LUMINYS

N9 Series Network Camera

User Manual

Rev. 1

Foreword

Revision History

Revision	Content	Release Date
1	Initial Release	July 2025

Safety Instructions

The following symbols might appear in the manual.

Symbol	Definition
⚠	Indicates a risk hazard that, if not avoided, may result in death, injury, property damage, data loss, decreased performance, or unpredictable outcomes.
	Offers methods to help you troubleshoot issues or save time.
ⓘ	Provides more context and information.

Before You Begin

The deployment and operation of network-based surveillance equipment may be regulated under local or regional laws. Before proceeding, it is the user's responsibility to ensure the legal use of this device in the intended environment.

Prior to installation, confirm that all items listed under the In the Box section are present and undamaged. Refer to the Quick Start Guide for safety notices, and follow the Installation instructions in this manual to avoid improper setup, performance issues, or equipment damage.

This network camera is intended for users with basic knowledge of networking environments. It supports a wide range of applications, such as video monitoring, event detection, and integrated system deployments. Refer to the Configuration chapter for setup guidance to ensure optimal performance.

In the Box

Ensure all of the following items are presented and undamaged prior to installation:

- Screws
- Desiccant bag
- Double-sided tape
- Sunshield
- Alignment sticker
- Rubber pad for mounting bracket
- Waterproof joint
- Quick start guide
- L-shape allen wrench
- Mounting plate

Table of Contents

Connecting to the Camera

Log In to the Webpage

This section explains how to log in to the webpage using Chrome as an example. Follow the steps below to log in to the camera's web interface.

1. Navigate to the Device's IP address using the browser's address bar.
2. Enter the Device's login credentials.
3. Hit **Login**.

Main Page

This section introduces the main interface layout and its key elements. The main page includes the following components: Logo, Host Name, Camera Control Area, Configuration Area, Menu, and Live View Window.

Host Name

The displayed host name can be modified to match deployment requirements, particularly in multi-camera environments.

Camera Control Area

Profile Mode

This area provides access to three pre-configured streaming profiles: Max. View, Recording View, and Live View. Each profile uses a distinct video stream with its own resolution, encoding parameters, multicast settings, and metadata configuration.

These profiles can be managed under **Configuration → Media → Media profiles**.

Manual Trigger

Use this control to manually activate or deactivate event triggers. Ensure event settings are configured in the Application section prior to use. Up to three event types can be defined.

To show or hide this control on the homepage, go to **Configuration → System → Homepage Layout → General settings → Customized** button, then adjust the “Show manual trigger button” checkbox.

Configuration Area

Configuration

Click this button to access the system’s configuration page. It is recommended that administrative access be secured with a password to prevent unauthorized changes.

Language

Select this option to choose the interface language. Supported languages include: English, Deutsch, Español, Français, Italiano, 日本語, Português, 简体中文, and 繁體中文.

Language preferences can also be updated from within the Configuration page.

Control Panel Options

Hide Button

Use this button to show or hide the control panel on the main interface.

Resize Buttons

The resize buttons adjust the display scale of the homepage:

1. **Auto:** Automatically fits the video cell to your display.
2. **100%:** Displays the homepage at its original size.
3. **50%:** Reduces the homepage view to 50% of its original size.
4. **25%:** Reduces the homepage view to 25% of its original size.

Snapshot

Click the **Snapshot** button to capture the current video frame. A pop-up window will display the snapshot. Right-click the image and choose **Save Picture As** to store it. File formats include **JPEG (.jpg)** and **BMP (.bmp)**.

Stop

Click the **Stop** button to end the video stream. Click **Resume** to restart it.

Volume

Adjust playback volume with the **slider bar** if audio is enabled.

Mute

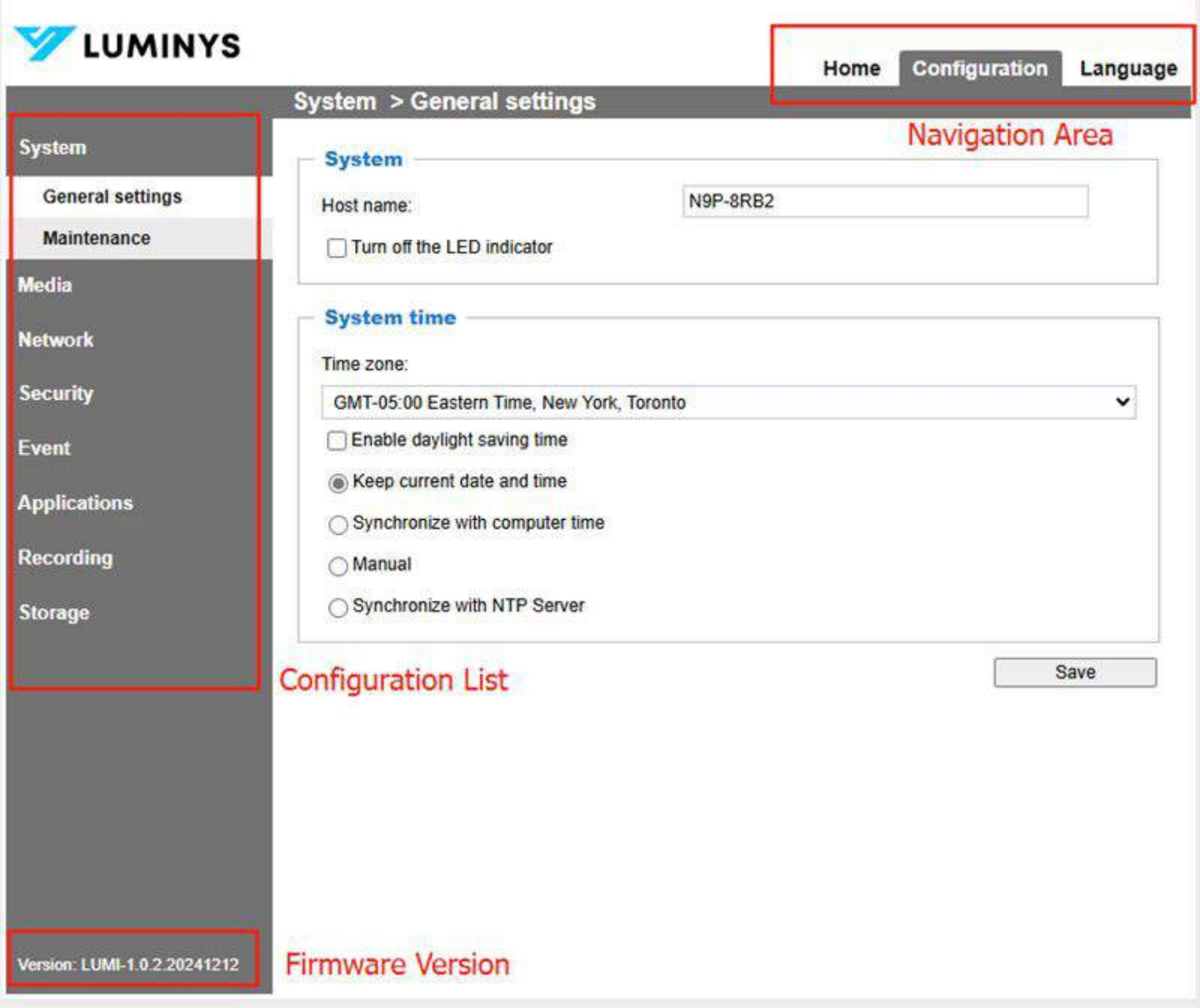
Click the **Mute** button to turn off audio. The button label will change to **Audio On**.

Full Screen

Click the **Full Screen** button to enter full-screen mode. Press the **Esc** key to return to normal view.

Configuration

The Configuration section provides access to all system settings required for device setup, customization, and management. Use the navigation menu to access different configuration categories, such as system, media, network, security, and event settings.

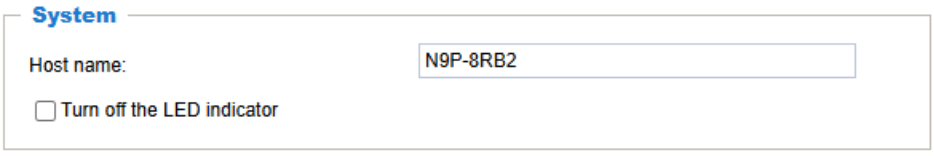


System Settings

This section provides configuration options for system identity, date and time settings, and general administrative tools.

General Settings

Menu Path: Configuration → System → General settings



This page allows administrators to define the device name and installation location for identification purposes.

Host Name

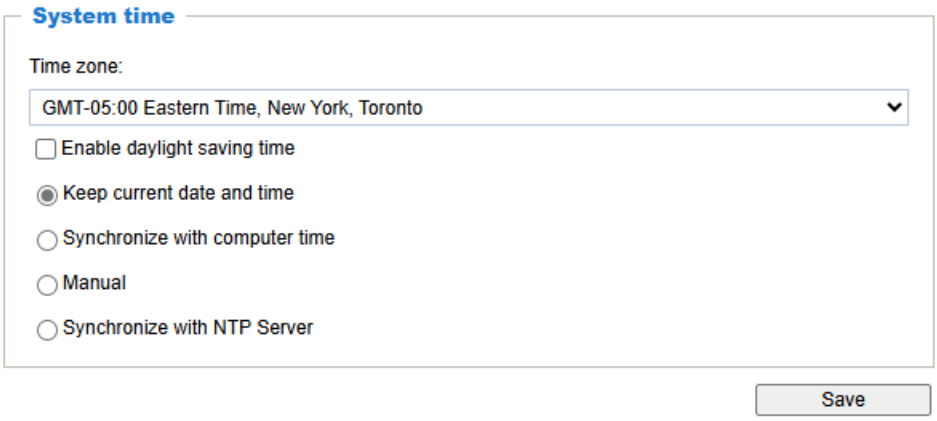
Specify a name for the device. This name will be displayed in the system interface.

Turn Off the LED indicator

Enable this option to switch off the device's status LED. This may be useful in environments where indicator lights are not desired, such as discreet monitoring setups.

System Time

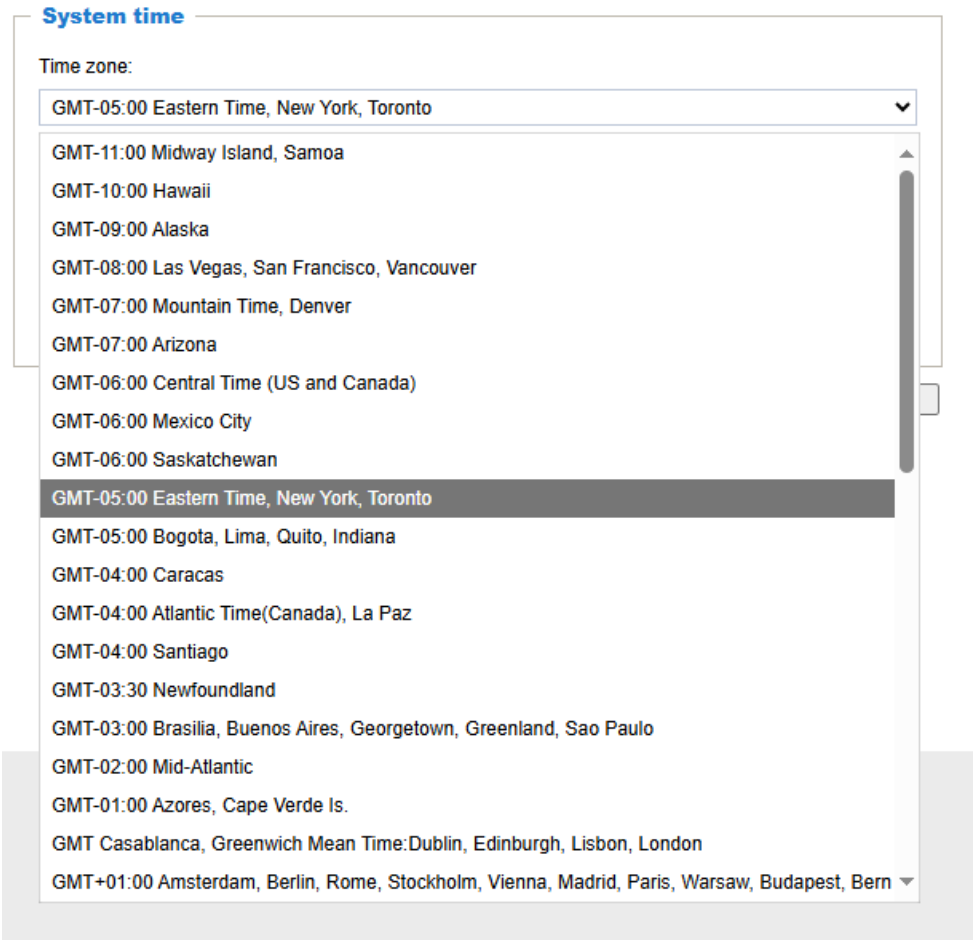
Menu Path: Configuration → System → System time



The system time must be accurately configured to ensure proper event logging and video timestamping. You can set the time manually or synchronize it with a time server.

Time Zone

Select the appropriate time zone for the installation site.



Synchronize With Computer Time

Use this option to align the camera's date and time with the local computer. The system will display the current time of the PC as a read-only reference once synchronization is applied.

Manual

Manually adjust the system's date and time.

Synchronize With NTP Server

Choose whether to synchronize the time with an NTP server. Enter the NTP server address if applicable.

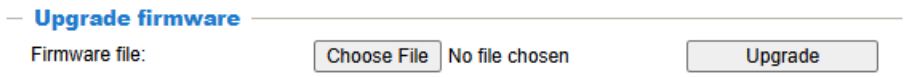
Maintenance

Menu Path: Configuration → System → Maintenance

This section provides tools for firmware upgrades, system reboot, and configuration file management.

Upgrade Firmware

Upload a firmware file to update the device. Ensure that the firmware is correct and compatible with the model before proceeding with the upgrade.



To upgrade the firmware, follow the steps below:

1. Download the latest firmware file from your provider.
2. Click **Browse**... and locate the firmware file on your computer.
3. Click **Upgrade**. The camera will begin the upgrade process and automatically restart once the upgrade completes.

If the upgrade is successful, the following message will appear:

Reboot system now!!
This connection will close.

At this point, reconnect to the camera interface once the system restarts.

If an invalid firmware file is selected, the system may display a message such as:

Starting firmware upgrade...
Do not power down the server during the upgrade.
The server will restart automatically after the upgrade is completed.
This will take about 1 - 5 minutes.
Wrong PKG file format
Unpack fail

Reboot

Restarts the device without altering current configuration settings.

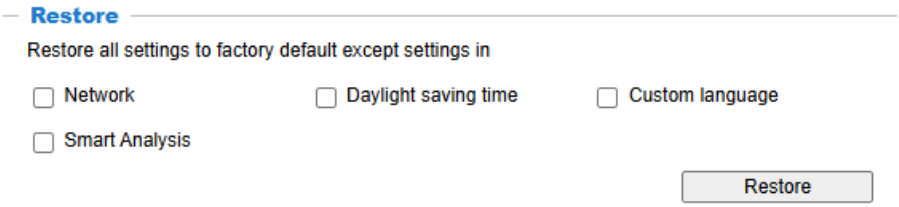
This feature allows you to reboot the network camera. The reboot process typically takes about one minute. Once completed, the live view page will automatically reload in your browser.

During the reboot, the system will display the following message:

> The device is rebooting now. Your browser will reconnect to http://192.168.5.151:80/
>
> If the connection fails, please manually enter the above IP address in your browser.

If the browser does not automatically reconnect after the reboot, manually enter the IP address of the network camera in the address bar to restore the connection.

Restore



The Restore function resets the device to its factory default settings. Before proceeding, you can choose to retain specific configuration items by selecting from the available options:

Network

Keeps the current network configuration (e.g., IP address, subnet mask, gateway).

Daylight Saving Time

Retains the current Daylight Saving Time setting.

Custom Language

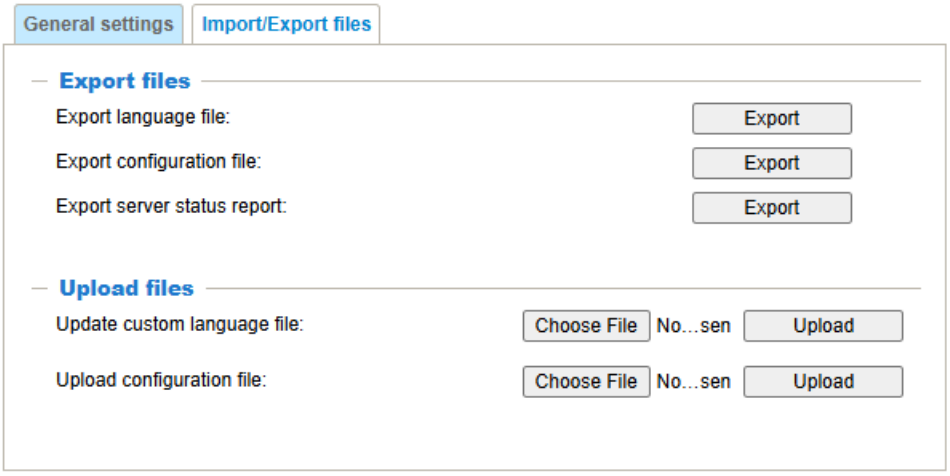
Preserves any custom language files uploaded to the system.If no options are selected, all configuration data will be erased, and the system will return to factory default settings.

During the restore process, the following message is displayed:

> The device is rebooting now. Your browser will reconnect to http://192.168.5.151:80/
>
> If the connection fails, please manually enter the above IP address in your browser.

Import/Export Files

This feature allows you to export or update configuration files, custom language files, and daylight saving time settings.



Export Language File

Click to export the current language strings. Supported languages include: English, Deutsch, Español, Français, Italiano, 日本語, Português, 简体中文, and 繁體中文.

Update Custom Language File

Click **Choose File**... and select your custom language file to upload.

Export Configuration File

Click to download all current device parameters and user-defined scripts as a configuration file.

Update Configuration File

Click **Choose File**... to upload a saved configuration file.

Note: The configuration file must match the model and firmware version of the device. Uploading an incompatible file is not recommended, especially if the device has static IP settings or custom configurations.

Export Server Status Report

Click to download a report containing server-related data such as system time, logs, process status, memory usage, file system status, network status, and kernel messages.

If an incorrect file format is selected during upload (e.g., a file without a .xml extension), the system will display the following warning:

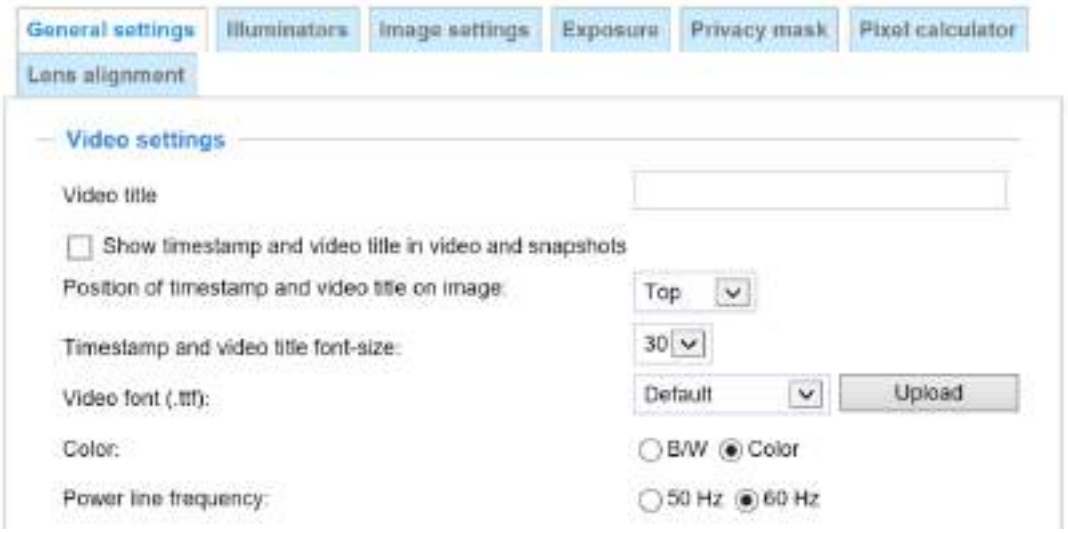
The file must have a .xml filename suffix.

Media Configuration

Image

Menu Path: Configuration → Media → Image

General Settings



Video Title

Enter a label to display in the video stream. The zoom level will also be shown when zooming in or out in the live view. Use the mouse scroll wheel to zoom, up to 12x magnification.

Position of Timestamp and Video Title on Image

Choose whether the timestamp and video title appear at the top or bottom of the video frame.

Timestamp and Video Title Font Size

Set the font size for the timestamp and video title overlays.

Video Font (.ttf)

Upload a TrueType Font (.ttf) file for use in video overlay text.

Color

Select whether the video should be shown in color or black and white.

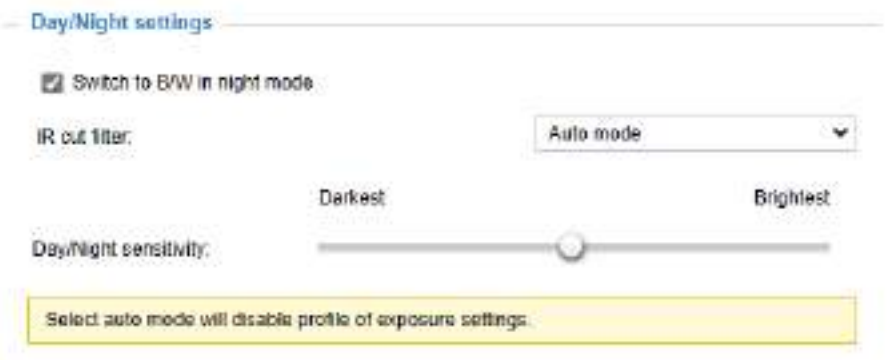
Power Line Frequency

Choose the appropriate setting (50Hz or 60Hz) based on your region's electrical frequency to help reduce flicker in certain lighting environments.

Note: After changing this setting, you must unplug and reconnect the device's power source for the update to take effect.

Day/Night Settings

This section configures how the camera switches between color and black-and-white modes based on lighting conditions.



Day/Night Mode

Select the camera's operating mode based on lighting conditions:

- **Auto:** Switches between day and night modes automatically.
- **Day:** Keeps the camera in color mode.
- **Night:** Keeps the camera in black-and-white mode.

IR Cut Filter

Select the operation mode for day and night behavior:

- **Auto:** Automatically switches between day and night based on scene brightness.
- **Day:** Forces the camera to remain in color mode.
- **Night:** Forces the camera to operate in black-and-white mode.

IR Cut Filter Sensitivity

Adjusts how responsive the IR cut filter is to changes in lighting. Higher sensitivity causes the filter to switch states more quickly when lighting conditions fluctuate.

IR Illuminator Control

Built-In IR Illuminator in Night Mode

Enable this option to activate the camera's onboard IR illuminator when low-light conditions are detected and night mode is triggered.

Smart IR

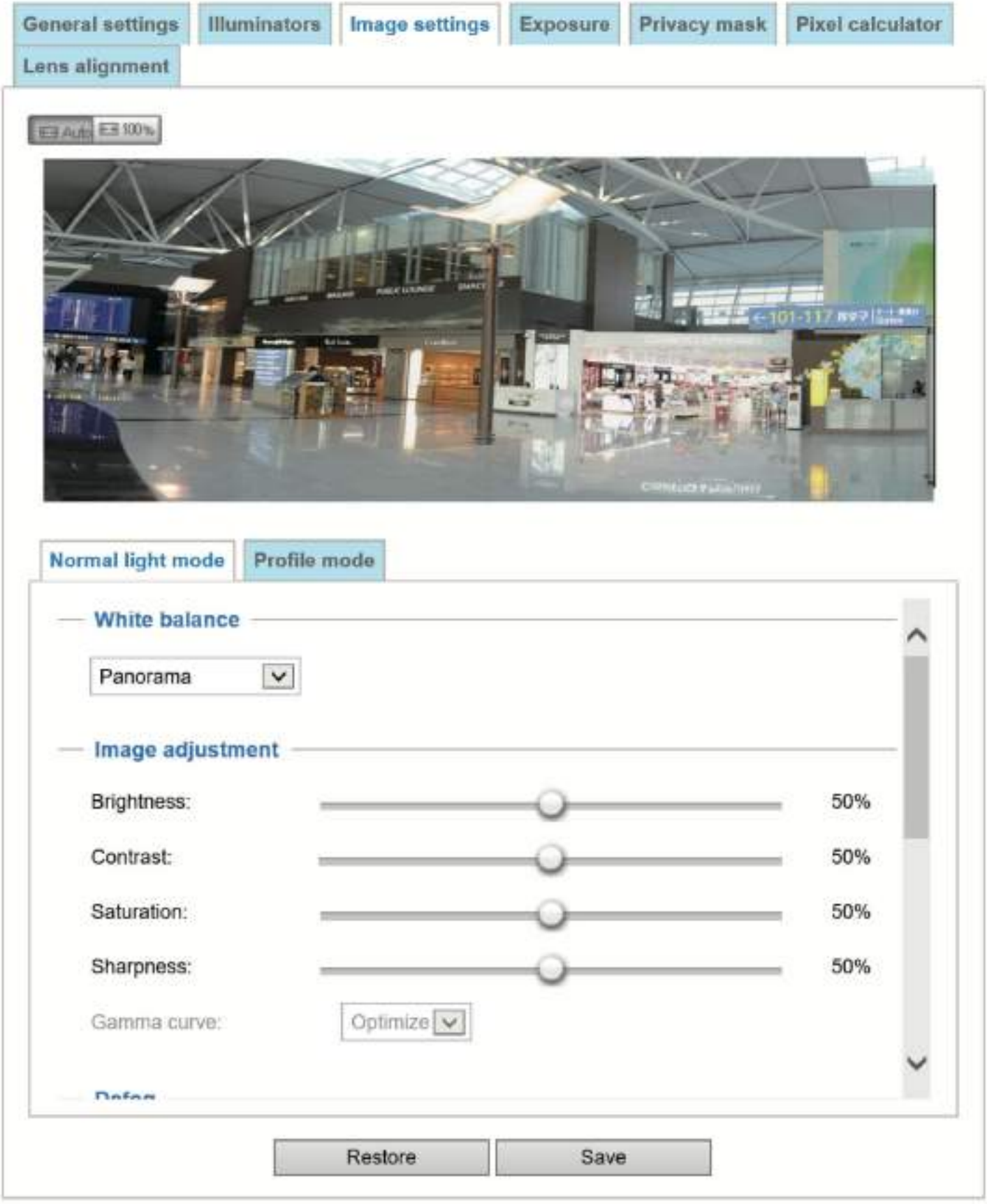
Anti-Overexposure: When enabled, the camera dynamically adjusts infrared output to prevent nearby objects from becoming overexposed in night mode.

The Smart IR function is most effective when subjects are close to the lens and IR light source. For example, if an object or person is within 3 meters of the camera, Smart IR helps reduce brightness distortion. However, at greater distances (such as 5 meters or more), the benefit of Smart IR becomes less significant.

Smart IR disabled; 5 M distance	Smart IR enabled; 5 M distance
	
Smart IR disabled; 3 M distance	Smart IR enabled; 3 M distance

Image Settings



Sensor Mode

By default, the firmware uses Panorama mode to create a continuous 180° panoramic image.

If Regional mode is selected, the camera presents four segmented views based on individual lighting conditions, without stitching them together.

White Balance

Adjust the camera's color temperature setting for accurate image coloration. You can follow these steps to set white balance for optimal color accuracy:

1. Hold a white or cool-colored object (such as white or light blue paper) in front of the lens. Allow the camera to auto-detect the white balance.
2. When the correct color temperature is displayed, click **On** to lock the current value.

You may also adjust the color tone manually by using the RGain and BGain sliders.

Use Snow mode in snowy or shaded environments where higher white balance values are often needed. This setting helps maintain color accuracy in conditions where traditional white balance tuning might fail.

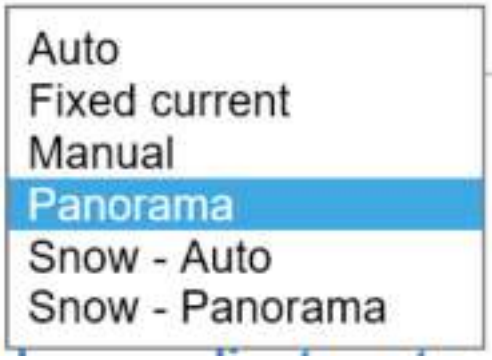


Image Adjustment

- **Brightness:** Adjusts the overall brightness of the image. Range: 0% to 100%.
- **Contrast:** Adjusts the contrast between dark and light areas. Range: 0% to 100%.
- **Saturation:** Adjusts the color intensity. Range: 0% to 100%.
- **Sharpness:** Enhances the clarity of edges and fine detail. Range: 0% to 100%.
- **Gamma Curve:** Adjusts tonal distribution between shadows and highlights. Range: 0.0 to 0.45. You may select a value or use firmware-optimized display settings to adjust contrast and luminance across bright and dark areas. Note: This option is disabled when WDR is enabled.

Defog

Improves image visibility in low-clarity conditions such as fog, smoke, or smog.

Highlight Mask

Strong light sources will be masked to reduce glare and improve contrast. This feature is helpful in high dynamic scenes to reduce spotlight effects. Note: Color fringing may occur around the edges of intense light sources.

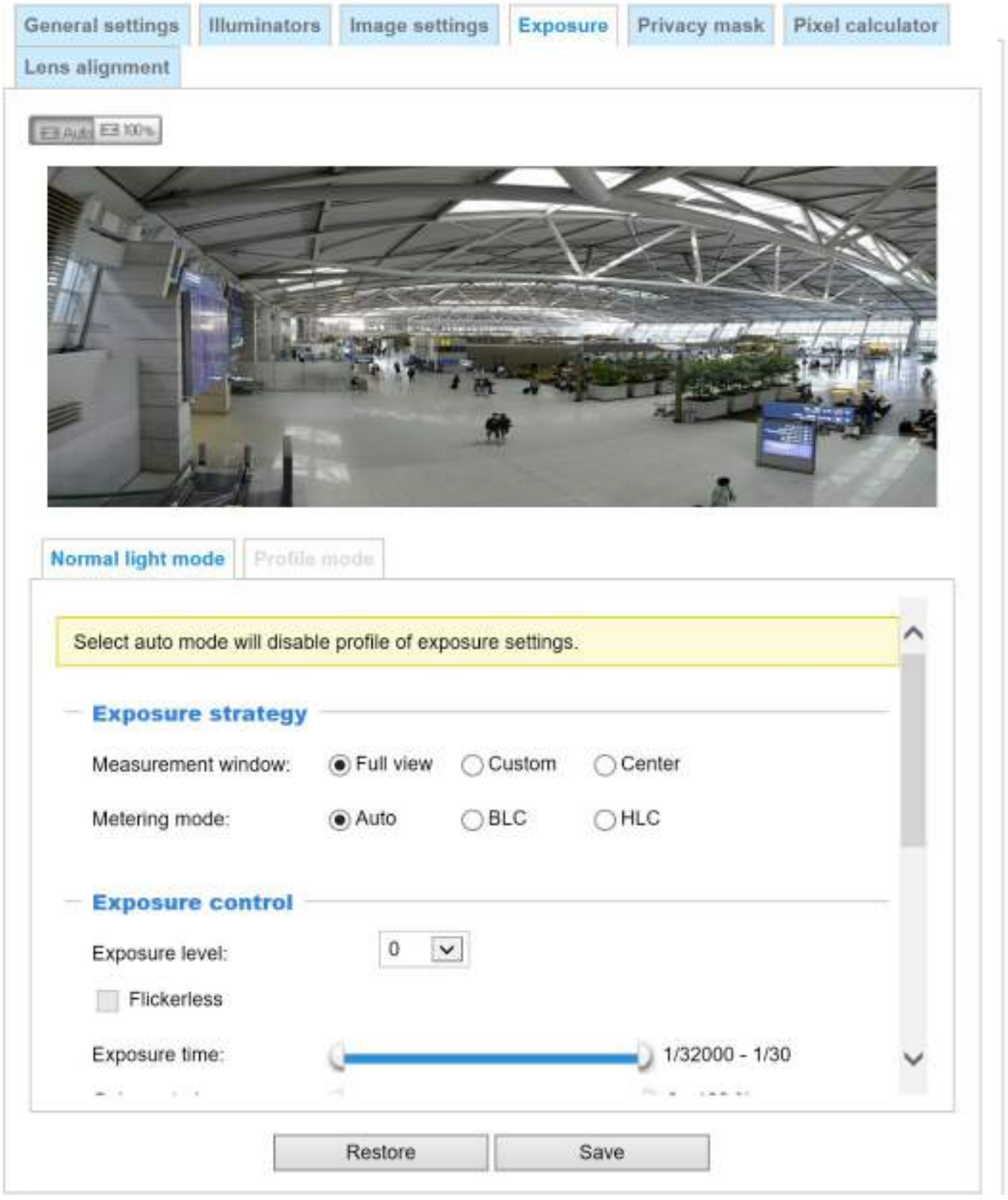
Noise Reduction

Enable this setting to reduce image noise and flicker, especially in low-light conditions. This applies the onboard 3D Noise Reduction function. Use the dropdown to select the desired reduction level.

3D Noise Reduction is most effective in low-light environments. In fast-moving scenes, it may produce motion trails or after-images. Lower the strength level or disable the function as needed.

Exposure

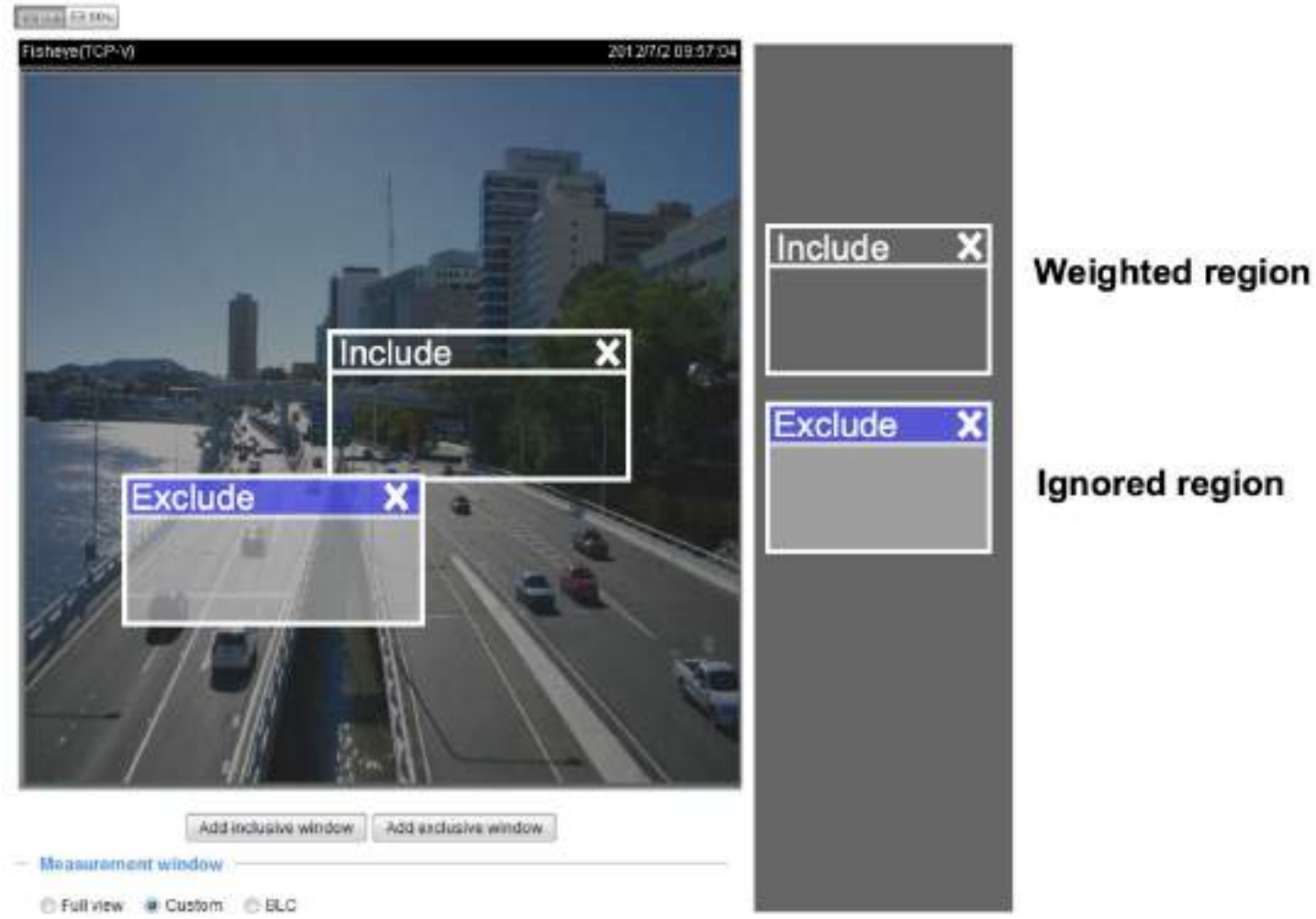
On this page, you can configure the exposure measurement window, exposure level, exposure mode, exposure time, gain control, and day/night mode settings.



Measurement Window

You can configure specific areas of the screen where the camera prioritizes light measurement. This helps avoid improper exposure caused by strong lighting, such as sunlight through windows.

- Full view: The entire scene is used to calculate exposure.
- Custom: Define up to 10 custom windows to include or exclude from exposure calculation.



Exposure Control

Exposure Level

Allows you to manually adjust the exposure from -0.7 to +0.7. A lower value makes the image darker; a higher value makes it brighter.

Exposure Time / Gain Control

Use the semi-circular sliders to define a range of shutter speeds and gain values. The system will automatically select the optimal combination. Shorter shutter speeds are useful for capturing motion but require higher gain for brightness. Longer shutter speeds provide more light but may result in blur from movement.

Flickerless

In fluorescent lighting, fixed iris cameras may display image flickering caused by mismatched power frequencies. Enabling this feature limits exposure time to 1/120 to 1/5 second to avoid this issue.

- In auto iris models, the iris adjusts automatically.
- In fixed iris models, brightness is adjusted digitally.

If overexposure is observed, consider disabling this option.

AE Speed Adjustment

This feature adjusts how quickly the system responds to changes in lighting. It is useful in environments like:

- Roadways or tunnels
- Parking entrances at night
- Vehicle-mounted installations

It allows the camera to quickly adapt to light level shifts when entering or exiting areas with different illumination.

WDR Pro

WDR (Wide Dynamic Range) helps maintain detail in scenes with both bright and dark areas. Use the checkbox to enable WDR Pro. Use the slider to select intensity based on contrast in your environment. Higher settings are recommended for strong backlighting or mixed lighting conditions.

WDR Enhanced

This function also improves detail in high-contrast scenes. When enabled, it balances brightness across dark and light regions of the image. Adjust the enhancement level using the slider based on your installation environment.

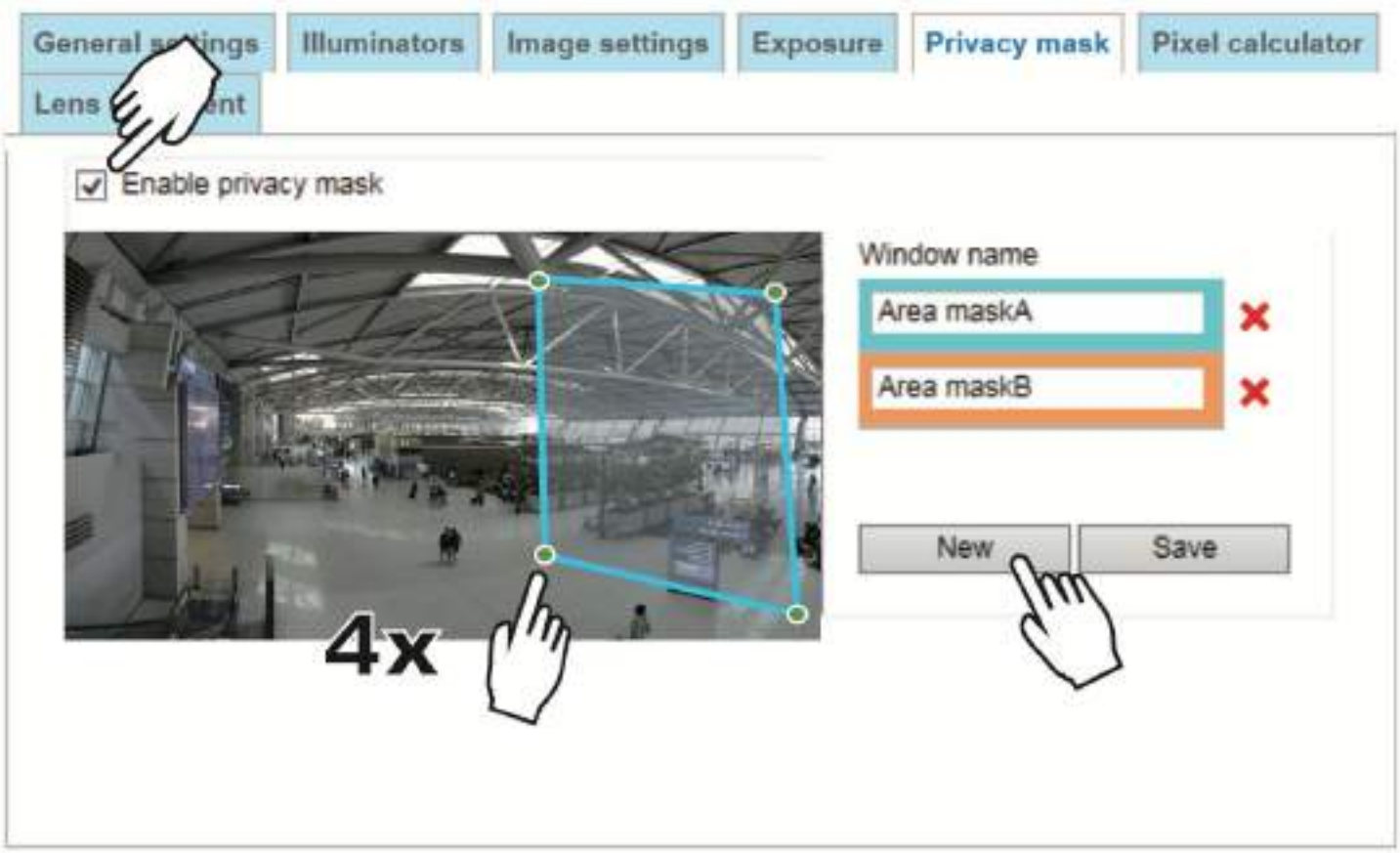
Profile Mode

Follow the steps below to set when the exposure settings should be applied.

1. Click the **Profile** mode tab.
2. Select one of the following modes: day mode, night mode, or schedule mode (requires manual input of start and end times).
3. Configure the exposure settings as needed.
4. Click **Save** to enable the setting and click Close to exit the page.

Privacy Mask

Click **Privacy Mask** to access the configuration page. This feature allows you to mask specific areas of the video feed to protect sensitive zones and maintain privacy.



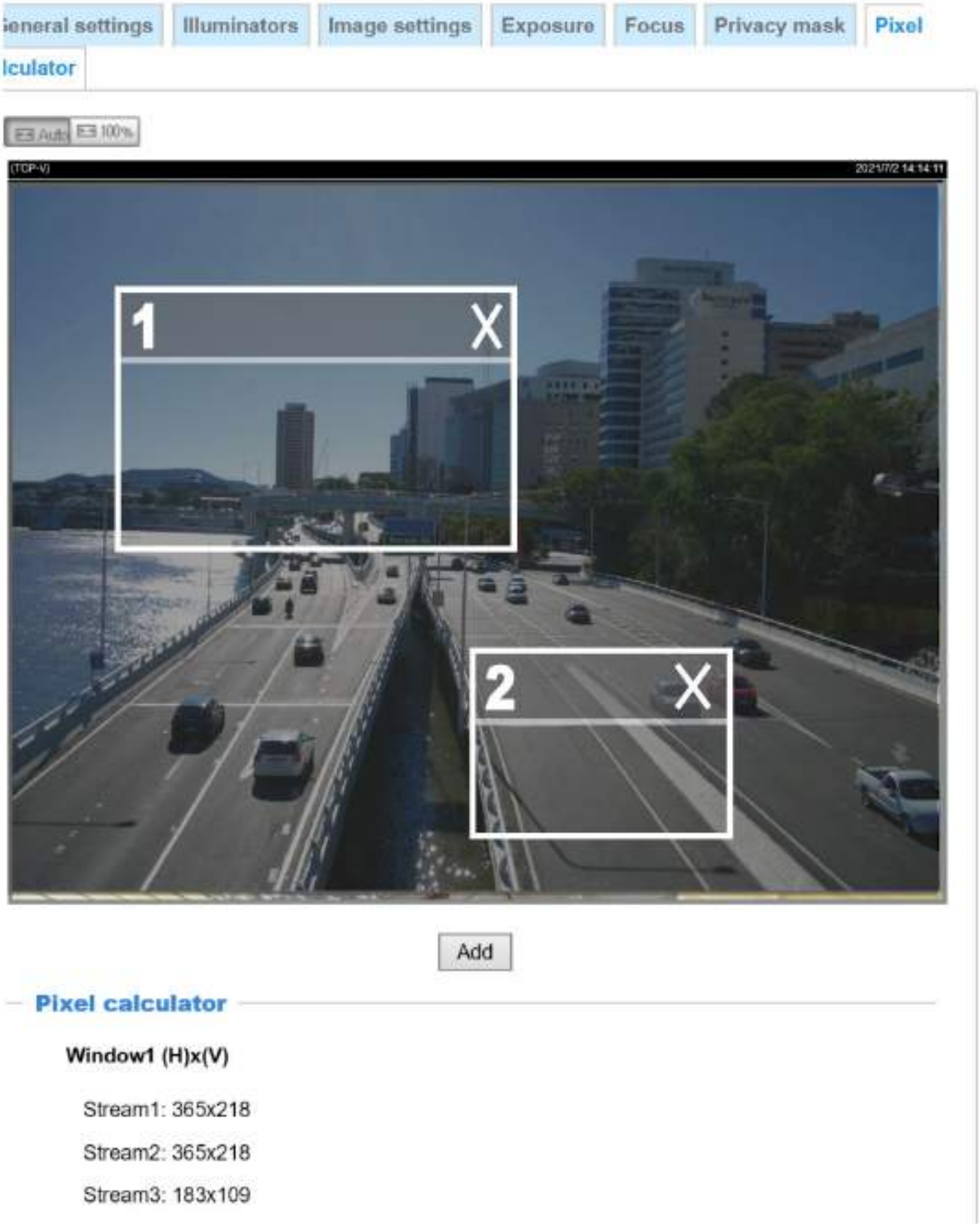
To create a privacy mask:

1. Click **New** to add a mask window.
2. Click four points in the image to define the shape of the mask area.
3. Enter a name for the mask window and click **Save** to apply the configuration.
4. Enable the privacy mask feature by checking the **Enable privacy mask** option.

Pixel Calculator

Click the **Add** button at the bottom of the screen to create a pixel calculator window. You can move and resize the window to align it with the area of interest.

Once added, the number of pixels along the edges of the window will be displayed. This helps determine whether the current image configuration meets certain requirements—such as the resolution needed for face recognition. For example, facial recognition typically requires a minimum of 130 pixels per meter.



The pixel values are shown per stream, depending on the resolution configured for each stream.

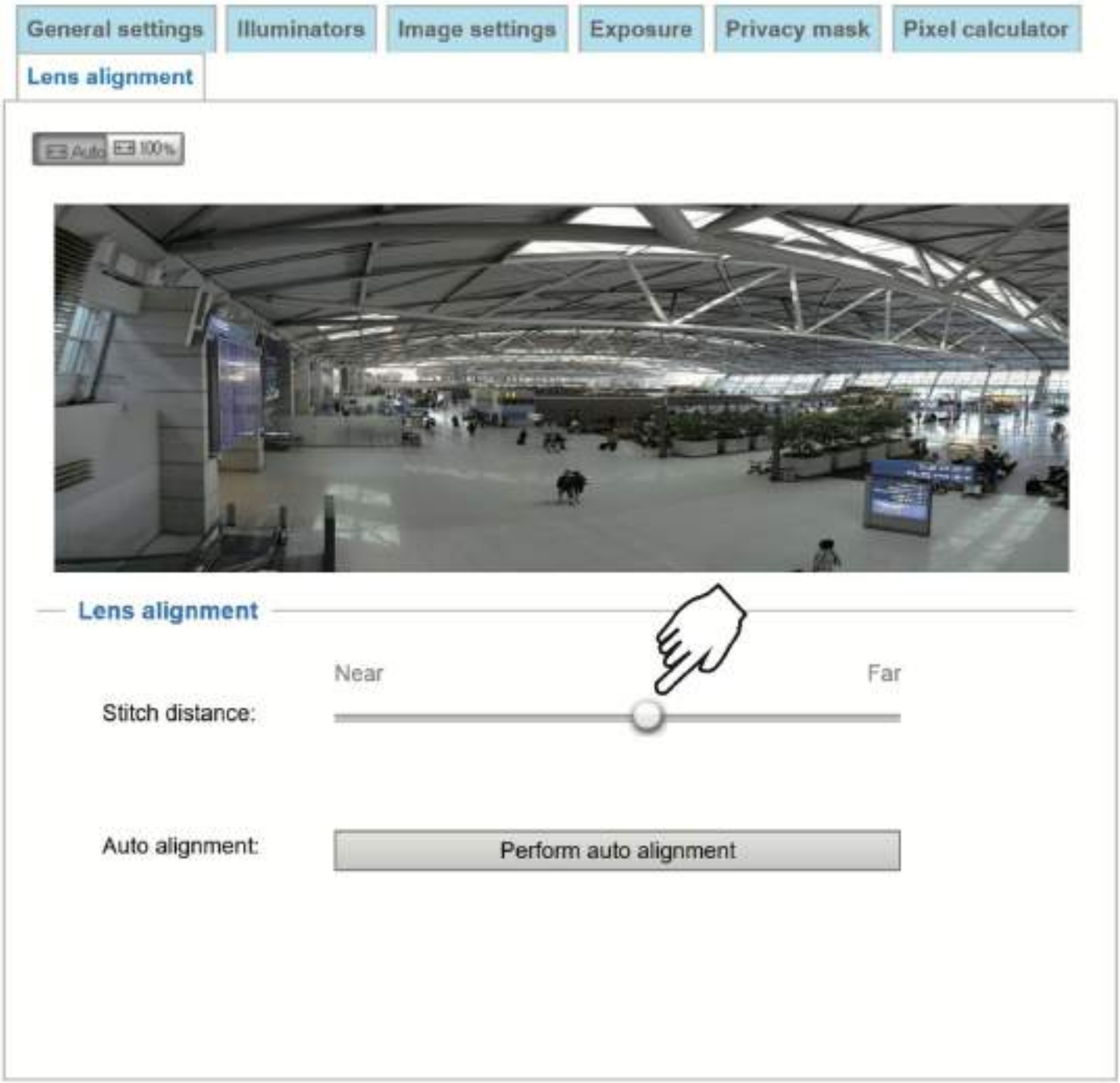
Lens Alignment

The default alignment distance is set to 10 meters. You can configure the distance between three (3) and 20 meters.

Because the fields of view (FOVs) from the dual lenses overlap slightly, the image stitching is optimized based on the distance to your intended area of interest. Use the slider to select the appropriate distance between the camera and your target scene for the most accurate stitched image.

The auto alignment option allows the system to automatically align and stitch the two image streams based on the current video feed. This process takes approximately one second to complete.

It is strongly recommended that there are no moving objects in the scene during the alignment process.

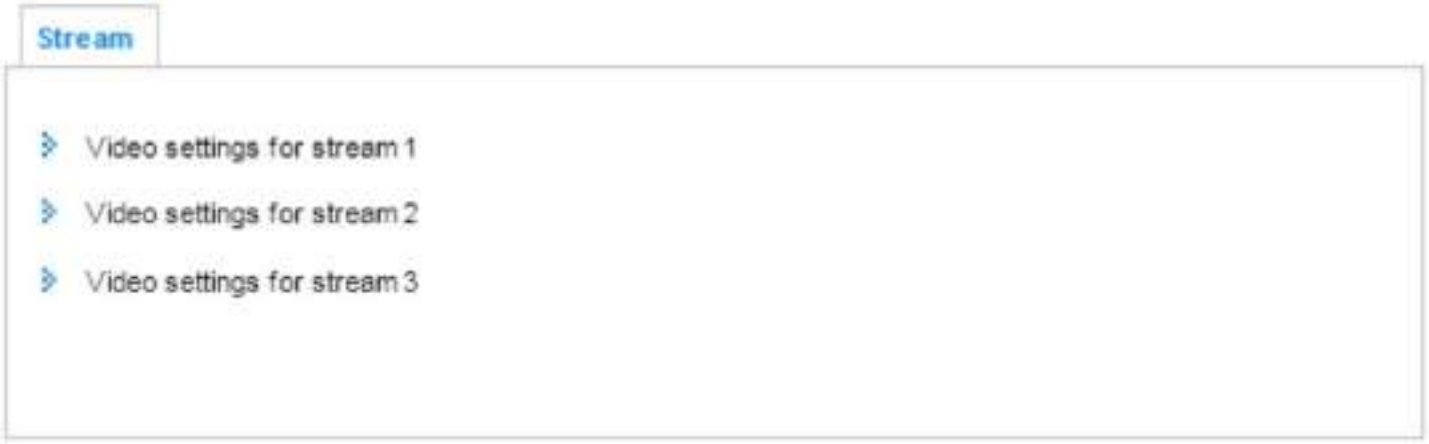


Once you are satisfied with the result, click **Save** to store the stitching configuration. If needed, click **Restore** to revert to the previous settings.

If your area of interest is located at a different distance, adjust the slider accordingly, and then perform the Auto alignment function again.

Video

Stream Settings



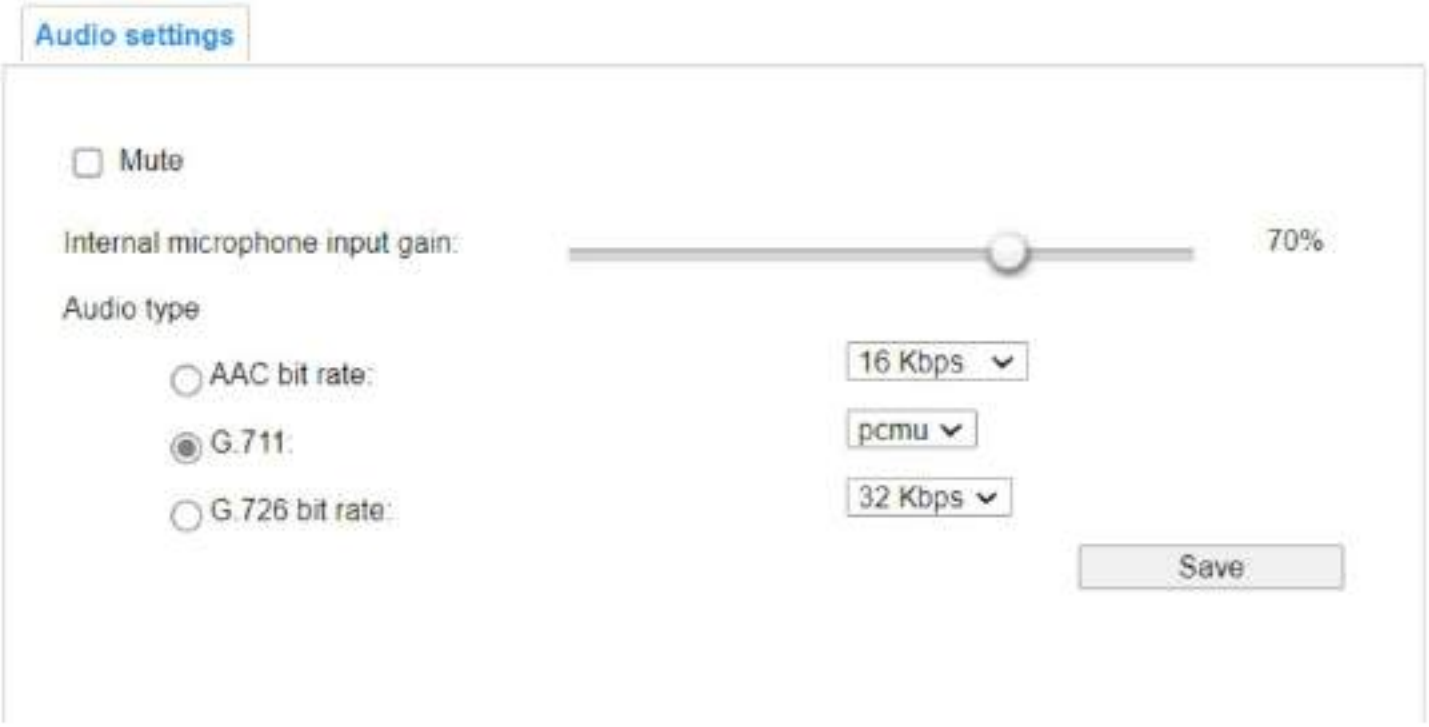
This network camera supports multiple video streams with configurable resolutions.

- Stream 1: Default frame size is 4864 x 1632
- Stream 2: Default frame size is 2432 x 816
- Stream 3: Default frame size is 1216 x 416

Click on a stream item to view its configuration details. The maximum frame size for each stream depends on your settings under the Viewing Window configuration.

Audio

Audio Settings



Mute

Enable this option to disable audio transmission from the camera to all connected clients. When mute is active, no audio will be transmitted—even if the client has enabled audio reception. In such cases, a notification message will appear on the client interface.

External microphone input

Adjust the gain level of the external microphone according to the surrounding environment. Available gain values range from +21 dB (highest sensitivity) to -33 dB (lowest sensitivity).

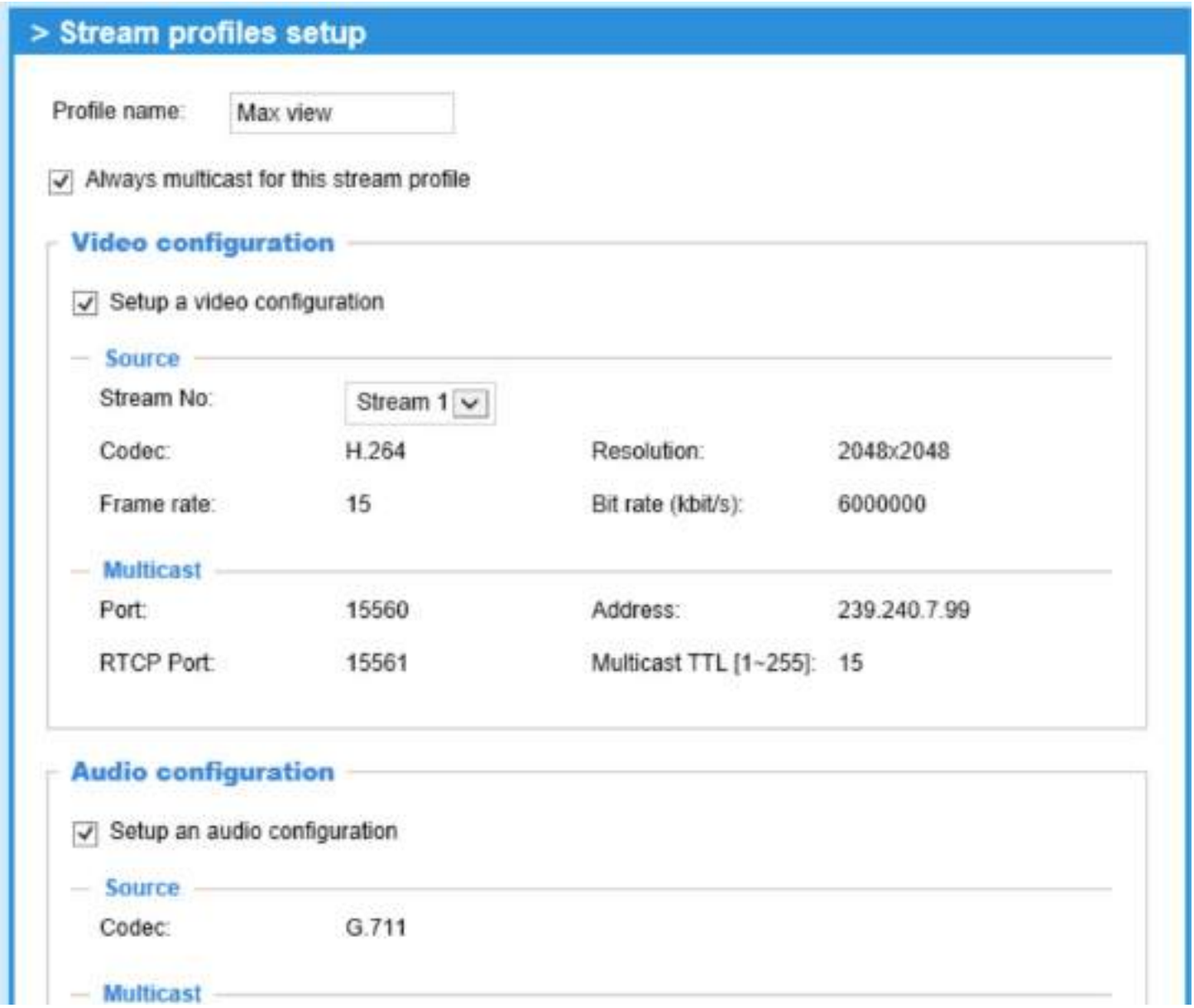
Audio type

Select the audio codec and sampling bitrate to be used:

- AAC: Widely compatible with modern devices. A typical setting is 32 kbps (AAC) or 64 kbps (MP3) for general voice transmission.
- G.711: Delivers good audio quality at approximately 64 kbps. Choose from PCMU (μ-Law) or PCMA (A-Law) encoding.
- G.726: A codec optimized for voice communication, supporting bitrates of 16, 24, 32, and 40 kbps.

After configuring these options, click **Save** to apply the audio settings.

Media Profiles



You can configure a dedicated video stream for each of the following default profiles:

- Max. View
- Recording
- Live View

Each profile supports independent stream settings such as resolution, frame rate, and codec. This allows you to optimize video performance for different use cases, including live monitoring and recording.

Network Settings

General Settings

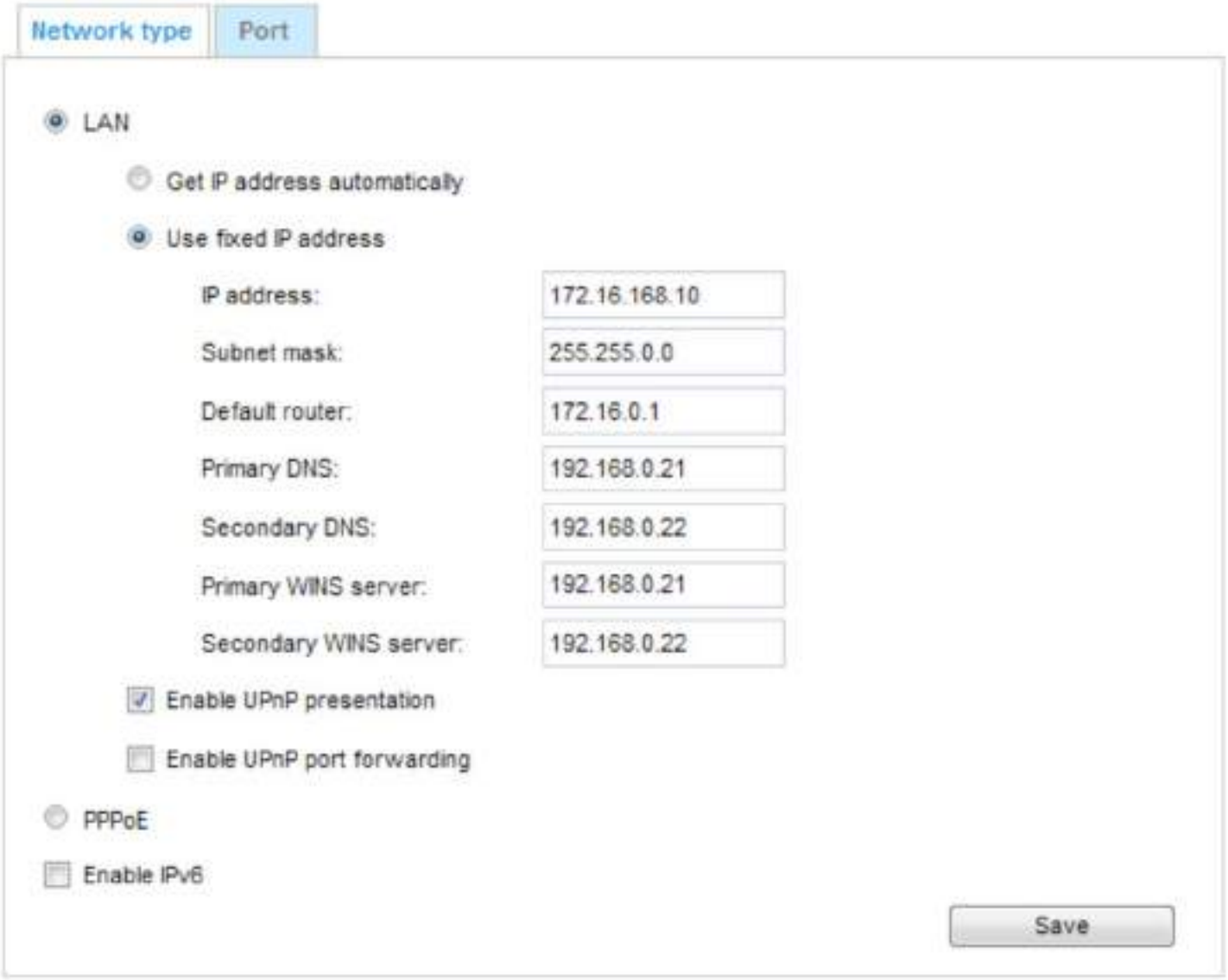
This section describes how to configure a wired network connection for the camera.

Network Type

LAN

Select this option when the camera is installed on a local area network (LAN) for internal access. This is the default setting. Click **Save** after configuration.

5. Get IP address automatically: The camera will request a dynamic IP from the DHCP server every time it connects to the network.
6. Use fixed IP address: Manually assign a static IP address. To set a fixed IP address, enter the static IP address, subnet mask, default gateway, and DNS server information provided by your network administrator or ISP.



7. **Subnet mask:** Defines whether the destination address is in the same subnet. Default: 255.255.255.0
8. **Default router:** The gateway address used to reach other subnets. Incorrect values may prevent connectivity.
9. **Primary DNS:** Translates domain names to IP addresses.
10. **Secondary DNS:** Serves as a fallback DNS server.
11. **Primary WINS server:** Maps NetBIOS names to IP addresses in a Windows environment.
12. Secondary WINS server: Backup WINS server.

UPnP

13. **Enable UPnP presentation:** When enabled, the camera appears in My Network Places on Windows systems that support UPnP.
14. **Enable UPnP port forwarding:** Allows the camera to automatically open required ports on a UPnP-enabled router for external access. Your router must support and have UPnP activated.

PPPoE (Point-to-Point over Ethernet)

Use this option if your camera connects directly to the internet through a DSL connection that requires a PPPoE account.

To configure:

1. Set up the camera on the LAN.
2. Navigate to Configuration → Event → Event settings → Add server to configure an email or FTP server.
3. Go to Add media and select System log to receive the camera's public IP address via email or FTP.
4. Navigate to Configuration → Network → General settings → Network type. Select PPPoE, enter the credentials provided by your ISP, and click **Save**.
5. The camera will restart.
6. After reboot, disconnect it from the LAN.

Enable IPv6

Select this option and click **Save** to activate IPv6 functionality. Please ensure that your network infrastructure and devices support IPv6. Supported browsers include Internet Explorer 6.5, Mozilla Firefox 3.0, or newer versions.

When IPv6 is enabled, the camera listens for router advertisements and automatically obtains a link-local IPv6 address.

Streaming Protocol

HTTP Streaming

To enable HTTP authentication for streaming, make sure the camera has an administrator password configured. Refer to Security → User Account for setup instructions.

Authentication

Two authentication methods are supported for HTTP transactions:

- **Basic:** Transmits the password in plain text. This carries a risk of interception.
- **Digest:** Encrypts the credentials using MD5 for enhanced protection against unauthorized access.

HTTP Port / Secondary HTTP Port

- Default HTTP port: 80
- Secondary HTTP port: 8080

These can be reassigned to a value between 1025 and 65535.

If either port is incorrectly configured, warning messages will be displayed. You may use either the HTTP port or secondary port to access the camera locally. Example (assuming HTTP port is 80 and secondary port is 8080):

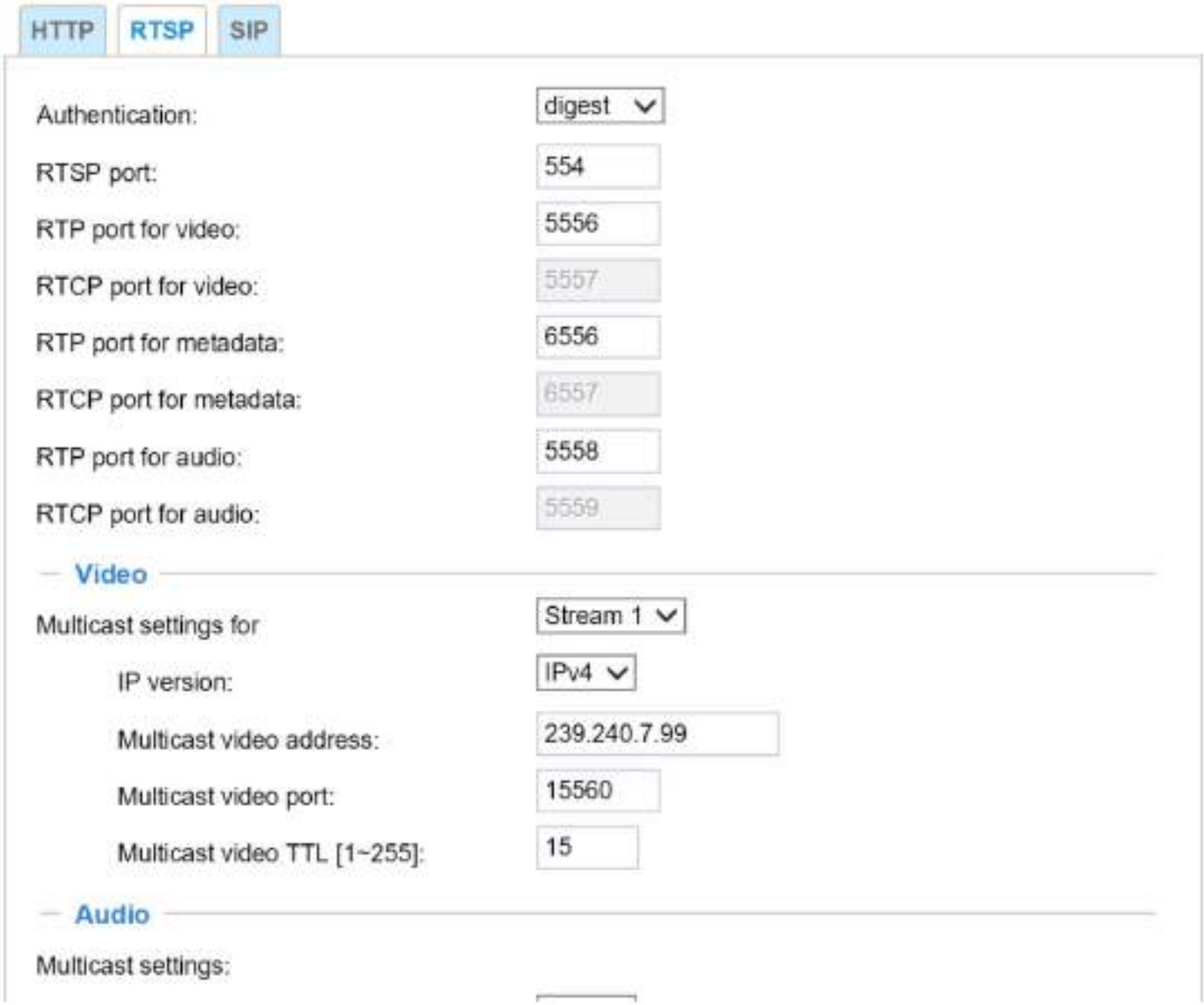
- http://192.168.4.160
- http://192.168.4.160:8080

Access Name for Stream 1 ~ 4

Each video stream has a unique access name. This is used to identify and retrieve each stream individually. You can assign or change these access names under Media → Video → Stream settings.

RTSP Streaming

To enable RTSP streaming with authentication, make sure a password has been configured for stream access. For setup details, refer to Security → User Account.



Authentication

RTSP streaming supports the following modes:

- **Disable:** No authentication required
- **Basic:** Transmits credentials in plain text
- **Digest:** Encrypts credentials using MD5 for enhanced security

Digest mode is recommended for protected network environments.

RTSP and RTP/RTCP Port Settings

- **RTSP Port:** Default is 554
- RTP Port for Video: Default is 5556
- RTP Port for Audio: Default is 5558

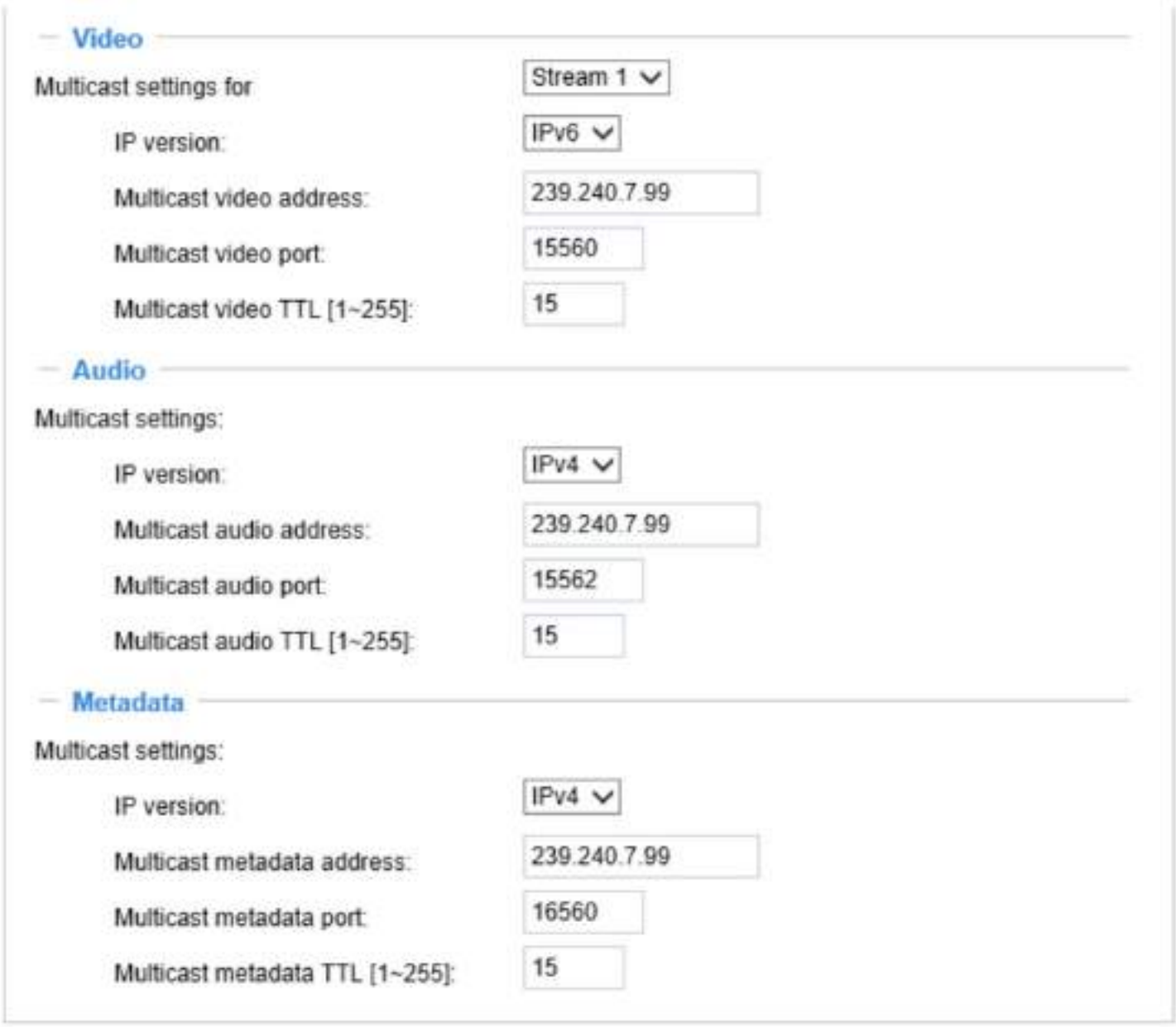
- RTCP Port for Video: Default is 5557
- RTCP Port for Audio: Default is 5559

RTP handles the transport of video and audio streams. RTCP monitors and provides feedback on streaming performance.

RTP port values must be even numbers; each RTCP port must be the next higher odd number. All ports must be in the range of 1025–65535. If invalid values are entered, warning messages will appear.

Multicast Settings

Click a stream number (#1–#3) to access multicast configuration for that stream. Always multicast: When enabled, the stream is continuously transmitted via multicast to the assigned multicast group.



DDNS

This section describes how to configure Dynamic Domain Name Service (DDNS) for the network camera. DDNS allows a camera assigned with a dynamic IP address to be accessed using a consistent hostname and domain, instead of relying on the changing IP.

- Enable DDNS: Check this option to activate DDNS functionality.
- Provider: Select your DDNS provider from the available list in the drop-down menu.

Quality of Service (QoS)

Quality of Service (QoS) refers to a resource management mechanism that helps ensure consistent performance for different services across a network. This is especially important in networks with limited bandwidth, where real-time applications like streaming video require stability and low latency.

QoS helps to:

- Prioritize network traffic and ensure performance levels for specific data flows
- Regulate bandwidth usage by application, improving network reliability and stability

Requirements for QoS and to use QoS features effectively:

- All routers and switches on the network must support QoS
- All video devices on the network must be QoS-enabled

QoS Models

CoS (Class of Service – VLAN 802.1p)

This method applies QoS at Layer 2 (Data Link Layer) of the OSI model. A 3-bit priority field is added to the VLAN MAC header to classify traffic with priority values from 0 (lowest) to 7 (highest). These values are interpreted by the switch, which uses them to queue packets accordingly.

- Input the VLAN ID (range: 0–4095) and select a priority value (range: 0–7) for each application.
- For example, assigning the highest priority to video ensures that those packets are transmitted first.

Note:

- A VLAN switch with 802.1p support is required
- Incorrect CoS settings may cause browser access failures
- CoS provides “best-effort” delivery and does not guarantee exact bandwidth or delivery timing
- CoS is easier to manage but does not scale well and lacks end-to-end assurance due to its L2 design

DSCP (DiffServ Code Point – DSCP-ECN Model)

This method operates at Layer 3 (Network Layer). Differentiated Services (DiffServ) mark packets using a 6-bit field in the IP header called DSCP. This field defines how routers treat each packet (known as Per Hop Behavior, or PHB).

The DSCP tag indicates priority levels and influences queuing, bandwidth allocation, and packet handling at each network hop.

Enter a DSCP value (0–63) for each application based on your desired traffic behavior.

Simple Network Management Protocol

SNMP consists of three main elements:

1. Manager – The network management station (NMS) responsible for monitoring and controlling devices
2. Agent – The software module installed on the device that reports status to the NMS
3. Managed device – A networked device such as a switch, router, printer, or IP camera that is monitored through SNMP

Before enabling SNMP on this page, make sure your NMS is already configured and active.

SNMP Configuration

Enable SNMPv1, SNMPv2c

Select this option to activate SNMPv1 or SNMPv2c. Enter the Read/Write community and Read Only community names as defined in your NMS.

Enable SNMPv3

SNMPv3 provides enhanced security through authentication and encryption.

- **Security name:** Choose the security profile (Read/Write or Read Only) and enter the associated name
- **Authentication type:** Select either MD5 or SHA
- **Authentication password:** Enter the password for authentication (minimum 8 characters)
- **Encryption password:** Enter the encryption password (minimum 8 characters)

FTP and SFTP

The newer firmware disables the FTP port by default for security reasons. To use FTP, go to Configuration → Network → FTP and manually enable the port. If the FTP port is closed, the camera will not be able to upload images or logs to an FTP server.

Ensure your FTP server is accessible and properly configured. Use correct login credentials and directory paths to ensure successful uploads.

SFTP (Secure File Transfer Protocol)

SFTP provides a secure method for transferring files using SSH encryption.

To use this feature, enter the following information:

- **Host:** The IP address or domain name of the SFTP server
- **Port:** The port used for SFTP (default is 22)
- **Username and Password:** Your SFTP login credentials
- **File path:** The target directory on the server
- **Public key:** Optional field for key-based authentication

Bonjour

Bonjour allows the camera to be discovered on Mac-based networks. This service simplifies the process of locating the camera by name rather than IP address.

The camera will appear in the Bonjour tab of the Safari browser using its designated device name.

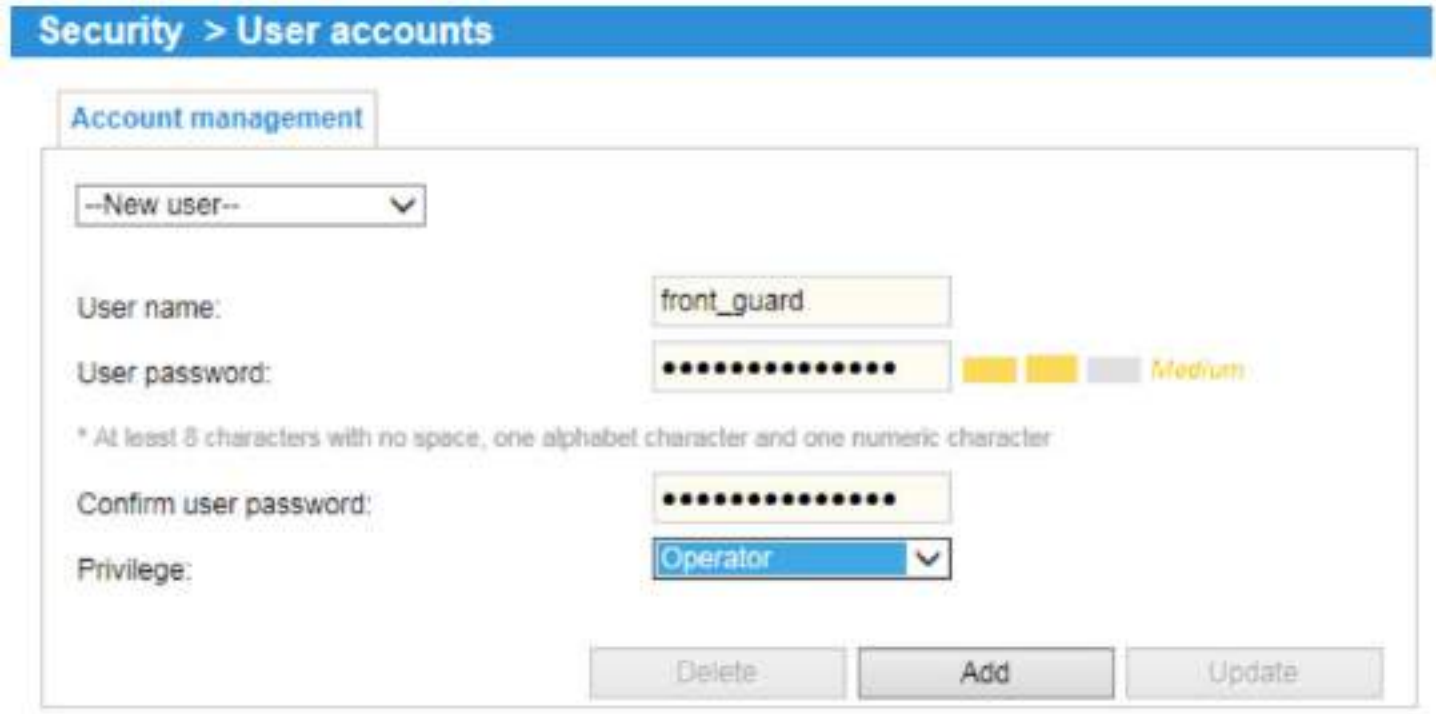
Security Settings

User Accounts

This section explains how to configure user account access for the camera.

The administrator account name is **admin**, which is permanent and cannot be deleted. Before adding new users, a password must first be set for the **admin** account. The administrator can create up to twenty (20) user accounts.

Account Management



To create a new user:

1. Click the **New User** option from the drop-down menu.
2. Enter the new user's name and password. Type the password in both fields for confirmation.

ⓘ You may include certain special characters in the password, such as **!**, **$**, **%**, **-**, **.**, **@**, **^**, _, and **~**. The strength of your password will be indicated as you type.

3. Select a privilege level for the new account from the following:
    - **Administrator**: Full access to all camera settings and features, including the **Configuration** page.
    - **Operator**: Access to live video and control of snapshot, screen, audio, and PTZ functions. Cannot access the **Configuration** page. However, Operators can send URL commands to retrieve or change parameters.
    - **Viewer**: View-only access to the live video stream via the main page. Cannot control PTZ or access configuration.
4. Click the **Add** button to save the new account.

Editing or Deleting a User

1. Select an existing user account from the list.
2. Make necessary changes, then click **Update** to apply changes or **Delete** to remove the account.

Hypertext Transfer Protocol Over SSL (HTTPS)

This section explains how to enable encrypted communication using HTTPS. Enabling HTTPS secures the camera's data transmission and prevents unauthorized access to the video stream and settings. Check **Enable HTTPS Secure Connection**, then choose one of the connection modes:

- **HTTP & HTTPS**: Allows both secure and non-secure access
- **HTTPS Only**: Forces secure access only

Access List

This section allows you to control which IP addresses are permitted to access the camera.

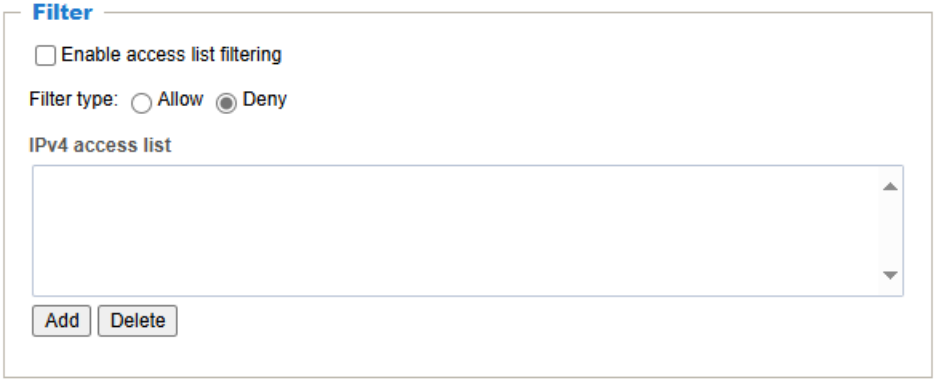
Enable Access List Filtering

Check this option and click **Save** to activate access list filtering.

Filter Type

- **Allow**: Only the IP addresses listed will be granted access. All others will be blocked.
- **Deny**: IP addresses listed will be blocked. All others will be allowed access.

ⓘ The **IPv6** access list field is visible only when **IPv6** is enabled under **Network –> General Settings**.



Administrator IP Address

To ensure continuous administrator access, check **Always allow the IP address to access this device** and enter the administrator's IP address in the field provided.

IEEE 802.1X

Enable this setting if your network uses IEEE 802.1X, a port-based access control protocol designed to secure local area networks (LAN). To successfully use this feature, your switch/access point and RADIUS server must support IEEE 802.1X authentication.

IEEE 802.1X uses the Extensible Authentication Protocol (EAP) to validate credentials between network clients and the server. If authentication is successful, a secure point-to-point connection is established. If not, access through the port is denied.

ⓘ The IEEE 802.1X architecture includes:

1. **Supplicant**: The client device (e.g., the camera) requesting network access.
2. **Authenticator**: The intermediary device (e.g., a network switch or access point) that controls access to the network based on authentication results.
3. **Authentication Server**: Typically a RADIUS server, which validates the credentials and determines whether access is granted.

To enable IEEE 802.1X:

1. **Obtain a Certificate**: Acquire a digital certificate for the camera from your Certificate Authority (CA). This certificate must be verifiable by the RADIUS server.

2. **Configure Settings Outside the Protected Network**: Temporarily connect the camera to a computer that is not inside the IEEE 802.1X-secured network. Open the configuration interface and select either **EAP-PEAP** or **EAP-TLS**. Input your **user ID** and **password** (issued by the CA), and upload the required certificate(s).

3. **Deploy the Camera**: Once settings are configured, connect the camera to the secured network (via a switch or access point with IEEE 802.1X enabled). Authentication will begin automatically.

ⓘ Authentication Flow:

1. The CA provides signed certificates to both the camera and the RADIUS server.
2. The camera (supplicant) initiates a connection via the switch (authenticator), presenting its credentials.
3. The switch forwards this information to the RADIUS server.
4. Upon successful verification, the switch updates the camera's status to "authorized" and permits network access.

Miscellaneous

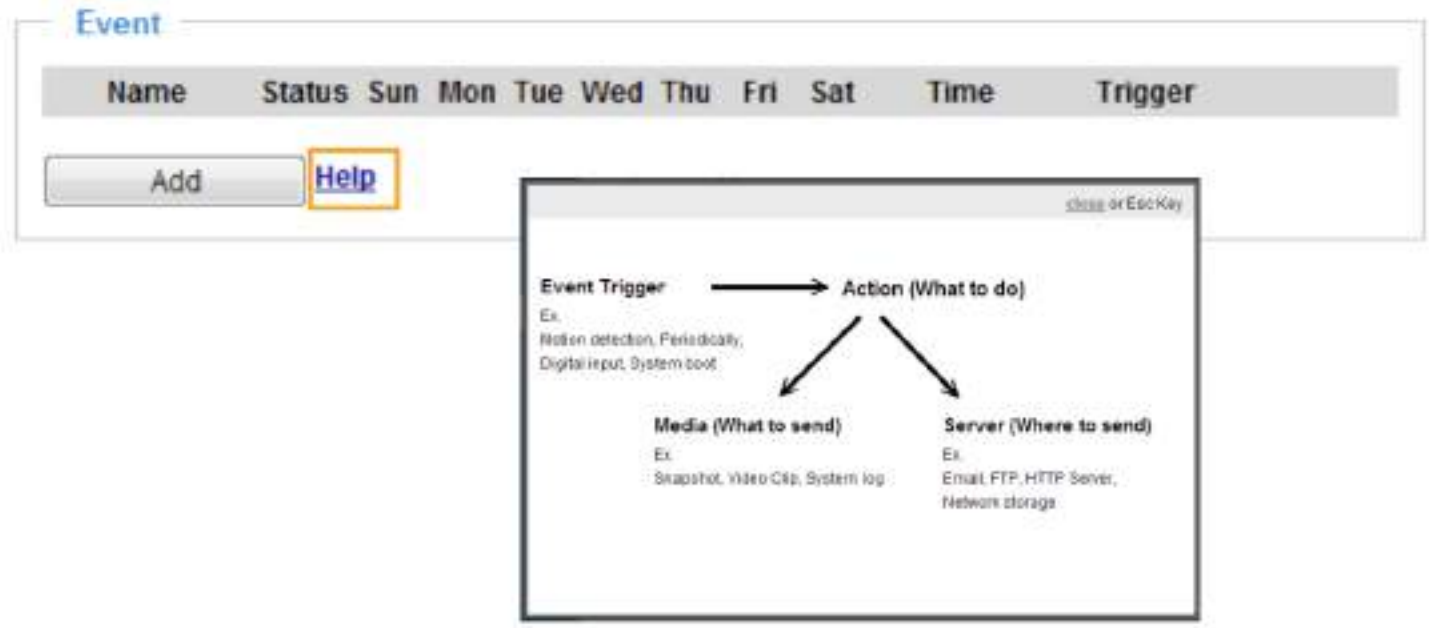
The embedded security utility includes protection against Cross-Site Request Forgery (CSRF) attacks. CSRF—also known as a one-click attack or session riding—is a type of malicious exploit where unauthorized commands are transmitted from a trusted user session.

This type of attack takes advantage of the user's browser, using mechanisms such as specially crafted image tags, hidden forms, or JavaScript XMLHttpRequests, to transmit unwanted requests. These actions can occur without the user's knowledge or interaction.

ⓘ Enabling CSRF protection is recommended to mitigate risks associated with forged requests and unauthorized camera control.

Event Management

This section explains how to configure the camera to respond to specific conditions—called **events**—by capturing and sending snapshots or video clips. The captured media can be delivered to external destinations such as **FTP**, **SFTP**, **HTTP**, or **Email** servers, or stored locally on an **SD card** or **network storage**. The instructions below outline how to create and manage event rules.



To begin configuration, you must first define the **server** and **media settings**. These determine what action the camera takes and where the media is sent when a trigger occurs. Click the **Add** button in the **Event** column to set up an event.

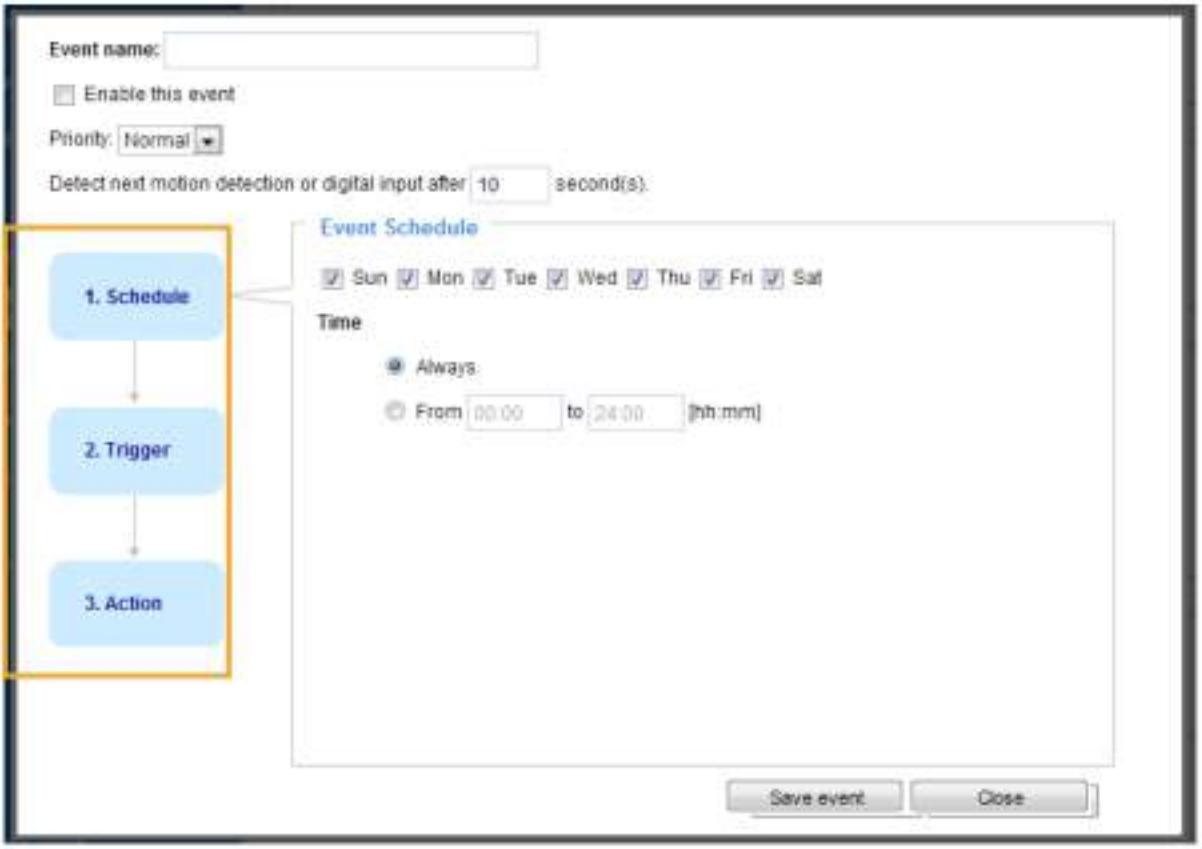
Each event rule includes the following components:

- **Schedule**

- **Trigger**
- **Action**

You may configure up to **three (3)** event rules.

Event Settings Interface



- **Event Name**: Enter a descriptive name for the event rule.
- **Enable This Event**: Check this option to activate the event rule.
- **Priority**: Select from **High**, **Normal**, or **Low**. Higher-priority events are processed first.
- **Detection Delay**: Enter the number of seconds to delay before the next trigger can be detected. This prevents rapid re-triggering.

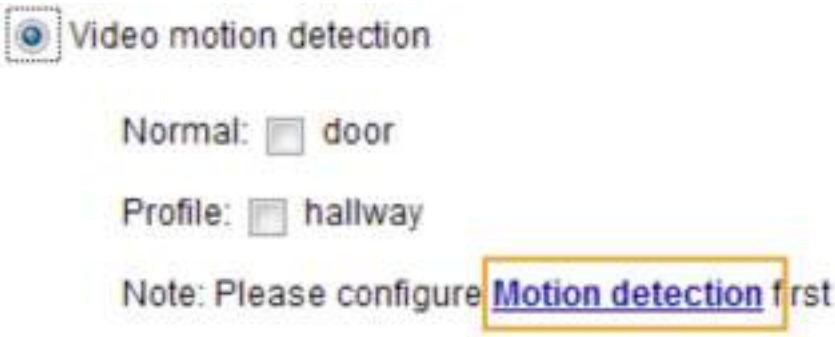
Schedule

Choose the days of the week and define time ranges using 24-hour format. The rule will only be active during the specified schedule.

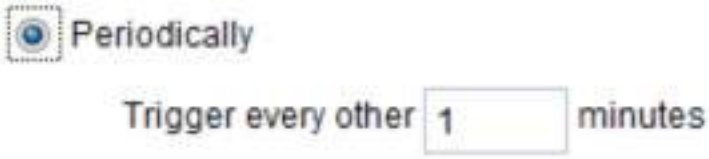
Trigger

Select the condition that activates the event rule. Available options:

- **Video Motion Detection**: Detects movement using a preconfigured detection window.

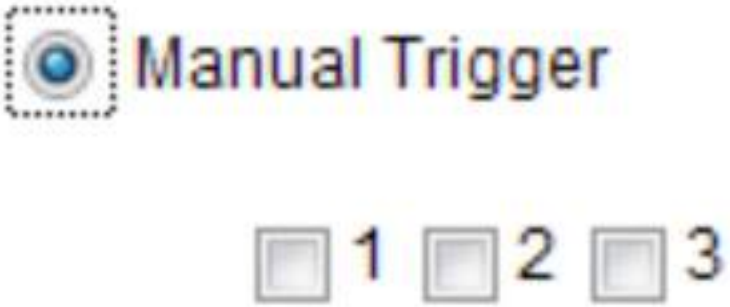


- **Periodically**: Triggers at fixed intervals, between **1 and 999 minutes**.



- **System Boot**: Triggers when the camera restarts.
- **Recording Notify**: Triggers when storage becomes full or begins overwriting.
- **Camera Tampering Detection**: Activates when tampering (e.g., lens covering) is detected. Must be preconfigured.

- **Audio Detection**: Triggers on unexpected sounds.
- **Manual Trigger**: Allows users to activate an event from the camera's homepage. Up to **three (3)** manual triggers may be created.

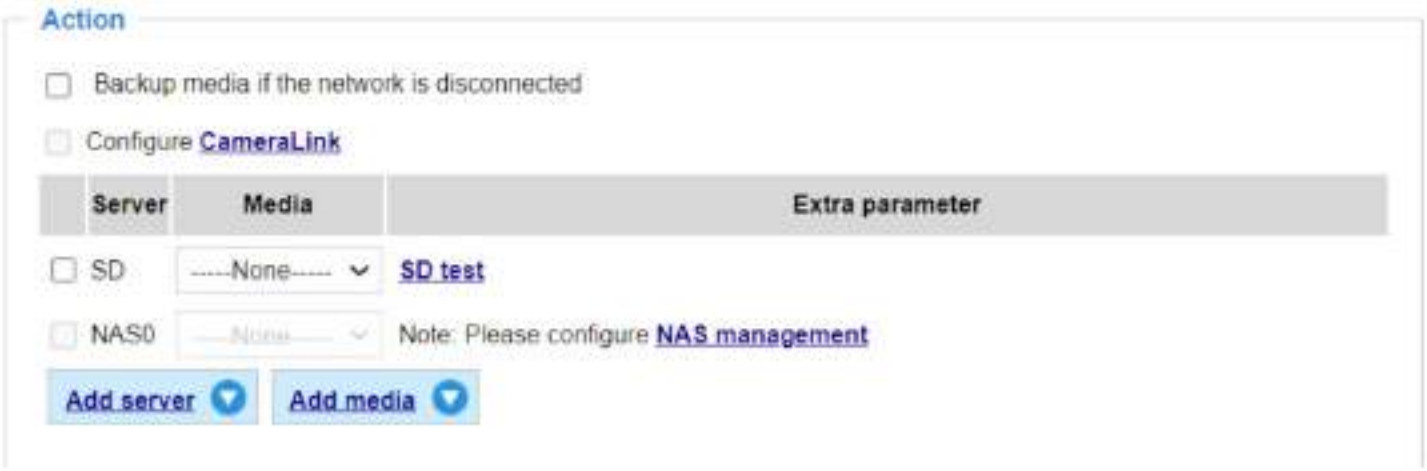


- **Shock Detection**: Uses built-in sensors to detect physical vibration or impact.

Action

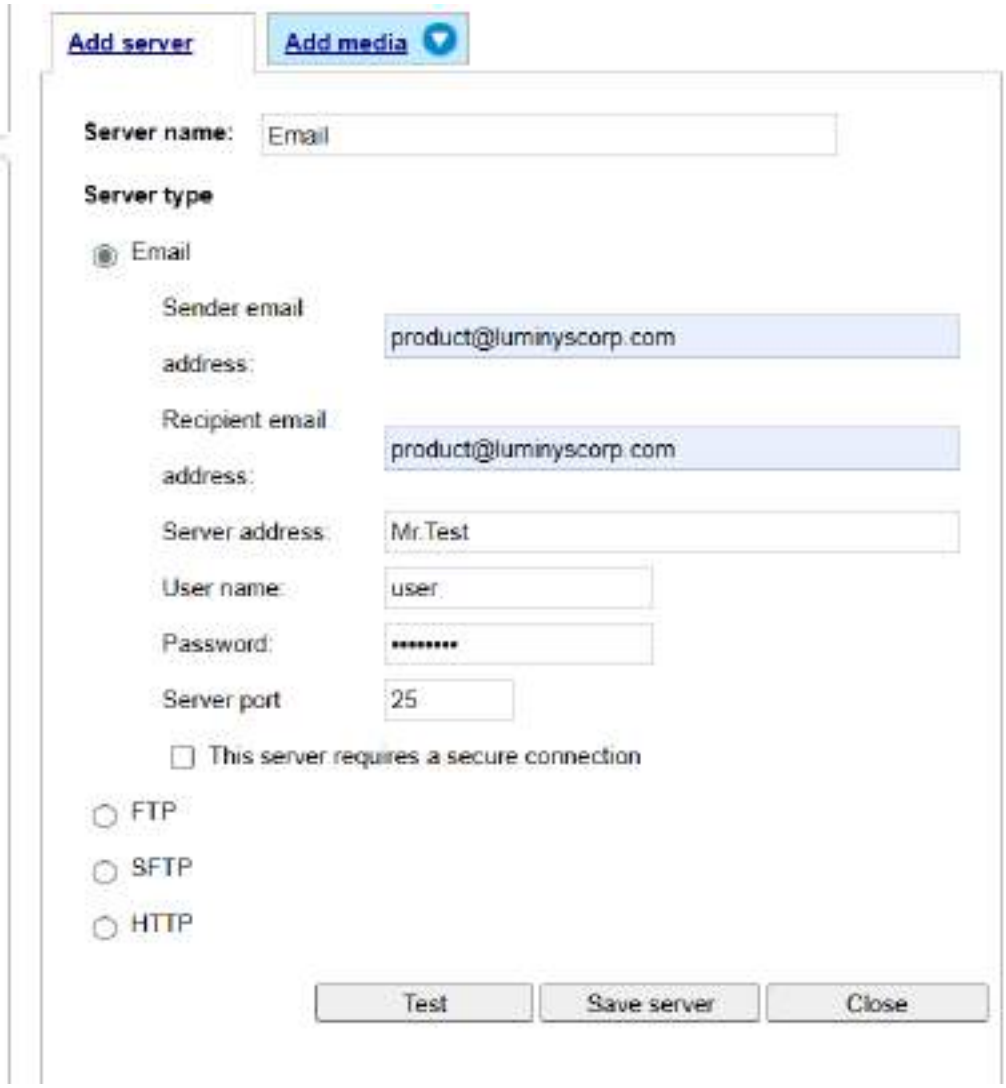
Select the action the camera performs once triggered:

- **Trigger Digital Output for (X) Seconds**: Activates the digital output port.
- **Backup Media If the Network Is Disconnected**: Saves media locally if the network is unavailable.
- **Configure CameraLink**: Sends a signal to another camera to trigger an action (e.g., preset movement).



Add Server

Click the **Add Server** button to configure where the media will be sent. Up to **five (5)** server settings can be defined.



Email

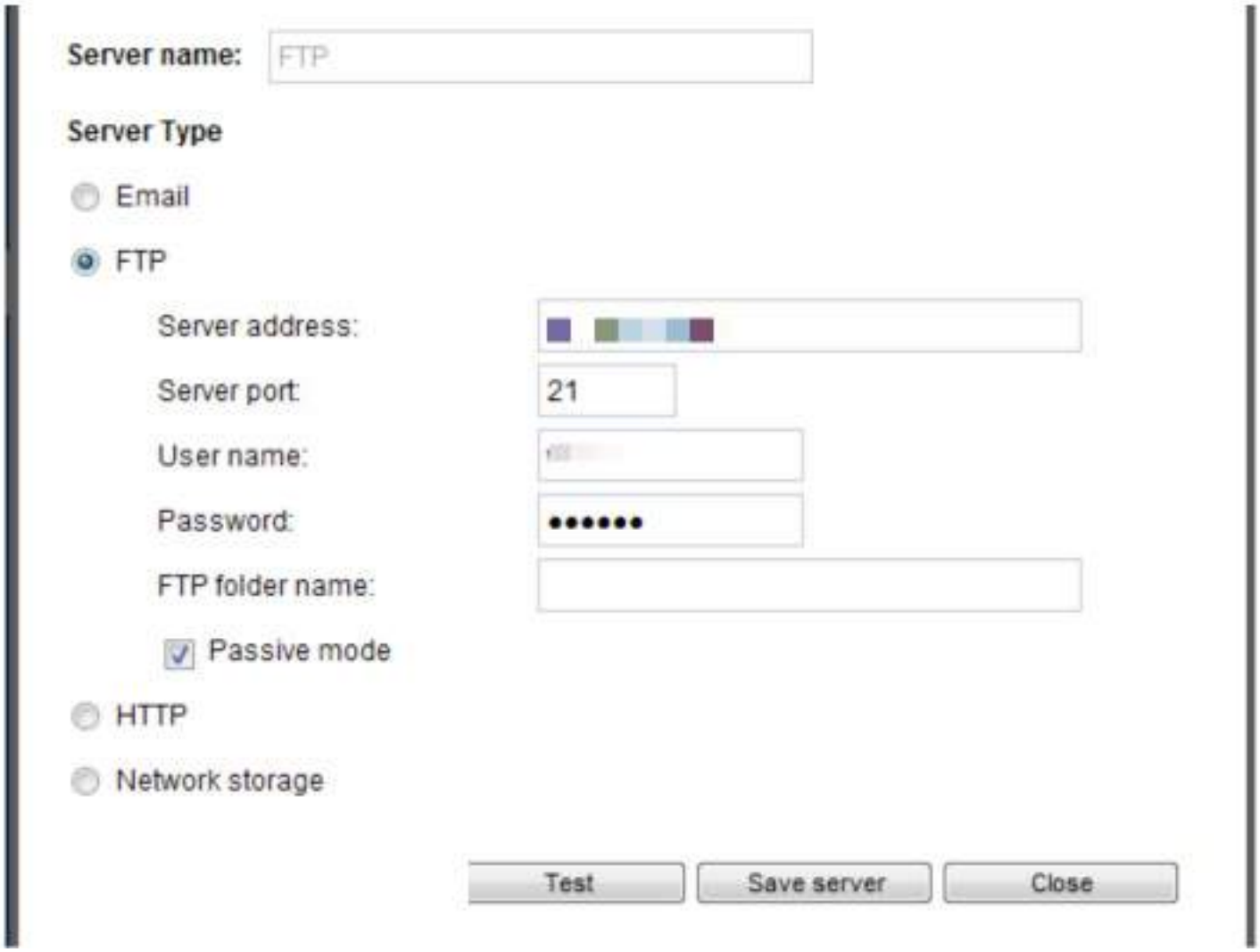
- **Server Name**
- **Sender Email / Recipient Email**
- **Server Address**
- **Port**: Default is **25**, range is **1025–65535**
- **Username / Password**
- **This Server Requires a Secure Connection (SSL)**: Enable if required by the SMTP server

ⓘ Click the **Test** button to verify that email settings are correct. If successful, a confirmation email will be sent and a pop-up window will confirm the result.

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

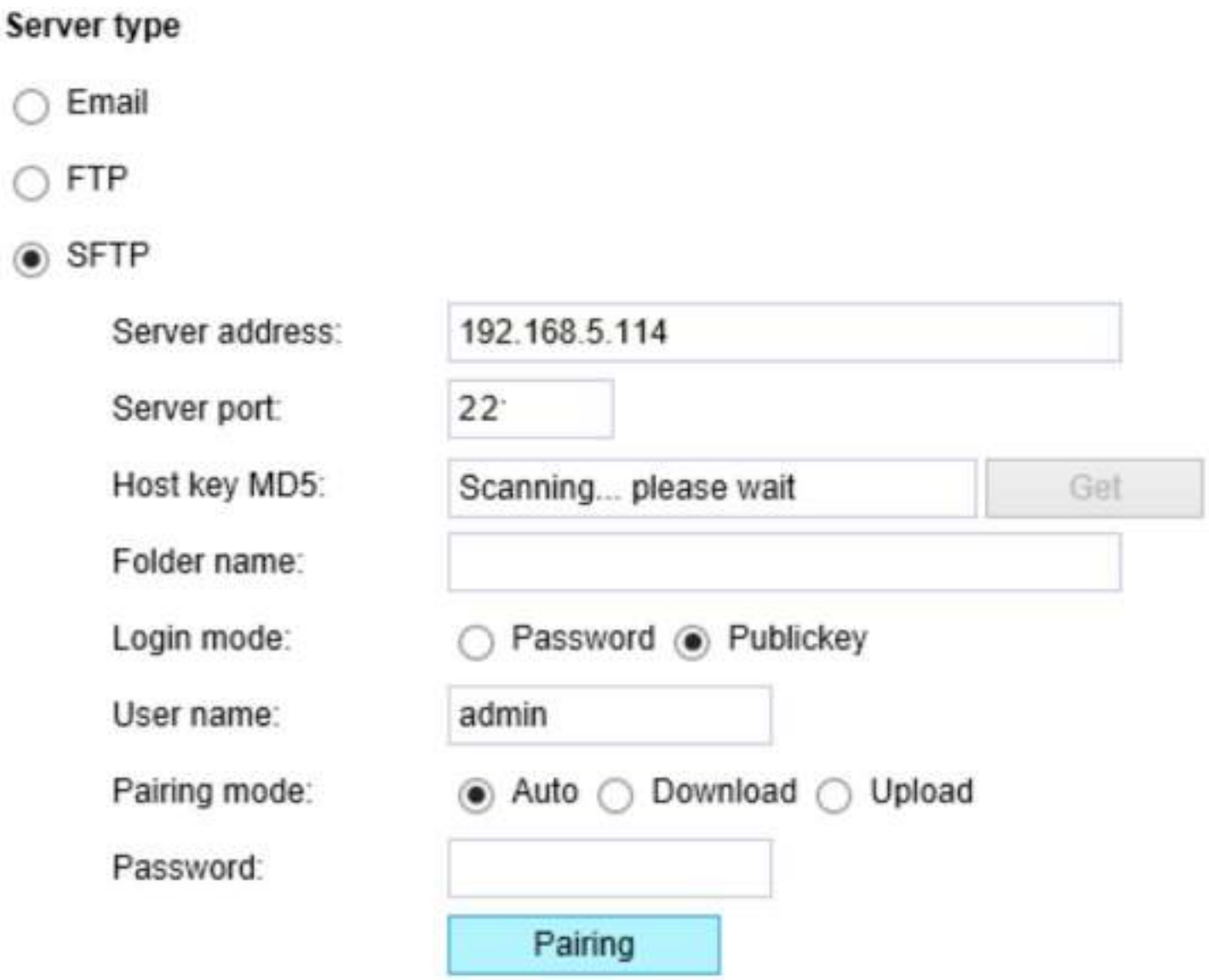
ⓘ After the first server is added, it will appear in the Server list. To add more servers, click **Add Server** again.

FTP



- **Server Name / Server Address**
- **Port**: Default is **21**, range **1025–65535**
- **Username / Password**
- **Passive Mode**: Check this if the FTP server uses passive mode for file transfers

SFTP



- **Server Name / Server Address**
- **Port**: Default is **22**
- **Username / Password**
- **Host Key MD5:** This optional feature lets you use key-based authentication. Click the **Get** button to retrieve the server's MD5 fingerprint. The fingerprint is stored by the camera and used to verify the identity of the SFTP server.

  ⓘ Maximum fingerprint length is **47 characters**.

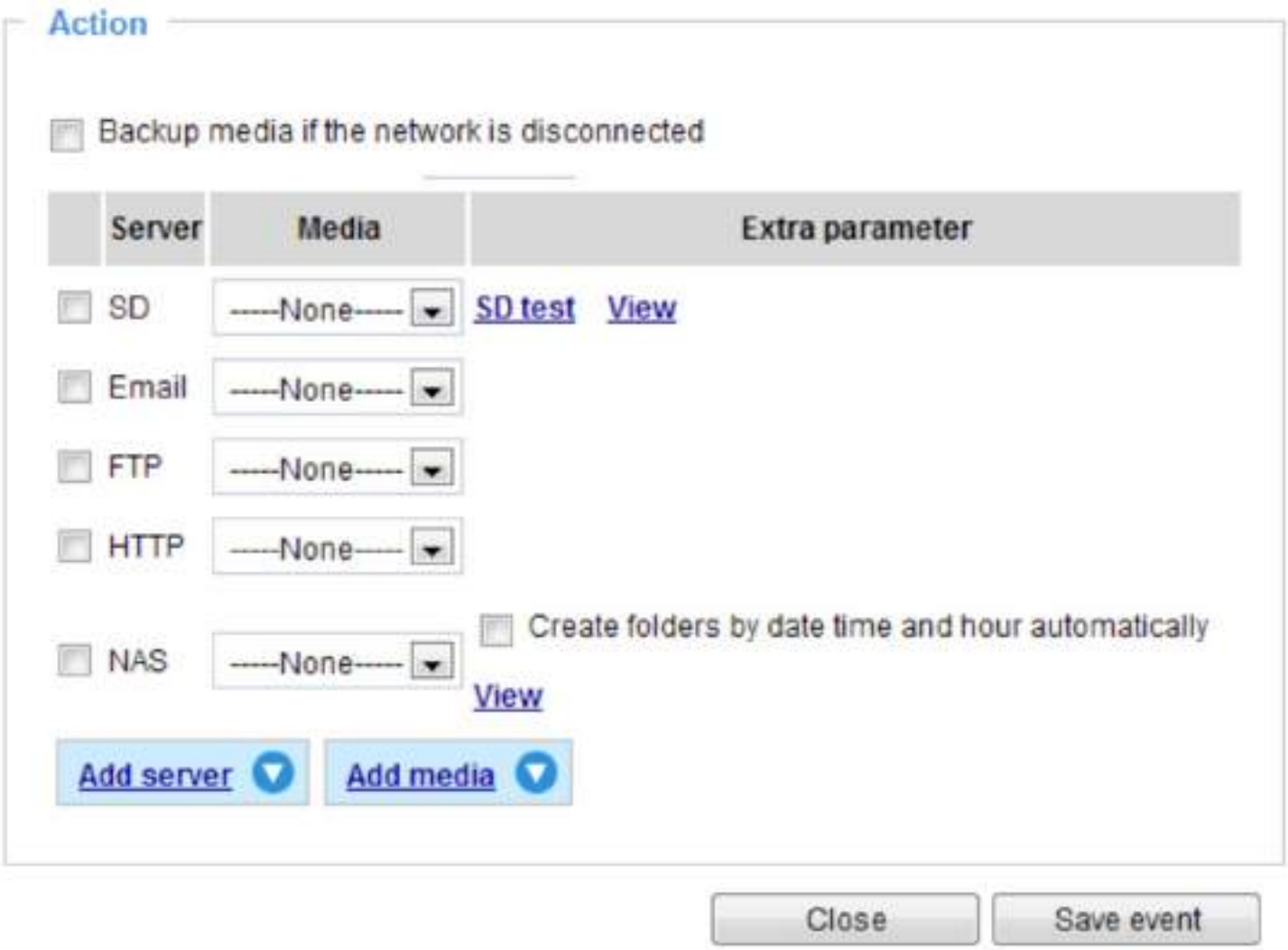
HTTP

- **Server Name**
- **HTTP URL**
- **Port**
- **Username / Password**

Network Storage

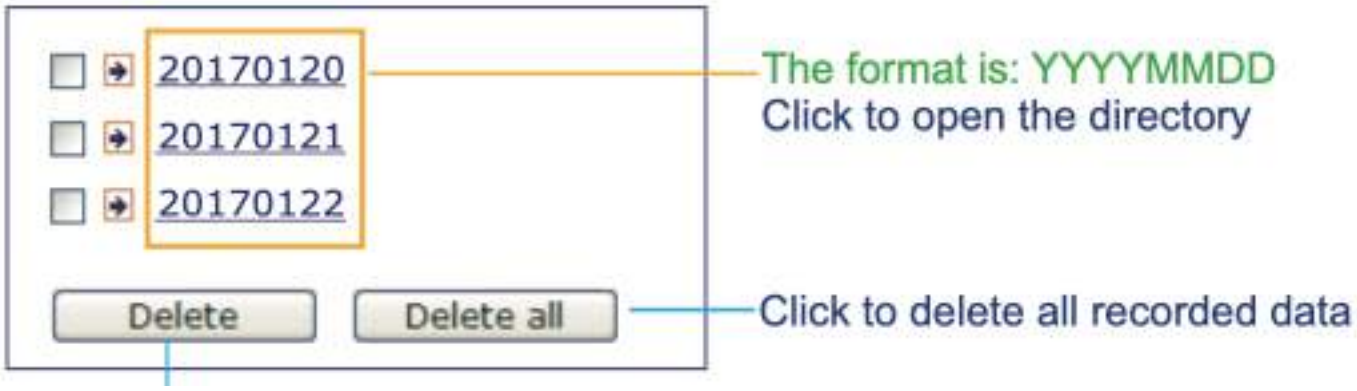
Choose **NAS** to send media to a networked storage device

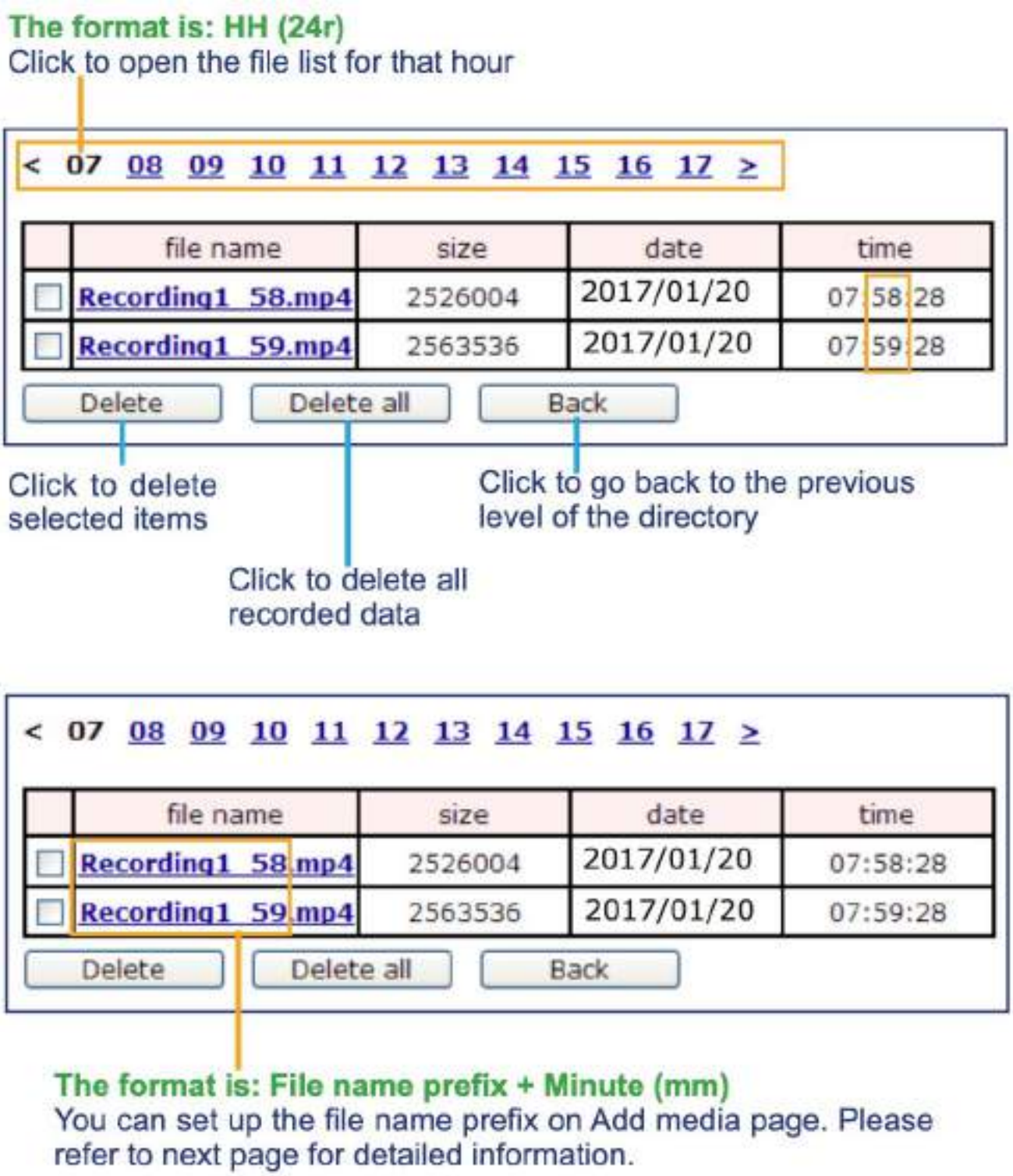
ⓘ Only one (1) NAS server can be configured



- SD Test: Click this to verify SD card status. A pop-up message will indicate success or failure. Format the SD card before use if needed.
- View: Opens a file list window.
    - For SD card: Opens the Local Storage page to manage SD-stored files.
    - For Network Storage: Opens a directory window to view NAS-stored data.

15. Create Folders by Date/Time Automatically: Enable this to organize files by timestamp. Each folder will contain:
16. Files labeled with date and hour (YYYYMMDD/HH)
17. Filename prefix + minute (Prefix_MM)

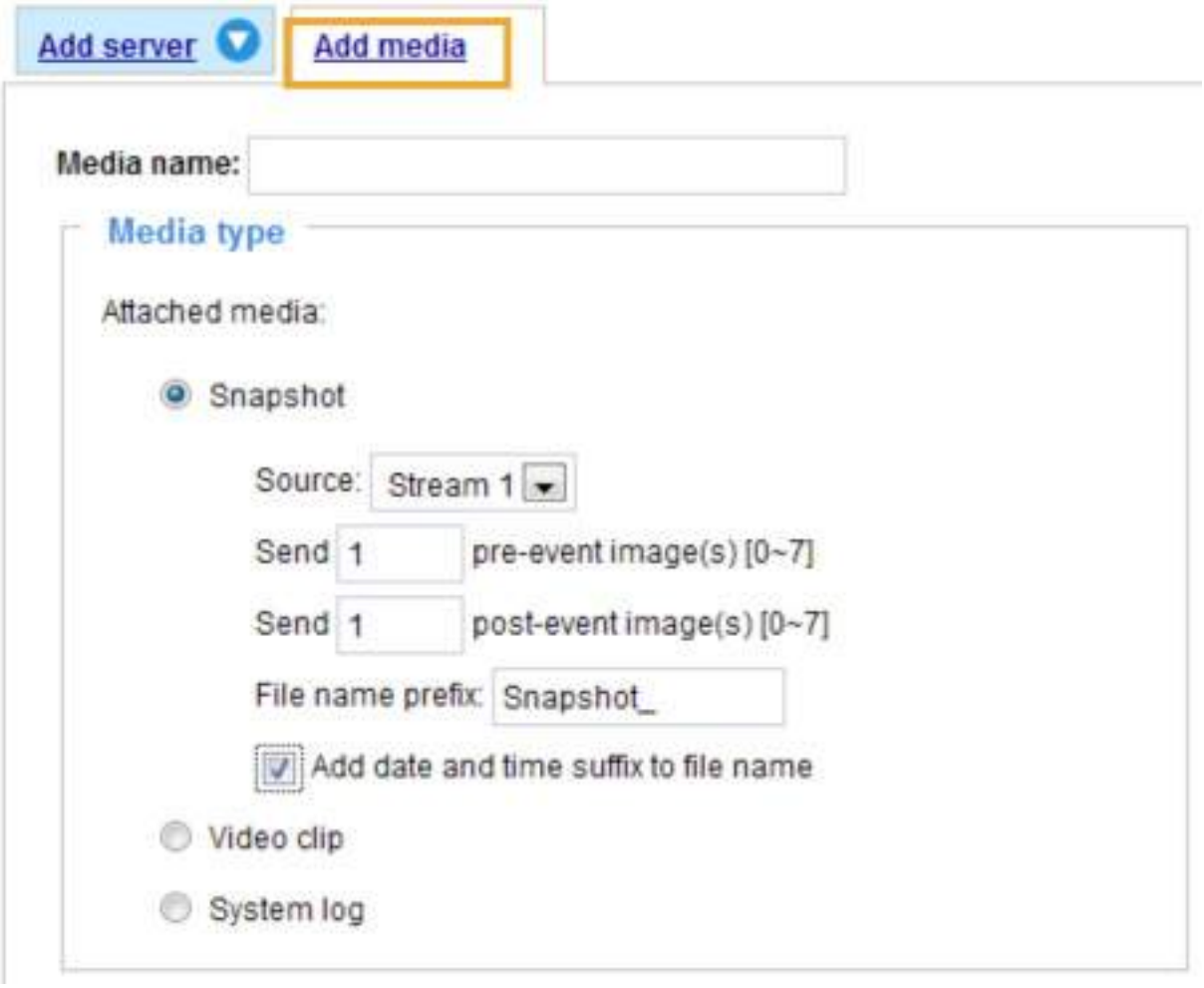




Click **Save Server** after completing the configuration.

Add Media

Click **Add Media** to define what content is generated and sent when the event is triggered. Up to **five (5)** media settings can be created.

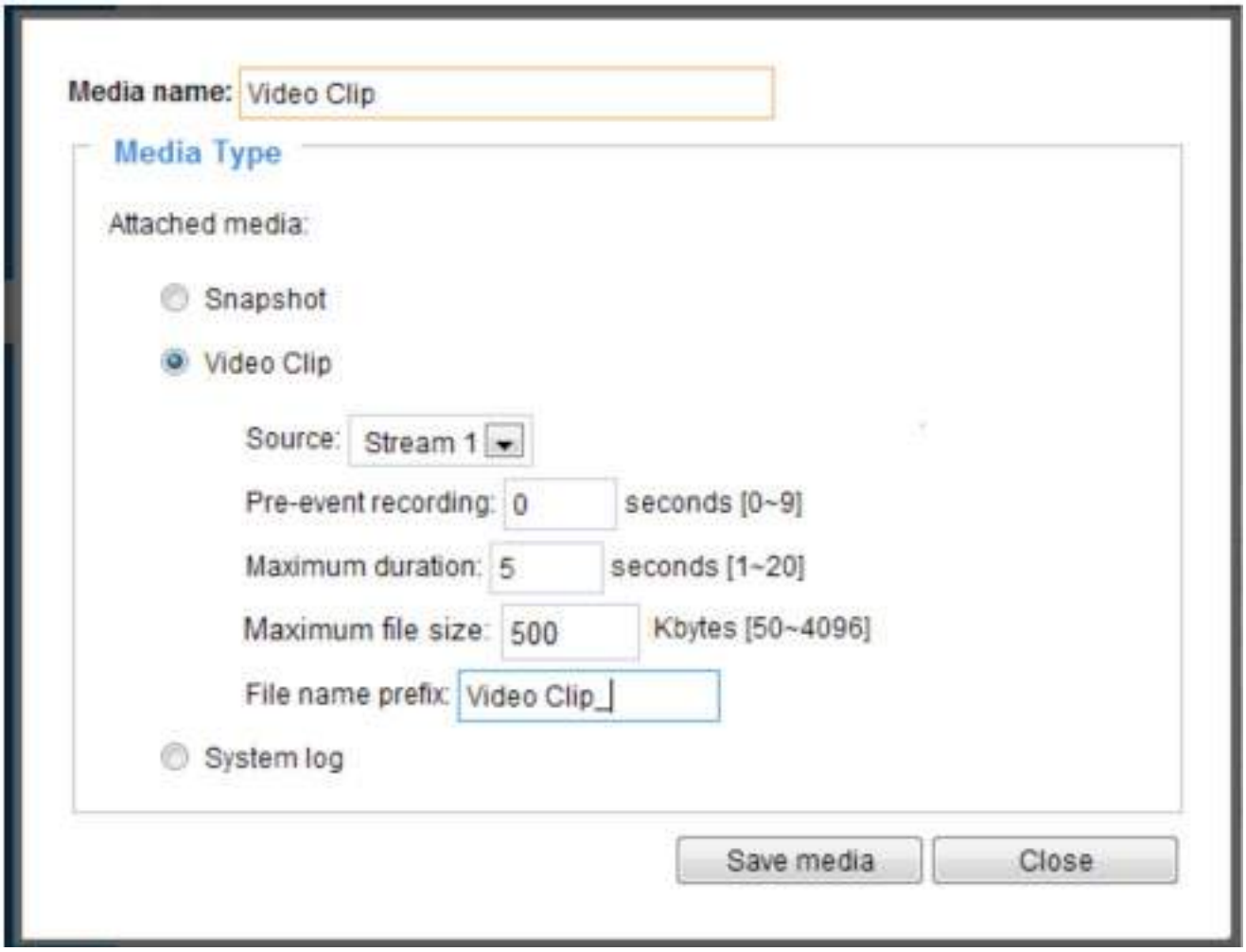


Snapshot

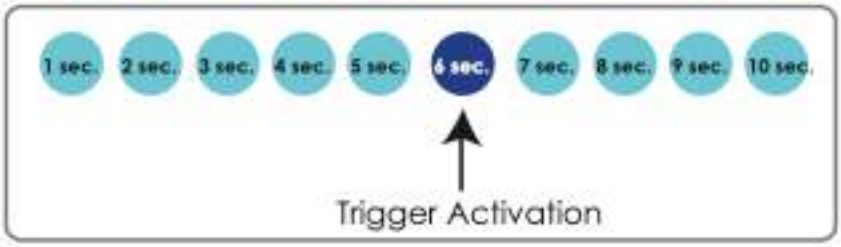
- **Media Name**
- **Source** (select the video stream)
- **Send Pre-Event Images**: Up to **seven (7)** images
- **Send Post-Event Images**: Up to **seven (7)** images

ⓘ If both pre- and post-event images are set to seven (7), the system captures a total of **15** images per trigger.

Video Clip



- **Media Name**
- **Source**
- **Pre-Event Buffer**: Up to **nine (9)** seconds
- **Maximum Duration**: Up to **20 seconds**

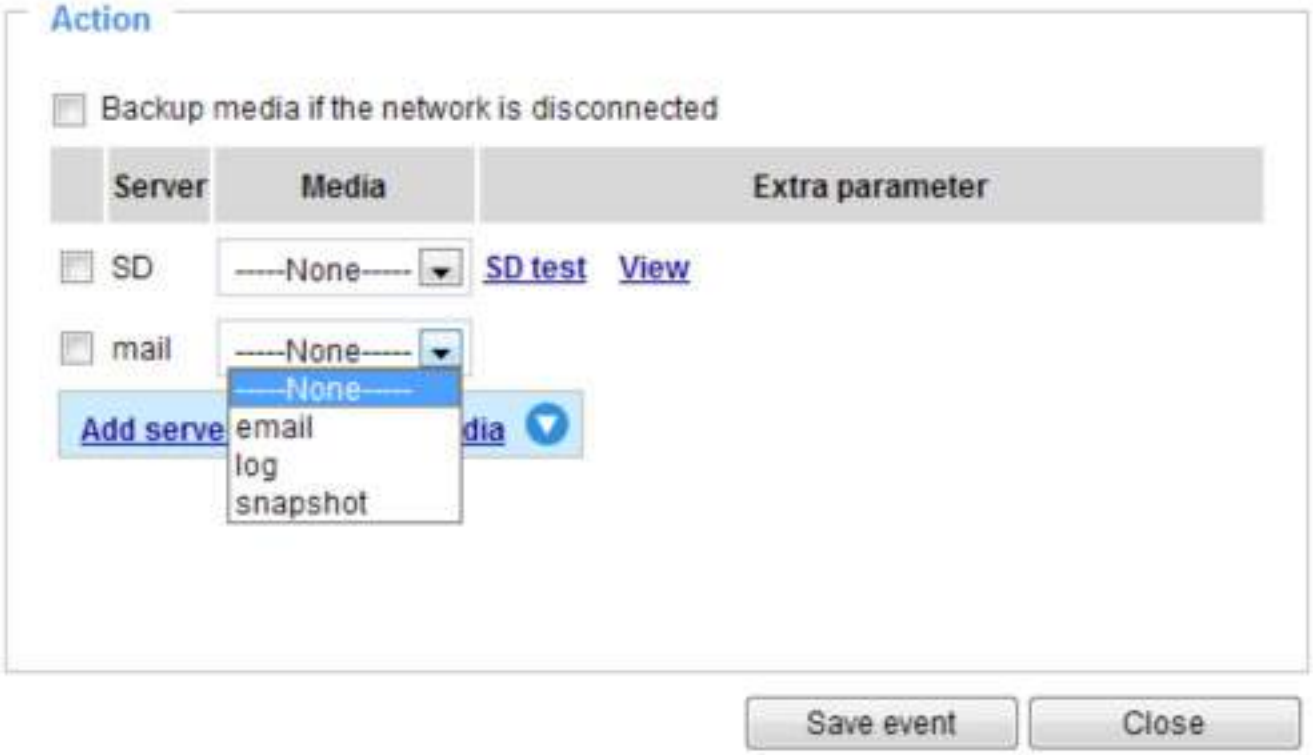


- **Maximum File Size**
- **File Name Prefix**

- **Add Date and Time Suffix**: Appends a timestamp in the format YYYYMMDD_HHMMSS

System Log

Select this option to generate and send a system log when triggered. Click **Save Media** when done.

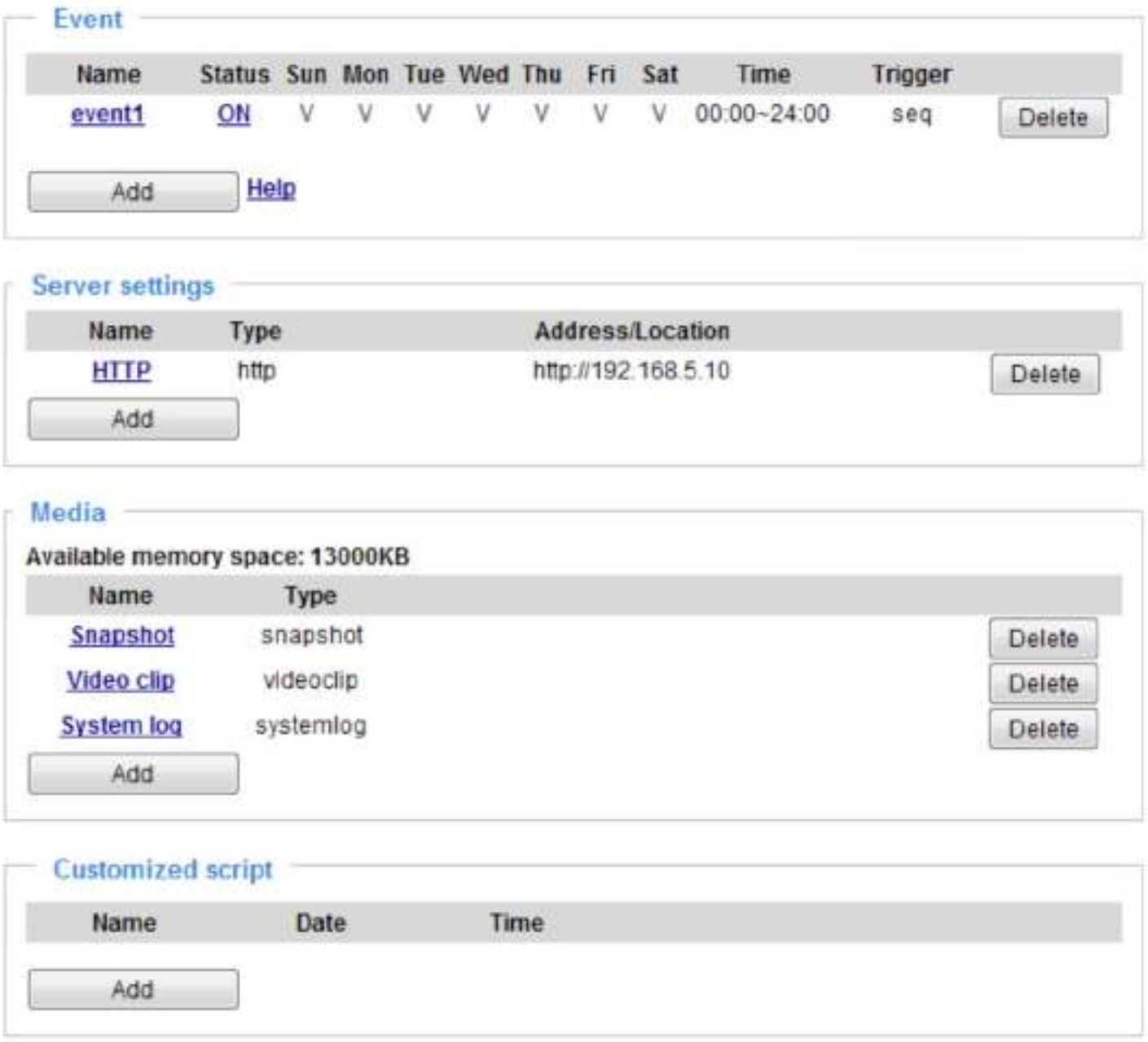


ⓘ You may only delete media or server settings if they are not assigned to an active event rule.

SD Card and Network Storage Controls

- **SD Test**: Click to test SD card functionality. A result window will indicate success or failure.
- **View**: Opens a file browser window.
    - If **SD** is selected: A local storage window opens for browsing saved footage.
    - If **NAS** is selected: A directory listing appears for browsing network footage.
- **Create Folders by Date/Time**: Automatically organizes storage into structured folders based on recording date and time.

Final Setup



Once all components of the event are configured:

1. Set **Status** to **ON**
2. Click **Save Event**
3. Click **Close**

ⓘ To delete an event, select it and click **Delete**.

ⓘ To disable an event without removing it, switch its status to **OFF**.

Application Features

Motion Detection

The Motion Detection feature allows you to monitor specific areas within the camera's field of view and trigger actions when movement is detected. You can configure up to **three (3)** separate motion detection windows. Each window can be resized and repositioned independently to match the surveillance area.

Window Settings

For each motion detection window, configure the following:

- **Sensitivity**: Determines how easily movement is detected. Higher values detect even small motions.
- **Percentage**: Defines the required level of pixel change (as a percentage of the window area) before triggering a motion event.

ⓘ When valid motion is detected: The detection window border turns **red**.

ⓘ If motion is detected but below the defined threshold: The window briefly flashes **yellow**.

To remove a motion detection window, click the **Delete** icon next to the window label. Click **Save** to apply your motion detection settings

Tampering Detection

Tampering Detection is designed to identify and respond to attempts to interfere with the camera's view—such as blocking, redirection, or deliberate image distortion.

Configurable Conditions

You may enable one (1) or more of the following conditions: Tampering Detection, Image Too Dark, Image Too Bright, or Image Too Blurry.

Each condition has a **Trigger Duration** setting, ranging from **10 seconds to 10 minutes**, which determines how long the anomaly must persist before an alert is triggered.

ⓘ Tampering alarms are based on the difference between the live video feed and a pre-captured background reference.

Trigger Threshold

The **Trigger Threshold** controls the detection sensitivity:

- A **lower** threshold increases sensitivity (easier to trigger).
- A **higher** threshold reduces sensitivity (avoids false alarms from minor changes).

Tampering Condition Descriptions

- **Too Bright**: Triggered by sudden exposure to intense lighting (e.g., flashlight). Detected by analyzing average scene brightness.
- **Too Dark**: Triggered when the lens is covered, darkened, or painted.
- **Too Blurry**: May result from intentional movement, defocus, or electromagnetic interference.

Integration With Event Rules

Tampering Detection can be used as an event **Trigger** in the camera's event management system. For example, a tampering event can automatically prompt the system to store snapshots or video clips.

See **Event Settings –> Trigger** for integration details.

Audio Detection

The Audio Detection feature is used to detect sudden changes in sound within the camera's environment. This can serve as a trigger condition for events, particularly in environments where video motion detection may not be effective.

Typical Use Cases

- Detection of activity outside the camera's field of view (e.g., gunshots, glass breaking).
- Monitoring a noisy facility that suddenly becomes quiet due to mechanical failure.
- Triggering a PTZ preset when a specific sound is detected.
- Monitoring dark environments where visual detection may be limited.

The system monitors the real-time sound input and compares it to a preset threshold. If the volume crosses that threshold, an alarm is triggered. The system visually displays input levels on a fluctuating yellow waveform chart.

How to Configure Audio Detection

1. Open the Audio Detection configuration window.
2. Observe the yellow waveform diagram that represents real-time input levels.
3. Click and drag the **Alarm Level** tab to your preferred trigger threshold.
4. Select the **Enable Audio Detection** checkbox.
5. Click **Save** to apply the configuration.

Important Notes

- The volume scale (0–100) shown beside the waveform does **not** represent dB values. Instead, it maps internally to the camera's sensitivity range. Use real-world test inputs to calibrate the Alarm Level setting.

- ⓘ Ensure that **audio is not muted** under **Configuration –> Media –> Audio**.

Some models may have audio muted by default due to the lack of a built-in microphone. An external microphone may be required.

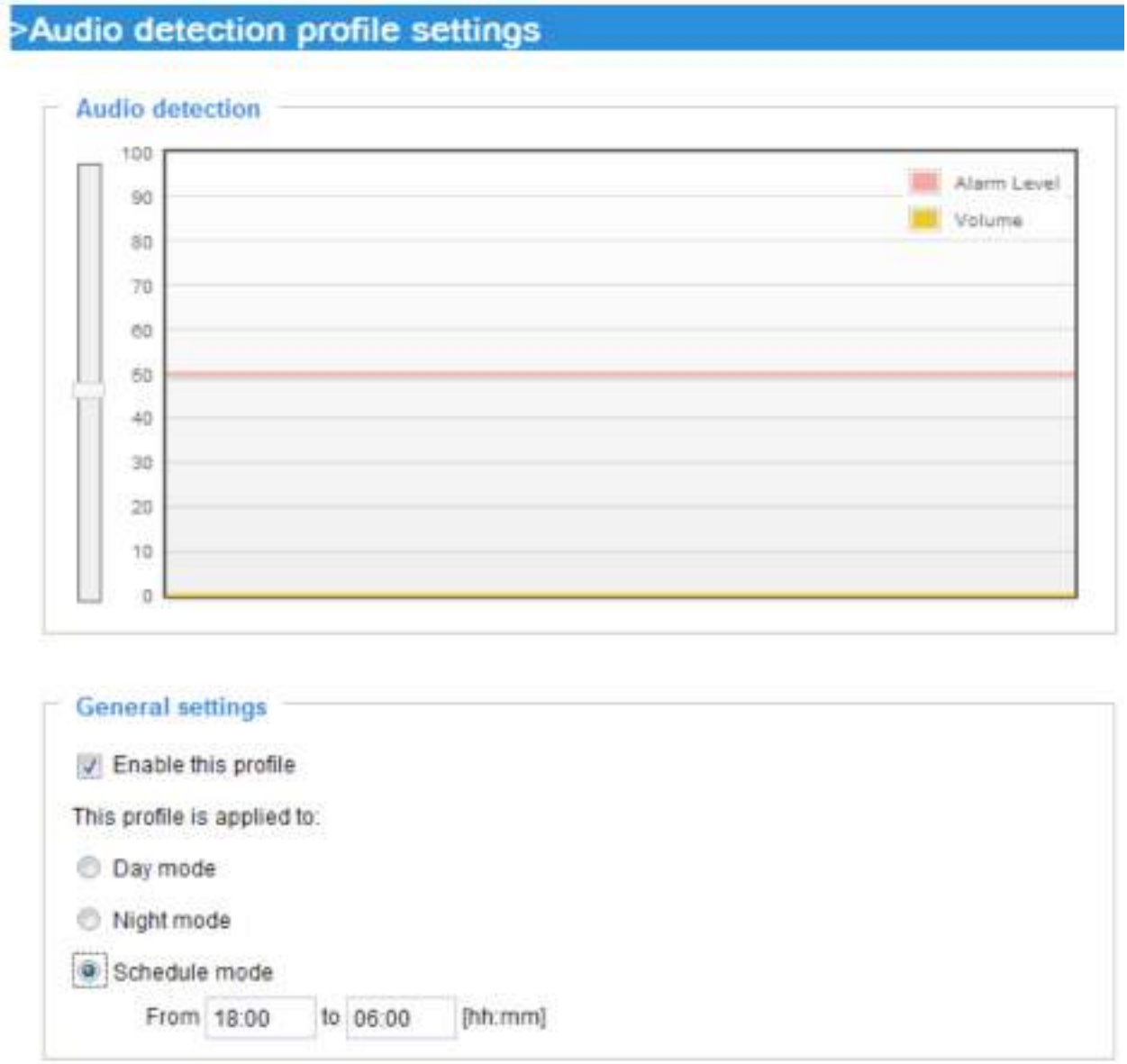
Best Practices

- If the alarm threshold is within **20%** of the detected sound level, false alarms may occur. Set the threshold higher or lower as appropriate to minimize errant triggers.
- To enable this feature, ensure that **Video Stream #1 is not set to Motion JPEG (MJPEG)**. Audio streams are only transmitted alongside **H.264/H.265** encoding.

Profile-Based Audio Detection

The system supports creating audio detection profiles for different time periods or environmental conditions. To configure a profile:

1. Select **Enable This Profile**.
2. Open the Audio Detection window to review the yellow waveform.
3. Drag the **Alarm Level** tab to the preferred value.
4. Select a profile mode: **Day**, **Night**, or **Schedule**.
5. If **Schedule** is selected, define the time range during which the profile is active.
6. Click **Save**, then **Close** to complete setup.

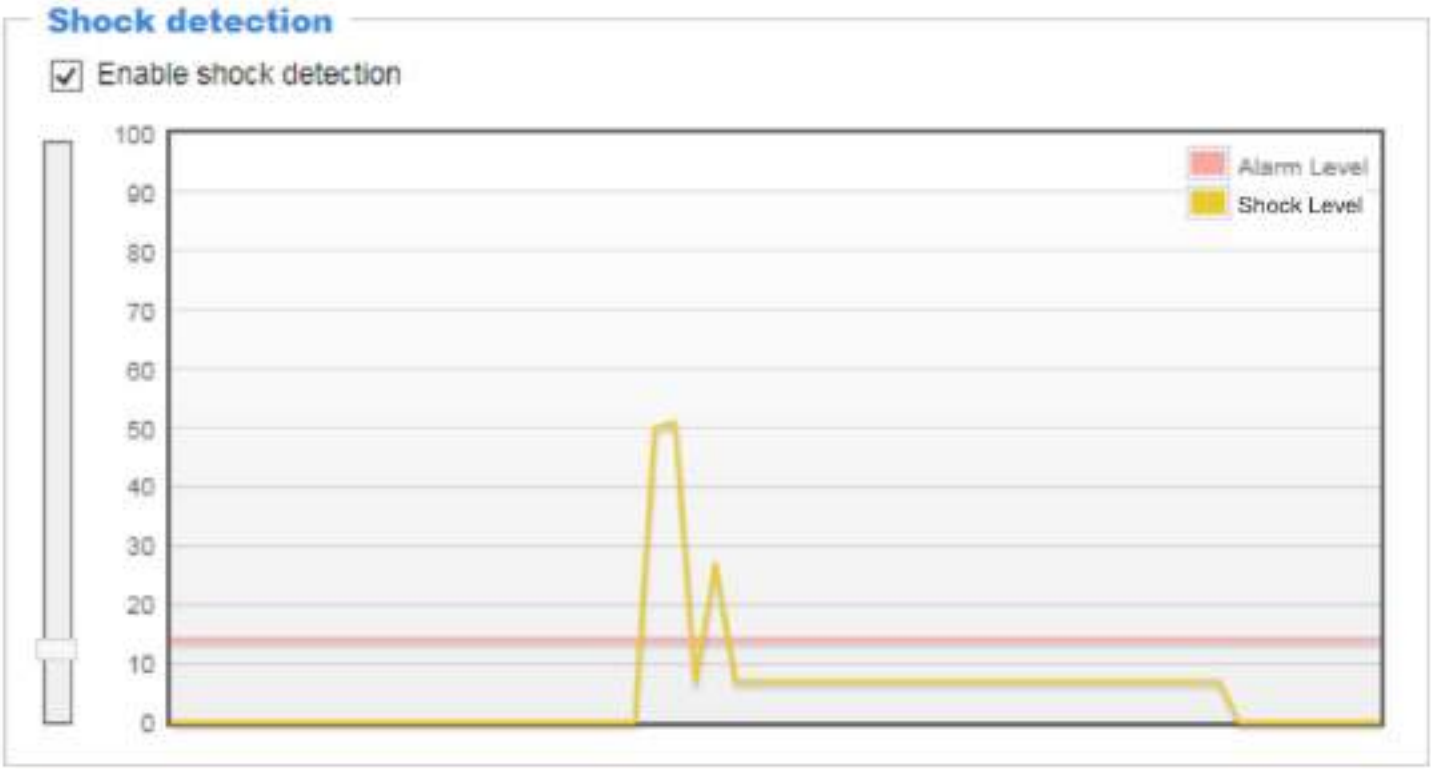


Shock Detection

The camera includes a built-in shock sensor that detects physical impacts. This feature is particularly useful in identifying attempts to tamper with or vandalize the camera. When a significant shock is detected, the camera can trigger an event alert or take other predefined actions.

How It Works

When the camera experiences a strong vibration or impact—such as being hit with an object—the built-in accelerometer detects the force and measures its intensity. For example, a **5kgm impact** typically causes the impact reading to spike to approximately **50%** on the measurement scale.



Configuration

1. Open the **Shock Detection** settings.
2. Adjust the **Alarm Level** slider to your preferred threshold percentage. This determines how much force is required to trigger a shock alert.
3. Select the **Enable Shock Detector** checkbox.
4. Click **Save** to apply the settings.

Technical Details

- **Sensor Range**: ±16G
- **Sensor Resolution**: Each **1G** (where **g = 9.8 m/s^2**) corresponds to **512** internal units.

ⓘ For example:

- A **2G** acceleration generates a value of 512 × 2 ÷ 16 = 64 units per axis.
- If all **three axes (X, Y, Z)** register the same 2G impact, the resulting shock level will be calculated as:

(64 + 64 + 64) × 100 ÷ 1024 = 18.75

This final percentage is what appears on the **Shock Detection chart** in the configuration UI.

Integration With Events

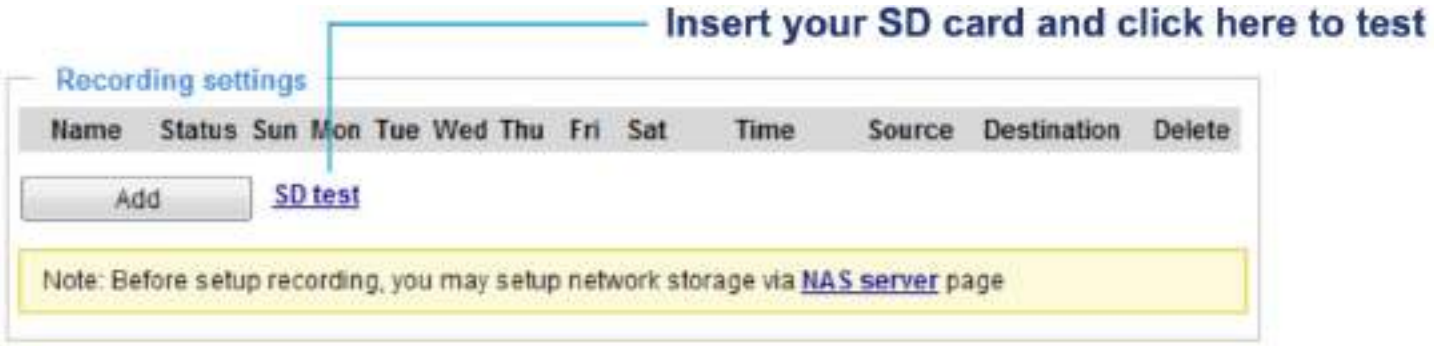
To activate automated responses (e.g., recording, alert emails), configure **Shock Detection** as a **trigger** under **Configuration –> Event Settings –> Trigger.** Refer to that section for step-by-step integration.

Recording Settings

This section explains how to configure video recording behavior for the camera.

Initial Setup

ⓘ Before using an SD card for the first time, format it via **Configuration –> Storage –> Local Storage**. Refer to that section for instructions.



Insert the SD card and click the **Test** button to verify readiness.

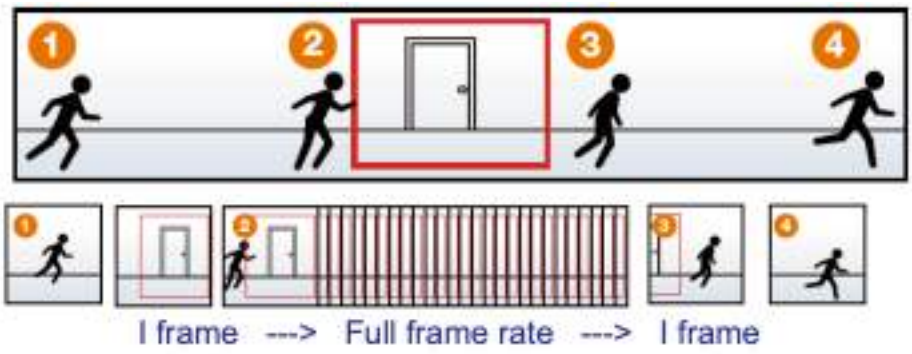
Creating a Recording Profile

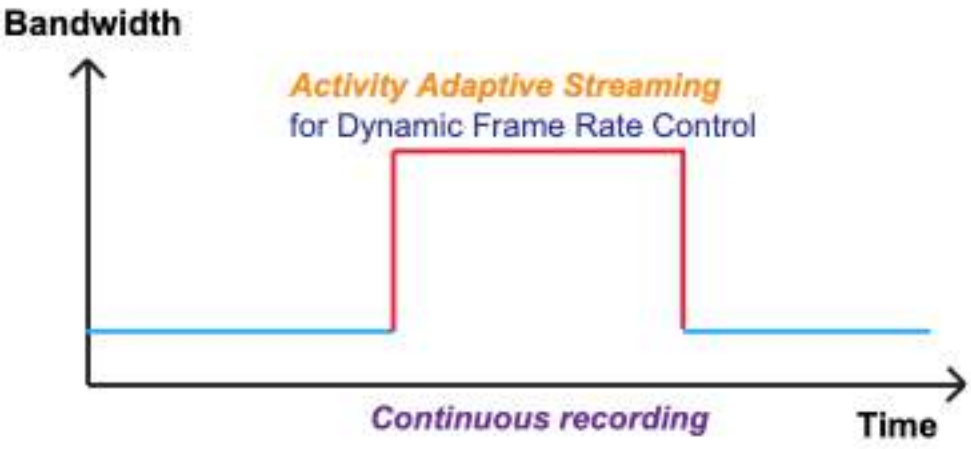
Click the **Add** button to open the recording configuration window. A maximum of **two (2)** recording profiles can be created.

Recording Name: Assign a label to this recording configuration.

Enable This Recording: Check to activate this recording setting.

With Adaptive Recording: When enabled, the frame rate will dynamically adjust based on trigger activity.





- For example, under an alarm trigger, the camera will use the configured high frame rate from the **Media –> Video** settings.
- When idle, it will reduce to low-bandwidth modes (e.g., I-frame only or 1 fps).

ⓘ Supported triggers for adaptive recording include **Motion Detection**, **Digital Input**, or **Manual Trigger**.

Pre-Event Recording / Post-Event Recording:

- The camera uses a buffer to store recent frames.
- Define the number of seconds to include before and after a trigger.

Priority: Select from **High**, **Normal**, or **Low**. Higher-priority recordings take precedence in execution.

Source: Choose the video stream to record from the profile list.

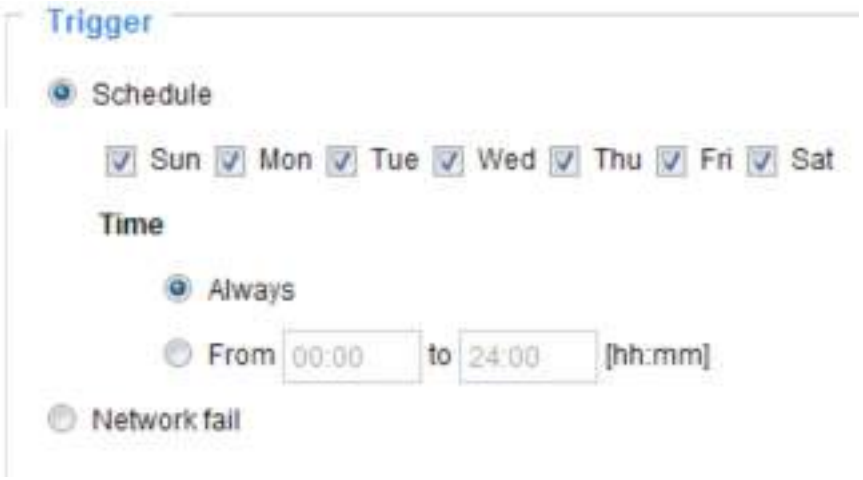
ⓘ To activate recording alerts, set up an event rule in **Configuration –> Event Settings**.

Adaptive Recording Behavior

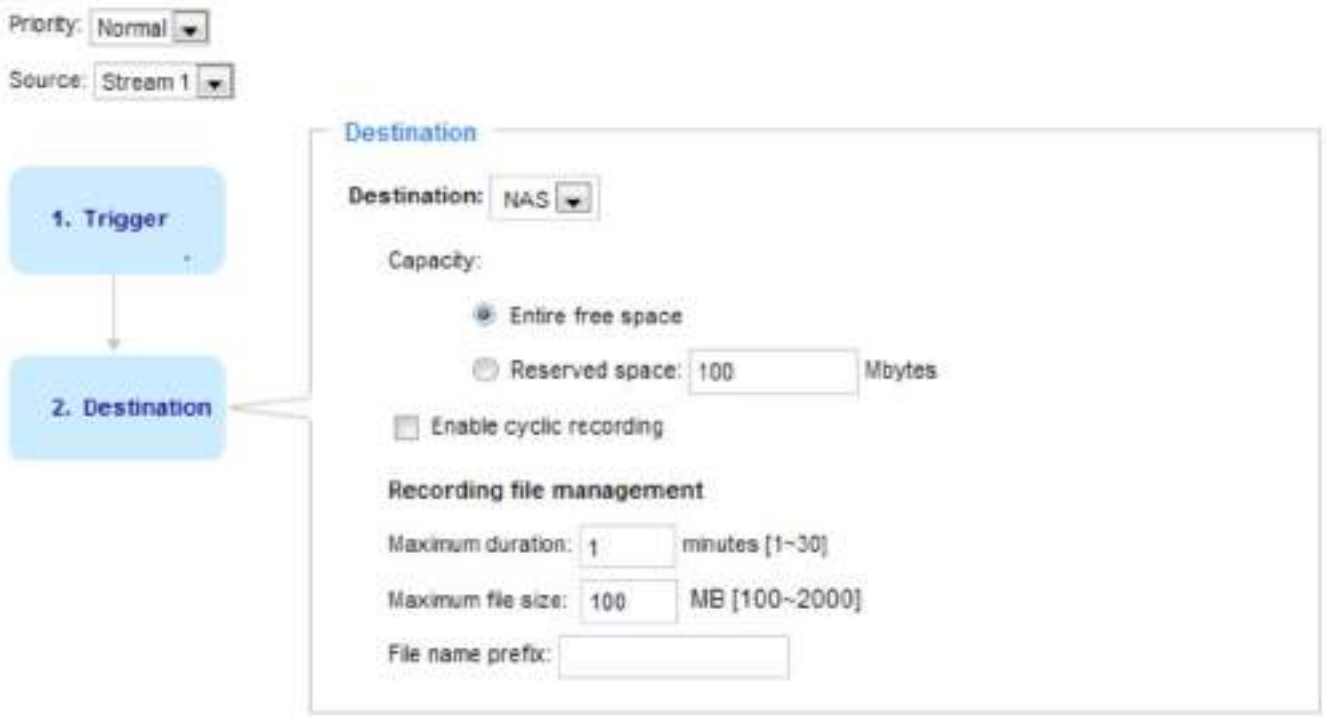
- **No Trigger Active**:
    - **JPEG mode**: records 1 frame per second
    - **H.264 mode**: records I-frame only
- If the **I-frame interval** exceeds 1 second, the system will reduce it to 1s automatically when adaptive mode is enabled.

Setup Steps

1. **Trigger:** Choose a trigger type.



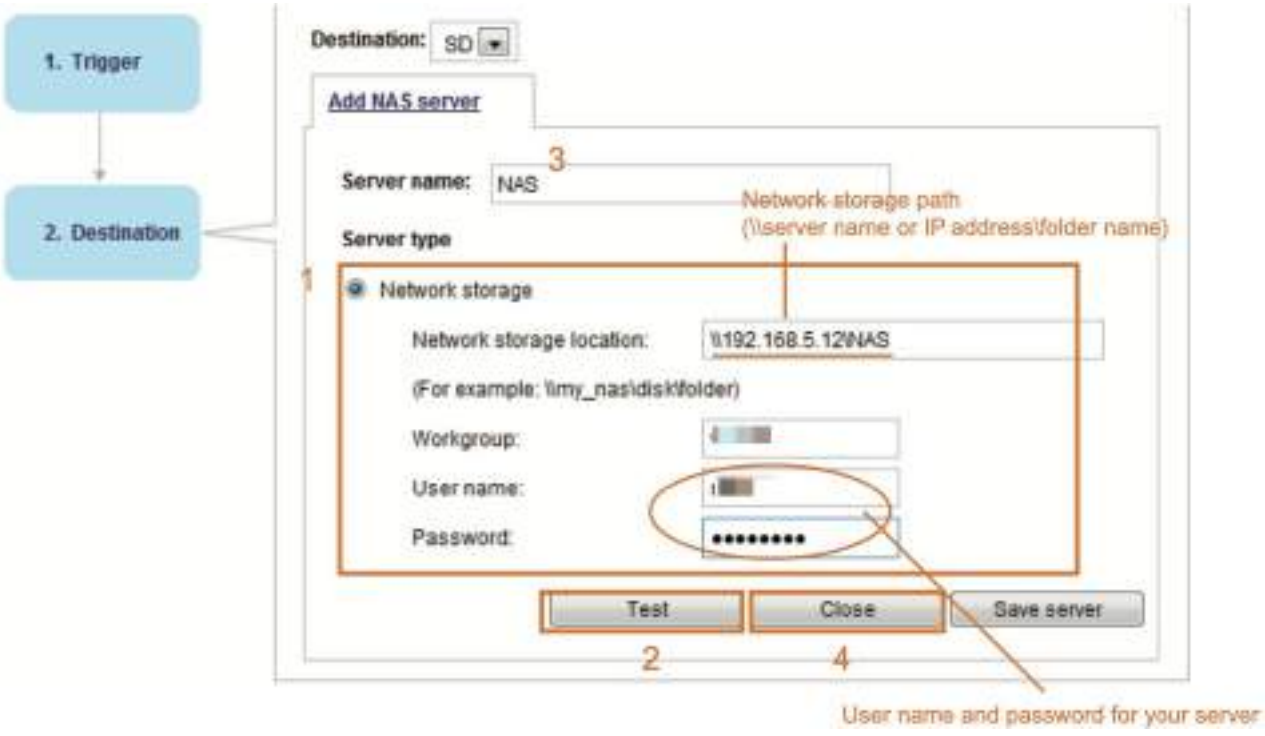
   - **Schedule**: Enables continuous recording based on a defined timetable.
   - **Network Failure**: Activates local SD card recording when the connection to NAS is lost.
2. **Destination:** Select one of the following.



- **SD Card**
- **NAS (Network Storage)**

If using NAS:

1. Click **Add NAS Server**



2. Enter:
    - Server path (e.g., \\IP\shared_folder)
    - Username and password
3. Click **Test** to validate connectivity.

4. Click **Save**, then **Close**

ⓘ A test file named test.txt will be written to confirm access.

Capacity and Storage Behavior

- **Capacity**: You can select to use full available space or specify a limit.
    - Ensure the **Recording Size Limit** exceeds the **Reserved Amount** if using cyclic storage.
- **Enable Cyclic Storage**: When full, older recordings are overwritten by newer files.
- **Reserved Amount**: This buffer allows for smooth transition between overwriting cycles.

Recording File Management

- **Max Duration**: Set the length of each recording file (in seconds).
- **Max File Size**: Define the size cap for each video file (in MB).
- **File Name Prefix**: Input custom text for file naming consistency.

Managing Recording Settings

- To delete a recording: Choose its name from the list and click **Delete**.

- To edit: Click the profile name.
- To disable: Click the **ON** status to toggle **OFF**.
- To browse recordings: Click the **NAS** or **SD Card** link in the Destination column.

ⓘ Folder names are date-based (e.g., 20230701, 20230702). See **Storage –> Content Management** for more.

Final Steps

After configuration:

- Check **Enable This Recording**
- Click **Save**
- Click **Close** to exit

The new profile will appear in the drop-down list on the Recording Settings page. When triggered, the system will begin saving video to the selected destination.

Storage Settings

This section describes how to manage SD card and NAS (Network Attached Storage) configurations, as well as how to search, access, and manage recorded video content stored on the device.

Local Storage (SD Card Management)

You can view the current SD card status and configure local storage options.

SD Card Format

- SD cards **larger than 32GB** are formatted using the **EXT4** file system.
- ⓘ Windows systems cannot read EXT4 by default. Use third-party tools if you need to access EXT4-formatted SD cards on a PC.

SD Card Status

- This column shows whether the SD card is inserted and available, and how much space is reserved or free.

ⓘ Always **turn off recording** before physically removing the SD card from the camera.

Important Notes

- The SD card has a limited lifespan. Replace it periodically for optimal performance.
- A portion of memory is reserved by the camera's internal file system.
- Do **not** use SD cards that contain files from other systems.
- Avoid renaming or moving folders manually on the SD card. This can cause storage errors.

NAS Management

Use this section to configure external NAS for recording and backup.

NAS Setup

1. Click the **NAS Management** tab.

2. Fill in the network path, username, and password.
    - Example path: \\192.160.5.122\NAS
3. Click **Test** to validate connectivity.
4. Click **Mount** to complete setup.

ⓘ Upon success, the system creates a file called test.txt on the NAS.

SD Card Control Options

- **Enable Cyclic Storage**: When enabled, old files are automatically overwritten when space is full.
- **Enable Automatic Disk Cleanup**: Enter the number of days to retain recordings.
    - Example: Set to **7 days** to keep the past week's recordings.
- **Maximum Duration for Keeping Files**: Set the retention window in days.

Click **Save** to apply all changes.

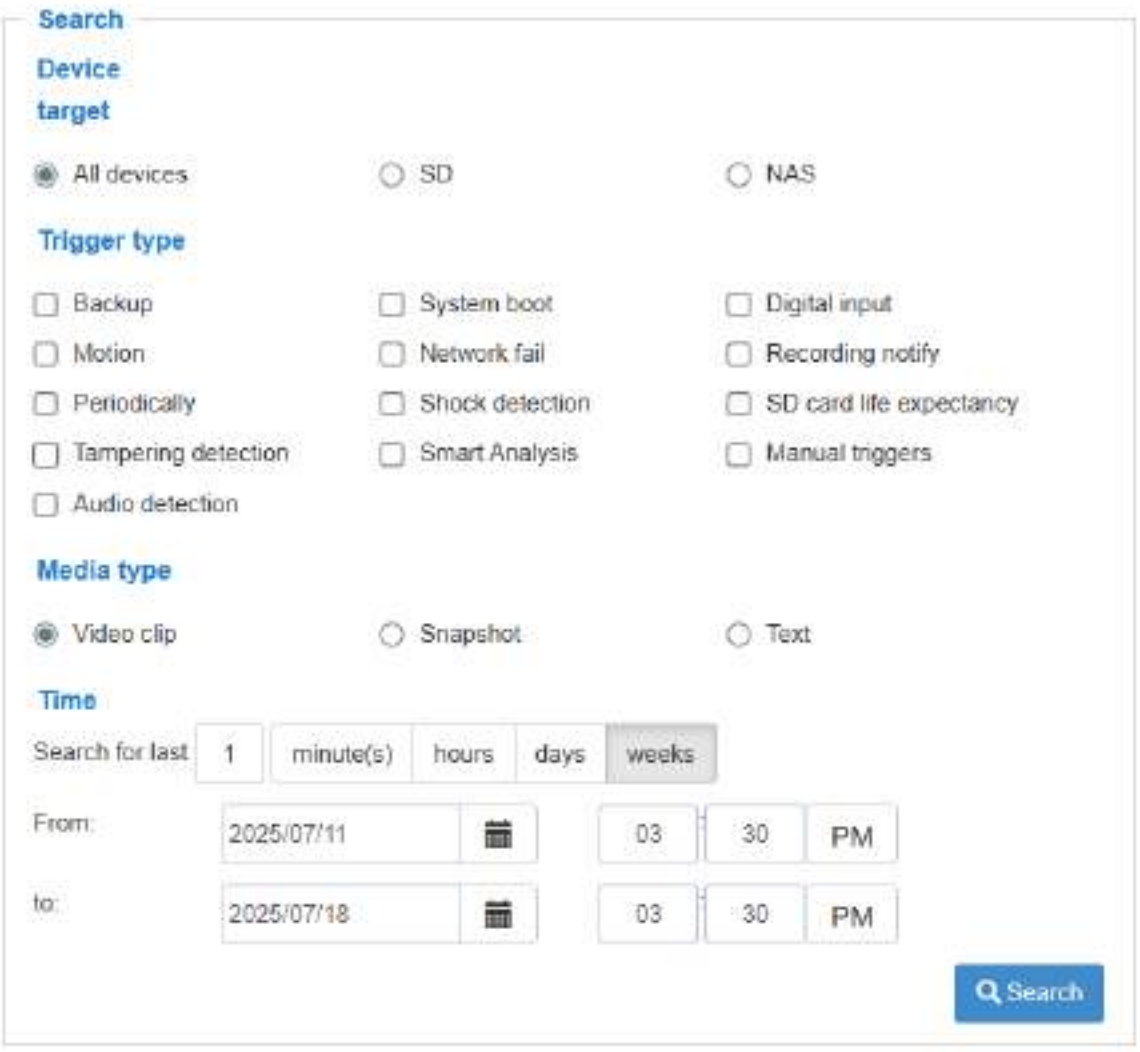
NAS Storage Settings

- **Minimum Reserved Storage Space**: Acts as a buffer for data overflow when cyclic storage is active.
- **Enable Cyclic Storage**: Same function as SD card cyclic mode.
- **Enable Automatic Disk Cleanup**: Choose the retention period (in days) for NAS recordings.
- **Maximum Duration for Keeping Files**: Define lifespan of each file set.

Content Management

This interface allows you to **search**, **play**, **download**, and **delete** recorded video stored on the camera.

Searching and Viewing the Records



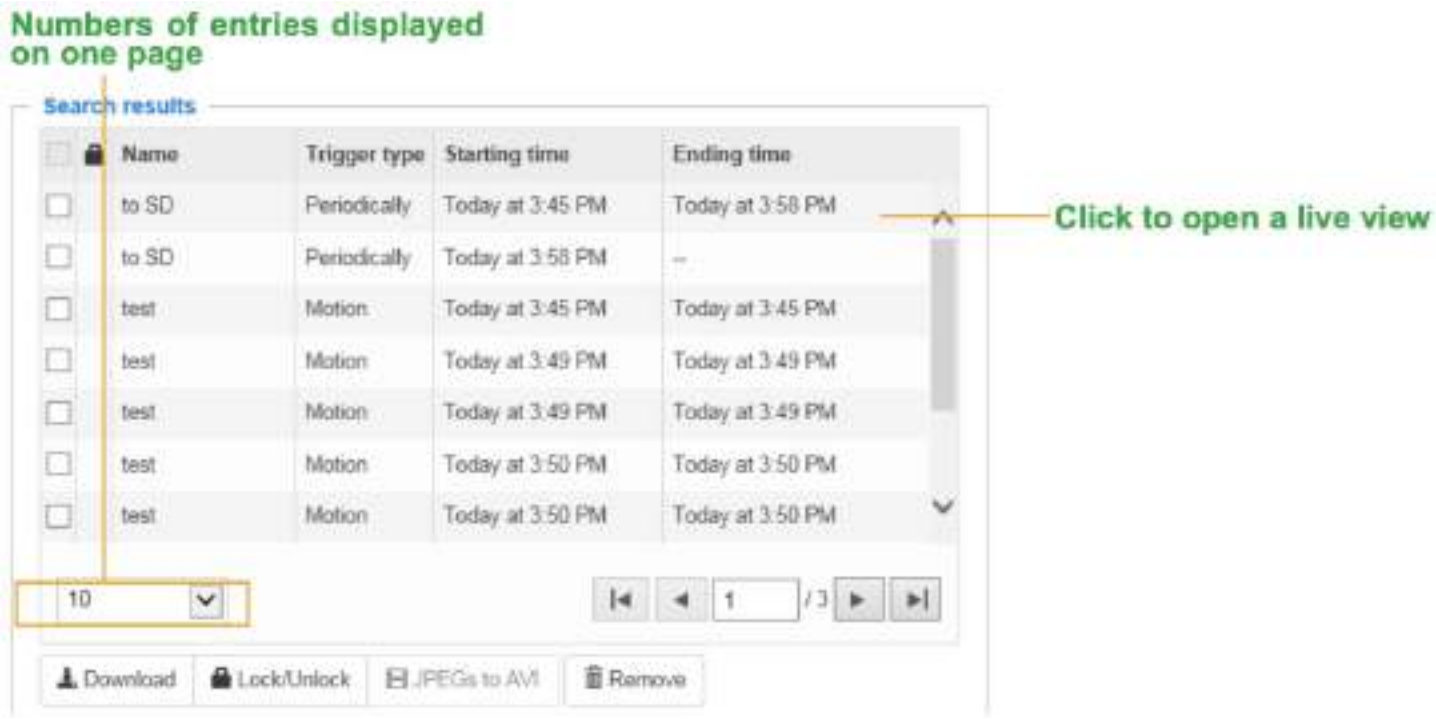
Set search criteria by:

- **File Attributes**: Filter by media type, trigger type, or file lock status.
- **Trigger Time**: Specify a date/time range.

Click **Search**. Results appear in a table with:

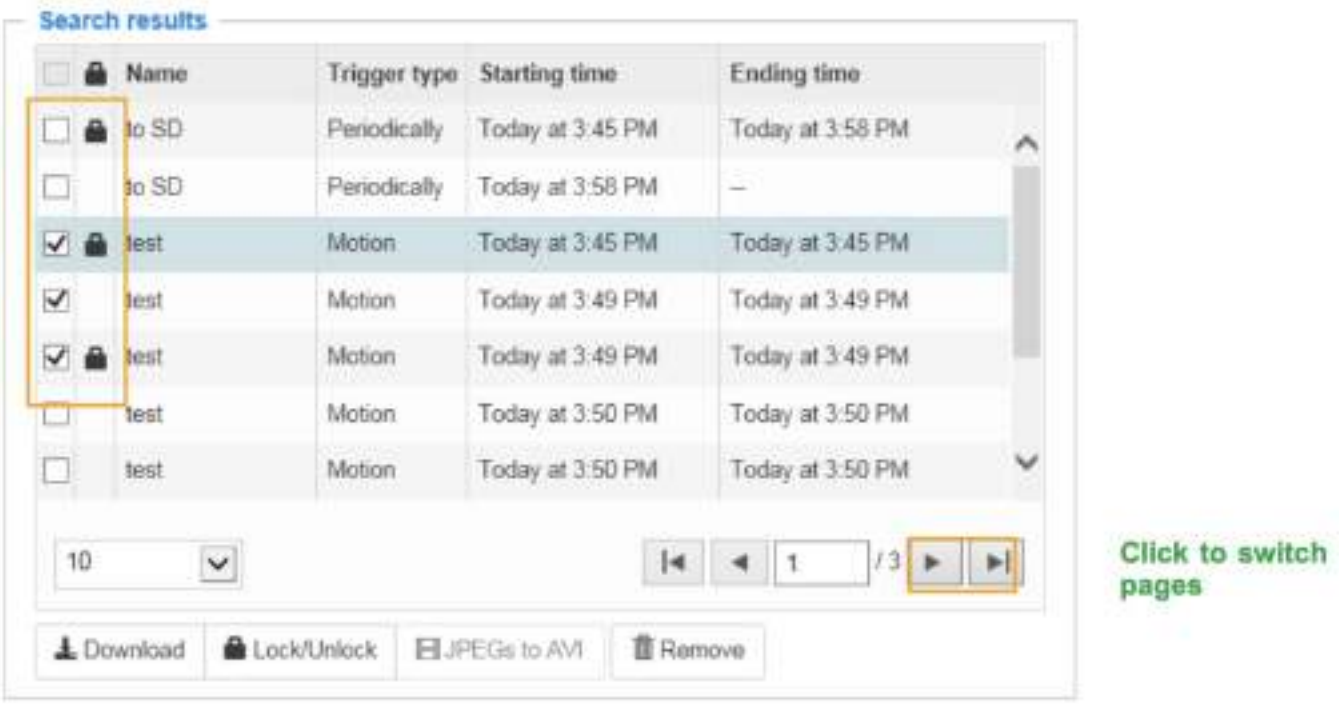
- **Trigger Time**
- **Media Type**
- **Trigger Type**
- **Locked Status**

Click column headers to sort results.



Available Functions

- **Play**: Highlight a file, then click Play to launch the built-in viewer.
- **Download**: Select a file and click **Download** to save it locally.
- **JPEGs to AVI**: Converts selected JPEG snapshots into an AVI video file.
- **Lock/Unlock**: Prevent a file from being deleted during cyclic overwrite.

- 

- **Remove**: Permanently delete selected files.
- **Pagination**: Use arrows to navigate between result pages.