User Guide

MOBOTIX 5MP Vandal Bullet Analytics Camera

© 2021 MOBOTIX AG

MOBOTIX EverClear

HEVCAdvance™

BeyondHumanVision

MOBOTIX MOVE

V1.02_11/30/2021, Order Code: Mx-VB2A-5-IR-VA

Table of Contents

Table of Contents **2**

Before You Start **5**
- Support 6
- Safety Notes 6
- Legal Notes 7

Overview **9**
- About the Camera 10
- Features 10
- Package Contents 11
- Dimensions 12
- microSD Card Slot/Factory Default Button 12

Connecting and Installing **15**
- Camera Cabling 16
- All-in-One Cable 16
- Connect Power 17
- Connect Ethernet Cable 17
- Connect Alarm I/O 18
- Waterproof Cable Connectors 18

Installation **19**
- General Remarks 20
- Ceiling/Wall Mounting 20

Configuration **23**
- System Requirements 24
- Accessing the Camera 24
- Setup Video Resolution 26
- Exporting/Importing Configuration Files 27

Menu Reference **29**
- Overview 30
- The Camera Menu 30
- The “Home” Tab 30
  - Function Items on Home Page 31
- The “System” Tab 33
  - System 34
  - Security 35
  - Network 41
  - DDNS 48
  - Mail 48

FTP 49
HTTP 49
MxMessageSystem 49
Events (Alarm Settings) 51
Storage Management 79
Recording 82
Schedule 83
File Location (Snapshots and Web Recording) 84
View Information 84
Factory Default 85
Software Version 86
Software Upgrade 86
Maintenance 87
The “Streaming” Tab 87
Video Configuration 88
Video Rotation 90
Video Text Overlay 90
Video ROI 91
Video ROI Encoding 92
Video OCX Protocol 92
Video Mask 93
Audio (Audio Mode and Bit Rate Settings) 93
The “Camera” Tab 94
Exposure 95
White Balance 96
Picture Adjustment 99
IR Function 100
Noise Reduction 101
WDR Function 102
Digital Zoom 102
Backlight 102
Profile 102
TV System 103
The “Logout” Tab 104
Appendix A: Installing UPnP Components 104
Appendix B: Converting IP Addresses from Decimal to Binary 104

Technical Support Information 107
Setup Internet Security 108

Technical Specifications 109

1

Before You Start

This section contains the following information:

Support 6

Safety Notes 6

Legal Notes 7

Support

If you need technical support, please contact your MOBOTIX dealer. If your dealer cannot help you, he will contact the support channel to get an answer for you as quickly as possible.

If you have internet access, you can open the MOBOTIX help desk to find additional information and software updates. Please visit:

www.mobotix.com > Support > Help Desk

Safety Notes

- This product must not be used in locations exposed to the dangers of explosion.
- Electrical systems and equipment may only be installed, modified and maintained by a qualified electrician or under the direction and supervision of a qualified electrician in accordance with the applicable electrical guidelines. Make sure to properly set up all electrical connections.
- Make sure to install this product in a well-ventilated spot and do not close off any vent openings.
- Do not use this product in a dusty environment.
- Protect this product from moisture or water entering the housing.
- Make sure that you install this product as outlined in this document. A faulty installation can damage the product!
- Do not replace batteries of the product. Batteries can explode if they are replaced by an incorrect type.
- This equipment is not suitable for use in locations where children are likely to be present.
- If using a Class I adapter, the power cord shall be connected to a socket-outlet with proper ground connection.
- To comply with the requirements of EN 50130-4 regarding the power supply of alarm systems for 24/7 operation, it is highly recommended to use an uninterruptible power supply (UPS) for powering the product.
- This equipment is to be connected only to PoE networks without routing to other networks.

Legal Notes

Legal Aspects of Video and Sound Recording

You must comply with all data protection regulations for video and sound monitoring when using MOBOTIX AG products. Depending on national laws and the installation location of the cameras, the recording of video and sound data may be subject to special documentation or it may be prohibited. All users of MOBOTIX products are therefore required to familiarize themselves with all applicable regulations and to comply with these laws. MOBOTIX AG is not liable for any illegal use of its products.

Declaration of Conformity

The products of MOBOTIX AG are certified according to the applicable regulations of the EC and other countries. You can find the declarations of conformity for the products of MOBOTIX AG on www.mobotix.com under **Support > Download Center > Certificates & Declarations of Conformity**.

RoHS Declaration

The products of MOBOTIX AG are in full compliance with European Unions Restrictions of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment (RoHS Directive 2011/65/EC) as far as they are subject to these regulations (for the RoHS Declaration of MOBOTIX, please see www.mobotix.com, **Support > Download Center > Documentation > Brochures & Guides > Certificates**).

Disposal

Electrical and electronic products contain many valuable materials. For this reason, we recommend that you dispose of MOBOTIX products at the end of their service life in accordance with all legal requirements and regulations (or deposit these products at a municipal collection center). MOBOTIX products must not be disposed of in household waste! If the product contains a battery, please dispose of the battery separately (the corresponding product manuals contain specific directions if the product contains a battery).

Disclaimer

MOBOTIX AG does not assume any responsibility for damages, which are the result of improper use or failure to comply to the manuals or the applicable rules and regulations. Our General Terms and Conditions apply. You can download the current version of the **General Terms and Conditions** from our website at www.mobotix.com by clicking on the corresponding link at the bottom of every page.

2

Overview

This section contains the following information:

About the Camera **10**

Features **10**

Package Contents **11**

Dimensions **12**

microSD Card Slot/Factory Default Button **12**

About the Camera

The Vandal Analytics Series is capable of supporting up to WDR Vandal Analytics @30 fps/720p @30 fps (WDR off Vandal Analytics @ 60 fps/720p @60 fps) video streaming. Moreover, combined with the latest WDR technology and low-light technology, the Vandal Analytics Series is able to deliver high quality images in the dark, low light condition.

The camera is designed to withstand ever-changing outdoor environment and is compliant with IP66 & IK10 standard. It is equipped with IR LED with an effective distance of up to 40 meters to ensure its usability under poor lighting condition. The camera operating temperature ranges from –55 to 60 °C/–41 to 140 °F with activated heater.

To make use of the camera's advanced video analytics capabilities, please consult the *Introduction to Video Analytics with MOBOTIXMOVE Cameras* manual available on **www.mobotix.com > Support > Download Center > Marketing & Documentation > Manuals**.

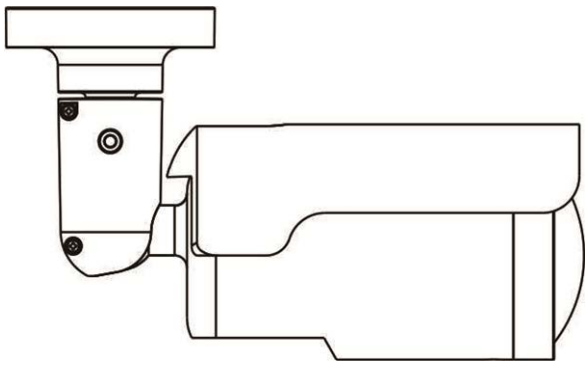
Features

- Multiple Progressive Scan CMOS Sensor Support of up to 2720x1976 (5MP) px resolution
- Multi Exposure Line-Interleaved WDR
- Multi Codec Support (H.265/H.264/MJPEG)
- Low Latency Streaming
- Quad Streams Support
- True Day/Night Function (ICR)
- IR LED (Working Distance up to 40 m)
- 3D Motion Compensated Noise Reduction (MCTF)
- Smart Event Functions:
  - External Input/Motion Detection/Network Failure Detection
  - Tampering Alarm/Periodical Event/Manual Trigger/Audio Detection
- Text Overlay and Privacy Masks
- Micro SD/ SDHC/ SDXC Card Support
- ONVIF Profile S/G/T Support
- Smart Low Bitrate Control
- Weatherproof (IP66)
- Vandal Proof (IK10 Rating)

Package Contents

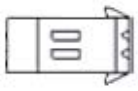
Check the package for the items listed below.

- Quick Installation
- Vandal Analytics H.265 Vandal Bullet IP Camera (cable included)



- 5-Pin Alarm Terminal Block

- 2-Pin Power Terminal Block



- Plastic Dowel (x5)

- M5 Standard Screw (x1)

- M4 Self-Tapping Screw (x5)

- Security Torx Key

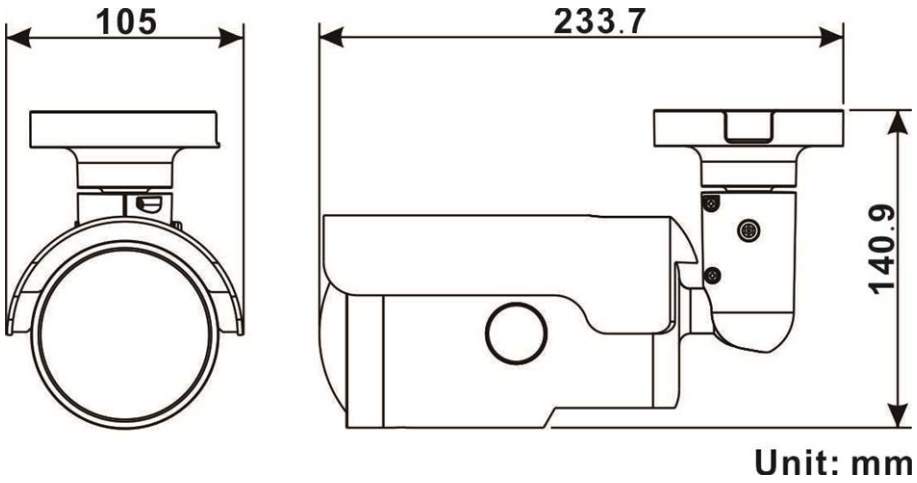
NOTE!
To use an external power supply, contact the camera manufacturer to confirm that the power supply complies with the LPS requirements and shares the same power specifications with the camera.

NOTE!
The supplied self-tapping screws are for soft substances/materials such as wood. For other installation environments such as cement wall, users MUST pre-drill and use plastic anchors before fastening the supplied self-tapping screws on the wall.

CAUTION!
Do not replace batteries of the camera. Risk of explosion may occur if the battery is replaced by an incorrect type.

Dimensions

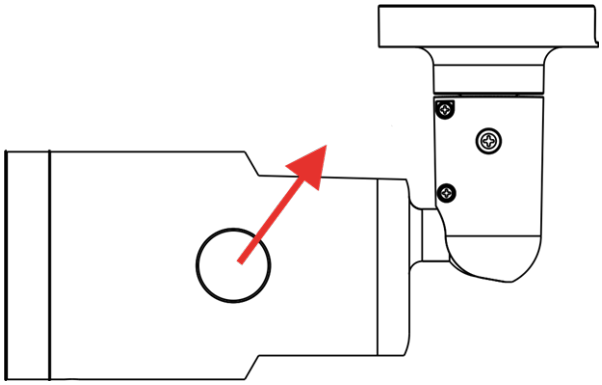
The dimensions of the camera are shown below.



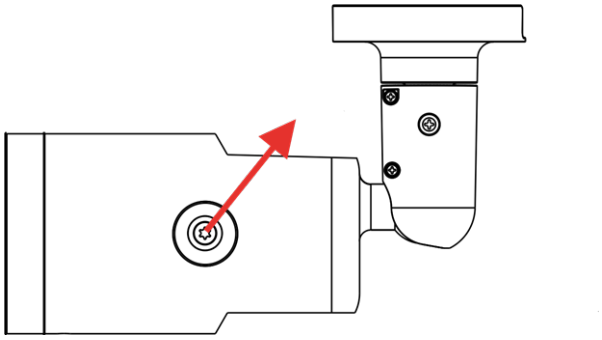
microSD Card Slot/Factory Default Button

The camera's microSD card slot and factory default button are inside the front housing. If users need to use them, the front housing must be opened. Follow the steps below to reach microSD card slot and factory default button.

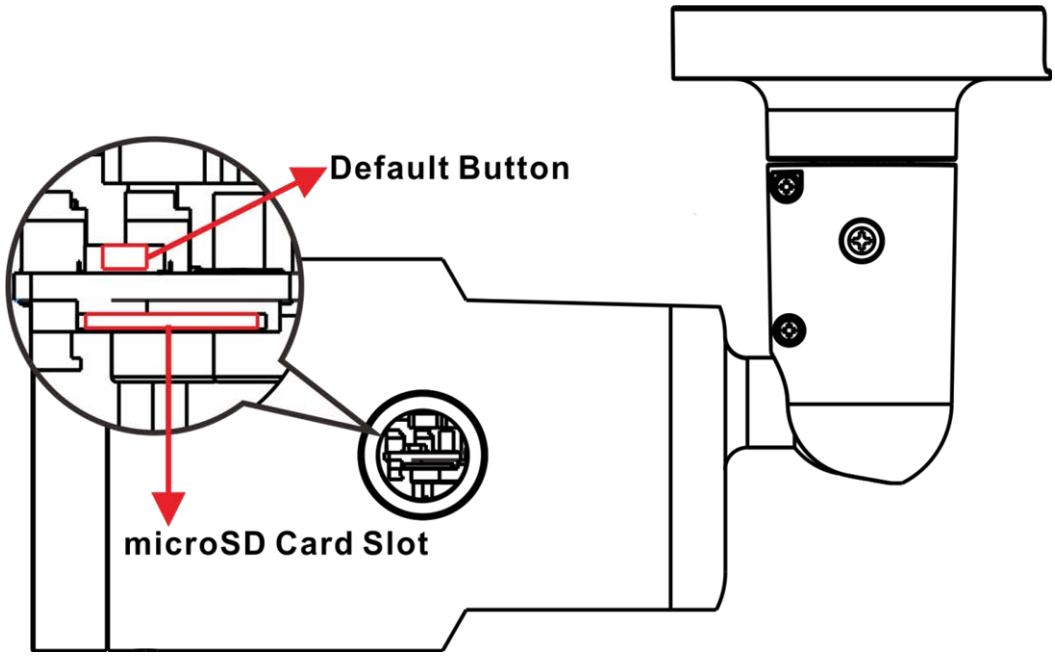
1. Open up the external cover using a flathead screwdriver.



2. Open up the internal cover using a security torx.



3. The positions of microSD card slot and default button are as shown.



NOTE!
It is not recommended to record with the microSD card for 24/7 continuously, as it may not be able to support long term continuous data read/write. Please contact the manufacturer of the microSD card for information regarding the reliability and life expectancy.

3

Connecting and Installing

This section contains the following information:

Camera Cabling **16**

All-in-One Cable **16**

Connect Power **17**

Connect Ethernet Cable **17**

Connect Alarm I/O **18**

Waterproof Cable Connectors **18**

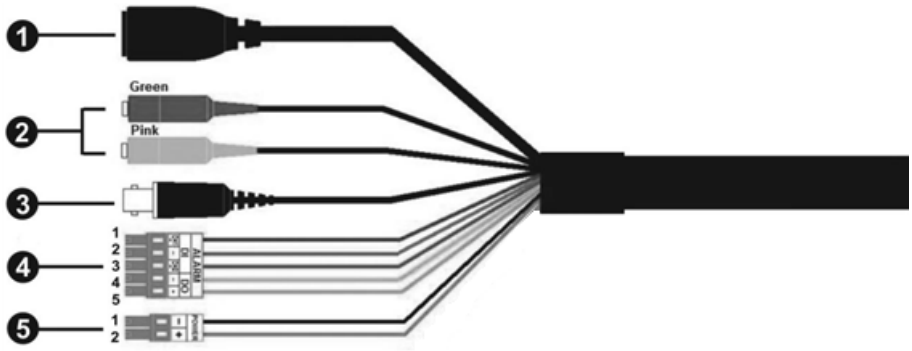
Camera Cabling

Before users connect cables, make sure that all cables and the power adapter are placed in dry and well-waterproofed environments, e.g. waterproof boxes. The purpose is to prevent moisture accumulation inside the camera and moisture penetration into cables, which might lead to camera breakdown. Please refer to the following sections to complete camera connection.

NOTE! This camera must be installed by qualified personnel and the installation should conform to all local codes.

All-in-One Cable

The diagram below shows the All-in-One cable of the camera. Definition for each cable is also given as follows.



No	Cable	Pin	Definition	Remarks
1	RJ-45	–	For network and PoE connections	
2	Audio I/O	Green	Audio Out / Mic Out (Line Out)	Two-way audio transmission
		Pink	Audio In / Mic In (Line In)	
3	BNC	–	For analog video output	

No	Cable	Pin	Definition		Remarks
4	Alarm I/O (5-pin Terminal Block)	1	Alarm In 2+		Alarm connection Do **NOT** connect external power supply to the alarm I/O connector of the IP camera!
		2	Alarm In -		
		3	Alarm In 1+		
		4	Alarm Out -		
		5	Alarm Out +		
5	Power (DC 12V / AC 24V) (2-pin Terminal Block)	1	DC 12V –	AC 24V 1	Power connection
		2	DC 12V +	AC 24V 2	

Connect Power

Use a DC 12V/AC 24V adapter and connect it to the 2-pin terminal block of the All-in-One cable and the power outlet. Alternatively, connect the Ethernet cable to the RJ-45 connector of the All-in-One cable, and plug the other end of the cable to a suitable Power Sourcing Equipment (PSE)/Power over Ethernet (PoE) switch.

NOTE! If PoE is used, make sure PSE is in use in the network.

Connect Ethernet Cable

To have the best transmission quality, cable length shall not exceed 100 meters. Connect one end of the Ethernet cable to the RJ-45 connector of the All-in-One cable, and plug the other end of the cable to the network switch or PC.

NOTE! In some cases, Ethernet crossover cable might be needed when connecting the camera directly to the PC.

Check the status of the link indicator and the activity indicator LEDs. If the LEDs are unlit, check the LAN connection.

- Green Link Light indicates good network connection.
- Orange Activity Light flashes for network activity indication.

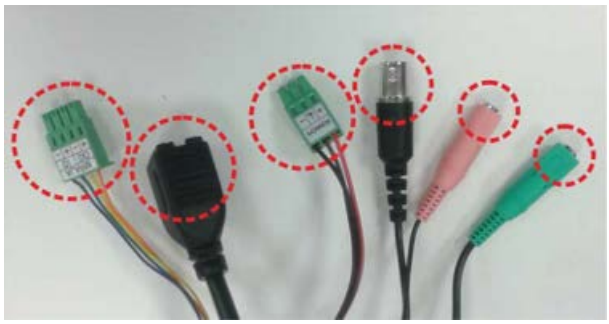
Connect Alarm I/O

For alarm I/O connection, please connect alarm devices to the 5-pin terminal block of the All-in-One cable.

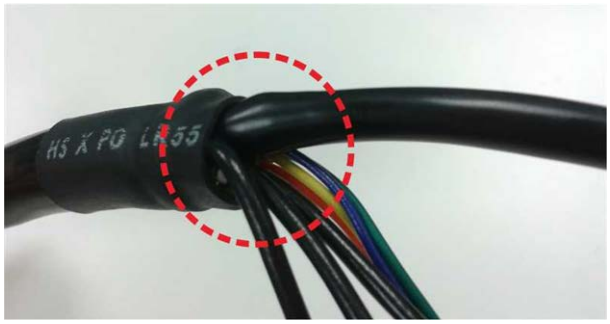
Waterproof Cable Connectors

Follow the steps below to waterproof the connectors of the All-in-One cable.

1. Connect the required devices to the All-in-One cable and coat the joints with silicone gel. There should be no gap between the connectors and the cables. For alarm I/O connector and power connector, make sure the side with wires attached is also sealed with silicone gel.



2. Seal the end of the rubber coating of the All-in-One cable as indicated in the figure on the right.
   Use enough silicone gel to fill in the hose and wrap around each wires; otherwise, waterproof function cannot be guaranteed.



4

Installation

This section contains the following information:

General Remarks **20**
Ceiling/Wall Mounting **20**

General Remarks

Read the instructions provided in this chapter thoroughly before installing the camera.

NOTE! This camera must be installed by qualified personnel and the installation must conform to all local codes.

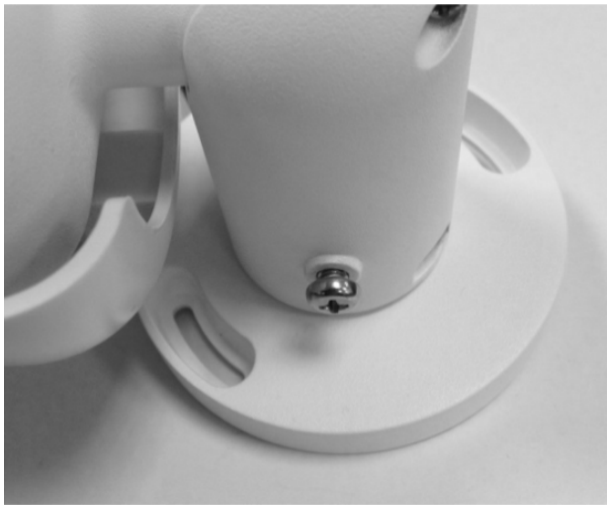
Ceiling/Wall Mounting

The camera can be installed directly on a wall or ceiling with the integrated adjustable Bracket Mount. Please note that the wall or ceiling must have enough strength to support the camera. Follow the steps below to install the camera.

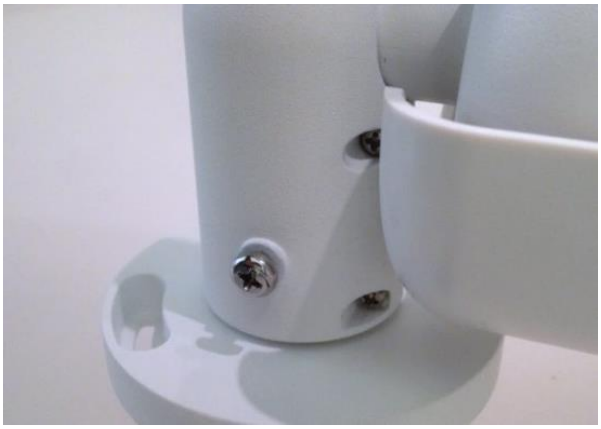
CAUTION! To prevent damage, loosen all mounting screws before adjusting the camera.

NOTE! To ensure that the unit is not affected by vibration, twisting, etc. after adjusting the camera, properly tighten all mounting screws.

1. Place the camera at the installation location. On the ceiling/wall, mark the position of the two screw holes of the camera.



2. If the screw holes are blocked by the camera body, loosen the screw shown in the right figure but do not detach it. Then rotate the camera body to reach the screw holes.



3. At the center of the two marked holes, drill a 30 mm diameter (radius as 15 mm) cable entry hole. Then drill a hole slightly smaller than the supplied plastic screw anchor on each marked screw hole.
   Thread the All-in-One cable of the camera through the cable entry hole. (Refer to chapter Camera Cabling for cable connections.)
4. Match the two screw holes of the camera with the plastic screw anchors at the installation location. Insert the plastic screw anchors into the two drilled holes, and then fasten the camera with the supplied M4x31 self-tapping screws.
5. Use a cross screwdriver to loosen the screw indicated in Figure 1, but do not detach it. Rotate the camera and point the camera to a desired direction. Then, tighten the screw. The camera joint will be fixed.

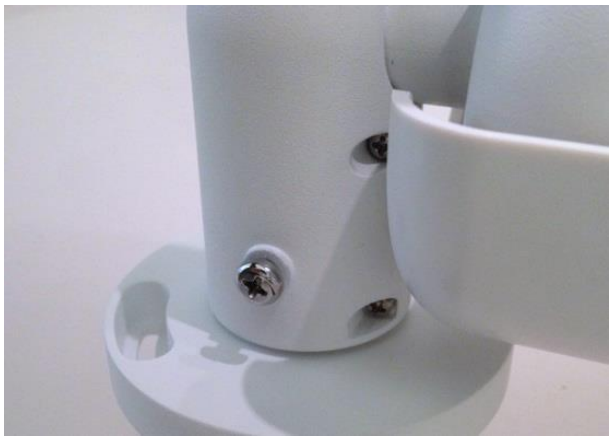


Figure 1

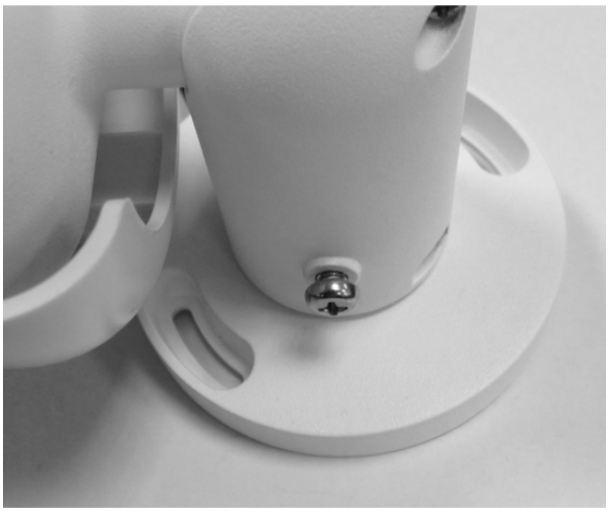


Figure 2

NOTE! If the camera joint is not tight enough for users, please fasten the supplied M5x10.5 standard screw into the hole as shown in Figure 2.

5

Configuration

This section contains the following information:

System Requirements **24**

Accessing the Camera **24**

Setup Video Resolution **26**

Exporting/Importing Configuration Files **27**

System Requirements

To perform the IP camera via web browser, please ensure the PC is in good network connection and meets system requirements as described below.

Items	System requirements
Personal Computer	Minimum: ■ Intel® Core™ i5-2430M @ 2.4 GHz ■ 4 GB RAM
	Recommended : ■ Intel® Core™ i7-870 @ 2.93 GHz ■ 8 GB RAM
Operating System	Windows 7 or later operating system
Web Browser	Microsoft Internet Explorer 11.0 Chrome Firefox Safari
Network Card	10Base-T (10 Mbps), 100Base-TX (100 Mbps) or 1000Base-T operation
Viewer	ActiveX control plug-in for Microsoft IE

NOTE! The ITE is to be connected only to PoE networks without routing to the outside plant or equivalent description.

Accessing the Camera

Accessing the Camera

The 5MP Vandal Bullet Analytics Camera supports all current browsers without requiring any additional plug-in or add-on (e. g. for H.264 / MJPEG support). Microsoft Internet Explorer with ActiveX is recommended for best performance and H.265 support

A client program will be automatically installed to the PC when connecting to the camera. If using Microsoft Internet Explorer, ensure downloading the ActiveX control is allowed by either changing the ActiveX controls and plug-in/add-on (H.264 and MJPEG) or setting Internet's security level to default.

ActiveX Controls and Plug-ins Settings	Internet Security Level Settings
1. Start the Internet Explorer (IE). 2. Select **Tools** from the main menu of the browser. Then click on **Internet Options**. 3. Click on the **Security** tab and select **Internet**, and click on **Custom level** to change ActiveX settings. 4. Set “ActiveX controls and plug-ins” items to **Prompt** or **Enable**.	1. Start the Internet Explorer (IE). 2. Select **Tools** from the main menu of the browser. Then click on **Internet Options**. 3. Click on the **Security** tab and select **Internet**. 4. Down the page, click on **Default Level** and **OK** to confirm the setting. Close the browser window.

Camera Login

The default IP address of the camera is: 10.x.x.x. By default, the camera starts as DHCP client and automatically tries to get an IP address from a DHCP server.

1. Enter the camera’s IP address in the URL bar of the web browser and hit “Enter”.
2. Enter the default username (**admin**) and password (**meinsm**).

   NOTE! ID and password are case sensitive.

   CAUTION! It is strongly advised to change the default password. Refer to the menu tree of your camera for further details.
3. In the Viewer installation window, click on **Next** to start installation.
4. The status bar will show the installation progress. After the installation is completed, click on **Finish** to exit the installation process.
5. Click on **Finish** to close the Viewer installation page.

NOTE! Once the Viewer is successfully installed, the Home page of the IP camera will be displayed as the figure below.

Motorized Lens Models

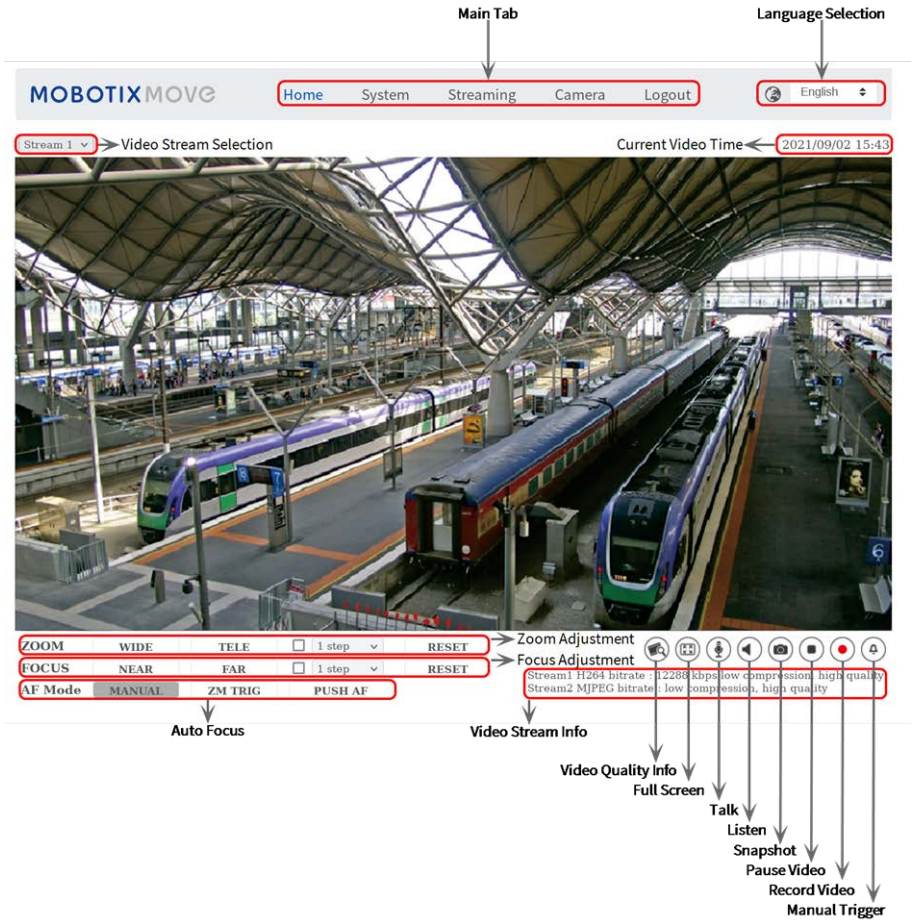


Fig. 1: Viewer Window

Zoom and Focus Adjustment

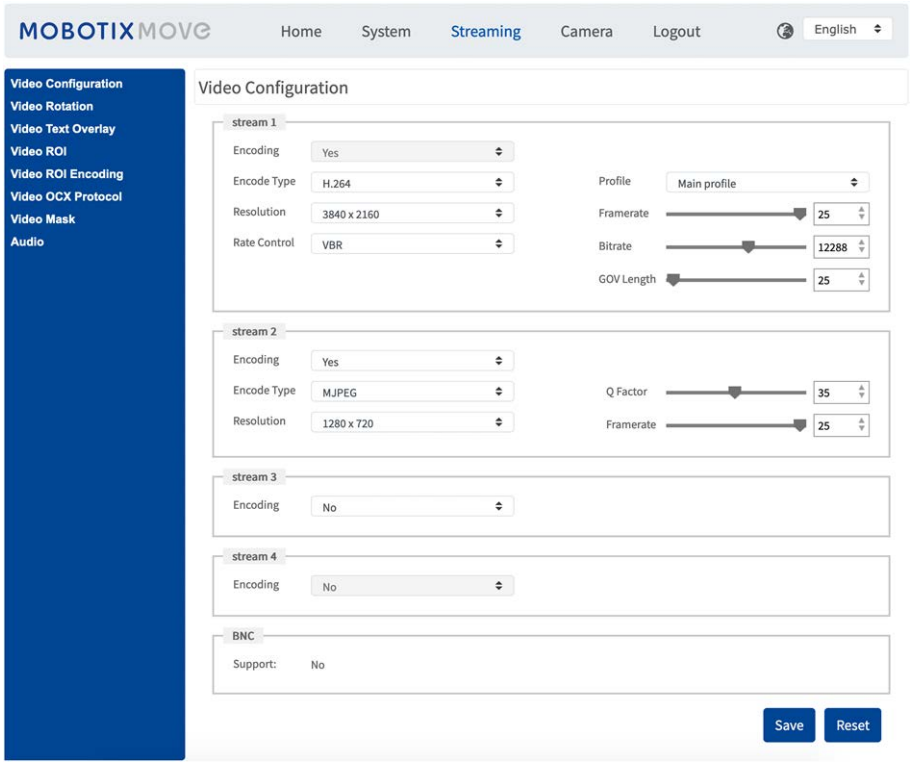
The live image will be displayed on the Home page when the camera is successfully accessed. If zoom or focus is not at the desired position, please use the function buttons on the Home page to adjust zoom and focus.

NOTE! Refer to the menu tree of the Vandal Analytics WDR IP camera for more button function details.

Setup Video Resolution

Users can setup video resolution on Video Configuration page of the user-friendly browser-based configuration interface.

The video resolution can be found under **Streaming > Video Configuration**.



The default values of video resolution are as below.

Vandal Analytics	H.265/H.264- 2688 × 1512 (30/25 fps) + H.265/H.264- 800 × 600 (30/25 fps)

Exporting/Importing Configuration Files

To export and import configuration files, users can access the Maintenance page on the user-friendly browser-based configuration interface.

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

Users can export configuration files to a specified location and retrieve data by uploading an existing configuration file to the camera. This is especially convenient to make multiple cameras having the same configuration.

Export

Users can save the system settings by exporting the configuration file (.bin) to a specified location for future use.

- Click on the **Export** button, and the popup File Download window will come out.
- Click on **Save** and specify a desired location for saving the configuration file.

Upload

To upload a configuration file to the camera, click on **Browse** to select the configuration file, and then click on the **Upload** button for uploading.

6

Menu Reference

This section contains the following information:

Overview **30**

The Camera Menu **30**

The “Home” Tab **30**

The “System” Tab **33**

The “Streaming” Tab **87**

The “Camera” Tab **94**

The “Logout” Tab **104**

Appendix A: Installing UPnP Components **104**

Appendix B: Converting IP Addresses from Decimal to Binary **104**

Overview

The 5MP Vandal Bullet Analytics Camera features newest Deep Neural Network technology. With the new hardware-accelerated engine that benefits from SoC Structure, it provides professional-level Video Analytics(VA) functions (e.g., object recognition, facial detection, facial recognition, license plate recognition).

The Camera Menu

The camera's Home Page shows these main tabs at the top:

The "Home" Tab, p. 30

Users can monitor the live video of the targeted area.

The "System" Tab, p. 33

The administrator can set host name, system time, root password, network related settings, etc. Further details will be interpreted in chapter System.

The "Streaming" Tab, p. 87

The administrator can configure video format, video compression, video OCX protocol, video frame rate and audio compression in this page.

The "Camera" Tab, p. 94

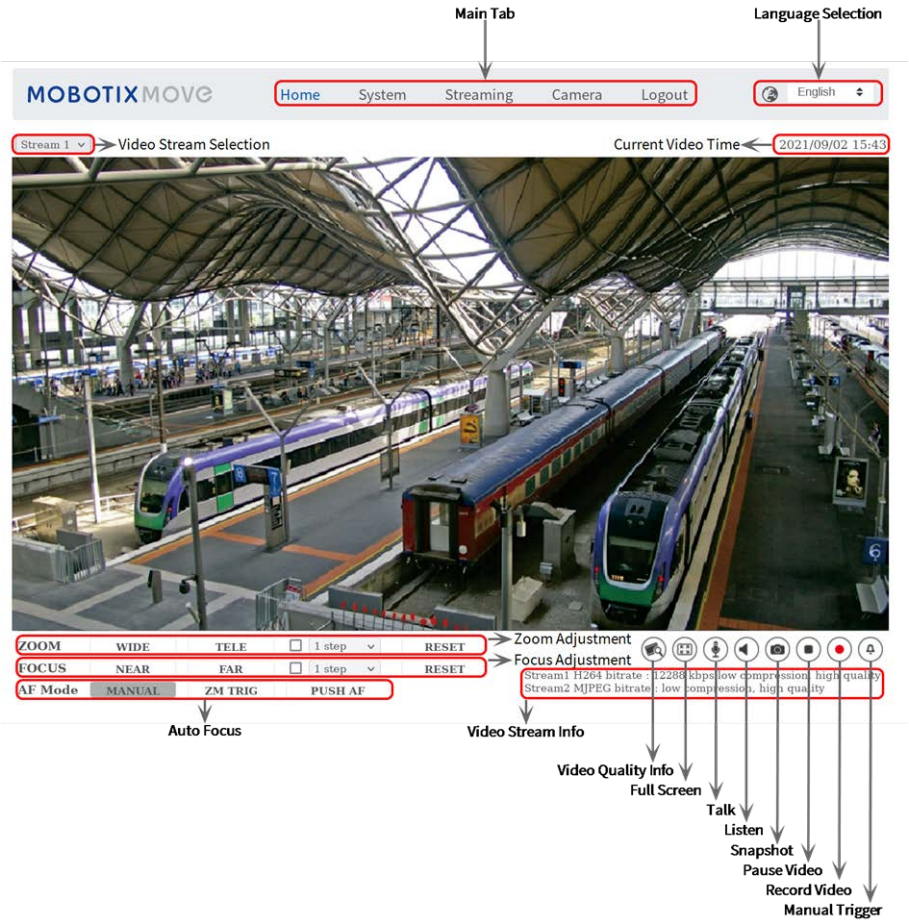
This setting page is only available for the administrator and user accounts that have been granted the privilege of camera control. The administrator and users can adjust various camera parameters including Exposure, White Balance, Sharpness, 2D/3DNR, Digital Zoom, WDR, etc.

The "Logout" Tab, p. 104

Click on the tab to logout the system. Click **Login** to re-login the camera with another username and password.

The "Home" Tab

Click on the tab **Home** to access the Home Page. There are several function buttons on this page. Detailed information of each item is as described in the following section.



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

Function Items on Home Page

Multiple Languages Support

Multiple languages are supported, including German, English, Spanish, French, Italian, Japanese, Portuguese, Russian, Simplified Chinese and Traditional Chinese for the viewer window interface.

Display Stream Selection

According to the streaming setting, users can choose the one stream to display from the drop-down menu.

Camera Info

Double-click on the live view pane, and the camera info window will pop up. Users can instant-aneously check the basic information of the camera, such as IP address, network status, video format, etc.

Digital Zoom Control

In the full screen mode, users can implement digital PTZ by scrolling up/down the mouse wheel (for zoom in/out). Users can click and drag the mouse to check the viewing area.

Video Quality

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

Full Screen

Image display size can be adjusted to full screen. Alternatively, right click on the Live Video Pane and select **Fullscreen** to go full screen.

To exit full screen mode, users can (1) tap **Esc** on the keyboard; (2) double-click on the Live Video Pane; (3) right click on the Live Video Pane and select **Normal view**.

Talk (On/Off)

Talk function allows the local site talks to the remote site. Click on the button to switch it to On/Off. Users must select the suitable transmission mode under this path: Streaming > Audio to enable this function.

Listen (On/Off)

Click on **Listen** to mute/activate the audio. Users must select the suitable transmission mode under Streaming > Audio to enable this function.

NOTE! Both Talk and Listen functions are only available for user accounts that have been granted this privilege by the administrator. Please refer to Security: Add user > Talk/Listen for further details.

Snapshot

Click on the button and the JPEG snapshots will automatically be saved in the appointed place. The default place of saving snapshots is: C:\. To change the storage location, please refer to section File Location for further details.

NOTE! With Windows 7 operating system or above, to implement the Snapshot function, users must run IE as administrator. Right click on the IE browser icon and select “Run As Administrator” to launch IE.

Live View Pause/Restart (Pause/Restart)

Click on Pause to disable video streaming, the live video will be displayed as black. Click on Restart to show the live video again.

Web Recording (On/Off)

Click on **Record** and the Live View through the web browser will be directly recorded to the specific location on the local hard drive, which could be configured in the File Location page. The default storage location for the web recording is: C:\. Please refer to section File Location for further details.

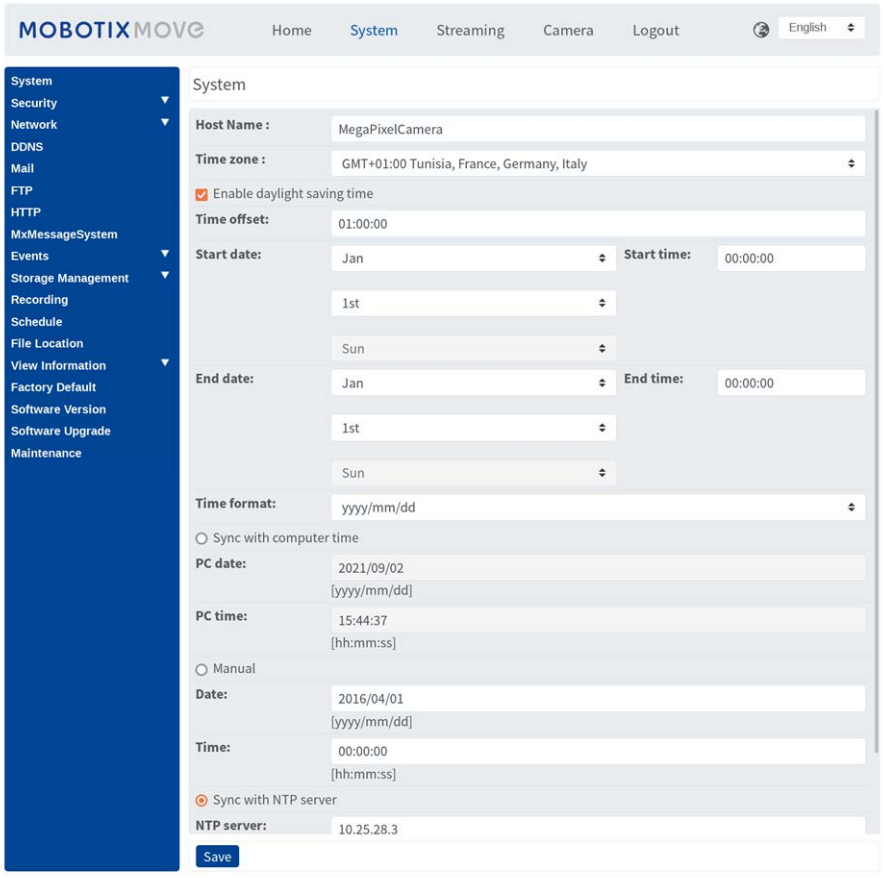
NOTE! With Windows 7 operating system or above, to implement the Web Recording function, users must run IE as administrator. To run IE as administrator, right click on the IE browser icon and select “Run As Administrator” to launch IE.

Manual Trigger (On/Off)

Click on **Manual Trigger** to turn on and off the manual trigger. Please refer to section Manual Trigger of the next chapter for further details.

The “System” Tab

Under the tab **System**, the categories are shown as the configure page below.



NOTE! Only Administrator can access the **System** configuration page.

System

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

Host Name

The name is for camera identification. If the alarm function (refer to section Events) is enabled and is set to send alarm messages by Mail/FTP, the host name entered here will be displayed in the alarm message.

Time Zone

Select the time zone from the drop-down menu according to the location of the camera.

Enable Daylight Saving Time

To enable DST, please check the item and then specify the time offset and the DST duration. The format for time offset is [hh:mm:ss]; for instance, if the amount of time offset is one hour, please enter “01:00:00” into the field.

Time format

Choose a time format (yyyy/mm/dd or dd/mm/yyyy) from the drop-down menu. The format of the date and time displayed above the live video window will be changed according to the selected format.

Sync with Computer Time

Select the item, and video date and time display will synchronize with the PC’s.

NOTE! Users MUST click on **Save** to confirm the setting. Otherwise, the time will not be synced.

Manual

The administrator can set video date and time manually. Entry format should be identical with the examples shown next to the enter fields.

Sync with NTP Server

Network Time Protocol (NTP) is an alternate way to synchronize the camera’s clock with a NTP server. Please specify the server that is wished to synchronize in the entry field. Then select an update interval from the drop-down menu. For further information about NTP, please see the web site: www.ntp.org.

NOTE! The synchronization will be done every time the camera boots up.

Click on **Save** to confirm the setting.

Security

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

Click on **Security**, there will be a drop-down menu with tabs including **User**, **HTTPS**, **IP Filter**, and **IEEE 802.1X**.

User

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

Admin Password

This item is for the administrator to reset password. Enter the new password in **Admin password** and **Confirm password**. The maximum length is 14 characters. The input characters/numbers will be displayed as dots for security purposes. Click on **Save** to confirm the changes. After the changes are confirmed, the web browser will ask the administrator to re-login to the camera with the new password.

NOTE! The following characters are valid: A-Z, a-z, 0-9, !#$%&’-.@^_~.

Add User

This item is for the administrator to add new users. Enter the new user’s name in **User name** and the password in **User password**. Username can be up to 16 characters, and the maximum length of the password is 14 characters. Tick the boxes below to give privileges for functions, including “Camera control”, “Talk” and “Listen”. Click on **Add** to add the new user. The name of the new added user will be displayed in the **User name** drop-down menu under **Manage User**. There is a maximum of twenty user accounts.

- **I/O access**
  This item supports fundamental functions that enable users to view the live video when accessing to the camera.
- **Camera control**
  This item allows the appointed user to change camera parameters on the **Camera** and **Pan Tilt** setting page.
- **Talk/Listen**
  This item allows the appointed user in the local site (camera site) to communicate with, for instance, the administrator in the remote site.

Manage User

- **Delete user**
  Pull down the **User name** drop-down menu and select the username that is wished to be deleted. Click on **Delete** to remove the selected name.
- **Edit user**
  Pull down the **User name** drop-down menu and select the username. Click on **Edit** and a popup window will appear. In the appeared window, enter the new user password and reset the privileges. Click on **Save** to confirm the changes. Then click on **Close** to complete the editing.

HTTP Authentication Setting

This setting allows secured connections between the IP camera and web browser by enforcing access controls to web resources. When users approach to the web browser, it’ll ask for username and password, which protects the camera settings or live streaming information from snooping. There are two security models available: Basic and Digest. Refer to the descriptions below for more details.

- **Basic**
  This mode can only provide basic protection for the connection security. There will still be risks for the password being intercepted.

- **Digest**
  Digest mode is a safer option for protection. The password is sent in an encrypted format to prevent it from being stolen.

NOTE! Users MUST click on **Save** to apply the setting.

Streaming Authentication Setting

This setting provides security against unauthorized users from getting streaming via Real Time Streaming Protocol (RTSP). If the setting is enabled, users will be requested to enter user name and password before viewing the live streams. There are three security modes available: Disable, Basic and Digest. Refer to the descriptions below for more details.

- **Disable**
  If disable mode is selected, there will be no security provided to against unauthorized access. Users will not be asked to input user name and password for authentication.
- **Basic**
  This mode can only provide basic protection for the live streams. There will still be risks for the password being intercepted.
- **Digest**
  Digest mode is a safer option for protection. The password is sent in an encrypted format to prevent it from being stolen.

NOTE! Users MUST click on **Save** to apply the setting.

Enable Account Lockout Function

The Account Lockout Function is to lock out an account when someone tries to log on unsuccessfully several times in a row. To protect user’s account, “Account Lockout Function’’ is activated when multiple login failures occur. Check the box **Enable Account Lockout Function** and enter the number of threshold and duration.

- **Threshold**
  Threshold is a maximum number of login attempts, ranging from 5-20 times. The default value is 5 (attempts).
- **Duration**
  Duration is the length of time that the account remains locked once the account lockout function is triggered, ranging from 1-60 minute(s). The default value is 10 (mins).

HTTPS

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

HTTPS allows secure connections between the camera and the web browser using **Secure Socket Layer (SSL)** or **Transport Layer Security (TLS)**, which ensure camera settings or

Username/Password info from snooping. It is required to install a self-signed certificate or a CA-signed certificate for implementing HTTPS.

To use HTTPS on the camera, an HTTPS certificate must be installed. The HTTPS certificate can be obtained by either creating and sending a certificate request to a Certificate Authority (CA) or creating a self-signed HTTPS certificate, as described below.

Enable HTTPS

Check the box to enable HTTPS secure connection. Once enabled, choose one from the following two secure modes.

- HTTP & HTTPS

  Under this mode, HTTP & HTTPS secure connections are enabled.
- HTTPS only

  Under this mode, the secure connection is ensured by HTTPS only.

Click on **Save** to save the setting.

Create Self-signed Certificate

Before a CA-issued certificate is obtained, users can create and install a self-signed certificate first.

Click on **Create** under “Create self-signed certificate” and provide the requested information to install a self-signed certificate for the camera. Please refer to the last part of this section Provide the Certificate Information for more details.

NOTE! The self-signed certificate does not provide the same high level of security as when using a CA-issued certificate.

Install Signed Certificate

Click on **Create Certificate Request** to create and submit a certificate request in order to obtain a signed certificate from CA.

Provide the request information in the create dialog. Please refer to the following section Provide the Certificate Information for more details.

When the request is complete, the subject of the Created Request will be shown in the field. Click on **Properties** below the Subject field, copy the PEM-formatted request and send it to the selected CA.

When the signed certificate is returned, install it by uploading the signed certificate.

Provide the Certificate Information

To create a Self-signed HTTPS Certificate or a Certificate Request to CA, please enter the information as requested.

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

- **Country**
  enter a two-letter combination code to indicate the country the certificate will be used in. For instance, type in “US” to indicate United States.
- **State or Province**
  Enter the local administrative region.
- **Locality**
  Enter other geographical information.
- **Organization**
  Enter the name of the organization to which the entity identified in “Common Name” belongs.
- **Organization Unit**
  Enter the name of the organizational unit to which the entity identified in “Common Name” belongs.
- **Common Name**
  Indicate the name of the person or other entity that the certificate identifies (often used to identify the website).
- **Valid Days**
  Enter the period in days (1 to 9999) to indicate the valid period of certificate.

Click on **OK** to save the Certificate Information after completing the setting.

IP Filter

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

With IP Filter, users can allow or deny specific IP addresses from accessing the camera.

Enable IP Filter

Check the box to enable the IP Filter function. Once enabled, the listed IP addresses (IPv4) in the **Filtered IP Addresses** list box will be allowed/denied to access the camera.

Select **Allow** or **Deny** from the drop-down menu and click on **Apply** to determine the IP filter behavior.

Add IP Address

Input IP address at the blank space below the **Filtered IP Address** list and click **Add**. The newly-added address will be shown in the list. Up to 256 IP address entries can be specified.

In addition, to filter a group of IP addresses, enter an address at the blank space followed with a slash and a number ranging from 1 to 31, e.g. 192.168.2.81/30. The number after the slash can define how many IP addresses will be filtered. For details, please refer to Example: Filtering a Group of Consecutive IP Addresses, p. 40 below.

Delete IP Address

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

Example: Filtering a Group of Consecutive IP Addresses

1. Convert 192.168.2.81 to binary numbers (see Appendix B: Converting IP Addresses from Decimal to Binary, p. 104). The binary numbers are 11000000.10101000.00000010.01010001. Users can refer to Appendix B: IP Addresses from Decimal to Binary for converting the IP addresses to binary numbers. The number “30” after the slash is referring to the first 30 digits of the binary numbers.
2. Convert a few IP addresses before and after 192.168.2.81 to binary numbers. Then compare their first 30 digits with the binary numbers of 192.168.2.81.
    1. Convert 192.168.2.80 to binary numbers. The binary numbers are 11000000.10101000.00000010.01010000. The first 30 digits are the same with the binary numbers of 192.168.2.81, thus 192.168.2.80 will be filtered.
    2. Convert 192.168.2.79 to binary numbers. The binary numbers are 11000000.10101000.00000010.01001111. The first 30 digits are different with the binary numbers of 192.168.2.81, thus 192.168.2.79 will not be filtered. This also means the IP addresses before 192.168.2.79 will not be filtered. Therefore, users can stop converting the IP addresses before 192.168.2.79 to binary numbers.
    3. Repeat the same procedure in “a” with the IP addresses after 192.168.2.81. Stop when the situation occurs in “b” happened. Namely, the 30th digit of the binary numbers of IP address 192.168.2.84 is different, and will not be filtered.

As a result, the IP addresses 192.168.2.80 to 192.168.2.83 will be filtered when entering 192.168.2.81/30. The following table clearly shows the 30^{th} digit of the binary numbers of IP addresses 192.168.79 and 192.168.84 are different from the others. Therefore, these two IP addresses will not be filtered.

IP Addresses	Binary Numbers
192.168.2.79	11000000.10101000.00000010.01001111
192.168.2.80	11000000.10101000.00000010.01010000
192.168.2.81	11000000.10101000.00000010.01010001
192.168.2.82	11000000.10101000.00000010.01010010
192.168.2.83	11000000.10101000.00000010.01010011
192.168.2.84	11000000.10101000.00000010.01010100

IEEE 802.1X

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

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

Choose **On** to enable the IEEE 802.1X function.

Select one among the four protocol types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS** and **EAP-PEAP**.

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

CA Certificate

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

Client Certificate/Private Key

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

Settings

- **Identity**

  Enter the user identity associated with the certificate. Up to 16 characters can be used.
- **Private Key Password**

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

Save IEEE 802.1X

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

Network

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

Click on **Network**, there will be a drop-down menu with tabs including **Basic**, **QoS**, **SNMP**, and **UPnP**.

Basic

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

This setting page is for setting a new IP address for the camera, configuring other network-related parameters and activating IPv6 address (if the network supports it).

General

This setting menu is for configuring a new IP address for the camera. To setup an IP address, please find out the network type first. Contact the network provider for it. Then refer to the network type and follow the instructions to setup the IP address.

NOTE! If the network type is Point-to-Point Protocol over Ethernet (PPPoE), please obtain the PPPoE username and password from the network provider.

- **Get IP address automatically (DHCP)**

  Select the item and click **Save** to confirm the new setting. A note for camera system reboot will appear. Click **OK** and the camera system will restart. The camera will be assigned with a new IP address. Close the web browser and search the camera through the installer program: DeviceSearch.exe. Refer to the steps below to connect the camera through “DeviceSearch” software.

  NOTE! Before searching the camera through DeviceSearch.exe, please record the camera’s MAC address, which can be found on the label or on the package container of the camera, for later use and identification in the future.

- Double-click on the program DeviceSearch.exe.
- After its window appears, click on **Device Search** on the top. All the finding IP devices will be listed in the page.
- Find the camera by its MAC address.
- Then double-click or right click and select **Browse** to access the camera directly by the web browser.
- A prompt window requesting for the username and the password will appear. Enter the username and the password to login to the camera.

- **Use fixed IP address**

  Select the item and insert the new IP address, e.g. 192.168.7.123. Note that the inserted IP address should be in the same LAN as the PC’s IP address. Then go to the Default gateway (explained later) blank and change the setting, e.g. 192.168.7.254. Click on **Save** to confirm the new setting. A note for system restart will appear, click **OK** and the camera system will restart. Wait for 15 seconds. The camera’s IP address in the URL bar will be changed, and users have to login again.

  When using a static IP address to connect the camera, users can access the camera by inputting the IP address in the URL bar and hit **Enter** on the keyboard. Alternatively, users can access the camera by the installer program: DeviceSearch.exe. Refer to the steps below to connect the camera through “DeviceSearch” software with a static IP address.

- Double-click on the program DeviceSearch.exe.
- After its window appears, click on **Device Search** on the top. All the finding IP devices will be listed in the page.
- Find the camera by its IP address.
- Then double-click or right click and select **Browse** to access the camera directly by the web browser.
- A prompt window requesting for the username and the password will appear. Enter the username and the password to login to the camera.
  - **IP address**

    This is necessary for network identification.
  - **Subnet mask**

    It is used to determine if the destination is in the same subnet. The default value is “255.255.255.0”.
  - **Default gateway**

    This is the gateway used to forward frames to destinations in different subnet. Invalid gateway setting will fail the transmission to destinations in different subnet.
  - **Primary DNS**

    Primary DNS is the primary domain name server that translates hostnames into IP addresses.
  - **Secondary DNS**

    Secondary DNS is a secondary domain name server that backs up the primary DNS.

- **Use PPPoE**

  For the PPPoE users, enter the PPPoE username and password into the enter fields, and click on **Save** to complete the setting.

Advanced

The following introduces the camera’s Web Server port, RTSP port, MJPEG over HTTP port, and HTTPS port.

- **Web Server port**

  The default web server port is 80. With the default web server port ‘80’, users can simply input the IP address of the camera in the URL bar of a web browser to connect the camera. When the web server port is changed to any number other than 80, users have to enter the camera’s IP address followed by a colon and the port number. For instance, a camera whose IP address is set as 192.168.0.100 and web server port as 8080 can be connected by entering “http://192.168.0.100:8080” in the URL bar.

- **RTSP port**

  The default setting of RTSP Port is 554; the RTSP Port should be set as 554 or from the range 1024 to 65535.

- **MJPEG over HTTP port**

  The default setting of MJPEG over HTTP Port is 8008; the MJPEG over HTTP Port should be set as 8008 or from the range1024 to 65535.

- **HTTPS port**

  The default setting of HTTPS Port is 443; the HTTPS Port should be set as 443 or from the range 1024 to 65535.

  NOTE! Please make sure the port numbers set above are not the same with each other; otherwise, network conflict may occur.

- **RTSP URL**

  When users use RTSP players to view the live streaming, the camera provides the flexibility to configure the streaming access name for stream 1 to stream 4. The streaming format is rtsp://**ip address**:**rtsp port**/**access name**. Take a camera whose IP address is set as 192.168.0.100 for example, if users enter “liveview.1” in the blank of stream 1 access name, the streaming address of stream 1 will be rtsp://192.168.0.100:554/liveview.1.

  NOTE! The maximum length of the access name is 32 characters, and the valid characters are A-Z, a-z, 0-9 and !#$%&’-.@^_~.

IPv6 Address Configuration

If the network supports IPv6, users can check the box beside **Enable IPv6** and click **Save**. An IPv6 address will appear beside **Address**, and users can use it to connect to the camera.

QoS

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

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

DSCP Settings

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

- **Management DSCP**

  NOTE! The class consists of HTTP traffic: Web browsing.

- **Stream 1~4 DSCP**

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

- **Video DSCP**

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

- **Audio DSCP**

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

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

VLAN

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

Check the box **Enable VLAN** to activate the VLAN function. Enter the VLAN ID. The allowed range of VLAN ID is from 1 to 4095. The default value is 20.

CoS

CoS stands for Class of Service. The higher the value of CoS is, the better transmission performance will be. The value also determines the transmission priority among the following three classes: Live Video, Live Audio and Management.

- **Live Video**

  The value range is from 0 to 7.

- **Live Audio**

  The value range is from 0 to 7.

- **Management**

  The value range is from 0 to 7.

SNMP

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

With Simple Network Management Protocol (SNMP) support, the camera can be monitored and managed remotely by the network management system.

SNMP v1/v2

- **Enable SNMP v1/v2**

  Select the version of SNMP to use by checking the box.

- **Read Community**

  Specify the community name that has read-only access to all supported SNMP objects. The default value is “public”.

- **Write Community**

  Specify the community name that has read/write access to all supported SNMP objects (except read-only objects). The default value is “private”.

SNMP v3

SNMP v3 supports an enhanced security system that provides protection against unauthorized users and ensures the privacy of the messages. Users will be requested to enter security name, authentication password and encryption password while setting the camera connections in the network management system. With SNMP v3, the messages sent between the cameras and the network management system will be encrypted to ensure privacy.

- **Enable SNMP v3**

  Enable SNMP v3 by checking the box.

- **Security Name**

  The maximum length of the security name is 32 characters.

  NOTE! The valid characters are A-Z, a-z, 0-9 and !#$%&’-.@^_~.

- **Authentication Type**

  There are two authentication types available: MD5 and SHA. Select **SHA** for a higher security level.

- **Authentication Password**

  The authentication password must be 8 characters or more. The input characters/numbers will be displayed as dots for security purposes.

  NOTE! The valid characters are A-Z, a-z, 0-9 and !#$%&’-.@^_~.

- **Encryption Type**

  There are two encryption types available: DES and AES. Select **AES** for a higher security level.

- **Encryption Password**

  The minimum length of the encryption password is 8 characters and the maximum length is 512 characters. The input characters/numbers will be displayed as dots for security purposes. The encryption password can also be left blank. However, the messages will not be encrypted to protect privacy.

  NOTE! The valid characters are A-Z, a-z, 0-9 and !#$%&’-.@^_~.

Traps for SNMP v1/v2/v3

Traps are used by the camera to send messages to a management system for important events or status changes.

- **Enable Traps**

  Check the box to activate trap reporting.

- **Trap address**

  Enter the IP address of the management server.

- **Trap community**

  Enter the community to use when sending a trap message to the management system.

Trap Option

- **Warm Start**

  A Warm Start SNMP trap signifies that the SNMP device, i.e. IP camera, performs software reload.

Click on **Save** when completed.

UPnP

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

UPnP Setting

- **Enable UPnP**

  When the UPnP is enabled, whenever the camera is presented to the LAN, the icon of the connected cameras will appear in My Network Places to allow for direct access.

  NOTE! To enable this function, please make sure the UPnP component is installed on the computer. Please refer to Appendix A: Install UPnP Components for UPnP component installation procedure.

- **Enable UPnP port forwarding**

  When the UPnP port forwarding is enabled, the camera is allowed to open the web server port on the router automatically.

  NOTE! To enable this function, please make sure that the router supports UPnP and it is activated.

- **Friendly name**

  Set a name for the camera for identity.

Click on **Save** when finished.

DDNS

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

Dynamic Domain Name System (DDNS) allows a host name to be constantly synchronized with a dynamic IP address. In other words, it allows those using a dynamic IP address to be associated to a static domain name so others can connect to it by name.

Enable DDNS

Check the item to enable DDNS.

Provider

Select one DDNS host from the provider list.

Host name

Enter the registered domain name in the field.

Username/E-Mail

Enter the username or E-mail required by the DDNS provider for authentication.

Password/Key

Enter the password or key required by the DDNS provider for authentication.

Mail

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

The administrator can send an E-mail via Simple Mail Transfer Protocol (SMTP) when an alarm is triggered. SMTP is a protocol for sending E-mail messages between servers. SMTP is a relatively

simple, text-based protocol, where one or more recipients of a message are specified and the message text is transferred.

Two sets of SMTP can be configured. Each set includes SMTP Server, Account Name, Password and E-mail Address settings. For SMTP server, contact the network service provider for more specific information.

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

FTP

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

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

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

HTTP

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

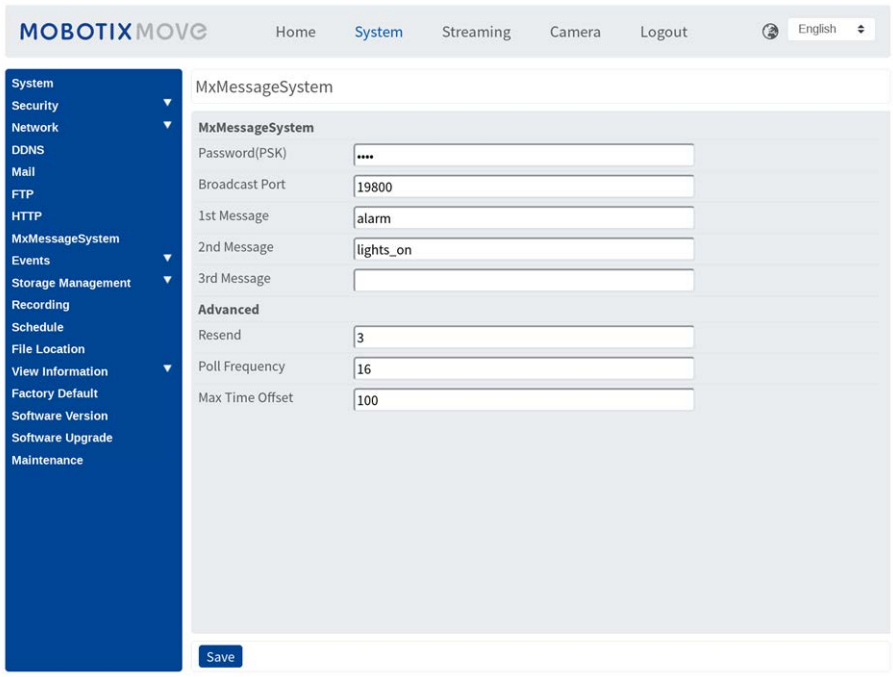
An HTTP Notification server can listen for the notification messages from the cameras by triggered events. Enter the HTTP details, which include server name (for instance, http://192.168.0.100/admin.php), username, and password in the fields. **Alarm** triggered and **Motion Detection** notifications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

Click on **Save** when finished.

NOTE! Please refer to Events > Application > Send HTTP notification for HTTP Notification settings.

MxMessageSystem

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



The Camera can send notifications via the MxMessageSystem by triggered events.

MxMessageSystem

Password (PSK): The communication is SSH encrypted. Enter your private security key.

Broadcast Port: Enter the broadcast port of the MxMessageSystem.

Messages: If the camera Enter up to three messages that can be send to the MxMessageSystem.

Advanced

Resend: This parameter specifies how often in total the message will be resent. Many resends increase the probability that the message is actually received, but they also create heavier network load.

Poll frequency: This parameter specifies how often per second the messages will be sent. A higher frequency reduces latency, but creates heavier network load.

Max. Time Offset: Maximum difference between the message timestamp and the system time. Messages with a greater difference are discarded. It is highly recommended to synchronize the system time of all message system components using NTP (in the Date and Time dialog).

Click on **Save** when finished.

NOTE! Refer to Events > Application > Send MxMessage events.

Events (Alarm Settings)

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

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

Application

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

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

Alarm Switch

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

Alarm Type

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

Triggered Action

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

- **Enable Alarm Output (high/low)**

  Select the item to enable alarm relay output.

- **IR Cut Filter**

  Select the item and the IR cut filter (ICR) of the camera will be removed (on) or blocked (off) when alarm input is triggered. This function is only available for models with IR cut filter.

  NOTE! The IR Function (refer to section IR Function) could not be set as **Auto** mode if this triggered action is enabled.

- **Send Message by FTP/E-Mail**

  The administrator can select whether to send an alarm message by FTP and/or E-mail when an alarm is triggered.

- **Upload Image by FTP**

  Select this item and the administrator can assign an FTP site and configure various parameters. When the alarm is triggered, event images will be uploaded to the appointed FTP site. Note that to implement this function, one of the streaming MUST be set as MJPEG; otherwise, this function will be grayed out and cannot be accessed.

  The **Pre-trigger buffer** function allows users to check what caused the trigger. The **Pre-trigger buffer** frame rate could be pre-determined. **Post-trigger buffer** is for users to upload certain amount of images after the alarm input is triggered.

  NOTE! Pre-trigger buffer generally ranges from 1 to 20 frames. However, the range will change accordingly if the frame rate of MJPEG on Streaming > Video Configuration is 6 or smaller.

  Check the box **Continue image upload** to upload the triggered images during certain time or keep uploading until the trigger is off. Select **Upload for __ sec** and enter the duration in the blank. The images of the duration will be uploaded to FTP when the alarm input is triggered. The setting range is from 1 to 99999 sec. Select **Upload during the trigger is active** to make the images keep being uploaded to FTP during the trigger active until the alarm is released. Set the Image frequency as the upload frame rate. The setting range is from 1 to 15 frames.

  NOTE! Make sure FTP configuration has been completed. Refer to section FTP for further details.

- **Upload Image by E-Mail**

  Select this item and the administrator can assign an E-mail address and configure various parameters. When the alarm input is triggered, event images will be sent to the appointed E-mail address. Note that to implement this function, one of the streaming MUST be set as MJPEG; otherwise, this function will be grayed out and cannot be accessed.

  The **Pre-trigger buffer** function allows users to check what caused the trigger. The **Pre-trigger buffer** frame rate could be pre-determined. On the other hand, **Post-trigger buffer** is for users to upload certain amount of images after alarm input is triggered.

  NOTE! Pre-trigger buffer generally ranges from 1 to 20 frames. However, the range will change accordingly if the frame rate of MJPEG on Streaming > Video Configuration is 6 or smaller.

  Check the box **Continue image upload** to upload the triggered images during certain time or keep uploading until the trigger is off. Select **Upload for __ sec** and enter the duration in the blank. The images of the duration will be uploading by E-mail when the alarm input is triggered. The setting range is from 1 to 99999 sec. Select **Upload during the trigger active** to make the images keep being uploaded to E-mail during the trigger active until the alarm is released. Set the Image frequency as the upload frame rate. The setting range is from 1 to 15 frames.

  NOTE! Make sure SMTP configuration has been completed. Refer to section Mail for further details.

- **Send HTTP Notification**

  Check this item and select the destination HTTP address. Then specify the parameters for event notifications by **Alarm** triggered. When an alarm is triggered, the HTTP notification will be sent to the specified HTTP server.

  For instance, if the custom parameter is set as “action=1&group=2”, and the HTTP server name is “http://192.168.0.100/admin.php”, the notification will be sent to HTTP server as “http://192.168.0.100/ admin.php/action=1&group=2” when alarm is triggered.

- **Send message by MxMessageSystem**
- Check this item and select a message to be send to the MxMessageSystem accordingly. If required add custom JSON parameters to the message.

- **Record Video Clip**

  Check this item and select a video recording storage type, **SD Card** or **NAS** (Network-Attached Storage). The alarm-triggered recording will be saved into the microSD/SD card or the NAS.

  The **Pre-trigger buffer** recording function allows users to check what caused the trigger. The pre-trigger buffer time range is from 1 to 3 sec.

  Select **Upload for __ sec** to set the recording duration after alarm is triggered. The setting range is from 1 to 99999 sec. Select **Upload during the trigger is active** to record the triggered video until the trigger is off.

  NOTE! Please make sure the local recording (with microSD/SD card) or the remote recording (with NAS) is activated so that this function can be implemented. Refer to section Recording for further details.

File Name

Enter a file name in the blank, e.g. image.jpg. The file name format of the uploaded image can be set in this section. Please select the one that meets the requirements.

- **Add date/time suffix**

  File name: imageYYMMDD_HHNNSS_XX.jpg

  Y: Year, M: Month, D: Day

  H: Hour, N: Minute, S: Second

  X: Sequence Number
- **Add sequence number suffix (no maximum value)**

  File name: imageXXXXXXX.jpg

  X: Sequence Number
- **Add sequence number suffix up to # and then start over**

  File Name: imageXX.jpg

  X: Sequence Number

  The file name suffix will end at the number being set. For example, if the setting is up to “10”, the file name will start from 00, end at 10, and then start all over again.
- **Overwrite**

  The original image in the FTP site will be overwritten by the new uploaded file with a static file-name.

Save

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

Motion Detection

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

Motion Detection function allows the camera to detect suspicious motion and trigger alarms by comparing sampling pixels in the detection area of two consecutive live images. When motion volume in the detection area reaches/exceeds the determined sensitivity threshold value, the alarm will be triggered.

The function supports up to 4 sets of Motion Detection Settings. Settings can be chosen from the Motion Detection drop-down menu.

Motion Detection

By default, Motion Detection function for each Motion Detection Setting is **Off**. Select **On** to enable Motion Detection. Users can also activate the function according to the schedule previously set in the **Schedule** setting page. Select **By schedule** and click **Please select...** to choose the desired schedule from the drop-down menu.

Motion Region Setup (Motion Region Paint)

The camera divides the detection area into 1200 (40x30) detection grids; users can draw the motion detection region using the paintbrush.

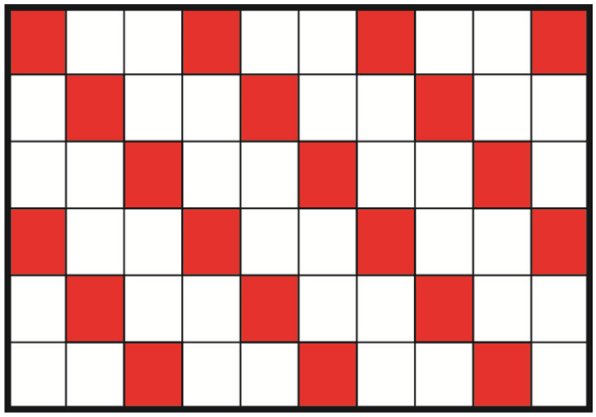
Check the box **Enable brush** and select the brush size, 1x1, 3x3 or 5x5. Then, left click and drag the mouse cursor to draw the preferred detection region. To erase the drawn detection region, left click and drag the mouse cursor on the colored grids.

Motion Detection Setting

Users could adjust various parameters of Motion Detection in this section.

- **Sampling pixel interval [1-10]:**

  This item is used to examine the differences between two frames. Users can configure the interval of sampling pixel. The default value is 1. For instance, if users set the interval as 3, IP camera system will take one sampling pixel from every 3 pixels of each row and each column in detection area (refer to the figure below). The alarm will be triggered when differences are detected.



- **Detection level [1-100]:**

  Users can configure detection level for each sampling pixel. Detection level is how much the camera can accept the differences between two sampling pixels. The smaller the value is, the more minor motions it detects. The default level is 10.

- **Sensitivity level [1-100]:**

  The default level is 80, which means if 20% or more sampling pixels are detected differently, system will detect motion. The bigger the value, the more sensitive it is. Meanwhile, when the value is bigger, the red horizontal line in the motion indication window will be lower accordingly.

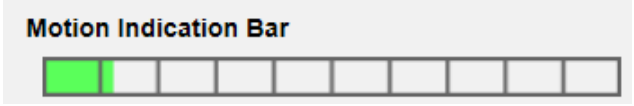
- **Time interval (sec) [0-7200]:**

  The value is the interval between each detected motion. The default interval is 10.

Motion Indication Bar

When Motion Detection function is activated and the motion is detected, the signals will be displayed on the motion indication bar. The motion indication bar will go green or red when there is any motion occurrence in the detection region.

Green suggests the occurring motion is detected and does not exceed the threshold of detection level and sensitivity level. No alarms will be triggered.



Red suggests the ongoing motion exceeds the threshold of detection level and sensitivity level. The alarm will be triggered.

Triggered Action (Multi-option)

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

- **Enable Alarm Output (high/low)**

  Check the item and select the predefined type of alarm output to enable alarm relay output when motion is detected.

- **Send Alarm Message by FTP/E-Mail**

  The administrator can select whether to send an alarm message by FTP and/or E-mail when motion is detected.

- **Upload Image by FTP**

  Select this item and the administrator can assign an FTP site and configure various parameters. When motion is detected, event images will be uploaded to the appointed FTP site. Note that to implement this function, one of the streaming MUST be set as MJPEG; otherwise, this function will be grayed out and cannot be accessed.

  The **Pre-trigger buffer** function allows users to check what caused the trigger. The **Pre-trigger buffer** frame rate could be pre-determined. On the other hand, **Post-trigger buffer** is for users to upload certain amount of images after motion event occurs.

  > **NOTE! Pre-trigger buffer** generally ranges from 1 to 20 frames. However, the range will change accordingly if the frame rate of MJPEG on Streaming > Video Configuration is 6 or smaller.

  Check the box **Continue image upload** to upload the triggered images during certain time or keep uploading until the trigger is off. Select **Upload for __sec** and enter the duration in the blank. The images of the duration will be uploaded to FTP when the motion event occurs. The setting range is from 1 to 99999 sec. Select **Upload during the trigger active** to make the images keep being uploaded to FTP during the trigger active until the event stops. Set the Image frequency as the upload frame rate. The setting range is from 1 to 15 frames per second.

  > **NOTE!** Make sure FTP configuration has been completed. Refer to section FTP for further details.

- **Upload Image by E-Mail**

  Select this item and the administrator can assign an E-mail address and configure various parameters. When motion is detected, event images will be sent to the appointed E-mail address. Note that to implement this function, one of the streaming MUST be set as MJPEG; otherwise, this function will be grayed out and cannot be accessed.

  The **Pre-trigger buffer** function allows users to check what caused the trigger. The **Pre-trigger buffer** frame rate could be pre-determined. On the other hand, **Post-trigger buffer** is for users to upload certain amount of images after the motion event occurs.

  > **NOTE! Pre-trigger buffer** generally ranges from 1 to 20 frames. However, the range will change accordingly if the frame rate of MJPEG on Streaming > Video Configuration is 6 or smaller.

  Check the box **Continue image upload** to upload the triggered images during certain time or keep uploading until the trigger is off. Select **Upload for __sec** and enter the duration in the blank. The images of the duration will be uploading by E-mail when the motion event occurs. The setting range is from 1 to 99999 sec. Select **Upload during the trigger active** to make the images keep being uploaded to E-mail during the trigger active until the event stops. Set the Image frequency as the upload frame rate. The setting range is from 1 to 15 frames per second.

  > **NOTE!** Make sure SMTP configuration has been completed. Refer to section Mail for further details.

- **Send HTTP Notification**

  Check this item, select the destination HTTP address, and specify the parameters for event notifications by **Motion Detection** triggered. When an alarm is triggered, the notification can be sent to the specified HTTP server.

  For instance, if the custom parameter is set as “action=1&group=2”, and the HTTP server name is “http://192.168.0.100/admin.php”, the notification will be sent to HTTP server as “http://192.168.0.100/ admin.php/action=1&group=2” when alarm is triggered.

- **Send message by MxMessageSystem**
- Check this item and select a message to be send to the MxMessageSystem accordingly. If required add custom JSON parameters to the message.

- **Record Video Clip**

  Check this item and select a video recording storage type, **SD Card** or **NAS** (Network-Attached Storage>. The Motion Detection recording will be stored in microSD/SD card or the NAS when motion is detected.

  The **Pre-trigger buffer** recording function allows users to check what caused the trigger. The pre-trigger buffer time range is from 1 sec. to 3 sec. Select **Upload for __ sec** to set the recording duration after motion is triggered. The setting range is from 1 to 99999 sec. Select **Upload during the trigger active** to record the triggered video until the trigger is off.

  NOTE! Please make sure the local recording (with microSD/SD card) or the remote recording (with NAS) is activated so that this function can be implemented. Refer to section Recording for further details.

File Name

Enter a file name in the blank, e.g. image.jpg. The uploaded image’s file name format can be set in this section. Please select the one that meets the requirements.

- **Add date/time suffix**

  File name: imageYYMMDD_HHNNSS_XX.jpg

  Y: Year, M: Month, D: Day

  H: Hour, N: Minute, S: Second

  X: Sequence Number
- **Add sequence number suffix (no maximum value)**

  File name: imageXXXXXXX.jpg

  X: Sequence Number
- **Add sequence number suffix up to # and then start over**

  File Name: imageXX.jpg

  X: Sequence Number

  The file name suffix will end at the number being set. For example, if the setting is up to “10”, the file name will start from 00, end at 10, and then start all over again.
- **Overwrite**

  The original image in the FTP site will be overwritten by the new uploaded file with a static filename.

Save

Click on **Save** to save the settings.

Network Failure Detection

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

Network Failure Detection allows the camera to ping another IP device (e.g. NVR, VSS, Video Server, etc.) within the network periodically and generates some actions in case of network failure occurs, for instance, a Video Server is somehow disconnected.

Being capable of implementing local recording (through microSD/SD card) or remote recording (via NAS) when network failure happens, the camera can be a backup recording device for the surveillance system.

Detection Switch

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

Detection Type

Input the IP device address and the period of ping time to ping. The camera will ping the IP device every N minute(s). If it fails for up to three times, the alarm will be triggered. The ping time setting range is from 1 to 99 min.

Triggered Action

The administrator can specify alarm actions that will take when network failure is detected. All options are listed as follows.

- **Enable Alarm Output (high/low)**

  Select the item to enable alarm relay output.
- **Send Alarm Message by FTP/E-Mail**

  The administrator can select whether to send an alarm message by FTP and/or E-mail when an alarm is triggered.
- **Send message by MxMessageSystem**
- Check this item and select a message to be send to the MxMessageSystem accordingly. If required add custom JSON parameters to the message.

- **Record Video Clip**

  Check the item and select a video recording storage type, **SD Card** or **NAS** (Network-Attached Storage). The alarm-triggered recording will be saved into the microSD/SD card.

  The **Pre-trigger buffer** recording function allows users to check what caused the trigger. The pre-trigger buffer time range is from 1 to 3 sec. Select **Upload for __ sec** to set the recording duration after alarm is triggered. The setting range is from 1 to 99999 sec. Select **Upload during the trigger active** to record the triggered video until the trigger is off.

  NOTE! Please make sure the local recording (with microSD/SD card) or the remote recording (with NAS) is activated so that this function can be implemented. Refer to section Recording for further details.

Save

Click on **Save** to save all the settings mentioned above.

Tampering

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

Tampering Alarm function helps the IP camera against tampering, such as deliberate redirection, blocking, paint spray, and lens cover, etc., through video analysis and reaction to such events by sending out notifications or uploading snapshots to the specified destination(s).

Detection of camera tampering is achieved by measuring the differences between the older frames of video (which are stored in buffers) and more recent frames.

Tampering Alarm

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

Tampering Duration

Minimum Tampering Duration is the time for video analysis to determine whether camera tampering has occurred. Minimum Duration could also be interpreted as defining the Tampering threshold; longer duration represents higher threshold. Settable Tampering Duration time range is from 10 to 3600 sec. The Default value is 20 sec.

Triggered Action

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

- **Enable Alarm Output (high/low)**

  Check the item and select the predefined type of alarm output to enable alarm output when tampering is detected.

- **Send Message by FTP/E-Mail**

  The administrator can select whether to send an alarm message by FTP and/or E-mail when tampering is detected.

- **Upload Image by FTP**

  Select this item and the administrator can assign an FTP site and configure various parameters. When tampering is detected, event images will be uploaded to the appointed FTP site. Note that to implement this function, one of the streaming MUST be set as MJPEG; otherwise, this function will be grayed out and cannot be accessed.

  The **Pre-trigger buffer** function allows users to check what caused the trigger. The **Pre-trigger buffer** frame rate could be pre-determined. On the other hand, **Post-trigger buffer** is for users to upload certain amount of images after tampering is triggered.

  > **NOTE! Pre-trigger buffer** generally ranges from 1 to 20 frames. However, the range will change accordingly if the frame rate of MJPEG on Streaming > Video Configuration is 6 or smaller.

  Check the box **Continue image upload** to upload the triggered images during certain time or keep uploading until the trigger is off. Select **Upload for __ sec** and enter the duration in the blank. The images of the duration will be uploaded to FTP when tampering is triggered. The setting range is from 1 to 99999 sec. Select **Upload during the trigger active** to make the images keep being upload to FTP during the trigger active until the tampering stops. Set the Image frequency as the upload frame rate. The setting range is from 1 to 15 frames.

  > **NOTE!** Make sure FTP configuration has been completed. Refer to section FTP for further details.

- **Upload Image by E-Mail**

  Select this item and the administrator can assign an E-mail address and configure various parameters. When tampering is detected, event images will be sent to the appointed E-mail address. Note that to implement this function, one of the streaming MUST be set as MJPEG; otherwise, this function will be grayed out and cannot be accessed.

  The **Pre-trigger buffer** function allows users to check what caused the trigger. The **Pre-trigger buffer** frame rate could be pre-determined. On the other hand, **Post-trigger buffer** is for users to upload certain amount of images after tampering occurs.

  NOTE! Normally the setting range of the **Pre-trigger buffer** is 1 to 20 frames. However, the setting range will change accordingly if the frame rate of MJPEG on the **Video Configuration** setting page is 6 or smaller.

  Check the box **Continue image upload** to upload the triggered images during certain time or keep uploading until the trigger is off. Select **Upload for __ sec** and enter the duration in the blank. The images of the duration will be uploading by E-mail when tampering is triggered. The setting range is from 1 to 99999 sec. Select **Upload during the trigger active** to make the images keep being upload to E-mail during the trigger active until tampering stops. Set the Image frequency as the upload frame rate. The setting range is from 1 to 20 frames.

  NOTE! Make sure SMTP configuration has been completed. Refer to section Mail for further details.

- **Send HTTP Notification**

  Check this item, select the destination HTTP address, and specify the parameters for HTTP notifications. When the Tampering Alarm is triggered, the HTTP notifications can be sent to the specified HTTP server.

  For instance, if the custom parameter is set as “action=1&group=2”, and the HTTP server name is “http://192.168.0.1/admin.php”, the notification will be sent to HTTP server as “http://192.168.0.1/admin.php? action=1&group=2” when alarm is triggered.

- **Send message by MxMessageSystem**
- Check this item and select a message to be send to the MxMessageSystem accordingly. If required add custom JSON parameters to the message.

- **Record Video Clip**

  Check this item and select a video recording storage type, **SD Card** or **NAS** (Network-Attached Storage). The alarm-triggered recording will be stored into microSD/SD card or the NAS.

  The **Pre-trigger buffer** recording function allows users to check what caused the trigger. The pre-trigger buffer time range is from 1 to 3 sec. Select **Upload for __ sec** to set the recording duration after tampering occurs. The setting range is from 1 to 99999 sec. Select **Upload during the trigger active** to record the triggered video until the trigger is off.

  NOTE! Please make sure the local recording (with microSD/SD card) or the remote recording (with NAS) is activated so that this function can be implemented. Refer to section Recording for further details.

File Name

Enter a file name in the blank, e.g. image.jpg. The uploaded image’s file name format can be set in this section. Please select the one that meets the requirements.

- **Add date/time suffix**

  File name: imageYYMMDD_HHNNSS_XX.jpg

  Y: Year, M: Month, D: Day

  H: Hour, N: Minute, S: Second

  X: Sequence Number

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

  File name: imageXXXXXXX.jpg

  X: Sequence Number

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

  File Name: imageXX.jpg

  X: Sequence Number

  The file name suffix will end at the number being set. For example, if the setting is up to “10”, the file name will start from 00, end at 10, and then start all over again.

- **Overwrite**

  The original image in the FTP site will be overwritten by the new uploaded file with a static file name.

Save

Click on **Save** to save all the settings mentioned above.

MxMessageSystem Event

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

MxMessageSystem Alarm function can trigger an action if a notification by the MxMessageSystem is received

MxMessageSystem Alarm

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

MxMessageSystem Setting

- **Message Path/Name:** Enter the message path of the MxMessage which should trigger an action. Minimum Tampering Duration is the time for video analysis to determine whether camera tampering has occurred. Minimum Duration could also be interpreted as defining the Tampering threshold; longer duration represents higher threshold. Settable Tampering Duration time range is from 10 to 3600 sec. The Default value is 20 sec.
- **Action Duration:** Set a time period in seconds after which a triggered action such as video recording is to be ended.

Triggered Action

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

- **Enable Alarm Output (high/low)**

  Check the item and select the predefined type of alarm output to enable alarm output when tampering is detected.
- **IR cut filter**

  Set the IR cut filter on (default) or off.
- **Send Message by FTP/E-Mail**

  The administrator can select whether to send an alarm message by FTP and/or E-mail when tampering is detected.

- **Upload Image by FTP**

  Select this item and the administrator can assign an FTP site and configure various parameters. When tampering is detected, event images will be uploaded to the appointed FTP site. Note that to implement this function, one of the streaming MUST be set as MJPEG; otherwise, this function will be grayed out and cannot be accessed.

  The **Pre-trigger buffer** function allows users to check what caused the trigger. The **Pre-trigger buffer** frame rate could be pre-determined. On the other hand, **Post-trigger buffer** is for users to upload certain amount of images after tampering is triggered.

  NOTE! Pre-trigger buffer generally ranges from 1 to 20 frames. However, the range will change accordingly if the frame rate of MJPEG on Streaming > Video Configuration is 6 or smaller.

  Check the box **Continue image upload** to upload the triggered images during certain time or keep uploading until the trigger is off. Select **Upload for __ sec** and enter the duration in the blank. The images of the duration will be uploaded to FTP when tampering is triggered. The setting range is from 1 to 99999 sec. Select **Upload during the trigger active** to make the images keep being upload to FTP during the trigger active until the tampering stops. Set the Image frequency as the upload frame rate. The setting range is from 1 to 15 frames.

  NOTE! Make sure FTP configuration has been completed. Refer to section FTP for further details.

- **Upload Image by E-Mail**

  Select this item and the administrator can assign an E-mail address and configure various parameters. When tampering is detected, event images will be sent to the appointed E-mail address. Note that to implement this function, one of the streaming MUST be set as MJPEG; otherwise, this function will be grayed out and cannot be accessed.

  The **Pre-trigger buffer** function allows users to check what caused the trigger. The **Pre-trigger buffer** frame rate could be pre-determined. On the other hand, **Post-trigger buffer** is for users to upload certain amount of images after tampering occurs.

  NOTE! Normally the setting range of the **Pre-trigger buffer** is 1 to 20 frames. However, the setting range will change accordingly if the frame rate of MJPEG on the **Video Configuration** setting page is 6 or smaller.

  Check the box **Continue image upload** to upload the triggered images during certain time or keep uploading until the trigger is off. Select **Upload for __ sec** and enter the duration in the blank. The images of the duration will be uploading by E-mail when tampering is triggered. The setting range is from 1 to 99999 sec. Select **Upload during the trigger active** to make the images keep being upload to E-mail during the trigger active until tampering stops. Set the Image frequency as the upload frame rate. The setting range is from 1 to 20 frames.

  NOTE! Make sure SMTP configuration has been completed. Refer to section Mail for further details.

- **Send HTTP Notification**

  Check this item, select the destination HTTP address, and specify the parameters for HTTP notifications. When the Tampering Alarm is triggered, the HTTP notifications can be sent to the specified HTTP server.

  For instance, if the custom parameter is set as “action=1&group=2”, and the HTTP server name is “http://192.168.0.1/admin.php”, the notification will be sent to HTTP server as “http://192.168.0.1/admin.php? action=1&group=2” when alarm is triggered.

- **Send message by MxMessageSystem**
- Check this item and select a message to be send to the MxMessageSystem accordingly. If required add custom JSON parameters to the message.

- **Record Video Clip**

  Check this item and select a video recording storage type, **SD Card** or **NAS** (Network-Attached Storage). The alarm-triggered recording will be stored into microSD/SD card or the NAS.

  The **Pre-trigger buffer** recording function allows users to check what caused the trigger. The pre-trigger buffer time range is from 1 to 3 sec. Select **Upload for __ sec** to set the recording duration after tampering occurs. The setting range is from 1 to 99999 sec. Select **Upload during the trigger active** to record the triggered video until the trigger is off.

  NOTE! Please make sure the local recording (with microSD/SD card) or the remote recording (with NAS) is activated so that this function can be implemented. Refer to section Recording for further details.

File Name

Enter a file name in the blank, e.g. image.jpg. The uploaded image’s file name format can be set in this section. Please select the one that meets the requirements.

- **Add date/time suffix**

  File name: imageYYMMDD_HHNNSS_XX.jpg

  Y: Year, M: Month, D: Day

  H: Hour, N: Minute, S: Second

  X: Sequence Number

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

  File name: imageXXXXXXX.jpg

  X: Sequence Number

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

  File Name: imageXX.jpg

  X: Sequence Number

  The file name suffix will end at the number being set. For example, if the setting is up to “10”, the file name will start from 00, end at 10, and then start all over again.

- **Overwrite**

  The original image in the FTP site will be overwritten by the new uploaded file with a static file name.

Save

Click on **Save** to save all the settings mentioned above.

Periodical Event

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

With Periodical Event setting, users can set the camera to upload images periodically to an FTP site or an E-mail address. For example, if the time interval is set to 60 seconds, the camera will upload images to the FTP site or the E-mail address every 60 seconds. The images to be uploaded are the images before and after the triggered moment. Users can define how many images to be uploaded in the **Triggered Action** section of this setting page.

Periodical Event

The default setting for the Periodical Event function is **Off**. Enable the function by selecting **On**.

Time Interval

The default value of the time interval is 60 seconds. The setting range of the time interval is from 60 to 3600 seconds.

Triggered Action

- **Upload Image by FTP**

  Select this item and the administrator can assign an FTP site and configure various parameters. Images will be uploaded to the appointed FTP site periodically. Note that to implement this function, one of the streaming MUST be set as MJPEG; otherwise, this function will be grayed out and cannot be accessed.

  The **Pre-trigger buffer** function can define how many images to be uploaded before the triggered moment. The **Post-trigger buffer** function can define how many images to be uploaded after the triggered moment.

  NOTE! Pre-trigger buffer generally ranges from 1 to 20 frames. However, the range will change accordingly if the frame rate of MJPEG on Streaming > Video Configuration is 6 or smaller.

  NOTE! Make sure FTP configuration has been completed. Refer to section FTP of this chapter for further details.

- **Upload Image by E-mail**

  Select this item and the administrator can assign an E-mail address and configure various parameters. Images will be uploaded to the appointed E-mail address periodically. Note that to implement this function, one of the streaming MUST be set as MJPEG; otherwise, this function will be grayed out and cannot be accessed.

  The **Pre-trigger buffer** function can define how many images to be uploaded before the triggered moment. The **Post-trigger buffer** function can define how many images to be uploaded after the triggered moment.

  NOTE! Pre-trigger buffer generally ranges from 1 to 20 frames. However, the range will change accordingly if the frame rate of MJPEG on Streaming > Video Configuration is 6 or smaller.

  NOTE! Make sure SMTP configuration has been completed. Refer to section Mail of this chapter for further details.

- **Upload Image to SD Card**

  Select this item, and then the images will be uploaded to the SD card periodically. Note that to implement this function, one of the streaming MUST be set as MJPEG; otherwise, this function will be grayed out and cannot be accessed.

  The **Pre-trigger buffer** function can define how many images to be uploaded before the triggered moment. The **Post-trigger buffer** function can define how many images to be uploaded after the triggered moment.

  NOTE! Pre-trigger buffer generally ranges from 1 to 20 frames. However, the range will change accordingly if the frame rate of MJPEG on Streaming > Video Configuration is 6 or smaller.

  NOTE! Before implementing **Upload Image to SD Card**, please make sure that the SD Card is properly detected and installed. Refer to Storage Management > SD Card > Device Information for further details.

- **Send message by MxMessageSystem**
- Check this item and select a message to be send to the MxMessageSystem accordingly. If required add custom JSON parameters to the message.

File Name

Enter a file name in the blank, e.g. image.jpg. The uploaded image’s file name format can be set in this section. Please select the one that meets the requirements.

- **Add date/time suffix**

  File name: imageYYMMDD_HHNNSS_XX.jpg

  Y: Year, M: Month, D: Day

  H: Hour, N: Minute, S: Second

  X: Sequence Number

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

  File name: imageXXXXXXX.jpg

  X: Sequence Number

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

  File Name: imageXX.jpg

  X: Sequence Number

  NOTE! The file name suffix will end at the number being set. For example, if the setting is up to “10”, the file name will start from 00, end at 10, and then start all over again.

- **Overwrite**

  The original image in the FTP site will be overwritten by the new uploaded file with a static filename.

Save

Click on **Save** to save all the settings mentioned above.

Manual Trigger

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

With Manual Trigger setting, the current image(s) or video can be uploaded to the appointed destination, such as an FTP site or an E-mail address. The administrator can specify the triggered actions that will take when the users switch the Manual Trigger button to ON. All options are listed as follows.

Manual Trigger

The default setting for the Manual Trigger function is **Off**. Enable the function by selecting **On**. After the Manual Trigger function is enabled, click the Manual Trigger button on the Home page to start uploading data. Click again to stop uploading.

Triggered Action

The administrator can specify alarm actions that will take at an alarm occurrence. All options are listed as follows.

- **Enable Alarm Output (high/low)**

  Select these items to enable alarm relay outputs.

- **IR Cut Filter**

  Select the item and the IR cut filter (ICR) of the camera will be removed (on) or blocked (off) when alarm input is triggered. This function is only available for models with IR cut filter.

  NOTE! The IR Function (refer to section IR Function) could not be set as **Auto** mode if this triggered action is enabled.

- **Send Message by FTP/E-Mail**

  The administrator can select whether to send an alarm message by FTP and/or E-mail when an alarm is triggered.

- **Upload Image by FTP**

  Select this item and the administrator can assign an FTP site and configure various parameters. When the alarm is triggered, event images will be uploaded to the appointed FTP site. Note that to implement this function, one of the streaming MUST be set as MJPEG; otherwise, this function will be grayed out and cannot be accessed.

  The **Pre-trigger buffer** function allows users to check what happened to cause the trigger. The **Pre-trigger buffer** frame rate could be pre-determined. On the other hand, **Post-trigger buffer** is for users to upload certain amount of images after the alarm input is triggered.

  NOTE! Pre-trigger buffer generally ranges from 1 to 20 frames. However, the range will change accordingly if the frame rate of MJPEG on Streaming > Video Configuration is 6 or smaller.

  Check the box **Continue image upload** to upload the triggered images during certain time or keep uploading until the trigger is off. Select **Upload for __sec** and enter the duration in the blank. The images of the duration will be uploaded to FTP when the alarm input is triggered. The setting range is from 1 to 99999 sec. Select **Upload during the trigger active** to make the images keep being uploaded to FTP during the trigger active until the alarm is released. Set the Image frequency as the upload frame rate. The setting range is from 1 to 15 frames per second.

  NOTE! Make sure the FTP configuration has been completed. Refer to section FTP for further details.

- **Upload Image by E-Mail**

  Select this item and the administrator can assign an E-mail address and configure various parameters. When the alarm is triggered, event images will be sent to the appointed E-mail address. Note that to implement this function, one of the streaming MUST be set as MJPEG; otherwise, this function will be grayed out and cannot be accessed.

  The **Pre-trigger buffer** function allows users to check what happened to cause the trigger. The **Pre-trigger buffer** frame rate could be pre-determined. On the other hand, **Post-trigger buffer** is for users to upload certain amount of images after alarm input is triggered.

  NOTE! Pre-trigger buffer generally ranges from 1 to 20 frames. However, the range will change accordingly if the frame rate of MJPEG on Streaming > Video Configuration is 6 or smaller.

  Check the box **Continue image upload** to upload the triggered images during certain time or keep uploading until the trigger is off. Select **Upload for __sec** and enter the duration in the blank. The images of the duration will be uploading by E-mail when the alarm input is triggered. The setting range is from 1 to 99999 sec. Select **Upload during the trigger active** to make the images keep being uploaded to E-mail during the trigger active until the alarm is released. Set the Image frequency as the upload frame rate. The setting range is from 1 to 15 frames per second.

  NOTE! Make sure SMTP configuration has been completed. Please refer to section Mail for further details.

- **Send HTTP notification**

  Check this item, select the destination HTTP address, and specify the parameters for event notifications by **Alarm** triggered. When an alarm is triggered, the notification can be sent to the specified HTTP server.

  For instance, if the custom parameter is set as “action=1&group=2”, and the HTTP server name is “http://192.168.0.1/admin.php”, the notification will be sent to HTTP server as “http://192.168.0.1/admin.php? action=1&group=2” when alarm is triggered.

- **Send message by MxMessageSystem**
- Check this item and select a message to be send to the MxMessageSystem accordingly. If required add custom JSON parameters to the message.

- **Record Video Clip**

  Check the item and select a video recording storage type, **SD Card** or **NAS** (Network-Attached Storage). The alarm-triggered recording will be saved into the microSD/SD card or the NAS.

  The **Pre-trigger buffer** recording function allows users to check what caused the trigger. The pre-trigger buffer time range is from 1 to 3 sec. Select **Upload for __ sec** to set the recording duration after alarm is triggered. The setting range is from 1 to 99999 sec. Select **Upload during the trigger active** to record the triggered video until the trigger is off.

  NOTE! Please make sure the local recording (with microSD/SD card) or the remote recording (with NAS) is activated so that this function can be implemented. Refer to section Recording for further details.

File Name

Enter a file name in the File name field, ex. image.jpg. The uploaded image’s file name format can be set in this section. Please select the one that meets the requirements.

- **Add date/time suffix**

  File name: imageYYMMDD_HHNNSS_XX.jpg

  Y: Year, M: Month, D: Day

  H: Hour, N: Minute, S: Second

  X: Sequence Number

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

  File name: imageXXXXXXX.jpg

  X: Sequence Number

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

  File Name: imageXX.jpg

  X: Sequence Number

  NOTE! The file name suffix will end at the number being set. For example, if the setting is up to “10”, the file name will start from 00, end at 10, and then start all over again.

- **Overwrite**

  The original image in the FTP site will be overwritten by the new uploaded file with a static file-name.

Save

Click on **Save** to save all the settings mentioned above.

Audio Detection

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

Audio Detection function allows the camera to detect audio and trigger alarms when audio volume in the detected area reaches/exceeds the determined sensitivity threshold value.

NOTE! Audio Detection function is only available for models equipped with Audio I/O function.

Audio Detection

In Audio Detection Setting, the default setting for the Audio Detection function is **Off**. Enable the function by selecting **On**.

Audio Detection Setting

Users could adjust various parameters of Audio Detection in this section.

- **Detection level [1-100]:**

  The item is to set detection level for each sampling volume; the smaller the value, the more sensitive it is. The default level is 10.
- **Time interval (sec) [0-7200]:**

  The value is the interval between each detected audio. The default interval is 10.

Triggered Action

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

- **Enable Alarm Output (high/low)**

  Select these items to enable alarm relay outputs.
- **Send Alarm Message by FTP/E-Mail**

  The administrator can select whether to send an alarm message by FTP and/or E-mail when audio is detected.

- **Upload Image by FTP**

  Select this item and the administrator can assign an FTP site and configure various parameters. When audio is detected, event images will be uploaded to the appointed FTP site. Note that to implement this function, one of the streaming MUST be set as MJPEG; otherwise, this function will be grayed out and cannot be accessed.

  The **Pre-trigger buffer** function allows users to check what happened to cause the trigger. The **Pre-trigger buffer** frame rate could be pre-determined. On the other hand, **Post-trigger buffer** is for users to upload certain amount of images after audio event occurs.

  NOTE! Pre-trigger buffer generally ranges from 1 to 20 frames. However, the range will change accordingly if the frame rate of MJPEG on Streaming > Video Configuration is 6 or smaller.

  Check the box **Continue image upload** to upload the triggered images during certain time or keep uploading until the trigger is off. Select **Upload for __sec** and enter the duration in the blank. The images of the duration will be uploaded to FTP when the audio event occurs. The setting range is from 1 to 99999 sec. Select **Upload during the trigger active** to make the images keep being uploaded to FTP during the trigger active until the event stops. Set the Image frequency as the upload frame rate. The setting range is from 1 to 15 frames per second.

  NOTE! Make sure FTP configuration has been completed. Refer to section FTP for further details.

- **Upload Image by E-Mail**

  Select this item and the administrator can assign an E-mail address and configure various parameters. When audio is detected, event images will be sent to the appointed E-mail address. Note that to implement this function, one of the streaming MUST be set as MJPEG; otherwise, this function will be grayed out and cannot be accessed.

  The **Pre-trigger buffer** function allows users to check what happened to cause the trigger. The **Pre-trigger buffer** frame rate could be pre-determined. On the other hand, **Post-trigger buffer** is for users to upload certain amount of images after the audio event occurs.

  NOTE! Pre-trigger buffer generally ranges from 1 to 20 frames. However, the range will change accordingly if the frame rate of MJPEG on Streaming > Video Configuration is 6 or smaller.

  Check the box **Continue image upload** to upload the triggered images during certain time or keep uploading until the trigger is off. Select **Upload for __sec** and enter the duration in the blank. The images of the duration will be uploading by E-mail when the audio event occurs. The setting range is from 1 to 99999 sec. Select **Upload during the trigger active** to make the images keep being uploaded to E-mail during the trigger active until the event stops. Set the Image frequency as the upload frame rate. The setting range is from 1 to 15 frames per second.

  NOTE! Make sure SMTP configuration has been completed. Refer to section Mail for further details.

- **Send HTTP Notification**

  Check this item, select the destination HTTP address, and specify the parameters for event notifications by **Audio Detection** triggered. When an alarm is triggered, the notification can be sent to the specified HTTP server.

  For instance, if the custom parameter is set as “action=1&group=2”, and the HTTP server name is “http://192.168.0.1/admin.php”, the notification will be sent to HTTP server as “http://192.168.0.1/admin.php? action=1&group=2” when alarm is triggered.

- **Send message by MxMessageSystem**
- Check this item and select a message to be send to the MxMessageSystem accordingly. If required add custom JSON parameters to the message.

- **Record Video Clip**

  Check this item and select a video recording storage type, **SD Card** or **NAS** (Network-Attached Storage>. The Audio Detection recording will be stored in microSD/SD card or the NAS when audio is detected.

  The **Pre-trigger buffer** recording function allows users to check what happened to cause the trigger. The pre-trigger buffer time range is from 1 to 3 sec. Select **Upload for __ sec** to set the recording duration after audio is triggered. The setting range is from 1 to 99999 sec. Select **Upload during the trigger active** to record the triggered video until the trigger is off.

  NOTE! Please make sure the local recording (with microSD/SD card) or the remote recording (with NAS) is activated so that this function can be implemented. Refer to section Recording for further details.

File Name

Enter a file name in the blank, e.g. image.jpg. The uploaded image’s file name format can be set in this section. Please select the one that meets the requirements.

- **Add date/time suffix**

  File name: imageYYMMDD_HHNNSS_XX.jpg

  Y: Year, M: Month, D: Day

  H: Hour, N: Minute, S: Second

  X: Sequence Number
- **Add sequence number suffix (no maximum value)**

  File name: imageXXXXXXX.jpg

  X: Sequence Number
- **Add sequence number suffix up to # and then start over**

  File Name: imageXX.jpg

  X: Sequence Number

  NOTE! The file name suffix will end at the number being set. For example, if the setting is up to “10”, the file name will start from 00, end at 10, and then start all over again.
- **Overwrite**

  The original image in the FTP site will be overwritten by the new uploaded file with a static file-name.

Save

Please click on **Save** to save all the Audio Detection settings mentioned above.

Storage Management

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

Click on **Storage Management**, there will be a drop-down menu with tabs including **SD Card** and **Network Share**.

SD Card

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

Users can implement local recording to the microSD/SDHC/SDXC card up to 128GB. This page shows the capacity information of the microSD/SD card and a recording list with all the recording files saved on the memory card. Users can also format the microSD/SD card and implement automatic recording cleanup through the setting page.

To implement microSD/SD card recording, please go to the **Recording** page (refer to section Recording) for activation.

NOTE! Please format the microSD/SDHC/SDXC card when using it for the first time. Formatting will also be required when a memory card is being used on one camera and later transferred to another camera with different software platform.

It is not recommended to record with the microSD/SD card for 24/7 continuously, as it may not be able to support long term continuous data read/write. Please contact the manufacturer of the microSD/SD card for information regarding the reliability and the life expectancy.

Device Information

After the microSD/SD card is inserted into the camera, the card information such as memory capacity and status will be shown at **Device Information**.

Recording Source

Select a video stream to set as the recording source. The default format of the video stream is **Stream 1**. Select a preferred stream from the drop-down list and click on **Save** to apply the setting.

Recording Filename Format

Select a format as the recording filename format. The default recording filename format is **Start time only**. Select a preferred format from the drop-down list and click on **Save** to apply the setting.

Device Setting

Click on **Format** to format the memory card. Two filesystems are provided, **vfat (default)** and **ext4 (recommended)**. It is recommended to select **ext4** as the filesystem for steady and better performances.

Disk Cleanup Setting

Check **Enable automatic disk cleanup** and specify the time **1~999 day(s) or 1~142 week(s)** and storage limits **1~99% full** to configure disk cleanup settings. Click on **Save** to confirm the settings.

Recording List

Enter the period in the date fields and click on **Search**. Select **Video** / **JPEG**, and then each video/image file on the microSD/SD card will be listed in the recording list. The maximum file size is 60 MB/per file.

When the recording mode is set as **Always** (consecutive recording) and the microSD/SD card recording is also allowed to be enabled by events triggered, once events occur, the system will immediately implement events recording to the memory card. After the recording of the events are finished, the camera will return to the regular recording mode.

- **Remove**

  To remove a file, select the file first, and then click **Remove** button.

- **Sort**

  Click on **Sort**, and the files in the Recording list will be listed in name and date order.

  The capital letters A/M/N/T/S/R/V/U at the beginning of the name denotes the sort of the recording as listed below.

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

- **Download**

  To open/download a video clip/image, select the file first, and then click on **download** below the Recording list field. The selected file window will pop up. Click on the AVI/JPEG file to directly open the file or download it to a specified location.

Network Share (NAS)

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

Users can store the recording videos to a network share folder, or NAS (Network-Attached Storage). A NAS device is used for data storage and data sharing via network. This page displays the capacity information of the network device and a recording list with all the recording files saved on the net-

work device. Users can also format the NAS and implement automatic recording cleanup through the setting page.

Device Information

When a NAS is successfully installed, the device information such as the memory capacity and status will be shown at **Device Information**.

Storage Settings

The administrator can set the camera to send the alarm messages to a specific NAS site when an alarm is triggered. Enter the network device details, which include host (the IP of the NAS), share (the folder name of the NAS), user name, and password, in the fields.

Click on **Save** when finished.

Storage Tools

Click on **Format** to format the NAS.

Recording Source

Select a video stream to set as the recording source. The default format of the video stream is **Stream 1**. Select a preferred stream from the drop-down list and click on **Save** to apply the setting.

Recording Filename Format

Select a format to set as the recording filename format. The default recording filename format is **Start time only**. Select a preferred format from the drop-down list and click on **Save** to apply the setting.

Disk Cleanup Setting

Check **Enable automatic disk cleanup** and specify the time **1~999 day(s) or 1~142 week(s)** and storage limits **1~99% full** to configure disk cleanup settings. Click on **Save** to confirm the settings.

Recording List

Each video file on the Network Share will be listed in the Recording list. The maximum file size is 60 MB/per file.

When the recording mode is set as **Always** (consecutive recording) and the NAS recording is also allowed to be enabled by events triggered, once events occur, the system will immediately implement events recording to NAS. After the recording of the events are finished, the camera will return to the regular recording mode.

- **Remove**

  To remove a file, select the file first, and then click on **Remove**.

- **Sort**

  Click on **Sort**, and the files in the Recording list will be listed in name and date order.

  The capital letter A/M/N/T/S/R/V/U in the very beginning of name denotes the sort of the recording as below.

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

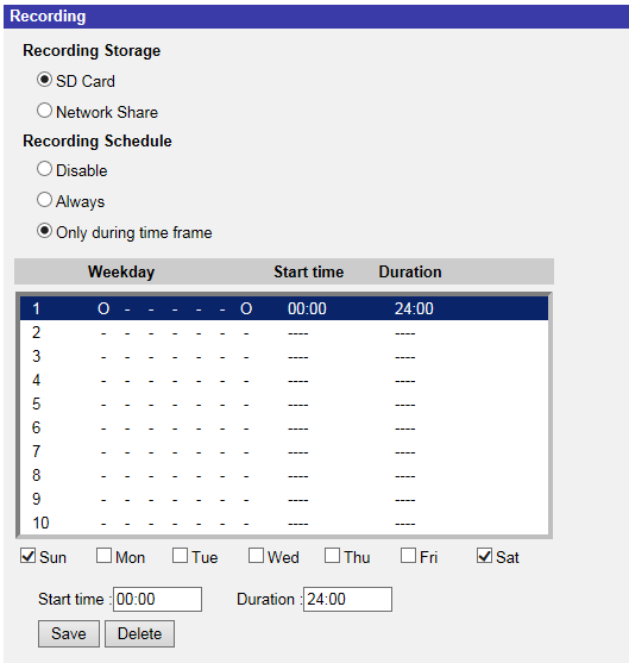
- **Download**

  To open/download a video clip, select the file first, and then click on **download** below the Recording list field. The selected file window will pop up. Click on the AVI file to directly play the video in the player or download it to a specified location.

Recording

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

In the **Recording** setting page, users can specify the recording schedule that fits the present surveillance requirement.



Recording Storage

Select a recording storage type, **SD Card** or **Network Share**.

Enable Recording Schedule

Two types of schedule mode are offered: **Always** and **Only during time frame**. Users can select **Always** to activate microSD/SD card or Network Share Recording all the time. Or, select a set of schedule from the time frame blank, check specific weekdays and setup the start time (hour:minute) and time period (hour:minute) to activate the recording at certain time frames. The setting range for the duration time is from 00:00 to 168:59. Please click on **Save** to save the setup.

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

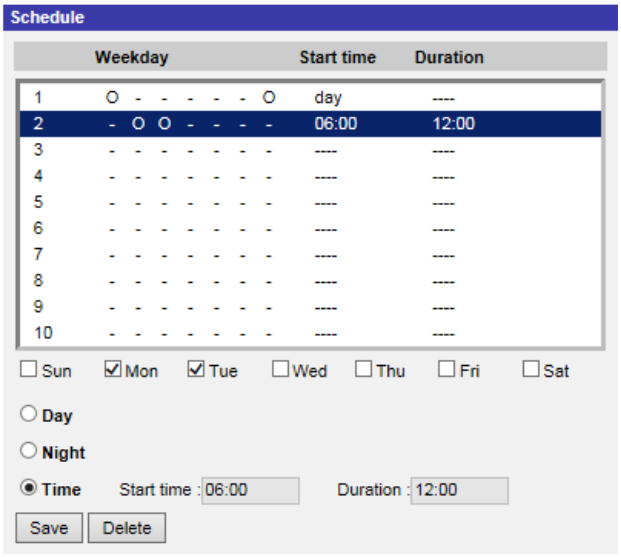
Disable Recording Schedule

- Select **Disable** to terminate the recording function.
- Click on **Save** when finished.

Schedule

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

This function allows users to setup schedules for features including: **Alarm Switch**, **Motion Detection** and **Network Failure Detection**. The function supports up to 10 sets of time frames in the time frame list.



Schedules Setup

1. Select a time frame from the time frame list.
2. Check the weekday boxes below to choose the specific weekdays.

3. Select a time mode, Day, Night or Time. Under Time mode, specify the start time (hour:minute) and the time duration (hour:minute) to activate the schedule triggered features. The setting range for the time duration is from 00:00 to 168:59.
4. Click on **Save** to save the setup. Alternatively, click on **Delete** to delete a chosen time frame.

Time Mode

- **Day**

  The camera profile will be loaded when IR cut filter is on.
- **Night**

  The camera profile will be loaded when IR cut filter is off.
- **Time**

  This indicates the start time and the time duration for the schedule.

  NOTE! Users MUST select **By schedule** under each feature setting page to enable the schedule function.

File Location (Snapshots and Web Recording)

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

Users can specify a storage location on the PC or in the hard drive for the snapshots and the live video recordings. The default setting is: C:\. Once the setting is confirmed, click on **Save**, and all the snapshots and the web recordings will be saved in the designate location.

NOTE! Make sure the selected file path contains valid characters such as letters and numbers.

NOTE! With Windows 7 operating system or above, to implement the Snapshot and Web Recording functions, users must run IE as administrator. To run IE as administrator, right click on the IE browser icon and select “Run As Administrator” to launch IE.

View Information

The View Information function can be found under this path: **System > View Information**.

Click on **View Information**, there will be a drop-down menu with tabs including **Log File**, **User Information**, and **Parameters**.

Log File

The Log File function can be found under this path: **System > View Information > Log File**.

Click on the tab to view the system log file. The camera keeps a record of the system’s behavior and information related to the camera. These log data can be exported for future use. Click **generate syslog** and the Save File As dialog window will pop up. The default file name is named after the model name and the MAC address as “Model Name-MAC-log.tgz”. Select the file destination and click **Save** to export the log data.

NOTE! “Save File As” dialog window may not show up immediately for the camera needs some time to process the log data.

User Information

The User Information function can be found under this path: **System > View Information > User Information**.

The administrator can view the privileges of each added user (refer to section Security) shown as below.

```
User: 1:1:0:1
```

- 1:1:0:1= I/O access: Camera control: Talk: Listen (refer to section Security)
- “1” denotes this user is allowed to access the function; whereas “0” suggests no access for this user is allowed.

Parameters

The Parameters function can be found under this path: **System > View Information > Parameter**.

Click on this item to view the parameter settings of the entire system, such as Camera Settings, Mask Information and Network Information.

Factory Default

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

Users can follow the instructions on this page to reset the camera to factory default settings if needed.

Full Restore

Click on **Full Restore** to recall the factory default settings. The camera system will restart in 30 seconds. The IP address will be restored to default. After the camera system is restarted, reconnect

the camera using the default IP address. The default IP address is 192.168.0.250.

Partial Restore

Click on **Partial Restore** to recall the factory default settings (excluding network settings). The camera system will restart in 30 seconds. Refresh the browser page after the camera system is restarted.

NOTE! The IP address will not be restored to default.

Reboot

Click on **Reboot** and the camera system will restart without changing the current settings. Refresh the browser page after the camera system is restarted.

Software Version

The Software Version can be found under this path: **System > Software Version**.

The current software version is displayed on the software version page.

Software Upgrade

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

NOTE! Make sure the upgrade software file is available before carrying out software upgrade.

The procedure of software upgrade is as below.

1. Click on **Browse** and locate the upgrade file, for example, “ulmage_userland”.

   NOTE! Do not change the name of the upgrade file, or the system will fail to find the file.

2. Pick a file type from the drop-down menu. In this case, select “ulmage+userland.img”.
3. Click on **Upgrade**. Then the system will prepare to start the software upgrade. Subsequently, an upgrade status bar will be displayed on the page to show the current upgrade process. After the upgrade process is finished, the viewer will return to the **Home** page.
4. Close the video browser.
5. Click on **Start** and activate the **Control Panel**. In the appeared window, double-click on **Add or Remove Programs**. A window with the **Currently install programs** list will pop up. In the list, select the viewer and click on <Remove> to uninstall the existing progam.
6. Open a new web browser and re-login the camera. Users will be prompted to download the viewer. Once the viewer is downloaded and installed, the live video will be available.

Maintenance

The Maintenance settings can be found under this path: **System > Maintenance**.

Users can export configuration files to a specified location and retrieve data by uploading the configuration file to the camera.

Export Files

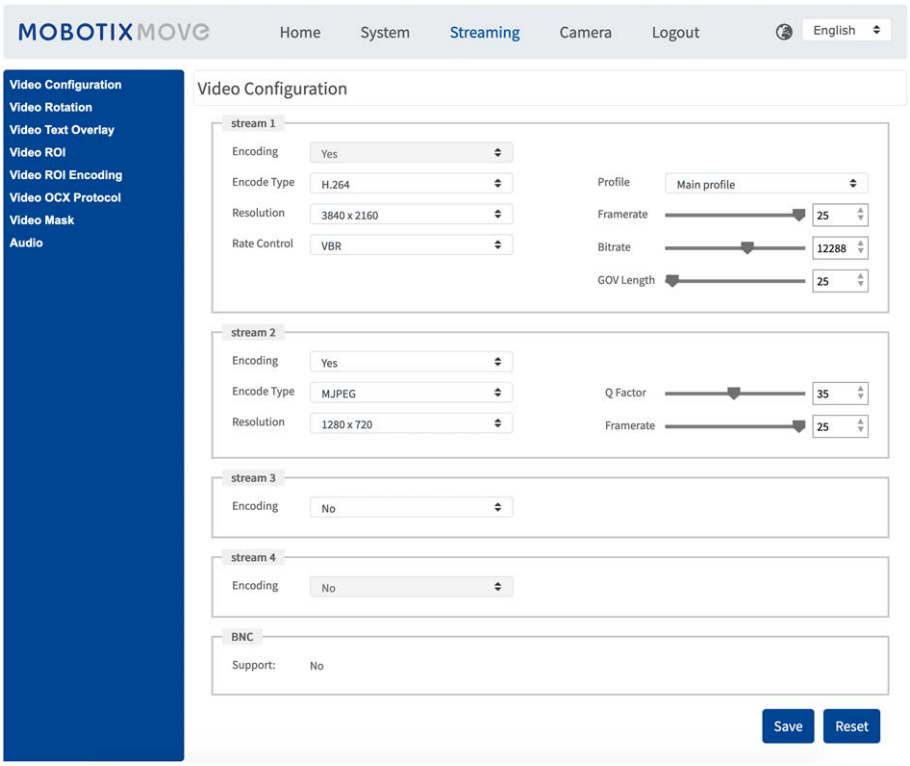
Users can save the system settings by exporting a configuration file (.bin) to a specified location for future use. Click on **Export**, and the popup File Download window will come out. Click on **Save** and specify a desired location for saving the configuration file.

Upload Files

To upload a configuration file to the camera, click on **Browse** to select the configuration file and then click on **Upload** for uploading.

The “Streaming” Tab

Under the tab **Streaming**, there are categories including: **Video Configuration**, **Video Rotation**, **Video Text Overlay**, **Video ROI**, **Video ROI Encoding**, **Video OCX Protocol**, **Video Mask**, and **Audio**.



In the **Streaming** submenu, the administrator can configure specific video resolution, video compression mode, video protocol, audio transmission mode, etc. Further details of these settings will be specified in the following sections.

NOTE! Only Administrator can access the **Streaming** configuration page.

Video Configuration

The Video Configuration setting can be found under this path: **Streaming > Video Configuration**.

Encoding

Select **Yes** from the drop-down menu to enable Stream 2~Stream 4 encoding. Or select **No** to disable the streaming encoding.

Encode Type

The available video resolution formats include H.265, H.264, and MJPEG. Users can select the preferred encode type from the drop-down menu.

Resolution

Video format and resolution combination will vary by users’ configuration. The following lists the default resolution of different IP camera models.

Framerate

Video framerate is for setting the frames per second (fps) if necessary.

- 5MP Vandal Bullet Analytics Camera

  The default setting of Stream 1 is 30 fps (NTSC) or 25 fps (PAL). The maximum frame rate range of each stream will change according to the selected video resolution.

NOTE! Low framerate will decrease video smoothness.

Profile

Users can set H.265/H.264 Profile to **High Profile** or **Main Profile** according to its compression needs. With the same bit rate, the higher the compression ratio, the better the image quality is. The default setting is **Main Profile**.

NOTE! Please make sure the higher compression ratio is supported by the system before setup.

Rate Control

There are three kinds of H.265/H.264 bit rate modes provided: CBR (Constant Bit Rate), VBR (Variable Bit Rate) and LBR (Low Bit Rate).

- **CBR**

  The sent-out video bitrate will be fixed and consistent to maintain the bandwidth.

- **VBR**

  Video bitrate varies according to the activity of the monitoring environment to achieve better image quality.

- **LBR**

  LBR keeps low bitrate and ensures superior image quality. To implement LBR control, setup the compression level and dynamic GOV for each streaming accordingly beforehand.

  - **Compression**

    Based on the current application area and streaming bitrate, select the most suitable compression level, high/mid/low.

    - Set **High**, and bitrate will vastly be reduced; however, image quality may be degraded at the same time.
    - Set **Low**, and bitrate will stably keep low while image quality remains high.

  - **Dynamic GOV**

    According to the amount of motion in the application area, the GOV length of the video will be adjusted dynamically to reduce more bitrate, especially for scenes with minor changes. The length of Dynamic GOV is from **GOV Length** to **Max. GOV** (4094).

    - Select **Enabled** and set **Max. GOV**. Then, click on **Save** to activate the setting.
    - If there is small or zero activity in the scene, set **Max. GOV** larger, the GOV length will be longer, resulting in lower bitrate and bandwidth.
    - If there are constant dynamic changes in the scene, it is suggested just adjust **GOV Length** and disable **Dynamic GOV**.

Click on **Save** to confirm the setting.

Bitrate

- 5MP Vandal Bullet Analytics Camera

  The default setting of the H.265/H.264 bitrate for Stream 1 is 12288 kbit/s; for Stream 2 is 4096 kbit/s; for Stream 3/ Stream 4 is 2048 kbit/s. The setting range is from 64 to 20480 kbps, and the total bit rate should not exceed 51200 kbps.

GOV Length

Users can set the GOV length to determine the frame structure (I-frames and P-frames) in a video stream to save bandwidth. Less bandwidth is needed if the GOV length is set to a high value. However, the shorter the GOV length, the better the video quality is.

- 5MP Vandal Bullet Analytics Camera

  The default setting for Stream 1 ~ Stream 4 is 25. The setting range of the GOV length is from 1 to 4094.

Q (Quality) Factor (MJPEG Only)

The default setting of MJPEG Q factor is 35; the setting range is from 1 to 70.

Video Rotation

Rotate Function

Users can change video display type if necessary. Selectable video rotate types include Mirror video and 90/180/270 degree clockwise rotate. Refer to the following descriptions for the different video rotate type.

- **Mirror**

  Select **yes** from the drop-down menu, and the image will be rotated horizontally.
- **Rotate Type**

  Users can choose 0, 90, 180, or 270 degree from the drop-down menu to rotate the image.

Click on **Save** to confirm the setting.

Video Text Overlay

Users can select the items to display data including date & time/text string/subtitle/image on the live video pane.

Overlay Type

Users can select at most three items out of four options including date & time/text string/sub-title/image to display on the live video pane.

- **Include Date & Time**

  Check the box to enable date & time display on the Live Video Pane and a Video Text Overlay Window will show up. Move the mouse cursor to the center of the window then click and drag the window to preferred display position. Users can choose to display date, time, or date & time from the drop-down menu, and decide the string align position (left/right).
- **Include Text String**

  Check the box to enable text string display on the Live Video Pane and a Video Text Overlay Window will show up. Move the mouse cursor to the center of the window then click and drag the window to preferred display position. Type the text to display in the entry field and decide the string align position (left/right). The maximum length of the text string is 15 alphanumeric characters.

- **Include Subtitle**

  Check the box to enable subtitle display on the Live Video Pane and a Video Text Overlay Window will show up. Move the mouse cursor to the center of the window then click and drag the window to preferred display position. Type the text to display in the entry field and decide the string align position (left/right). Users can set at most 5 subtitles, and the maximum length of each subtitle is 16 alphanumeric characters.

- **Include Image**

  Check the box to enable image display on the Live Video Pane and a Video Text Overlay Window will show up. Move the mouse cursor to the center of the window, click and drag the window to preferred display position, and then decide the string align position (left/right).

Click on **Set** to confirm the setting.

Text Overlay Setting

Users can choose the Text Overlay Color (black, white, yellow, red, green, blue, cyan, or magenta) and Text Overlay Size (small, medium, or large) of the display date & time/text string/subtitle.

Click on **Set** to confirm the setting.

Image Overlay Setting

Users can upload an image and set its transparency to display on the live video pane. The setting range of image transparency is from 0 to 255; the lower the value, the more transparent it is. Users must save the image as a 8-bit BMP file; the length should be the multiple of 32, and the width should be the multiple of 4. The maximum resolution of the image should not exceed 32768 pixels.

Click on **Set** and **Upload** to confirm the setting.

Video ROI

The Video ROI setting can be found under this path: **Streaming > Video ROI**.

ROI stands for Region of Interest. This function allows users to select specific monitoring region for Stream 1~Stream 4, instead of showing the full image.

NOTE! To use ROI function, dual streaming or above must be enabled and the resolution of each streaming must be different.

Enable Stream 1~ Stream 4 ROI Setting

Check the boxes and Stream 1~ Stream 4 ROI Window will be displayed. Note that video ROI is NOT available for the streaming set as the highest resolution among the enabled streaming. To adjust the ROI Window, click and drag the edge of the window outward/inward. To shift the window to the intended location, click the center of the ROI Window and drag the mouse cursor. Then, click **Save** to apply the setting.

Video ROI Encoding

The Video ROI Encoding setting can be found under this path: **Streaming > Video ROI Encoding**.

Video ROI Encoding is to set the compression of the selected zone within ROI for better performances; at most three zones can be set in the interested region. However, this function does NOT support MJPEG video format.

The following shows how to setup Video ROI Encoding. To implement this function, Video ROI must be setup beforehand.

- Select a video stream from **Video Stream**.
- Select **Enable** from **ROI Encoding** to implement ROI Encoding.
- Click on **Add**, click and drag the center of the window to move it to the interested location; click and drag the edge of the window outward/inward to resize the window.

  NOTE! The total size of the three windows CANNOT be larger than the half size of the ROI. When exceeds, a warning window will pop up.

- Choose the quality of the setting zone from **Quality**.

  The higher the value, the better the image quality (higher bitrate) of the setting zone will be. On the contrary, the lower the value, the lower the image quality (lower bitrate) of the selected area will be.
- Click on **Save** to apply the setting.

Video OCX Protocol

The Video OCX Protocol setting can be found under this path: **Streaming > Video OCX Protocol**.

In the **Video OCX protocol** setting page, the administrator can select RTP over UDP, RTP over RTSP (TCP), RTSP over HTTP or MJPEG over HTTP, for streaming media over the network. In the case of multicast networking, users can select the Multicast mode. Click on **Save** to confirm the setting.

Video OCX protocol setting options include:

- **RTP over UDP/RTP over RTSP(TCP) / RTSP over HTTP/MJPEG over HTTP**
- **Multicast Mode**

  Enter all required data, including **Multicast Stream 1~4 Video Address/ Multicast Stream Audio Address**, **Multicast Port** and **Multicast TTL** into each blank.

Click on **Save** to confirm the setting.

Video Mask

The Video Mask setting can be found under this path: **Streaming > Video Mask**.

Active Mask Function

- **Add a Mask**

  Check a Video Mask checkbox, and a red frame will come out in the Live Video pane. Use the mouse to drag and drop to adjust the mask’s size and place it on the target zone. At most 5 video masks can be set.

  NOTE! It is suggested to set the Video Mask slightly bigger than the object.

- **Cancel a Mask**

  Un-check the Video Mask checkbox meant to be deleted; the mask will disappear from the Live Video pane instantly.

Mask Setting

- **Mask color**

  The selections of Mask color include black, white, yellow, red, green, blue, cyan, and magenta. Click on **Save** to confirm the setting.

Audio (Audio Mode and Bit Rate Settings)

The Audio Mode setting can be found under this path: **Streaming > Audio**.

In this page, the administrator can adjust the sound transmission mode, the audio gain levels and the audio bit rate. Setting for enabling sound recording to the microSD/SD card is also available.

Transmission Mode

- **Full-duplex (Talk and Listen simultaneously)**

  In the Full-duplex mode, the local and remote sites can communicate with each other simultaneously, i.e. both sites can speak and listen to the other side at the same time.

- **Half-duplex (Talk or Listen, not at the same time)**

  In the Half-duplex mode, the local/remote site can only talk or listen to the other site at a time.

- **Simplex (Talk only)**

  In the Talk only Simplex mode, the local/remote site can only talk to the other site.

- **Simplex (Listen only)**

  In the Listen only Simplex mode, the local/remote site can only listen to the other site.

- **Disable**

  Select the item to turn off the audio transmission function.

Server Gain Setting

Set the audio input/output gain levels for the sound amplification. The audio input gain value is adjustable from 1 to 10. The audio output gain value is adjustable from 1 to 6. The sound will be turned off if the audio gain is set to “Mute”.

Bit Rate

Selectable audio transmission bit rate include 16 kbps, 24 kbps, 32 kbps, 40 kbps, uLAW (64 kbps), ALAW (64 kbps), AAC (128 kbps), PCM (128 kbps), PCM (256 kbps), PCM (384 kbps), and PCM (768 kbps). Higher bit rate will let higher audio quality and require bigger bandwidth. Click on **Save** to confirm the setting.

Input Type

Selectable input types are **Line in** and **External Mic**. If the audio input is from the audio device connected via the Audio In connecters, users should select “Line in”. If the audio input is from the microphone connected via the Audio In connecters, users should select “External Mic” for better sound quality. Click on **Save** to confirm the setting.

Recording to Storage

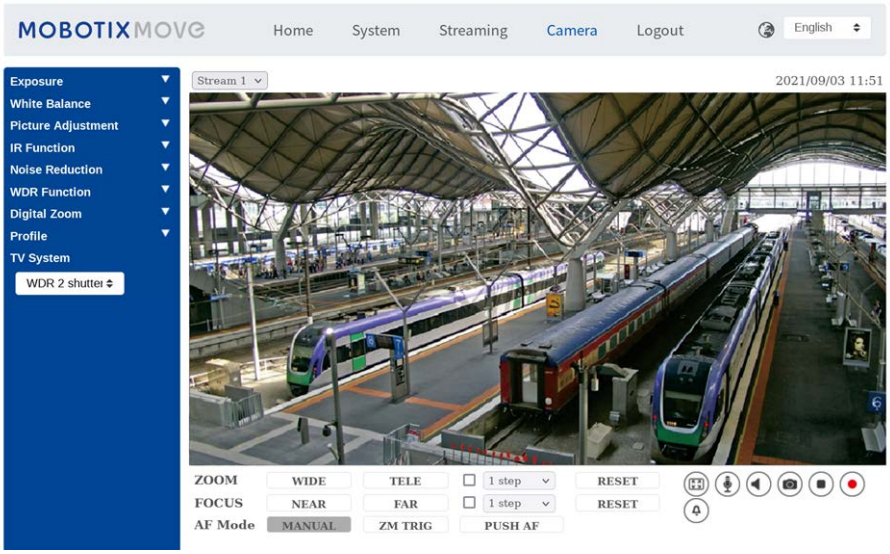
Select **Enable** from the drop-down menu to enable audio recording with videos into the microSD/SD card or the NAS.

NOTE! If the chosen bit rate is not compatible with the player, there will only be noise instead of audio during playback.

Click on **Save** to confirm the setting.

The “Camera” Tab

Under the tab **Camera**, there are submenus including: **Exposure**, **White Balance**, **Picture Adjustment**, **IR Function**, **Noise Reduction**, **WDR Function**, **Digital Zoom**, **Backlight**, **Profile**, and **TV System**.



Exposure

The Exposure setting can be found under this path: **Camera > Exposure**.

Exposure is the amount of light received by the image sensor. It is determined by the width of lens diaphragm opening, the shutter speed and other exposure parameters. With these items, users can define how the Auto Exposure function works. Users can select one of the exposure modes according to the operating environment. Each exposure mode is specified as follows.

Auto Mode

- **Max Gain**

  Maximum Gain can be set to reduce image noises. The Max Gain ranges from 3dB to 48dB, or select **Off** to disable the function. The default setting is 48dB.

- P-Iris Priority Mode

  P-iris priority mode is only available for Zoom Lens and Motorized Lens models. In addition, applied with different lens, the related setting options also vary. Refer to the following for further details.

  - Motorized Lens

    Click on , and the camera will automatically detect the best iris size for the environment. If necessary, users can select and manually to adjust the iris size. Alternatively, click on to reset the iris size, and the iris size will be set to the largest. Then, users can manually adjust the iris size by selecting and . The minimum shutter speed can be set from 1/500 to 1 sec. (NTSC) or 1/425 to 1/1.5 sec. (PAL).

Manual Mode

With this mode, users can select the suitable shutter speed, iris size and gain value according to the environmental illumination.The shutter speed ranges from 1/10000 to 1 sec. (NTSC) or from 1/10000 to 1/1.5 sec. (PAL)

The range of the iris size is from 0 to 9, or select **Full open** to fully open the iris. The gain value range is from 3 dB to 48 dB, or select **Off** to disable the function.

NOTE! The **Iris Size** setting is only available for models with Zoom Lens.

NOTE! The **Gain** setting is not available for Box Camera. Note that for Motorized Lens models, the iris size setting differs. To set the iris size, click on , and the camera will auto detect the best iris size for the environment. If necessary, users still can manually adjust the iris size by selecting and . Alternatively, click on to reset the iris size. The iris size will be set to the largest. Then, users can manually adjust the iris size by selecting and .

White Balance

The White Balance setting can be found under this path: **Camera > White Balance**.

A camera needs to find reference color temperature, which is a way of measuring the quality of a light source, for calculating all the other colors. The unit for measuring this ratio is in degree Kelvin (K). Users can select one of the White Balance Control modes according to the operating environment. The following table shows the color temperature of some light sources for reference.

Light Sources	Color Temperature in K
Cloudy Sky	6,000 to 8,000
Noon Sun and Clear Sky	6,500
Household Lighting	2,500 to 3,000
75-watt Bulb	2,820
Candle Flame	1,200 to 1,500

AWB.normal

The AWB (Auto White Balance).normal mode is suitable for environments with light source having color temperature in the range roughly from 2700K to 7800K.

AWB.wide

With AWB (Auto White Balance).wide function, the white balance in a scene will be automatically adjusted while temperature color is changing. The ATW Mode is suitable for environments with light source having color temperature in the range roughly from 2500K to 10000K.

AWB.all

The AWB (Auto White Balance).all mode is suitable for environments with light source having color temperature under 2500K or over 10000K.

Smart Mode

The Smart mode is suitable for environments with one single background color which is strongly saturated, for instance, in a forest.

One Push

With One Push function, white balance is adjusted and fixed according to the scene the camera sees at the moment. This function is best for situations with minimal scene changes and continuous lighting. The function is suitable for light sources with any kind of color temperature. Follow the steps below to set the white balance.

- Point the camera to the monitoring area.
- Select **One Push** in the White Balance setting menu
- Click the button to adjust the color tone of the live images.

  In this mode, the value of white balance will not change as the scene or the light source varies. Therefore, users might have to re-adjust the white balance by clicking the button again when needed.

Smart Touch Mode

With Smart Touch function, users can select an area in the camera scene as the reference point for white balance. Please ensure that the background color of the selected area is white. Smart Touch function is suitable for environments with unchanged brightness level.

Manual Mode

In this mode, users can manually adjust the White Balance value. Input a number between 0 to 249 for “Rgain/Bgain” to adjust the red/blue illuminant on the Live Video Pane. The following describes several situations that might occur during the White Balance manual adjustment.

- The video image turns reddish (as the left picture below).

  The higher the Rgain value, the redder the image will be. To solve the problem, reduce the Rgain value, and the video image will turn less reddish.

Reddish Image

Corrected White Balance

- The video image turns greenish (as the left picture below).

  The lower the Rgain value, the greener the image will be. To solve the problem, Increase the Rgain value, and the video image will turn less greenish.

Greenish Image

Corrected White Balance

- The video image turns bluish (as the left picture below).

  The higher the Bgain value, the bluer the image will be. To solve the problem, reduce the Bgain value, and the video image will turn less bluish.

Bluish Image

Corrected White Balance

- The video image turns yellowish (as the left picture below).

  The lower the Bgain value, the yellower the image will be. To solve the problem, Increase the Bgain value, and the video image will turn less yellowish.

Yellowish Image

Corrected White Balance

The following image displays the general color shifts of the scene when different Rgain/Bgain combinations are applied.

Picture Adjustment

The Picture Adjustment setting can be found under this path: **Camera > Picture Adjustment**.

Brightness

The brightness level of the images is adjustable from -12 to +13. The default value is 0.

Sharpness

The sharpness level of the images is adjustable from +0 to +15. The edge of the objects is enhanced as the sharpness level increases. The default value is +4.

Contrast

The contrast level of the images is adjustable from -6 to +19. The default value is 0.

Saturation

The saturation level of the images is adjustable from -6 to +19. The default value is 0.

Hue

The hue level of the images is adjustable from -12 to +13. The default value is 0.

IR Function

The IR Function setting can be found under this path: **Camera > IR Function**.

NOTE! This function is ONLY available for models with IR function.

Day/Night Function

This item is for users to define the action of the IR cut filter and IR LED lights. Refer to the descriptions of each option below to select a suitable mode.

- **Auto Mode**

  With this mode, the camera can decide the occasion to remove the IR cut filter. Please refer to IR Function: Day/Night Threshold for further details.

- **Night Mode**

  Use this mode when the environment light level is low. The IR cut filter will be removed to allow the camera to deliver clear images in black and white.

- **Day Mode**

  Select this mode to turn on the IR cut filter. The IR cut filter can filter out the IR light and allows the camera to deliver high quality images in color.

- **Smart Mode**

  With Smart mode, the camera will decide the occasion to remove the IR cut filter. The Smart mode mechanism can judge whether the main light source is from IR illumination. If so, the IR cut filter will be kept removed (i.e. monochrome/night mode).

  NOTE! It is recommended to select “Smart Mode” when the camera sets high zoom ratio for close-up view.

- **Light Sensor Mode (Default)**

  In this mode, for cameras with built-in IR LED modules, the light sensor will decide the occasion to turn the IR LED lights on/off. For cameras with non-IR modules, the light sensor will decide the occasion to take the IR cut filter on/off.

- **Light On Mode (Built-in IR LED Modules Only)**
  In this mode, IR LED lights will always be on.
- **Light Off Mode (Built-in IR LED Modules Only)**
  In this mode, IR LED lights will always be off.

Day/Night Threshold

This item is for users to set when the camera should switch from day mode to night mode or vice versa. The camera will sense the surrounding brightness, and the threshold value stands for the level of the light. Once the camera detects the light level reaches the set threshold, the camera will automatically switch to Day/Night Mode. The range of the level is from 0 to 10, (darker = 0; brighter = 10).

- **Night Mode to Day Mode**
  The lower the value, the earlier the camera switches to Day mode. The default value is 7.
- **Day Mode to Night Mode**
  The higher the value, the earlier the camera switches to Night mode. The default value is 3.

  NOTE! Equipped with different CMOS sensors, the time the camera switches to Day/Night mode may also vary from models to models even if the threshold is set to the same value.

IR Light Compensation

With the IR Light Compensation function, the camera can prevent the center object close to the camera from being too bright when IR LED lights are turned on.

Noise Reduction

The Noise Reduction setting can be found under this path: **Camera > Noise Reduction**.

The camera provides multiple **Noise Reduction** options for delivering optimized image quality especially in extra low-light conditions.

3DNR

3DNR (3D Noise Reduction) function delivers optimized image quality especially in extra low-light conditions.

Different levels of 3DNR are provided, including 3DNR Low, 3DNR Mid and 3DNR High. Higher level of 3DNR generates relatively enhanced noise reduction.

2DNR

2DNR (2D Noise Reduction) function delivers clear images without motion blurs in extra low-light conditions.

Select **on** to turn on 2DNR function; otherwise, select **off** to turn off 2DNR function.

ColorNR

In a dark or insufficient light environment and the camera is under color mode, ColorNR (Color Noise Reduction) can eliminate color noise.

Three levels of ColorNR, including Color Low, Color Mid and Color High, are provided. The higher level of ColorNR generates relatively enhanced noise reduction.

WDR Function

The WDR Function setting can be found under this path: **Camera > WDR Function**.

The Wide Dynamic Range (WDR) function is for solving high contrast or changing light issues to enhance video display quality. Different level options for WDR include Low, Mid and Hi. Higher level of WDR represents wider dynamic range, so that the camera can catch a greater scale of brightness.

Digital Zoom

The Digital Zoom setting can be found under this path: **Camera > Digital Zoom**.

The digital zoom of the camera is adjustable from x2 to x10.

NOTE! This function is NOT available for hemispheric camera models.

Backlight

The Backlight setting can be found under this path: **Camera > Backlight**. Backlight function is NOT available when TV system is set as “WDR 2 Shutter”.

The Backlight Compensation function prevents the center object from being too dark in surroundings where excessive light is behind the center object. Select **on** to turn on the function; otherwise, select **off** to turn off the function.

Profile

The Camera Profile setting can be found under this path: **Camera > Profile**.

Camera Profile allows users to setup the desired image parameters for specific environments with different time schedules. Users can setup at most 10 sets of camera parameter configuration under the

Camera tab. To enable this function, users must setup the schedules in advance. Refer to section Schedule for further details of schedule setup. Then, follow the steps below to setup a camera profile.

Camera Profile Setup

1. In the “Camera” tab, setup the camera parameters, such as White Balance, Picture Adjustment, etc., excluding TV System.
2. Click on Profile and its setting menu will be displayed. Select a number from the Num drop-down menu.
3. Input a name for the profile in the Name field.
4. Click on below the Name field. The camera configuration is saved and applied to the profile. Now a camera profile is created and saved.
5. Select a profile from the Num drop-down menu.
6. Tick the By schedule box. Check the desired schedule(s) from the Schedule drop-down menu. Multiple schedules can be applied to one profile.
7. Click on below **By schedule**.
8. Follow the steps above to set the rest of the profiles.

Now, the camera will automatically switch profiles according to the schedule. Alternatively, manually select a number from the Num drop-down menu. Then, click on , the camera will load and apply the setting of the profile.

NOTE! If users wish to set the camera parameters to factory default setting, select **Normal** from the Num drop-down menu. The camera will start loading the default values.

NOTE! Users MUST set the camera parameter of the last profile as the default setting. Thus, if there are gaps among schedules, the camera will apply the setting of the last profile.

TV System

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

Select the video format that matches the present TV system from the drop-down menu. The following table shows the available video formats for different types of models. The supported video formats for each model are marked by “v”.

The “Logout” Tab

Click on the tab **Logout** on the top of the page, and the login window will pop up. This enables login with a different username.

Appendix A: Installing UPnP Components

Please follow the instructions below to install UPnP components on Windows computers.

1. In Windows, go to **Start**, click on **Control Panel**, and then double-click on **Add or Remove Programs**.
2. Click on **Add/Remove Windows Components** in the **Add or Remove Programs** page.
3. Select **Networking Services** from the Components list in Components Wizard window of the Windows, and then click **Details**.
4. Select **UPnP User Interface** in the Networking Services’ subcomponents list and then click on **OK**.
5. Click on **Next** in the Windows Components Wizard window.
6. Click on **Finish** to complete installation.

Appendix B: Converting IP Addresses from Decimal to Binary

Follow the example below to convert the IP addresses to binary numbers. Use the calculator on the computer for conversion. The calculator can be found under this path: **Start > All Programs > Accessories > Calculator**. For Windows XP and Windows Vista, click **View** on the calculator and click **Scientific**. For Windows 7 and Windows 8, click **View** on the calculator and click **Programmer**. Then follow the steps in the following example to convert the IP addresses.

The example below shows how to convert 192.168.2.81 to binary numbers.

1. On the left of the calculator, select **Dec**. Then enter the first decimal number of the IP address, “192”. Select **Bin** and the number will be converted to binary number. Repeat the same procedure with the rest of decimal numbers. Remember to select **Dec** before entering the next decimal number. Otherwise a decimal number cannot be entered. The table below shows the binary number of each decimal number.

Decimal Numbers	Binary Numbers
192	11000000
168	10101000
2	10
81	1010001

2. Each binary number should have eight digits. If a binary number does not have eight digits, please add 0 in front of it until it does. The binary number of each decimal number should be as follow.

Decimal Numbers	Binary Numbers
192	11000000
168	10101000
2	00000010
81	01010001

Therefore, the binary numbers of IP address 192.168.2.81 is 11000000.10101000.00000010.01010001.

7

Technical Support Information

This section contains the following information:

Setup Internet Security **108**

Technical Specifications **109**

Setup Internet Security

If ActiveX control installation is blocked, please either set Internet security level to default or change ActiveX controls and plug-ins settings.

Internet Security Level: Default

1. Start the Internet Explorer (IE).
2. Click on the **Tools** tab on the menu bar and select **Internet Options**.
3. Click on the **Security** tab, and select **Internet** zone.
4. Down the page, click on the **Default Level** button and click on **OK** to confirm the setting. Close the browser window, and restart a new one later to access the IP camera.

ActiveX Controls and Plug-ins Settings

1. Repeat **Step 1 to Step 3** of the previous section above.
2. Down the page, click on the **Custom Level** button to change ActiveX controls and plug-ins settings. The Security Settings window will pop up.
3. Under **ActiveX controls and plug-ins**, set **ALL** items (as listed below) to **Enable** or **Prompt**. Please note that the items vary by IE version.

ActiveX Controls and Plug-In Settings

- Binary and script behaviors.
- Download signed ActiveX controls.
- Download unsigned ActiveX controls.
- Allow previously unused ActiveX controls to run without prompt.
- Allow Scriptlets.
- Automatic prompting for ActiveX controls.
- Initialize and script ActiveX controls not marked as safe for scripting.
- Run ActiveX controls and plug-ins.
- Only allow approved domains to use ActiveX without prompt.
- Script ActiveX controls marked safe for scripting*.
- Display video and animation on a webpage that does not use external media player.

NOTE! These items may vary according to the IE version used.

4. Click on **OK** to accept the settings. A prompt window will appear for confirming the setting changes, click **Yes** to close the Security Settings window.
5. Click on **OK** to close the Internet Options screen.
6. Close the browser window, and restart a new one later to access the IP camera.

Technical Specifications

Product Information

Product Name	5MP Vandal Bullet Analytics Camera
Order Code	Mx-VB2A-5-IR-VA

Image Quality

Image Sensor	5MP, 1/2.7“ Progressive CMOS
Effective (Used) Pixels	H x V = 2720x1976 (5MP)
Pixel Size	2.0 µm
Frame Rate (maximum)	**WDR on:** H.265/H.264: 2688x1944 @30 fps + 1024x768 @30 fps H.265/H.264: 2592x1944 @30 fps + 1280x720 @30 fps H.265/H.264: 2688x1512 @30 fps + 1280x1024 @30 fps H.265/H.264: 1920x1080 @30 fps + 1920x1080 @30 fps MJPEG: 1080p @30 fps **WDR off:** H.265/H.264: 2688x1944 @30 fps + 1024x768 @30 fps H.265/H.264: 2592x1944 @30 fps + 1280x720 @30 fps H.265/H.264: 2688x1512 @30 fps + 1280x1024 @30 fps H.265/H.264: 1920x1080 @60 fps + 1280x1024 @44 fps H.265/H.264: 1920x1080 @60 fps + 1280x720 @60 fps Stream 1 (main stream) with resolutions below 1920x1080 can support 2 streams @60 fps MJPEG: 1080p @60 fps
Front Glass Coating	Superhydrophilic MOBOTIX EverClear nano coating transforms water droplets into an ultra-thin water film upon impact. The coating ensures best image quality in rain and difficult external conditions and it reduces reflections and noise in low-light scenarios. EverClear is dirt-repellent and increases the stability as well as the scratch-resistance of the front glass, further reducing maintenance efforts. Coating endurance up to 3 years depending on environmental conditions and cleaning treatment.

Lens

Minimum Illumination	Color: 0.08 lux B/W: 0.008 lux
Lens Characteristics	Motorized Lens: Zoom, Focus, P-IRIS Focal Length: 2.7 to 12 mm Aperture: F1.6 to F2.9 Horizontal Field of View: 96.76° (Wide), 34.13° (Tele) Vertical Field of View: 52.21° (Wide), 19.24° (Tele)

Camera

Day/Night	Automatic mechanically switchable IR-cut filter
Shutter Time	**Automatic Mode:** Up to 1/10000 s
WDR	Up to 130 dB Multi Exposure WDR & HDR Engine support
Zoom	Optical: 4.4x, Digital 10x
Image settings	Color, Brightness, Sharpness, Contrast White Balance, Exposure Control 2DNR, 3DNR, NR by Motion Masking, Text Overlay
Corridor Mode	90°, 180°, 270° Rotation

Video Codec

Compression/Encoding	H.265/H.264/MJPEG
Streaming	Up to 4 individually configurable streams in H.264/H.265/MJPEG Configurable resolution/frame rate/bandwidth LBR/VBR/CBR in H.265/H.264

Audio Codec

Compression/Encoding	G.711/G.726/AAC/LPCM
Streaming	2-Way, bidirectional
Audio Input	Line In: Max 6.2 Vpp Signal In, Input Impedance: 33 kΩ
Audio Output	Line Out: 1 Vrms Signal Out, Output Resistance: 200 Ω

Network

Interface	10/100 Mbps Ethernet
Security	User Authentication/HTTPS/IP Filter/IEEE 802.1x
Supported Protocols	iARP, PPPoE, IPv4/v6, ICMP, IGMP, QoS, TCP, UDP, DHCP, UPnP, SNMP, SMTP, RTP, RTSP, HTTP, HTTPS, FTP, NTP, DDNS, SMBv2
ONVIF conformance	Supports profiles S/G/T
Supported Browsers	Microsoft Internet Explorer 10 or higher, Google Chrome, Mozilla Firefox, Apple Safari; Microsoft Internet Explorer with ActiveX is recommended for best performance and H.265 support

System Integration

Base Video Analytics	■ Motion Detection ■ Tampering ■ Audio noise Detection (ext. microphone required)
Enhanced Video Analytics (embedded)	■ Abandoned objects ■ Intrusion ■ Sabotage ■ Wrong direction ■ Loitering ■ Object count ■ Object removal 2 analytics functions can be activated simultaneously
Event Triggers	■ External input ■ Analytics ■ Network failure detection ■ Periodical event ■ Manual trigger
Event Actions	■ External output activation ■ Video and audio recording to edge storage ■ File upload: FTP, network share and email ■ Notification: HTTP, FTP, email

General

Casing	Metal Back Housing, PC Front
Device Color	PC front cover: RAL9003 Sunshield: ■ Logo color: Pantone 286C and Pantone Gray 6 Cu ■ Body color: RAL9003 ■ Back metal body: RAL9003
Power	PoE IEEE802.3af, class 0, max. 13 W 12 V DC, max. 13 W 24 V AC, max. 14 W (25 VA)
Connectors	RJ45, Alarm in x2, Alarm out x1, 12 VDC Terminal Block, 24 VAC Terminal Block, Audio in 3.5 mm Jack, Audio out 3.5 mm Jack, CVBS Connector COAX (75 Ohm) (CVBS output available with max. 2 activated streams)
IR Illumination	Up to 40 m distance depending on scenery reflection
Video Storage	Support for microSD/microSDHC/microSDXC card, Support for recording to NAS, MOBOTIX MOVE NVR
Environmental Protection Class	IP66/IK10
Operating Temperature	–55 to 60 °C/–41 to 140 °F with activated heater
Cold Start Temperature	–30 °C/–22 °F
Relative Humidity	10 to 90 % non-condensing
Storage Conditions	–20 to 70 °C/–4 to 158 °F
Approvals	EMC: CE/FCC Safety: LVD Environmental: IP66, IK10

Dimensions	ø 105x233.8 mm
Weight	1280 g

MOBOTIX

BeyondHumanVision

EN_11/21

MOBOTIX AG • Kaiserstrasse • D-67722 Langmeil • Tel.: +49 6302 9816-103 • sales@mobotix.com • www.mobotix.com

MOBOTIX is a trademark of MOBOTIX AG registered in the European Union, the U.S.A., and in other countries. Subject to change without notice. MOBOTIX do not assume any liability for technical or editorial errors or omissions contained herein. All rights reserved. © MOBOTIX AG 2020