



**HD9112F12**

**12MP OUTDOOR ULTRA HD FISHEYE CAMERA**

**User Manual**



AvertX HD9112F12 12MP Outdoor Ultra HD Fisheye Camera

Operations Manual

Manual Edition 38111AA – May 2024

©2024, AvertX

All Rights Reserved

No part of this document may be reproduced by any means, electronic or mechanical, for any purpose, except as expressed in the Software License Agreement. AVERTX shall not be liable for technical or editorial errors or omissions contained herein. The information in this document is subject to change without notice.

The information in this publication is provided “as is” without warranty of any kind. The entire risk arising out of the use of this information remains with recipient. In no event shall AVERTX be liable for any direct, consequential, incidental, special, punitive, or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption or loss of business information), even if AVERTX has been advised of the possibility of such damages or whether in an action, contract or tort, including negligence.

This software and documentation are copyrighted. All other rights, including ownership of the software, are reserved to AvertX. AVERTX, and AvertX, are registered trademarks of AVERTX in the United States and elsewhere; Windows is a registered trademark of Microsoft Corporation. All other brand and product names are trademarks or registered trademarks of the respective owners.

The following words and symbols mark special messages throughout this guide:

**WARNING:** Text set off in this manner indicates that failure to follow directions could result in bodily harm or loss of life.

**CAUTION:** Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.

---

## IMPORTANT SAFEGUARDS

---

1. **Read Instructions**  
Read all of the safety and operating instructions before using the product.
2. **Retain Instructions**  
Save these instructions for future reference.
3. **Attachments / Accessories**  
Do not use attachments or accessories unless recommended by the appliance manufacturer as they may cause hazards, damage product and void warranty.
4. **Installation**  
Do not place or mount this product in or on an unstable or improperly supported location. Improperly installed product may fall, causing serious injury to a child or adult, and damage to the product. Use only with a mounting device recommended by the manufacturer, or sold with the product. To ensure proper mounting, follow the manufacturer's instructions and use only mounting accessories recommended by manufacturer.
5. **Power source**  
This product should be operated only from the type of power source indicated on the marking label.

---

## Precautions

---

### Operating

- Before using, make sure power supply and others are properly connected.
- While operating, if any abnormal condition or malfunction is observed, stop using the camera immediately and then contact AvertX Customer Support.

### Handling

- Do not disassemble or tamper with parts inside the camera.
- Do not drop or subject the camera to shock and vibration as this can damage camera.
- Care must be taken when you clean the clear lens cover. Scratches and dust will ruin the image quality of your camera. Do not use strong or abrasive detergents when cleaning the camera body. Use a dry cloth to clean the camera when it is dirty. In case the dirt is hard to remove, use a mild detergent and wipe the camera gently.

### Installation and Storage

- Do not install the camera in areas of extreme temperatures in excess of the allowable range. (-22°F ~ 131°F / -30°C ~ 55°C)
- Avoid installing in humid or dusty places. The relative humidity must be below or at 90%.
- Avoid installing in places where radiation is present.
- Avoid installing in places where there are strong magnetic fields and electric signals.
- Avoid installing in places where the camera would be subject to strong vibrations.
- Never face the camera toward the sun. Do not aim at bright objects. Whether the camera is in use or not, never aim it at the sun or other extremely bright objects. Otherwise the camera may be damaged.

---

## REGULATION

---

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This symbol on the product or on its packaging indicates that this product shall not be treated as household waste in accordance with Directive 2002/96/EC. Instead it shall be handed over to the applicable collection point for the recycling of electrical and electronic equipment. By proper waste handling of this product you ensure that it has no negative consequences for the environment and human health, which could otherwise be caused if this product is thrown into the garbage bin. The recycling of materials will help to conserve natural resources.

For more details information about recycling of this product, please contact your local city office, your household waste disposal service or the shop where you purchased the product.

Compliance is evidenced by written declaration from our suppliers, assuring that any potential trace contamination levels of restricted substances are below the maximum level set by EU Directive 2002/95/EC, or are exempted due to their application.

---

## WARNING

---

DANGEROUS HIGH VOLTAGES ARE PRESENT INSIDE THE ENCLOSURE.

REFER SERVICING TO QUALIFIED PERSONNEL ONLY.

---

## CAUTION

---



# TABLE OF CONTENTS

<b>INTRODUCTION.....</b>	<b>6</b>
Overview .....	6
Product Features .....	6
<b>GETTING STARTED .....</b>	<b>7</b>
Box Contents.....	7
Camera Overview .....	8
Camera Dimensions .....	8
Connections.....	8
Power Connection .....	9
Resetting The Camera and MicroSD Card Slot.....	9
<b>CONNECTING.....</b>	<b>10</b>
Bench Test .....	10
Network Camera Manager .....	10
Launch Network Camera Manager .....	10
Connecting to the Camera .....	11
Connecting in a Web Browser .....	11
Username and Password.....	11
Connecting a Stream .....	11
Logging Into the Web Interface .....	11
<b>LIVE VIEW.....</b>	<b>12</b>
Setup.....	13
System Setting .....	13
Picture Setup .....	13
Streaming Setting .....	13
<b>ADVANCED .....</b>	<b>14</b>
System Setting .....	14
Camera Setup.....	14
User Setup.....	16
IP Address .....	18
Network Advanced.....	21
Network Security.....	24
Alarm Application .....	26
Tampering and Network Failure Detection.....	29
Network Failure Detection.....	32
Mail, HTTP and FTP Setup .....	33
SD Card .....	35
Network Share .....	37
Recording Schedule .....	39
Maintenance .....	42
Software.....	43
Log File .....	44
Picture Setting .....	45
Camera Setup.....	45
Motion Detection .....	50
Video Mask .....	55
Fisheye Setting .....	56
Text Overlay .....	57
Streaming Setting .....	59
Video Resolution.....	59
Video Rotation .....	61
Web Viewer .....	62
Audio.....	63

# INTRODUCTION

## OVERVIEW

---

The AvertX HD9112F12 outdoor 12MP IP fisheye camera is equipped with a 1.65mm fixed lens for 360° single-camera coverage in ultra high-definition. True WDR, true day/night, and adaptive IR technology ensure the HD9112F12 provides only exceptional image quality in diverse lighting environments. Adaptive IR technology enhances low-light image performance by adjusting IR output to prevent overexposure of objects as they move closer to the camera. Additional features include audio in/out, as well as alarm in and relay out connections supported by the enhanced remote monitoring capabilities of the OWS platform.

The HD9112F12 is ONVIF™ and NDAA compliant, and fully compatible with AvertX Connect, allowing multiple users to concurrently view high-quality images and set up cameras and recorders remotely using a web browser.

## PRODUCT FEATURES

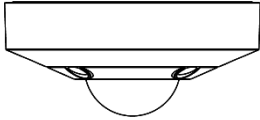
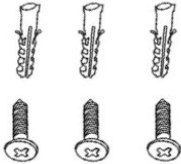
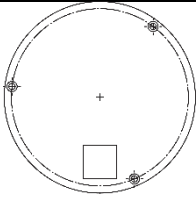

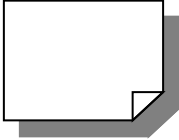
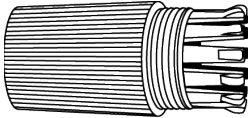
- True WDR @ 12MP
- Edge Dewarping
- 360° Coverage
- Adaptive IR
- Alarm I/O
- Two-way Audio
- IK10 Impact Protection Rating
- IP66 Ingress Protection Rating
- Smart Compression
- NDAA Compliant

# GETTING STARTED

## BOX CONTENTS

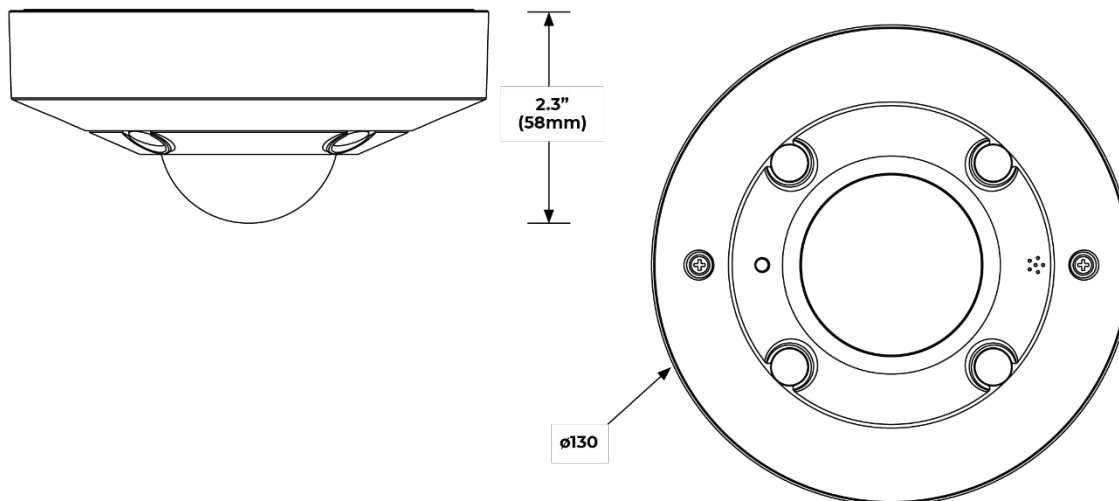
---

Before proceeding, please confirm that the box contains the items listed here. Please contact your dealer for assistance if any item is missing or has defects.

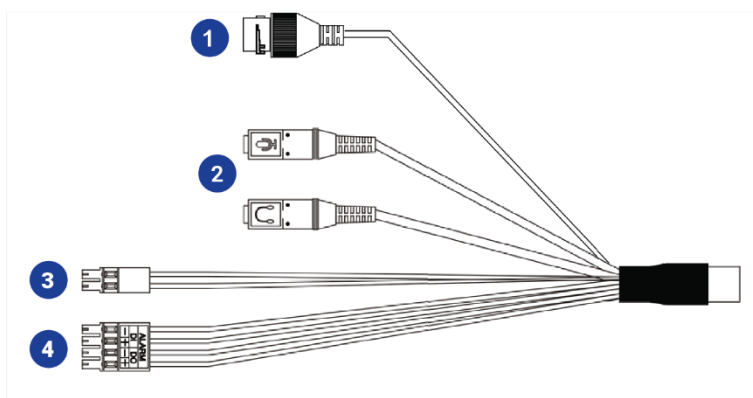
 <p>AVX-HD9112F12 Fisheye Camera</p>	 <p>Self-tapping screws/M4/6.8MM (x3) &amp; and Plastic Anchors 4- 5MM (x 3)</p>
 <p>Mounting Template</p>	 <p>Security Torx Tool</p>
 <p>Quick Start Guide</p>	 <p>Waterproof Cable Connector</p>

## CAMERA OVERVIEW

### CAMERA DIMENSIONS



### CONNECTIONS



1	RJ-45	For connector and PoE connections	
2	Audio I/O	Pink	Audio In (Line In)
		Green	Audio Out (Line Out)
3	Power (12vDC)*	Black	DC 12V -
		Red	DC 12V +
4	Alarm I/O	1	Alarm In -
		2	Alarm In +
		3	Alarm Out -
		4	Alarm Out +

\*12vDC power input port should be plugged when not in use.

## POWER CONNECTION

For an adequate power connection, use a 12vDC adaptor. Alternatively, you can power the camera by PoE if a Power Sourcing Equipment (PSE) switch is available. Ensure that the camera's power cable is correctly and firmly connected.

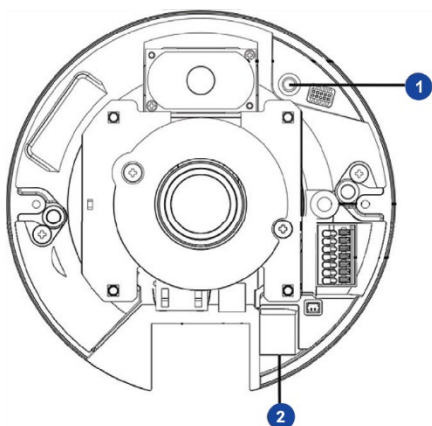
---

**Note:** *Recommends against using more than one power source at a time. Do not use a PoE power source when providing the camera with 12vDC power.*

---

If using Power over Ethernet (PoE), make sure Power Sourcing Equipment (PSE) is in use in the network.

## RESETTING THE CAMERA AND MICROSD CARD SLOT



Supports up to 512GB microSD card for Edge storage. Do not add or remove the microSD card when the camera is powered on.

1	Reset Button	To restore the camera to factory defaults: <ol style="list-style-type: none"><li>1. Disconnect power for 30 seconds.</li><li>2. Reconnect power and wait 30 seconds.</li><li>3. Press and hold the reset button for 20 seconds.</li></ol>
2	MicroSD Card Slot	Supports up to 512GB microSD card for Edge storage. <b>Do not add or remove the microSD card when the camera is powered on.</b>

# CONNECTING

## BENCH TEST

---

AvertX recommends bench testing your camera(s) before installation. This will confirm that your camera is functioning correctly before it is installed and possibly out of reach.

To bench test your camera, attach the camera network connector to your recorder and test whether or not the camera is functioning correctly. Once the camera is connected to the recorder, test all functions to ensure proper operation.

If the camera will not connect or is not functioning correctly, do not install, and contact AvertX Support.

## NETWORK CAMERA MANAGER

---

Network Camera Manager (**NCM**) is a software tool that allows you to quickly and easily connect and configure your AvertX IP cameras. This software allows you to assign IP addresses, configure video settings, and update firmware on multiple cameras at once.

NCM is pre-installed on all AvertX ProConnect recorders and is also available for download at **[www.avertx.com/support](http://www.avertx.com/support)** for installation on your personal computer or laptop.

### LAUNCH NETWORK CAMERA MANAGER

Open the Settings menu, go to the **Cameras** page and click **Advanced** (located towards to top-middle on the page).

---

**Note:** *If you cannot connect to the camera you may need to change the camera's IP address to match your network settings.*

---

### Finding Network Devices

Click **Refresh** to reload the Device List.

To narrow your search by Camera Model or Network Location, use the Model Filter and Networks dropdowns.

### Changing the IP Address

AvertX recorders will automatically apply a DHCP IP address. If you are not connecting the camera to an AvertX recorder or DHCP network, you must set a static IP address. NCM allows you to do this in the bottom left corner:

1. Select the applicable camera.
2. Enter the **IP address**, **Subnet Mask**, **Gateway**, and **DNS**.
3. Click **Apply**.
4. Wait 10 seconds and click **Refresh**.

## CONNECTING TO THE CAMERA

---

### CONNECTING IN A WEB BROWSER

1. Type the IP address of the camera in a web browser.  
- OR -  
Use the **Network Camera Manager** software and locate the camera on the list, then click **Load** in the row of the desired camera.
2. Log in to the camera with the appropriate User Name and Password.

#### *Username and Password*

**IMPORTANT:** AvertX cameras ship without a default password; the admin password is required to gain access or establish a connection.

The admin user password can be set using the following methods:

1. AvertX ProConnect recorders will check the camera for a password once connected.
  - i. **If AvertX software does not detect a password, it will set the camera password to a secure text string of 8 to 16 characters** (Including upper-case letters, lower-case letters, digits and special characters (!"#\$%&'()\*+,-./:;<=>?@[\\]^\_`{|}~ space)).
2. Network Camera Manager
3. Camera Web Browser

### CONNECTING A STREAM

AvertX IP cameras are optimized for use with AvertX ProConnect recorders, but you can also connect to your AvertX IP cameras using third party software like VLC media player (<http://www.videolan.org>).

To connect the camera, you may need to provide the stream URL. All AvertX IP cameras are capable of delivering two RTSP streams over HTTP. The stream URLs are listed below:

- rtsp://< IPADDRESS >/Streaming/Channels/101
  - H.264 Stream 1
- rtsp://< IPADDRESS >/Streaming/Channels/102
  - H.264 Stream 2

---

**Note:** VLC will ask for the username and password for your AvertX camera.

---

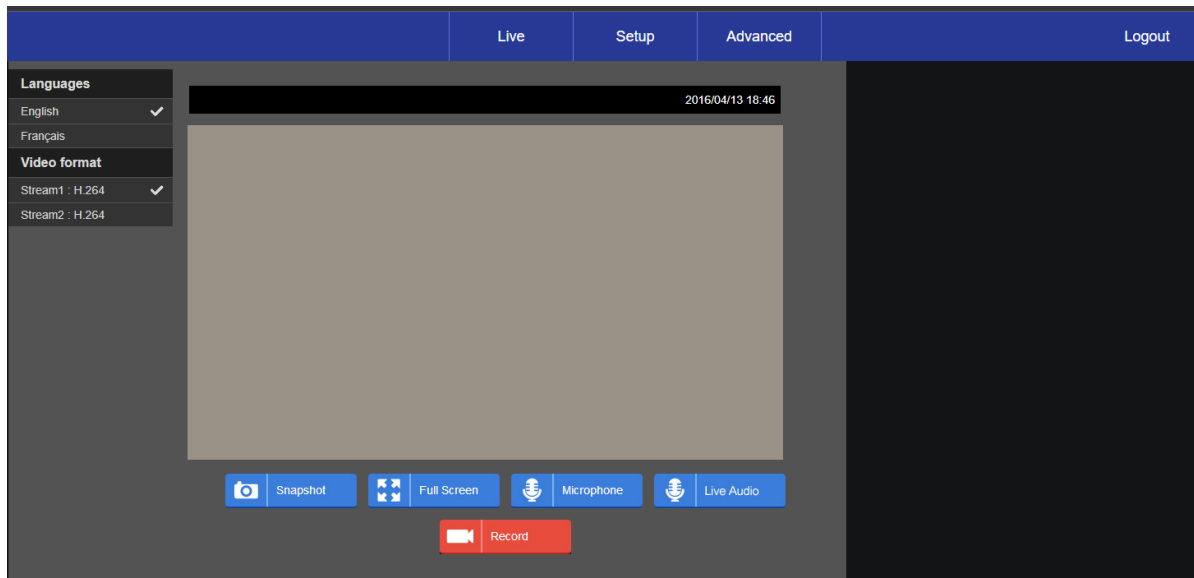
## LOGGING INTO THE WEB INTERFACE

---

The default static IP address of the camera is 192.168.51.2, and the default subnet mask is 255.255.255.0. DHCP is turned on by default. If a DHCP server is used in the network, the IP address of your camera will be assigned dynamically.

- Browse to the login page by entering the IP address of your camera in the address bar.
- Enter the **username** and **password**, and then click **Login**.
  - For the first login, use the default username: **admin**
  - You will be prompted to change the password.

# LIVE VIEW



The camera displays a live view using the MJPEG stream for setup purposes.

**Setup** – Go to the Setup tab to access the camera menus

**Advanced** – Go to the Advanced tab to configure advanced camera features

**Logout** – Log out the current user

**Languages** – Select menu and live screen language

**Video format** – Select camera stream

**Snapshot** – Take a snapshot of the live screen image

**Full Screen** – Display camera image in full screen mode

**Microphone** – Select to talk via the camera microphone

**Live Audio** – Select to listen to audio via the camera

**Record** – Select to record live video

## SETUP

---

The Setup menu allows for quick camera configuration. The same tabs can be found in the Advanced menus. Follow the links below for full descriptions of Setup and Settings options:

### SYSTEM SETTING

[Camera Name](#)

[User Setup](#)

[IP Address](#)

### PICTURE SETUP

[Camera Tab](#)

[Motion Detection](#)

### STREAMING SETTING

[Video Resolution](#)

[Video Rotation](#)

## ADVANCED

### SYSTEM SETTING

#### Camera Setup

The Camera Setup tab displays the product model, time zone, daylight saving time option, date format, and the option to sync camera time with a computer, NTP server, or manually enter a time.

Host Name :

Time zone :

GMT-08:00 Pacific Time (USA & Canada) ▼

☐ Enable daylight saving time

Time offset:

01:00:00

Start date:

Jan ▼

1st ▼

Sun ▼

Start time:

00:00:00

End date:

Jan ▼

1st ▼

Sun ▼

End time:

00:00:00

Date format:

yyyy/mm/dd ▼

☒ Sync with computer time

PC date:

2022/03/17

[yyyy/mm/dd]

PC time:

10:13:50

[hh:mm:ss]

☐ Manual

Date:

2016/04/01

[yyyy/mm/dd]

Time:

00:00:00

[hh:mm:ss]

☐ Sync with NTP server

NTP server:

0.0.0.0

[host name or IP address]

Update interval:

Every hour ▼

Save

**Host Name** - The Host Name is for camera identification. If the alarm function is enabled and is set to send alarm messages by Mail / FTP, the 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** - Check to enable DST, 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** - Video date and time display will synchronize with the PC's time.

**Manual** - The administrator can set video date and time manually. Entry format should be identical with the examples shown next to the entry 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 to synchronize with in the entry field. Then select an update interval from the drop-down menu.

<b>Note</b> The synchronization will be done every time the camera boots up.
--

Click **Save** after making any changes to Camera Setup.

## User Setup

The User Setup tab allows you to set an admin password, add users and permissions, set authentication type and enable a lockout function for login attempts.

The screenshot displays the 'User Setup' configuration page. It includes several sections: 'Admin Password' with fields for 'Admin password' and 'Confirm password' and a 'Save' button; 'Add User' with fields for 'User name' and 'User password', checkboxes for 'I/O access', 'Camera control', 'Talk', and 'Listen', and an 'Add' button; 'Manage User' with a 'User name' dropdown menu and 'Delete' and 'Edit' buttons; 'HTTP Authentication Setting' with a 'Type' dropdown menu and a 'Save' button; 'Streaming Authentication Setting' with a 'Type' dropdown menu and a 'Save' button; and 'Enable Account Lockout Function' with a checkbox, a 'Threshold' field set to 5, a 'Duration' field set to 10, and a 'Save' button.

**Admin Password** – This allows the administrator to reset the 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 **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 allows 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 **I/O access**, **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** – I/O access supports fundamental functions that enable users to view the live video when accessing to the camera.
- **Camera control** – Camera control allows the appointed user to change camera parameters on the **Camera** and **Pan Tilt** setting page.
- **Talk/Listen** – Talk/Listen 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 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 popup window, enter the new user password and reset the privileges. Click **Save** to confirm the changes. Then click **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 access the camera through a web browser, they will have to enter a username and password. There are two security models available: **Basic** and **Digest**.

- **Basic** - This mode provides basic protection for connection security.
- **Digest** - Digest mode provides additional protection. The password is sent in an encrypted format to prevent it from being stolen.

**Streaming Authentication Setting** - This setting provides security against unauthorized users from receiving streaming via Real Time Streaming Protocol (RTSP). If this setting is enabled, users will be asked to enter a username and password before viewing live streams. There are three security modes available: **Disable**, **Basic** and **Digest**.

- **Disable** - If disable mode is selected, there will be no security provided against unauthorized access. Users will not be asked to input a username and password for authentication.
- **Basic** - This mode provides basic protection for live streams.
- **Digest** - Digest mode provides additional protection. The password is sent in an encrypted format to prevent it from being stolen.

**Enable Account Lockout Function** - The Account Lockout Function locks out an account when someone tries to log on unsuccessfully several times in a row. To protect a user's account, the Account Lockout Function is activated when multiple login failures occur. Check the box **Enable Account Lockout Function** and enter values for **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).

Click **Save** after making any changes to User Setup.

## IP Address

The IP Address tab allows you to configure the connected camera network settings.

**General**  
☒ Get IP address automatically  
☐ Use fixed IP address  
IP address   
Subnet mask   
Default gateway   
Primary DNS   
Secondary DNS   
☐ Use PPPoE  
User name   
Password

**Advanced**  
Web Server port   
RTSP port   
MJPEG over HTTP port   
HTTPS port

**IPv6 Address Configuration**  
☐ Enable IPv6 Address :

**General** – These settings are for configuring a new IP address for the camera.

- **Get IP address automatically (DHCP)** - Select **Get IP address automatically** and click **Save** to confirm the new setting. A note for a camera system reboot will appear. Click **OK** and the camera system will restart. The camera will be assigned a new IP address.
- **Use fixed IP address** - Select **Use fixed IP address** and insert the new IP address. Then insert the Default gateway. Click **Save** to confirm the new setting. When a note for system restart appears, 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.
- **Use PPPoE** - For PPPoE users, enter the PPPoE **User name** and **Password** into the fields, and click **Save**.

**Advanced** – Advanced is for configuring 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 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 is 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 range 1024 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** Port numbers cannot be the same; otherwise, network conflict may occur.

**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.

Click **Save** after making any changes to Network Setup.

**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.

**DDNS**

**Dynamic DNS**  
Use Dynamic DNS If You Want To Use Your DDNS Account.

☐ **Enable DDNS**

Provider

DynDNS.org(Dynamic) ▾

Host name

Username/E-mail

Password/Key

\*\*\*\*

Save

**Enable DDNS** - Check 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.

Click **Save** after making any changes to DDNS.

## Network Advanced

**QoS** - QoS allows 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.

The screenshot shows a web interface for QoS configuration. At the top, there's a tab labeled 'QoS'. Below it, the 'DSCP Settings' section is visible. It contains several input fields, all currently set to '0'. The settings are organized as follows:

- Management DSCP**: Input field with value 0.
- Stream1 DSCP**:
  - Video**: Input field with value 0.
  - Audio**: Input field with value 0.
- Stream2 DSCP**:
  - Video**: Input field with value 0.
  - Audio**: Input field with value 0.
- Stream3 DSCP**:
  - Video**: Input field with value 0.
  - Audio**: Input field with value 0.
- Stream4 DSCP**:
  - Video**: Input field with value 0.
  - Audio**: Input field with value 0.

At the bottom of the settings area, there is a 'Save' button.

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

- **Management DSCP** - The class consists of HTTP traffic: Web browsing.
- **Stream 1-4 DSCP** - Users can set the Audio/Video DSCP of each stream.

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

**Audio DSCP** - This setting is only available for the cameras that support audio.

Click **Save** after making any changes to QoS.

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

**SNMP Settings**

**SNMP v1/v2**

☐ Enable SNMP v1

☐ Enable SNMP v2

Read Community

Write Community

**SNMP v3**

☐ Enable SNMP v3

Security Name

Authentication Type

Authentication Password

Encryption Type

Encryption Password

**Traps for SNMP v1/v2/v3**

☐ Enable traps

Trap address

Trap community

Trap Option

☐ Warm start

## SNMP v1 / v2

- **Enable SNMP v1 / v2** - Select the version of SNMP 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. 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 (IP camera) performs software reload.

Click **Save** after making any changes to SNMP.

## Network Security

### HTTPS

**Enable HTTPS** Disable ▾

Save

**Installed Certificate**

Subject

No certificate installed.

Properties Remove

### IP Filter

☐ **Enable IP filter**

Deny ▾ the following IP addresses Apply

Filtered IP Addresses

Delete

0.0.0.0 Add

### IEEE 802.1X

**IEEE 802.1X** ☐ On ☒ Off

Save

**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 and secure Username / Password. HTTPS requires installing a self-signed certificate or a CA-signed certificate.

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.

**Enable HTTPS** - Check the box to enable an 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**.

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

- **Add IP Address** - Input the IP address in the field 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.
- **Delete IP Address** - To remove an IP address from the **Filtered IP Address** list, please select the address and click on **Delete**.

**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**.

Click **Save** after making any changes to Network Security.

## Alarm Application

The camera supports one alarm input and one relay output to catch event images.

**Application**

**Alarm Switch**

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

**Alarm Type**

☐ Normal close ☒ Normal open

**Triggered Action**

☒ Enable alarm output high ☐ IR cut filter on

☐ Send message by FTP ☐ Send message by E-Mail

☐ Upload image by FTP ☐ Upload image by E-Mail

☐ Send HTTP notification ☐ Record video clip

**File Name**

File Name :

☒ Add date/time suffix

☐ Add sequence number suffix (no maximum value)

☐ Add sequence number suffix up to  and then start over

☐ Overwrite

**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:

- **Enable Alarm Output** - Select **high** or **low** 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 cannot be set to **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** - 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** One of the streams must be set as MJPEG; otherwise this function cannot be accessed.

- **Pre-trigger buffer** - Allows users to check what caused the trigger. The **Pre-trigger buffer frame rate** can be pre-determined.
- **Post-trigger buffer** - Upload a certain amount of images after the alarm input is triggered.

**Note** The **Pre-trigger buffer** generally ranges from 1 to 20 frames.

- **Continue image upload** - Upload the triggered images during a certain time or keep uploading until the trigger is off.
- **Upload for \_\_ sec** - Enter the duration in the field. Images will be uploaded to the FTP for the duration when the alarm input is triggered. The setting range is from 1 to 99999 sec.
- **Upload during the trigger is active** - Continually upload to FTP until the alarm is released.
- **Image frequency** - Upload frame rate. The setting range is from 1 to 15 frames.

**Note** The FTP configuration must be completed before selecting upload options.

- **Upload Image by E-Mail** - 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** One of the streams must be set as MJPEG; otherwise this function cannot be accessed.

- **Pre-trigger buffer** - Allows users to check what caused the trigger. The **Pre-trigger buffer frame rate** can be pre-determined.
- **Post-trigger buffer** - Upload a certain amount of images after the alarm input is triggered.

**Note** The **Pre-trigger buffer** generally ranges from 1 to 20 frames.

- **Continue image upload** - Upload the triggered images during a certain time or keep uploading until the trigger is off.
- **Upload for \_\_ sec** - Enter the duration in the field. Images will be uploaded to the E-mail for the duration when the alarm input is triggered. The setting range is from 1 to 99999 sec.
- **Upload during the trigger is active** - Continually upload to E-mail until the alarm is released.
- **Image frequency** - Upload frame rate. The setting range is from 1 to 15 frames.

**Note** The SMTP configuration must be completed before selecting upload options.

- **Send HTTP Notification** - Check to select the destination HTTP address. Specify the parameters for event notifications by **Alarm** triggered. When an alarm is triggered, the HTTP notification will be sent to the specified HTTP server.
- **Record Video Clip** - Check to 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.
  - **Pre-trigger buffer** - Allows users to check what caused the trigger. The pre-trigger buffer time range is from 1 to 3 sec.
  - **Upload for \_\_ sec** - Set the recording duration after an alarm is triggered. The setting range is from 1 to 99999 sec.
  - **Upload during the trigger is active** - Record triggered video until the trigger is off.

**Note** Either **microSD/SD card** or **NAS** must be enabled for recorded video to save.

- **File Name** – Enter a file name in the field. The file name format of the uploaded image can be set to one of the following:
  - **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.

Click **Save** to save any changes made to the Alarm Application page.

## Tampering and Network Failure Detection

The Tampering Alarm function helps the IP camera against tampering, such as deliberate redirection, blocking, paint spray, or a covered lens, etc., through video analysis and reaction to such events by sending out notifications or uploading snapshots to the specified destinations.

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

**Tampering Alarm**  
☒ Off ☐ On ☐ By schedule Please select ...

**Tampering Duration**  
Minimum duration  sec

**Triggered Action**  
☐ Enable alarm output high ☐ Record video clip  
☐ Send message by FTP ☐ Send message by E-Mail  
☐ Upload image by FTP ☐ Upload image by E-Mail  
☐ Send HTTP notification

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

### Network Failure Detection

**Detection Switch**  
☒ Off ☐ On ☐ By schedule Please select ...

**Detection Type**  
Ping the IP address  every  minutes

**Triggered Action**  
☐ Enable alarm output high ☐ Send message by FTP ☐ Send message by E-Mail  
☐ Record video clip

**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; a longer duration represents a higher threshold. The 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 trigger when tampering is detected.

- **Enable Alarm Output** - Check **high** or **low** 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** - 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** One of the streams must be set as MJPEG; otherwise this function cannot be accessed.

- **Pre-trigger buffer** - Allows users to check what caused the trigger. The **Pre-trigger buffer frame rate** can be pre-determined.
- **Post-trigger buffer** - Upload a certain amount of images after the alarm input is triggered.

**Note** The **Pre-trigger buffer** generally ranges from 1 to 20 frames.

- **Continue image upload** - Upload the triggered images during a certain time or keep uploading until the trigger is off.
- **Upload for \_\_ sec** - Enter the duration in the field. Images will be uploaded to the FTP for the duration when tampering is triggered. The setting range is from 1 to 99999 sec.
- **Upload during the trigger is active** - Continually upload to FTP until the alarm is released.
- **Image frequency** - Upload frame rate. The setting range is from 1 to 15 frames.

**Note** The FTP configuration must be completed before selecting upload options.

- **Upload Image by E-Mail** - The administrator can assign an E-mail address and configure various parameters. When tampering is triggered, event images will be sent to the appointed E-mail address.

**Note** One of the streams must be set as MJPEG; otherwise this function cannot be accessed.

- **Pre-trigger buffer** - Allows users to check what caused the trigger. The **Pre-trigger buffer frame rate** can be pre-determined.
- **Post-trigger buffer** - Upload a certain amount of images after tampering is triggered.

**Note** The **Pre-trigger buffer** generally ranges from 1 to 20 frames.

- **Continue image upload** - Upload the triggered images during a certain time or keep uploading until the trigger is off.

- **Upload for \_\_ sec** - Enter the duration in the field. Images will be uploaded to the E-mail for the duration when tampering is triggered. The setting range is from 1 to 99999 sec.
- **Upload during the trigger is active** - Continually upload to E-mail until tampering stops.
- **Image frequency** - Upload frame rate. The setting range is from 1 to 15 frames.

**Note** The SMTP configuration must be completed before selecting upload options.

- **Send HTTP Notification** - Check to select the destination HTTP address. Specify the parameters for HTTP notifications. When the tampering alarm is triggered, the HTTP notification will be sent to the specified HTTP server.
- **Record Video Clip** - Check to 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.
  - **Pre-trigger buffer** - Allows users to check what caused the trigger. The pre-trigger buffer time range is from 1 to 3 sec.
  - **Upload for \_\_ sec** - Set the recording duration after tampering occurs. The setting range is from 1 to 99999 sec.
  - **Upload during the trigger is active** - Record triggered video until the trigger is off.

**Note** Either **microSD/SD card** or **NAS** must be enabled for recorded video to save.

- **File Name** – Enter a file name in the field. The file name format of the uploaded image can be set to one of the following:
  - **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.

Click **Save** to save any changes made to the Tampering page.

## Network Failure Detection

Allows the camera to ping another IP device within the network periodically and generates some actions in case a network failure occurs.

Being capable of implementing local recording (through a 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** - Check **high** or **low** 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.
- **Record Video Clip** - Check to 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.
  - **Pre-trigger buffer** - Allows users to check what caused the trigger. The pre-trigger buffer time range is from 1 to 3 sec.
  - **Upload for \_\_ sec** - Set the recording duration after an alarm is triggered. The setting range is from 1 to 99999 sec.
  - **Upload during the trigger is active** - Record triggered video until the trigger is off.

<b>Note</b> Either <b>microSD/SD card</b> or <b>NAS</b> must be enabled for recorded video to save.
---

Click **Save** to save any changes made to the Network Failure Detection page.

## Mail, HTTP and FTP Setup

### Mail

#### SMTP

1st SMTP (mail) server

1st SMTP (mail) server port

1st SMTP account name

1st SMTP password

1st recipient email address

☐ 1st SMTP SSL

Test the connection to the specified SMTP (mail) server

2nd SMTP (mail) server

2nd SMTP (mail) server port

2nd SMTP account name

2nd SMTP password

2nd recipient email address

☐ 2nd SMTP SSL

Test the connection to the specified SMTP (mail) server

Sender email address

### HTTP

#### HTTP

1st HTTP server

1st HTTP user name

1st HTTP password

2nd HTTP server

2nd HTTP user name

2nd HTTP password

**Mail** - The administrator can send an E-mail via Simple Mail Transfer Protocol (SMTP) when an alarm is triggered.

Two sets of SMTP can be configured. Each set includes **SMTP Server, Account Name, Password** and **E-mail Address** settings.

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 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**.

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

**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, 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.

## SD Card

Users can implement local recording to the microSD/SDHC/SDXC card up to 512GB. 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.

### SD Card

#### Device Information

Device type:	SD Card - n/a		
Free space:	0KB	Total size:	0KB
Status:	No	Full:	No

#### Recording source

Recording source: Stream 1 Save

#### Recording filename format

Format : Start time only Save

#### Device Setting

Format device : vfat (default) Format

#### Disk Cleanup Setting

☐ Enable automatic disk cleanup

Remove recordings older than: 1 day(s)

Remove oldest recordings when disk is: 85 % full

Save

#### Recording List

From 2016-04-17 to 2016-04-17 Search

Date (yyyy-mm-dd) Date (yyyy-mm-dd)

☒ Video ☐ JPEG

FileName	Size
----------	------

Remove Sort download

**Note** Please format the microSD/SDHC/SDXC card when using it for the first time.

**Note** 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.

**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** or **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**.
- **Sort** - Click **Sort**, and the files in the Recording list will be listed in name and date order.
- **Download** - To open / download a video clip / image, select the file first, and then click **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

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

**Device Information**

Device type:	Network Share		
Free space:	0GB	Total size:	0GB
Status:	offline	Full:	No

**Storage Settings**

Protocol: SAMBA

Host:

Share:

User name:

Password:

Save

**Recording source**

Recording source: Stream 1 Save

**Recording filename format**

Format : Start time only Save

**Storage Tools**

Format device Format

**Disk Cleanup Setting**

☐ Enable automatic disk cleanup

Remove recordings older than: 1 day(s)

Remove oldest recordings when disk is: 85 % full

Save

**Recording List**

From 2016-04-17 to 2016-04-17 Search

Date (yyyy-mm-dd) Date (yyyy-mm-dd)

FileName	Size
<div></div>	

Remove Sort download

**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 **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 **Remove**.
- **Sort** - Click **Sort**, and the files in the Recording list will be listed in name and date order.
- **Download** - To open / download a video clip / image, select the file first, and then click **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.

## Recording Schedule

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

**Recording**

**Recording Storage**  
☒ SD Card  
☐ Network Share

**Recording Schedule**  
☒ Disable  
☐ Always  
☐ Only during time frame

	Weekday	Start time	Duration
1	- - - - -	---	---
2	- - - - -	---	---
3	- - - - -	---	---
4	- - - - -	---	---
5	- - - - -	---	---
6	- - - - -	---	---
7	- - - - -	---	---
8	- - - - -	---	---
9	- - - - -	---	---
10	- - - - -	---	---

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

☐ Day  
☐ Night  
☒ Time

Start time :  Duration :

**Interval Recording****Interval Recording**  
☒ Off ☐ On**Time Interval**  
Minimum interval  
 sec**Triggered Action**  
☐ Upload image by FTP ☐ Upload image by E-Mail  
☐ Upload image to SD card**File Name**  
File Name : ☒ Add date/time suffix  
☐ Add sequence number suffix (no maximum value)  
☐ Add sequence number suffix up to  and then start over  
☐ Overwrite

**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, set a schedule on the time frame. Check specific days, select **Day**, **Night** or **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.

- **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.

Click **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 **Save** when finished.

## Interval Recording

**Interval Recording** - 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** - The administrator can assign an FTP site and configure various parameters. Images will be uploaded to the appointed FTP site periodically.

**Note** One of the streams must be set as MJPEG; otherwise this function cannot be accessed.

- **Pre-trigger buffer** - Defines how many images are uploaded before the triggered moment.
- **Post-trigger buffer** - Defines how many images are uploaded after the triggered moment.

**Note** The **Pre-trigger buffer** generally ranges from 1 to 20 frames.

- **Upload Image by E-Mail** - The administrator can assign an E-mail address and configure various parameters. Images will be sent to the appointed E-mail address periodically.

**Note** One of the streams must be set as MJPEG; otherwise this function cannot be accessed.

- **Pre-trigger buffer** - Defines how many images are uploaded before the triggered moment.

- **Post-trigger buffer** - Defines how many images are uploaded after the triggered moment.

**Note** The **Pre-trigger buffer** generally ranges from 1 to 20 frames.

- **Upload Image to SD Card** – Check for images to be uploaded to the SD Card periodically.

**Note** One of the streams must be set as MJPEG; otherwise this function cannot be accessed.

- **Pre-trigger buffer** - Defines how many images are uploaded before the triggered moment.
- **Post-trigger buffer** - Defines how many images are uploaded after the triggered moment.

**Note** The **Pre-trigger buffer** generally ranges from 1 to 20 frames.

- **File Name** – Enter a file name in the field. The file name format of the uploaded image can be set to one of the following:

- **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.

Click **Save** to save any changes made to the Interval Recording.

## Maintenance

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

The screenshot shows a web interface with two main sections. The first section, titled 'Configuration', contains two sub-sections: 'Export Files' and 'Upload Files'. Under 'Export Files', there is a text label 'Export configuration files' and an 'Export' button. Under 'Upload Files', there is a text label 'Select configuration files', a file selection input with a 'Choose File' button and the text 'No file chosen', and an 'Upload' button. The second section, titled 'Factory Default', contains three sub-sections. The first sub-section is titled 'Restore factory settings and lose any changes?' with the text 'Device restarting, please wait.' and a 'Full Restore' button. The second sub-section is titled 'Restore factory settings (excluding network settings)' and has a 'Partial Restore' button. The third sub-section is titled 'Reboot the system.' and has a 'Reboot' button.

**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.

### Factory Default

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

**Full Restore** - Reset the camera to factory default settings. The camera will restart in 30 seconds. All settings, including the IP address and user credentials will be restored to default.

**Partial Restore** - Reset all camera settings, excluding network settings and user credentials, to factory default settings. The camera will restart in 30 seconds. Refresh the browser page after the camera system is restarted.

**Reboot** - Restart the camera without changing any current settings.

## Software

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

**Software version**  
The CPU version is **pc20220114UX**

**Upgrade**  
**Follow These Steps To Do The Software Upgrade**  
**Step1:**  
Upload the binary file  

**Choose File** No file chosen

  
**Step2:**  
Select binary file you want to upgrade  

OpenEye\_pcxxxxxxxUX.fw ▼

  
**Step3:**  
Click the upgrade button to start the upgrade process  

**Upgrade**

To upgrade the camera software:

1. Click on **Browse** and locate the upgrade file.
2. Pick a file type from the drop-down menu.
3. Click on **Upgrade**.

## Log File

The camera keeps a record of the system's behavior and information related to the camera. This log data can be exported for future use. Click **generate syslog** and the **Save File As** dialog window will pop up. Select the file destination and click **Save** to export the log data.

### System Log

```
[Tue Nov 30 08:55:08 2021] --Network interface initialized start
[Tue Nov 30 08:55:08 2021] --Network interface initialized end
[Tue Nov 30 08:55:08 2021] --Host IP = 192.168.0.250
[Tue Nov 30 08:55:08 2021] --Subnet Mask = 255.255.255.0
[Tue Nov 30 08:55:08 2021] --Gateway = 192.168.0.254
[Tue Nov 30 08:55:08 2021] --MAC address = 00:D0:89:16:00:11
[Tue Nov 30 08:55:39 2021] --Admin@::ffff:192.168.0.5 GET /cgi-bin/videoanalytics_checkkey.cgi HTTP/
[Tue Jan 4 19:03:50 2022] --Network interface initialized start
[Tue Jan 4 19:04:14 2022] --Network interface initialized end
[Tue Jan 4 19:04:14 2022] --Host IP = 192.168.2.11
[Tue Jan 4 19:04:14 2022] --Subnet Mask = 255.255.255.0
[Tue Jan 4 19:04:14 2022] --Gateway =
[Tue Jan 4 19:04:14 2022] --MAC address = 00:D0:89:16:00:11
[Tue Jan 4 19:05:14 2022] --Admin@::ffff:192.168.2.8 GET /cgi-bin/admin/beforeupgrade.cgi HTTP/1.1
[Tue Jan 4 19:06:13 2022] --Admin@::ffff:192.168.2.8 POST /cgi-bin/admin/firmwareupgrade.cgi?filena
[Tue Jan 4 19:07:10 2022] --Network interface initialized start
[Tue Jan 4 19:07:24 2022] --Network interface initialized end
[Tue Jan 4 19:07:24 2022] --Host IP = 192.168.2.11
[Tue Jan 4 19:07:24 2022] --Subnet Mask = 255.255.255.0
[Tue Jan 4 19:07:24 2022] --Gateway =
[Tue Jan 4 19:07:24 2022] --MAC address = 00:D0:89:16:00:11
[Tue Jan 4 19:08:27 2022] --Admin@::ffff:192.168.2.8 GET /cgi-bin/admin/param.cgi?action=list&group
[Tue Jan 4 19:08:46 2022] --Network interface initialized start
[Tue Jan 4 19:08:54 2022] --Network interface initialized end
[Tue Jan 4 19:08:54 2022] --Host IP = 192.168.2.11
```

generate syslog

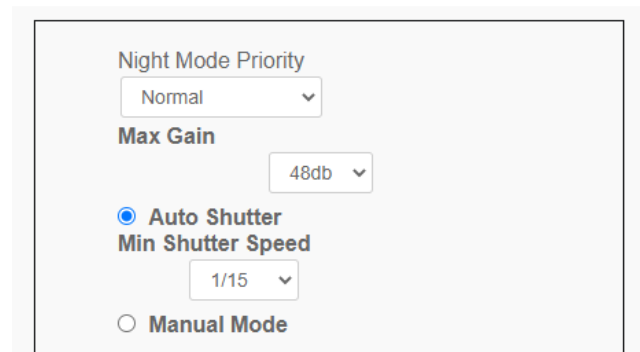
## PICTURE SETTING

### Camera Setup

You can adjust the camera image settings under Camera Setup.

#### 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.



**Night Mode Priority** - Choose between **Normal** or **High Light Detail**

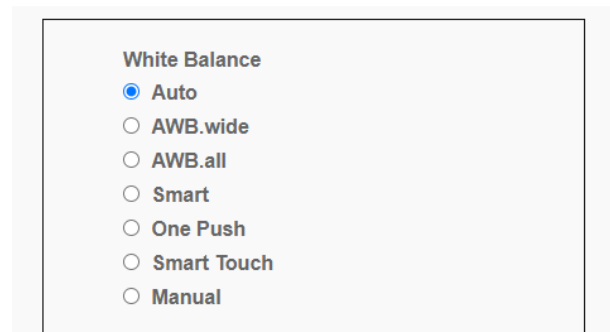
**Max Gain** - Maximum Gain can be set to reduce image noises. The Max Gain ranges from 3dB to 48dB, or select **Off** to disable the function. The default setting is 48dB.

**Auto Shutter Mode** - In this mode, the camera will automatically adjust the shutter speed according to the light intensity. The minimum shutter speed range is configurable from 1/500 to 1 sec.

**Manual Mode** - With this mode, users can select the suitable shutter speed and gain value according to the environmental illumination. The shutter speed range is from 1/10000 to 1 sec.

## 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. Users can select one of the White Balance Control modes according to the operating environment.




**Auto** - The **Auto** mode is suitable for environments with light source having color temperature in the range roughly from 2700K to 7800K.


**AWB.wide** - With the **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 the **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:

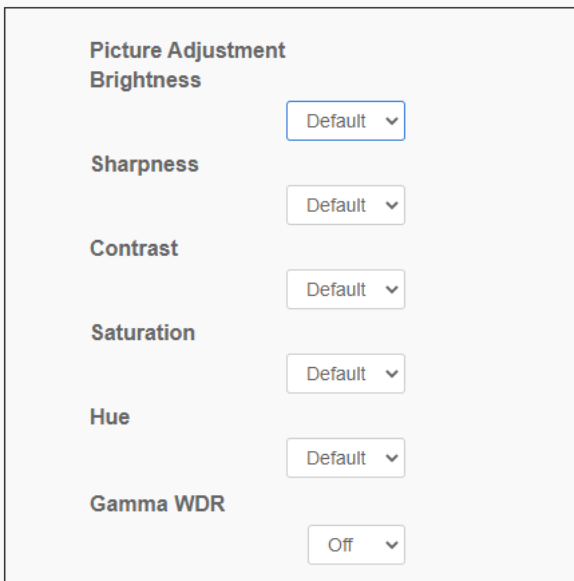
1. Point the camera to the monitoring area.
2. Select **One Push** in the White Balance setting menu.
3. Click the  button to adjust the color tone of the live images.

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

**Smart Touch Mode** - With the **Smart Touch function**, users can select an area in the camera scene as the reference point for white balance. Make sure that the background color of the selected area is white. The Smart Touch function is suitable for environments with an 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** or **Bgain** to adjust the red / blue illumination on the Live Video Pane. The following describes several situations that might occur during the White Balance manual adjustment.

## Picture Adjustment

A screenshot of a 'Picture Adjustment' settings menu. The menu is titled 'Picture Adjustment' and contains several options, each with a dropdown arrow. The options are: 'Brightness' (set to 'Default'), 'Sharpness' (set to 'Default'), 'Contrast' (set to 'Default'), 'Saturation' (set to 'Default'), 'Hue' (set to 'Default'), and 'Gamma WDR' (set to 'Off'). The menu is displayed in a light gray box with a thin black border.

Picture Adjustment

Brightness Default ▾

Sharpness Default ▾

Contrast Default ▾

Saturation Default ▾

Hue Default ▾

Gamma WDR Off ▾

**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.

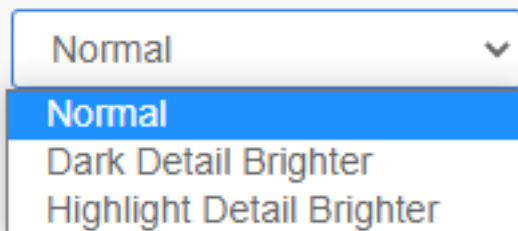
**Saturation** - The saturation level of the images is adjustable from -6 to +19. The default value is 0.

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

**Gamma WDR** - Enable Gamma WDR to distinguish the bright and dark areas in the same image. Select between **Low**, **Mid**, **High** or **Auto**.

### Color Style

Color Style defaults to **Normal**. Depending on the lighting environment, select **Dark Detail Brighter** or **Highlight Detail Brighter**.

A screenshot of a 'Color Style' dropdown menu. The menu is open, showing four options: 'Normal' (selected and highlighted in blue), 'Dark Detail Brighter', and 'Highlight Detail Brighter'. The menu is displayed in a light gray box with a thin black border.

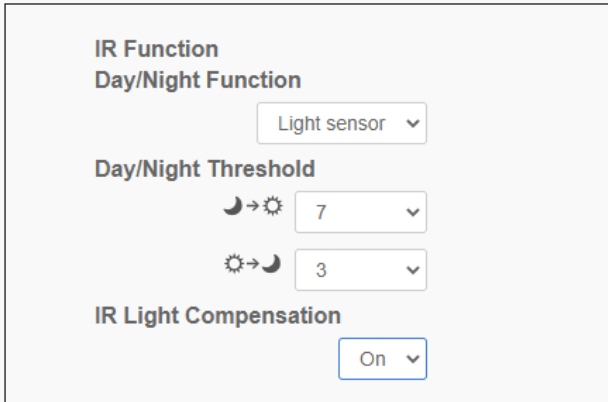
Normal ▾

Normal

Dark Detail Brighter

Highlight Detail Brighter

## IR Function



IR Function

Day/Night Function

Light sensor ▼

Day/Night Threshold

☾→☀ 7 ▼

☀→☾ 3 ▼

IR Light Compensation

On ▼

**Day/Night Function** - 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.
- **Light Sensor Mode (Default)** – Select this mode to allow the light sensor to decide when to turn the IR LED lights on / off.
- **Light On Mode** - In this mode, IR LED lights will always be on.
- **Light Off Mode** - In this mode, IR LED lights will always be off.
- **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 remain removed (i.e. monochrome/night mode).

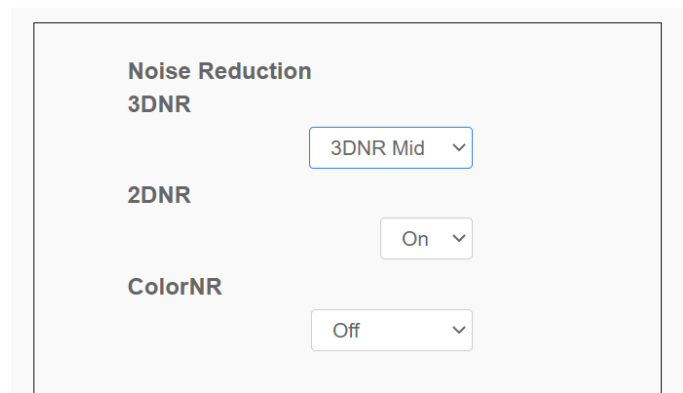
**Day/Night Threshold** - Day/Night Threshold determines when the camera should switch from day mode to night mode or vice versa. Once the camera detects the light level reaches the set threshold, the camera will automatically switch to Day/Night Mode. The range of the level is from 0 to 10, (darker = 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.

**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 the IR LED lights are turned on.

## 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.

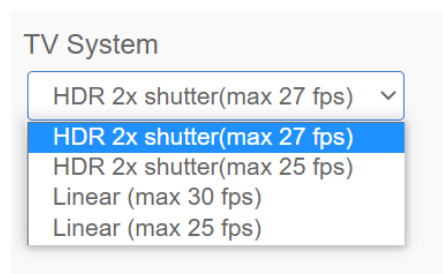
Select **on** to turn on 2DNR function; otherwise, select **off** to turn off 2DNR function.

**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.

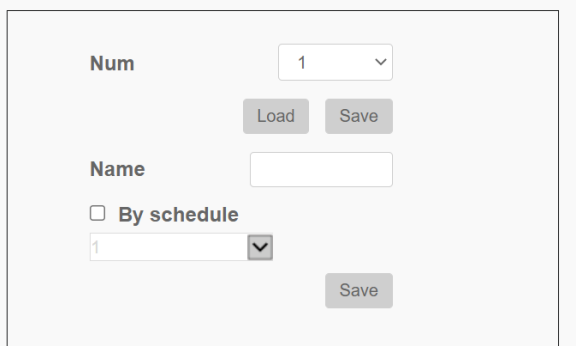
## TV System

Select the video format that matches the present TV system from the drop-down menu. Choose between **HDR 2x shutter(max 27 fps)**, **HDR 2x Shutter(max 25 fps)**, **Linear (max 30 fps)**, and **Linear (max 25 fps)**.



## 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 the Schedule section for further details on schedule setup. Then, follow the steps below to setup a camera profile.

The screenshot shows a web-based configuration interface for a camera profile. It features a 'Num' dropdown menu with '1' selected, a 'Load' button, and a 'Save' button. Below these is a 'Name' text input field. Further down is a checkbox labeled 'By schedule' which is currently unchecked. Underneath the checkbox is a small dropdown menu showing '1'. At the bottom right of the form is another 'Save' button.

1. In the **Camera** tab, set 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. Select a profile from the **Num** drop-down menu.
5. Check the **By schedule** box.
6. Check the desired schedule(s) from the **Schedule** drop-down menu. Multiple schedule can be applied to one profile.
7. Click **Save**.
8. Follow the steps above to set other profiles.

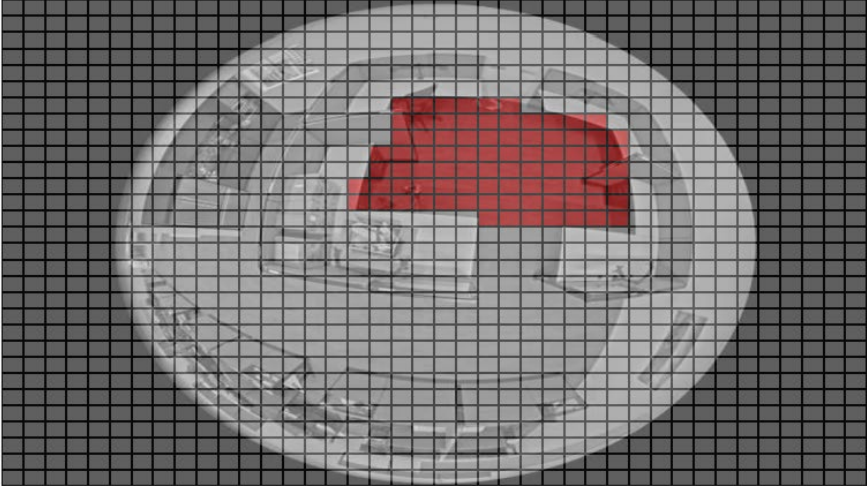
The camera will automatically switch profiles according to the schedule. Alternatively, users can manually select a number from the **Num** drop-down menu.

**Note** The last profile created will function as the new default setting. If there are gaps among schedules, the camera will apply the setting of the last profile.

**Note** Select **Normal** to set the camera back to factory default settings.

## Motion Detection

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



Motion Indication Bar

Motion Detection

1

☐ Off
☒ On
☐ By schedule

Please select ...

Motion Detection Setting

Sampling pixel interval [1-10]

1

Detection level [1-100]

10

Sensitivity level [1-100]

80

Time interval(sec) [0-7200]

10

Save

Motion Region Paint

☒ Enable brush

1x1

Triggered Action

☐ Enable alarm output

high

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

File Name

File Name : image.jpg

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

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

**Motion Indication Bar** - When the Motion Detection function is activated and motion is detected, the signals will be displayed on the motion indication bar. The motion indication bar will display 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.

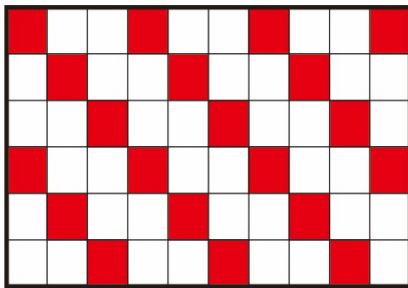
#### Motion Indication Bar



**Motion Detection** - By default, the 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 Detection Setting** - Users can adjust various parameters of Motion Detection.

- **Sampling pixel interval [1-10]** - **Sampling pixel interval** examines the differences between two frames. Users can configure the interval of sampling pixels. The default value is 1. For example, 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 the detection area (refer to the figure below). The alarm will be triggered when differences are detected.



- **Detection level [1-100]** - Users can configure the 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, the 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 lower accordingly.
- **Time interval (sec) [0-7200]** - The value is the interval between each detected motion. The default interval is 10.

**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 **Enable brush** box 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.

**Triggered Action (Multi-option)** - The administrator can specify the alarm actions that will take when motion is detected. All options are listed as follows:

- **Enable Alarm Output** - Check **high** or **low** 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** - 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 a 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 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.

- **Upload Image by E-Mail** - 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 is 6 or smaller.

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

- **Send HTTP Notification** - Check **Send HTTP Notification**, select the destination HTTP address, and specify the parameters for event notifications when a **Motion Detection** is triggered. When an alarm is triggered, the notification can be sent to the specified HTTP server.
- **Record Video Clip** - Check **Record Video Clip** and select a video recording storage type, **SD Card** or **NAS (Network-Attached Storage)**. The Motion Detection recording will be stored in the microSD/SD card or the NAS when motion is detected.

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.

- **File Name** – Enter a file name in the field. The file name format of the uploaded image can be set to one of the following:

- **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.

Click **Save** to save any changes made to the Motion Detection.

## Video Mask

### Active Mask Function

- ☐ Enable to display Mask1
- ☐ Enable to display Mask2
- ☐ Enable to display Mask3
- ☐ Enable to display Mask4
- ☐ Enable to display Mask5

### Mask Setting

Mask color black ▼

save

### Active Mask Function

- **Add a Mask** - Check an **Enable to display Mask** checkbox, and a red frame will display in the Live Video pane. Drag and drop to adjust the mask's size and place it on the target zone. Five video masks can be set.

**Note** Set the Video Mask slightly bigger than the object.

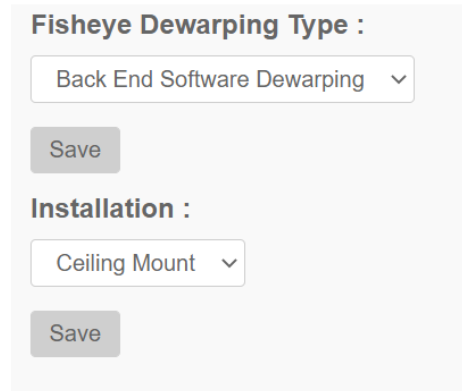
- **Cancel a Mask** - Un-check the checkbox to delete a Video Mask; the mask will disappear from the Live Video pane.

### Mask Setting

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

## Fisheye Setting

**Fisheye Dewarping Type** - Choose a method to dewarp the fisheye source images. The options are **Front End Camera Dewarping** and **Back End Software Dewarping**. After a dewarping type is selected, click **Save**.



**Fisheye Dewarping Type :**

Back End Software Dewarping ▾

Save

**Installation :**

Ceiling Mount ▾

Save

- **Front End Camera Dewarping** - Front End Camera Dewarping is a dewarping method that corrects fisheye source images. Dewarping images from the camera can reduce network usage and image processing load of the backend device. It also allows the camera to record or take snapshots of the dewarped images.

With this method, when viewing the dewarped images from the camera's web browser configuration interface, the video format of the stream needs to be set.

- **Back End Software Dewarping** - Back End Software Dewarping is a dewarping method that corrects the fisheye source images by a backend device or a backend software with a dewarping function. Dewarping by this method can correct high resolution images and deliver clear dewarped images.

With this method, users can also view the dewarped images from the camera's web browser configuration interface. The fisheye source images will be dewarped by the Viewer and displayed on the home page. However, users can only record video or take snapshots of the fisheye source images delivered from the camera.

**Installation** - Select the camera's installation method, so the dewarped images can be viewed with the correct viewing modes. Select a method from the drop-down list according to the location that the camera is installed. Choose **Ceiling Mount** if the camera is mounted to the ceiling, or select **Wall Mount** if the camera is mounted to the wall.

Click **Save** after setting Fisheye Dewarping Type and Installation.

## Text Overlay

Display data including date & time / text string / subtitle / image on the live video pane.

**Overlay type**

☒ Include date & time  
type date ▼  
String align Left ▼

☒ Include text string  
  
String align Left ▼

☒ Include subtitle  
  
  
  
  
  
String align Left ▼

☒ Include Image  
Image align Left ▼

**Text overlay setting**

Text overlay color white ▼    Text overlay size Small ▼

**Image overlay setting**

Image transparency 255

Image upload Choose File No file chosen

**Overlay Type** - Users can select at most three items out of four options including date & time / text string / subtitle / 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. Click and drag Date & Time to the 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. Click and drag the text string to the 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. Click and drag the subtitle to a 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. Click and drag the image to the preferred display position, and then decide the string align position (left / right).

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

**Text Overlay Setting** - 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 settings.

**Image Overlay Setting** - 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 an 8-bit BMP file; the length should be a multiple of 32, and the width should be a multiple of 4. The maximum resolution of the image should not exceed 32768 pixels.

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

## STREAMING SETTING

### Video Resolution

The screenshot displays a web-based configuration interface for video streaming settings. It is organized into four main sections: 'stream 1', 'stream 2', 'stream 3', and 'MJPEG'. Each section contains various settings for video encoding and resolution.

**stream 1**

- Encoding: Yes (dropdown)
- Encode Type: H.264 (dropdown)
- Resolution: 4000 x 3000 (dropdown)
- Rate Control: LBR (dropdown)
- Compression: High (dropdown)
- Dynamic GOV: Enabled (dropdown)
- Profile: Main profile (dropdown)
- Framerate: 15 (slider and input)
- Bitrate: 8192 (slider and input)
- GOV Length: 30 (slider and input)
- Max. GOV: 60 (slider and input)

**stream 2**

- Encoding: Yes (dropdown)
- Encode Type: H.264 (dropdown)
- Resolution: 720 x 480 (dropdown)
- Rate Control: VBR (dropdown)
- Profile: Main profile (dropdown)
- Framerate: 10 (slider and input)
- Bitrate: 1024 (slider and input)
- GOV Length: 20 (slider and input)

**stream 3**

- Encoding: No (dropdown)

**MJPEG**

- Encode Type: MJPEG (dropdown)
- Resolution: 640 x 480 (dropdown)
- Framerate: 10 (slider and input)

At the bottom right of the interface are two buttons: 'Save' and 'Reset'.

**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.

**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 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**, or **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 settings.

**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**.

**Framerate** - Video framerate is for setting the frames per second (fps) if necessary. The default setting is 25 fps (Front End) or 20 fps (Back end). The maximum framerate range of each stream will change according to the selected video resolution.

**Bitrate** - The default setting of the H.265/H.264 bitrate for Stream 1/ Stream 2 is 4096 kbit/s. The setting range is from 64 to 20480 kbps, and the total bit rate should not exceed 40960 kbps.

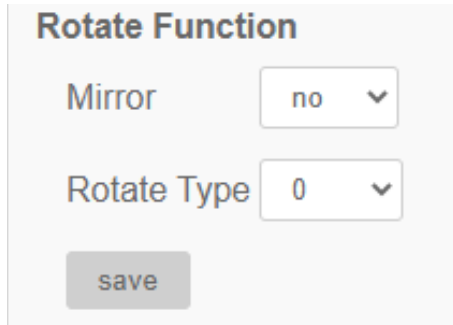
**GOV Length** - Users can set the GOV length to determine the frame structure (I-frames and P-frames) in a video stream to save bandwidth. Less bandwidth is needed if the GOV length is set to a high value. However, the shorter the GOV length, the better the video quality. The default setting for Stream 1/ Stream 2 is 50. The setting range of the GOV length is from 1 to 4094.

**Q (Quality) Factor (Encode Type MJPEG Only)** - The default setting of MJPEG Q factor is 35; the setting range is from 1 to 70.

Click **Save** to confirm Video Resolution settings. Click **Reset** to return to previous settings.

## 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.

A screenshot of a web interface titled "Rotate Function". It contains two settings: "Mirror" with a dropdown menu currently showing "no", and "Rotate Type" with a dropdown menu currently showing "0". Below these settings is a grey button labeled "save".

**Rotate Function**

Mirror no ▼

Rotate Type 0 ▼

**save**

- **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** degrees from the drop-down menu to rotate the image.

Click **Save** to confirm the settings.

## Web Viewer

With the **Video OCX protocol setting**, 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 :**

☒ RTP over UDP  
☐ RTP over RTSP(TCP)  
☐ RTSP over HTTP  
☐ MJPEG over HTTP  
☐ Multicast mode

Multicast Stream 1 Video Address	<input type="text" value="0.0.0.0"/>	Port	<input type="text" value="0"/>	TTL	<input type="text" value="1"/>
Multicast Stream 2 Video Address	<input type="text" value="0.0.0.0"/>	Port	<input type="text" value="0"/>	TTL	<input type="text" value="1"/>
Multicast Stream 3 Video Address	<input type="text" value="0.0.0.0"/>	Port	<input type="text" value="0"/>	TTL	<input type="text" value="1"/>
Multicast Stream 4 Video Address	<input type="text" value="0.0.0.0"/>	Port	<input type="text" value="0"/>	TTL	<input type="text" value="1"/>
Multicast Stream Audio Address	<input type="text" value="0.0.0.0"/>	Port	<input type="text" value="0"/>	TTL	<input type="text" value="1"/>

**Note:**  
This page only applies to video streams going to a ActiveX viewer.

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 **Save** to confirm the settings.

## Audio

The administrator can adjust the sound **Transmission Mode**, the **Server Gain Setting** and the audio **Bit Rate**. Setting for enabling sound recording to the microSD/SD card is also available.

**Audio**

**Transmission Mode:**

- ☐ Full-duplex (Talk and listen simultaneously)
- ☐ Half-duplex (Talk or listen, not at the same time)
- ☐ Simplex (Talk only)
- ☒ Simplex (Listen only)
- ☐ Disable

**Server Gain Setting:**

Input gain:

Output gain:

Bit Rate:

Save

**Recording to Storage:**

Save

### Transmission Mode

- **Full-duplex (Talk and Listen simultaneously)** - In Full-duplex mode, the local and remote sites can communicate with each other simultaneously.
- **Half-duplex (Talk or Listen, not at the same time)** - In the Half-duplex mode, the local / remote sites can either talk or listen to the other site, but not simultaneously.
- **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** - 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 includes **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 rates will allow for higher audio quality and require a bigger bandwidth. Click **Save** to confirm the settings.

**Input Type** - Selectable input types are **Line in** and **External Mic**. If the audio input from the **audio device** is connected via the Audio In connectors, users should select **Line in**. If the audio input from the **microphone** is connected via the Audio In connectors, users should select **External Mic** for better sound quality. Click **Save** to confirm the settings.

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

<b>Note</b> If the chosen bit rate is not compatible with the player, there will only be noise instead of audio during playback.
--

Click **Save** to confirm the settings.

Are any parts of this manual incomplete or unclear? Please let us know! Contact us at [support@avertx.com](mailto:support@avertx.com) with your comments.

[www.avertx.com](http://www.avertx.com)

1-855-2AVERTX  
© 2024 AvertX

All rights reserved. No part of this publication may be reproduced by any means without written permission from AvertX. The information in this publication is believed to be accurate in all respects. However, AvertX cannot assume responsibility for any consequences resulting from the use thereof. The information contained herein is subject to change without notice. Revisions or new editions to this publication may be issued to incorporate such changes.