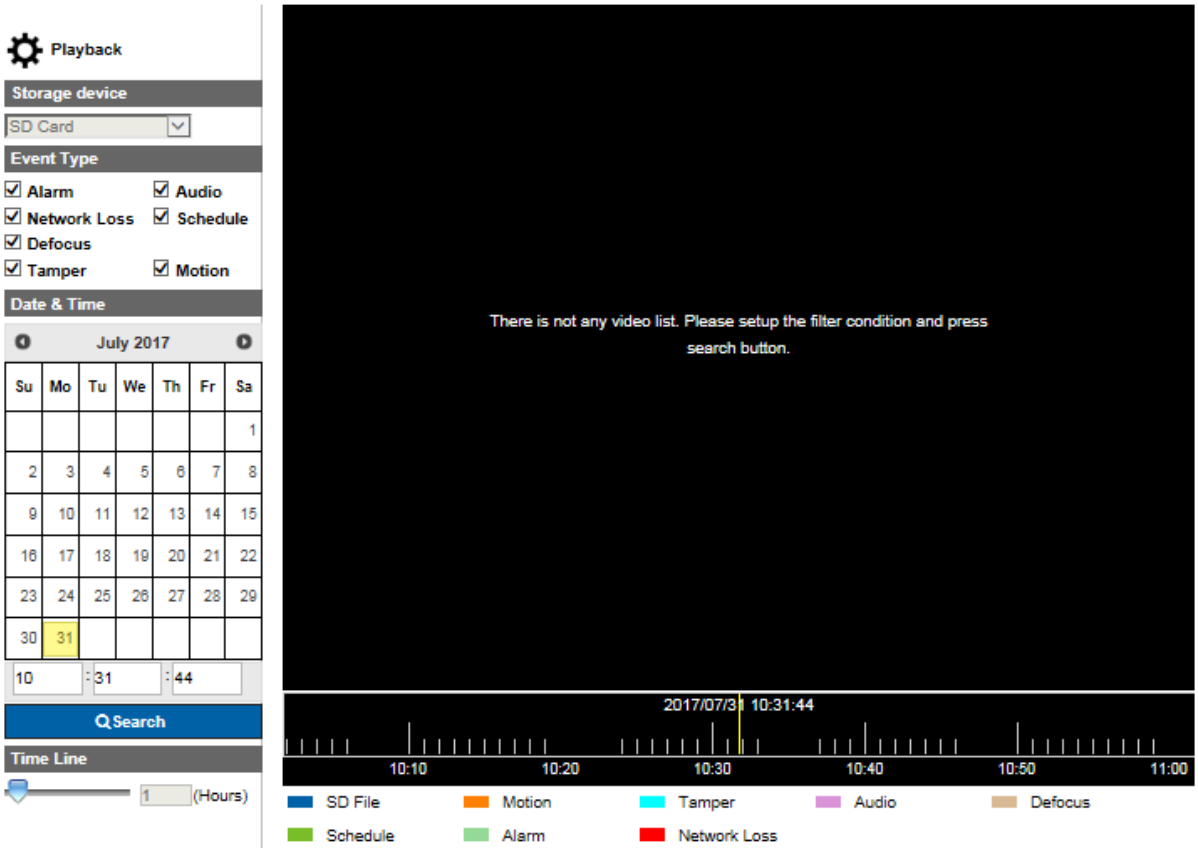


Figure: Playback

Storage device: SD Card

Till this moment, the only storage device supported by our camera is micro SD Card.

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

After selecting the edge storage, videos can be searched based on type of events that triggered video recording, and day and time recording was stored.

Check the boxes to select the type of events that possibly trigger the video you are searching for.

Date & Time

User can pick the exact date and time segment to search for recorded video, by clicking on a date on the calendar and entering time, respectively.

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 above configuration choices.

Time Line: 0.5 ~ 6 (hours)

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

Timeline Area

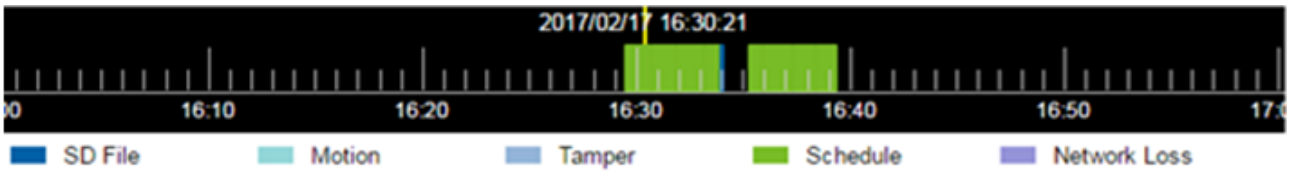


Figure: Time Line Area

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 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. Pay attention 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 not selected types 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

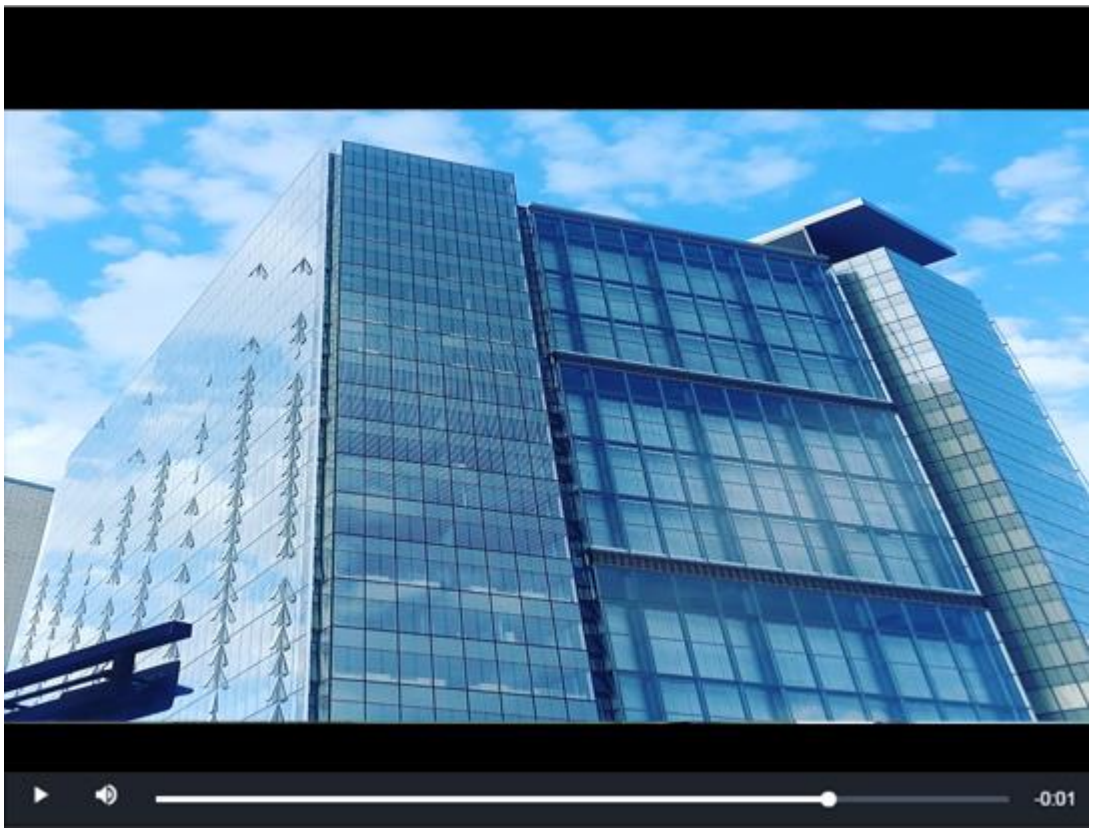


Figure: Display and Playback Toolbar

- To play a video, simply hover over a color bar on timeline area till a hoverbox shows up, then click on the color bar for the recorded video automatically start playing on the display.
- While the video is playing, user can hover over the displaying video to activate playback toolbar. Refer to table below for more details on Playback Toolbar.

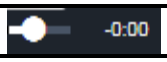
Icon	Definition
	The "Pause" button is for pausing video
	The "Play" button is for start playing video after pausing
	The "Mute" button is for muting video
	The "Unmute" button is for unmuting video
	The "Volume" button is for adjusting volume of video. Hover over mute or unmute button to activate volume button.
	Displaying video progress bar

Table: Playback Toolbar Icons Definition

Configuration

After clicking "**Configuration**", the screen will be shown as below, with several menu options on the left side for users to configure. We will thoroughly introduce them one by one in the following chapters.

1. LPR

1.1 LPR

The "LPR" page is exclusively designated for LPR (License Plate Recognition) models and contains features related to LPR configurations for a variety of environments that cover most of the scenarios of general conditions. The dynamic schedule time settings, additionally, further allows LPR to be upgraded to a more precise and integrated solution for all-dimensional applications.

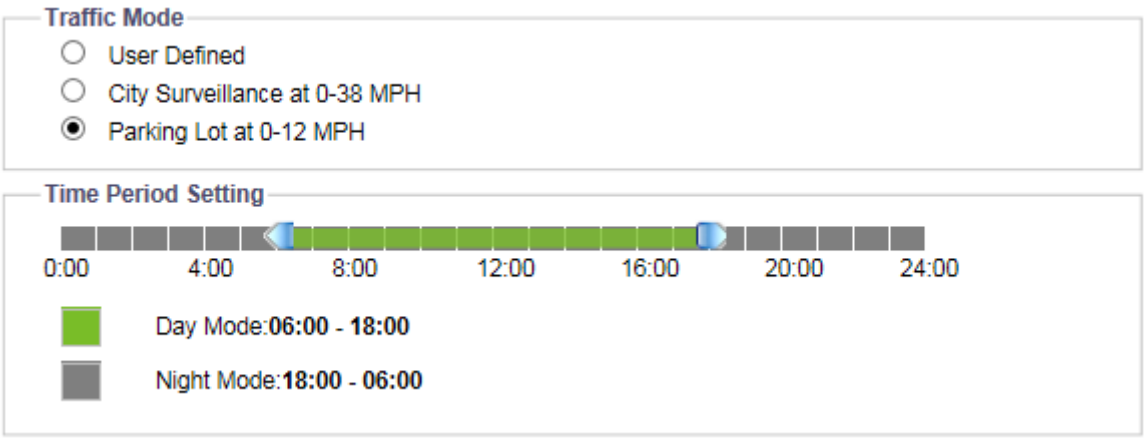


Figure: LPR Setting

Traffic Mode

User Defined

A flexible mode that can be fully customized. It is highly recommended for technician with expertise to adopt this mode.

City Surveillance

For most of the traffic flows within cities, due to common speed limits imposed on many roads and streets for safety concerns. City Surveillance mode with predefined parameters combinations, can precisely recognize license plates of vehicles moving within speed ranging from 0 to 38mph.

Parking Lot

Generally, within parking lots vehicles are allowed to move with slower speed range, and sometimes such as in basement light intensity is dim. Consequently, it is critical to build a group of parameters that fit in those extreme conditions. Parking Lot mode, with available recognized speed from 0 to 12mph, has the ideal configuration for user to apply for parking lots with ease.

Time Period Setting

Used for defining a time range for "Day Mode" and "Night Mode". On the bar chart, individually click the blue arrows, and then drag them left or right to select the desired time range. Green region

represents selected day time range while gray region represents selected night time range. The exact time ranges for Day and Night Modes are shown in the illustration below the bar chart.

1.2 Day Mode / Night Mode

Exposure

This section is only available when "User Defined" mode is selected under Traffic Mode section.

Figure: Exposure Settings

Exposure Mode : Auto/ Shutter Priority/ Manual

There are 3 modes to select from, which are described below.

- Auto: With certain pre-settings, before taking videos, the camera automatically determines the correct exposure for pictures without user input settings for further exposure.
- Shutter Priority: It enables user to select a specific shutter speed for adjustment of aperture, ensuring a correct and proper exposure.
- Manual: A mode that allows user to manually control both gain value and shutter speed. It is recommended for an experienced administrator to adopt this mode.

Max Shutter Time : 1/60 ~ 1/7.5

Select the maximum shutter time for the "Auto" exposure mode only.

Min Shutter Time : 1/10000 ~ 1/120

Select the minimum shutter time for the "Auto" exposure mode only.

P Iris Control : Auto/ Manual

P Iris, with built-in stepper motor, assists camera to regulate the iris position precisely in light of volatile light conditions, thus optimizing result of crisp image with better depth of field. 2 options are available for selection as below:

- Auto: Iris position will alter itself accurately in accordance with the fluctuant light intensities within the applied environment to bring about a superior image quality at its best.
- Manual : 1~5

  Iris position will be kept within the selected level. 1 stands for the fully open status, whereas 5 represents the minimum level for iris position.

EV : -2 ~ 2

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

Note	•	EV is NOT available when exposure mode "Manual" is selected.

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

Set an area for Backlight Compensation. Backlight Compensation is a function that achieves the brightness of a selected area to optimal image level. This function is necessary when an auto iris lens tends to close quickly due to an intense light coming from back of object in the area wished to view, resulting in an area that is too dark and difficult to see. In this case, users may set the area corresponding to the portion wished to see. The area size illustrations are roughly as follows.

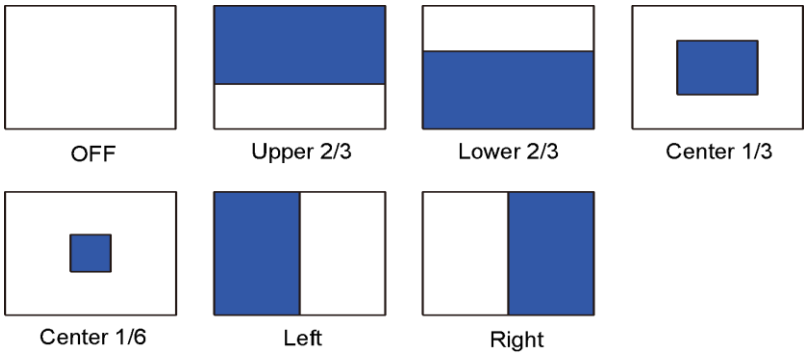


Figure: BLC Settings Illustrations

Note	•	BLC is NOT available when exposure mode "Manual" is selected.

HLC : On/ Off

High Light Compensation (HLC) is a function that suppresses intensified light sources in camera coverage so that image will be free from disturbance of strong light and thus details like license plate under strong headlight can be recognized clearly.

Note	•	HLC is NOT available when exposure mode "Manual" is selected.

Shutter : 1/10000 ~ 1/7.1

Selecting 1/10000 provides the fastest shutter speed.

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

Gain : 0 ~ 36

Larger the value, more intensity of lights come into the camera and vice versa.

Note	•	Gain is available only when both "User Defined" mode is selected under Traffic Mode section and "Manual" exposure model is selected.

Basic Color

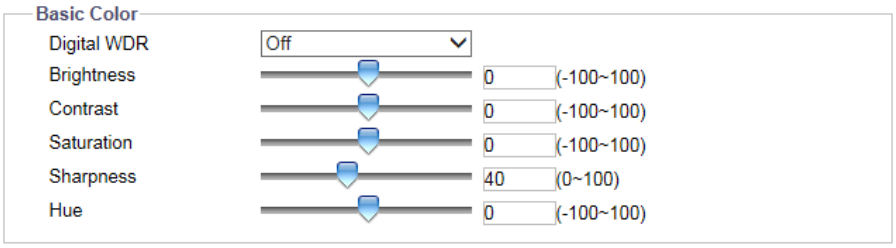


Figure: Basic Color Settings

Digital WDR : High/ Mid/ Low/ Off

In contrast to True WDR, the sensor-based technology, Digital WDR, which is based on software algorithm that optimizes image quality by adjusting the gamma value, facilitates better quality of details within both bright and dark areas, in a way that there are crystal clear details in both extreme areas; that is to say, bright areas are not saturated, and dark areas are not too murky.

Item	Option/ Range	Description
Brightness	-100 ~ 100	Selecting the higher value provides the brighter image.
Contrast	-100 ~ 100	Selecting the higher value provides the higher contrast image.
Saturation	-100 ~ 100	Decreasing saturation brings the image closer to a grayscale (that is, monochrome) image. Selecting 100 provides the highest image saturation.
Sharpness	0 ~ 100	Increasing the sharpness value will sharpen the edges and small feature of viewing images. If the edges appear too smooth or blurred, increase the sharpness; otherwise, decrease the sharpness. Selecting higher value provides the sharper image.
Hue	-100 ~ 100	Selecting the higher value provides the deeper hue effect.

IR LED

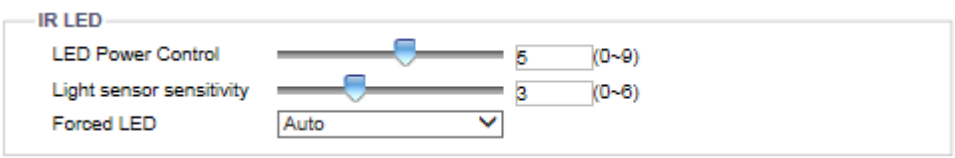


Figure: IR LED Settings

LED Power Control : 0 ~ 9

Adjust desirable intensity of IR LED in accord with application applied. Larger the number, the stronger the LED power is; smaller the number, conversely, the lighter it will be.

Light Sensor Sensitivity : 0 ~ 9

Slide the bar or input a number for a desired sensitivity of light sensor. Bigger the number, the more sensitive the light sensor is; smaller the number, on the other hand, the slighter it will be.

ICR Control

Corresponding to manipulation between daytime and nighttime, ICR (Infrared Cut filter Removal) is a mechanical design that facilitates infrared cut filter switch subtly in accordance with level of light intensity. Generally, with abundant light level in daytime, infrared cut filter is placed between image sensor and lens to efficiently filter out near IR wave spectrum, which distorts image colors in daytime. By contrast, infrared cut filter is supposed to be removed in night or low-light environments since camera requires additional IR to produce clear image under low-lux time and thus infrared cut filter is no longer useful for this application.

Figure: ICR Control Settings

Mode : Auto/ Color/ B/W

Select from the following 3 options for applying ICR control:

- Auto: Select it to allow ICR on and off automatically based on ambient light intensity.
- Color: ICR will be forcibly activated to filter out redundant IR spectrum that distorts colors of image.
- B/W: ICR will be disabled to allow IR illuminator to regularly brighten image in low-lux application.

Note	• If the setting of Exposure is "Manual", ICR Control Mode options are "Color" and "B/W" only.

2. Encode

Figure: Encode Settings

Profile

Current Profile : 1/ 2/ 3

User is strongly recommended to define different settings under each stream to flexibly bring about better video transmission for varied network environments and applications. By default, there are 3 profiles to be selected from and each profile contains 3 streams for individual further configuration. The detailed configurations for each stream are explicitly described in the following lines.

Stream

Corridor : On/ Off

In vertically oriented shape scenarios, e.g., sideway, aisle, corridor, because of the characteristics of these scenarios, which require more details in vertical areas, the prevailed 16:9 aspect ratio is not that appropriate and large portion of bandwidth is wasted in landscape field of view. Consequently, in order to optimize the image result for corridor-like applications, click "On" to enable this function so that the image will be rotated right 90 degrees to a 9:16 aspect ratio that perfectly fits portrait-like scenarios, reducing bandwidth and storage consumption.

Codec : MJPEG/ H.264

- MJPEG: Each video frame is individually compressed as single jpeg image with full-scale contents itself and can be retouched freely with ease. However, due to completeness of each frame, it results in larger file size and thus easily tends to lose frames under limited network bandwidth.
- H.264: The widespread video compression format that adopts intelligent technology to record variation 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 previous MJPEG codec.

Compression & Framerate

Compression options are 2048×1536, 1920×1080, 1280×960, 1280×720, 800×600, 640×480, 640x360,

320x240, 320x176, and frame rate are corresponding to the resolution, streams and codec selected.

Note	• Please check "Appendix: Product Comparison-Max resolution & frame rate" for the detail. • Please check "Table: Correlations of Resolution/Streams/FPS/Codecs" for the correlated value of each other.

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 value, the higher priority it will be.

Profile : High Profile/ Main Profile/ Baseline Profile

There are 3 different kinds of profiles for H.264 codec and the compression ratio, where the protocol for each type varies. Users may choose a proper one for desired applications or contact IT personnel for more information.

SVC-T : On/ Off

Although with a maximum of 2 profiles for video codec, sometimes it is not resilient enough for multiple applications usage in a volatile world. Consequently, SVC-T (Scalable Video Coding) is designed to overcome variety of scenarios by providing more subset bitstream layers, which has temporal scalability, to adapt into both fluctuant network bandwidth and different devices clients. For example, when a mobile phone under less network bandwidth requests live video from surveillance camera wih SVC-T enabled, the decoded video will be effectively adjusted and transmitted to fit this scenario, thus retaining the image quality of readability and conserving resources largely. On the other hand, when other client with better resources, e.g. desktop, requests live video, the decoded transmission will offer a live video with more frame rates and crystal quality video.

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 larger file size and thus consume more network bandwidth, while lower bit rate value, has slighter loading on network bandwidth due to smaller file size but with inferior image quality.

CBR Bit Rate / Max Bit Rate: 64 ~ 12000

The default bit rate synchronizes with the maximum resolution, e.g. 3MP@30fps model has 3000 bps as default. It is recommended to use the default bit rate as it provides 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 more compliant 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 codec is selected.

GOP : 1 ~ 60/ 1 ~ 50

Group of pictures 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.

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

Select the Quality Level number from 1 to 10 for H.264 Codec with VBR or CVBR 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.

Resolution	Aspect Ratio	Codec	FPS	Single Stream	Dual Stream	Triple Stream
3M	4:3	H.264	30	2048X1536	2048X1536 + 800x600 (All smaller resolution are available)	2048X1536 + 800x600 + 800x600 (All smaller resolution are available)
2M	16:9	H.264/MJPEG	30	1920x1080	1920x1080 + 1280x720 (All smaller resolution are available)	1920x1080 + 1280x720 + 800x600 (All smaller resolution are available)
1.2M	4:3	H.264/MJPEG	30	1280X960	1280X960 + 800x600 (All smaller resolution are available)	1280x960 + 800x600 + 800x600 (All smaller resolution are available)
1M	16:9	H.264/MJPEG	30	1280X720	1280x720 + 1280x720 (All smaller resolution are available)	1280x720 + 1280x720 + 800x600 (All smaller resolution are available)

Table: Correlations of Resolution/Streams/FPS/Codecs

3. Images

3.1 White Balance

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

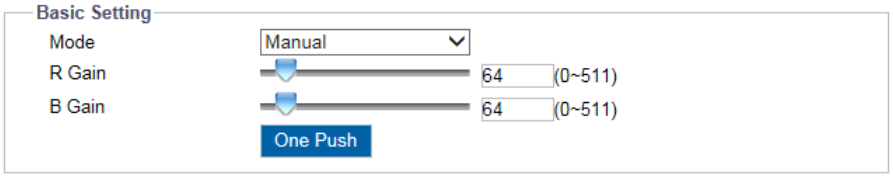


Figure: White Balance Settings

Basic Setting

Mode : ATW/ Auto/ Manual

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

R Gain/ B Gain: It 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.

3.2 Basic Setting

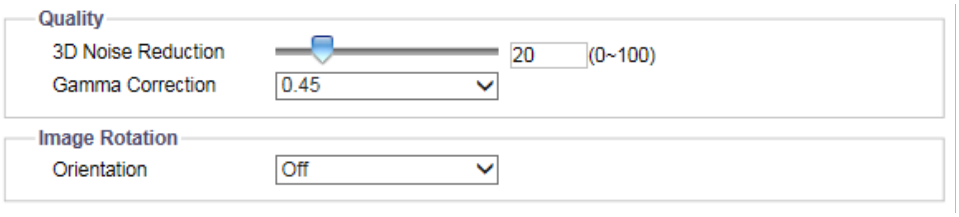


Figure: Basic Settings

Quality

3D Noise Reduction : 0 ~ 100

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

Gamma Correction : 1/ 0.45

Set gamma correction, which matters when you need to display an image accurately on different monitor screens, between 1 and 0.45 for better rendition in varied screens.

Image Rotation

Orientation : Off/ Flip/ Mirror/ Both

- Off: Disable video orientation function.
- Flip: Vertically reflect the display of the video.
- Mirror: Horizontally reflect the display of the video.
- Both: Both vertically and horizontally reflect the display of the video.

Note	• Mirror function will vary by different model, please check "Appendix: Product Comparison-Value Added" for details.

4. Back Focus / Lens Control

4.1 Back Focus / Lens Control

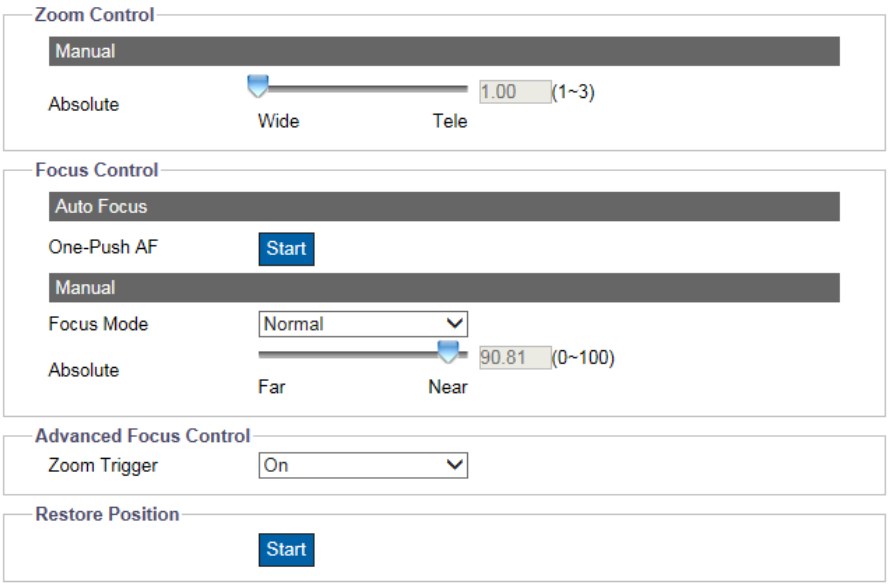


Figure: Lens Control/ Back Focus Settings

Zoom Control

Absolute : 1 ~ 3

By dragging the bar for Manual Zoom Control, user can zoom in the lens for a close-up view (Tele). On the other hand, user can also zoom out the lens for a view of wide angle (Wide). The number at the right corner indicates the current zoom magnification. Selecting 3 provides the highest magnification.

Note	• Zoom Control is supported only by motorized lens, please check "Appendix: Product Comparison-Lens Control" for details.

Focus Control

One-Push AF : Start

Click "Start" to have the lens focus automatically and immediately.

Focus Mode : Normal/ Advanced

There are 2 options within dropdown menu for selection of manual focus control.

- Normal: The "Absolute" option below is designed for user to manually drag and adjust the bar to an appropriate back focus setting. "Near" is for close-up view, while "Far" goes along with view of wide angle. Adjust it based on your zoom magnification of optional lens for a proper back focus. The number at the right corner indicates the current back focus value.
- Advanced: Due to defocus issue that sometimes happens between day and night mode switch, both the "Day Position" and "Night Position" sections here allow user to precisely define a specific

value for back focus settings on day mode and night mode individually, hereby improving the accuracy of back focus for different time sessions by a large scale.

Advanced Focus Control

Zoom Trigger : On/ Off

- Due to the swift changes of surrounding light intensity between day and night environment, lens focus will be affected, more or less, by certain level. Selecting "On" makes focus amended automatically for the changes occurred from day to night mode, or vice versa.

Note	• Advanced Focus Control is supported only by motorized lens, please check "Appendix: Product Comparison-Lens Control" for details.

•

Restore Position : Start

Click "Start" to restore the zoom magnification and focus of lens back to its default settings.

5. Video

5.1 Privacy Zone

Privacy Zone enables user to black out a specific portion of the screen for privacy concern. 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 sets of privacy zones for users to define. After setting up a privacy zone, the live view image will appear a frame, whose color, size and position can be customized by user's preference.

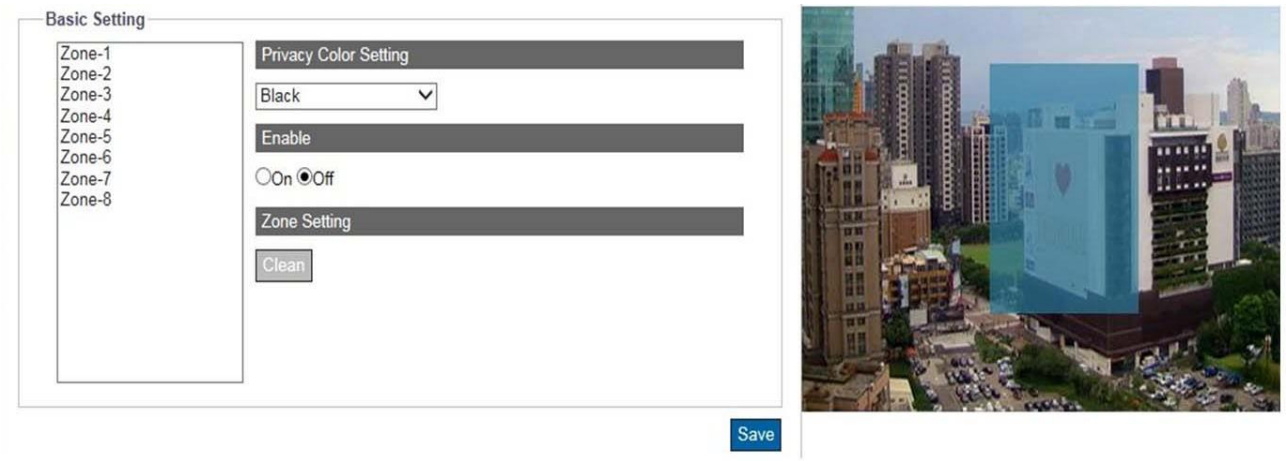


Figure: Privacy Zone Setting

To set up a privacy zone, user needs first to turn on any of the eight privacy zones (multiple available) and adjust the privacy mask size by pressing with left click and dragging to outline a desired privacy frame. Also, user can select a desired color (Black, Grey or White) for privacy zone. Press "Save" to make settings take effect. If you intend to delete settings, click "Clean" to wipe out privacy zone settings.

Note	• Please set the privacy zone slightly larger than the actual area to ensure privacy concern. • The maximum size of privacy zone shall reach full resolution.

5.2 Enhanced Codec

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

Dynamic ROI: It is for the camera to dynamically adjust compression based on what it believes is relevant. For example, the camera would be able to detect objects and decide higher or lower compression levels they would be. 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 to the average-sampling of current standard fixed GOP structure, with dynamic GOP the encoder has great freedom in I-, P- and B-frame selection. The dynamic GOP structure keeps temporal importance information of frames in the encoded video, which helps in adaptation to bandwidth decrease and temporal-SNR quality tradeoff decision. It also helps in storing more information with restricted resource, results in code efficiency increasing and better user perception.

The Enhanced Codec technology features the both 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 exploitation as the following elaborate descriptions.

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 crystal image quality within the zone, while the undefined zone, due to less important, will be sacrificed for image quality by higher compression ratio.

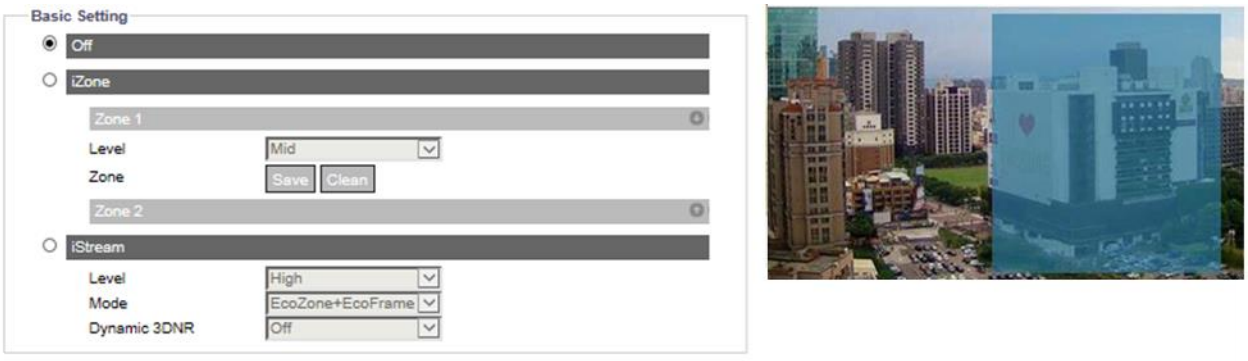


Figure: iZone Settings

First, turn one of the Zone or both on and click and drag left button on the right-side preview image to outline a desired zone. Also, user can select a wanted level for each Zone. Press "Save" to make settings take effect. If you want to delete settings, click "Clean" to wipe out the selected Zone settings.

iStream

This is a groundbreaking technology that helps saving network bandwidth efficiently whilst maintaining the crystal image quality for critical image details based on the 2 cutting-edge features as follows:

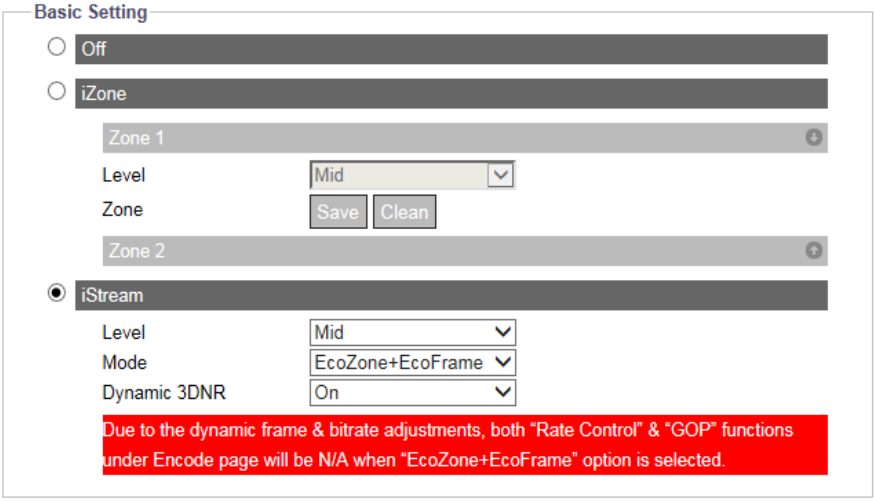


Figure: iStream Settings

- EcoZone

As opposed to iZone, the newly introduced "EcoZone" can swiftly identify dynamic motions occurred within a scene and retain its details with clear quality, whereas the rest areas, e.g. static background, will be imposed on higher compression level, thus economically decreasing bandwidth on less important things and still keeping the dynamic motions details for future forensic purpose. The intensity for EcoZone can be defined by the "Level" dropdown menu.

- EcoFrame

By enabling the proprietary EcoFrame function, the overall bitrate, i.e. bandwidth utilization, will be reduced even further. When less motion happens within a scene, e.g. storeroom, I-frame number, which is needed when motions are in scene, will be cut down largely by EcoFrame activation. Based on divergent complexity of scenes and motions occurred, a large amount of bandwidth saving can be achieved to render a compact yet valuable performance on bandwidth utilization. Note that it is compulsory to enable both EcoZone & EcoFrame functions simultaneously by selecting the option "EcoZone + EcoFrame" since EcoFrame is per se an enhancing technology that is based on EcoZone to promote the overall efficiency by a large scale. The intensity for EcoZone + EcoFrame can be defined by the "Level" dropdown menu as well.

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

- Dynamic 3DNR

While 3DRN allows user to adjust noise reduction level manually, dynamic 3DRN 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 Images will become unavailable.

6. Network

6.1 General

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

Basic Settings

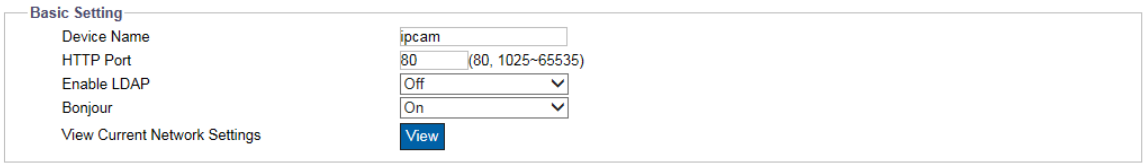


Figure: Network Basic Settings

HTTP Port : 1025 ~ 65535

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

View Current Network Settings : View

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

IP Settings

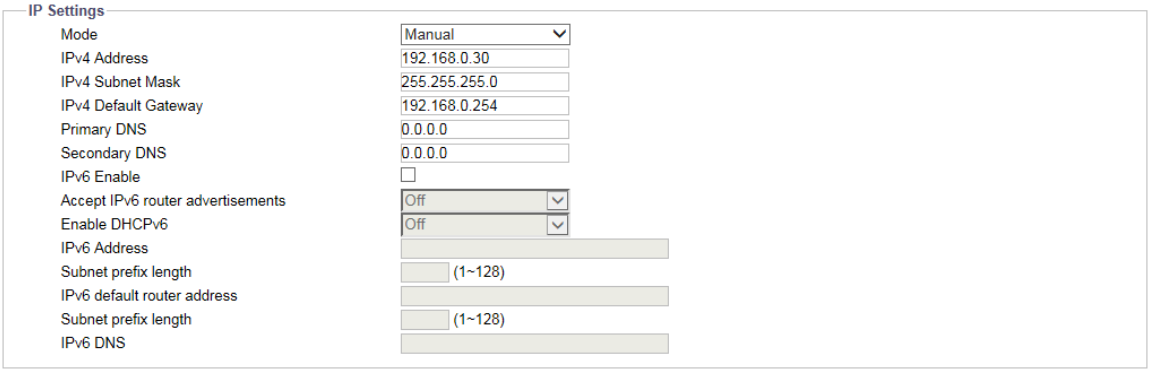


Figure: Network IP Settings

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 which 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 substantially practical for assigning an IP address automatically for camera when DHCP is not available within the connected internet environment.
IPv4 Address		Manually set an IP address under IPv4.
IPv4 Subnet Mask		Please 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/ 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.

Wire 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 is able to receive and transmit in full line rate simultaneously without the issue of collision. For the number to Mbps, larger the number, faster it results in; smaller the number, on the other hand, slower it brings about. "Auto" simply lets the camera to decide which mode to adopt.

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 Finder 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 synchronously.
- Device Name: Only device name will be shown.
- User Input: User can input a friendly customized name for the camera.

SSL

Enable SSL : On/ Off

Turn Secure Sockets Layer (SSL) on to enable communication security mechanism over internet network.

6.2 FTP Server

FTP (File Transfer Protocol), transferring files via TCP-based network, e.g. Internet, is a generally 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 9.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.

Port: 21/ 1025 ~ 65535

Input a value or 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:

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

To log into the FTP server and access the SD card, simply enter ftp://<Login ID>:<Password>@<ip address> in the search field of Microsoft's Internet Explorer, then the recordings will show up. The default setting, for example, is ftp://admin:1234@192.168.0.30. The maximum connection for FTP server is up to 30.

6.3 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.

Port : 1025 ~ 65535

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

- SD card access:

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

To log into the SFTP and access the SD card, simply enter ftp://<Login ID>:<Password>@<ip address> in the search field of Microsoft's Internet Explorer, then the recordings will show up. The default setting, for example, is ftp://admin:1234@192.168.0.30. The maximum connection for SFTP server is up to 30.

6.4 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 the way how client and server communicate packets with each other. Specifically, unicast transmits packets under 1 to 1 device method and multicast, on the other hand, transmits via the way of 1 to multiple devices. Hence, unicast requires large network bandwidth and occupies 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 on condition that all relevant peripheral devices like switch or router support the multicast protocol. Please adopt proper method based on your network applications for better 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.

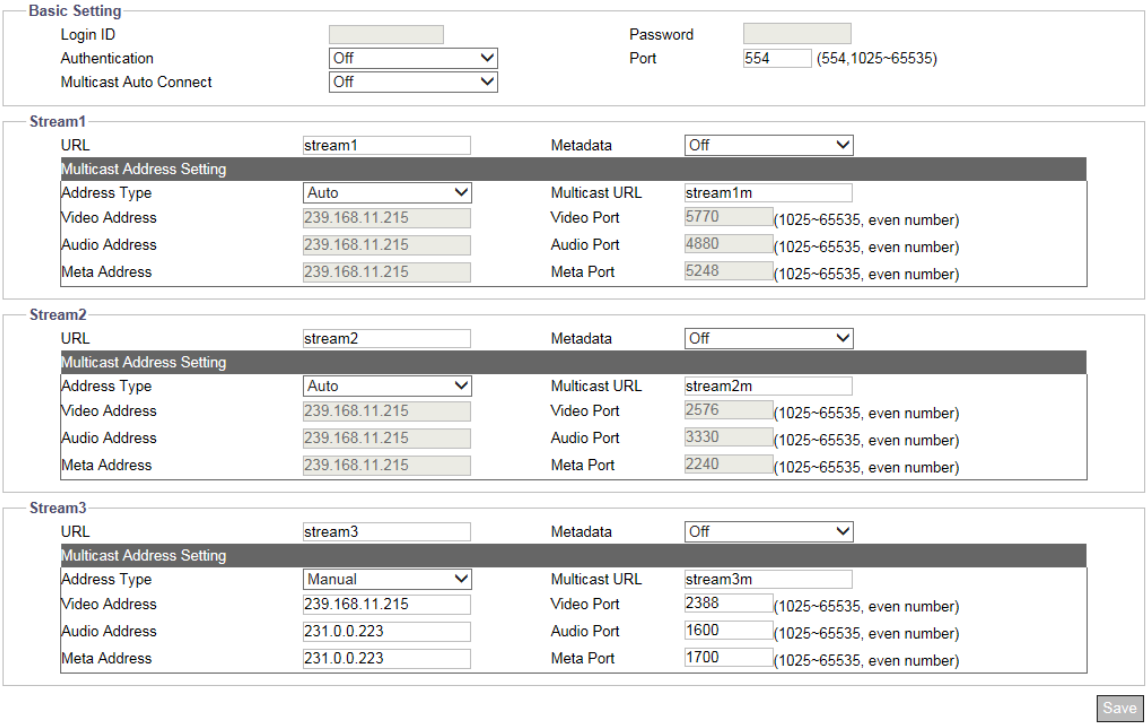


Figure: RTSP Settings

Basic Settings & Authentication

Enabling the authentication will improve the verifying mechanism and thus make the RTSP connection process more secure and much safer. To enable it, simply enter the Login ID, Password and Port (554 by default) with Authentication turned "ON". Turning Auto Connect "ON" will enable auto connection. Please note that it is not required to enable authentication beforehand to proceed with RTSP.

URL

Input a preferred name for representing each RTSP Stream URL. Basically it refers to Unicast URL protocol which transmitting 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 urlstream. After define preferred URL name for each stream, via 3rd party software you can, 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 to enable data about data, which means the data information will be allocated systematically, allowing similar data together by certain criteria and also distinguishing dissimilar data organizationally to effectively transmitting date information.

Multicast URL

Differing from URL, Multicast URL can transmit data from one host to a single host or to all hosts, thus consuming less network bandwidth with more flexibility. However, it is required to make sure if the peripherals connected with the camera are all compatible with Multicast in advance. For multicast, user can change address, port and urlstream. The address for Multicast is roughly the same as the previous URL. Please 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 advance to the further Video, Audio and Meta settings below, while "Auto" simply 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, as the UI implies, have a certain IP address range (224.0.1.1 – 239.255.255.254) for user to define individually.

6.5 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 newest version featuring improvements in performance, flexibility and security.

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

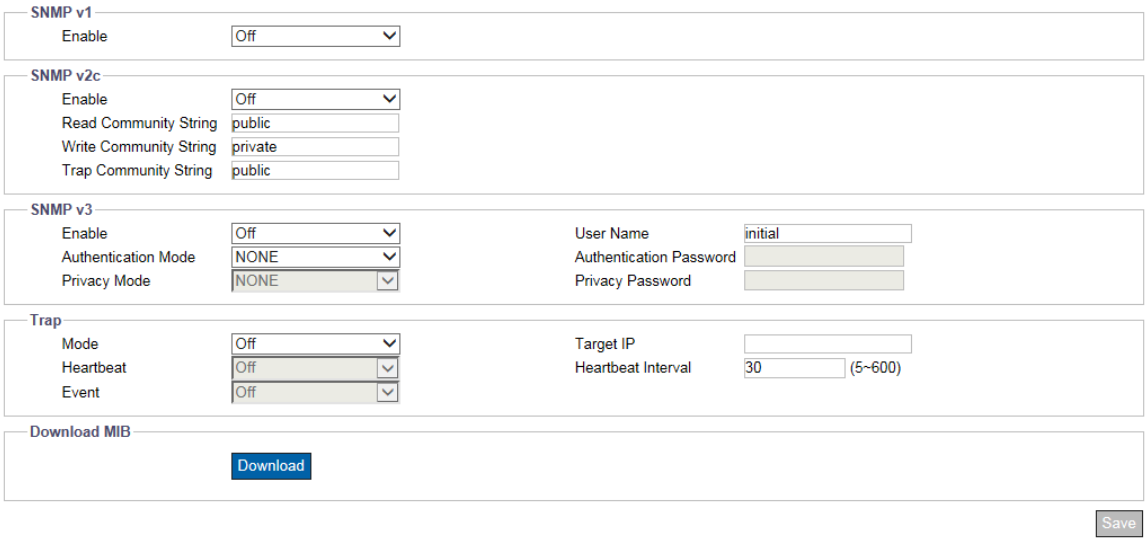


Figure: SNMP Settings

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. Tick "ON" 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 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 in a given interval. Tick "On" or "Off" to enable or disable heartbeat function here.

Heartbeat Interval: 5 ~ 600

Input desired values in seconds for Interval of Heartbeat.

Event : On/ Off

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

6.6 802.1X

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 further 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.

6.7 Firewall

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

Figure: Firewall Settings

Basic Setting

Mode : Allow/ Deny/ Off

- Allow: Select this option to make inputted IP addresses allowed to access IP camera.
- Deny: Select this option to make inputted IP addresses denied to access IP camera.
- Off: Select this option, none of 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 inputting address, check the box in front of each inputted address to activate the filters of allow or deny.

6.8 DDNS

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

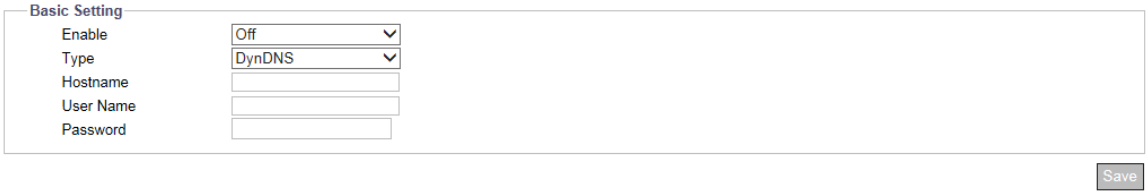


Figure 3 - 22: DDNS Settings

Basic Setting

Enable : ON/ Off

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

There are 4 types of DDNS for selection as the following items.

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

6.9 SSL

Method : None/ Self Signed/ Request/ Upload Certificate

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

- Self Signed: Self-signed certificate is a private own key that has no connection with person or organization that perform authorized certificate signing procedure. For self-signed certificate, user can create CSR (Certificate Signing Request) by filling below 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.

Note

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

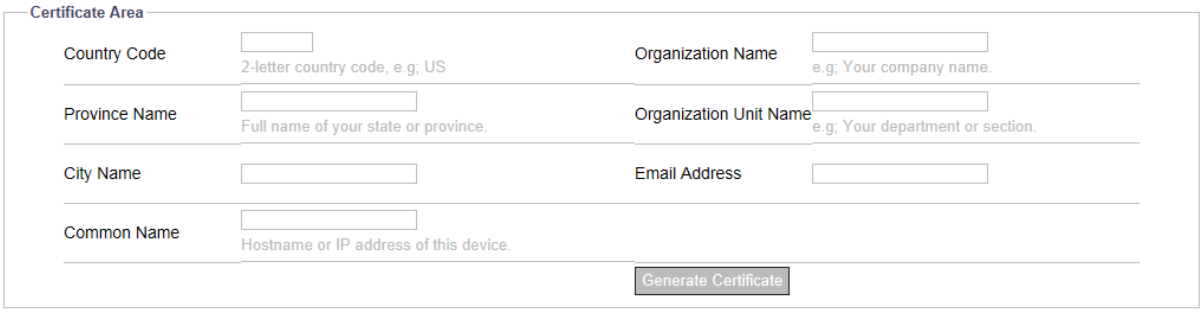


Figure: Self Signed & Request Settings

- Request

  Roughly similar to the settings of Self-Signed, by clicking the "Generate Certificate" after inputting the required fields, Request will provide user, apart from 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 authorized person or organization, followed by clicking the "Upload" to complete the SSL procedure.

Figure: Upload Certificate

6.10 RTMP

RTMP (Real Time Messaging Protocol), which is developed and owned by Macromedia, is a specific protocol for streaming video, audio and data via internet for general use.

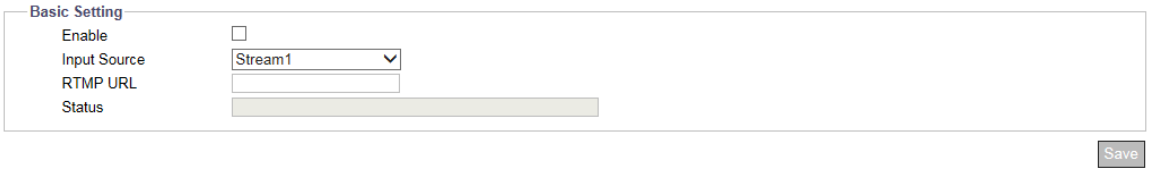


Figure: RTMP Settings

Item	Option/ Range	Description
Enable		Check this box to enable the function.
Input Source	Stream1/ Stream2/ Stream3	Select which stream (1 / 2 / 3) to be adopted as the input source for streaming.
RTMP URL		Input an URL address of RTMP provided by service server.
Status		The most current status of RTMP streaming will be shown here.

6.11 HLS

HLS (HTTP Live Streaming), the HTTP-based protocol for media streaming communications, can allow user to access live view image directly through like VLC player by the HLS URL provided.

Figure: HTTP Live Streaming Settings

Item	Option/ Range	Description
Enable		Check this box to enable the function.
Input Source	Stream1/ Stream2/ Stream3	Select which stream (1 / 2 / 3) to be adopted as the input source for streaming.
HLS URL		After enabling, an URL of HLS will appear within the field via which user can access the live streaming of the camera.

6.12 QoS

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

Figure: QoS Settings

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

7. System

7.1 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 setting Date and Time: Manually set date and time 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)

Time Zone Setting

First choose one of the regions from the left drop-down menu, and select the corresponding city, based on your located country/area, from the right drop-down menu.

7.2 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 understanding.

Figure: Audio Settings

Audio In Setting

Source : Line In/ Mic In

Select which audio source will be connected from the following 2 options.

- Line In: via audio line in source.
- Mic In: via microphone in source.

Enable : On/ Off

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

Encoding : G.711 A-law/ G.711 µ-law

2 audio codecs, G.711 A-law and G.711 µ-law, can be selected for audio input encoding.

Level : High/ Mid/ Low

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

Note

- The audio output performance shall not be 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 or ActiveX) rather than camera, the current supported formats are g.711a and g.711u.
- Audio function will vary by different model, please check "Appendix: Product Comparison-I/O Port" for details.

7.3 Firmware

Information about camera firmware is explicitly written under this page. User can manually upgrade System Firmware if upgrade is available. All motions of camera will be stopped during the firmware upgrade. Please 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 "Upload" to locate a corresponding firmware file and click "Upgrade" to proceed.

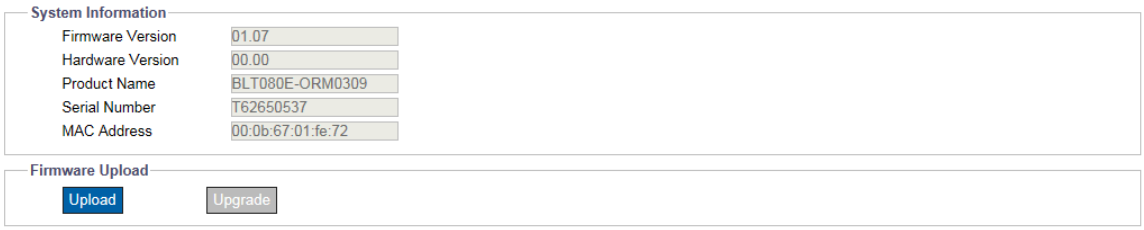


Figure: Firmware Settings

Note	• Power can't be lost when upgrading firmware since it will cause the upgrade failure and manufacturer maintenance will be therefore required.

7.4 Initialization

Figure: Initialize Settings

System Frequency : 60Hz/ 50Hz

Select "60Hz" or "50Hz" in accordance with different requirements. Flickering by fluorescent light can be reduced by selecting the proper power frequency.

TV Format : Full/ 4:3/ 16:9

Select an appropriate TV format from the drop-down menu in accordance with different aspect ratio monitor.

Import Setting

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

Export Setting

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

Configuration Setting

Reboot

Press "Reboot" to simply reboot the camera.

Software Factory Default

Press it to reset all configuration settings back to factory defaults excluding network settings.

Hardware Factory Default

Press it to reset all configuration settings back to factory defaults.

7.5 Advanced Security

Just as in our houses the main electrical panel is used for shutting off the electrical power of entire house or individual rooms, so Advanced Secure functionality is used for completely or partially turning off the access and connection to cameras. Advanced Secure is a way to make IP camera even safer.

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

Active Prevention has priority over Passive Protection. Hence, for instance 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 button at the end of the page after changing configurations for the settings take effect.

Active Prevention

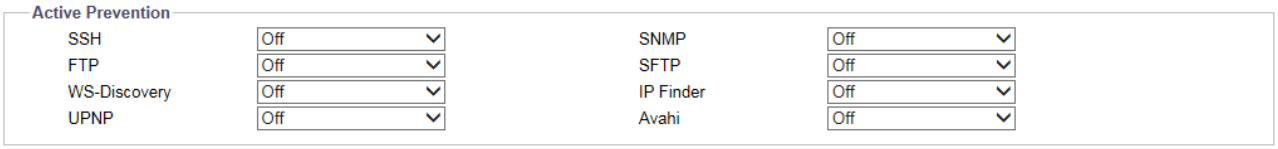


Figure: Active Prevention

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

For each protocols and services 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

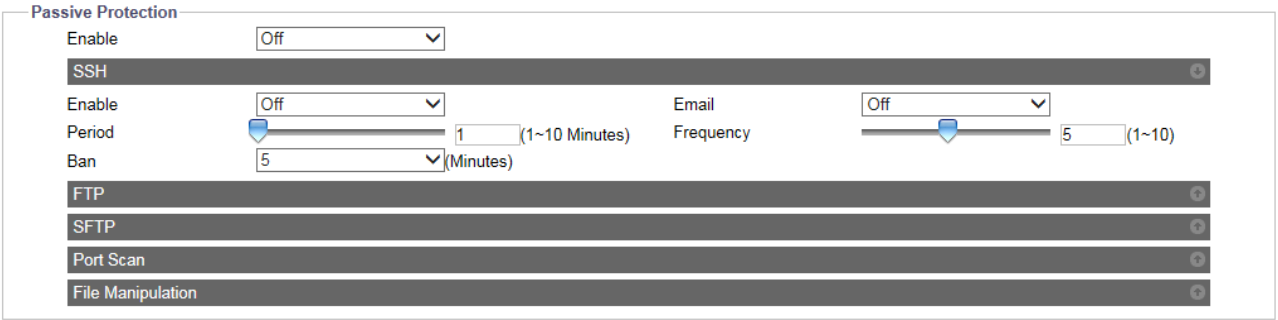


Figure: Passive Protection

Enable : On/ Off

While Active Prevention simply blocks the access and connection to the camera, Passive Protection on the other hand, 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, then send an email to a predefined user as notification.

Set "On" to activate Passive Protection mode. However, further configurations are needed to activate or deactivate specific protocols or services.

When enable is "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 a period 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 of time 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 period of time in minutes in which an IP address will be banned for trying and failing to access or connect to camera with certain frequency within a period of time. Or set the period of time 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

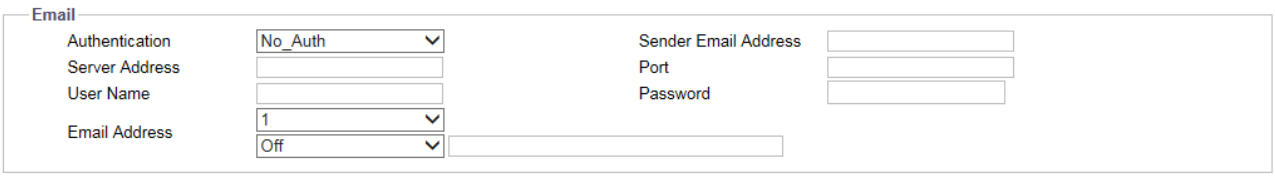


Figure: Email.

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

Please, refer to "*11.2Email*" 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 "On" to allow email to be sent to the user. Next, separately, enter the user email address for each user.

Banned IP List

Figure: Active Prevention

Whenever an IP address is banned, it will be shown on the Banned IP List together with 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.

7.6 OSD

This section allows user to enable OSD (On Screen Display) s

ettings. In addition, it extends the OSD function to accord with the occurrence of events.

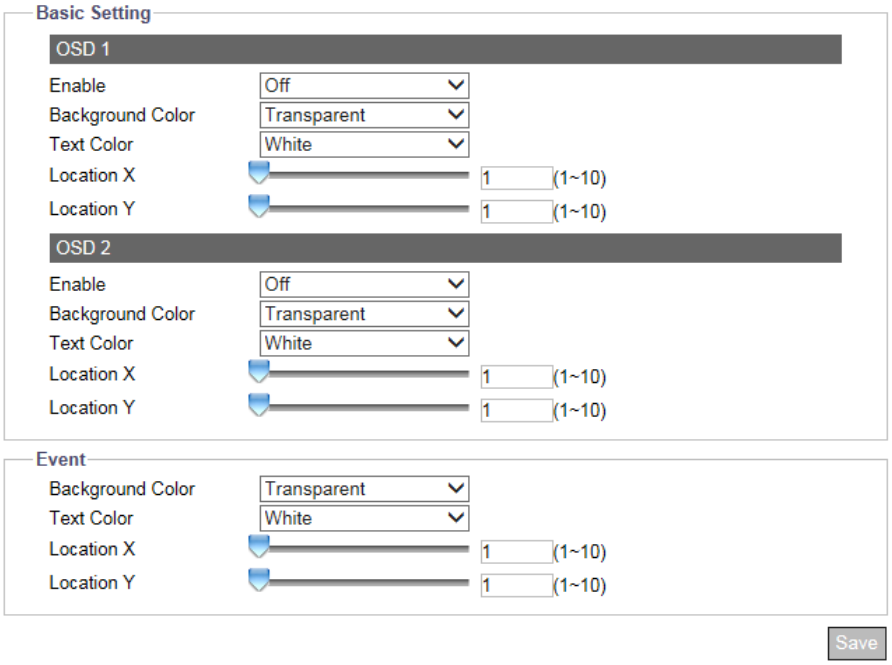


Figure: OSD Settings

Basic Setting

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

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

Event

When an event is triggered, OSD can be displayed on screen to highlight and inform user.

7.7 Events

As an intelligent apparatus, the IP camera is capable of automatically detecting scores of events such as motion, tamper, network loss, alarm, etc., and taking actions to inform the user about the occurrences. Consequently, the Event Search section assists administrator to have detailed yet systematic analysis on each individual event with its type, counts and time.

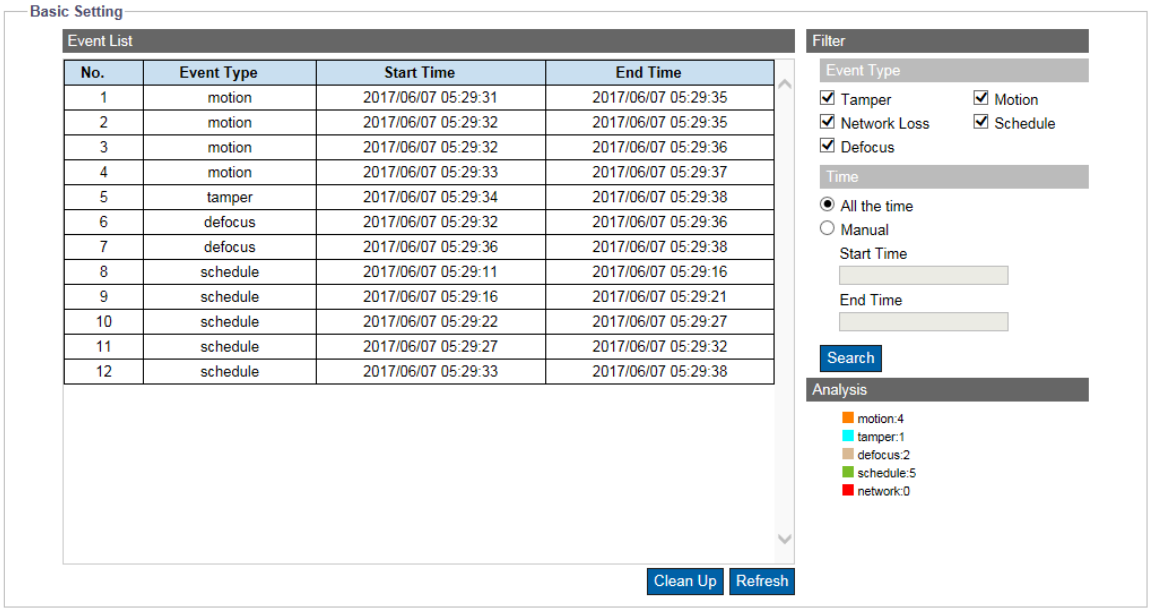


Figure: Events

Basic Setting

Event list displays all events identified by the camera, with information including types, starting time, and ending time. Click on "**Refresh**" to get a most updated list of events that are enabled for detection in Event Source. Click on "**Clean Up**" to clear this list.

Under Filter, select the type of events included and select either "All the time" or "Manual" followed by input of time in "Start" and "End" time fields to define the time frame these types of events took place.

A list of counts of the entire types of events is displayed under Analysis on the lower right to give an overview of how frequent each type of the event took place.

8. Account

8.1 Account Management

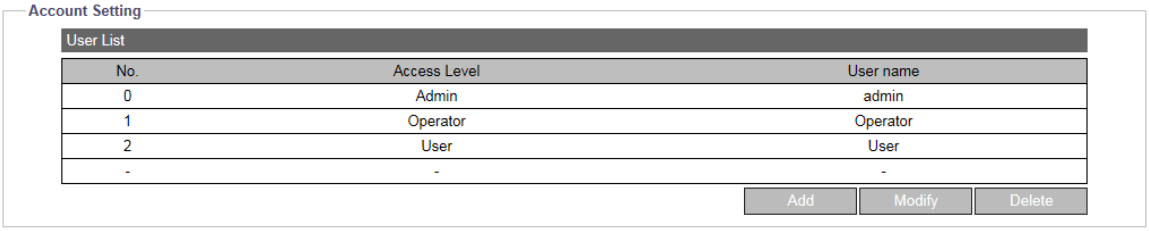


Figure: Account Settings

Account Setting

Access Level : Admin/ Operator/ User

- Admin: "Admin" level has the highest privilege control for accessing camera, which can handle both live view and all the configuration settings. The default username and password for Admin are "admin" and "1234" respectively.
- Operator: Differing from Admin, Operator level can only access camera for live view, storage, and remote lens control functions.
- User: Being the lowest level, User level can only access camera for live view function.

Add Users

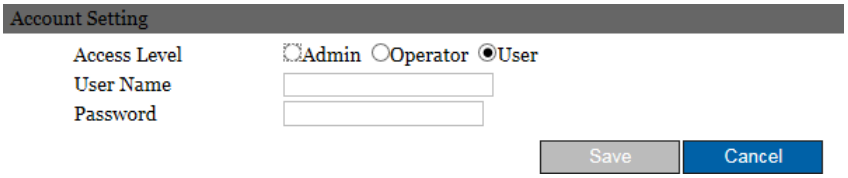


Figure: Add Admin/ Operator/ User

- Add: Place the mouse cursor over the blank column and click the "Add" button. The prompt window will pop up for you to input customized username and password for new user, the level (Admin, Operator or User) of which is also available to be selected here.

Note	•	Up to 10 users are available to coexist.

Modify & Delete Users

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

Caution	•	The login Username and Password must be 4 to16 characters long with the valid

alphanumeric value merely including '0' to '9', 'a' to 'z', 'A' to 'Z', '.','-','+','_'and '@'.

- The username cannot be the same as any currently existed username, including "admin".
- A user may reset the Account Management system to the camera's default settings.

8.2 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, have a major role in both intranet and internet applications to facilitate information sharing between devices.

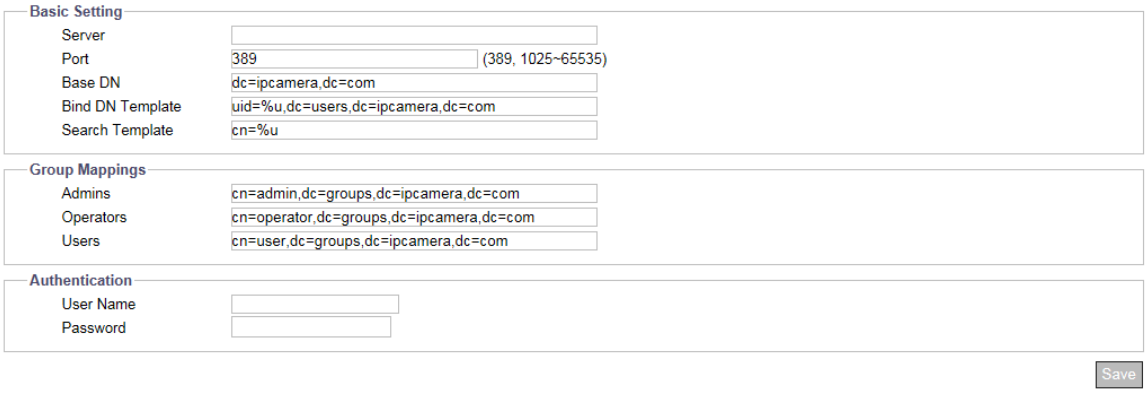


Figure: LDAP Settings

Basic Setting

Server

Input a server for LDAP.

Port : 1025 ~ 65535

It is recommended to use the default port number 389; however, if it is required to change the port number, please 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 has full access to live view functionalities.

Operators: relates to the LDAP operator privileges, which can watch live view and operate snapshot, manual recording and full screen.

Users: relates to the LDAP user privileges, which can only watch 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 inputted username for correct authentication.

9. Event Source

Event source configurations are consisted of Event Specific, Handler and Arming Schedule. The table below gives an overview of event source configurations and dependencies.

Type	Settings			Remark
	Event Specific	Handler	Arming Schedule	
Alarm	NO/NC	V	V	Model Dependency.
Audio	Sound Intensity	V	V	Model Dependency.
Motion	Object Size, Sensitivity	V	V	
Network	Wire Network Lost/ Wire Network Conflict	V	-	Not support HTTP Generic Event.
Schedule	Regular/Persist trigger event action (without event source as premise)	V	V	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 event occurs. Check the box to activate this function.

Note	• The available numbers of alarm output will vary by different model, please check "Appendix: Product Comparison-I/O Port" for details.

Audio

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

  10 sound types are available to be chosen from the drop-down menu for audio output. Be sure to set up the sound file beforehand. Refer to the "***11.7Sound***" section for details.

Note	• The availability of audio will vary by different model, please check "Appendix: Product Comparison-I/O Port" for details.

Snapshot : Store to Edge/ Store to FTP

- Store to Edge: Check the box to save snapshot to the inserted SD card when event occurs.
- Store to FTP: Check the box to save snapshot to the FTP remote device when event occurs. Note that under Handler, the camera act as FTP client, while the remote device act as FTP server, and the FTP server path should be properly configured in advance in "***11.3FTP***" section.

Recording

- Edge Record: Check the box to save the recorded video to the inserted SD card when event occurs.

Email

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

OSD

- Enable: Check the box to enable the OSD function when 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 to be chosen from the dropdown menu for message notification. After user set the type of method, please refer to "***11.8HTTP Generic Event***" section for details about method setting.

Arming Schedule Setting : Monday~Sunday (24H)

Under this section, user can freely set up an ideal 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 00 to 24 hours. Click the "Edit" button at the upper-left corner to enter the setting page.

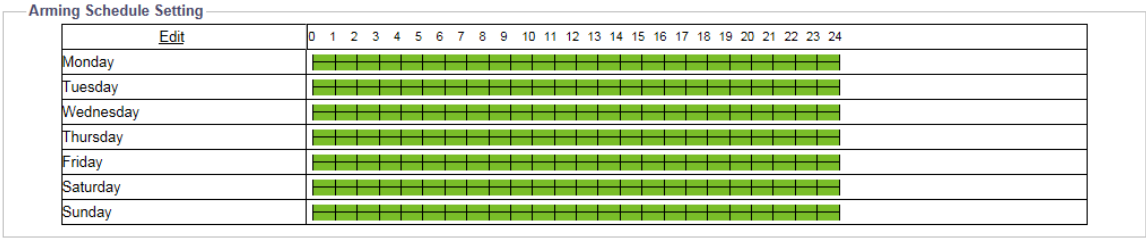


Figure: Arming Schedule Setting

After clicking "Edit", the prompt setting page will be shown as follows. User is able to individually establish up to 3 sets of time range 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. Take the screenshot below for example, we can clearly see that the 2 time ranges, Monday (08:00 – 24:00) and Tuesday (03:00 – 15:00), are properly defined and checked. And the above screenshot further 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.

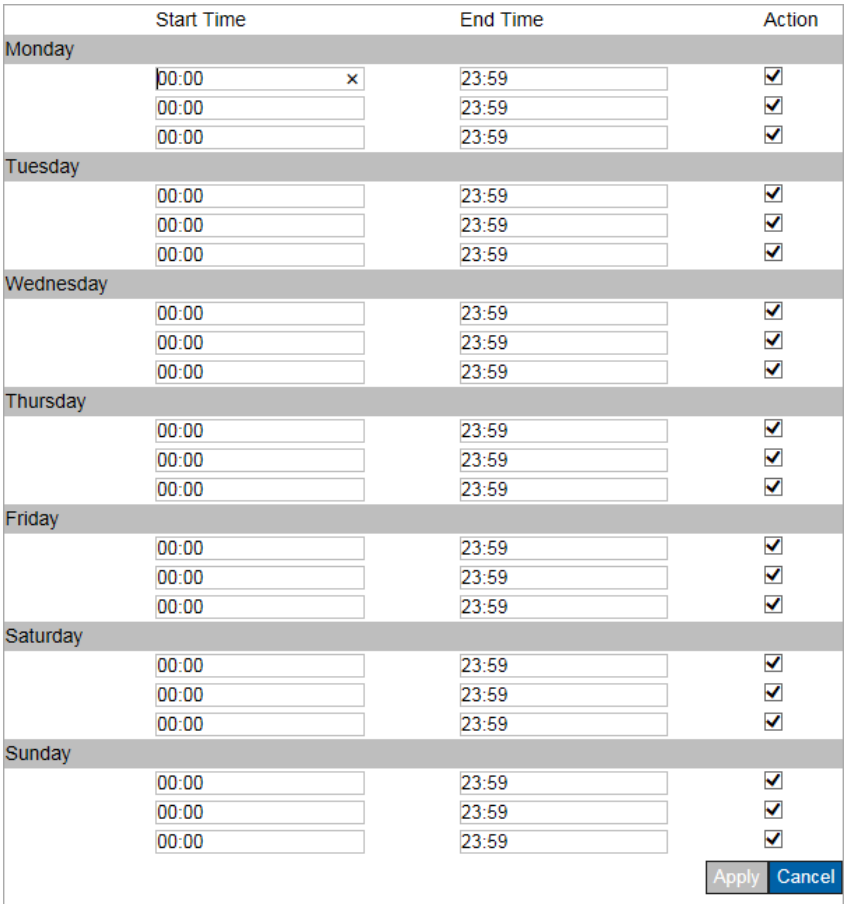


Figure: Arming Schedule Setting

9.1 Alarm

Connecting an alarm input device with the camera can largely extend alert functions. For example, when an infrared detector connected with the camera detects motion based on heat emission, an alarm input message will be sent to the camera. On the other hand, by connecting with an alarm output device such as siren, the camera will send signal to notify siren and thus make it activated 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.

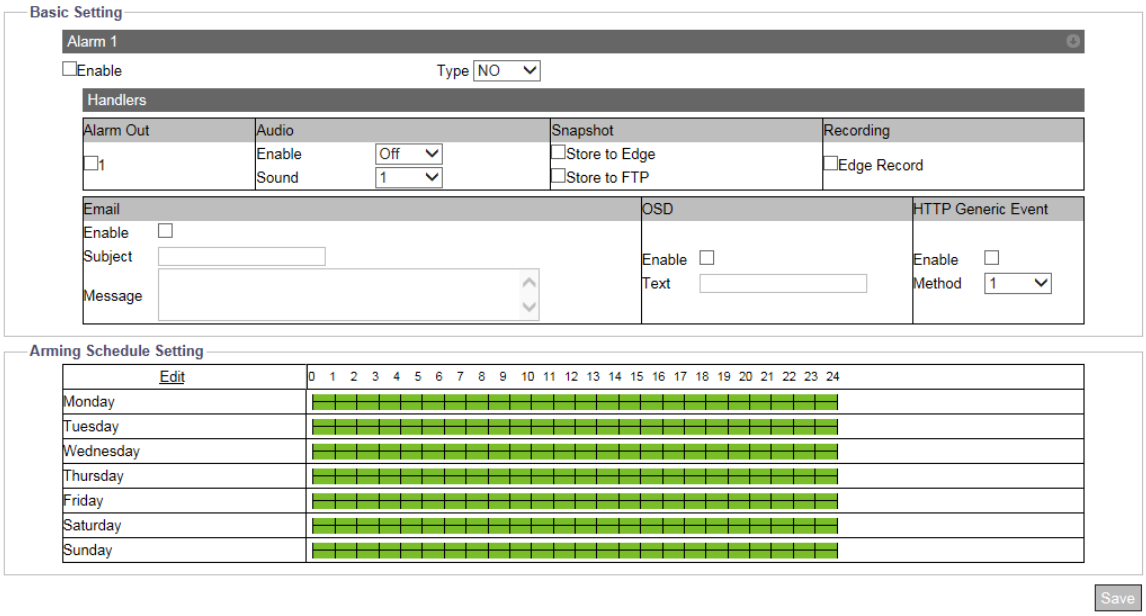


Figure: Alarm Event Settings

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.

9.2 Audio

By connecting with an audio input device, e.g., microphone, the camera can receive an audio input signal from the microphone, and react with the certain responses which are preset under this section. Check the information below for more understanding.

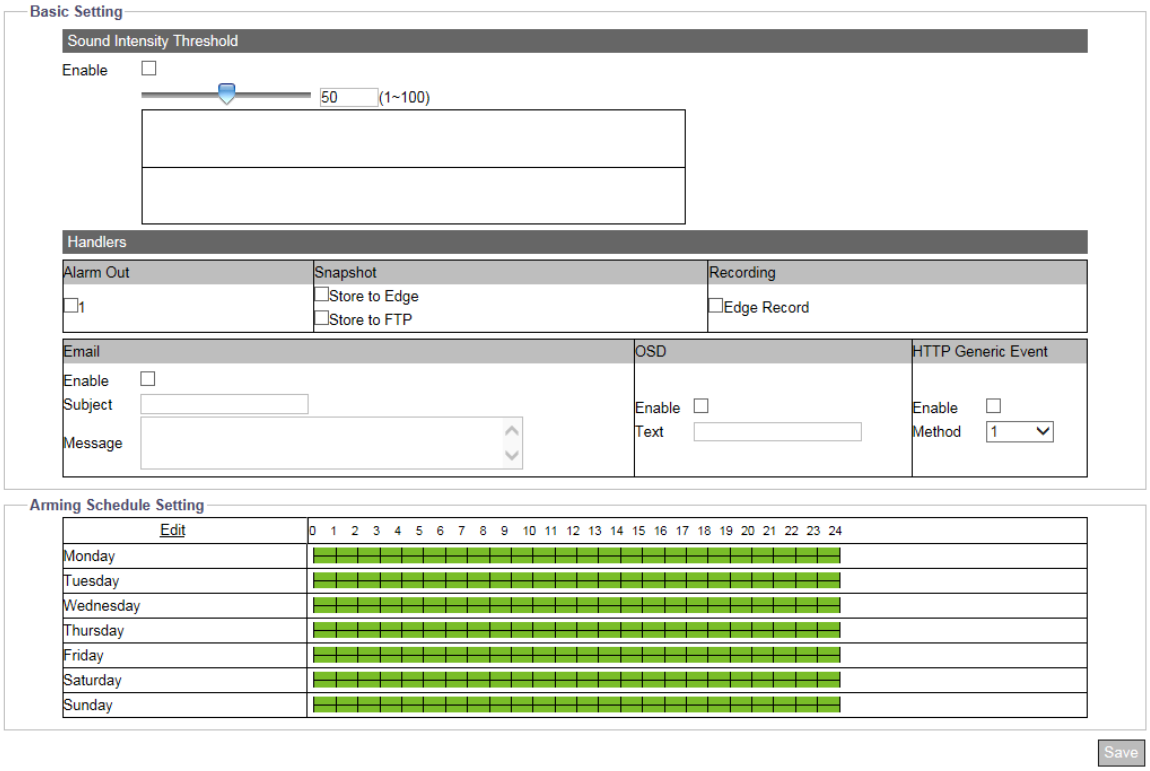


Figure: Audio Event Settings

Basic Setting

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

Sound Intensity Threshold : 1 ~ 100

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

9.3 Motion

This function is designed to establish related actions when the camera detects motion issues. A maximum of 4 sets of motion detection areas can be customized by users.

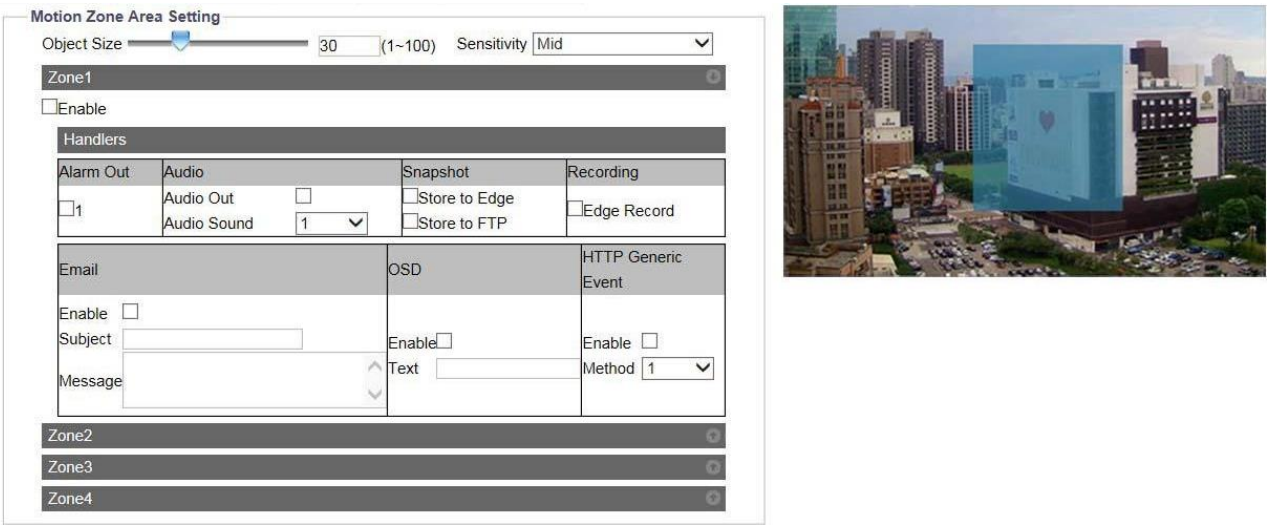


Figure: Motion Detection Settings

Motion Zone Area Setting

Object Size : 1 ~ 100

Lower the value, smaller the object that can be detected, and vice versa.

Sensitivity: High/ Mid/ Low

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.

Enable

Draw a desired size with position on the right-side preview image for motion detection followed by checking the box and clicking "Save" to have the settings take effect.

9.4 Network

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

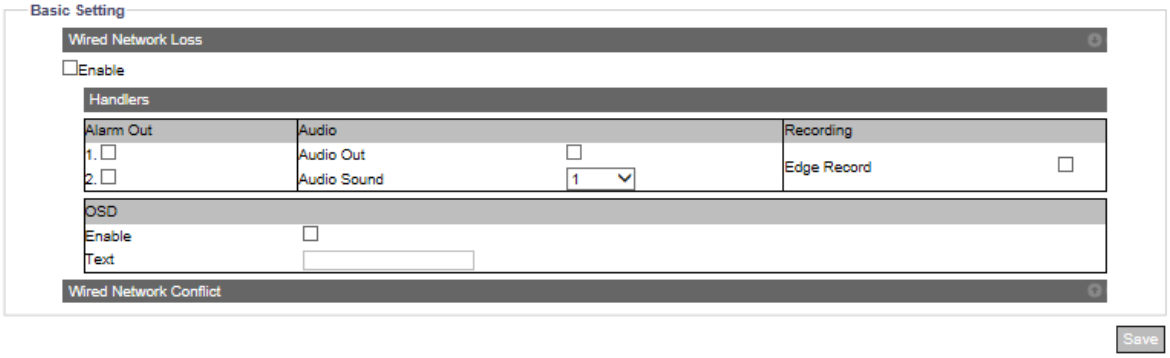


Figure: Network Event Settings

Basic Setting

- **Wired Network Loss**

Check the box to enable the detection of network lost. When the camera loses internet access, the network lost 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 conflicts 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.

9.5 Schedule

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

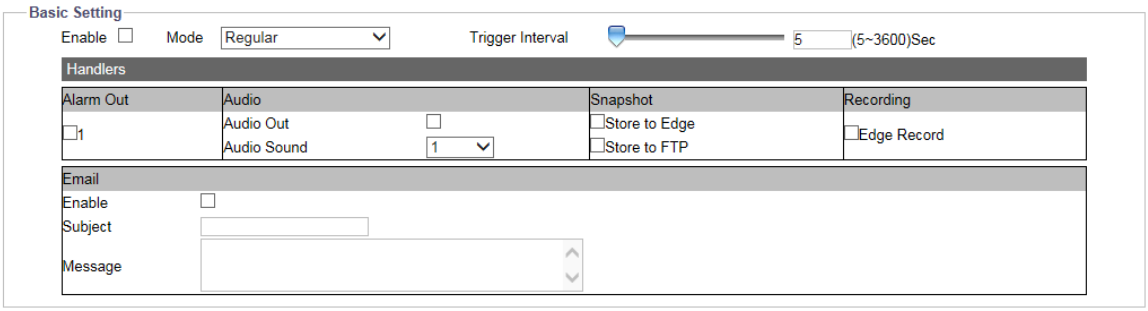


Figure: Recoding Schedule Settings

Basic Setting

Enable: Check the box to enable recording schedule function.

Mode : Regular/ Persistent

- Regular: It means that when enabled; the recording schedule will progress regularly based on the trigger interval settings.
- Persistent: When enabled, regardless of interval, the recording schedule will progress persistently.

Trigger Interval : 5 ~ 3600 (sec)

It's about interval pertaining to above "Regular" mode. For example, if "60", schedule under Regular mode triggers on 60 seconds per time.

9.6 Tamper

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

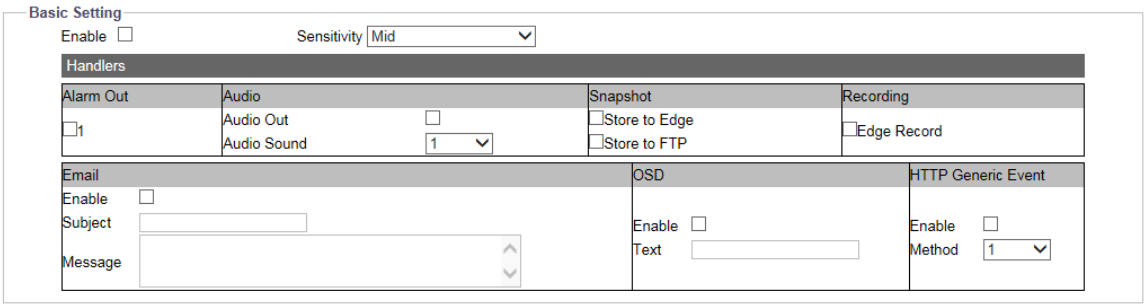


Figure: Tamper Detection Settings

Basic Setting

Enable: Check the box to enable tamper detection.

Sensitivity : High/ Mid/ Low

Set the sensitivity for tamper detection. High means that camera tends to be triggered with slight tamper issue, while Low means that camera is triggered with only major tamper issue.

9.7 mSD Healthiness

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

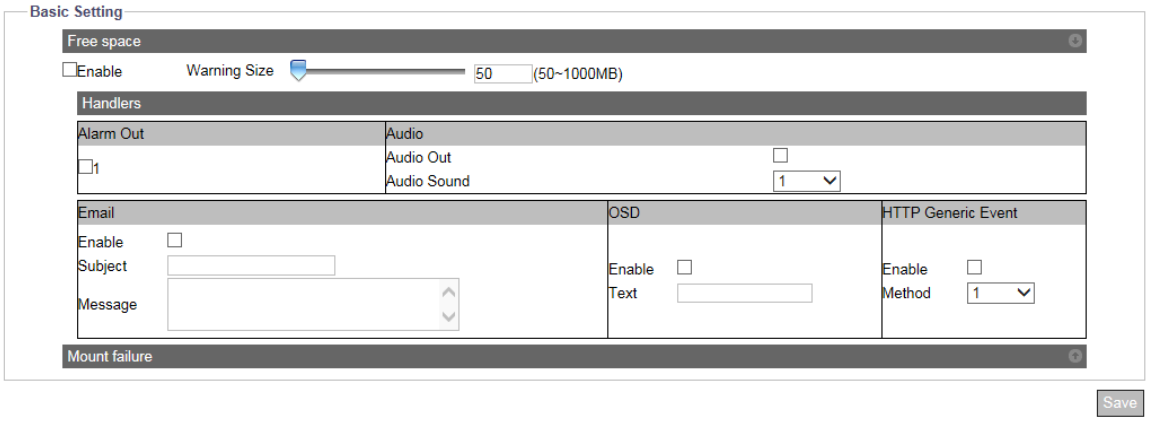


Figure: mSD Healthiness Settings

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".

10. Video Analytics

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 that helps administrator not need to keep staying in front of the monitor by recording only critical scenes where events happen to facilitate interoperability and largely reduce required recording storage for surveillance camera.

Video Analytics configurations are consisted of VA specific, Handler and Arming Schedule. Table below give the 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.	-	-	
Border Line	Set line 1~3 and direction.	V	V	
Loitering	Set area and trigger interval.	V	V	
Area Counting	Set area.	-	-	
Intrusion	Set area.	V	V	
Departure	Set area.	V	V	
Withdraw	Set object and trigger interval.	V	V	
Adverse Way	Set line and angle.	V	V	
Abandon	Set area and trigger interval.	V	V	

General

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

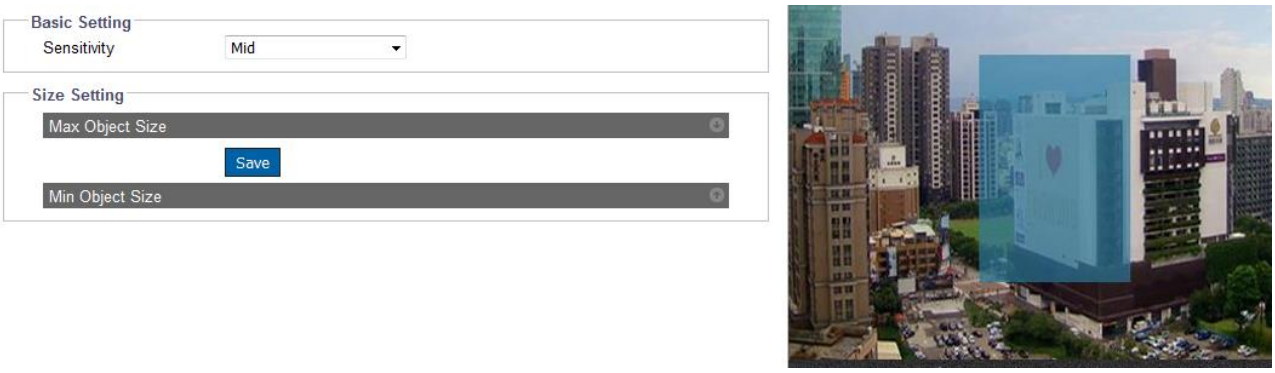


Figure: General Settings

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, whilst Low, on the other hand, stands for triggering occurs only when major events happen.

Size Settings

Max Object Size (REQ-VA-010)

Draw a desired maximum object size within the right-side preview window followed by clicking the "Save" to enable the settings. Any object larger than the maximum size defined here will neither be detected, nor triggered.

Min Object Size (REQ-VA-010)

Draw a desired minimum object size within the right-side preview window followed by clicking the "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 accord with desired objects to be detected. By doing so, the accuracy of VA functions will be escalated by a large scale.

Line Counting

This function is designed to count the moving objects that passed through the designated line defined by users. The ideal 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. (REQ-VA-002)

Figure: Line Counting Settings

Line Setting

Reference Border Line

Pressing this button will allow user to apply the identical line deployment settings referred from Border Line 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 (REQ-VA-011)

Press and hold on the right-side preview image to draw a line on the wanted area followed by clicking the "Save" button to have the settings take effect. Up to 3 lines can be assigned concurrently.

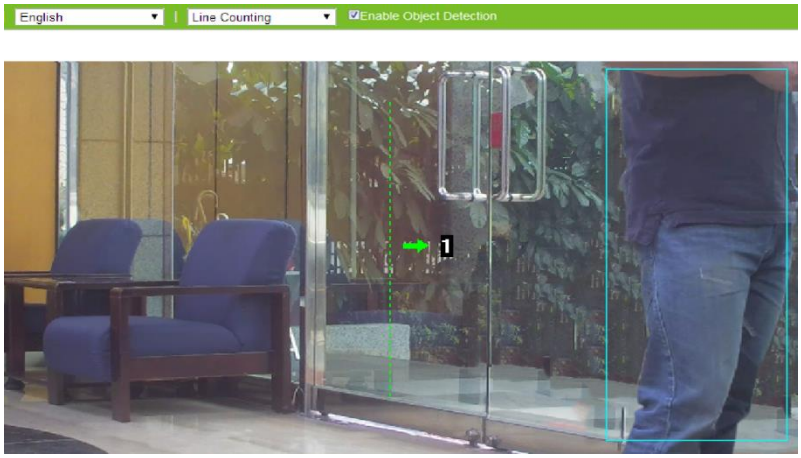


Figure: Line Counting Performance On Live View

Performance

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

Border Line

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 critical coffer is located to efficiently monitor any suspect person crossing the borderlines deployed. (REQ-VA-004)

Figure: Borderline 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 (REQ-VA-011)

Press and hold on the right-side preview image to draw a line on the wanted area followed by clicking the "Save" button to have the settings take effect. Up to 3 lines can be assigned concurrently.

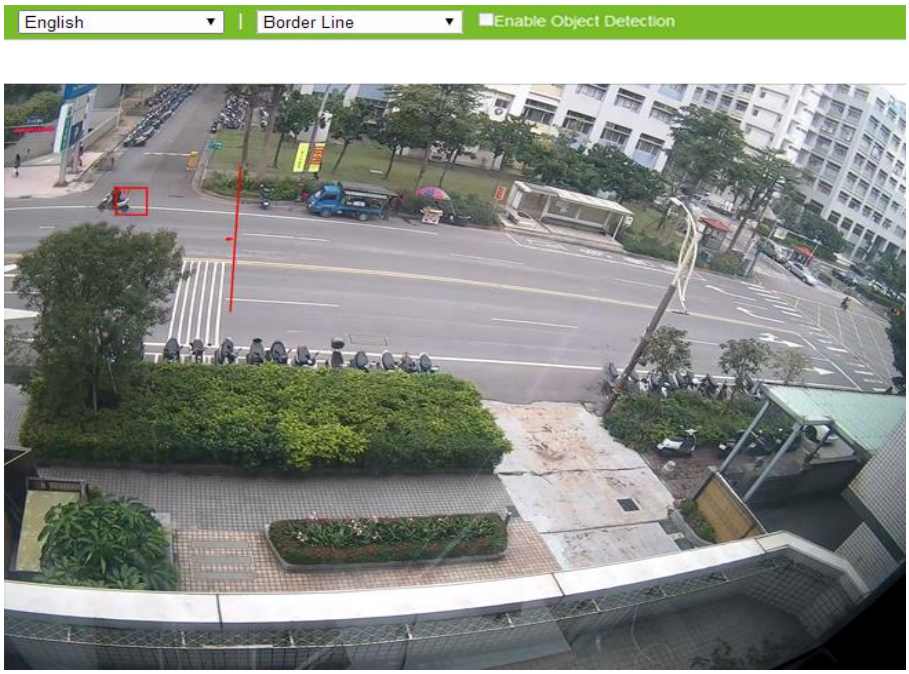


Figure: Border Line Performance On Live View

Performance

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

Loitering

This function is designed to intelligently keep an eye on suspect objects that enter and linger for a certain period within the alerted area defined by administrator. It is practical to monitor key zone without paying extra 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. (REQ-VA-001)

Trigger Interval : 5 ~ 300

Define a value for the threshold period to trigger loitering alarm by any suspect object that enter and linger the zone over the value.

Method (REQ-VA-012)

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

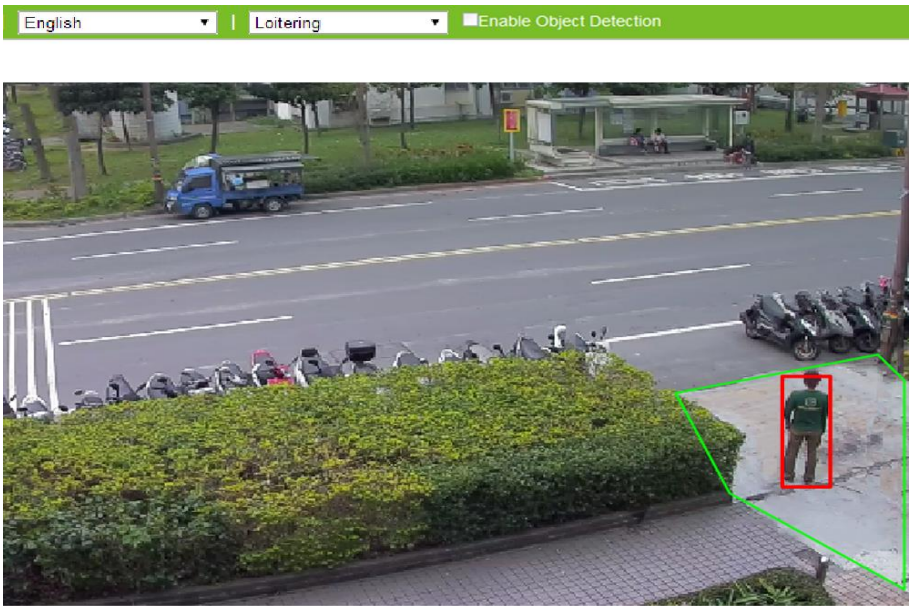


Figure: Loitering Performance On Live View

Performance

Switch to the Live View page and select "Loitering" from the lower-left VA dropdown menu. When

there's a moving object traveling into and lingering within the designated zone over a certain period of time defined by administrator as the above image, the rectangular frame enclosing the suspect object is highlighted with red color for distinctive identification. Besides, any moving object within the live view will be framed by a blue rectangle for clear recognition.

Area Counting

For some scenarios, e.g., parking lot, administrator may have the great intension to compile statistics of objects that get into or move off the location. By implementing the Area Counting function, administrator can grasp a well-knit statistics gathered by intelligent surveillance camera with ease.

Figure: Area Counting Settings

Basic Setting

Enable: Check the box to enable the area counting function. (REQ-VA-009)

Location X & Location Y : 1 ~ 10

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

Reference Departure Area & Reference Intrusion Area

Pressing the buttons will allow user to apply the identical area deployment settings referred from Departure Area and Intrusion Area functions individually, an easy way to prompt setup and implement.

Reset Counting

Pressing the button will erase the accumulated counting records.

Method (REQ-VA-012)

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

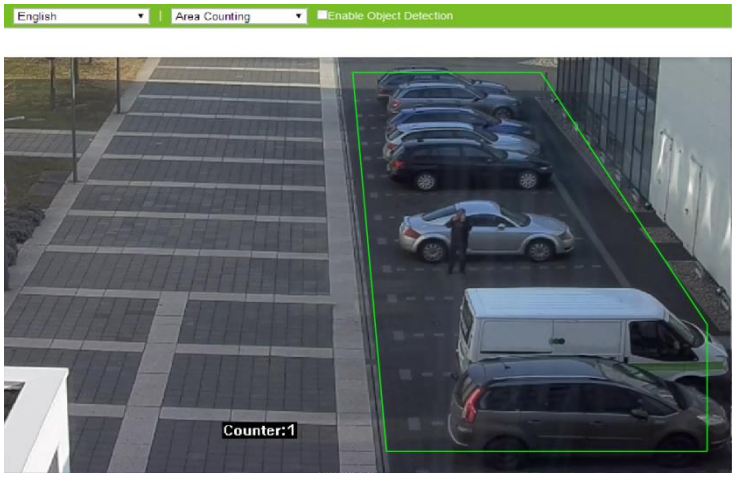


Figure: Area Counting Performance On Live View

Performance

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

Intrusion

Different from Border Line in partial ways, Intrusion is a function where administrator can assign an irregular shape (octagonal form at the maximum) to fence off any suspicious object from entering. In certain scenarios, administrator can effortlessly have a well command of critical zone and receive prompt warning once any object trespasses the defined critical zone in a real-time manner. (REQ-VA-003)

Figure: Intrusion Settings

Basic Setting

Enable: Check the box to enable the intrusion detecting function. (REQ-VA-003)

Reference Area Counting & Reference Departure Area

Pressing the buttons will allow user to apply the identical area deployment settings referred from Area Counting and Departure Area functions individually, an easy way to prompt setup and implement.

Method (REQ-VA-012)

Draw a desired shape (octagon at the maximum) covering the critical zone for intrusion detection followed clicking "Save" to have the settings take effect.

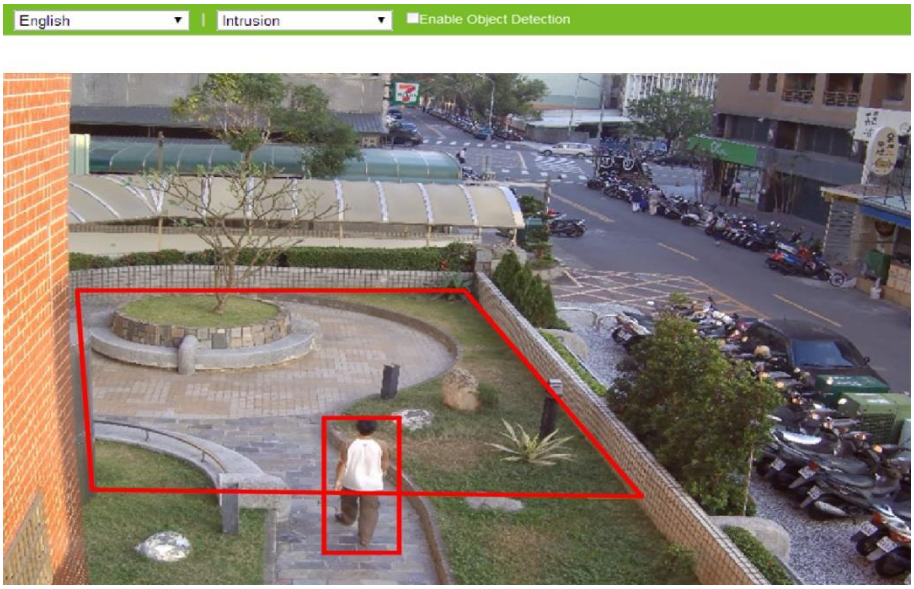


Figure: Intrusion Performance On Live View

Performance

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

Departure

As opposed to Intrusion function, Departure is implemented to have supervision on moving objects that overstep the predefined area. In certain scenarios, e.g., child care center, administrator is in great need of control on children within limited space. Departure, therefore, is the very answer, via intelligent monitor, to the application.

Figure: Departure Settings

Basic Setting

Enable: Check the box to enable the departure detecting function. (REQ-VA-007)

Reference Area Counting & Reference Intrusion Area

Pressing the buttons will allow user to apply the identical area deployment settings referred from Area Counting and Intrusion Area functions individually, an easy way to prompt setup and implement.

Method (REQ-VA-012)

Draw a desired shape (octagon at the maximum) covering the critical zone for departure detection followed clicking "Save" to have the settings take effect.

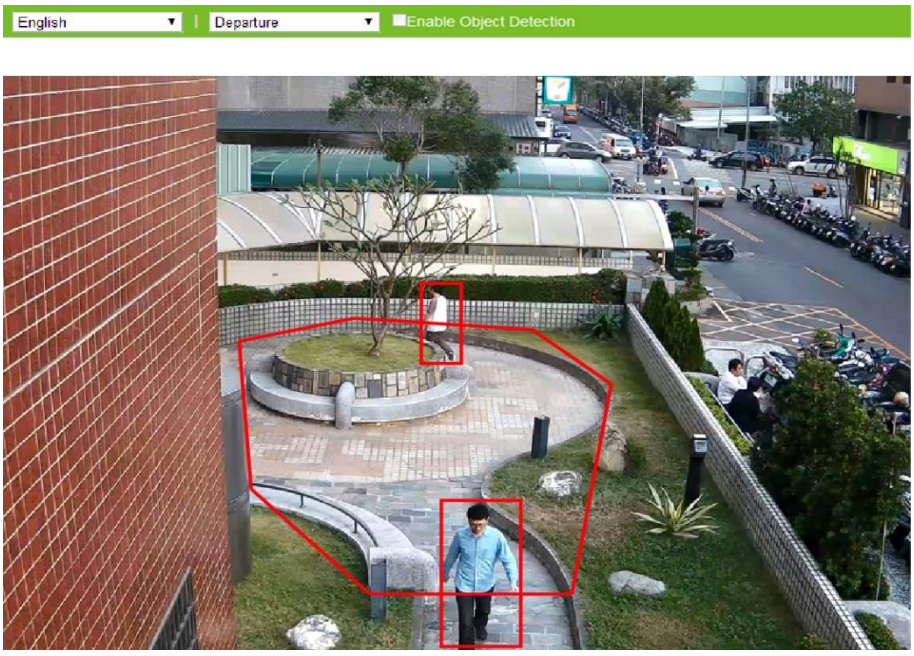


Figure: Departure Performance On Live View

Performance

Switch to the Live View page and select "Departure" from the lower-left VA dropdown menu. When there's a moving object overstepping the boundary of the designated critical zone defined by administrator as the above image, both the rectangular frame enclosing the moving object and the defined zone are highlighted with red color for distinctive identification. Besides, any moving object within the live view will be framed by a blue rectangle for clear recognition.

Withdrawn

For owner of jewelry store, the most vital thing is to secure each one of the jewelry, gem as well as gold ornament in an extremely safe manner. Withdrawn detection is thereby developed to meet the objectives which will guarantee valuable items that are marked with withdrawn settings are properly monitored and safeguarded.

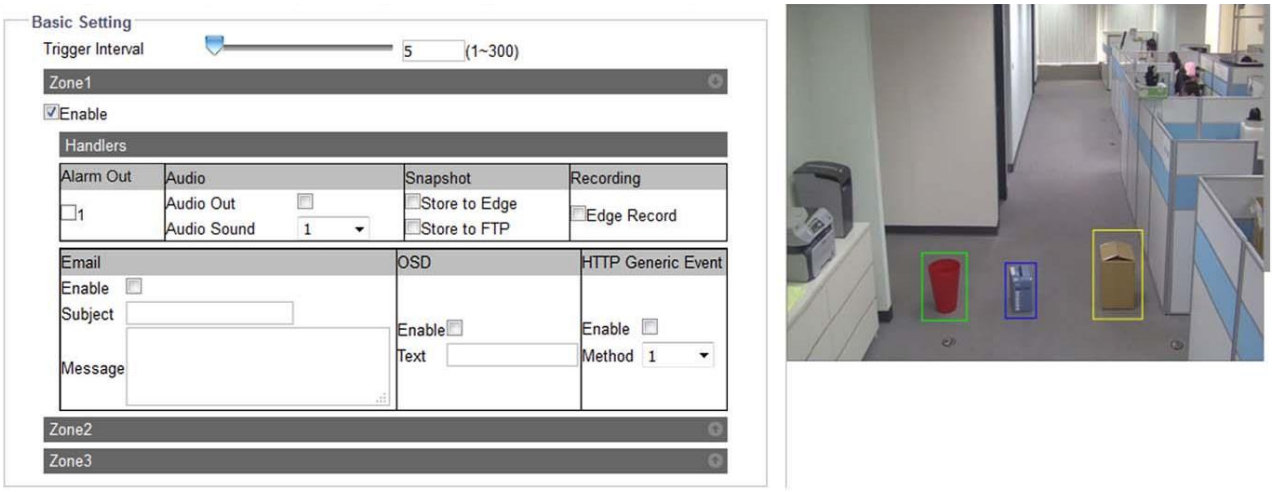


Figure: Withdrawn Settings

Basic Setting

Trigger Interval

Define an exact threshold of time period to trigger withdrawn detection.

Zone 1 ~ 3 (REQ-VA-008)

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 (REQ-VA-012)

Draw a desired rectangular zone covering the critical item for withdrawn detection followed clicking "Save" to have the settings take effect. Up to 3 zones can be set up in the meantime by varied color indications.

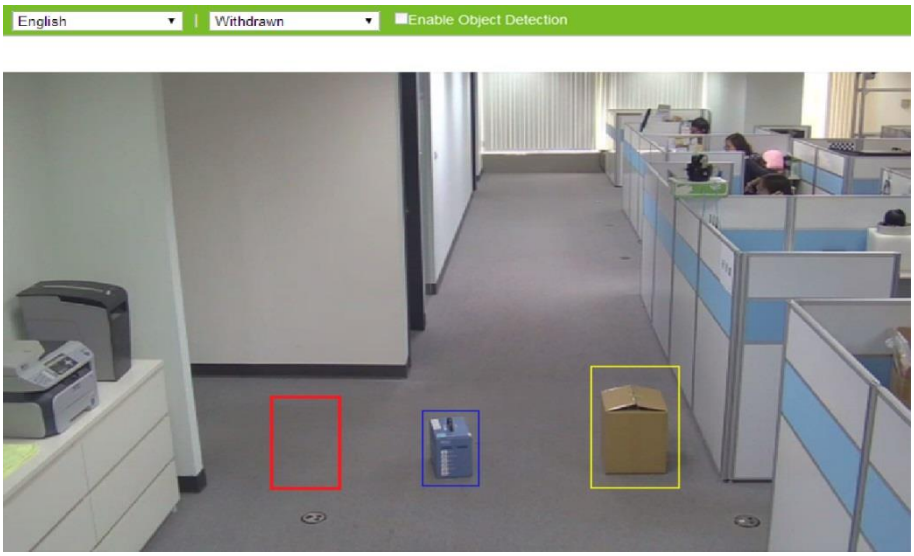


Figure: Withdrawn Performance On Live View

Performance

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

Adverse Way

Among intricate traffic thoroughfares in different cities, it is not uncommon to see some one-way streets arrangement. For transportation bureau accountable for public traffic flows, the Adverse Way function is able to help control some vehicles that may violate regulations for one-way street in a particularly intelligent manner.

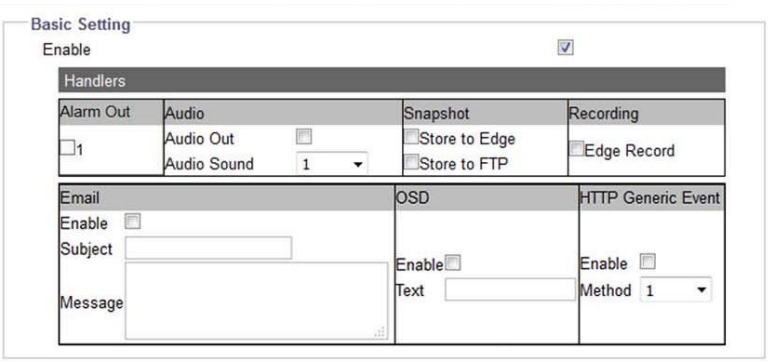


Figure: Adverse Way Settings

Basic Setting

Enable: Check the box to enable the adverse detecting function. (REQ-VA-005)

Method (REQ-VA-011)

Press and hold the mouse to draw a green linear on targeted area, and the blue included angle, in the proximity of the green linear, 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 adverse way

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.

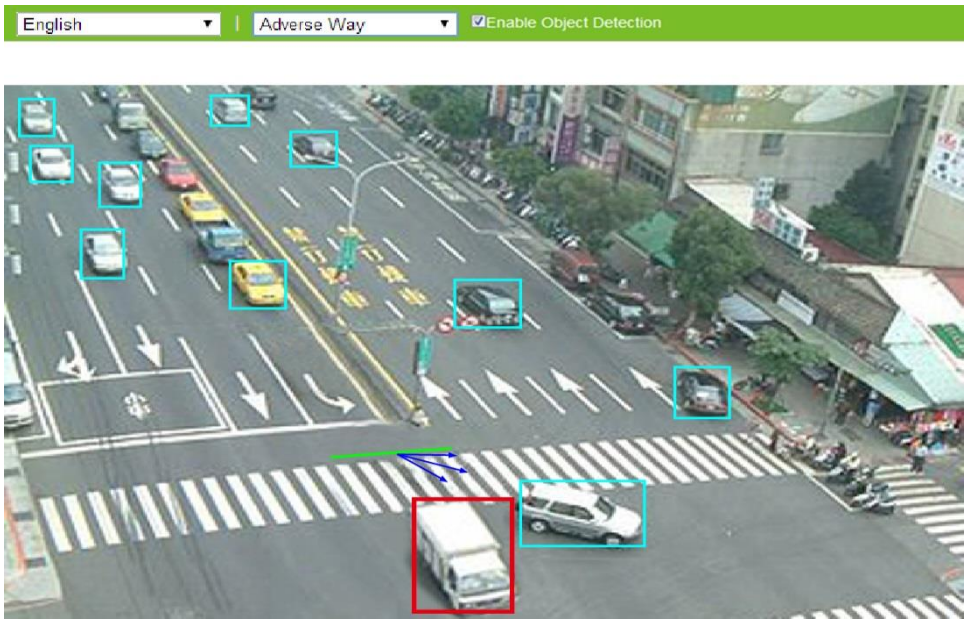


Figure: Adverse Way Performance On Live View

Performance

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

Abandon

Terrorist attack has prevailed around the world and claimed thousands of lives so far. As an intelligent surveillance camera, the wisely detected function "Abandon" is therefore specifically designed for preventing terror-like events in a precautious manner. Any object deposited intentionally within some critical places, e.g., entrance of building or subway station hall, by deliberate person can be intelligently detected and determined as a suspicious abandoned object.

Figure: Abandon Settings

Basic Setting

Enable: Check the box to enable the abandon detecting function. (REQ-VA-006)

Trigger Interval : 5 ~ 300

Define a value for the threshold period to trigger abandon alarm by any suspect object that was left within the zone over the value.

Method (REQ-VA-012)

Draw a desired shape (octagon at the maximum) covering the key zone for abandon detection followed clicking "Save" to have the settings take effect.

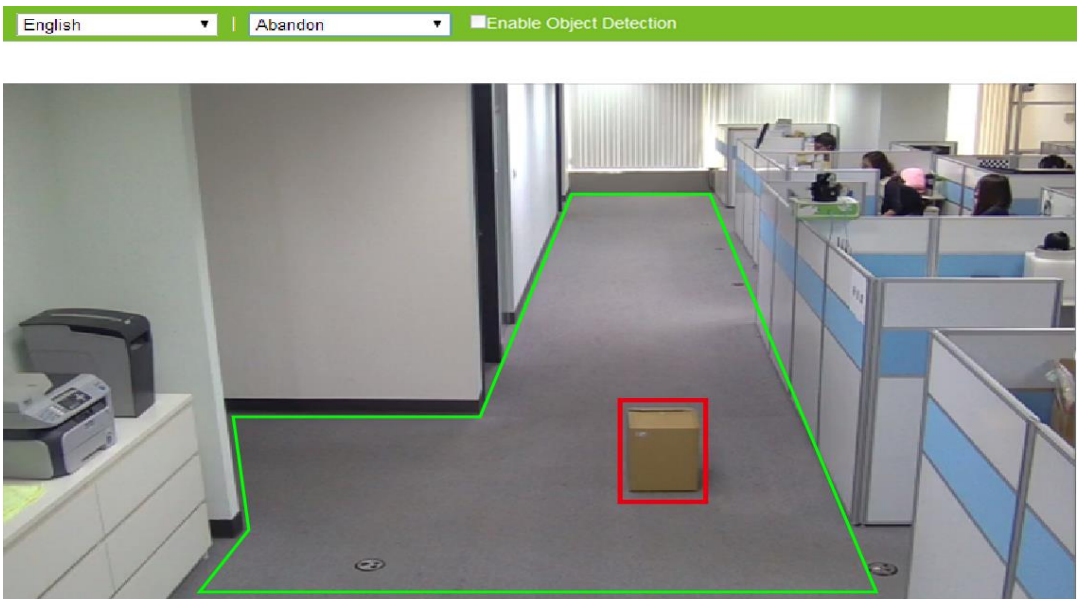


Figure: Abandon Performance On Live View

Performance

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

11. Event Setting

11.1 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.

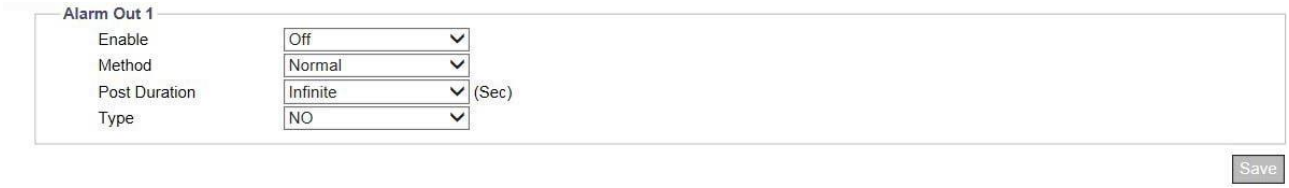


Figure: Alarm Output Settings

Alarm Out

Enable : Select "On" to activate this function.

Note	• The available number of alarm output will vary by different model, please check "Appendix: Product Comparison-I/O Port" for details.

Method : Pulse/ Normal

There are 2 methods to proceed with alarm output as follows.

- Normal: It's the standard method to execute alarm output function where user can define a period of duration from options within dropdown menu of Post Duration.

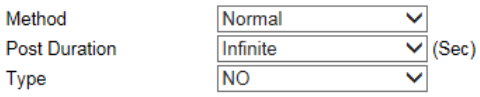


Figure: Normal Method Settings

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

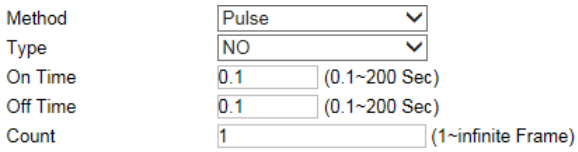


Figure: Pulse Method Settings

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

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

Type: NO/ NC

Define which type to be adopted 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 under only Pulse method.

Off Time : 0.1 ~ 200 (sec)

Define a specific interval for each alarm output triggering under only Pulse method.

Count : 1 ~ Infinite

Define how many counts will be performed for alarm output.

11.2 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.

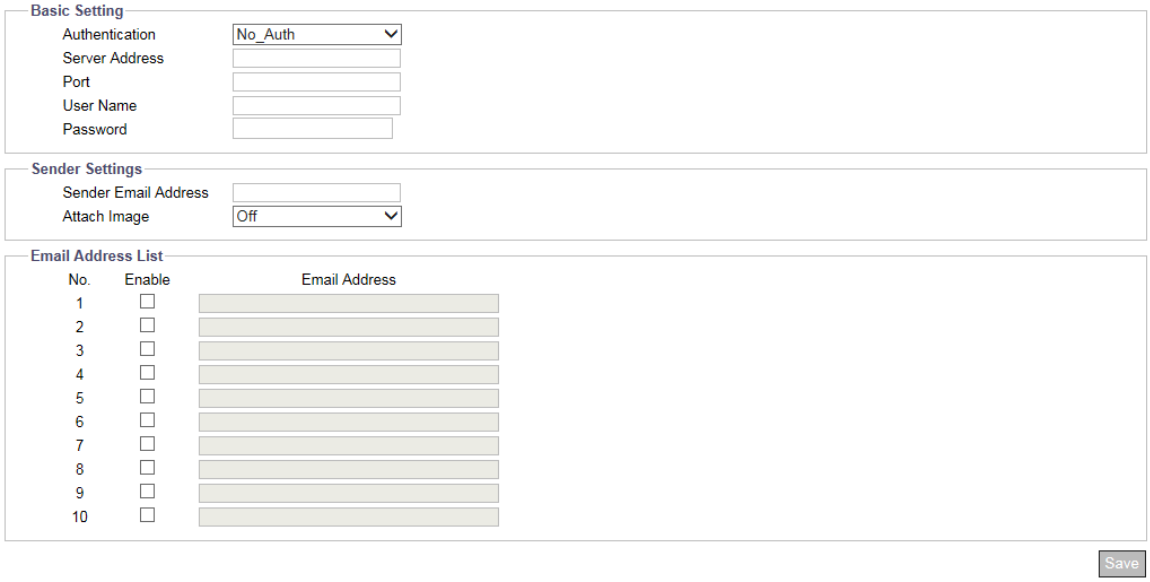


Figure: Email Settings

Basic Setting

Authentication: No_Auth/ SMTP_Plain/ Login/ TSL-TTLS

Select an authentication type as following details:

- 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. Ask technician for details if necessary.

User Name

Input a username with privilege to access the server.

Password

Input the password associated with the username.

Sender Settings

Sender Email Address

Define the sender email address into the field.

Attach Image : On/ Off

Select "On" to enable attaching the detected image of events to the sending email.

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. There're maximum 10 email addresses can be defined here.

11.3 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 a FTP server address.

Port : 1025 ~ 65535

Set "21" as default or change to dedicated number. Ask technician for details if necessary.

Username

Input a username with privilege to access the server.

Password

Input the password associated with the username.

Mode : Active/ Passive

Decide which connection mode to be utilized as the following details:

- Active: The camera will keep reconnecting with the designated FTP site when selecting "Active", which occupies more network bandwidth but with instant response to FTP.
- Passive: By selecting this option, the camera will only connect with the designated FTP site when necessary, which largely help save the network bandwidth.

11.4 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.

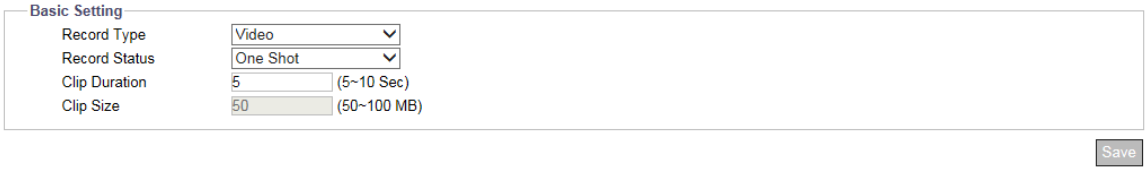


Figure: Record Settings

Basic Setting

Record Type: Audio and Video/ Video

Choose which record type to be adopted:

- 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

Choose type of video codec.

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

11.5 SD Card

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

Figure: SD Card Settings

Basic Setting

Overwrite : On/ Off

Means that recorded files will be overwritten when SD card is in full capacity. Basically, the recording program will erase the earliest file and store another new one file when the remaining capacity of mounted SD card is below 20MB. Select ON to enable this function.

Status

It shows status about if SD card is inserted and well mounted.

SD Format

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

11.6 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 a 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 a number of frames to be captured after an event occurred.

11.7 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.

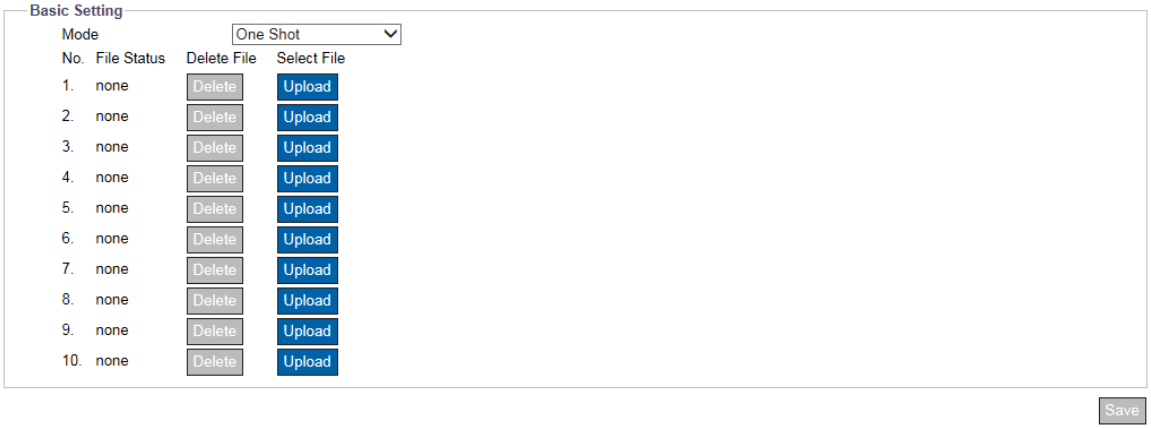


Figure: Sound Settings

Basic Setting

Mode : One Shot/ Infinite

- One Shot: The sound of audio out will be played for only 1 time.
- Infinite: As opposed to One Shot, "Infinite" keeps the sound playing infinitely.

No.

The numerical order list of each sound file.

File Status

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

Select File

Click the "Upload" 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.

11.8 HTTP Generic Event

HTTP Generic Event can help user to 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 the type of method for the trigger event.

Title

Preset the title of messages.

URL

Input the web address of NVR. Please follow the user manual of NVR for the detail of 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 more complex way to transmit messages but it is also a little safer than Get.

User Name

Enter a designated username for authentication to the accessed NVR.

Password

Enter the password corresponding to the inputted 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.

Appendix: Product Comparison

Model Type	LPR
	SN-IPR56/20AKDN
Video Compression	Enhanced H.264
	Motion JPEG
Max Resolution & Frame Rate	3Mp at 60/50fps
Lens Control	Motorized lens
	Easy for AF Adjustment
Day & Night	True D/N (ICR)
IR Control	Smart IR, Adaptive IR
I/O Port	Audio 1/1 Alarm 1/1
Event Trigger	Schedule, Motion, Tampering, Network Loss Detection, Audio Intensity Detection, Alarm Input, mSD healthiness
Event Actions	E-mail Notification, FTP Recording, SD Card Recording, OSD Indication, Sound Playback, Alarm out Http Generic Event
Storage	Micro SDHC/SDXC slot
Internet Security	HTTPS, IEEE 802.1X, digest authentication,
	IP filtering, Advanced Security
RS485 Interface	-
ABF Control	-
Value Added	Digital WDR, 3DNR, Mirror

Note: Product specifications and pictures are subject to change without prior notice.

Notices

This manual is intended for administrators and users of
network camera, and applicable firmware is specified in the cover page.
It includes instructions for using and managing the camera on your network.
Previous experience in networking will be of useful when using this product.
The network camera supports ONVIF profile S, profile G, profile Q.
For more information about ONVIF go to www.onvif.org