Honeywell 60 Series IP Cameras Configuration Guide

HC60W35R2 HC60W45R2 HC60WB5R2 HC60WZ2E30
HC60W35R4 HC60W45R4 HC60WB5R5

Recommended

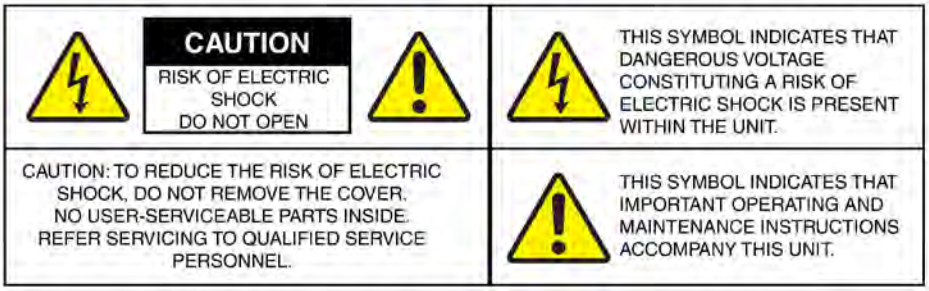
Find the latest version of this and other Honeywell 60 Series IP camera documents on the Honeywell Video website. Go to: http://www.honeywellvideosystems.com/ndaa/ to find your camera and view/download the latest documentation.

Refer to the Honeywell Open Technology Alliance to learn more about our open and integrated solutions (go to: http://www.security.honeywell.com/hota/).

Revisions

Issue	Date	Revisions
A	03/2020	New document.

Cautions and Warnings



WARNING **Installation and servicing should be performed only by qualified and experienced technicians to conform to all local codes and to maintain your warranty.**

WARNING **To ensure compliance with electrical safety standards, CSA Certified/UL Listed LPS or Class 2 power adapters are required. Power over Ethernet (PoE) shall be provided by listed Information Technology Equipment meeting the IEEE 802.3af PoE standard. The PoE is not intended to be connected to exposed (outside plant) networks.**

The Ethernet connection is not intended to be connected to exposed (outside plant) networks. Do not connect two power sources to the camera at the same time.

WARNING **To comply with EN50130-4 requirements, a UPS should be employed when powering the camera from 24 V AC.**

Caution **Invisible LED radiation (850 nm). Avoid exposure to beam.**

Regulatory Statements

Photo biological safety

This product fulfills the requirements for photo biological safety according to IEC/EN 62471 (risk group 1).

General Data Protection Regulation

Please be aware that this product can store personal data.

Personal data is protected by the General Data Protection Regulation (2016/679) in Europe and therefore the owners of personal data have obtained certain rights thanks to this regulation.

We strongly advise you to be fully aware of these owner ("data subjects") rights as well as which limitations you have to obey regarding the use and distribution of this data.

Further details can be found on the GDPR website of the EU:
https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

FCC Compliance Statement (For IPC Model)

Information to the User: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Note	Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class B digital apparatus complies with Canadian ICES-003.

FCC Compliance Statement (For PTZ Model)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense. Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class A digital apparatus complies with Canadian ICES-003.

Manufacturer's Declaration of Conformance

North America

The equipment supplied with this guide conforms to UL 62368-1 and CSA C22.2

No. 62368-1.

Europe

The manufacturer declares that the equipment supplied with this guide is compliant with the European Parliament and Council Directive on the Restrictions of the use of certain hazardous substances in electrical and electronic equipment (2015/863/EU), General Product Safety Directive (2001/95/EC), and the essential requirements of the EMC Directive (2014/30/EU), conforming to the requirements of standards EN 55032 for emissions, EN 50130-4 for immunity, and EN 62368-1 for electrical equipment safety.

Waste Electrical and Electronic Equipment (WEEE)

Correct Disposal of this Product (applicable in the European Union and other European countries with separate collection systems).

This product should be disposed of, at the end of its useful life, as per applicable local laws, regulations, and procedures.

Safety Instructions

Before installing or operating the unit, read and follow all instructions. After installation, retain the safety and operating instructions for future reference.

1. **HEED WARNINGS** - Adhere to all warnings on the unit and in the operating instructions.
2. **INSTALLATION**
   - Install in accordance with the manufacturer's instructions.
   - Installation and servicing should be performed only by qualified and experienced technicians to conform to all local codes and to maintain your warranty.
   - Any wall or ceiling mounting of the product should follow the manufacturer's instructions and use a mounting kit approved or recommended by the manufacturer.
3. **POWER SOURCES –** This product should be operated only from the type of power source indicated on the marking label. If you are not sure of the type of power supplied to your facility, consult your product dealer or local power company.
4. **MOUNTING SYSTEM** - Use only with a mounting system recommended by the manufacturer, or sold with the product.
5. **ATTACHMENTS/ACCESSORIES** - Do not use attachments/accessories not recommended by the product manufacturer as they may result in the risk of fire, electric shock, or injury to persons.
6. **CLEANING** - Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning.

7. **SERVICING** - Do not attempt to service this unit yourself. Refer all servicing to qualified service personnel.
8. **REPLACEMENT PARTS** - When replacement parts are required, be sure the service technician has used replacement parts specified by the manufacturer or have the same characteristics as the original part. Unauthorized substitutions may result in fire, electric shock or other hazards. Using replacement parts or accessories other than the original manufacturers may invalidate the warranty.

Warranty and Service

Subject to the terms and conditions listed on the product warranty, during the warranty period Honeywell will repair or replace, at its sole option, free of charge, any defective products returned prepaid.

In the event you have a problem with any Honeywell product, please call Customer Service at 1.800.323.4576 for assistance or to request a **Return Merchandise Authorization (RMA)** number.

Be sure to have the model number, serial number, and the nature of the problem available for the technical service representative.

Prior authorization must be obtained for all returns, exchanges, or credits. **Items shipped to Honeywell without a clearly identified Return Merchandise Authorization (RMA) number may be refused.**

Table of Contents

Figures

Tables

About This Document

This document provides instructions for accessing, configuring, and operating the Honeywell 60 Series IP cameras. This document is intended for system installers, administrators, and operators.

Overview of Contents

This document contains the following chapters and appendixes:

- *Chapter 1, Introduction*, provides an overview of the main features of the Honeywell 60 Series IP cameras.
- Chapter *2 , Accessing the Camera*, describes how to install the Unified Tool to access the camera remotely from a web browser. It also describes how to update your camera's firmware.
- *Chapter 3, Logging In and Viewing Live Video*, describes how to log in to a camera and using the main page.
- *Chapter 4, Configuring Camera Settings*, describes how to configure the camera settings.
- *Chapter 5, Configuring PTZ Settings*, describes how to configure the PTZ settings.
- *Chapter 6, Configuring Network Settings*, describes how to configure the network settings.
- *Chapter 7, Configuring Video Analytics*, describes how to configure video analytics.
- *Chapter 8, Configuring Storage Settings*, describes how to configure storage settings.
- *Chapter 9, Configuring System Settings*, describes how to configure general system settings.
- *Chapter 10, Viewing System Information*, describes how to view system log, access log and firmware version.
- *Chapter 11, Troubleshooting*, lists common problems and solutions.
- *Chapter 12, Appendix*, lists the descriptions of symbols.

1 Introduction

This chapter contains the following sections:

Overview

Honeywell 60 Series IP cameras integrate traditional camera and network video technology, combining video data collection and transmission. These flexible, fully featured cameras are the ideal choice for a wide range of indoor and outdoor surveillance applications.

The cameras offer 2, 4 or 5 megapixel resolution at up to 60 frames per second and use video compression technology to save bandwidth and storage while ensuring maximum video quality. All the cameras are True Day/Night with intelligent IR capability, providing up to 197 ft (60 m) of illumination in low-light and nighttime scenes. Also, all the cameras support WDR function at up to 120 dB.

Each camera comes with configurable motion detection and camera tamper detection and supports up to 5 user-defined privacy mask areas. In addition to a 12 VDC adapter (for IPC models) or 24 VAC/VDC adapter (for PTZ models), all the cameras support Power over Ethernet (PoE), eliminating the need for a separate power supply and associated wiring. All models also support local video storage on microSDHC cards (up to 256 GB) when network service is interrupted.

Key Features

Key features of the Honeywell 60 Series IP cameras include the following:

Camera

- Up to 5MP (2560x1920) cameras.
- Video parameter setup, such as electronic shutter and gain.
- Motion detection.
- Camera tampering detection.
- True WDR (120 dB).
- True day/night mode using a removable IR cut filter.
- Low-light with 2D/3D noise reduction saving storage and bandwidth together with smart codec.
- Built-in G sensor for third party application integration.
- For use as part of Video Systems which comply with NDAA Section 889.

- PTZ settings (only for HC60WZ2E30).
- FIPS chipset build-in

Storage

- Central server backup (configure in Event settings).
- Recording over Internet, files stored on client PC.

Network

- Up to 10 connections.
- Compatible with the following network protocols: IPv4, IPv6, TCP/IP, HTTP, HTTPS, UPnP, RTSP/RTP/RTCP, IGMP/Multicast, SMTP, DHCP, NTP, DNS, DDNS, CoS, QoS, SNMP, 802.1X, UDP, ICMP, ARP, TLS.
- Support the following security modes: User account and password protection, HTTPS, IP Filter, Digest authentication, TLS1.2 only, Stream encryption, AES128/256, SSH/Telnet closed, PCIDSS compliance, FIPS Chipset Built-In.
- Support the following languages: English, French, German, Italian, Japanese, Portuguese, Russian, Spanish, Traditional Chinese.
- Camera configuration and management via Ethernet.

Events and Analytics

- Support the following Video Analytics types: Intrusion, loiter, line crossing, unattended object, missing object, face detection.
- Support the following event types: Video motion detection, Periodically, Alarm input, System boot, Recording notification, Camera tampering detection.
- Support the following event linkage mode: Event notification using digital output, HTTP, Email and MicroSD card.

User Management

- Each user belongs to specific group.
- Different user rights for each group.

System Management

- Log function.
- Support controlling access permission by verifying the client PC's IP address.
- System resource information and running real-time status display.

2 Accessing the Camera

This chapter contains the following sections:

Installing the Unified Tool

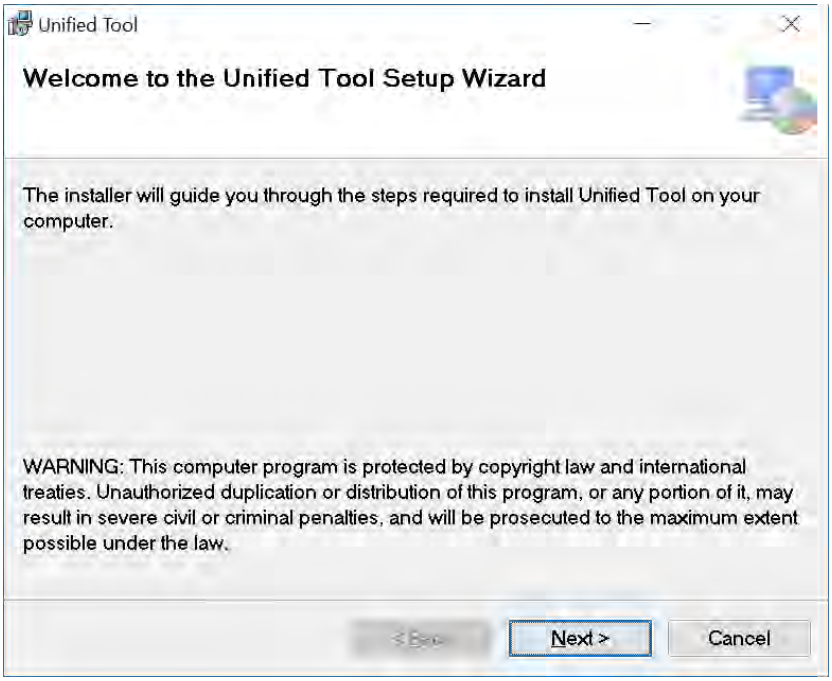
To get the installation package of Unified Tool:

- Browse to https://mywebtech.honeywell.com, login, navigate to Download Center → Video → IP Cameras → Camera Discovery Tools & Utilities → Honeywell Unified Tool, and then download the installation package of Unified Tool to your computer. You need to unzip the package.
- Copy the installation package of Unified Tool from the CD along with the package of the camera to your computer.

To install the Unified Tool:

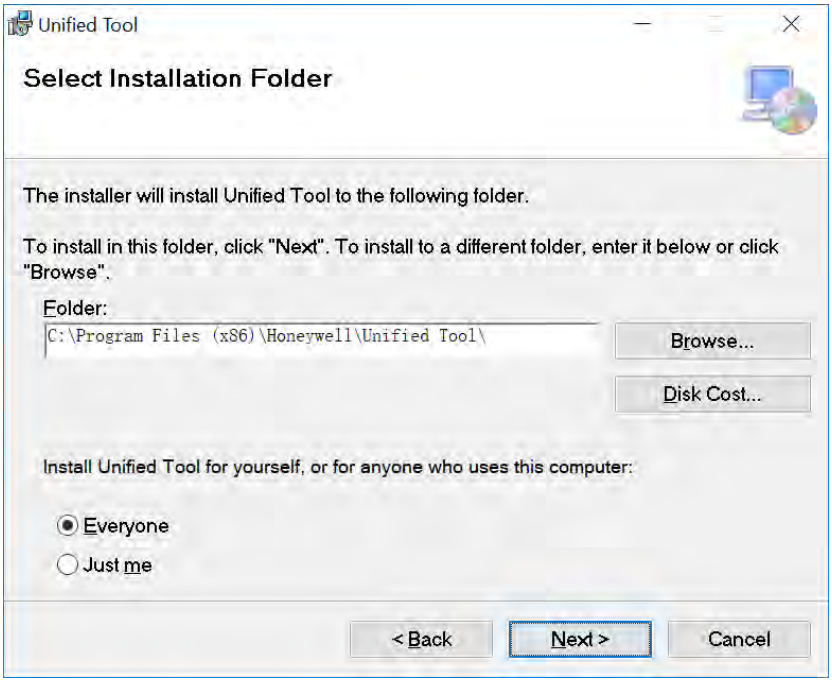
1. Double-click the installation program  in the installation package to install the Unified Tool.

Figure 2-1 Install Unified Tool



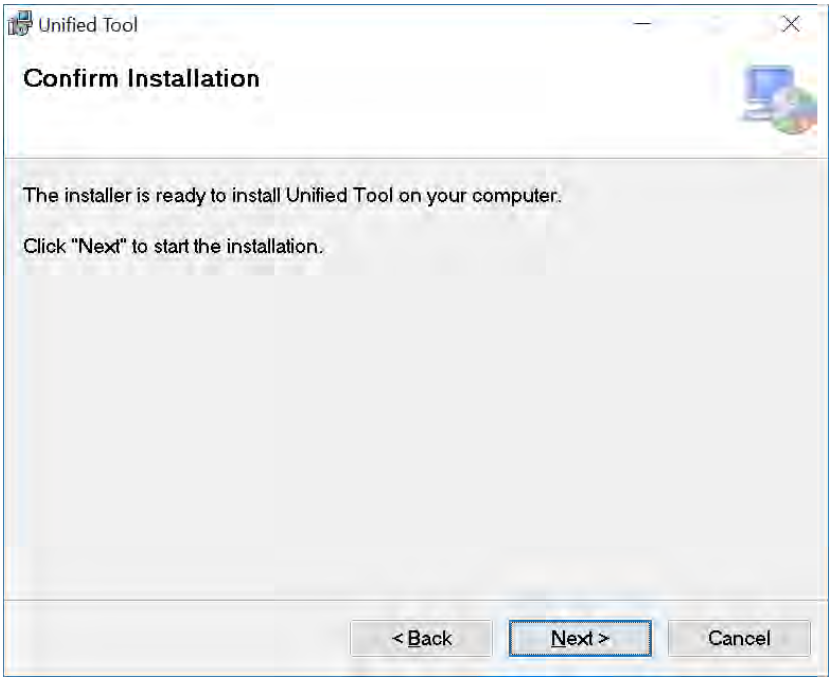
2. Click **Next** and the following figure is displayed:

Figure 2-2 Select Installation Folder



3. Follow the on-screen instructions to configure your settings and click **Next** and the following figure is displayed:

Figure 2-3 Confirm Installation



4. Click **Next** and the installer will install Unified Tool on your computer. After the installation is completed, click **Close**. A shortcut of Unified Tool will be displayed on the desktop.

Discovering Your Camera on the Network

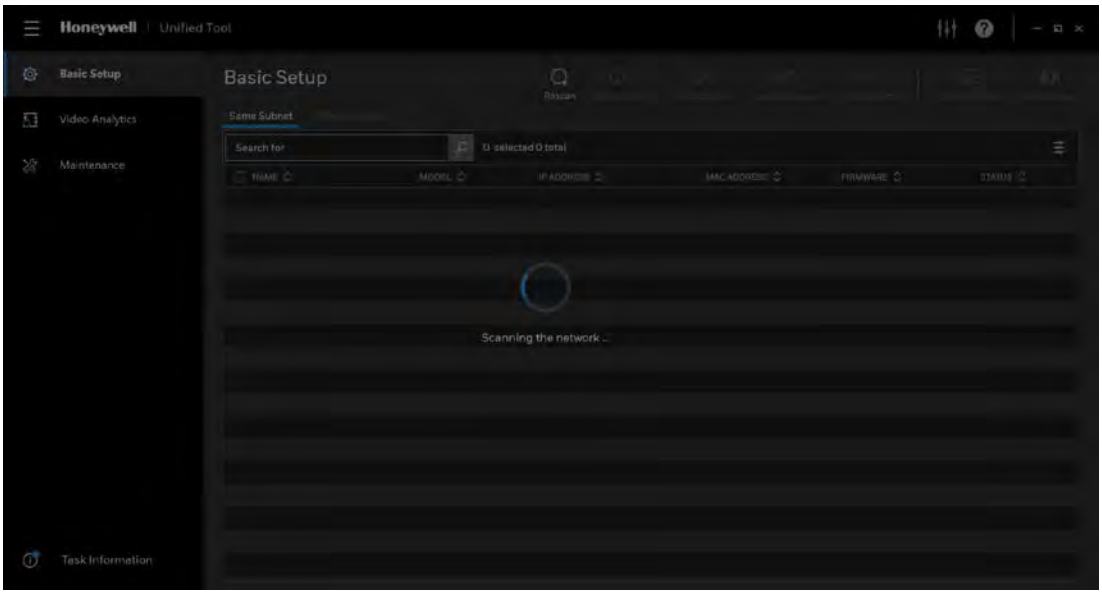
Double-click  on the desktop and the following figure is displayed:

Figure 2-4 Splash Screen

1. Select your language from the dropdown list of Language. Currently, only English is supported.
2. Check “Don’t show the splash window on startup” and this page can be skipped next time.

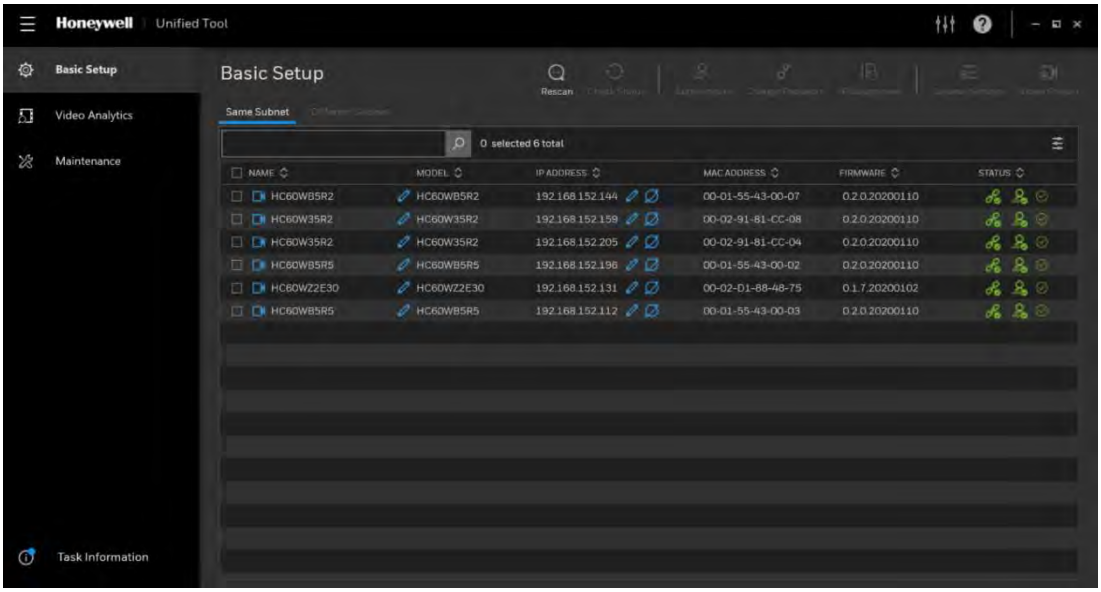
   If you want to check the splash window again, click  as shown in *Figure 2-6* and select the checkbox of Show the splash page on startup.
3. Click **CONTINUE**. It will scan devices in the network automatically.

Figure 2-5 Scanning the network



After the scanning, all scanned devices in the same subnet and different subnet will be displayed in the devices list.

Figure 2-6 Device List

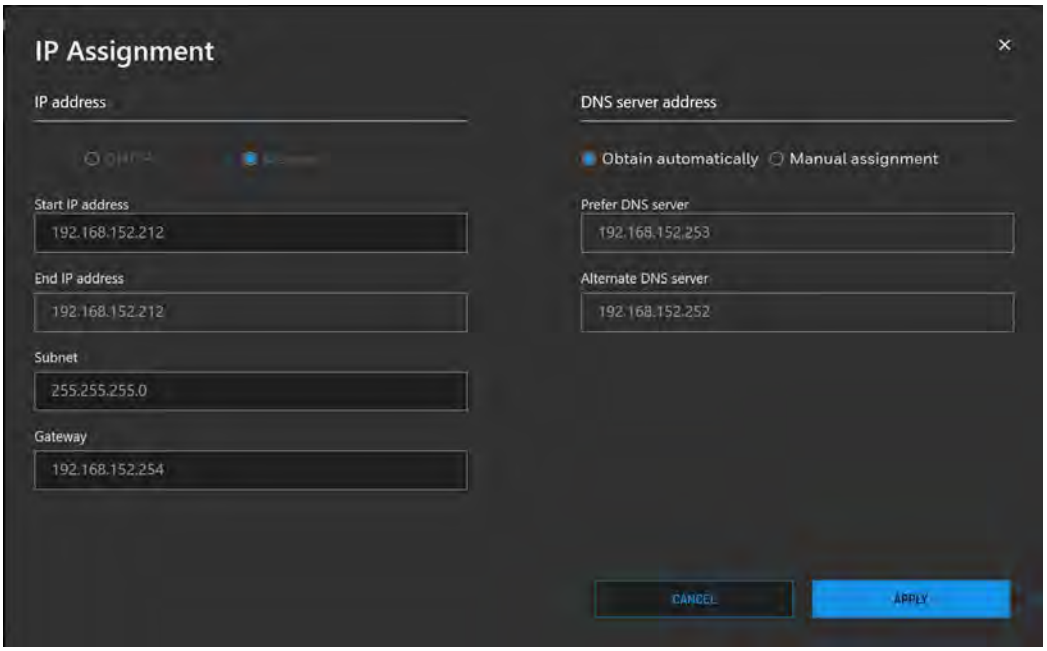


Assigning a New IP Address to Your Camera

The current IP address of your camera appears in the **IP ADDRESS** column of the devices list. If you want, you can assign a new static IP address to the camera.

Select the target device(s) as shown in *Figure 2-6*, click IP Assignment and the following figure is displayed:

Figure 2-7 IP Assignment



Configure IP Address Setting

- To obtain IP address, subnet mask, and default gateway settings automatically, select the check box of **DHCP**.
- To configure IP address, subnet mask, and default gateway settings manually, select the check box of **Manual** and enter the settings. If you enter the start IP address, the system can calculate the end IP address automatically according to the number of your selected device(s).
- After all settings are completed, click **APPLY**.

Configure DNS Server Address

- To obtain the DNS server address automatically, select the check box of **Obtain automatically**.
- To manually enter the DNS server address, select the check box of **Manual assignment** and enter the settings.
- After all settings are completed, click **APPLY**.

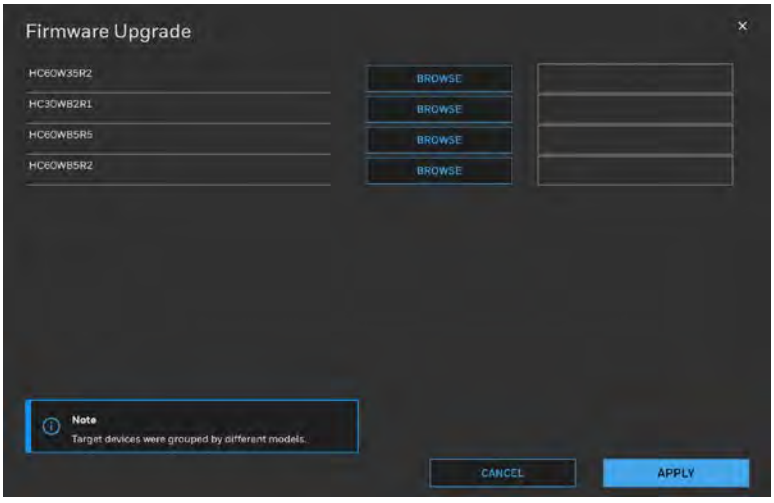
Upgrading the Camera's Firmware

Before you begin using your camera, make sure you have the latest firmware installed. You can upgrade a single camera or multiple cameras at the same time.

Select the **Maintenance** tab from the left pane as shown in *Figure 2-6*, select target device(s) and click 

and the following window is displayed:

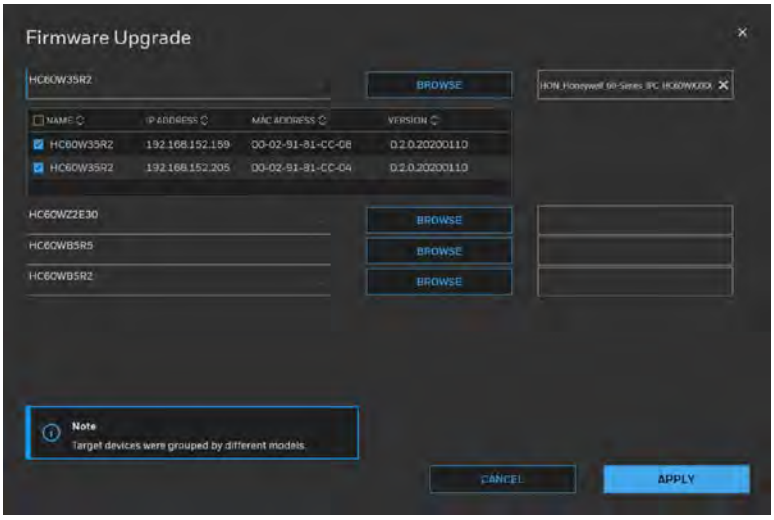
Figure 2-8 Firmware Upgrade



The devices were grouped by model. To upgrade the firmware:

1. Select the target device(s) under a model.
2. Click **BROWSE** and select the upgrade file from your computer.

Figure 2-9 Firmware Upgrade 2



3. Click **APPLY**. You can check the progress status in the device list.

Accessing the Camera from a Web Browser

To access the camera from a web browser, click  next to the IP address of the device as shown in *Figure 2-6*.

3 Logging In and Viewing Live Video

This chapter contains the following sections:

Logging In to the Camera via the Web Client

Using the web client, you can monitor live video, play back recorded video, and configure camera settings.

Before You Begin

Before you log in to the web client, ensure that the following conditions are met:

- The camera is properly connected to the network.
- The camera's IP address and the PC's IP address are in the same network segment. If there is a router, set the corresponding gateway and subnet mask.
- A network connection has been established. To check this, ping the camera's IP address. (Enter "ping [IP address]").

Logging in to the Camera

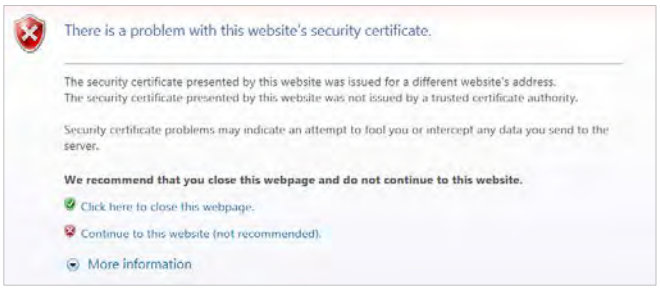
Logging in via Internet Explorer

1. Open **Internet Explorer**, type the camera's IP address in the address bar, and then click **Enter**. For example, if your camera's IP address is **192.168.1.108**, you would type https://192.168.1.108.

Note	Internet Explorer 11 with ActiveX plug-in is supported.

2. The following window is displayed. Click **Continue to this website (not recommended)**.

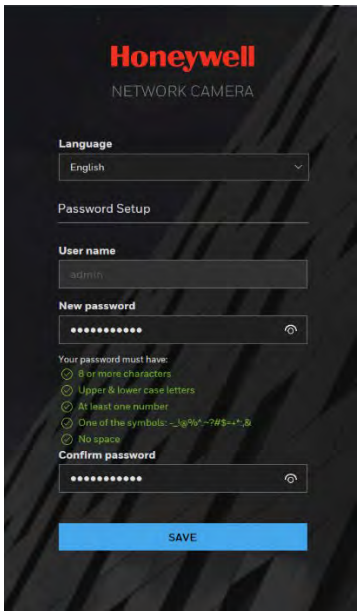
Figure 3-1 Security Certificate Problem



For how to resolve the security certificate problem, see *Export CA Certificate* on page *81*.

3. For security purposes, you are required to create a new secure password at the first login.

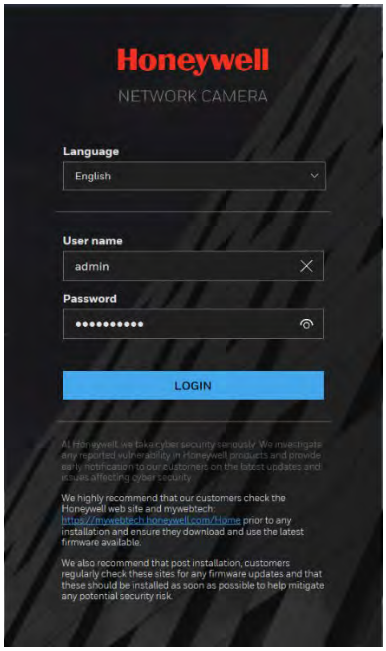
Figure 3-2 Change Password



The password must be at least 8 characters in length and contain at least one uppercase letter, one lowercase letter, one number, and one special character (!?@#$%=+*-_:;.&^~). The password cannot be blank. Click **SAVE**.

4. The login screen is displayed. Enter the admin user name and password, and then click **LOGIN**.

Figure 3-3 Login Page



If you are logging in for the first time, you will be prompted to download and install the plugin. Follow the on-screen instructions to install it. When the installation is complete, the web client automatically refreshes and the main page opens (*Figure 3-7*).

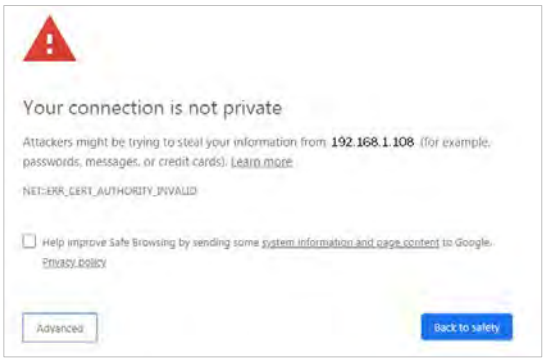
Logging in via Google Chrome

1. Open **Google Chrome**, type the camera's IP address in the address bar, and then click **Enter**. For example, if your camera's IP address is **192.168.1.108**, you would type https://192.168.1.108.

Note	Chrome 79.0 is supported.

2. The following window is displayed. Click **Advanced**.

Figure 3-4 Safety Problem



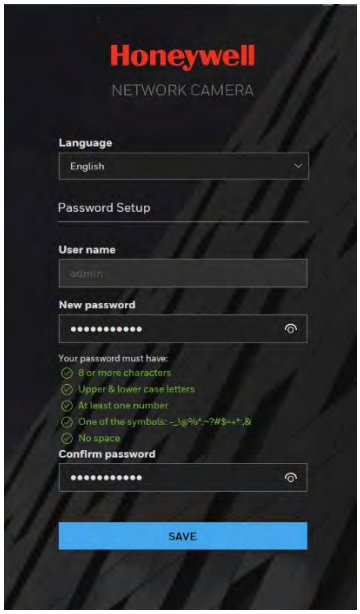
3. The following window is displayed. Click **Proceed to 192.168.1.108 (unsafe)**.

Figure 3-5 Security Certificate Problem

For how to resolve the security certificate problem, see *Export CA Certificate* on page *81*.

5. For security purposes, you are required to create a new secure password at the first login.

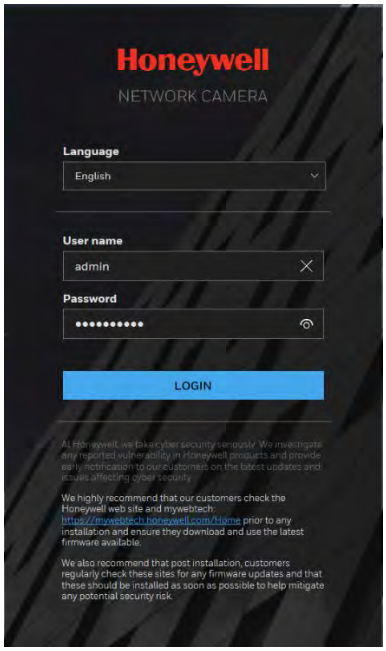
Figure 3-6 Change Password



The password must be at least 8 characters in length and contain at least one uppercase letter, one lowercase letter, one number, and one special character (!?@#$%=+*-_:,.&^~). The password cannot be blank. Click **SAVE**.

4. The login screen is displayed. Enter the admin user name and password, and then click **LOGIN**.

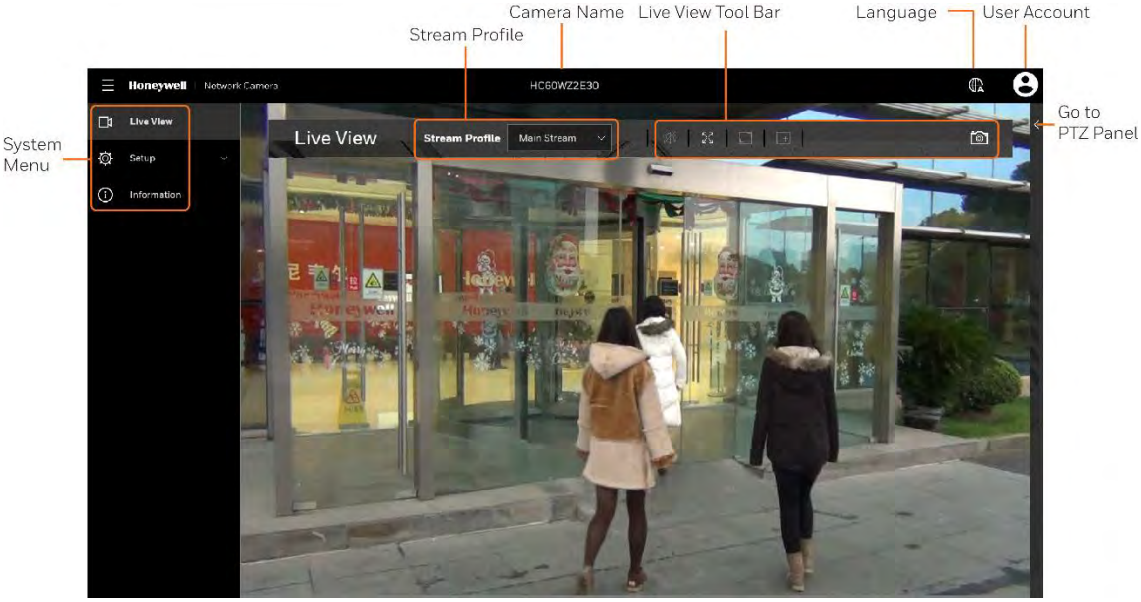
Figure 3-7 Login Page



Using the Main Page

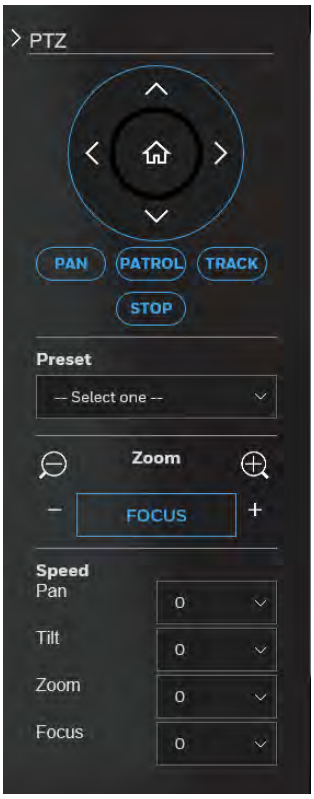
The main page includes the following areas: system menu, live view tool bar, language selection and user account settings.

Figure 3-8 Main Page



For PTZ model, a PTZ panel can be accessed by clicking on the right.

Figure 3-9 PTZ Panel



For details on PTZ operation, see *Configuring PTZ Settings* on page *36*.

System Menu

When you log in to the camera using the web client, the main page opens by default. To access the setup page or information page, select the corresponding tab.

Stream Profile

To set the stream profile, in the **Stream Profile** list, select **Main Stream**, **Sub Stream**, or **Third Stream**.

Main Stream	Delivers high definition video for real-time monitoring, recording, and storage. Uses the most bandwidth.
Sub Stream	Delivers low/standard definition video, typically for remote monitoring in lower network bandwidth environments.
Third Stream	Delivers low definition video.

The properties for each stream type are configured on the **Setup → Camera Setup → Video** page (see *Configuring Video Settings* on page *21*).

Camera Name

You can change the camera name according to your needs. For more information, see *Configuring System General Settings* on page *77*.

Live View Tool Bar

From the Live View toolbar, you can zoom in on a scene, take a snapshot, or manually record video. These controls are described in more details below.

Figure 3-10 Live View Window Controls

Table 3-1 Live View Window Controls

Icon	Description
	Click to turn on the audio to listen to the monitoring site. Click it again to turn off the audio. (The audio couldn't be closed in the Chrome browser)
	Click to switch to the full screen mode. Press the "Esc" key or double click the screen to switch to the normal mode.
	Click to auto fit the image. (This function is not applicable in the Chrome browser)
	Click and uncheck **Disable digital zoom** in the pop up window to enable the zoom operation. The navigation screen shows the part of the image being magnified. To resize the navigation area, drag the border. To move to a different area you want to magnify, drag the navigation screen. To zoom the image, scroll the mouse wheel. (This function is not applicable in the Chrome browser)
	Click to capture and save video images. The captured images will be displayed in a pop-up window. Right click the image and select **Save picture as** to save it in JPEG (*.jpg) or BMP (*.bmp) format.

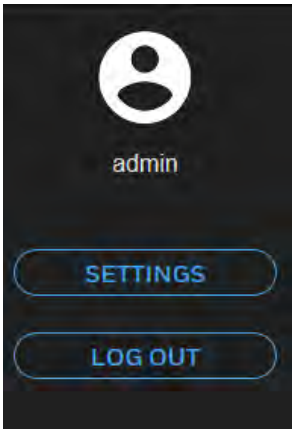
Language

To switch a language, click as shown in *Figure 3-8*.

User Account

To configure user account or log out the current account, click as shown in *Figure 3-8* and the following figure is displayed:

Figure 3-11 User Account



To configure the user account, click **SETTINGS**. For details, see *Configuring User Accounts Settings* on page *82*.

To log out the current account, click **LOG OUT**.

4 Configuring Camera Settings

This chapter contains the following sections:

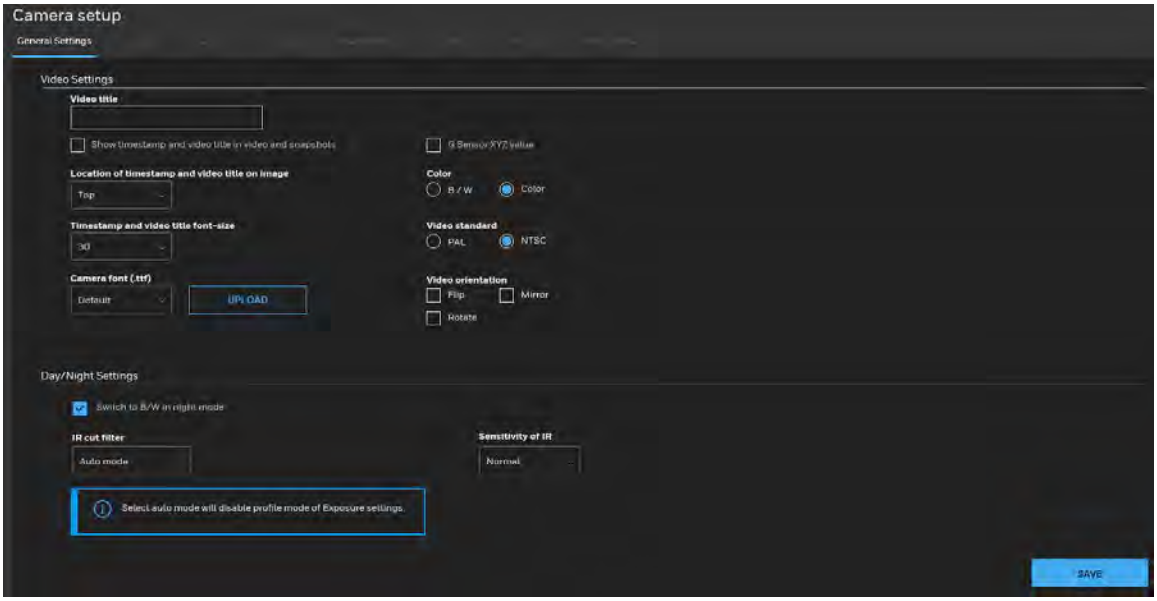
Note	Click **SAVE** to enable the settings after you completed the settings on each page.

Configuring General Settings

Go to **Setup →Camera Setup→General Settings**.

On this page, you can configure the general video settings and day/night settings.

Figure 4-1 General Settings



Video Settings

Video Title: Enter a name that will be displayed on the title bar of the live video.

Show times tamp and video title in video and snapshots: Check to display timestamp and video title in live video and snapshots.

G Sensor XYZ value: Check to display G-sensor XYZ value on the screen. The G-sensor XYZ value is recommended for the third party platform to perform data conversion.

Location of time stamp and video title on image: Select a position from the dropdown list to display timestamp and video title on the top or at the bottom of the video stream.

Time stamp and video title font-size: Select a font size for the timestamp and title.

Camera font (.ttf): You can select a True Type font file for the display of textual messages on video.

Color: Select to display color or black/white video streams.

Video Standard: Select the video standard: NTSC or PAL.

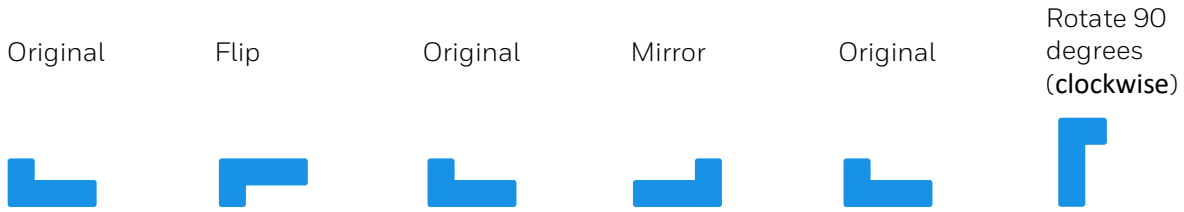
Note	If the video standard is changed, you must disconnect and reconnect the power cord of the camera in order for the new setting to take effect.

Video orientation:

- Flip: vertically reflect the display of the live video;
- Mirror: horizontally reflect the display of the live video.

- Select both Flip and Mirror if the camera is installed upside-down (e.g., on the ceiling) to correct the image orientation.
- Rotate: Rotate the video by 90 degrees or 270 degrees. The rotation here indicates clockwise rotation. Rotation can be applied with flip, mirror, and physical lens rotation settings to adapt to different mounting locations, such as a corridor.

Figure 4-2 Video Orientation



Note	The flip/mirror/rotate operation will clear the video settings, privacy mask settings, exposure window, motion detection settings, preset position and focus window.

Day/Night Settings

Switch to B/W in night mode: Check to enable the camera to automatically switch to Black/White during night mode.

Mode:

- Auto mode (The Day/Night Exposure Profile will not be available if Auto mode is selected)

  The camera automatically removes the filter by judging the level of ambient light.

Note	Select auto mode will disable profile of exposure settings.

- Day mode

  In day mode, the camera switches on the IR cut filter at all times to block infrared light from reaching the sensor so that the colors will not be distorted.

- Night mode

  In night mode, the camera switches off the IR cut filter at all times for the sensor to accept infrared light, thus helping to improve low light sensitivity.

- Schedule mode

  The camera switches between day mode and night mode based on a specified schedule. Enter the start and end time for day mode. The time format is [hh:mm] and is expressed in 24-hour clock time. By default, the start and end time of day mode are set to 07:00 and 18:00.

Sensitivity: Adjust the responsiveness of the IR filter to lighting conditions as **Low**, **Normal**, or **High**.

Configuring Video Settings

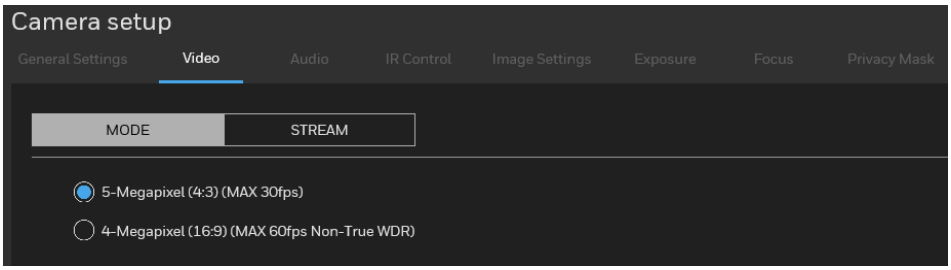
Go to **Setup →Camera Setup → Video**.

This section describes how to configure viewing window and video streaming properties (format, resolution, frame rate, bit rate, I-frame interval, etc.).

Mode

Go to **Setup →Camera Setup → Video→ Mode**.

Figure 4-3 Mode



5-Megapixel (4:3) (MAX 30fps): Select it and the maximum resolution will be 2560x1920. The aspect ratio will be 4:3.

4-Megapixel (16:9) (Max 60fps Non-True WDR): Select it and the maximum resolution will be 2560x1440. The aspect ratio will be 16:9.

2-Megapixel (16:9) (Max 60fps): Select it and the maximum resolution will be 1920x1080. The aspect ratio will be 16:9.

2-Megapixel (16:9) (Max 30fps): Select it and the maximum resolution will be 1920x1080. The aspect ratio will be 16:9.

Note	• 5-Megapixel and 4-Megapixel are applicable for HC60W35R2/HC60W45R2/HC60WB5R2/HC60W35R4/HC60W45R4/HC60WB5R5. • 2-Megapixel is applicable for HC60WZ2E30.

Note	Changing the video mode will clear the following settings: privacy mask, exposure widow, motion, preset position and focus window.

Video Stream

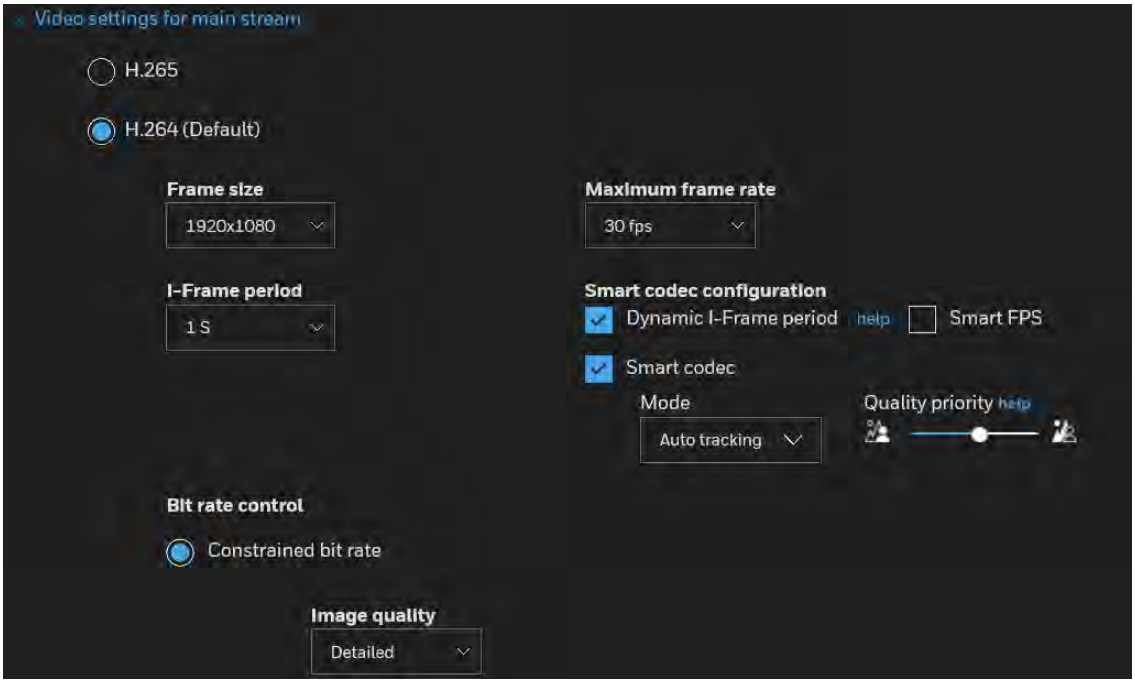
Go to **Setup →Camera Setup → Video→ Stream**.

See the following table for streams and frame sizes of each model:

Table 4-1 Stream and Frame Size Matrix

Model	Main Stream	Sub Stream	Third Stream
HC60W35R2/ HC60W35R4/ HC60W45R2/ HC60W45R4/ HC60WB5R2/ HC60WB5R5	2560×1440/ 1920×1080/ 1600×904/ 1360×768/ 1280×720/ 640×360 (1-25/30fps), 1920x1080/ 1600x904/ 1360x768/ 1280x720/ 640x360 (1-50/60fps), 2560x1440 (1-50fps)	2560×1440/ 1920×1080/ 1600×904/ 1360×768/ 1280×720/ 640×360 (1-25/30fps), 1920x1080/ 1600x904/ 1360x768/ 1280x720/ 640x360 (1-50/60fps), 2560x1440 (1-50fps)	1280x960/ 640x480 (1-25/30fps), 1280x720/ 640x360 (1-50/60fps)
HC60WZ2E30	1920×1080/ 1280x720/ 640x360	1280x720/ 640x360	640x360

Figure 4-4 Video Stream



Frame size

Set different video resolutions for different viewing devices. For example, you can configure a smaller frame size and lower bit rate for remote viewing on mobile phones and a larger video size and a higher bit rate for live viewing on web browsers, or recording the stream to an NVR. A larger frame size takes up more bandwidth.

Maximum frame rate

This limits the maximum refresh frame rate per second. Set the frame rate higher for smoother video quality and for recognizing moving objects in the field of view.

If the power line frequency is set to PAL, the frame rates are selectable from 1-50 fps. If the power line frequency is set to NTSC, the frame rates are selectable from 1-60 fps. You can also select **Customized** and manually enter a value.

The frame rate will decrease if you select a higher resolution.

Intra frame period

Determine how often for firmware to plant an I frame. The shorter the duration, the more likely you will get better video quality, but at the cost of higher network bandwidth consumption. Select the intra frame period from the following durations: 1/4 second, 1/2 second, 1 second, 2 seconds, 3 seconds, and 4 seconds.

Smart codec configuration

Dynamic Intra frame period

High quality motion codecs, such as H.265, utilize the redundancies between video frames to deliver video streams at a balance of quality and bit rate. The encoding parameters are summarized and illustrated below. The I-frames are completely self-referential and they are largest in size. The P-frames are predicted frames. The encoder refers to the previous I- or P-frames for redundant image information.

Smart FPS

In a static scene, the algorithm puts old frames in queue when no motions occur in scene. When motions occur, the encoding returns to normal to deliver real-time streaming.

By queuing the old frames from a static scene, both the computing efforts and the size of P frames are reduced. It is beneficial for keeping up with the frame rate requirements.

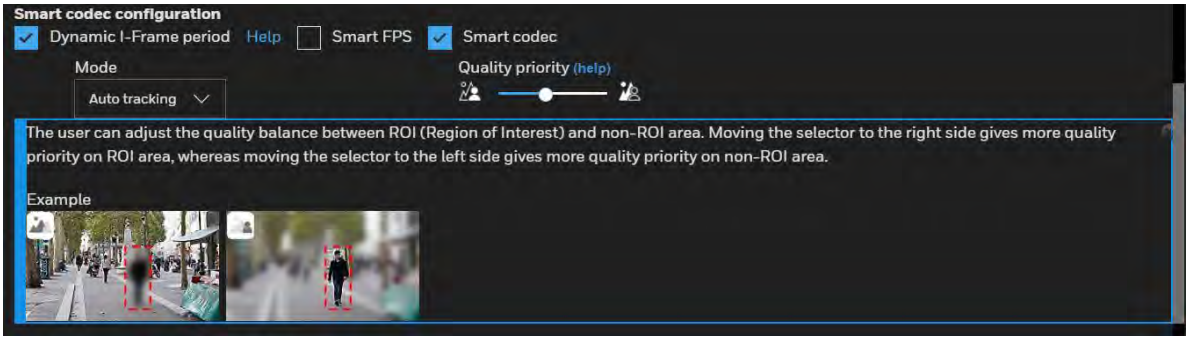
A default frame difference threshold, 1%, is embedded in firmware for returning from Smart FPS to normal encoding when motions occur.

Smart codec

Smart codec effectively reduces the quality of the whole or the non-interested areas on a screen and therefore reduces the bandwidth consumed.

You can manually specify the video quality for the foreground and the background areas.

Figure 4-5 Smart codec



Select an operation mode if Smart codec is preferred.

- Auto tracking: The Auto mode configures the whole screen into the non-interested area. The video quality of part of the screen returns to normal when one or more objects move in that area. The remainder of the screen where there are no moving objects (no pixel changes) will still be transmitted in low-quality format.
- Manual: The Manual mode allows you to configure 3 ROI windows (Region of Interest, with Foreground quality) on the screen. Areas not included in any ROI windows will be considered as the non-interested areas. The details in the ROI areas will be transmitted in a higher-quality video format.
- Hybrid: The major difference between the “Manual” mode and the “Hybrid” mode is that:

  In the “Hybrid“ mode, any objects entering the non-interested area will restore the video quality of the moving objects and the area around them. The video quality of the associated non-interested area is immediately restored to normal to cover the moving objects.

  In the “Manual” mode, the non-interested area is always transmitted using a low-quality format regardless of the activities occurring inside.
- Quality priority: Drag the slider to adjust the quality contrast between the ROI and non-interested areas.
  - The farther the slider is to the right, the higher the image quality of the ROI areas.
  - On the contrary, the farther the slider to the left, the higher the image quality of the non-interested area.

  In this way, you may set up an ROI window as a privacy mask by covering a protected area using an ROI window, while the rest of the screen becomes the non-interested area. You may then configure the non-interested area to have a high image quality, or vice versa.

Bit rate control

Constrained bit rate

A complex scene generally produces a larger file size, meaning that higher bandwidth will be needed for data transmission. The bandwidth utilization is configurable to match a selected level, resulting in mutable video quality performance.

- **Image quality**: Select a desired quality ranging from Medium to Excellent. If you select **Customized**, you can enter a value to specify the quality.
- **Maximum bit rate**: Select a bit rate from the dropdown list. The bit rate ranges from 20 Kbps to a maximum of 80 Mbps. If you select **Customized**, you can enter a value to specify the maximum bit rate.
- **Priority**: If **Frame rate** is selected, the camera will try to maintain the frame rate per second performance, while the image quality will be compromised. If **Image quality** is selected, the camera may drop some video frames in order to maintain image quality.

Fixed quality

All frames are transmitted with the same quality.

- Quality: Select a desired quality ranging from Medium to Excellent. If you select **Customized**, you can enter a value to specify the quality.

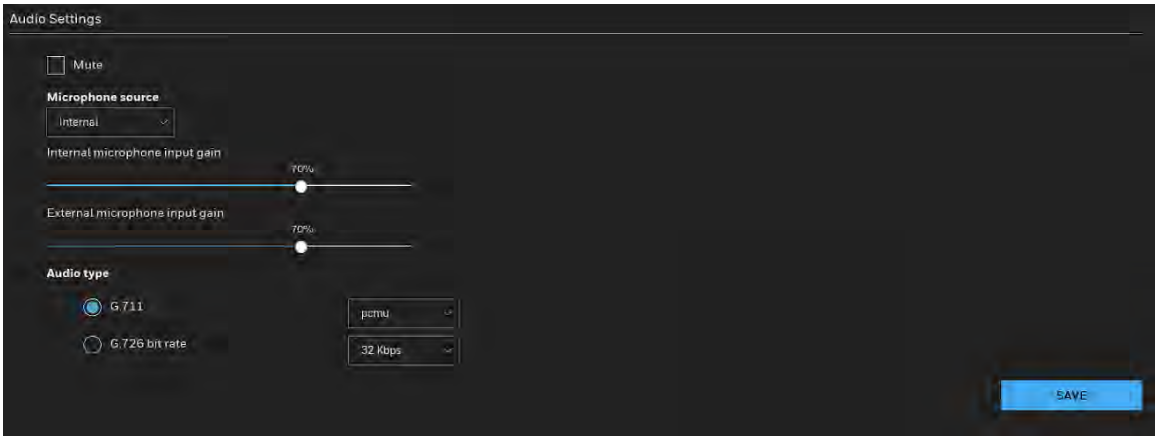
- Maximum bit rate: Select a bit rate from the dropdown list. The bit rate ranges from 1 Mbps to a maximum of 40Mbps. If you select **Customized**, you can enter a value to specify the maximum bit rate.

  The Maximum bit rate setting in the Fixed quality configuration can ensure a reasonable and limited use of network bandwidth. For example, in low light conditions where a Fixed quality setting is applied, video packet sizes can tremendously increase when noises are produced with electrical gains.

Configuring Audio Settings

Go to **Setup →Camera Setup → Audio**.

Figure 4-6 Audio



Mute: Check to disable audio transmission from the Network Camera to all clients.

Microphone source: Select **Internal** or **External** from the dropdown list.

Note	The Internal microphone source is applicable for HC60W35R2 & HC60W35R4.

Internal microphone input gain: Select the gain of the internal audio input according to ambient conditions. Adjust the gain from 0% (least) to 100% (most).

Note	The Internal microphone input gain is applicable for HC60W35R2 & HC60W35R4.

External microphone input gain: Select the gain of the external audio input according to ambient conditions. Adjust the gain from 0% (least) to 100% (most).

Audio type: Select audio codec as G.711 or G.726 and the bit rate.

- G.711 provides good sound quality and requires about 64Kbps. Select pcmu (μ-Law) or pcma (A-Law) mode.
- G.726 is a speech codec standard covering voice transmission at rates of 16, 24, 32, and 40kbit/s.

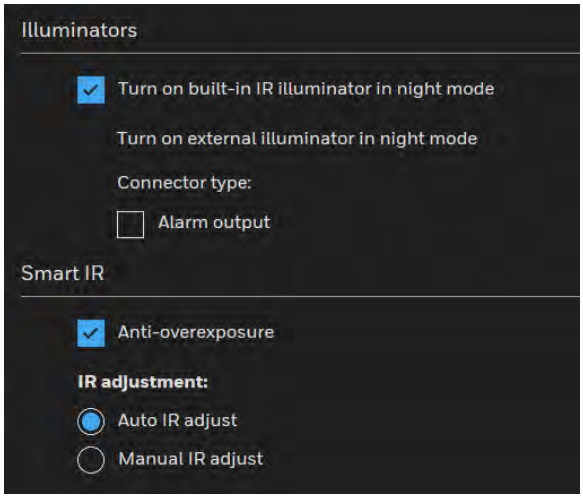
After you complete the settings on this page, click **SAVE** to enable the settings.

Configuring IR Control Settings

Go to **Setup →Camera Setup→IR Control**.

On this page, you can turn on the IR illuminator and adjust the luminance of IR lights.

Figure 4-7 IR Control Settings



IR Illuminators

Turn on built-in IR illuminator in night mode: Check to turn on the camera's onboard IR illuminator when the camera detects low light condition and enters the night mode.

Turn on external illuminator in night mode: Check the connector type to turn on the camera's external IR illuminator when the camera detects low light condition and enters the night mode. You should connect an alarm output first.

Note	The built-in IR illuminator function is not applicable for HC60WZ2E30.

Smart IR

Anti-overexposure: When checked, the camera automatically adjusts the shutter speed, Gain and IRIS through algorithm of the firmware in order to avoid over-exposure in the night mode.

IR Adjustment: Adjust the luminance of IR lights.

- Auto IR adjust: Select it to control the luminance of IR lights automatically.
- Manual IR adjust: Select it to control the luminance of IR lights manually. To increase the luminance of IR lights, drag the slider to the right; to decrease the luminance of IR lights, drag the slider to the left.

Note	The Smart IR function is not applicable for HC60WZ2E30.

Configuring Image Settings

Go to **Setup →Camera Setup → Image Settings**.

On this page, you can configure the White balance and adjust Image parameters.

Two sets of image settings are available:

- In **Normal Light Mode** tab, configure normal situations for image settings.
- In **Profile Mode** tab, configure special situations for image settings.
  - Night Mode: Check **Enable to apply these settings at** and select this mode to apply the settings at night.
  - Schedule Mode: Check **Enable to apply these settings at** and select this mode to apply the settings at a specific period. Enter the time manually in the field.

Figure 4-8 Image Settings

White Balance

Adjust the value for the best color temperature.

Auto: Select it and the camera will automatically adjust the color temperature.

Fixed current: Select it and the camera will use current color temperature value.

Manual: You may manually tune the color temperature by dragging the R Gain and B Gain slider.

Image Adjustment

Brightness: Adjust the image brightness level (0% to 100%).

Contrast: Adjust the image contrast level (0% to 100%).

Saturation: Adjust the image saturation level (0% to 100%).

Sharpness: Adjust the image sharpness level (0% to 100%).

Gamma curve: Adjust the image sharpness level (0.45 to 1, Detailed to Contrast).

- Optimize: The system automatically adjusts the gamma curve.
- Manual: Drag the slider to change the preferred level of Gamma correction towards higher contrast or towards the higher luminance for detailed expression for both dark and lighted areas of an image.

Note	The Gamma curve function is disabled when the WDR feature in Exposure settings is enabled.

Defog

Check to improve the visibility quality of captured image in poor weather conditions such as smog, fog, or smoke.

3D Noise Reduction

Drag the slider to adjust the reduction strength (from low to high).

Note	3D Noise Reduction is mostly applied in low-light conditions. In a low-light condition with fast moving objects, trails of after-images may occur. You may then select a lower strength level.

Note	All changes made to image settings are directly shown on screen. To recall the original settings without incorporating the changes, click **RESTORE**. After you completed the settings, click **SAVE**.

Configuring Exposure Settings

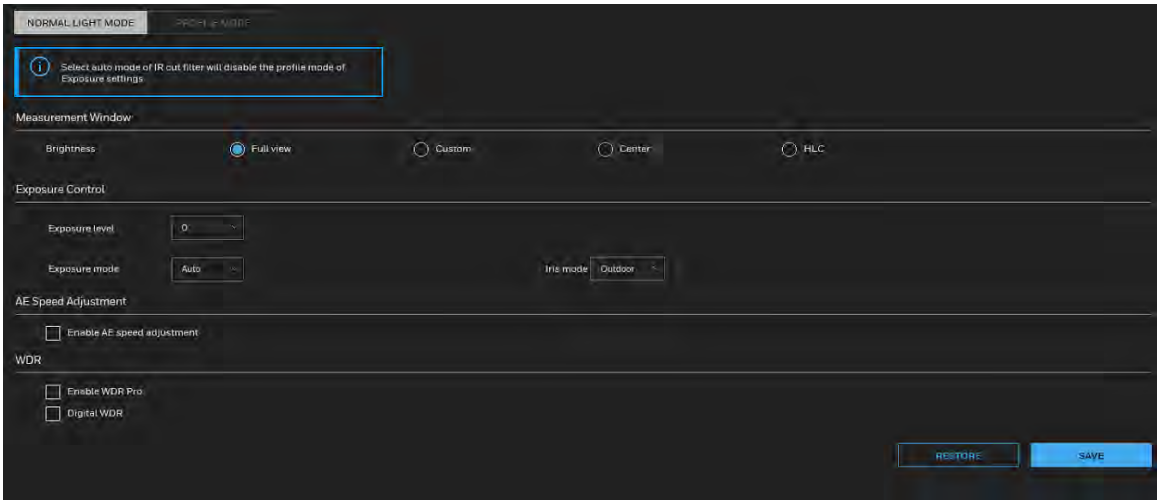
Go to **Setup →Camera Setup → Exposure**.

On this page, you can set the Exposure measurement window, Exposure level, Exposure mode, Exposure time, Gain control, and Day/Night mode settings.

Two sets of exposure settings are available:

- In **Normal Light Mode** tab, configure normal situations for image settings.
- In **Profile Mode** tab, configure special situations for image settings.
  - Night Mode: Check **Enable to apply these settings at** and select this mode to apply the settings at night.
  - Schedule Mode: Check **Enable to apply these settings at** and select this mode to apply the settings at a specific period. Enter the time manually in the field.

Figure 4-9 Exposure



Measurement Window

Measurement Window: This function allows users to set measurement window(s) for low light compensation. For example, where low-light objects are posed against an extremely bright background. You may want to exclude the bright sunlight shining through a building's corridor.

- Full view: Calculate the full range of view and offer appropriate light compensation.
- Custom: Manually add customized windows as inclusive or exclusive regions. A total of 10 windows can be configured.

  The inclusive windows have a higher priority. You can overlap these windows, and, if you place an exclusive window within a larger inclusive window, the exclusive part of the overlapped windows will be deducted from the inclusive window. An exposure value will then be calculated out of the remaining of the inclusive window.
- Center: This option will automatically add an inclusive window in the middle of the window and give the necessary light compensation.

- HLC (Highlight Compensation): Firmware detects strong light sources and compensates on affected spots to enhance the overall image quality. For example, the HLC helps reduce the glares produced by spotlights or headlights.

Exposure Control

Exposure level: You can manually set the exposure level, which ranges from -2.0 to +2.0 (dark to bright) (for IPC model) or from -0.7 to +0.7 (for PTZ model).

Exposure mode: Select an exposure mode (**Auto** or **Manual**) from the dropdown list.

- If you select **Auto**, you can set the Iris mode to **Outdoor** or **Indoor**.
- If you select **Manual**, you can drag the slider of Iris adjustment, Exposure time and Gain Control to get the best image quality.

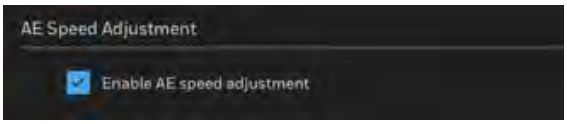
Note	The exposure mode function is not applicable for HC60WZ2E30.

Flickerless: Check to reduce flicker in the image.

AE Speed Adjustment

Check **Enable AE speed adjustment** to apply it in fast changing lighting conditions, such as a highway lane or entrance of a parking area at night where cars passing by with their lights on and it can bring fast changes in light levels. It is also applicable to a situation if the camera is installed on a vehicle, and when it needs to adapt to fast changes of light when entering and leaving a tunnel.

Figure 4-10 AE Speed Adjustment



Note	The AE Speed Adjustment function is not applicable for HC60WZ2E30.

WDR

Figure 4-11 WDR

True WDR: Check to enable the Wide Dynamic Range function which can capture details in a high contrast environment. Use the slide bar to select the strength (from **Low** to **High**), depending on the lighting condition at the installation site. You can select a higher effect when the contrast is high (between the shaded area and the light behind the objects).

Digital WDR: Check to enable the Digital Wide Dynamic Range function. Use the slide bar to select the strength (from **Low** to **High**).

Digital WDR is a software-based technique that enhances the image quality by adjusting the gamma value to brighten dark areas. True WDR is a sensor-based technology. A True WDR CCTV can produce images with an extremely wide dynamic range. The WDR image sensor can capture several images with short and long exposures, then combining them into a single frame.

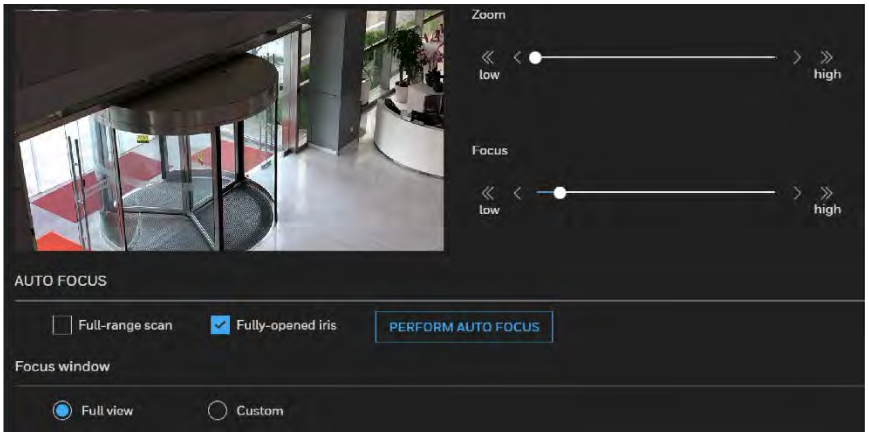
Configuring Focus

Note	The Focus function is not applicable for HC60WZ2E30.

Focus here refers to the Remote Focus, applicable to the cameras that are equipped with a stepping motor lens. The automated focus adjustment function eliminates the needs to physically adjust camera focus. In an outdoor deployment consisting of a large number of cameras, the auto focus function can be very helpful when these cameras become out of focus after days or weeks of operation. And that can easily result from the effects of natural forces, e.g., shrink and expand due to a wide range of operating temperatures and the vibration caused by wind.

Go to **Setup →Camera Setup → Focus**.

Figure 4-12 Focus



- To zoom in on an image, drag the slider to the right.
- To zoom out on an image, drag the slider to the left.
- To fine-tune the zoom, click « ‹ or › ».

Note	If you are not satisfied with the results of zooming, click **PERFORM AUTO FOCUS**. It may take about 15 to 20 seconds (full-range scan unchecked) or 30 to 80 seconds (full-range scan checked) to perform the auto focus scan. You may still need to fine-tune the focus depending on the live image on your screen.

To perform the automated Focus function:

1. Select from the bottom of the screen whether you want to perform focus adjustment on the **Full view** or within a **Custom** focus window. You can create a custom window and click and drag the window to a desired position on screen.
2. It is recommended to **Reset** to the default back focus position of the sensor board.
3. You can check **Fully-opened iris** (default) to increase the iris size for a better focus adjustment result.
4. Check **Fully-opened iris** or **Full-range scan** buttons.

   Full-range scan: Check it and a full-range scan through the camera's entire focal length can take about 30 to 80 seconds. If it is not checked, the auto focus scan will only go through the length where optimal focus may occur, and that takes about 15 to 20 seconds. In theory, best results of the auto scan can be acquired when the camera's iris is fully open.
5. Wait for the scan to complete. After a short while, the clearest image obtained should be displayed and the optimal focus range achieved. Use the arrow marks on the sides to fine-tune the focus if you are not satisfied with the results. You may still need to use the arrow marks to fine-tune the focus depending on the live image on your screen. “>” means moving from wide to tele end; and “<” tele to wide.

Focus window:

By default, the optimal focus is found on a full view window. You may designate a custom window within your current field of view to acquire the best focus out of it. However, you cannot place a focus window on a distant background, e.g., a hall way that stretches away for 3 meters or farther. Doing so you will not benefit from the Focus window function.

- Full view: The focus tuning takes place by referring to the full view.
- Custom: You can create a focus window and drag it to a place of interest in your view window.

Note	It is recommended that this function be used only when you have a solid object in your view window that is showing a consistent color or texture. This function will not take effect if you set the focus window on a distant background.

Configuring Privacy Mask

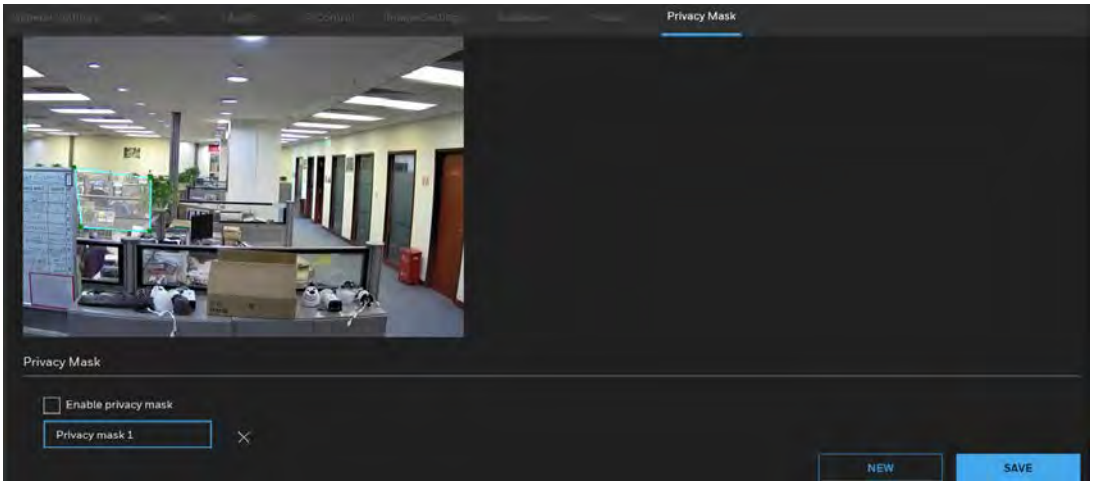
On this page, you can block out sensitive view areas to address privacy concerns.

Go to **Setup →Camera Setup → Privacy Mask**.

To configure privacy masks for Non-PTZ models:

1. Click **NEW** to add a new privacy mask window on the video screen.
2. Use 4 mouse clicks to create a new masking window, which is recommended to be at least twice the size of the object (height and width) you want to cover.
3. Enter a name for the privacy mask and click **SAVE** to enable the setting.
4. Check **Enable privacy mask** to enable this function.

Figure 4-13 Privacy Mask



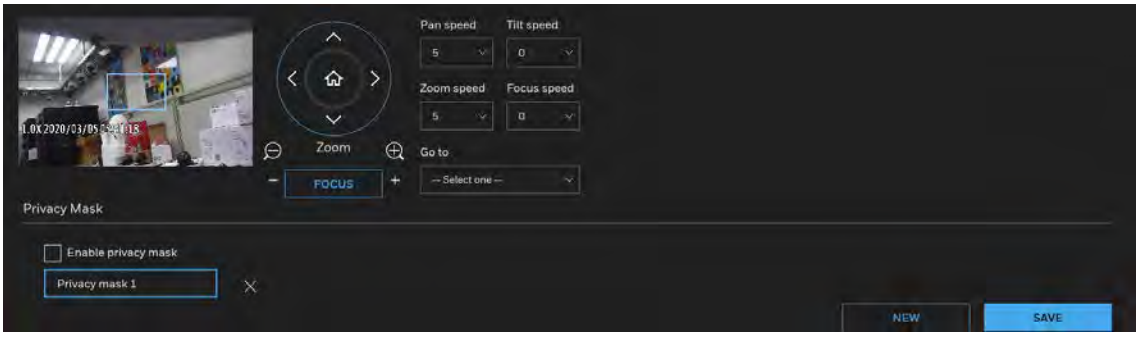
Note	• Up to 5 privacy mask windows can be configured on the same screen. • If you want to delete the privacy mask window, click the 'x' mark on the right side of privacy mask window name.

Configuring Privacy Mask (For HC60WZ2E30)

To configure privacy masks for HC60WZ2E30:

1. Click the Enable privacy mask checkbox to enable this function and click **SAVE**.
2. Click **NEW** to add a privacy mask window on the video screen.
3. Enter a name for the privacy mask window.
4. Use mouse clicks on the screen to move to a place where you want to create a mask. You can also use the PTZ panel to fine-tune the move to the target area. For how to use the PTZ panel, see *PTZ Operations* on page *36*.
5. If preferred, move the field of view to other places to create more privacy masks.

Figure 4-14 Configuring Privacy Mask (HC60WZ2E30)



Note	• The navigation buttons here also support the continuous move. You can click and hold down the button to move across the screen until you release the button. • Up to 24 privacy mask windows can be configured over the camera's hemispheric coverage. • If you want to delete the privacy mask window, click the 'x' mark on the right side of privacy mask window name.

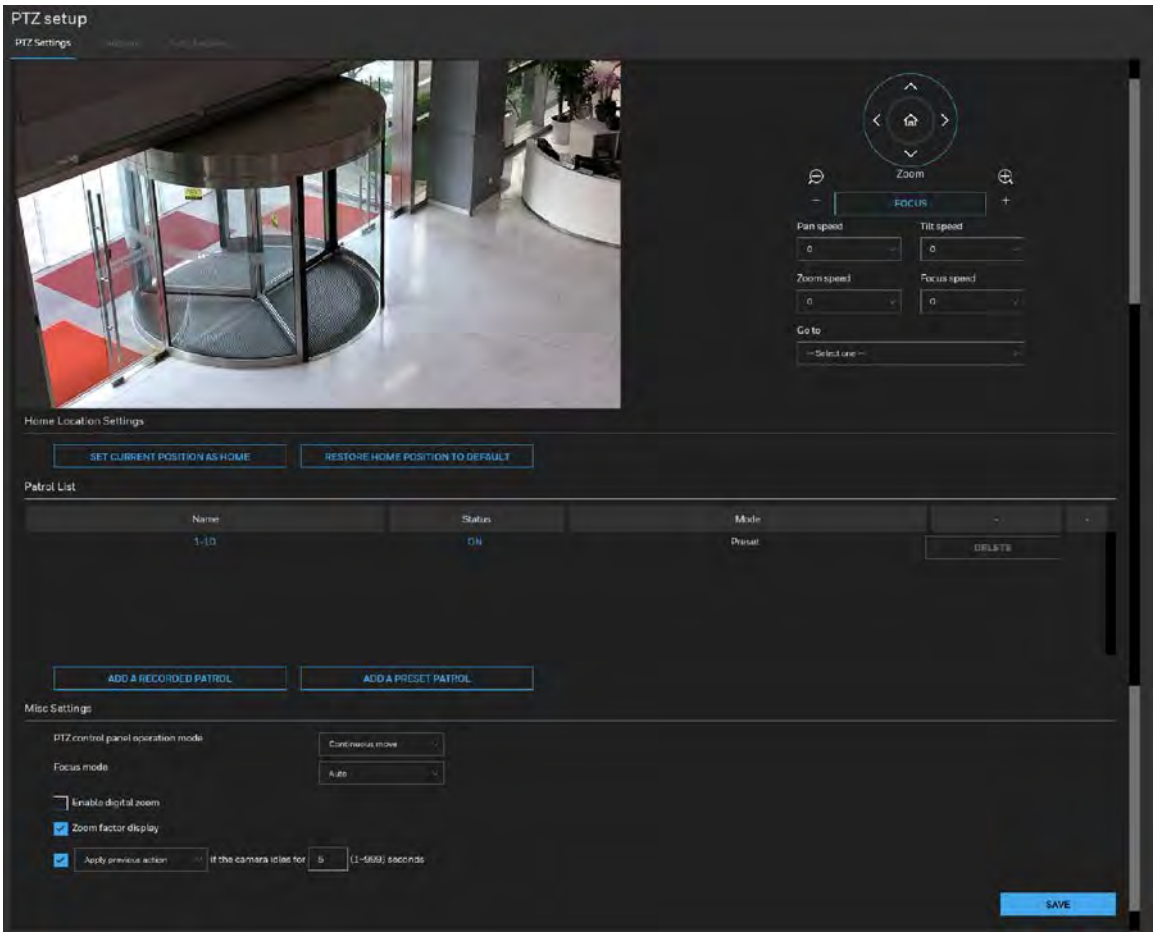
5 Configuring PTZ Settings

This section describes how to control the camera's Pan/Tilt/Zoom operation.

PTZ Settings

Go to **Setup → PTZ Setup →PTZ Settings**.

Figure 5-1 PTZ Setup



PTZ Operations

Move: Click , , , or to move the video image up, down, to the left or to the right. To return to the home location, click .

Zoom: Click  to zoom out the video image, or click  to zoom in the video image.

Pan Speed: Select a speed (-5 to 5) from the dropdown list.

Tilt Speed: Select a speed (-5 to 5) from the dropdown list.

Zoom Speed: Select a speed (-5 to 5) from the dropdown list.

Focus Speed: Select a speed (-5 to 5) from the dropdown list.

Go to: Select a preset location from the drop-down list, and the camera will move to the selected position. You should set a preset location first. See *Preset and Patrol Settings* on page *39*.

Home Location Settings

SET CURRENT POSITION AS HOME: Click to set the current position as the home location.

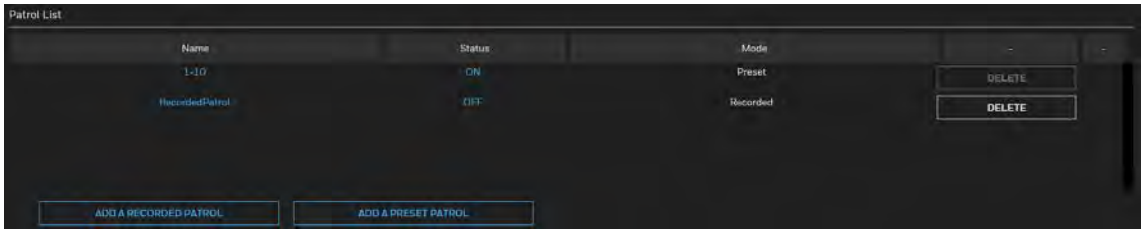
RESTORE HOME POSITION TO DEFAULT: Click to restore the home position to default.

Patrol List

This patrol list displays the configured patrols. Note that only one patrol can be applied at a time. To enable/disable an existing patrol, click **ON/OFF**.

Click **ADD A RECORDED PATROL** or **ADD A PRESET PATROL** below to create a recorded patrol or a preset patrol.

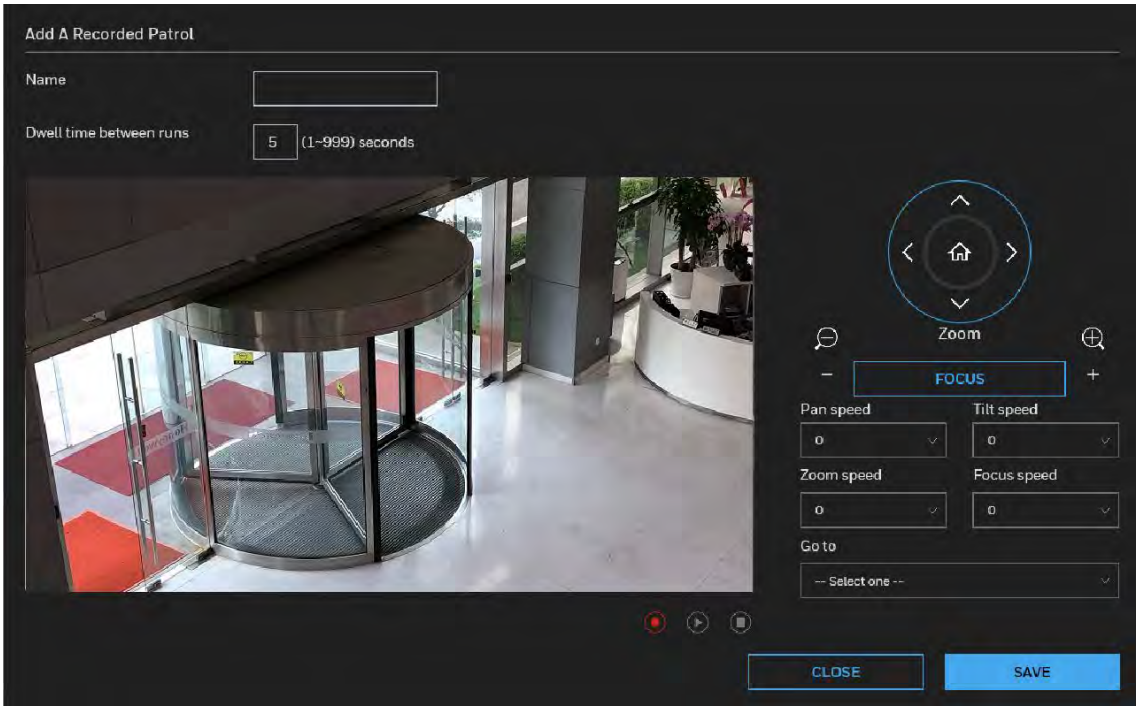
Figure 5-2 Patrol List



Adding A Recorded Patrol

The recorded patrol allows you to record the process moving along interested points (positions) in your surveillance area while the camera memorizes every Pan/Tilt/Zoom/Focus commands you gave in the process. You can then save the process as a recorded patrol. Due to the limitation on system memory, you can configure 4 recorded patrols, each with a length of 2 minutes.

Figure 5-3 Add A Recorded Patrol



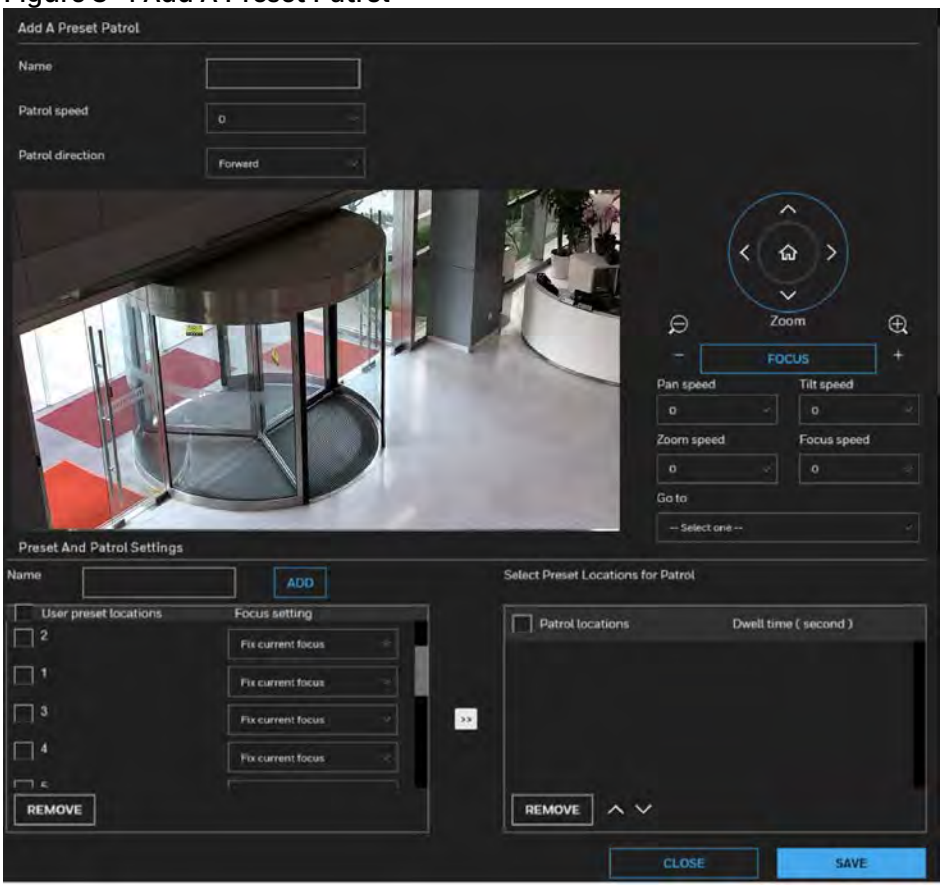
To create a recorded patrol:

1. Enter a name for the patrol.
2. Enter a dwell time between runs.
3. Click on the screen or operate the PTZ panel to select a field of view as your start point.
4. Select the Pan/Tilt/Zoom/Focus speed.
5. Click  to start scanning through your surveillance area by moving along and staying at the points of your interest. Click  again to stop the recording when you visited all of your points of interest. Zoom and focus are also supported.
6. To review your recorded patrol, click  . To stop the review, click  . When you are satisfied with the recording, click **SAVE** and then click **CLOSE** to leave the configuration page. Note that if you start a new recording without saving the previous one, the previous recording will be abandoned.
7. To implement the patrol schedule, click **ON** for the patrol in the patrol list (see *Patrol List* on page *37*), and then click 

on the PTZ panel (see *Figure 3-9*) in the main page.

Adding a Preset Patrol

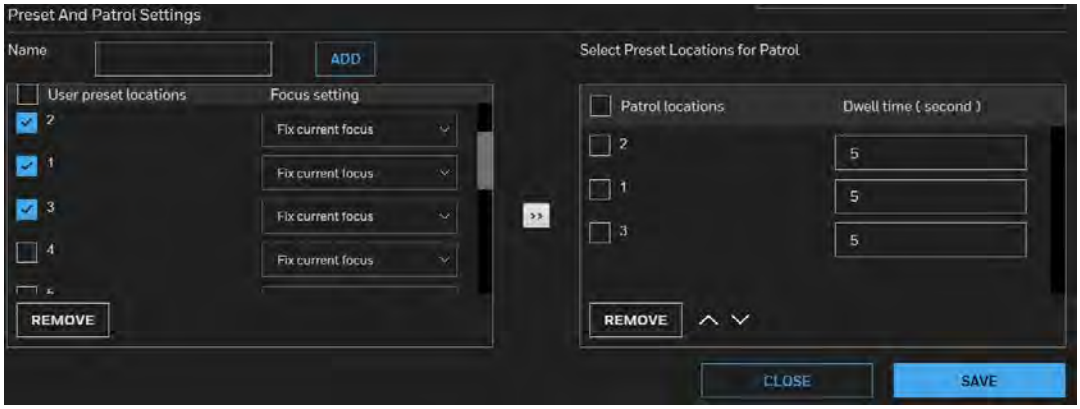
Figure 5-4 Add A Preset Patrol



1. Enter a name for the preset patrol.
2. Select a patrol speed form the dropdown list.
3. Select a patrol direction from the dropdown list.
4. Click on the screen or operate the PTZ panel to adjust the shooting area to the desired position.
5. Select the Pan/Tilt/Zoom/Focus speed.
6. Enter a name for the preset. Click **ADD** and the preset will be listed in the User preset locations list. Repeat the above steps to add more preset locations. To remove a preset, select it and click **REMOVE**.
7. Select the preset locations in the preset locations list, and click 

.
8. The selected preset locations will be displayed in the Patrol locations list. The default dwell time is 5 seconds. Set the Dwelling time for the preset location during an auto patrol.

Figure 5-5 Set a Patrol



9. To delete a preset location from the Patrol locations list on the right pane, select the check box of target patrol locations and click **REMOVE**.
10. To rearrange the patrol order, select a location and click  or  .
11. Select patrol locations you want to use in the list and click **SAVE** to enable the patrol settings.
12. To implement the patrol schedule, click **ON** for the patrol in the patrol list (see *Patrol List* on page *37*), and then click 

on the PTZ panel (see *Figure 3-9*) in the main page.

Misc Settings

Figure 5-6 Misc Settings

PTZ control panel operation mode: This determines how your mouse and PTZ control panel works on a live view window.

- **Continuous move**: It allows your screen control action to continue as long as you click and hold down the left mouse button. For example, if you click on the left button on the PTZ control panel, the camera's view should continuously rotate to the left until you release the button. The same applies to arrow keys, Zoom, and Focus buttons on the PTZ panel.
- **Click to move**: One action taken effect with one click.

Focus mode: Select a focus mode from the dropdown list. Auto, One-time focus, Spotlight avoidance and Manual can be selected.

- **Auto**: Select this mode and the camera will auto focus all the time, except the presets with fixed focus. This mode is applicable to most scenarios.
- **One-time focus**: Select this mode and the camera will auto focus once after the PTZ control is stopped.
- **Spotlight avoidance**: Select this mode and the camera will perform the focus in accordance with the spot light environment at night.
- **Manual**: Select this mode to manually adjust the focus.

Enable digital zoom: Select the checkbox and you will be able to zoom in on an image by up to 360X magnification with the combination of the 30x mechanical zoom and another 12X digital zoom.

Zoom factor display: Select the checkbox to display zoom factor on the video image.

Apply previous action if the camera idles for 5 seconds: From the dropdown list, select an action to be taken when the camera sits idle for a configurable period time. For example, you can let camera resume a patrol tour. The resumed patrol will continue from the last preset position. You may also let the camera return to the home position. The idle state does not include the situations when the camera is performing pan or patrol action.

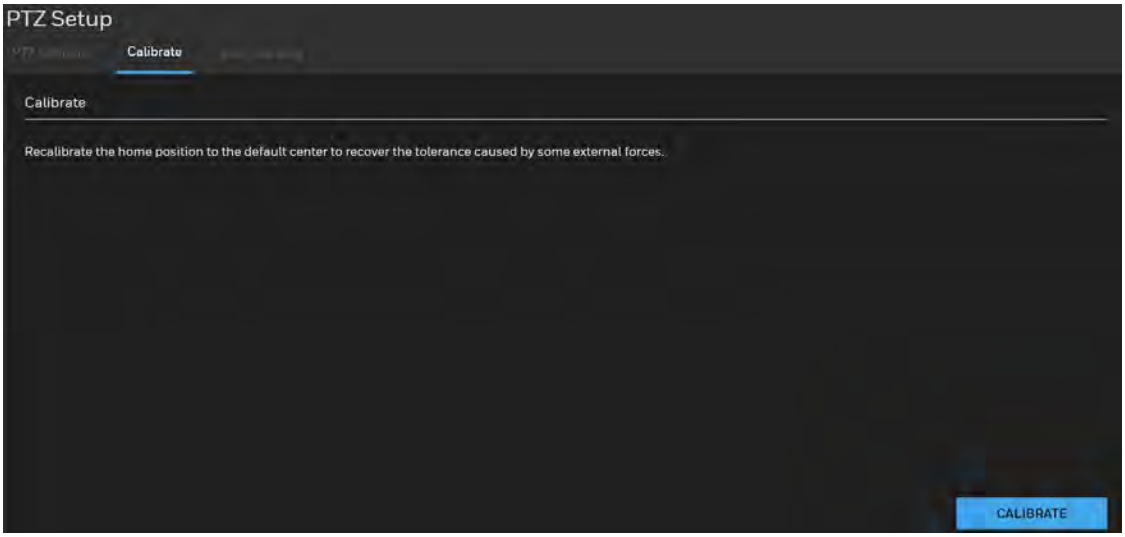
- Enable auto tracking: Select it and the camera will perform auto tracking. It will return home position before auto tracking.
- Return to home position: Select it and the camera will return to home position.
- Start to pan: Select it and the camera will start to pan.
- Start to patrol: Select it and the camera will start to patrol.

Calibrate

Go to **Setup → PTZ Setup → Calibrate**.

This function re-calibrates the home position to the default center to recover any displacement caused by external forces. Please note that there is no confirm message after using the function, and the calibration immediately takes place. If, after a long use, a user finds it is difficult to move camera's field of view to a specific point, use this function to restore the camera's original coordinates in pan and tilt motions.

Figure 5-7 Calibrate

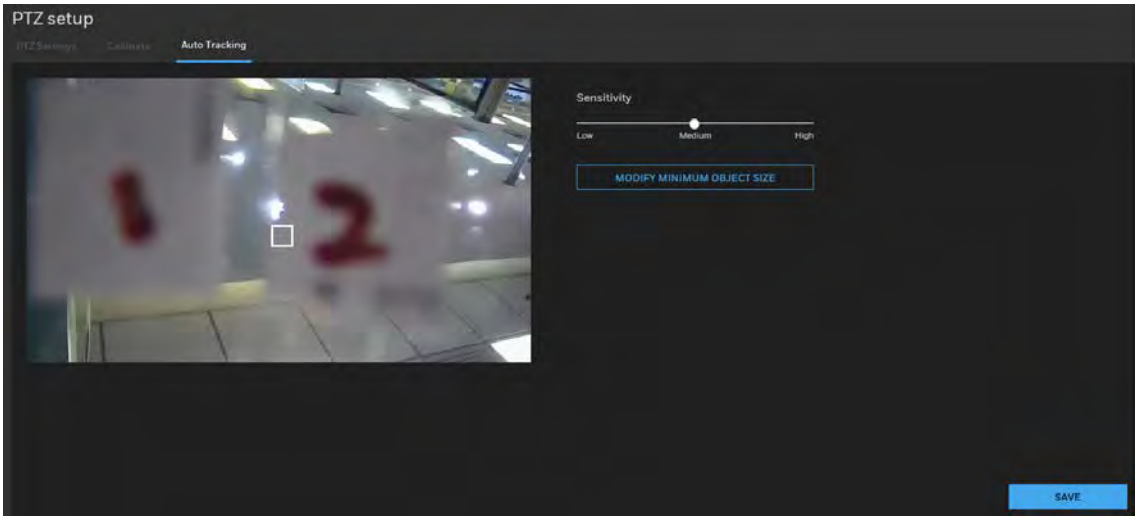


Auto Tracking

You can modify the minimum object size as the triggering factor while performing the Auto Tracking function. You can move the camera view to an area of your interest, estimate, and define the possible size of objects. For example, you can designate the object size such as that of a human trespasser. The silhouette of the tresspasser must be larger than the whole of the object size square box. The minimum object size is 30x30 pixels within a 320x420 view window.

Go to **Setup → PTZ Setup → Auto Tracking**.

Figure 5-8 Auto Tracking



Sensitivity: Drag the slider bar horizontally to adjust the sensitivity of the tracking function.

Modify minimum object size: Click it and the grey rectangle on the video will be turn white. You can drag the rectangle and move it to the target place. You can also resize the rectangle by adjusting the width and length.

After all settings are completed, click **SAVE**.

On the PTZ panel of live view, click 

on the PTZ panel (see *Figure 3-9*) in the main page. If there is an intruder, the camera will follow and track the intruder. To stop the auto tracking, click any buttons on the PTZ panel, or a mouse click takes place on a view window.

You can choose to perform other functions, such as pan or patrol, simply by clicking their buttons on the PTZ panel while the camera is performing the auto tracking function.

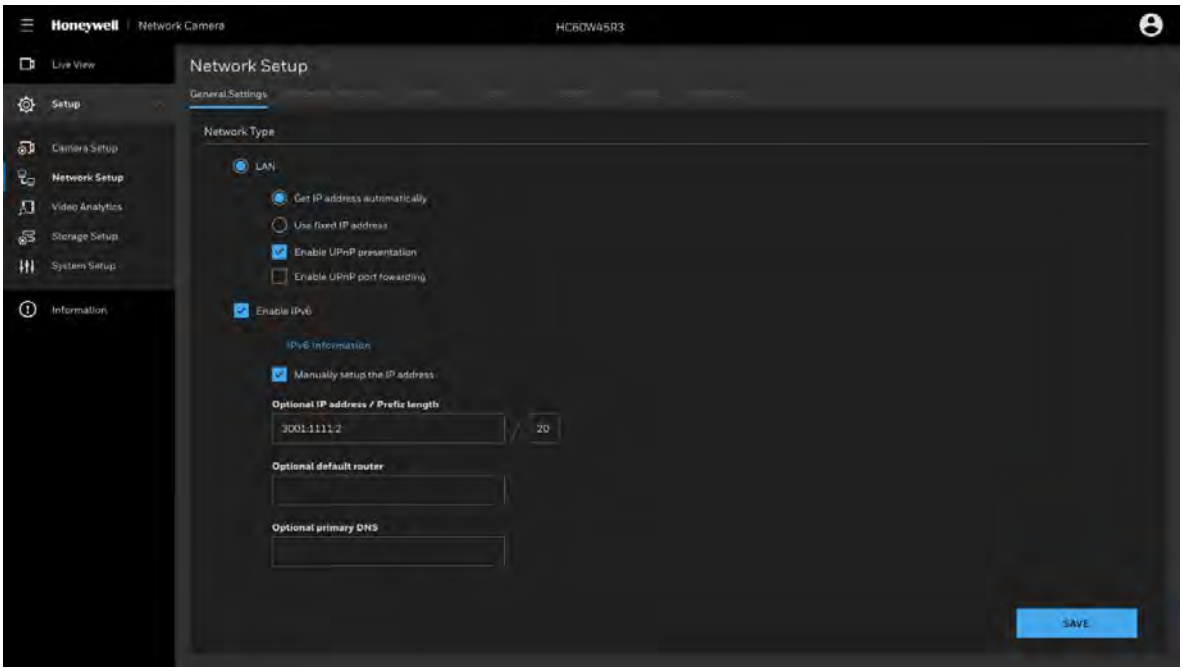
6 Configuring Network Settings

This chapter contains the following sections:

Configuring Network General Settings

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

Figure 6-1 Network Type



LAN

Get IP address automatically: Select this option to obtain an available dynamic IP address assigned by the DHCP server each time the camera is connected to the LAN.

Use fixed IP address: Select this option to manually assign a static IP address to the camera.

- IP address:

1. You can make use of Unified Tool in the software CD to easily set up the camera on LAN. See *Accessing the Camera* on page *3*.
2. Enter the Static IP, Subnet mask, Default router, and Primary DNS provided by your ISP or network administrator.

- Subnet mask: This is used to determine if the destination is in the same subnet. The default value is “255.255.255.0”.
- Default router: This is the gateway used to forward frames to destinations in a different subnet. Invalid router setting will disable the transmission to destinations across different subnets.
- Primary DNS: The primary domain name server that translates hostnames into IP addresses.
- Secondary DNS: Secondary domain name server that backups the Primary DNS.
- Primary WINS server: The primary WINS server that maintains the database of computer names and IP addresses.
- Secondary WINS server: The secondary WINS server that maintains the database of computer names and IP addresses.

Enable UPnP presentation: Select this option to enable UPnP presentation for your camera so that whenever a camera is presented to the LAN, the shortcuts to connected cameras will be listed in Network and Sharing Center. You can click the shortcut to link to the web browser.

Note	To utilize this feature, make sure the UPnP component is installed on your computer.

Enable UPnP port forwarding: To access the camera from the Internet, select this option to allow the camera to open ports automatically on the router so that video streams can be sent out from a LAN. To utilize of this feature, make sure that your router supports UPnP and it is activated.

Enabling UPnP in Windows

The UPnP protocol is used to detect network devices with clients running Windows.

The camera can be detected by Windows' built-in network browser.

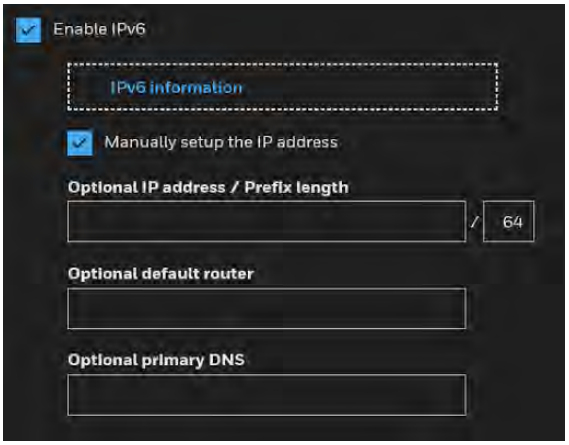
To enable UPnP in Windows 10:

1. Go to **Start→ Control Panel→ Network and Sharing Center**.
2. On the left pane, click **Change advanced sharing settings**.
3. On your current network profile, in the **Network discovery** area, click **Turn on network discovery**, and then click **Save changes**.

Enable IPv6

Select this option and click **SAVE** to enable IPv6 settings.

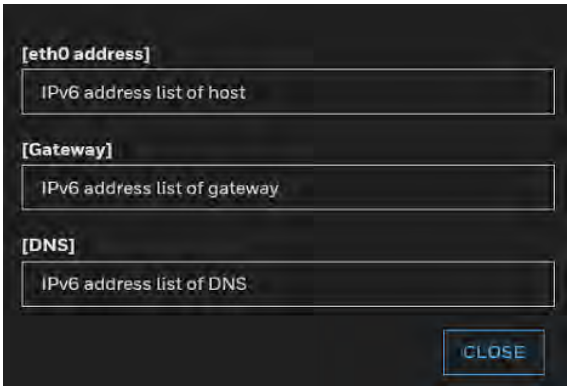
Figure 6-2 Enable IPv6



When IPv6 is enabled, by default, the network camera will listen to router advertisements and be assigned with a link-local IPv6 address accordingly.

IPv6 Information: Click to obtain the IPv6 information as shown below.

Figure 6-3 IPv6 Information



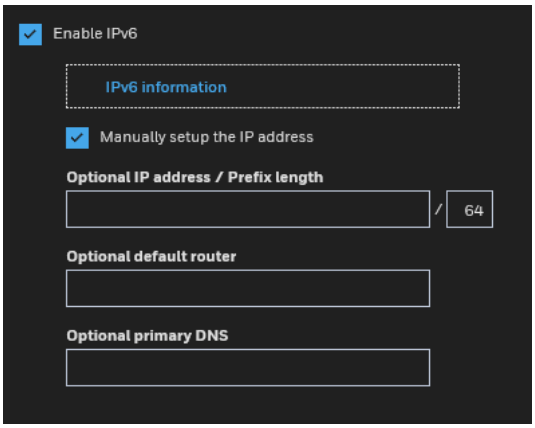
If your IPv6 settings are successful, the IPv6 address list will be listed in the pop-up window.

Follow the steps below to link to an IPv6 address:

1. Open your web browser.
2. Enter the link-global or link-local IPv6 address in the address bar of your web browser.
3. The format should be: http://[2001:0c08:2500:0002:0202:d1ff:fe04:65f4]/
4. Press **Enter** on the keyboard or click **Refresh** button to refresh the webpage.

Manually setup the IP address: Select this option to manually set up IPv6 settings if your network environment does not have DHCPv6 server and router advertisements-enabled routers. If you check this item, the following blanks will be displayed for you to enter the corresponding information:

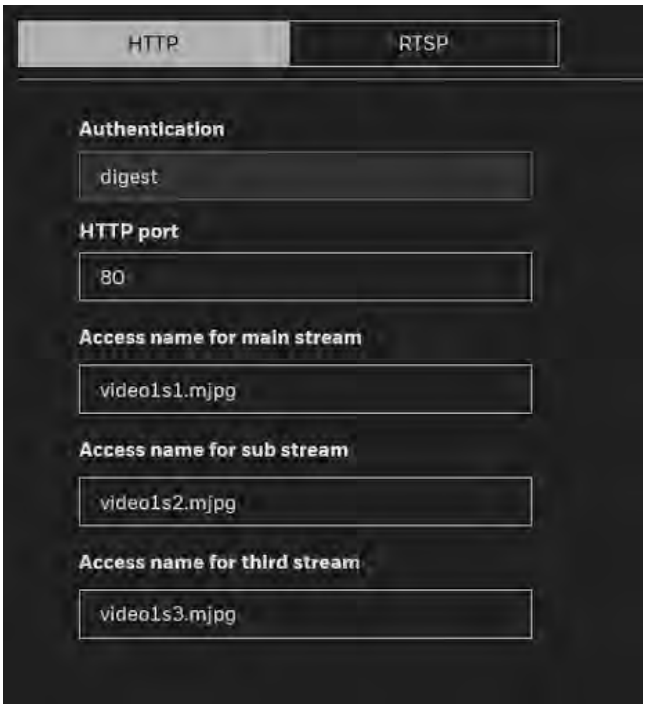
Figure 6-4 Manually setup IP Address



Configuring Streaming Protocols

Go to **Setup→Network Setup→Streaming Protocols**.

Figure 6-5 Streaming Protocols - HTTP



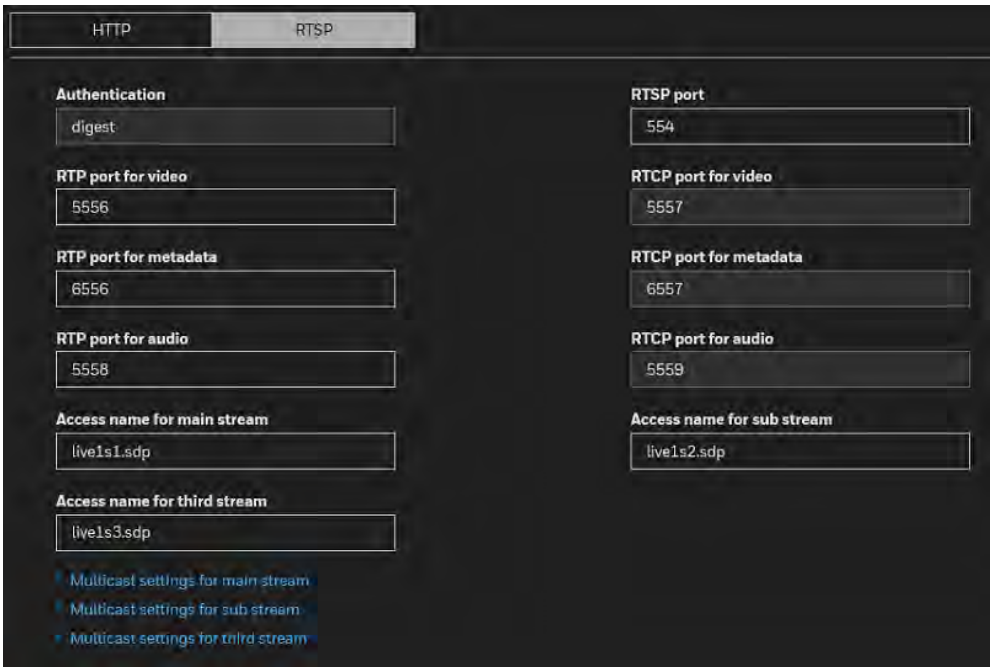
To utilize HTTP authentication, make sure that you have set a password for the camera first. For more information, see *Configuring User Accounts Settings* on page *82*.

Authentication (digest): User credentials are encrypted with MD5 algorithm which provide better protection against unauthorized accesses.

HTTP port: By default, the HTTP port is set to 80. It can also be assigned to another port number between 1025 and 65535.

Access name for main stream/sub stream/third stream: The camera supports multiple streams simultaneously. The access name is used to identify different video streams. You can set up the video quality of linked streams. For more information, see *Video Stream* on page *22*.

Figure 6-6 Streaming Protocols – RTSP



To utilize RTSP streaming authentication, make sure that you have set a password for controlling the access to video stream first. For more information, see *Configuring User Accounts Settings* on page *82*.

Authentication (digest): User credentials are encrypted with MD5 algorithm which provides better protection against unauthorized access.

Access name for main stream/sub stream/third stream: The camera supports multiple streams simultaneously. The access name is used to differentiate the streaming source.

If you want to use an RTSP player to access the camera, you have to set the video mode to H.264 or H.265 and use the following RTSP URL command to request transmission of the streaming data.

rtsp://<ip address>:<rtsp port>/<access name for stream 1 to 3>

For example, when the access name for stream 1 is set to live.sdp:

1. Launch an RTSP player.
2. Choose **File → Open URL**. A URL dialog box will pop up.
3. Type the above URL command in the text box.
4. The live video will be displayed in your player.

RTSP port /RTP port for video / RTCP port for video:

- RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default, the RTSP port number is set to 554.
- The RTP (Real-time Transport Protocol) is used to deliver video data to the clients. By default, the RTP port for video is set to 5556.

- The RTCP (Real-time Transport Control Protocol) allows the camera to transmit the data by monitoring the Internet traffic volume. By default, the RTCP port for video is set to 5557.

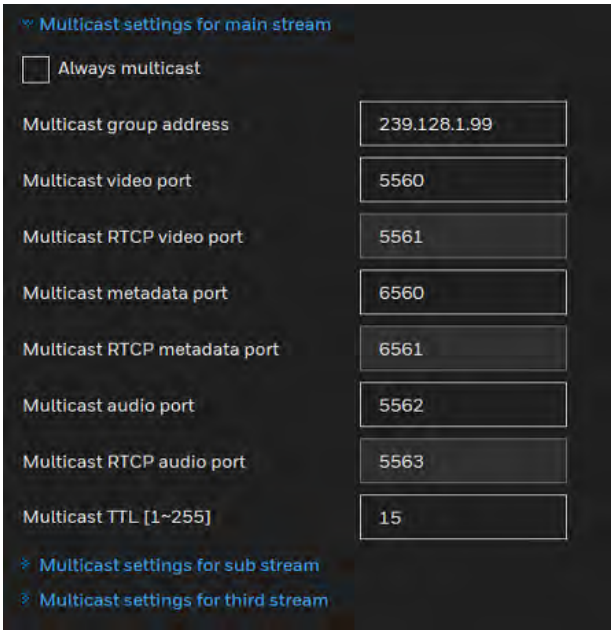
The ports can be changed to values between 1025 and 65535. The RTP port must be an even number and the RTCP port is the RTP port number plus one, and thus is always an odd number. When the RTP port changes, the RTCP port will change accordingly.

RTP port for metadata: By default, the RTP port for metadata is set to 6556.

RTCP port for metadata: By default, the RTCP port for video is set to 6557.

Multicast settings for streams: Click to display the detailed configuration information.

Figure 6-7 Multicast Settings



Always multicast: Check to enable multicast for video streams.

Multicast group address: Enter the Multicast group address.

Multicast video port/Multicast RTCP video port: The ports can be changed to values between 1025 and 65535. The multicast video port must be an even number and the multicast RTCP video port number is the multicast video port number plus one, and thus is always odd. When the multicast video port changes, the multicast RTCP video port will change accordingly.

Multicast metadata port/Multicast RTCP metadata port: The ports can be changed to values between 1025 and 65535. The multicast metadata port must be an even number and the multicast RTCP metadata port number is the multicast metadata port number plus one, and thus is always odd. When the multicast metadata port changes, the multicast RTCP metadata port will change accordingly.

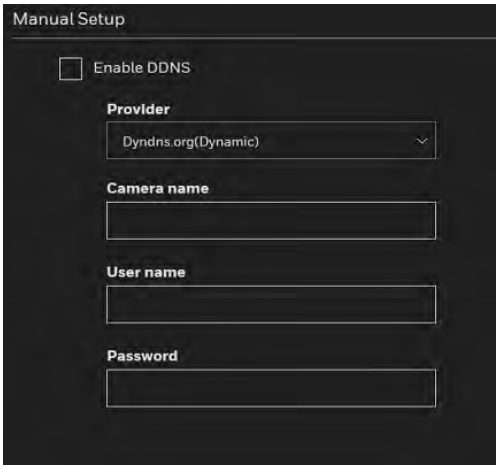
Multicast TTL [1~255]: The multicast TTL (Time To Live) is the value that tells the router the range a packet can be forwarded. The default value is **15**.

Configuring DDNS Settings

Go to **Setup→Network Setup→DDNS**.

This section describes how to configure the dynamic domain name service for the camera. DDNS is a service that allows your camera, especially when assigned with a dynamic IP address, to have a fixed host and domain name.

Figure 6-8 DDNS



Enable DDNS: Check to enable the DDNS setting.

Note	Before utilizing this function, apply for a dynamic domain account first and then access the system through that domain. Refer to the following link to apply for a dynamic domain account: http://www.dyndns.com/

Provider: Select a DDNS provider from the dropdown list.

Camera name: Enter the camera name of your dynamic domain account.

User name: Enter the user name of your dynamic domain account.

Password: Enter the password of your dynamic domain account.

Configuring QoS Settings

Go to **Setup →Network Setup →Qos**.

Quality of Service (QoS) is a network security mechanism. It fixes problems with network delays and jams. For network service, the quality of service includes the transmission bandwidth, delay, and packet loss, for example. Through QoS, you can guarantee the transmission bandwidth, reduce the delay, reduce the loss of data packets, and enhance the transmission quality with packet prioritization.

To utilize QoS in a network environment, the following requirements must be met:

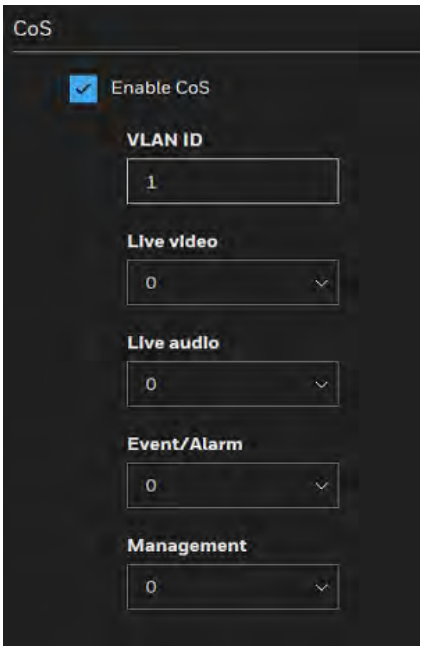
- All network switches and routers in the network must include support for QoS.

- The network video devices used in the network must be QoS-enabled.

CoS

CoS refers to Class of Service. It indicates the frame priority level from 0 (lowest) to 7 (highest). The priority is set up on the network switches, which then use different queuing disciplines to forward the packets.

Figure 6-9 Cos



Enter the **VLAN ID** of your switch (0~4095) and choose the priority for each application (0~7).

If you assign Video the highest level, the switch will handle video packets first.

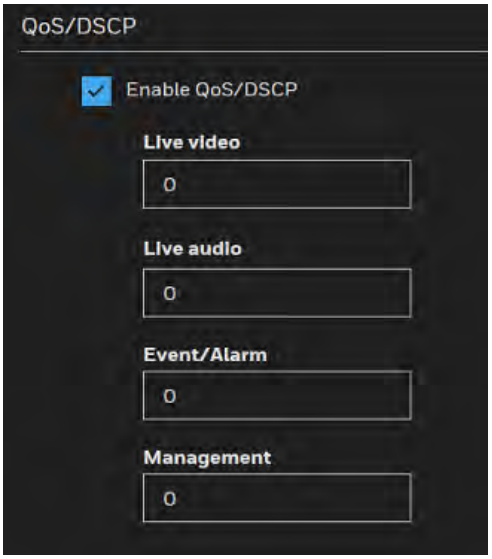
Note

- A VLAN Switch (802.1p) is required. Web browsing may fail if the CoS setting is incorrect.
- The Class of Service technologies do not guarantee a level of service in terms of bandwidth and delivery time; they offer a "best-effort." Users can think of CoS as "coarsely-grained" traffic control and QoS as "finely-grained" traffic control.
- Although CoS is simple to manage, it lacks scalability and does not offer end-to-end guarantees since it is based on L2 protocol.

QoS/DSCP

Routers at each network node classify packets according to their DSCP ((Differentiated Services Codepoint) value and give them a particular forwarding treatment; for example, how much bandwidth to reserve for it.

Figure 6-10 QoS/DSCP



Specify the DSCP value for each application (0~63).

Configuring SNMP Settings

Go to **Setup →Network Setup → SNMP**.

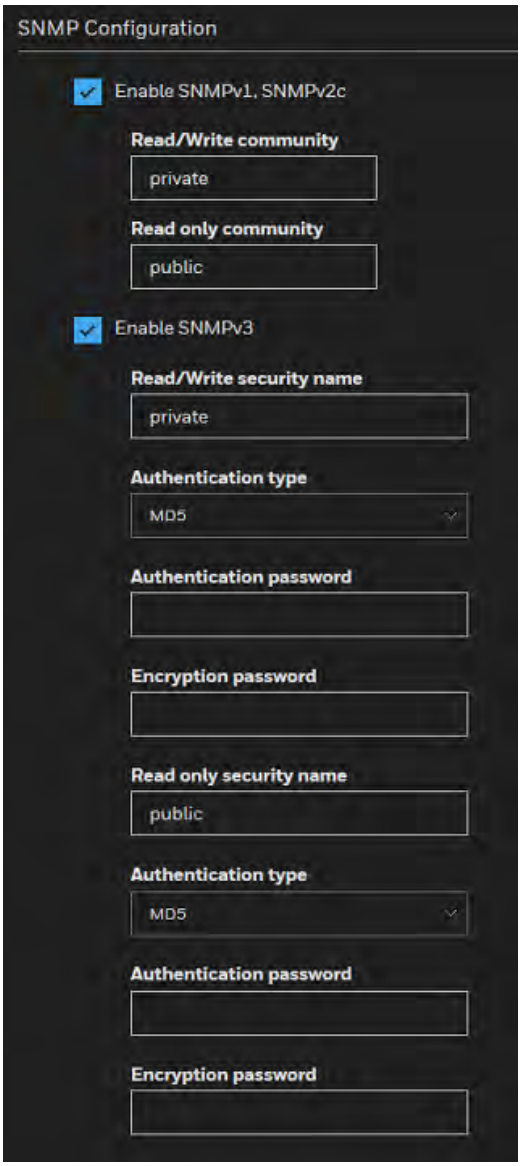
SNMP (Simple Network Management Protocol) is a protocol for collecting, organizing, and exchanging management information between managed devices on a network.

The SNMP consists of the following three key components:

- Manager: Network-management station (NMS), a server which executes applications that monitor and control managed devices.
- Agent: A network-management software module on a managed device which transfers the status of managed devices to the NMS.
- Managed device: A network node on a managed network. For example: routers, switches, bridges, hubs, computer hosts, printers, IP telephones, network cameras, web server, and database.

Before configuring SNMP settings on the page, enable your NMS first.

Figure 6-11 SNMP Configurations



Enable SNMPv1, SNMPv2c: Check to enable SNMPv1, SNMPv2c.

Enter the names of Read/Write community and Read Only community according to your NMS settings.

Enable SNMPv3: Check to enable SNMPv3 which contains cryptographic security, a higher security level.

- Security name: Choose Read/Write or Read Only and enter the community name according to your NMS settings.
- Authentication type: Select MD5 or SHA as the authentication method.
- Authentication password: Enter the password for authentication (at least 8 characters).
- Encryption password: Enter a password for encryption (at least 8 characters).

Configuring HTTPS Settings

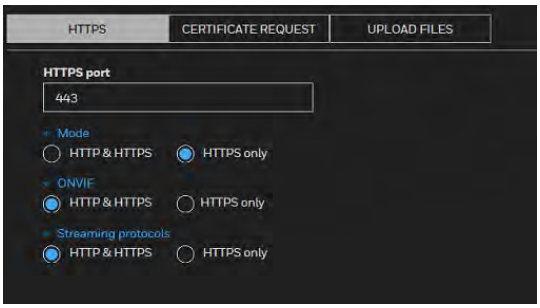
Go to **Setup →Network Setup → HTTPS**.

HTTPS

Go to **Setup →Network Setup → HTTPS→ HTTPS**.

This section explains how to enable authentication and encrypted communication. It helps protect streaming data transmission over the Internet on higher security level.

Figure 6-12 HTTP



HTTP & HTTPS: Select it and the web browser can be accessed via HTTP or HTTPS.

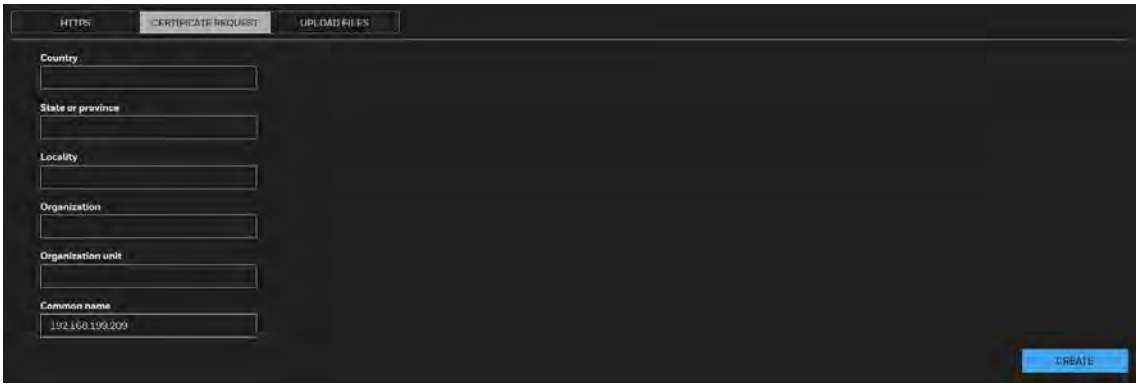
HTTPS only: Select it and the web browser can only be accessed via HTTPS with higher security level. This option is selected by default.

Certificate Request

Go to **Setup →Network Setup → HTTPS→ Certificate Request**.

You can fill in certificate information and the certificate request file can be exported to the certificate issuing authority for signing and then being imported to camera.

Figure 6-13 Certificate Request



Enter the information of Country, State or province, Locality, Organization and Organization unit. Click **CREATE**.

Click **EXPORT** to export the certificate request to your local computer. After you get the signing certificate from the certificate issuing authority, click **CHOOSE FILE** and **UPLOAD** to import it to the camera. The imported certificate will replace the original self-signed certificate of the camera.

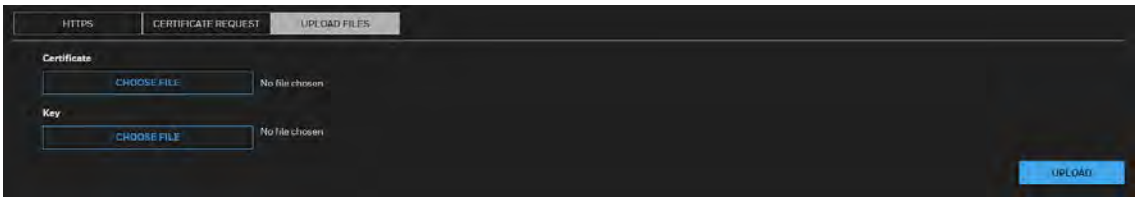
After the certificate file is uploaded successfully, if you want to remove the certificate, click **REMOVE**.

Upload files

Go to **Setup →Network Setup → HTTPS→ Upload files**.

You can import the certificate from third party here.

Figure 6-14 Upload files



To import the certificate from third party:

1. In the **Certificate** field, click **CHOOSE FILE** to select a certificate file you have already applied from 3rd party or CA domain.
2. In the **Key** field, click **CHOOSE FILE** to select a certificate key you have already applied from 3rd party or CA domain.
3. Click **UPLOAD** and reboot camera.

After the certificate file is uploaded successfully, if you want to remove the certificate, click **REMOVE**.

Note

- Supported certificate type: HTTPS protocol.
- Supported certificate file format: *.cert format.
- Supported Key format: PEM format.

Configuring IEEE 802.1X Settings

Go to **Setup →Network Setup →802.1X**.

IEEE802.1X is the access control and authentication protocol for local and metropolitan area networks. It uses a port-based network access control protocol to restrict unauthorized user and/or device access to the LAN. The network devices, intermediary switch/access point/hub, and RADIUS server must support and enable 802.1x settings.

To configure IEEE 802.1x settings:

1. Before connecting the camera to the protected network with 802.1x, apply a digital certificate from a Certificate Authority (i.e., your network administrator) which can be validated by a RADIUS server.
2. Connect the camera to a PC or notebook outside of the protected LAN. Open the configuration page of the camera as shown below.

Figure 6-15 IEEE 802.1X Configurations – EAP-PEAP

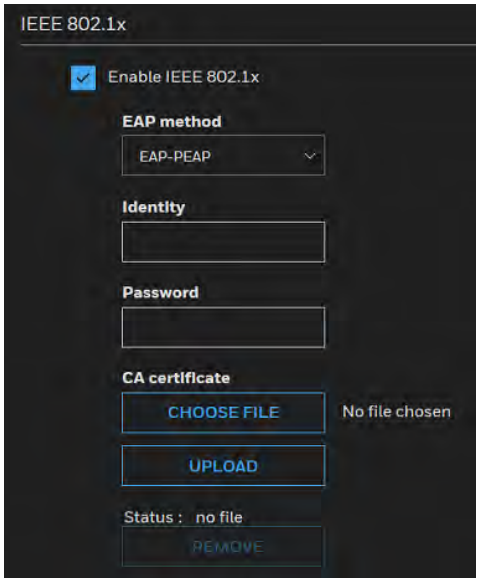
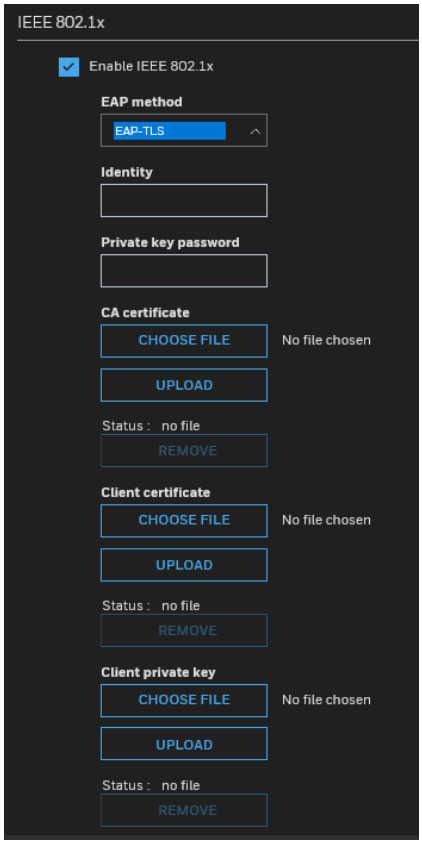


Figure 6-16 IEEE 802.1X Configurations – EAP-TLS



Select **EAP-PEAP** or **EAP-TLS** as the EAP method. Enter your ID and password issued by the CA, and then upload related certificate(s).

3. When all settings are complete, move the camera to the protected LAN by connecting it to an 802.1x enabled switch. The devices will then start the authentication automatically.

7 Configuring Video Analytics

This chapter contains the following sections:

Configuring Motion Detection Settings

Go to **Setup →Video Analytics → Motion Detection**.

Two sets of motion detection settings are available:

- In **Normal Light Mode** tab, configure normal situations for motion detection settings.
- In **Profile Mode** tab, configure special situations for motion detection settings.
  - Night Mode: Check **Enable to apply these settings at** and select this mode to apply the settings at night.
  - Schedule Mode: Check **Enable to apply these settings at** and select this mode to apply the settings at a specific period. Enter the time manually in the field.

Motion Detection

The Motion Detection detects motions in customized windows. If a motion is detected, the frame of the customized window will become flashing red.

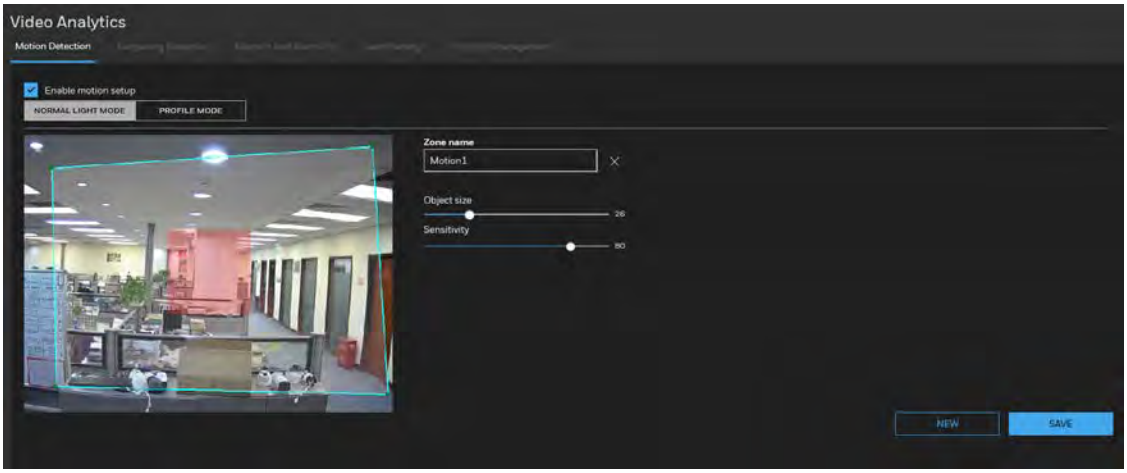
To enable motion detection:

1. Click **NEW** to add a new motion detection window.
2. In the Window Name text box, enter a name for the motion detection window.
   a. Draw a detection area by clicking four corner points on the target area. You can change the shape of the detection area by dragging the corner points.
   b. Drag the object size slider to change the minimum size of item to trigger an alarm. An object size box will appear in the center of screen for your reference (in semi-transparent red). An intruding object must be larger than the Object size to trigger an alarm. Change the object size according to the live view.
   c. To delete a window, click  on the right of the window name.
3. Define the sensitivity to moving objects by moving the Sensitivity slider. A high sensitivity is prone to produce false alarms such as the fast changes of light (such as day/night

mode switch, turning lights on/off). A movement must persist longer than 0.3 second for the motion to be detected.

4. Click **SAVE** to enable the settings.
5. Select **Enable motion detection** to enable this function.

Figure 7-1 Configuring Motion Detection Settings



Configuring Tampering Detection Settings

Go to **Setup →Video Analytics → Tampering Detection**.

This section explains how to configure camera tamper detection settings. With tamper detection, the camera is capable of detecting incidents such as **redirection**, **blocking or defocusing**, or even **spray paint**.

Figure 7-2 Tampering Detection Configurations

Tampering detection: Check to enable tampering detection.

Image too dark detection: Check to enable image too dark detection. Too dark can be a cover on the camera or a spraying paint on the camera.

Image too bright detection: Check to enable image too bright detection. Too bright can be a flash light shining to the camera.

Image too blurry detection: Check to enable image too blurry detection. To blurry can be the result of strong interference on the camera, such as EMI interference.

Trigger duration: It specifies a set of time before the tampering is considered as a real alarm. This helps avoid false alarms by short-lived changes.

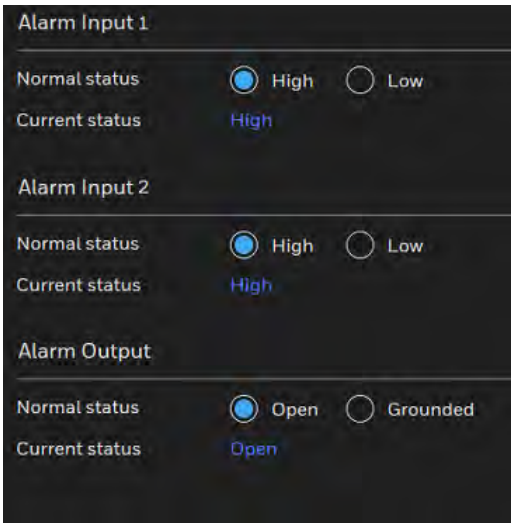
Trigger threshold: It determines how sensitive the tamper detection setting is. The lower the threshold value, the easier the detection is triggered.

You can configure Tampering Detection as a trigger element to the proactive event configurations in **Video Analytics → Event settings → Trigger.** For example, when the camera is tampered with, camera can be configured to send the pre- and post-event video clips to a networked storage device. For more information, see *Trigger* on page *61*.

Configuring Alarm In and Alarm Out

Go to **Setup →Video Analytics → Alarm In and Alarm Out.**

Figure 7-3 Alarm In and Alarm Out



Alarm in: Select High or Low to define normal status for the alarm input. Connect an alarm input from a sensor device to the camera, the camera will report the current signal status. You may then configure the Normal status (non-trigger status) as High or Low.

Alarm out: Select High or Low to define normal status for the alarm output. Connect an output line to an external device, the camera will report the current signal status. You may then configure the Normal status (non-trigger status) as High or Low.

Set up the event source as Alarm In on **Event Settings → Trigger**. For detailed information, see *Trigger* on page *61*.

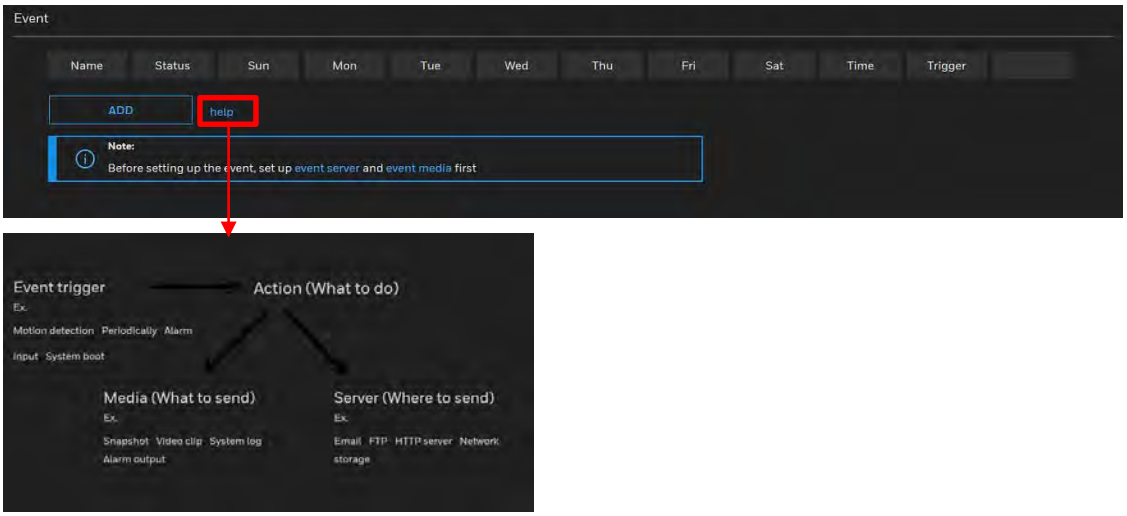
Configuring Event Settings

Go to **Setup →Video Analytics → Event Settings**.

This section describes how to configure the camera to respond to particular situations (event). A typical application is that when a motion is detected, the camera sends buffered images to an e-mail address as notifications. Click **Help**, there is an illustration shown in the pop-up window explaining that an event can be triggered by many sources, such as motion

detection or external alarm input devices. When an event is triggered, you can specify what type of action that will be performed. You can configure the camera to send snapshots or videos to your email address.

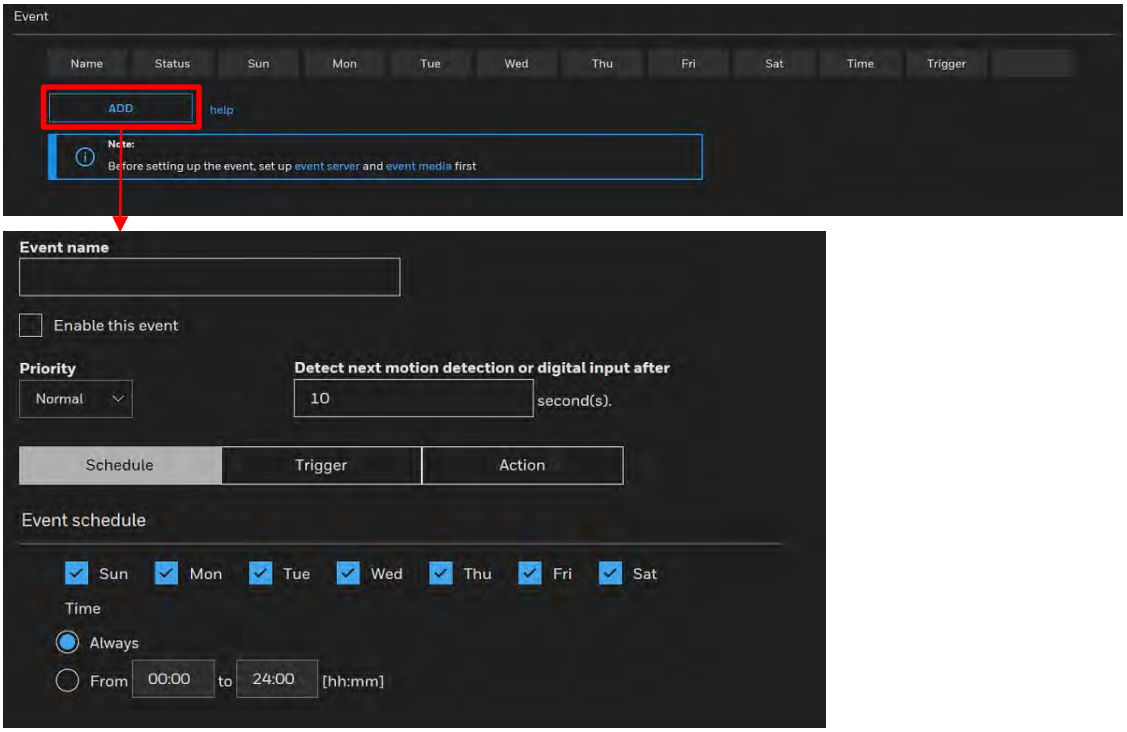
Figure 7-4 Event Settings



Event

In the **Event** tab, click **ADD** to open the event settings window. Here you can arrange three elements -- Schedule, Trigger, and Action to set an event. A total of 3 event settings can be configured.

Figure 7-5 Event



- **Event name**: Enter a name for the event setting.
- **Enable this event**: Check to enable the event setting.
- **Priority**: Select the relative importance of this event (**High**, **Normal**, or **Low**). Events with a higher priority setting will be executed first.
- **Detect next motion detection or digital input after x seconds**: Enter the duration in seconds to pause motion detection after a motion is detected. This can prevent event-related actions to take place too frequently.

Schedule

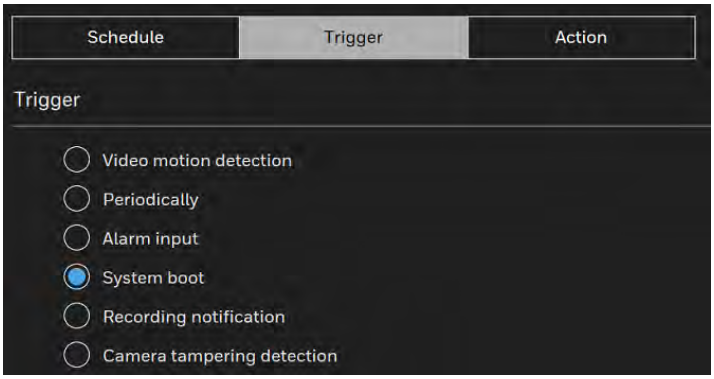
Specify the period of time during which the event trigger will take effect. Select the days of a week and the time in a day (in 24-hr time format) for the event triggering schedule. For example, you may prefer an event to be triggered only during the off-office hours.

Trigger

This is the cause or stimulus which defines when to trigger the camera.

There are several choices of trigger sources as shown below:

Figure 7-6 Trigger Sources



Video motion detection

This option makes use of the built-in motion detection mechanism as a trigger source. To enable this function, you need to configure a Motion Detection Window first. For more information, see *Configuring Motion Detection Settings* on page *57*.

Periodically

This option allows the camera to trigger periodically for every other defined minute. Up to 999 minutes can be set.

Alarm input

This option allows the Network Camera to use an external digital input device or sensor as a trigger source. Depending on your application, there are many choices of digital input devices on the market which helps to detect changes in temperature, vibration, sound, and light, etc.

System boot

This option triggers the camera when the power to the camera is disconnected and re-connected.

Recording notification

This option allows the camera to trigger when the recording disk is full or when recording starts to overwrite older data.

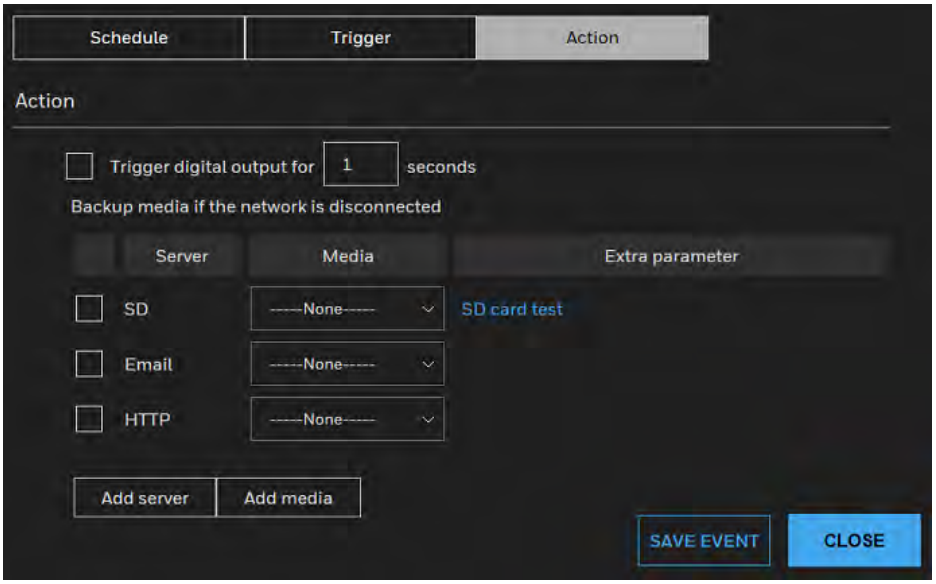
Camera tampering detection

This option allows the camera to trigger when the camera detects that is being tampered with. To enable this function, you need to configure the Tampering Detection option first, see *Configuring Tampering Detection Settings* on page *58*.

Action

It defines the actions to be performed by the camera when a trigger is activated.

Figure 7-7 Action



Trigger digital input for x seconds: Select this option to trigger alarm output for x seconds. Enter a value in the textbox.

Backup media if the network is disconnected:

Select this option to backup media files to SD card if the network is disconnected. This function will apply after you configure the Email and HTTP. For example, if a snapshot is supposed to be delivered to an Email receiver, in the event of network failure, the snapshot will be saved in the SD card.

Trigger auto tracking: Select this option to trigger auto tracking. This function is applicable to HC60WZ2E30.

Move to preset location: Select this option to trigger the camera to preset location. Select a preset location from the dropdown list. You should configure preset locations first, see *Adding a Preset Patrol* on page *39*. This function is applicable to HC60WZ2E30.

SD Test: Click to test your SD card. The system will display a message indicating the result as a success or a failure. If you want to use your SD card for local storage, format it before use. For more information, see *SD Card Format* on page *70* .

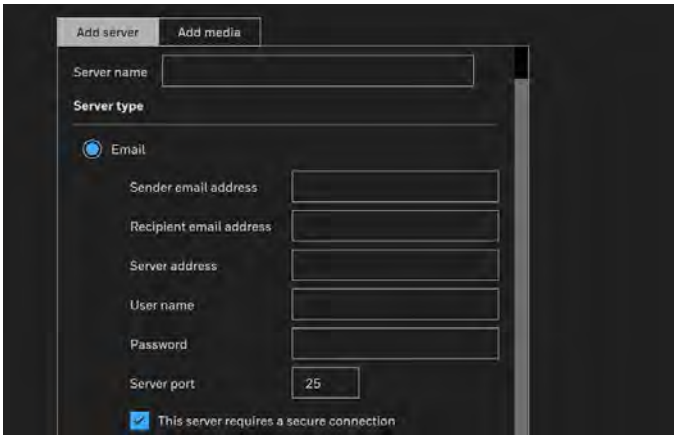
Add Server

Note	Before adding server or adding media, click **SAVE EVENT** to avoid that the event will be lost when adding server or adding media.

Click **Add server** to open the server setting window. You can specify where the notification messages are sent to when a trigger is activated. A total of 5 server settings can be configured.

There are the following server types available: Email and HTTP. Select the item to display the detailed configuration options. You can configure either one or all of them.

Figure 7-8 Add Server



Server type - Email

Select to send the media files via email when a trigger is activated.

- Server name: Enter a name for the server setting.
- Sender email address: Enter the email address of the sender.
- Recipient email address: Enter the email address of the recipient.
- Server address: Enter the domain name or IP address of the email server.
- User name: Enter the user name of the email account if necessary.
- Password: Enter the password of the email account if necessary.
- Server port: The default mail server port is set to 25. You can also manually set another port.
- If your SMTP server requires a secure connection (SSL), select **This server requires a secure connection (SSL).**
- To verify if the email settings are correctly configured, click **Test**. The result will be shown in a pop-up window. If successful, you will also receive an email indicating the result.

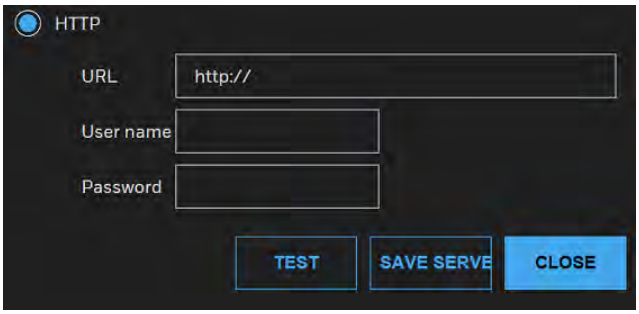
Click **SAVE SERVER** to enable the settings.

After you configure the first event server, the new event server will be automatically display on the Server list. If you wish to add other server options, click **Add server**.

Server type - HTTP

Select to send the media files to an HTTP server when a trigger is activated.

Figure 7-9 Server type – HTTP



- Server name: Enter a name for the server setting.
- URL: Enter the URL of the HTTP server.
- User name: Enter the user name if necessary.
- Password: Enter the password if necessary.

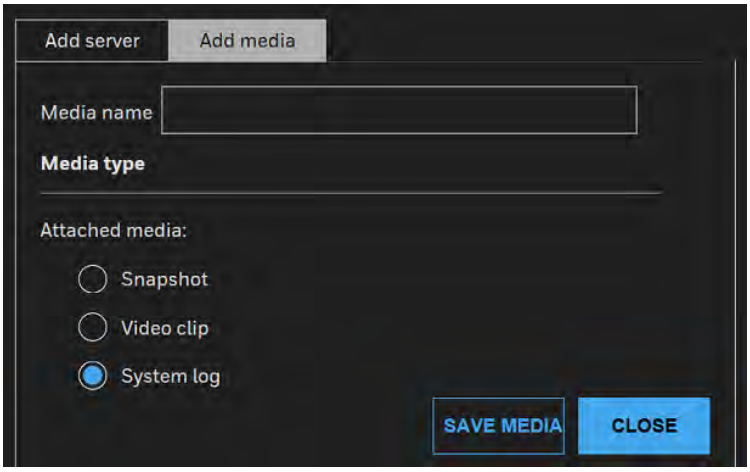
To verify if the HTTP settings are correctly configured, click **TEST**. The result will be shown in a pop-up window. If successful, you will receive a test.txt file on the HTTP server.

Click **SAVE SERVER** to enable the settings.

Add Media

Click **Add media** to open the media setting window. You can specify the type of media that will be sent when a trigger is activated. A total of 5 media settings can be configured. There are three choices of media types available: Snapshot, Video Clip, and System log. Select the item to display the detailed configuration options. You can configure either one or all of them.

Figure 7-10 Add Media



Media type – Snapshot

Select to send snapshots when a trigger is activated.

- Media name: Enter a name for the media setting.
- Source: Select to take snapshots from any of the video streams.
- Send pre-event images:

  The camera has a buffer to temporarily hold data up to a certain limit. Enter a number to decide how many images to capture before a trigger is activated. Up to 7 images can be generated.

- Send post-event images:

  Enter a number to decide how many images to capture after a trigger is activated. Up to 7 images can be generated.

  For example, if both the Send pre-event images and Send post-event images are set to 7, a total of 15 images can be generated after a trigger is activated.

- File name prefix

  Enter the text that will be appended to the front of the file name.

- Add date and time suffix to the file name

  Select this option to add a date/time suffix to the file name.

Click **SAVE MEDIA** to enable the settings. The new media server will be automatically displayed in the Media list. If you wish to add more media options, click **ADD MEDIA**.

Media type - Video clip

Select to send video clips when a trigger is activated.

- Media name: Enter a name for the media setting.
- Source: Select a video stream as the source of video clip.
- Pre-event recording

  The camera has a buffer to temporarily hold data up to a certain limit. Enter a number to decide the duration of recording before a trigger is activated. Up to 9 seconds can be set.

- Maximum duration

  Specify the maximum recording duration in seconds. The duration can be up to 10 seconds.

  For example, if pre-event recording is set to five seconds and the maximum duration is set to ten seconds, the camera continues to record for another 4 seconds after a trigger is activated.

- Maximum file size

  Specify the maximum file size allowed. Some users may need to stitch the video clips together when searching and packing up forensic evidence.

- File name prefix

  Enter the text that will be appended to the front of the file name.

Click **SAVE MEDIA** to enable the settings.

Media type - System log

Select to send a system log when a trigger is activated.

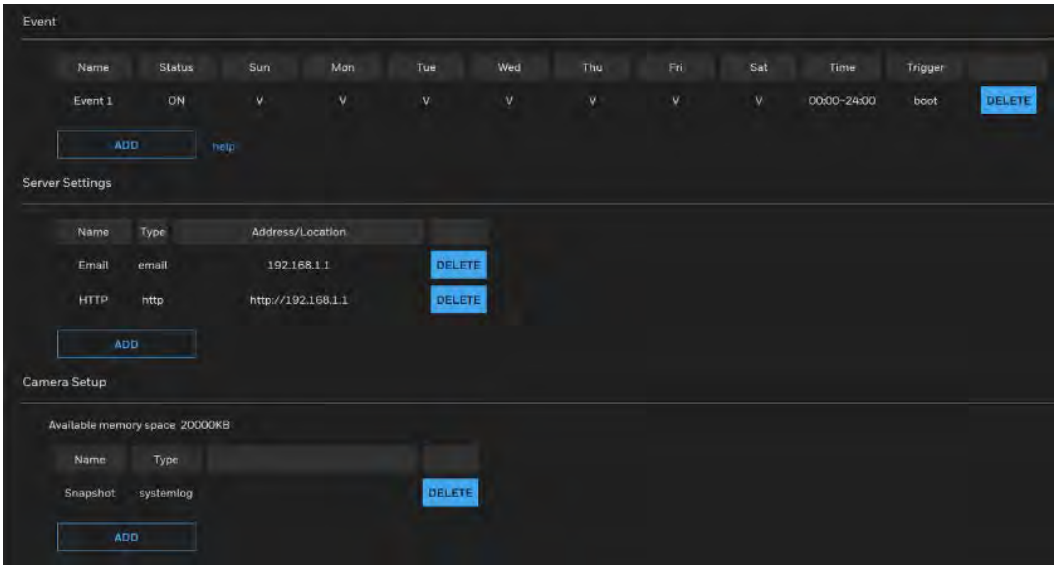
Click **SAVE MEDIA** to enable the settings, and then click **CLOSE** to exit the page.

In the Event settings tab, the Servers and Medias you configured will be listed. Make sure the Event Status is set to **ON**, in order to enable the event triggering action.

When completed, click **SAVE EVENT** to enable the settings and click **CLOSE** to exit Event Settings page. The new Event / Server settings / Media will be displayed in the event drop-down list on the Event setting page.

See the example of the Event setting page below:

Figure 7-11 Event Settings Examples



When the Event Status is **ON**, the event configuration above is triggered by motion detection, the camera will automatically send snapshots via e-mail.

If you want to stop the event trigger, you can click on the **ON** button to turn it to **OFF** status or click **DELETE** to remove the event setting.

To remove a server setting from the list, select a server name and click **DELETE**.

You can only delete a server setting when it is not applied in an existing event setting.

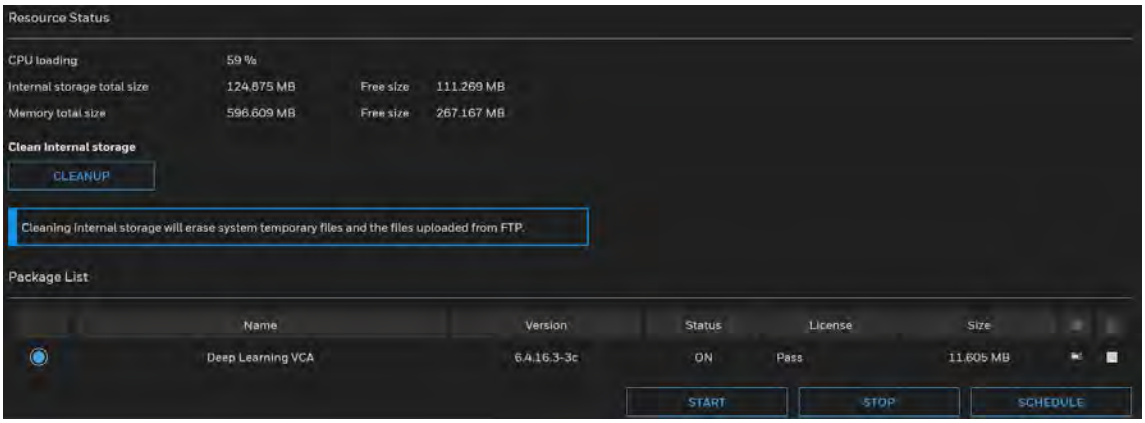
To remove a media setting from the list, select a media name and click **DELETE**.

You can only delete a media setting when it is not applied in an existing event setting.

Package Management

Go to **Setup →Video Analytics → Package Management.**

Figure 7-12 Package Management



The Resource Status shows the information of CPU loading, total size of internal storage, total size of memory and total size of SD card. If the total size of internal storage is not enough, click **CLEANUP** to clean the internal storage.

Click **Deep Learning VCA**, you can enter the interface of Video Analytics for intelligent video applications such as face detection, intrusion detection, loitering detection, missing object detection, unattended object detection, and line crossing detection. For how to configure the VA settings, refer to the user guide of Video Analytics.

To start running the Deep Learning VCA package, click **START**.

To stop running the Deep Learning VCA package, click **STOP**.

To delete the Deep Learning VCA package, click  .

If you want to apply the Deep Learning VCA settings at a specific period, click **SCHEDULE**, enter the time manually in the field and click **SAVE**.

8 Configuring Storage Settings

This chapter contains the following sections:

SD Card Management

Go to **Setup →Storage Setup →SD Card Management**.

This section describes how to manage the local storage on the camera. Here you can view SD card status, and implement SD card control.

See the following table for compatible SD Card.

Table 8-1 Compatible SD Card

SD Card Brand	Model	Size
Sandisk	microSDXC UHS-I Card	256 GB
Toshiba	microSDXC UHS-I Card	256 GB
Samsung	microSDXC UHS-I Card	256 GB
Toshiba	microSDXC UHS-I Card	128 GB
Sony	Sony Smart SD micro SDXC 64G	64 GB
Sony	Ultra microSDHC UHS-I 48MB/s	64 GB
Sandisk	microSDHC UHS-I Card	32 GB
Transcend	Transcend microSDHC 4G Class4	4 GB

Note

- It is recommended to turn OFF the recording activity before you remove an SD card from the camera.
- The lifespan of an SD card is limited. Regular replacement of the SD card can be necessary.
- Camera file system takes up several megabytes of memory space. The storage space cannot be used for recording.
- Using an SD card that already contains data recorded by another device should not be used in this camera.
- Do not modify or change the folder names in the SD card. That may result in camera malfunctions.
- If you want to use the SD card in another camera, format the SD card in another camera first. For how to format the SD card, see *SD Card Format* on page *70*.

SD Card Status

This tab shows the status and reserved space of your SD card. Remember to format the SD card when using it for the first time, see *SD Card Format* on page *70*.

Figure 8-1 No SD Card

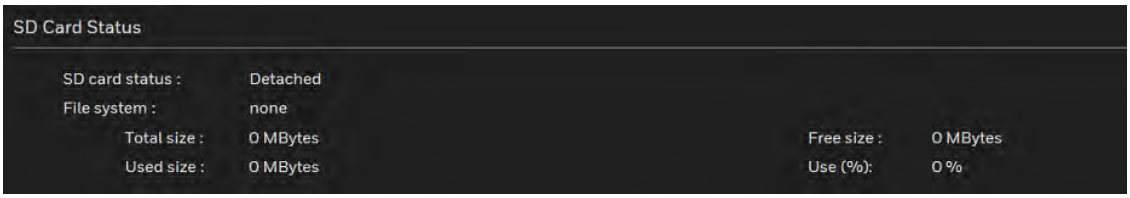
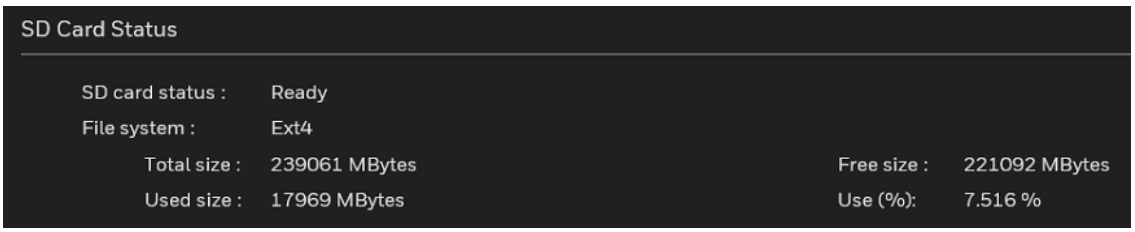
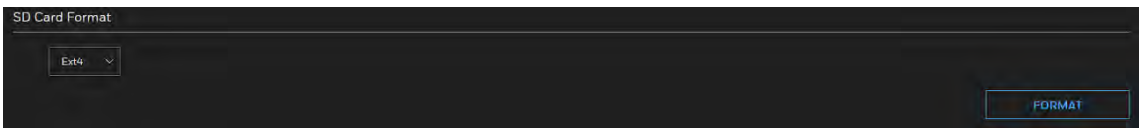


Figure 8-2 SD Card Onboard



SD Card Format

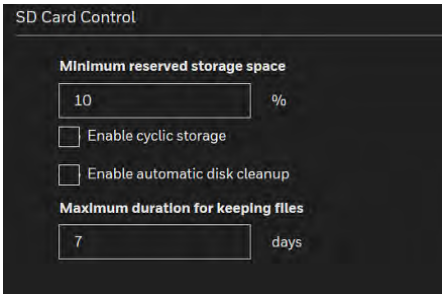
Figure 8-3 SD Card Format



To format the SD Card, click **FORMAT**.

SD Card Control

Figure 8-4 SD Card Control



Minimum reserved storage space: Enter a percentage for minimum storage space you want to reserve.

- **Enable cyclic storage**: Check to enable cyclic recording. When the maximum capacity is reached, the oldest file will be overwritten by the latest one.
- **Enable automatic disk cleanup**: Check to enable automatic disk cleanup. Enter the number of days you wish to retain a file. For example, if you enter “7 days”, the recorded files will be stored on the SD card for 7 days.

Click **SAVE** to enable your settings.

Content Management

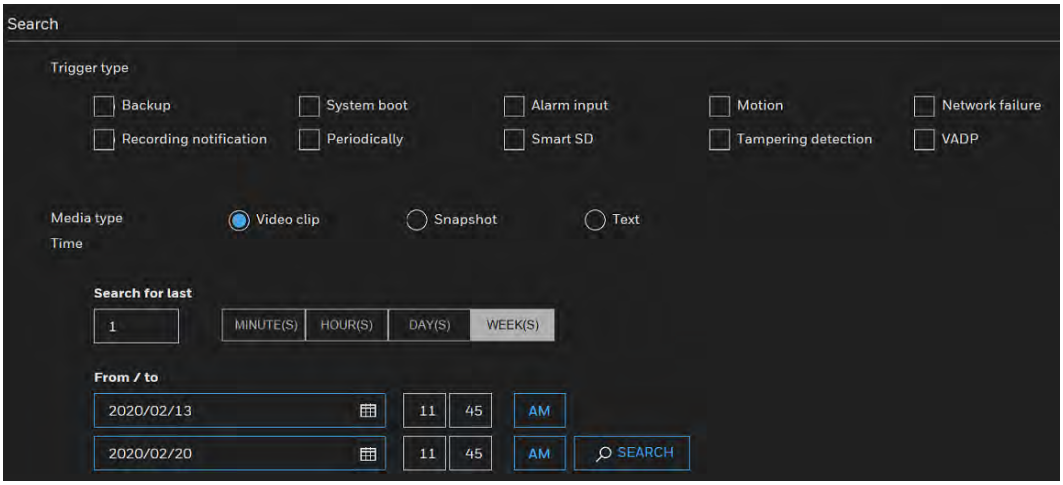
Go to **Setup →Storage Setup →Content Management**.

This section describes how to manage the content of recorded videos on the camera. Here you can search and view the records and view the searched results.

Searching and Viewing the Records

This tab allows the user to set up search criteria for recorded data. If you do not select any criteria and click **SEARCH**, all recorded data will be listed in the **Search Results** tab.

Figure 8-5 Search



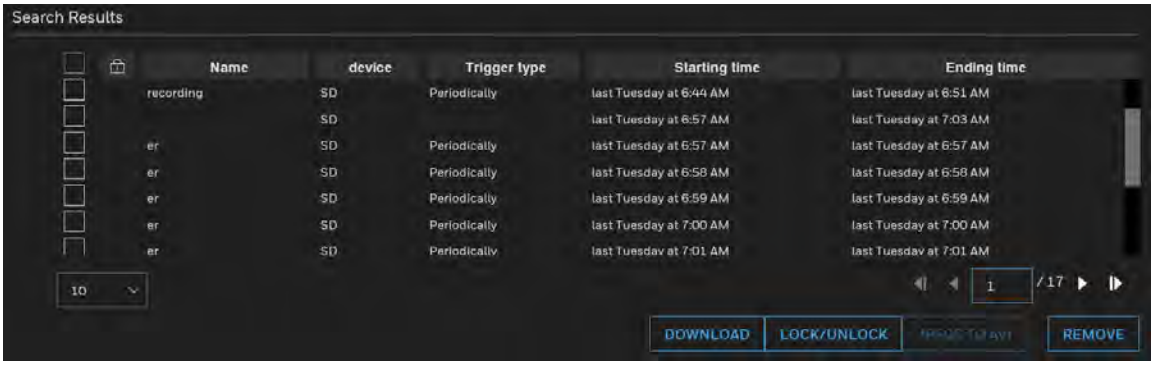
- Trigger Type: Select one or more trigger types.
- Media Type: Select a media type (Video clip, snapshot or text).
- Time: Manually enter the time range you want to search for contents created at a specific point in time.

Click **SEARCH** and the recorded data corresponding to the search criteria will be listed in **Search Results** tab.

Search Results

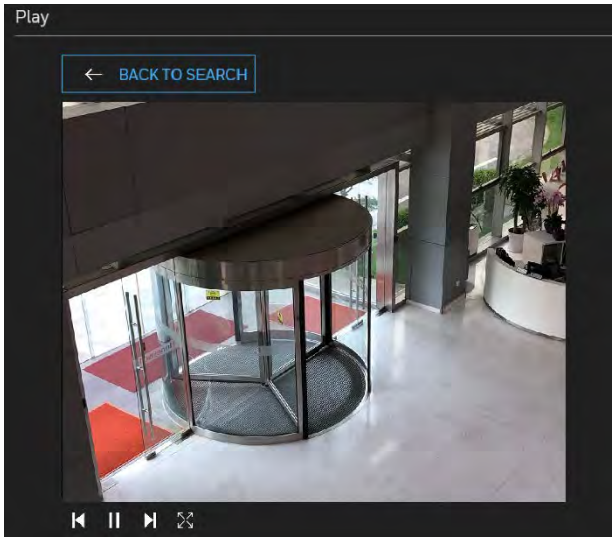
The following is an example of search results. To sort the search results, click each column header.

Figure 8-6 Search Results



- Play: Click on a search result and a Play window will be displayed for immediate review of the selected file.

Figure 8-7 Play Search Result



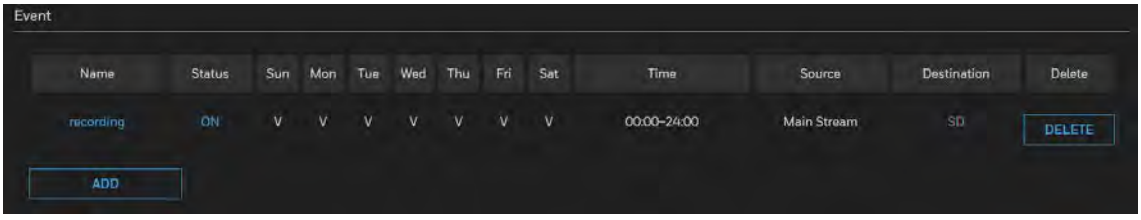
- Download: Click on a search result and click **DOWNLOAD,** and a file download window will pop up for you to save the file. You can play the video clip by VLC player.
- JPEGs to AVI: This functions only applies to "JPEG" format files such as snapshots. You can select several snapshots from the list, then click **JPEGS TO AVI**. Those snapshots will be converted into an AVI file.
- Lock/Unlock: Select the checkbox in front of a desired search result, then click **LOCK/UNLOCK**. The selected items will become Locked, which will not be deleted during cyclic recording. You can click again to unlock the selections.
- Remove: Select the desired search results, then click **REMOVE** to delete the files.

Recording Settings

Go to **Setup →Storage Setup →Recording Settings**.

This section describes how to configure the recording settings for the camera.

Figure 8-8 Recording Settings



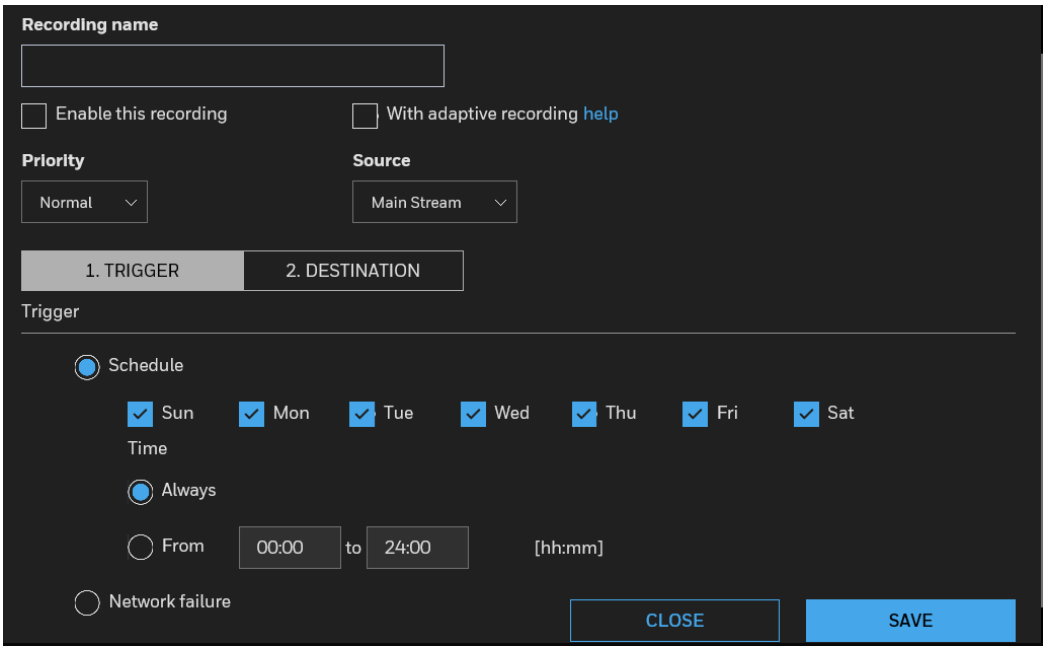
SD Test: Insert the SD card and click here to test.

Note	Format your SD card via the camera's web console when using it for the first time. For more information, see *SD Card Status* on page *70*.

Adding a Recording Setting

Click **ADD** as shown in *Figure 8-8* to open the recording setting window. On this page, you can define the adaptive recording, recording source, recording schedule, and recording capacity. A total of 2 recording settings can be configured.

Figure 8-9 Recording Settings Details



- Recording name: Enter a name for the recording setting.
- Enable this recording: Select this option to enable video recording.
- With adaptive recording:

  Select this option will activate the frame rate control according to alarm trigger.

  The frame control means that when there is a triggered alarm, the frame rate will raise up to the value you've configured on the Video quality page. For more information, see *Smart codec configuration* on page *24*.

  If you enable adaptive recording on a camera, only when an event is triggered on camera will the server record the full frame rate streaming data; otherwise, it will only request the I frame data during normal monitoring, thus effectively saves bandwidths and storage space.

Note

- To enable adaptive recording, make sure you've set up the trigger source such as Motion Detection or Manual Trigger. For more information, see *Configuring Event Settings* on page *59*.
- When there is no alarm trigger:
  - JPEG mode: record 1 frame per second.
  - H.264 mode: record the I frame only.
- When the I frame period is >1s on Video settings page, firmware will force decreasing the I frame period to 1s when adaptive recording is enabled.

- Priority: Select the relative importance of this recording (High, Normal, or Low). Recording with a higher priority setting will be executed first.
- Source: Select a video stream as the recording source.

Note To enable recording notification, configure ***Event* settings** first, see *Configuring Event Settings* on page *59*.

Setting up a Recording

To set up a recording:

1. Select a trigger source.

   Schedule: The server will start to record files on the local storage.

   Network failure: When network fail, the server will start to record files on the local storage (SD card).

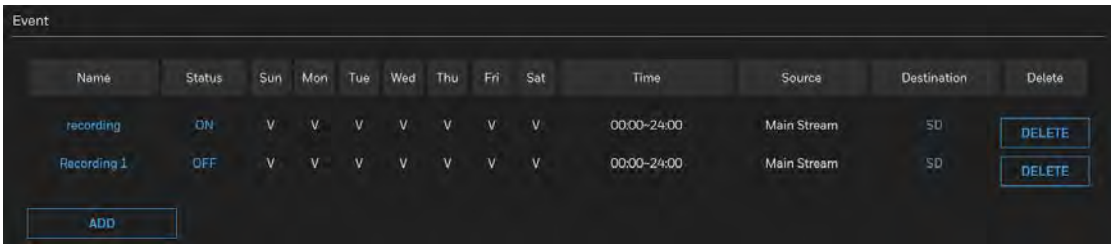
2. Set a destination (SD) for the recorded video files.
   - Manually assign the Maximum duration and the Maximum file size for each recording footage.
   - File name prefix: Enter the text that will be appended to the front of the file name.

If you want to enable recording notification, click **Event** to configure event triggering settings. For more information, see *Configuring Event Settings* on page *59*.

When completed, select **Enable this recording**. Click **SAVE** to enable the setting and click **CLOSE** to exit this page. When the system begins recording, it will send the recorded files to the network storage. The new recording name will be displayed on the recording settings page as shown below.

To remove a recording setting from the page, click **DELETE**.

Figure 8-10 Recording 1



- Click Recording 1 (Name): Opens the Recording Settings page to modify.
- Click ON (Status): The Status will become OFF and stop recording.
- Click SD (Destination): Opens the file list of recordings.

9 Configuring System Settings

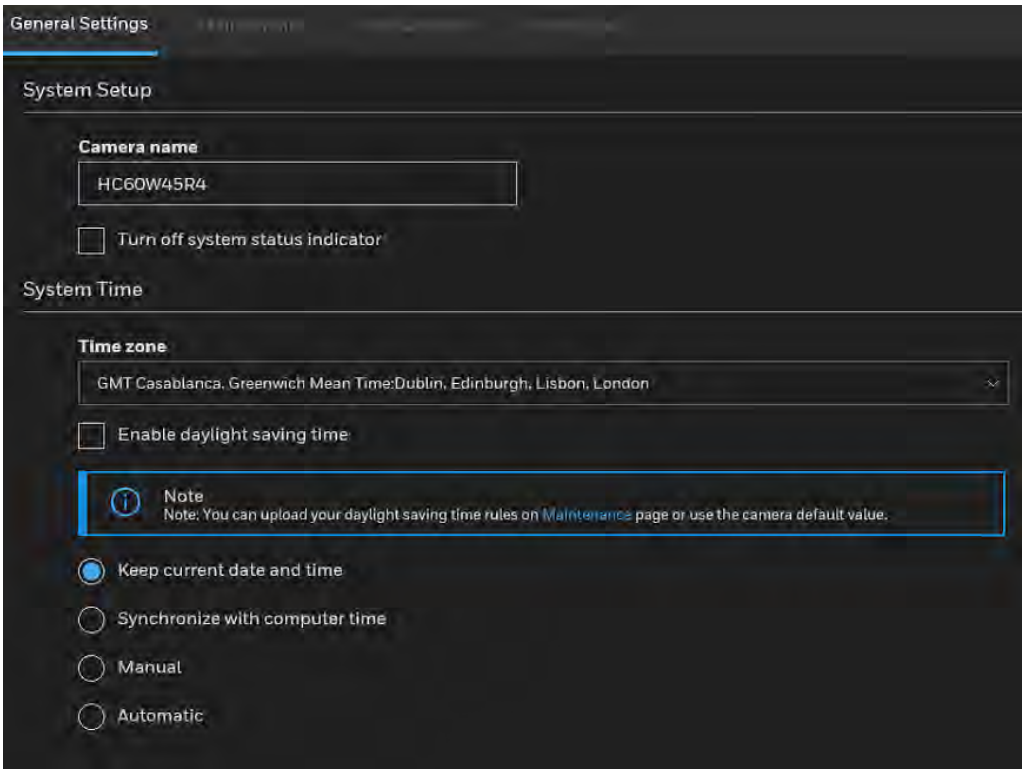
This chapter contains the following sections:

Configuring System General Settings

Go to **Setup →System Setup →General Settings**.

This section explains how to configure the basic settings for the camera, such as the host name and system time.

Figure 9-1 Configuring System General Settings



Camera Name: Enter a name for the camera. The text will be displayed at the top of the main page.

Turn off the LED indicators: If you do not want others to notice the network camera is in operation, you can select this option to turn off the LED indicators.

Time zone: Select the appropriate time zone from the dropdown list. If you want to upload Daylight Savings Time rules, see *Configuring Maintenance Settings* on page *78* .

Keep current date and time: Select this option to preserve the current date and time of the camera. The camera's internal real-time clock maintains the date and time even when the power of the system is turned off.

Synchronize with computer time: Select this option to synchronize the date and time of the camera with the local computer. The read-only date and time of the PC is displayed as updated.

Manual: The administrator can enter the date and time manually. The date and time format are [yyyy/mm/dd] and [hh:mm:ss].

Automatic: The Network Time Protocol is a protocol which synchronizes computer clocks by periodically querying an NTP Server.

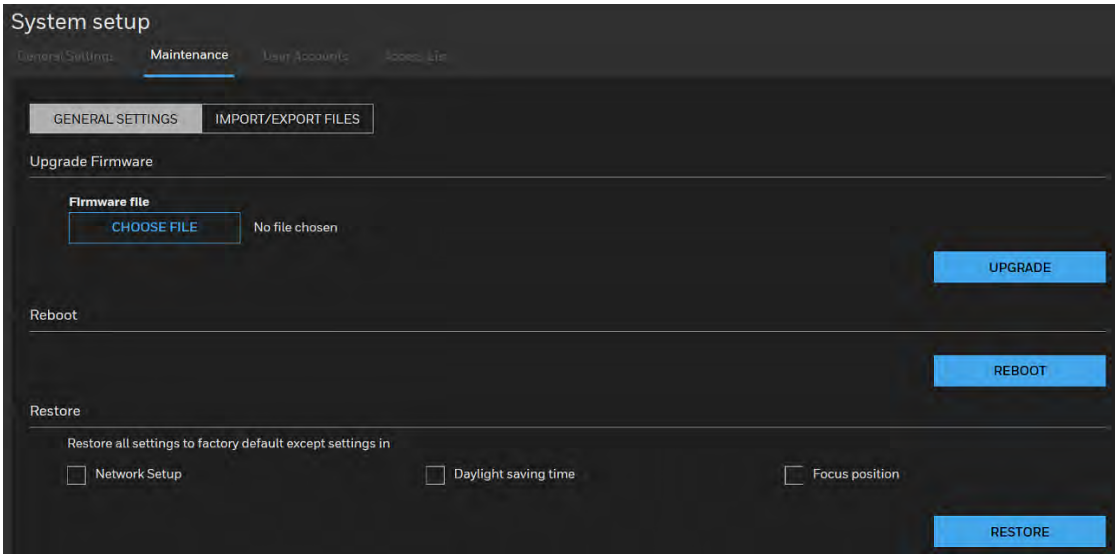
- NTP server: Assign the IP address or domain name of the time-server. Leaving the text box blank connects the camera to the default time servers. The precondition is that the camera must have the access to the Internet.
- Update interval: Select to update the time using the NTP server on an hourly, daily, weekly, or monthly basis.

Configuring Maintenance Settings

Go to **Setup →System Setup →Maintenance**.

This chapter describes how to restore the camera to factory default, upgrade firmware version, etc.

Figure 9-2 Maintenance



Upgrading Firmware

On this page, you can upgrade the firmware of the camera. It takes a few minutes to complete the process.

Note	• Do not power off the camera during the upgrade. • If an SD card is used in your camera, backup your SD card contents if necessary before the upgrade.

Follow the steps below to upgrade the firmware:

1. Click **CHOOSE FILE** and locate the firmware file.
2. Click **UPGRADE**. The camera starts to upgrade and will reboot automatically when the upgrade completes.

Note	• If an SD card is used in your camera, it will be formatted automatically after the upgrade. The formatting may take 5 to 20 minutes. • After the SD card is formatted, it will be encrypted and its content cannot be read on other cameras. • If you want to use the SD card in another camera, format the SD card in another camera first. For how to format the SD card, see *SD Card Format* on page *70*. • A new SD card inserted to camera will also be formatted automatically after the camera is upgraded.

If the upgrade is successful, the “Reboot system now!! This connection will close” message will be displayed. After that, re-access the camera. If an SD card is inserted to the camera, wait for the SD card formatting to complete.

Rebooting the Camera

On this page, you can reboot the camera. It takes about one minute to complete. After it is completed, the live video page will be displayed in your browser.

If the connection fails after rebooting, manually enter the IP address of the camera in the address field to resume the connection.

Restoring the Camera

Restore the camera to factory default settings.

Network Setup: Check to retain the Network Type settings (see *Configuring Network General Settings* on page *44*).

Daylight Saving Time: Check to retain the Daylight Saving Time settings (see *Importing /Exporting Files* on page *80*).

Focus position: Check to retain the lens focus position using the previously saved position parameters.

If none of the options is selected, all settings will be restored to factory default. Click **RESTORE** and the camera will be rebooted.

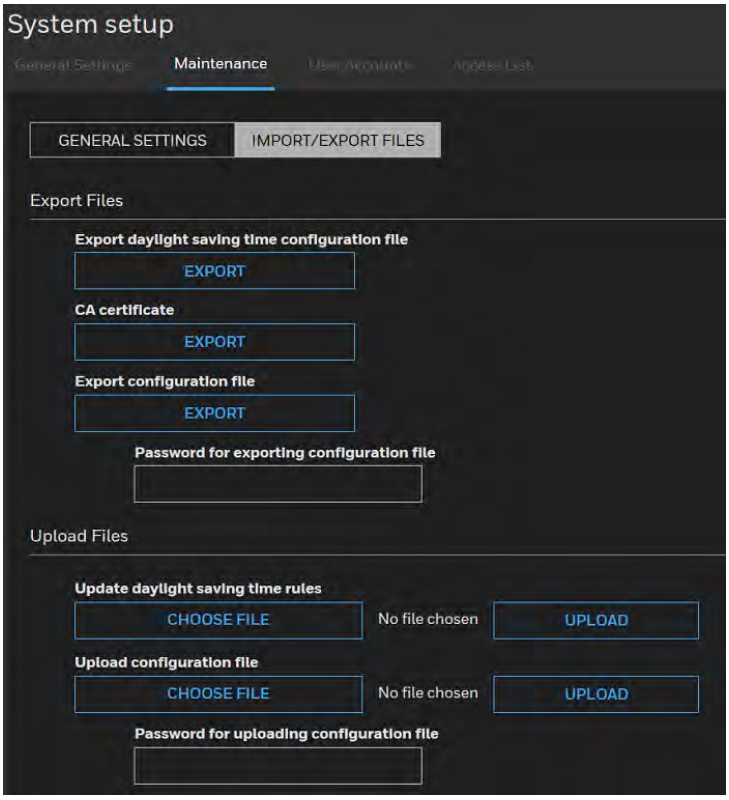
After it is completed, the live video page will be displayed in your browser.

If the connection fails after rebooting, manually enter the IP address of the camera in the address field to resume the connection.

Importing /Exporting Files

Export / Update daylight saving time rules, custom language file, configuration file, and server status report.

Figure 9-3 Import/Export Files



Export daylight saving time configuration file

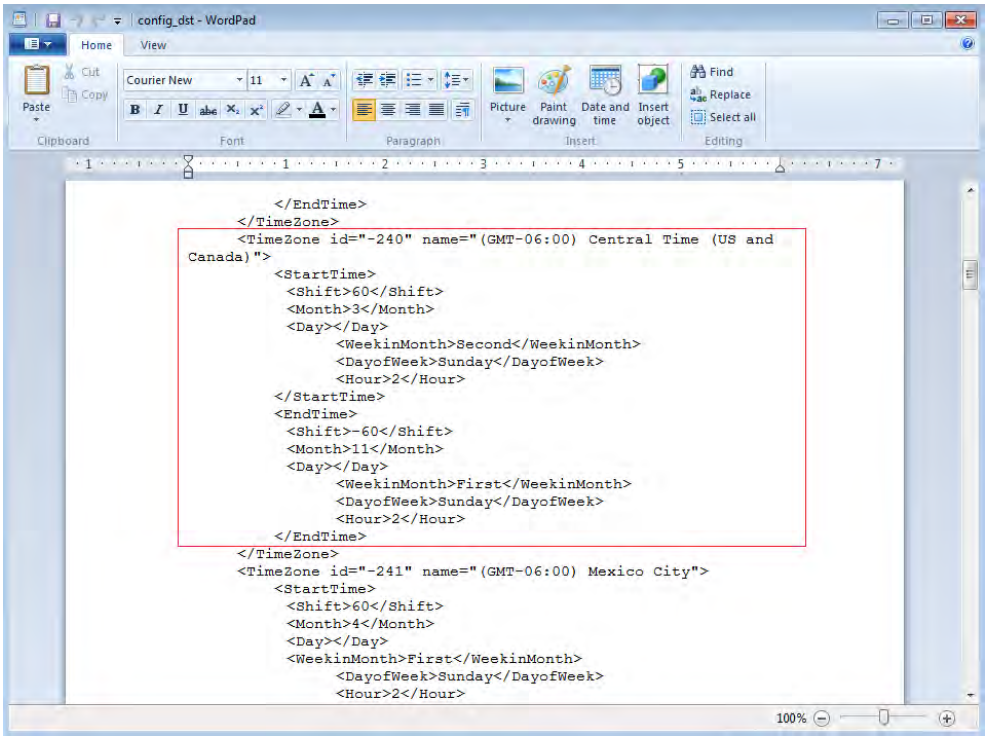
Follow the steps below to export daylight saving time configuration file from the camera and set the start and end time of DST.

1. Click **EXPORT** under Export daylight saving time configuration file.

2. A file download dialog will be displayed. Click **Open** to review the XML file or click **Save** to store the file for editing.
3. Open the file with Microsoft® Wordpad and locate your time zone; set the start and end time of DST.

After it is completed, save the file.

In the example below, DST begins each year at 2:00 a.m. on the second Sunday in March and ends at 2:00 a.m. on the first Sunday in November.



Export CA Certificate

The camera uses HTTPS, a secure communication protocol that verifies the identities of visited websites and servers and encrypts data exchanged between the client and the server. When you log in to the camera's web client for the first time, some browsers may display a warning that the connection is not private/secure. To access the web client, you must install a Honeywell-signed security certificate.

1. Click **Export** to save the root certificate (ca.crt) on your local computer.
2. Go to the directory where you saved the certificate and double-click the certificate. The **Certificate** window opens.
3. In the **Certificate** window, on the **General** tab, click **Install Certificate** to open the Certificate Import Wizard.
4. Click **Next** to continue.
5. Click **Place all certificates in the following store**, click **Browse**, click **Trusted Root Certification Authorities**, and then click **OK**.
6. Click **Next**, and then click **Finish** to close the Certificate Import Wizard. A confirmation dialog box appears with the message "The import was successful."

7. Click **OK**, and then click **OK** to close the Certificate window. And now your browser will not display a warning that the connection is not private/secure.

Note	Please ensure to install the certificate to ensure a secure communication with the camera and to avoid delays in the web page navigation.

Export configuration file

Enter a password for exporting the configuration file and then click **EXPORT** to export all parameters for the camera and user-defined scripts.

Update daylight saving time rules

Follow the steps below to update daylight saving time rules:

1. Click **CHOOSE FILE** under Update daylight saving time rules.
2. Select the XML file to update.
3. Click **UPLOAD**.

Upload configuration file

Follow the steps below to upload a configuration file:

1. Enter the password for uploading the configuration file. The password must be the same with the password of the configuration file you set for exporting, or the uploading will be failed. For example, if you set the password A for the configuration file A and you set the password B for the configuration file B. When you want to upload the configuration file B, you must use the password B.
2. Click **CHOOSE FILE** to locate the configuration file and then click **UPLOAD** to upload the configuration file.

The model and firmware version of the device should be the same as the configuration file. If you have set up a fixed IP or other special settings for your device, it is not suggested to update a configuration file.

If the power is disconnected during firmware upgrade or if there is unknown reason causing abnormal LED status, and a Restore cannot recover normal working condition, you can perform the following steps to activate the camera with its backup firmware:

a. Press and hold down the reset button for at least one minute.

b. Power on the camera until the Red LED blinks rapidly.

c. After boot up, the firmware should return to the previous version before the camera hanged. (The procedure should take 5 to 10 minutes, longer than the normal boot-up process). When this process is completed, the LED status should return to normal.

Configuring User Accounts Settings

Go to **Setup →System Setup →User Accounts**.

This section describes how to create multiple accounts and grant privileges to these accounts.

Account Management

Figure 9-4 Account Management

The administrator account name is “admin”, which is permanent and cannot be deleted.

The administrator can create up to 20 user accounts.

To create a new user:

1. Select New user from the dropdown list.
2. Enter the new user’s name and password and confirm the password. Some, but not all special ASCII characters are supported. You can use “!?@#$%=+*-_:,.&^~” in the password combination.
3. Select the privilege level for the new user account. Click **ADD** to enable the setting.

The privilege levels are listed below:

Role	Privilege
Administrator	Full control
Viewer	Live, Language

Access rights are sorted by user privilege (Administrator, Operator, and Viewer). Only administrators can access the Configuration page. Viewers can only access the main page for live viewing.

To change a user’s access rights or delete user accounts:

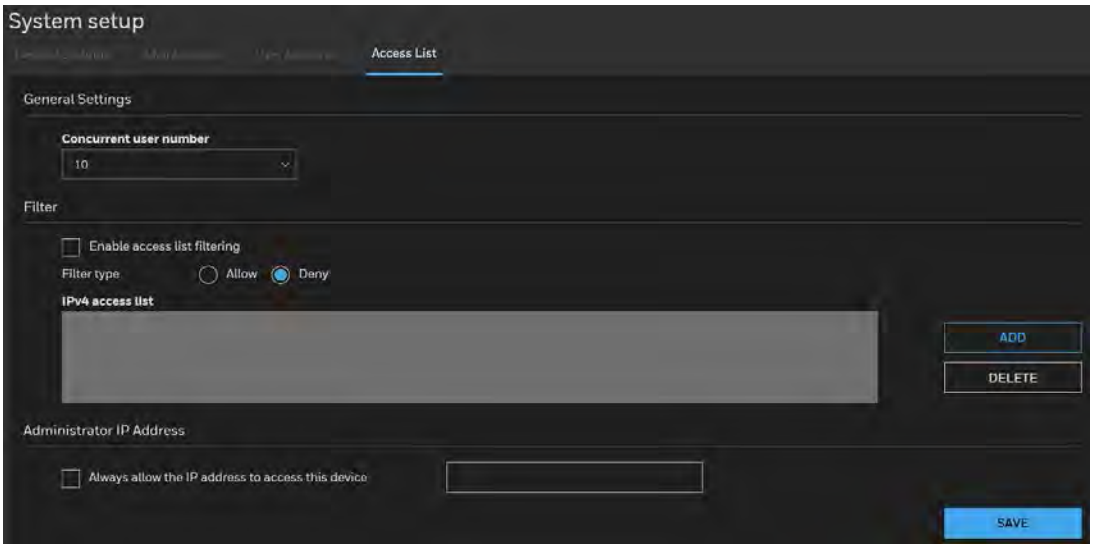
1. Select an existing account to modify.
2. Make necessary changes and click **UPDATE** or **DELETE** to enable the setting.

Configuring Access List Settings

Go to **Setup →System Setup →Access List**.

This section describes how to control access permission by verifying the client PC's IP address.

Figure 9-5 Access List



General Settings

Concurrent user number: Simultaneous live viewing for 1~10 clients (including main stream to third stream). The default value is 10.

Filter

Enable access list filtering: Check this item and click **SAVE** to enable the access list filtering function.

Filter type: Select **Allow** or **Deny** as the filter type. If you choose Allow Type, only those clients whose IP addresses are on the Access List below can access the camera, and the others cannot. On the contrary, if you choose Deny Type, those clients whose IP addresses are on the Access List below will not be allowed to access the camera, and the others can.

Click **ADD** and you can add a rule to the following Access List.

Single: This rule allows the user to add an IP address to the Allowed/Denied list.

Network: This rule allows the user to assign a network address and corresponding subnet mask to the Allow/Deny List. The address and network mask are written in CIDR format.

Range: This rule allows the user to assign a range of IP addresses to the Allow/Deny List.

Note	• The IPv6 access list column will not be displayed unless you enable IPv6 on the Network page. For more information about IPv6 Settings, see *Enable IPv6* on page 45. • The **Range** rule only applies to IPv4 addresses.

Administrator IP address

Always allow the IP address to access this device: Check it and add the Administrator's IP address in this field to make sure the Administrator can always connect to the device.

10 Viewing System Information

This chapter contains the following sections:

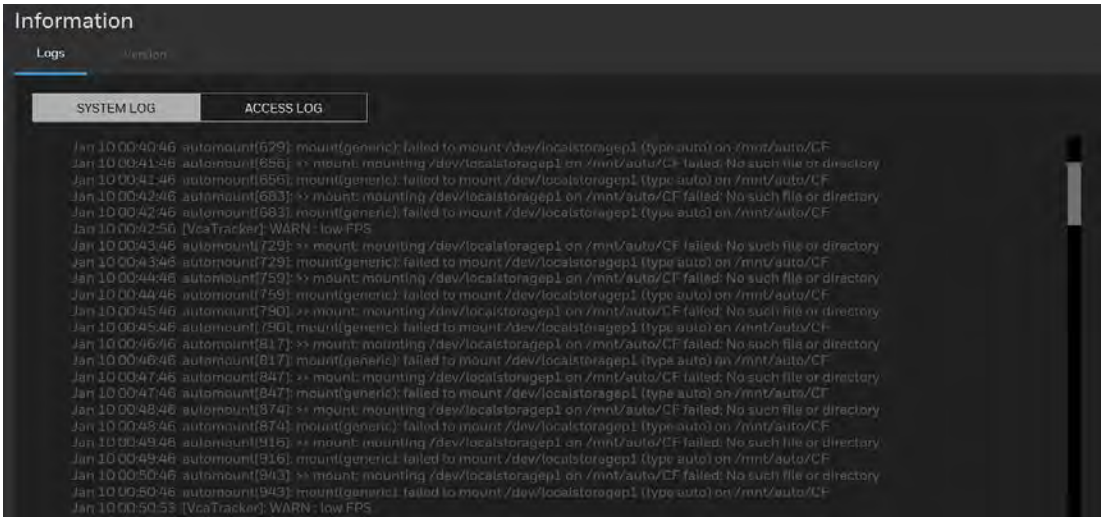
Log

Go to **Setup →Information →Logs**.

System Log

System log displays the system events in a chronological order. The system log is stored in the camera's buffer area and will be deleted after the camera is rebooted.

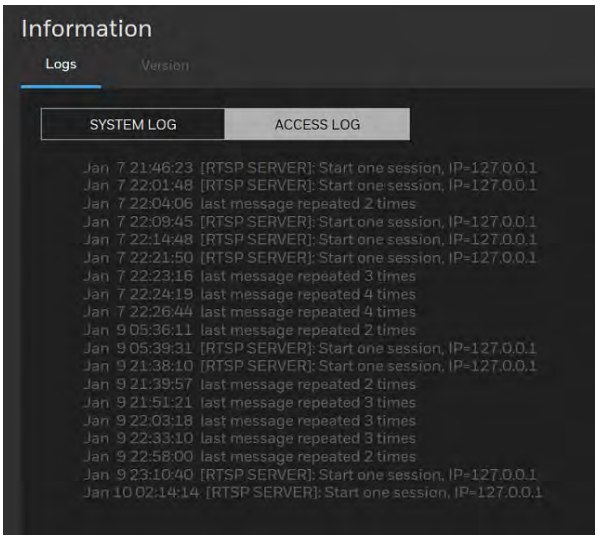
Figure 10-1 System Log



Access Log

Access log displays the access time and IP address of all viewers (including operators and administrators) in a chronological order. The access log is stored in the camera's buffer area and will be will be deleted after the camera is rebooted.

Figure 10-2 Access Log



Version

Go to **Setup →Information →Version**.

On the **Version** page, you can view the software version.

11 Troubleshooting

Troubleshooting for Common Issues

Refer to the following guidelines to troubleshoot any performance issues. If you require additional assistance, contact Honeywell Technical Support (see back cover for contact information).

Table 11-1 Troubleshooting

Issues	Solutions
Cannot install/log in to web client.	• Ensure that your browser's security settings allow ActiveX controls. • Ensure that you have a valid network setup and that you are using the correct login user name and password.
Power supply is unstable.	• Use of a UPS power supply is strongly recommended.
Camera webpage has abnormal display.	• Clear the cache of browser
The audio will not stop automatically when switching from live page to settings page.	• Manually turn off the audio on live page

12 Appendix

List of Symbols

The following is a list of symbols that may appear on the camera:

Symbol	Explanation
	The WEEE symbol. This symbol indicates that when the end-user wishes to discard this product, it must be sent to separate collection facilities for recovery and recycling. By separating this product from other household-type waste, the volume of waste sent to incinerators or landfills will be reduced, and thus natural resources will be conserved.
	The UL compliance logo. This logo indicates that the product has been tested and is listed by UL (formerly Underwriters Laboratories).
	The FCC compliance logo. This logo indicates that the product conforms to Federal Communications Commission compliance standards.
	The direct current symbol. This symbol indicates that the power input/output for the product is direct current.
	The alternating current symbol. This symbol indicates that the power input/output for the product is alternating current.
	The RCM compliance logo. This logo indicates that the product conforms with Australian RCM guidelines.
	The CE compliance logo. This logo indicates that the product conforms to the relevant guidelines/standards for the European Union harmonization legislation.
	The caution symbol. This symbol indicates important information.
	The protective earth (ground) symbol. This symbol indicates that the marked terminal is intended for connection to the protective earth/grounding conductor.

EAC	Eurasian Conformity (EAC) RoHS

Honeywell Building Technologies – Security Americas (Head Office)
Honeywell Commercial Security
715 Peachtree St. NE
Atlanta, GA 30308
www.security.honeywell.com/
☏ +1 800 323 4576

Honeywell Building Technologies – Security Mexico
Mexico: Av. Santa Fe 94, Torre A, Piso 1, Col. Zedec,
CP 0121, CDMX, Mexico.
Colombia: Edificio Punto 99, Carrera 11a.
98-50, Piso 7, Bogota, Colombia.
clarsupport@honeywell.com
www.honeywell.com
☏ 01.800.083.59.25

Honeywell Colombia SAS
Carrera 11A # 98-50, Edificio Punto 99, Piso 7
Bogotá DC, Colombia

Honeywell Building Technologies – Security Middle East/N. Africa
Emaar Business Park, Sheikh Zayed Road
Building No. 2, 2nd floor, 201
Post Office Box 232362
Dubai, United Arab Emirates
www.honeywell.com/security/me
☏ +971 44541704

Honeywell Building Technologies – Security Europe/South Africa
Aston Fields Road, Whitehouse Industrial Estate
Runcorn, WA7 3DL, United Kingdom
www.honeywell.com/security/uk
☏ 08448 000 235

Honeywell Building Technologies – Security Northern Europe
Stationsplein Z-W 961, 1117 CE Schiphol-Oost, The Netherlands
www.security.honeywell.com/nl
☏ +31 (0) 299 410 200

Honeywell Building Technologies – Security Deutschland
Johannes-Mauthe-Straße 14 72458 Albstadt, Germany
www.security.honeywell.de
☏ +49 (0) 7431 801-0

Honeywell Building Technologies – Security France
Immeuble Lavoisier
Parc de Haute Technologie 3-7 rue Georges Besse
92160 Antony, France
www.security.honeywell.com/fr
☏ +33 (0) 1 40 96 20 50

Honeywell Building Technologies – Security Italia SpA
Via Achille Grandi 22, 20097 San Donato Milanese (MI),
ITALY
www.security.honeywell.com/it

Honeywell Building Technologies – Security España
Josefa Valcárcel, 24
28027 - Madrid
España
www.honeywell.com
☏ +34 902 667 800

Honeywell Building Technologies – Security Россия и СНГ
121059 Moscow, UI, Kiev 7 Russia
www.security.honeywell.com/ru
☏ +7 (495) 797-93-71

Honeywell Building Technologies – Security Asia Pacific
Building #1, 555 Huanke Road, Zhang Jiang Hi-Tech Park
Pudong New Area, Shanghai, 201203, China
www.asia.security.honeywell.com
☏ 400 840 2233

Honeywell Building Technologies – Security and Fire (ASEAN)
Honeywell International Sdn Bhd
Level 25, UOA Corp Tower, Lobby B, Avenue 10, The Vertical,
Bangsar South City, 59200, Kuala Lumpur, Malaysia
Visit Partner Connect: www.partnerconnect.honeywell.com
Email: buildings.asean@honeywell.com
Technical support (Small & Medium Business):
Vietnam: +84 4 4458 3369
Thailand: +66 2 0182439
Indonesia: +62 21 2188 9000
Malaysia: +60 3 7624 1530
Singapore: +65 3158 6830
Philippines: +63 2 231 3380

Honeywell Home and Building Technologies (India)
HBT India Buildings
Unitech Trade Centre, 5th Floor,
Sector – 43, Block C, Sushant Lok Phase – 1,
Gurgaon – 122002, Haryana, India
Visit Partner Connect: www.partnerconnect.honeywell.com
Email: HBT-IndiaBuildings@honeywell.com
Toll Free No: 1-800-103-0339
☏ +91 124 4975000

Honeywell Building Technologies – Security and Fire (Korea)
Honeywell Co., Ltd. (Korea)
5F SangAm IT Tower,
434, Worldcup Buk-ro, Mapo-gu,
Seoul 03922, Korea
Visit: http://www.honeywell.com
Email: info.security@honeywell.com
Customer support: HSG-CS-KR@honeywell.com; +82 1522-8779
☏ +82-2-799-6114

Honeywell Building Technologies – Security & Fire (Pacific)
Honeywell Ltd
9 Columbia Way
BAULKHAM HILLS NSW 2153
Visit: www.honeywellsecurity.com.au
Email: hsf.comms.pacific@Honeywell.com
Technical support:
Australia: 1300 220 345
New Zealand: +64 9 623 5050

www.honeywell.com/security
+1 800 323 4576 (North America only)
https://www.honeywellsystems.com/ss/techsupp/index.html
Document 800-26140 Rev A – 03/2020