Honeywell

Honeywell 60 Series

Panoramic Camera

HC60WM20R1

User Guide

Recommended

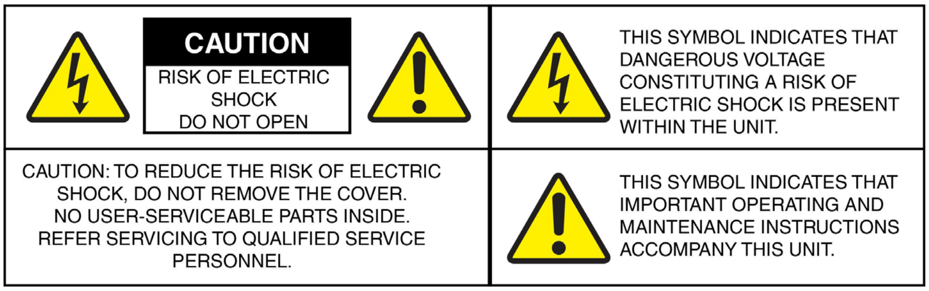
Find the latest version of this and other Honeywell documents on our website: https://buildings.honeywell.com/security.

Copy Right

Revision

Issue	Date	Revisions
A	10/2023	New document.

Cautions and Warnings



CAUTION

RISK OF ELECTRIC SHOCK
DO NOT OPEN

THIS SYMBOL INDICATES THAT DANGEROUS VOLTAGE CONSTITUTING A RISK OF ELECTRIC SHOCK IS PRESENT WITHIN THE UNIT.

CAUTION: TO REDUCE THE RISK OF ELECTRIC SHOCK, DO NOT REMOVE THE COVER. NO USER-SERVICEABLE PARTS INSIDE. REFER SERVICING TO QUALIFIED SERVICE PERSONNEL.

THIS SYMBOL INDICATES THAT IMPORTANT OPERATING AND MAINTENANCE INSTRUCTIONS ACCOMPANY THIS UNIT.

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, Local Certified / 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 802.3bt PoE standard. The PoE is not intended to be connected to exposed (outside plant) networks. Consult Honeywell for the recommended adapter.**

Warning: **To comply with EN50130-4 requirements, a UPS should be employed when powering the camera from 24 VAC.**

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

Regulatory Statements

Photobiological safety

This product fulfills the requirements for photobiological 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

Information to the User: 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 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 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 (2011/65/EU) as Amended by RoHS 3 (2015/863), 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.

Check Local Waste Guidelines

Components of this product require separate waste collection. Check local waste guidelines for sorting rules

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 & Viewing Live Video, describes how to log in to a camera and using the main page.
- Chapter 4, Configuring Camera Settings, describes camera configurations.
- Chapter 5, Configuring Network Settings, describes network configurations.
- Chapter 6, Configuring Video Analytics, describes video analytics configurations.
- Chapter 7, Configuring Storage Settings, describes storage configurations.
- Chapter 8, Configuring System Settings, describes general system configurations.
- Chapter 9, Viewing System Information, describes system information, such as version, log and online user information.
- Chapter 10, Troubleshooting, lists common problems and solutions.
- Chapter 11, Appendix, lists the descriptions of symbols.

CHAPTER

1 INTRODUCTION

This chapter contains the following sections:

- Overview, page 2
- Key Features, page 2

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 with 4 sensor/Lens at up to 30 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 (30 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 24 VAC adapter, 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 micro SDHC cards (up to 1T) when network service is interrupted.

Key Features

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

Camera

- Up to 5MP (2688x1920) with 4 sensor/Lens
- 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 3D noise reduction saving storage and bandwidth together with smart codec
- For use as part of Video Systems which comply with NDAA Section 889
- FIPS chipset build-in

Storage

- Central server backup (configure in Event settings)
- Recording over Internet, files stored on SD card/SFTP

Network

- Up to 10 connections
- Compatible with the following network protocols: IPv4, IPv6, TCP/IP, HTTP, HTTPS, RTSP/RTP/RTCP, IGMP/Multicast, SMTP, DHCP, NTP, DNS, DDNS, QoS, SNMP, 802.1X, UDP, ICMP, ARP, TLS, SFTP
- 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 event types: Video motion detection, Periodically, Alarm input, System boot, Recording notification, Camera tampering detection, Audio detection
- Support the following event linkage mode: Event notification using digital output, HTTP, Email, SFTP 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

CHAPTER

2 ACCESSING THE CAMERA

This chapter contains the following sections:

Installing the Unified Tool

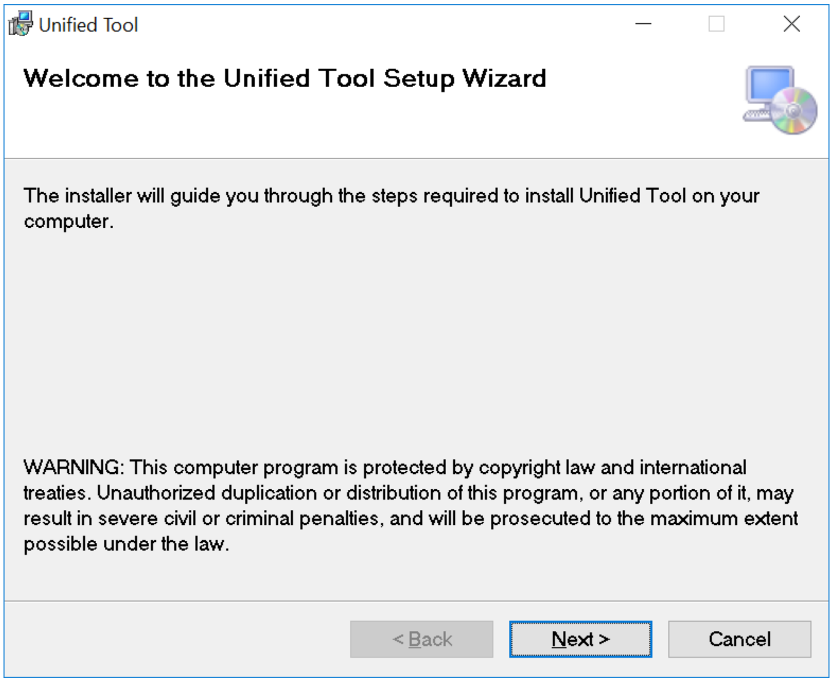
To get the installation package of Unified Tool:

Go to https://myhoneywellbuildingsuniversity.com and login. Go to **Technical Support Self-Service → Download Center → Video → Tools → Camera Tools → Unified Tool**. Download and unzip the installation package of Unified Tool to your computer.

To install the Unified Tool:

1. Double-click the installation program in the installation package.

Figure 1 Install Unified Tool



Unified Tool

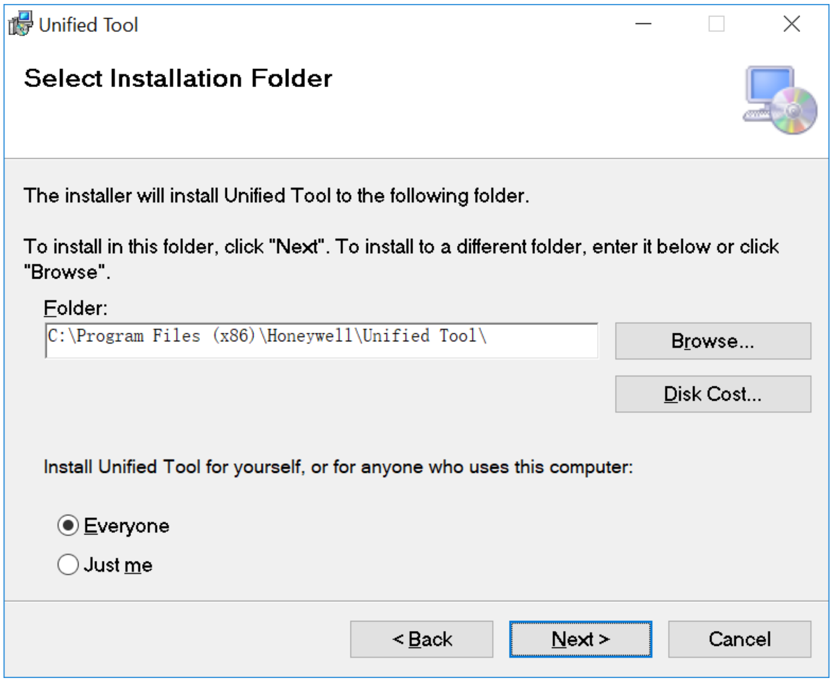
Welcome to the Unified Tool Setup Wizard

The installer will guide you through the steps required to install Unified Tool on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

2. Click Next and the following figure is displayed:

Figure 2 Select Installation Folder



Unified Tool

Select Installation Folder

The installer will install Unified Tool to the following folder.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files (x86)\Honeywell\Unified Tool\

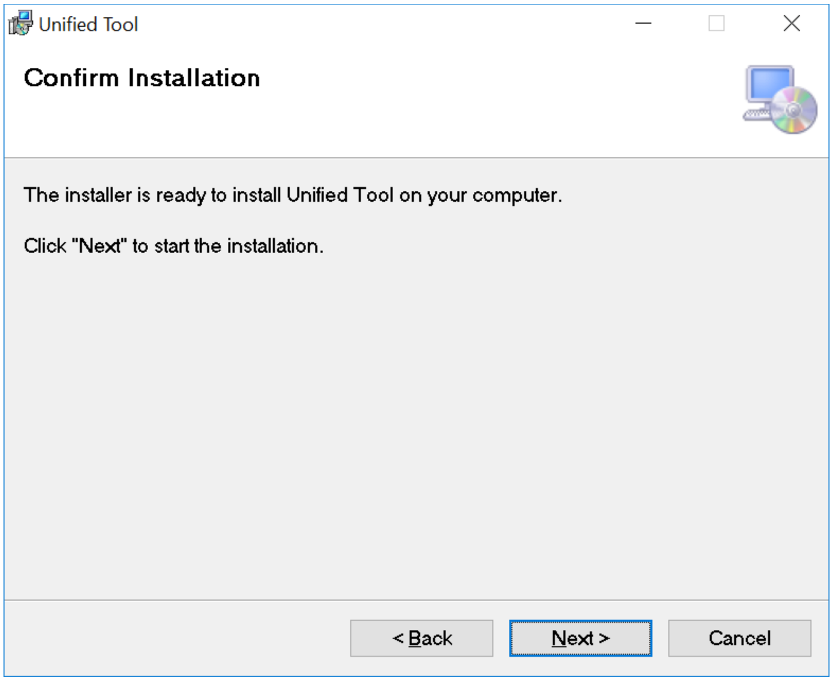
Install Unified Tool for yourself, or for anyone who uses this computer:

● Everyone

○ Just me

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

Figure 3 Confirm Installation



The installer is ready to install Unified Tool on your computer.

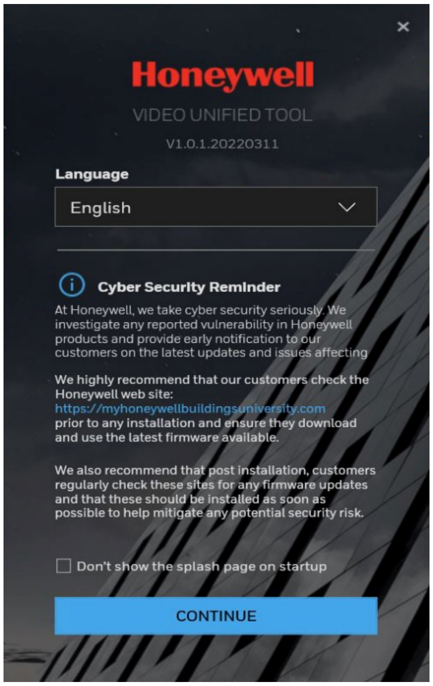
Click "Next" to start the installation.

4. Click Next. When the installation is completed, click Close. A shortcut of Unified Tool will be displayed on your desktop.

Discovering Your Camera on the Network

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

Figure 4 Splash Screen



Honeywell

VIDEO UNIFIED TOOL

V1.0.1.20220311

Language

English

Cyber Security Reminder

At Honeywell, we take cyber security seriously. We investigate any reported vulnerability in Honeywell products and provide early notification to our customers on the latest updates and issues affecting

We highly recommend that our customers check the Honeywell web site:
https://myhoneywellbuildingsuniversity.com
prior to any installation and ensure they download and use the latest firmware available.

We also recommend that post installation, customers regularly check these sites for any firmware updates and that these should be installed as soon as possible to help mitigate any potential security risk.

□ Don't show the splash page on startup

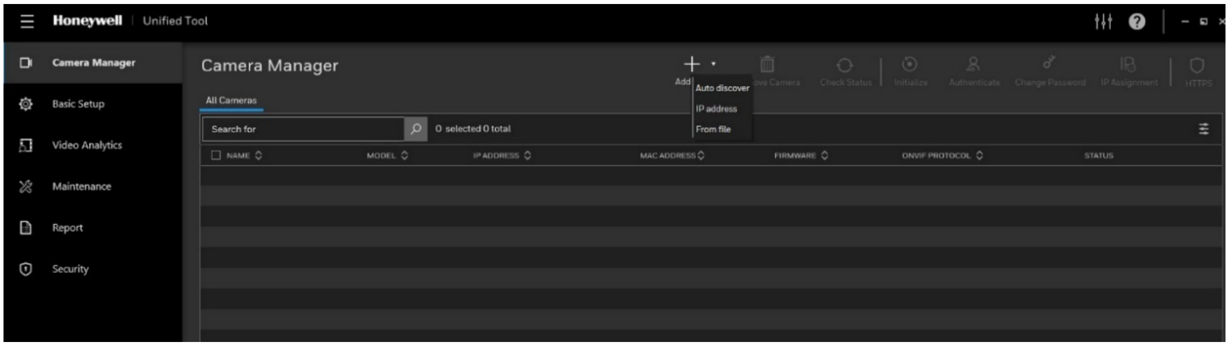
CONTINUE

2. Select your language from the dropdown list of Language. Currently, English and traditional Chinese are supported.

3. 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 5. and select the checkbox of Show the splash page on startup.

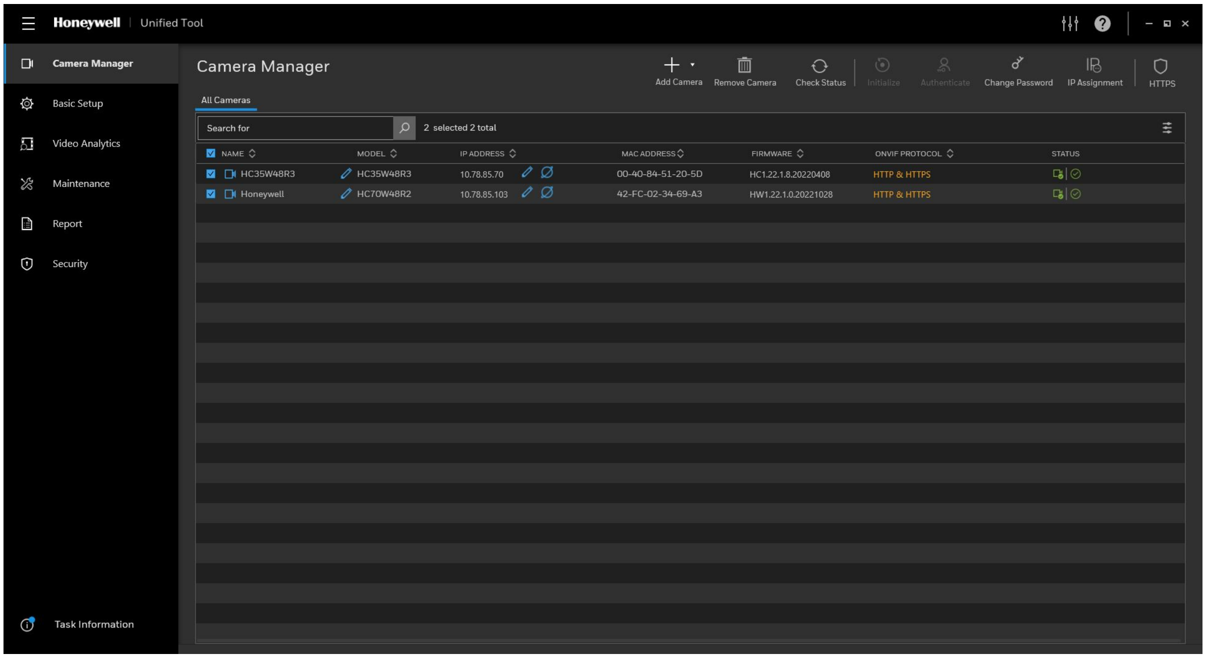
4. Click + Add Camera on the main page and select Auto discover/IP address/From file on the drop list to discover the cameras.

Figure 5 Discover Cameras



After the discovering, all discovered devices in the same subnet and different subnet will be displayed in the devices list.

Figure 6 Device List



Camera Manager

2 selected 2 total

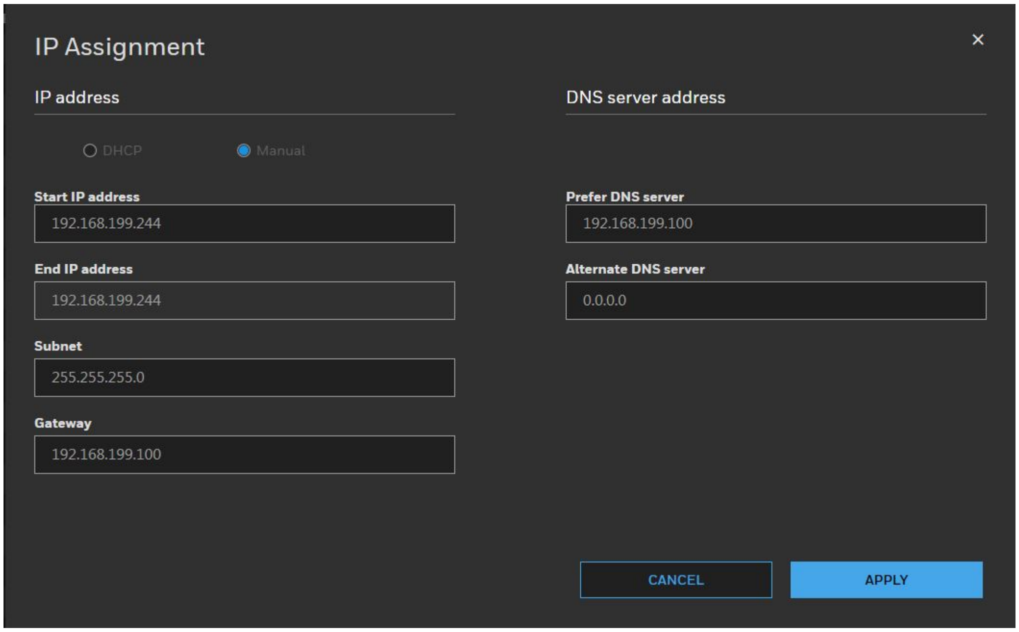
NAME	MODEL	IP ADDRESS	MAC ADDRESS	FIRMWARE	ONVIF PROTOCOL	STATUS
☑ HC35W48R3	HC35W48R3	10.78.85.70	00-40-84-51-20-5D	HC1.22.1.8.20220408	HTTP & HTTPS	✓
☑ Honeywell	HC70W48R2	10.78.85.103	42-FC-02-34-69-A3	HW1.22.1.0.20221028	HTTP & HTTPS	✓

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 5, click IP Assignment and the following figure is displayed:

Figure 7 IP Assignment



IP Assignment

IP address

○ DHCP ● Manual

Start IP address: 192.168.199.244

End IP address: 192.168.199.244

Subnet: 255.255.255.0

Gateway: 192.168.199.100

DNS server address

Prefer DNS server: 192.168.199.100

Alternate DNS server: 0.0.0.0

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

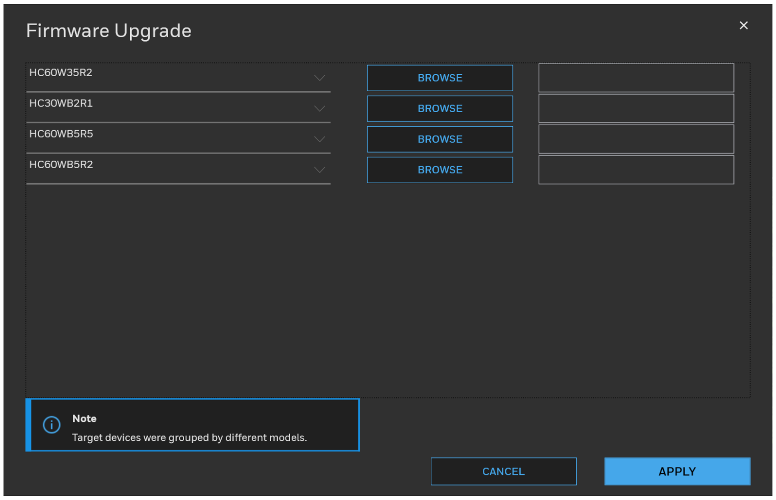
Configure the DNS server address and click **APPLY**.

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 5, select target device(s) and click Firmware Update and the following window is displayed:

Figure 8 Firmware Upgrade



Firmware Upgrade

HC60W35R2

HC30WB2R1

HC60WB5R5

HC60WB5R2

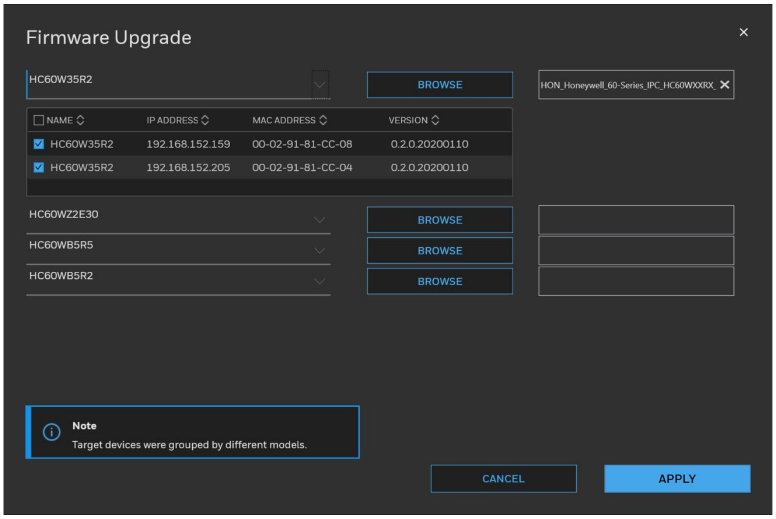
Note

Target devices were grouped by different models.

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 9 Firmware Upgrade 2



Firmware Upgrade

HC60W35R2

HON_Honeywell_60-Series_IPC_HC60WXXRX_

☐ NAME	IP ADDRESS	MAC ADDRESS	VERSION
☑ HC60W35R2	192.168.152.159	00-02-91-81-CC-08	0.2.0.20200110
☑ HC60W35R2	192.168.152.205	00-02-91-81-CC-04	0.2.0.20200110

HC60WZ2E30

HC60WB5R5

HC60WB5R2

Note
Target devices were grouped by different models.

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 6.

CHAPTER

3

LOGGING IN & 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

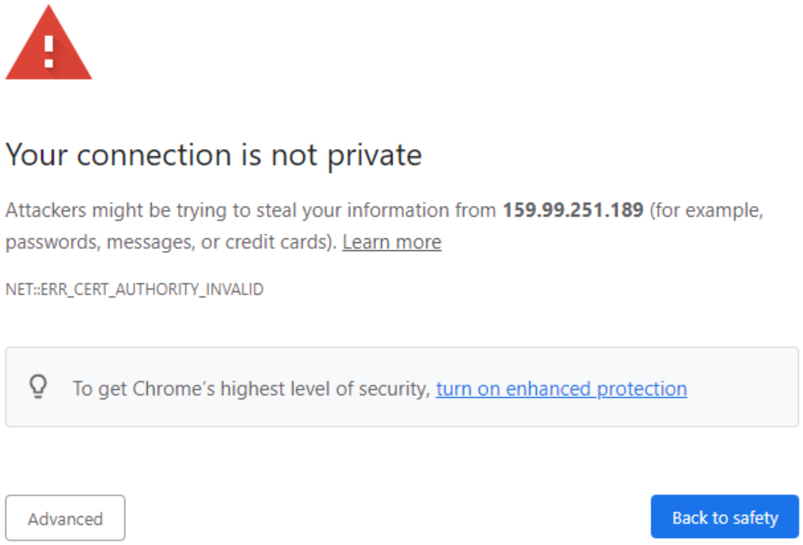
Logging in Via Google Chrome/Edge

1. Type the camera's IP address in the address bar of the browser and press Enter on the keyboard. For example, if your camera's IP address is 159.99.251.189, you would type https://159.99.251.189.

Note: *Chrome/Edge 88.0 (or later) is supported.*

2. The following window is displayed. Click Advanced.

Figure 10 Safety Problem



Your connection is not private

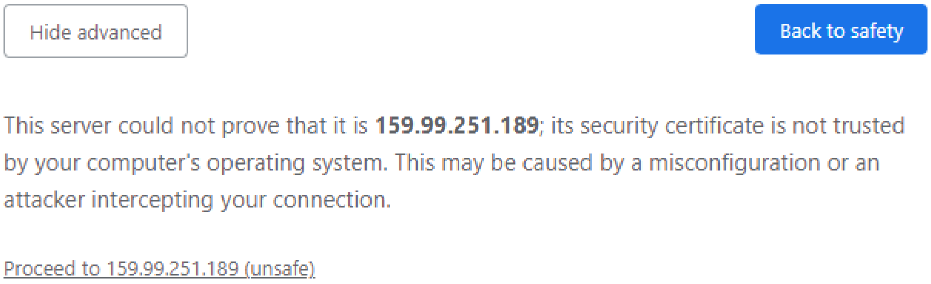
Attackers might be trying to steal your information from **159.99.251.189** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

To get Chrome's highest level of security, turn on enhanced protection

3. The following window is displayed. Click Proceed to 159.99.251.189 (unsafe).

Figure 11 Security Certificate Problem



This server could not prove that it is **159.99.251.189**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

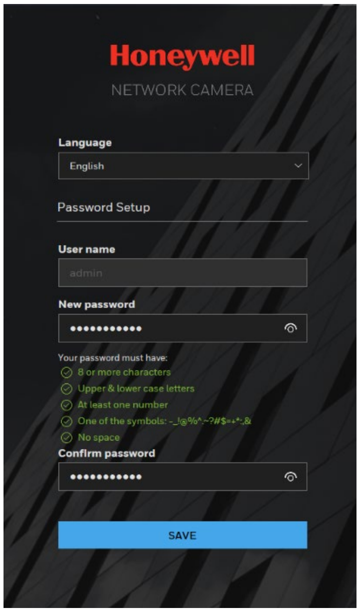
Proceed to 159.99.251.189 (unsafe)

For how to resolve the security certificate problem, see Export CA Certificate on page 74.

4. Setup a new password according to the password requirements at the first login. Click SAVE.

   The password cannot be blank.

Figure 12 Change Password



Language: English

Password Setup

User name: admin

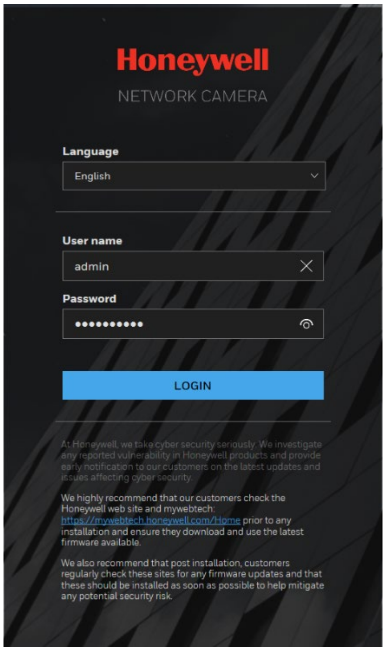
New password: ●●●●●●●●●●●

Your password must have:
- ✓ 8 or more characters
- ✓ Upper & lower case letters
- ✓ At least one number
- ✓ One of the symbols: -_!@%^.~?#$=+*:;&
- ✓ No space

Confirm password: ●●●●●●●●●●●

5. Enter the user name as admin and newly created password. Click LOGIN.

Figure 13 Login Page



Language: English

User name: admin

Password: ●●●●●●●●●●

At Honeywell, we take cyber security seriously. We investigate any reported vulnerability in Honeywell products and provide early notification to our customers on the latest updates and issues affecting cyber security.

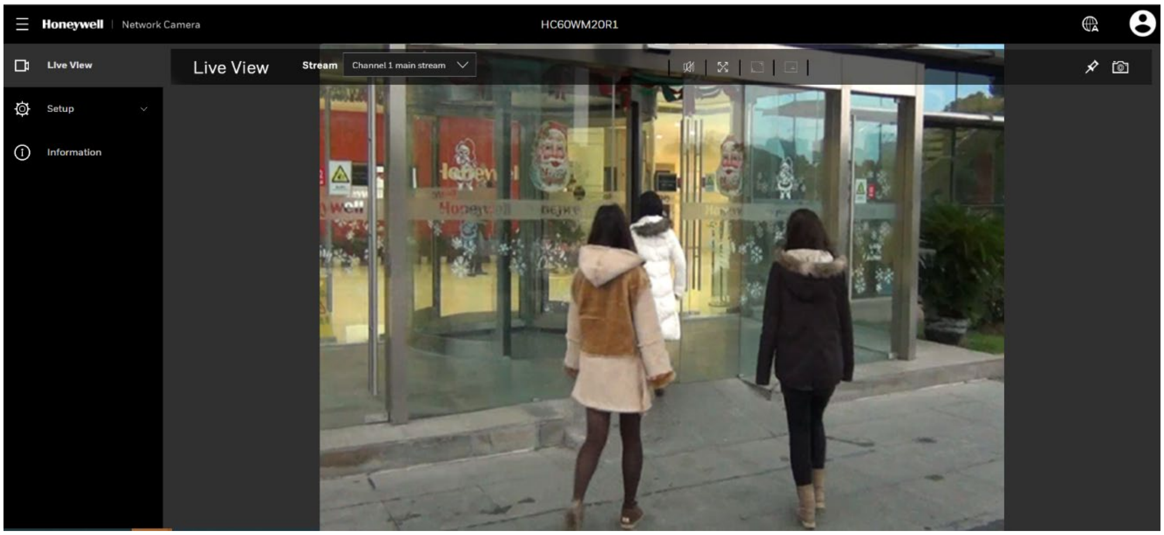
We highly recommend that our customers check the Honeywell web site and mywebtech: https://mywebtech.honeywell.com/Home prior to any installation and ensure they download and use the latest firmware available.

We also recommend that post installation, customers regularly check these sites for any firmware updates and that these should be installed as soon as possible to help mitigate any potential security risk.

Using the Main Page

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

Figure 14 Main Page



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 **Channel 1/2/3/4 main stream or Channel 1/2/3/4 sub 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.

The properties for each stream type are configured on the **Setup → Camera Setup → Video** page (see Configuring Video Settings on page 20).

Camera Name

You can change the camera name according to your needs. For more information, see Configuring System General Settings on page 69.

Live View Tool Bar

From the Live View toolbar, the controls are described in more details below.

Figure 15 Live View Window Controls

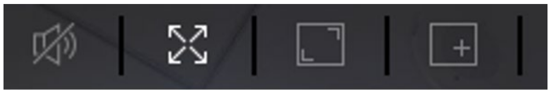


Table 1 Live View Window Controls

Icon	Description
🔊	Click to turn on the audio to listen to the monitoring site. Click it again to turn off the audio. (The audio button is grey 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.
⛶	This function is not applicable for the current version. Click to auto fit the image.
⊞	This function is not applicable for the current version. Click and uncheck **Disable digital zoom** to enable the zoom operation. The navigation screen shows the part of the image being magnified. To resize the navigation area, put the cursor on a border and 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.

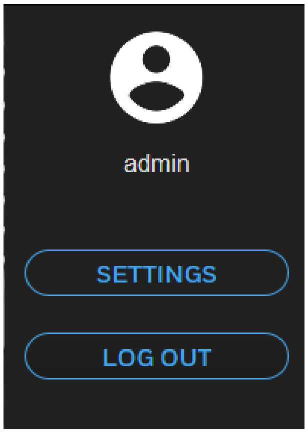
Language

To switch a language, click 🌐 as shown in Figure 14.

User Account

To configure user account or log out the current account, click 👤 as shown in Figure 14 and the following figure is displayed:

Figure 16 User Account



To configure the user account, click **SETTINGS**. For details, see Configuring User Accounts Settings on page 75.

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

CHAPTER

4

CONFIGURING CAMERA SETTINGS

This chapter contains the following sections:

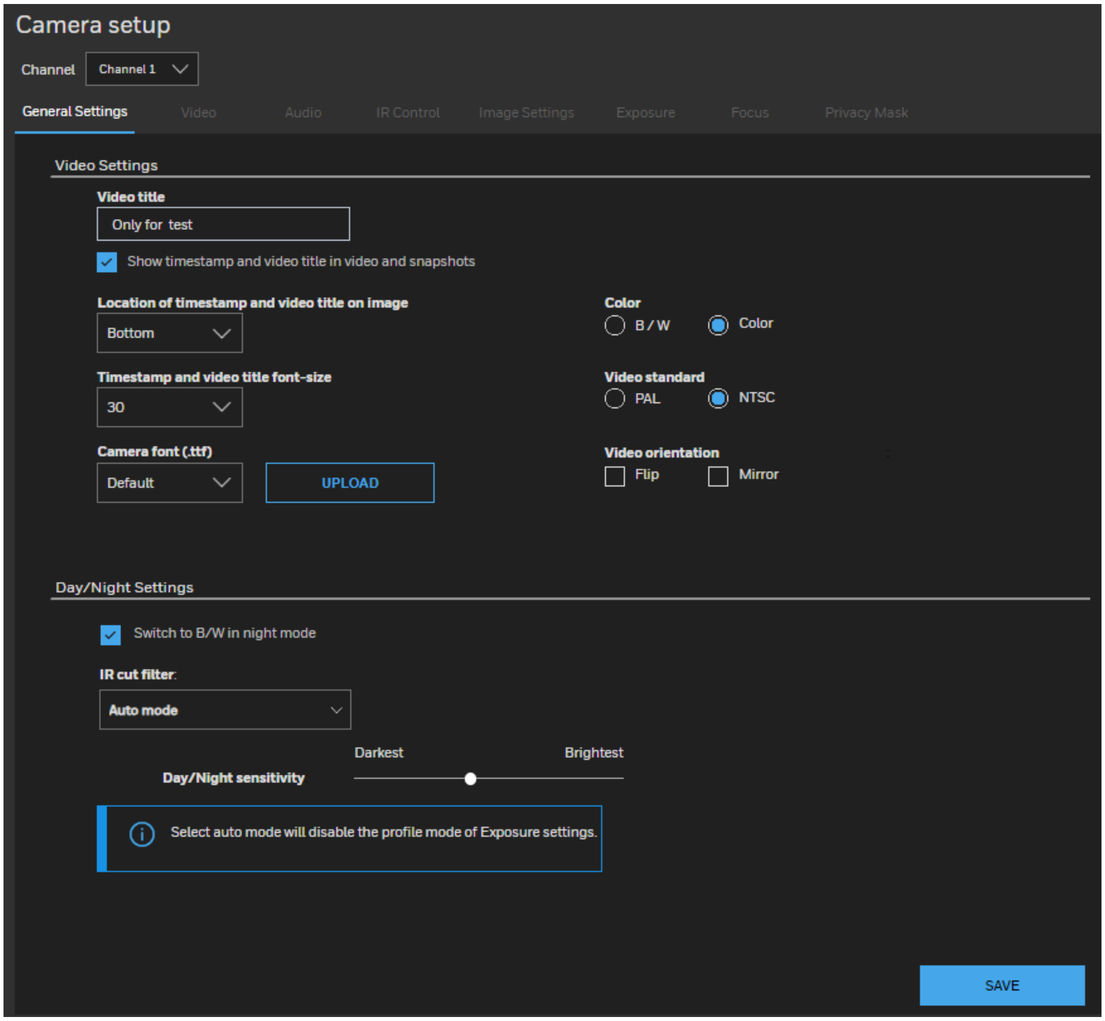
Note: *Click SAVE to enable the settings after you completed the settings on each page.*

Configuring General Settings

Go to **Setup →Camera Setup**. Select Channel information with Channel 1/2/3/4. Each channel is independent, and can be configured with different settings as below.

Go to **General Settings**. On this page, you can configure the general video settings and day/night settings.

Figure 17 General Settings



Channel: Channel 1

Video Settings

Video title: Only for test

☑ Show timestamp and video title in video and snapshots

Location of timestamp and video title on image: Bottom

Timestamp and video title font-size: 30

Camera font (.ttf): Default

Color: ○ B / W ● Color

Video standard: ○ PAL ● NTSC

Video orientation: □ Flip □ Mirror

Day/Night Settings

☑ Switch to B/W in night mode

IR cut filter: Auto mode

Day/Night sensitivity: Darkest — Brightest

Select auto mode will disable the profile mode of Exposure settings.

Video Settings

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

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

Location of timestamp 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.

Timestamp 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.

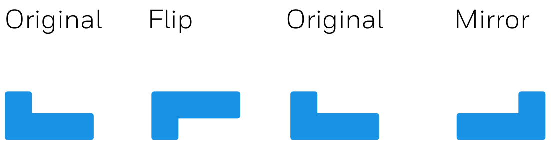
Video Standard: Select the video standard: NTSC or PAL.

Note: *If the video standard is changed, you must disconnect and reconnect the power cord of the camera 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.

Figure 18 Video Orientation



Note: *The flip/mirror 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.

IR cut filter:

- **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.
- **Synchronize with digital input**

  The camera switches between day mode and night mode synchronizing with digital input 1 (Alarm in).

- **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.

  Day/Night sensitivity: Adjust the responsiveness of the IR filter to lighting conditions within Darkest and Brightest.

Configuring Video Settings

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

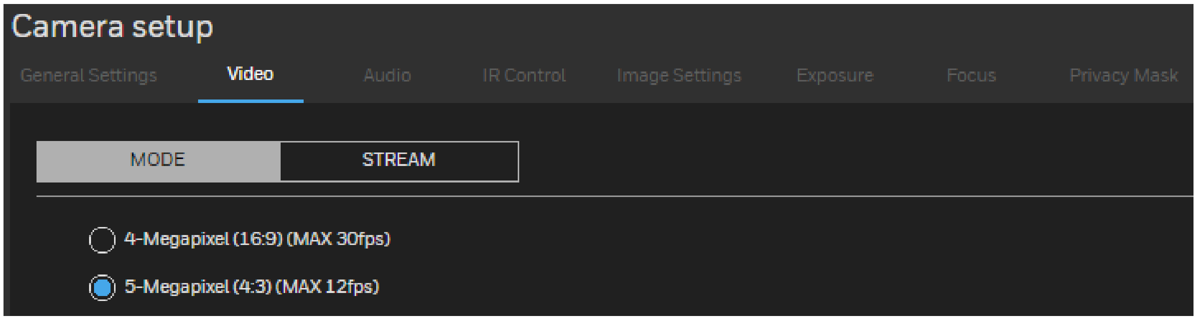
This section describes how to configure viewing window and video streaming properties (format, resolution, frame rate, bit rate, I-frame interval, etc.).

Mode

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

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

Figure 19 Mode Tab 1



○ 4-Megapixel (16:9) (MAX 30fps)

● 5-Megapixel (4:3) (MAX 12fps)

4-Megapixel (16:9) (MAX 30fps): Select it and the maximum resolution will be 2560x1440. The aspect ratio will be 16:9.

5-Megapixel (4:3) (MAX 12fps): Select it and the maximum resolution will be 2560x1920. The aspect ratio will be 4:3.

Video Stream

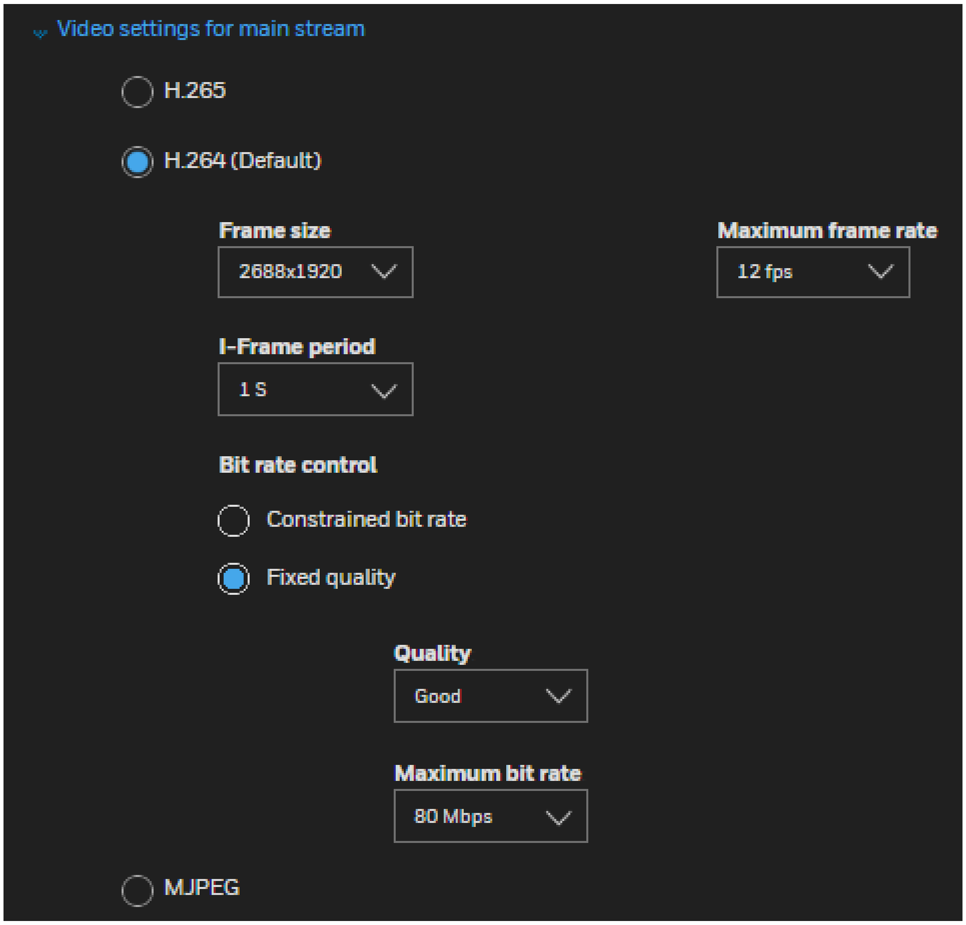
Go to **Setup →Camera Setup → Video→ Stream**. Select **Channel** information with **Channel 1/2/3/4**. Each channel is independent, and can be configured with different settings as below.

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

Table 2 Stream and Frame Size Matrix for Channel 1/2/3/4

Model	Main Stream	Sub Stream
HC60WM20R1	**5M:** 2688 x 1920, 2560 x 1920, 2160 x 1536, 2048 x 1536, 1680 x 1200, 1600 x 1200, 1344 x 960, 1280 x 960, 672 x 480, 640 x 480, MAX 12 fps @ 5 M mode **4M:** 2560 x 1440, 1920 x 1080, 1280 x 720, 640 x 360, MAX 25/30 fps @ 4 M mode	**5M:** 1280 x 960, 672 x 480, 640 x 480, MAX 12 fps @ 5 M mode **4M:** 1280 x 720, 640 x 360, MAX 25/30 fps @ 4 M mode

Figure 20 Video Stream



Video settings for main stream

○ H.265

● H.264 (Default)

Frame size: 2688x1920

Maximum frame rate: 12 fps

I-Frame period: 1 S

Bit rate control

○ Constrained bit rate

● Fixed quality

Quality: Good

Maximum bit rate: 80 Mbps

○ MJPEG

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 1-25 fps. If the power line frequency is set to NTSC, the frame rates are selectable from 1-30 fps. You can also select **Customized** and manually enter a value.

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

It is recommended to set 25 fps for all channels when the WDR enabled. The limitation is listed as below.

Table 3 Maximum Frame Rate Limitation

WDR On/Off	**Maximum Frame Rate(fps)**				**Recommend**
	ch1	**ch2**	**ch3**	**ch4**	
Off	30	30	30	30	Yes
On	25	25	25	25	Yes
On	30	30	20	20	Yes
On	30	30	25	25	Yes
On	30	30	30	10	Yes
On	30	30	30	20	Yes
On	30	30	30	24	Yes
On	30	30	30	25	No
On	30	30	30	30	No

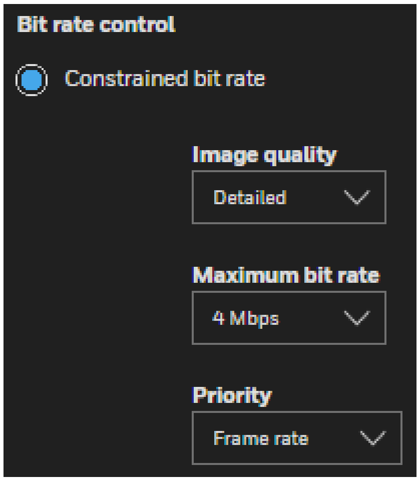
I-frame Period

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.

Bit rate control

Constrained Bit Rate

Figure 21 Constrained Bit Rate



Bit rate control

● Constrained bit rate

Image quality: Detailed

Maximum bit rate: 4 Mbps

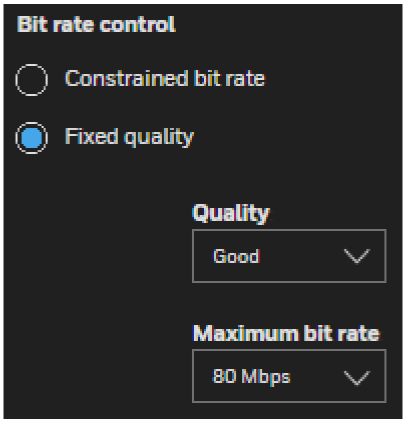
Priority: Frame rate

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

Figure 22 Fixed Quality



Bit rate control

○ Constrained bit rate

● Fixed quality

Quality: Good

Maximum bit rate: 80 Mbps

All frames are transmitted with the same quality.

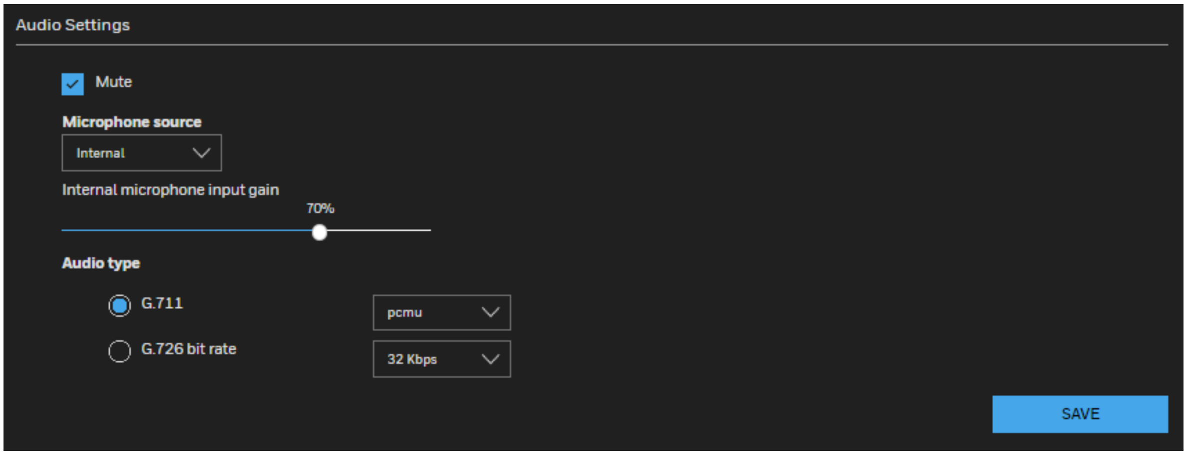
- **Quality**: Select a desired quality ranging from **Medium** to **Excellent**. If you select **Customized**, you can enter a value to specify the quality.
- **Maximum bit rate**: Select a bit rate from the dropdown list. The bit rate ranges from 1 Mbps to a maximum of 80Mbps. If you select Customized, 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 23 Audio



Audio Settings

☑ Mute

Microphone source

Internal

Internal microphone input gain

70%

Audio type

● G.711 pcmu

○ G.726 bit rate 32 Kbps

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

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

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).

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 bit rate.

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

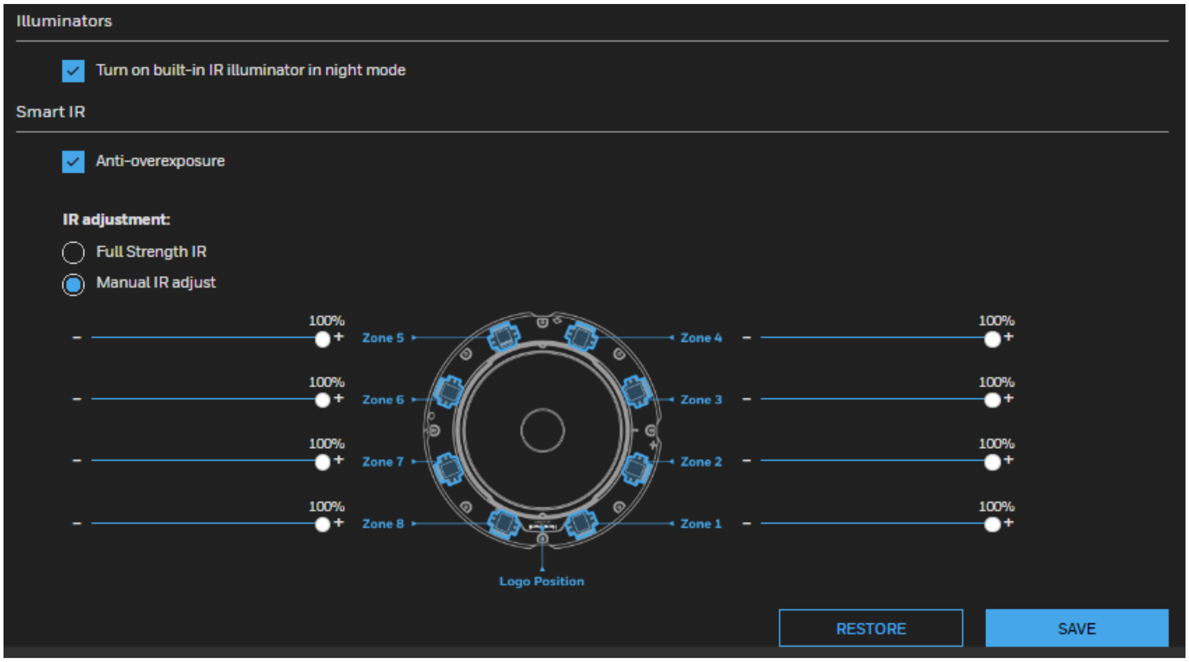
After you complete the settings on this page, click **SAVE** to enable the settings.

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 24 IR Control Settings



Illuminators

☑ Turn on built-in IR illuminator in night mode

Smart IR

☑ Anti-overexposure

IR adjustment:

○ Full Strength IR

● Manual IR adjust

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.

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.

- **Full Strength IR**: Select it to control the luminance of IR lights automatically with full strength IR.
- **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.

Configuring Image Settings

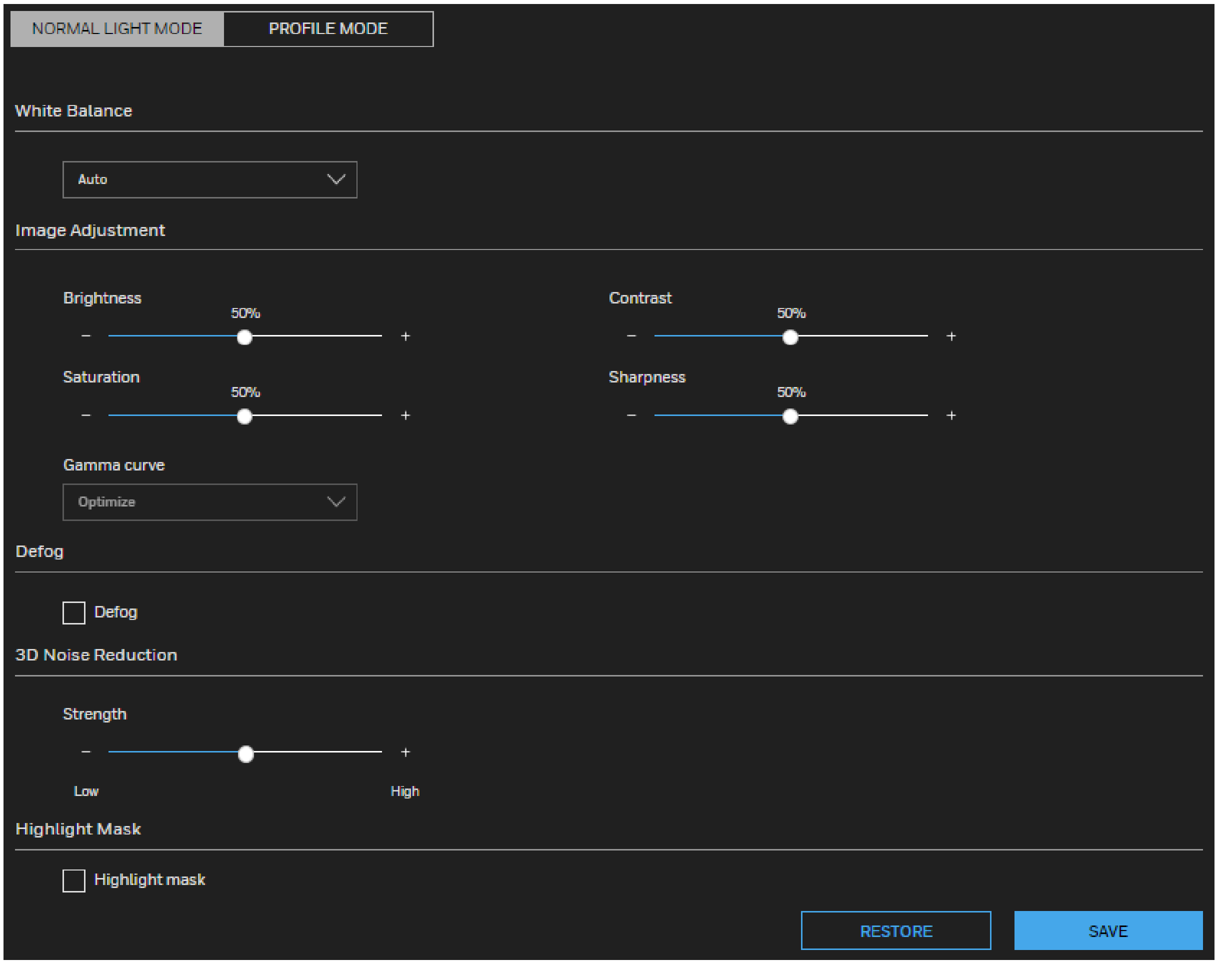
Go to **Setup →Camera Setup → Image Settings**.

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 25 Image Settings



White Balance

Auto

Image Adjustment

Brightness 50%

Contrast 50%

Saturation 50%

Sharpness 50%

Gamma curve

Optimize

Defog

□ Defog

3D Noise Reduction

Strength

Low High

Highlight Mask

□ Highlight mask

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.*
- *The brightness setting from 0% to 100% doesn't have obvious change due to the limitation of Sony senor.*

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.*

Highlight Mask

Check to mask the overexposed zone in the images to decrease the uncomfortableness for monitoring.

Configuring Exposure Settings

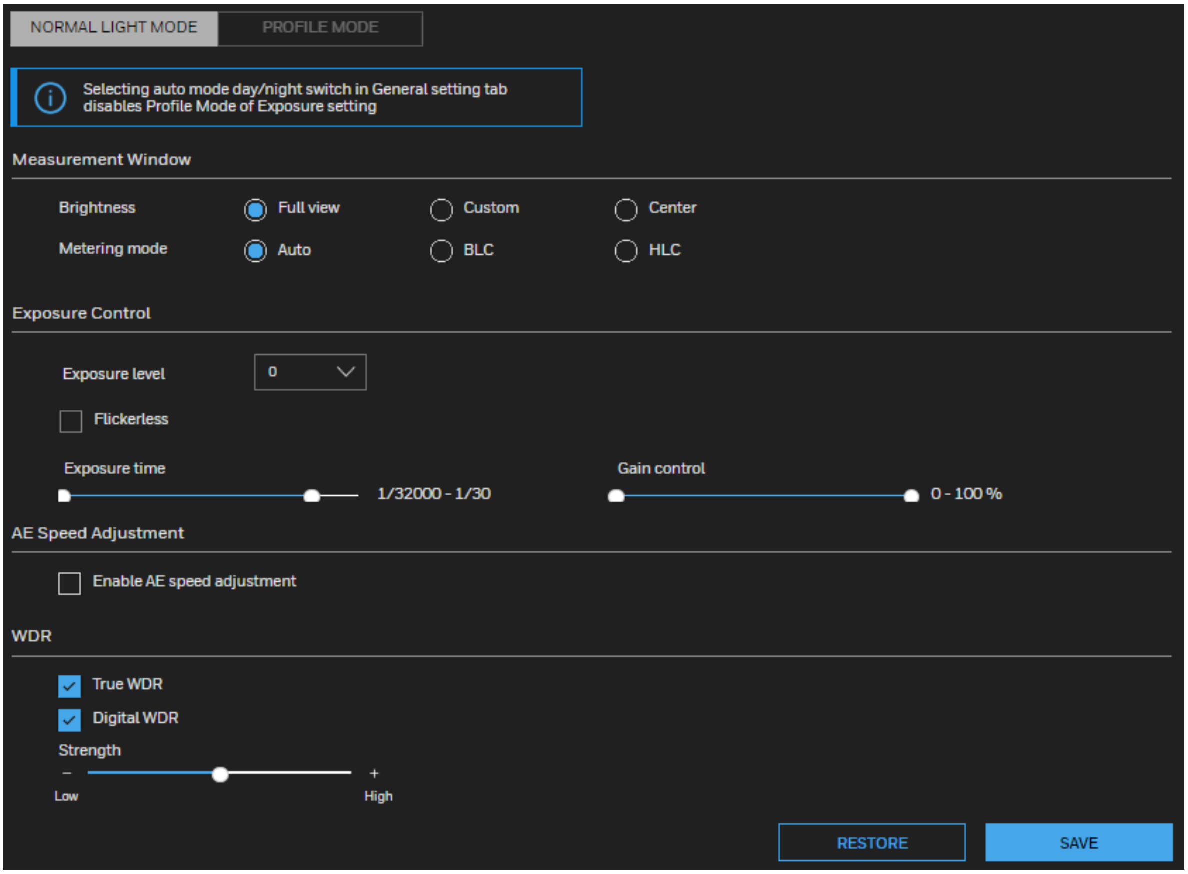
Go to **Setup →Camera Setup → Exposure**.

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 26 Configure Exposure



NORMAL LIGHT MODE | PROFILE MODE

Selecting auto mode day/night switch in General setting tab disables Profile Mode of Exposure setting

Measurement Window

Brightness ● Full view ○ Custom ○ Center

Metering mode ● Auto ○ BLC ○ HLC

Exposure Control

Exposure level 0

□ Flickerless

Exposure time 1/32000 - 1/30

Gain control 0 - 100 %

AE Speed Adjustment

□ Enable AE speed adjustment

WDR

☑ True WDR

☑ Digital WDR

Strength

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.

Brightness:

- **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.

Metering mode:

- **Auto:** The algorithm chooses the best metering strategy
- **BLC:** This metering method increases the weight of dark area

- **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~+2.0 (dark to bright).

Flickerless: Check to reduce flicker in the image.

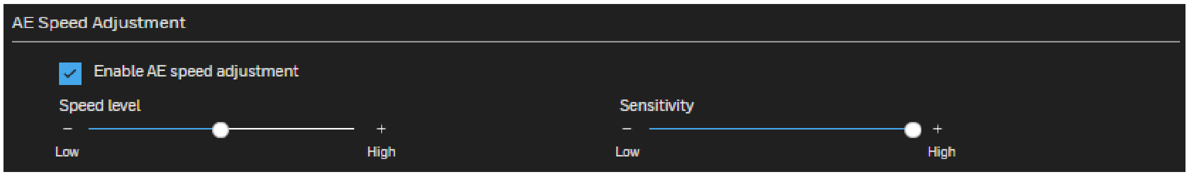
You can drag the slider of **Exposure time** and **Gain Control** to get the best image quality.

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.

You can drag the slider of **Speed level** and **Sensitivity** to get the best image quality.

Figure 27 AE Speed Adjustment

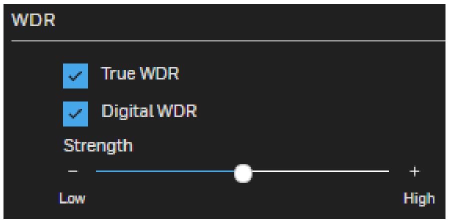


AE Speed Adjustment

☑ Enable AE speed adjustment

WDR

Figure 28 WDR



WDR

☑ True WDR

☑ Digital 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**).

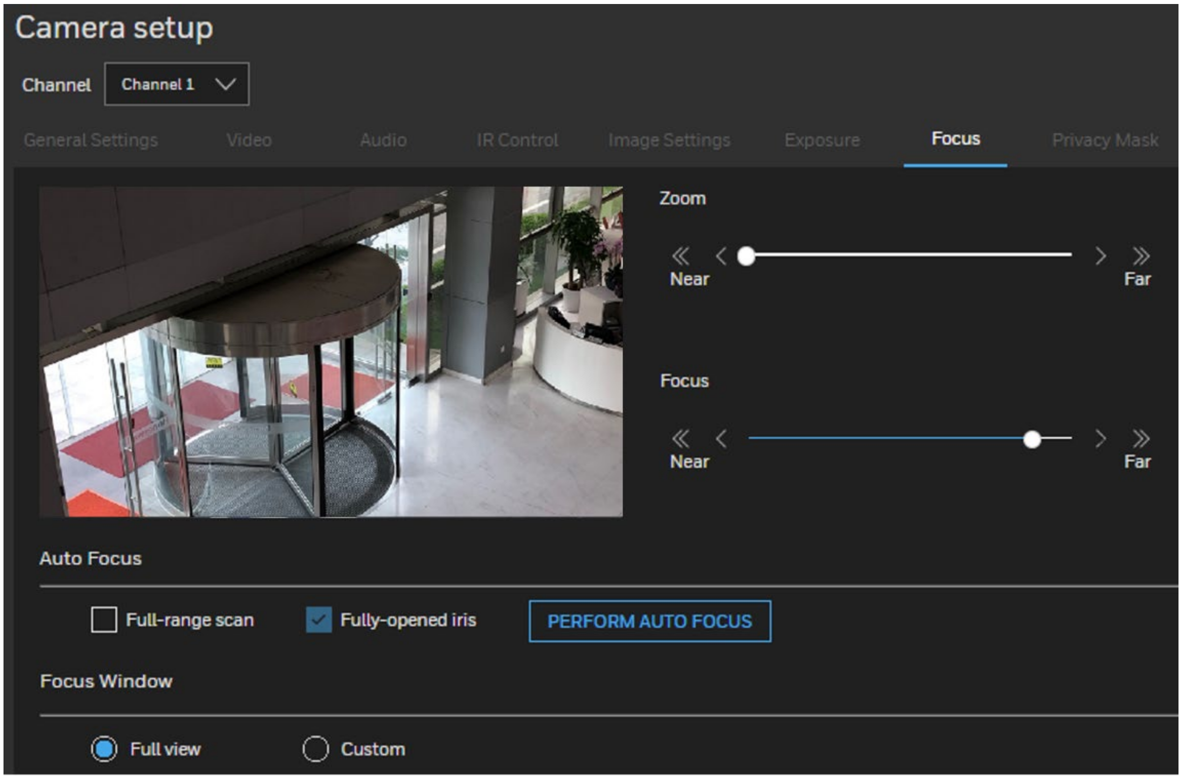
Digital WDR is a software-based technique that enhances the image quality by adjusting the gamma value to brighten dark areas. True WDR is a sensor-based technology. A True WDR CCTV can produce images with an extremely wide dynamic range. The WDR image sensor can capture several images with short and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

Configuring Focus

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 29 Focus



Camera setup

Channel: Channel 1

Auto Focus

□ Full-range scan ☑ Fully-opened iris

Focus Window

● Full view ○ Custom

- 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.*

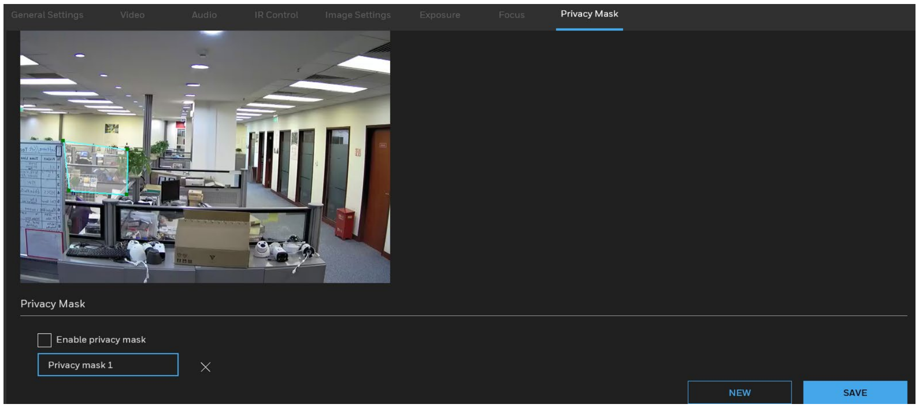
Configuring Privacy Mask

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

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

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 30 Privacy Mask



Note:
- *The setting size of privacy object should be 2.5 times of the object size.*
- *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.*

CHAPTER

5

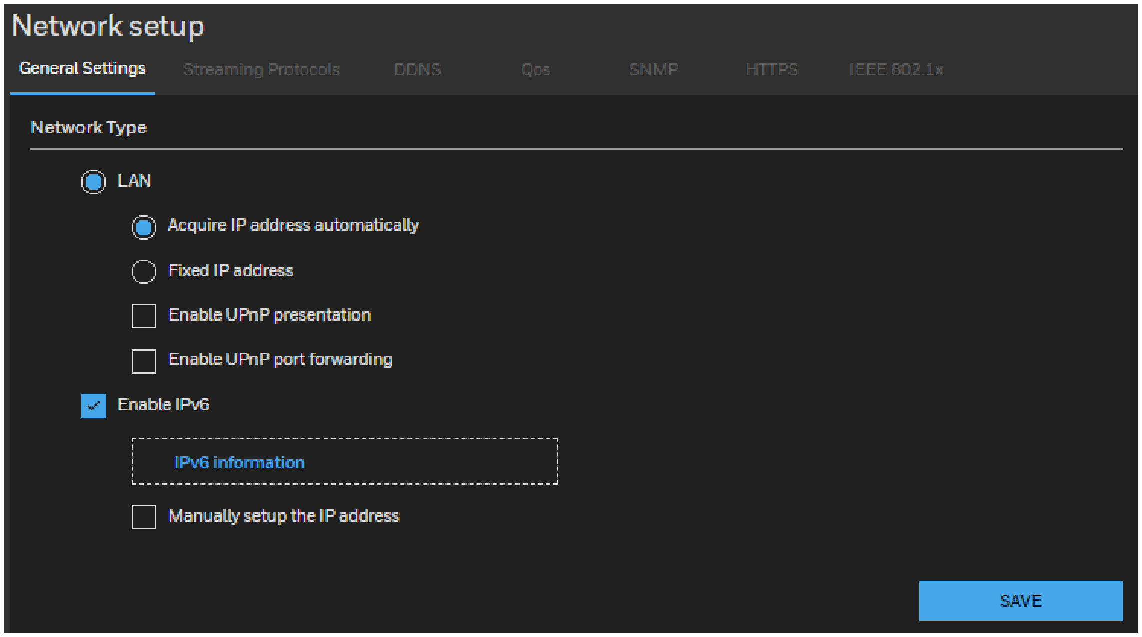
CONFIGURING NETWORK SETTINGS

This chapter contains the following sections:

Configuring Network General Settings

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

Figure 31 Network Type



Network Type

● LAN

● Acquire IP address automatically

○ Fixed IP address

□ Enable UPnP presentation

□ Enable UPnP port forwarding

☑ Enable IPv6

□ Manually setup the IP address

LAN

Acquire 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.

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

- **IP address**:

You can make use of Unified Tool to easily set up the camera on LAN. See Accessing the Camera on page 4.

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 data base 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:

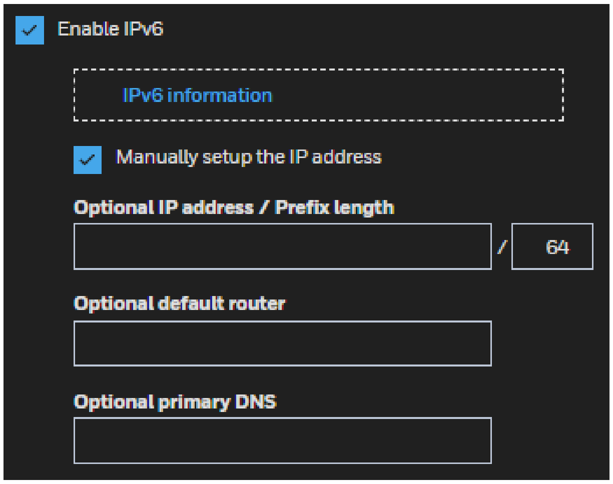
1. Go to Start→ Control Panel→ Network and Sharing Center.

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.

Enable IPv6

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

Figure 32 Enable IPv6



☑ Enable IPv6

IPv6 information

☑ Manually setup the IP address

Optional IP address / Prefix length: / 64

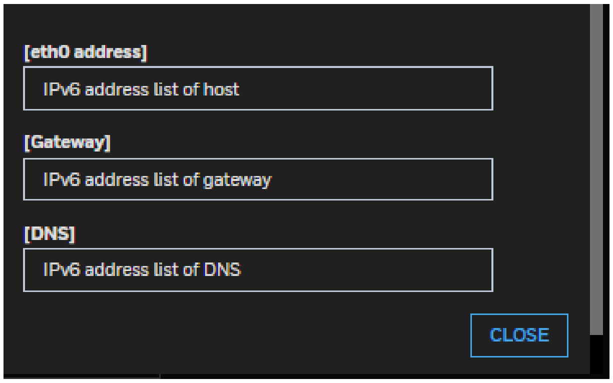
Optional default router

Optional primary DNS

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 33 IPv6 Information



[eth0 address]: IPv6 address list of host

[Gateway]: IPv6 address list of gateway

[DNS]: IPv6 address list of DNS

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

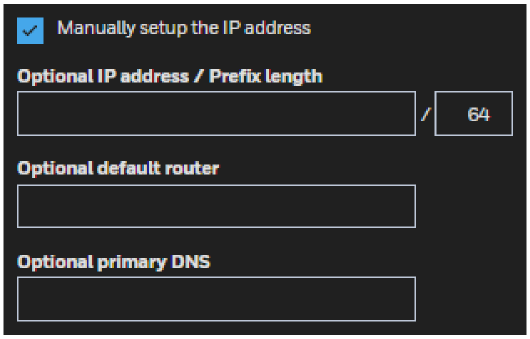
Follow the steps below to link to an IPv6 address:

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 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 34 Manually setup IP Address



☑ Manually setup the IP address

Optional IP address / Prefix length

/ 64

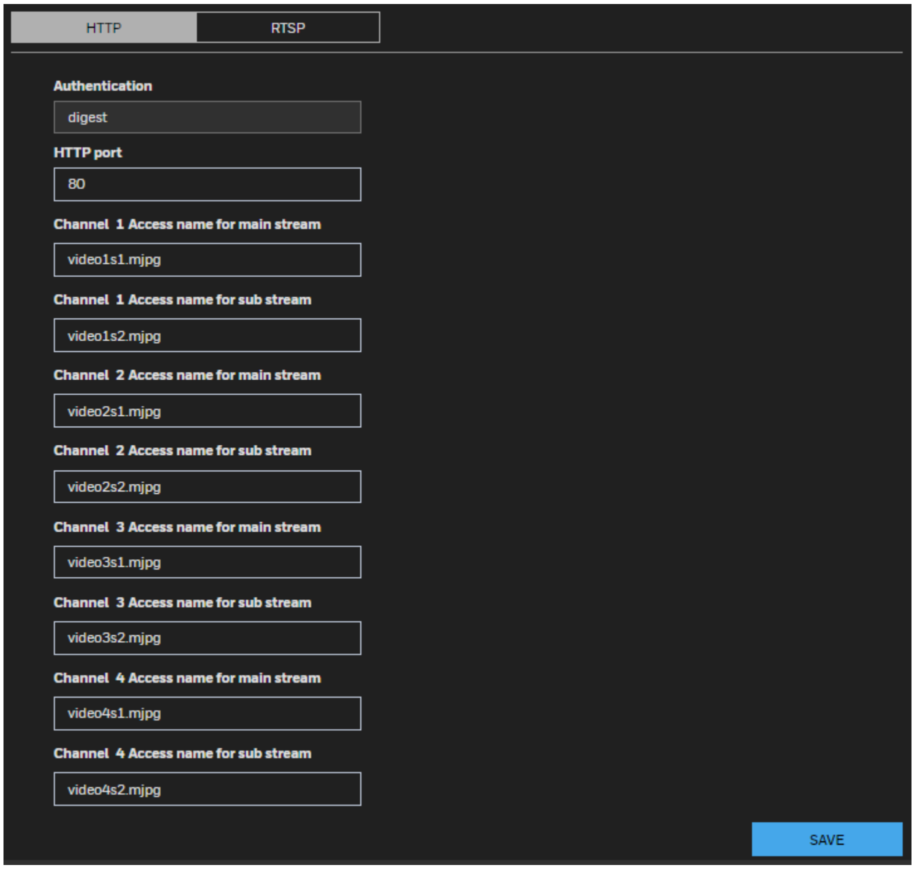
Optional default router

Optional primary DNS

Configuring Streaming Protocols

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

Figure 35 Streaming Protocols - HTTP



Authentication: digest

HTTP port: 80

Channel 1 Access name for main stream: video1s1.mjpg

Channel 1 Access name for sub stream: video1s2.mjpg

Channel 2 Access name for main stream: video2s1.mjpg

Channel 2 Access name for sub stream: video2s2.mjpg

Channel 3 Access name for main stream: video3s1.mjpg

Channel 3 Access name for sub stream: video3s2.mjpg

Channel 4 Access name for main stream: video4s1.mjpg

Channel 4 Access name for sub stream: video4s2.mjpg

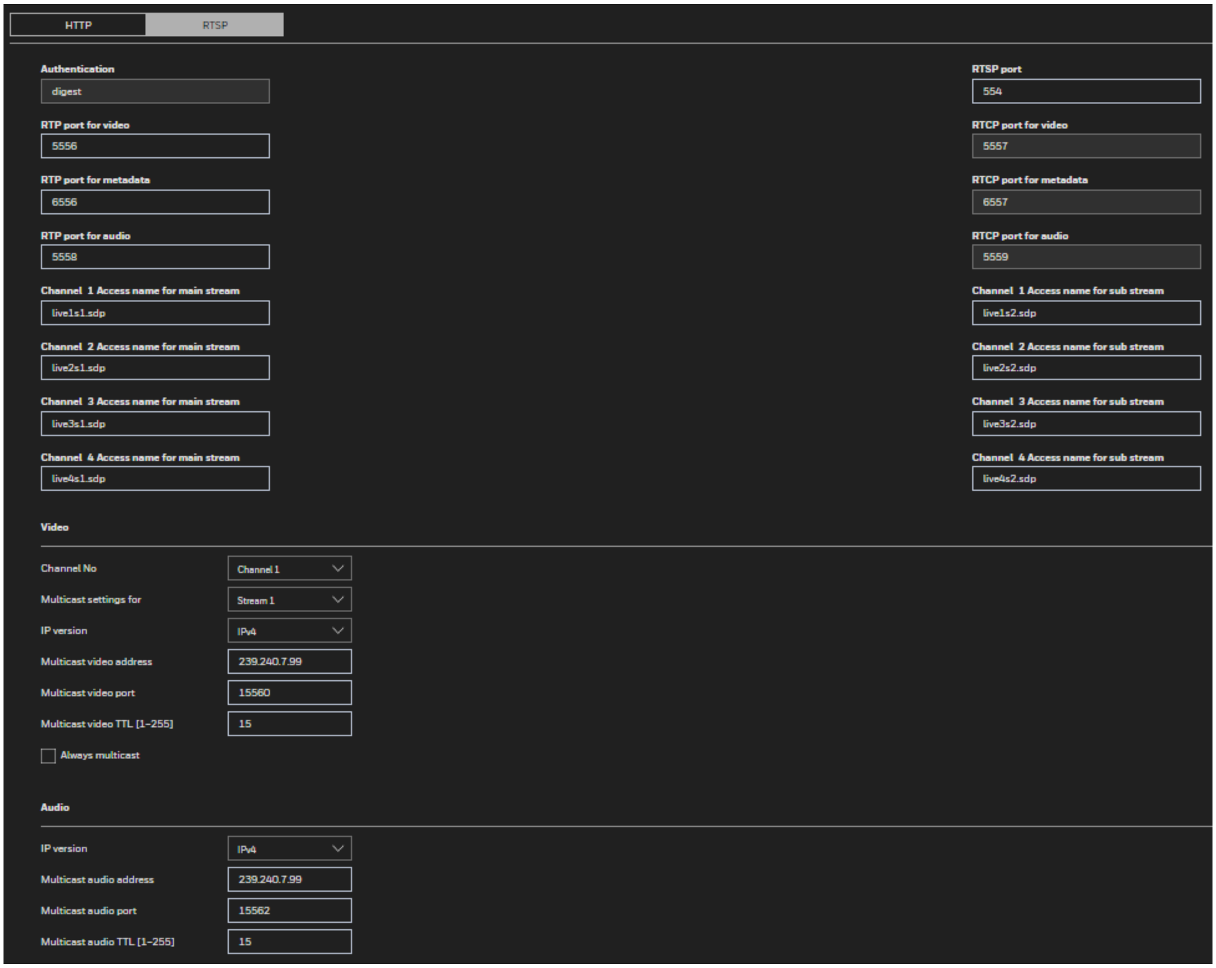
To utilize HTTP authentication, make sure that you have set a password for the camera first. For more information, see Configuring User Accounts Settings on page 75.

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.

Channel 1/2/3/4 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 21.

Figure 36 Streaming Protocols – RTSP



Authentication: digest

RTP port for video: 5556

RTP port for metadata: 6556

RTP port for audio: 5558

Channel 1 Access name for main stream: live1s1.sdp

Channel 2 Access name for main stream: live2s1.sdp

Channel 3 Access name for main stream: live3s1.sdp

Channel 4 Access name for main stream: live4s1.sdp

RTSP port: 554

RTCP port for video: 5557

RTCP port for metadata: 6557

RTCP port for audio: 5559

Channel 1 Access name for sub stream: live1s2.sdp

Channel 2 Access name for sub stream: live2s2.sdp

Channel 3 Access name for sub stream: live3s2.sdp

Channel 4 Access name for sub stream: live4s2.sdp

Video

Channel No: Channel 1

Multicast settings for: Stream 1

IP version: IPv4

Multicast video address: 239.240.7.99

Multicast video port: 15560

Multicast video TTL [1~255]: 15

□ Always multicast

Audio

IP version: IPv4

Multicast audio address: 239.240.7.99

Multicast audio port: 15562

Multicast audio TTL [1~255]: 15

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 75.

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

Channel 1/2/3/4 Access name for main stream/sub 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 is set as below:

live1s1.sdp for channel 1 stream 1

live1s2.sdp for channel 1 stream 2

live2s1.sdp for channel 2 stream 1

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.

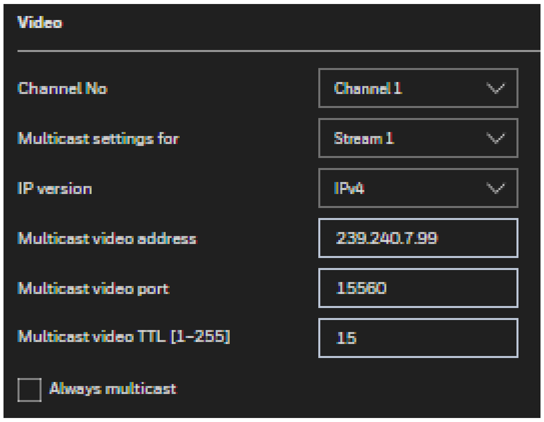
RTCP port for metadata: By default, the RTCP port for video is set to 6557.

RTP port for audio: By default, the RTP port for metadata is set to 5558.

RTCP port for audio: By default, the RTCP port for metadata is set to 5559.

Multicast settings for Stream 1/2: Select Stream 1 or Stream 2 to display the detailed configuration information.

Figure 37 Multicast Settings



Video

Channel No: Channel 1

Multicast settings for: Stream 1

IP version: IPv4

Multicast video address: 239.240.7.99

Multicast video port: 15560

Multicast video TTL [1~255]: 15

□ Always multicast

Always multicast: Check to enable multicast for video streams.

Multicast video/audio address: Enter the Multicast group address.

Multicast video/audio 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.

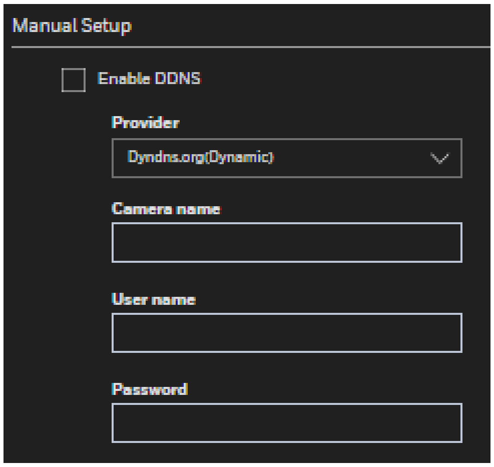
Multicast TTL [1~255]: The multicast TTL (Time To Live) is the value that tells the router the range a packet can be forwarded. The default value is **15**.

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 38 DDNS



Manual Setup

□ Enable DDNS

Provider: Dyndns.org(Dynamic)

Camera name:

User name:

Password:

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.

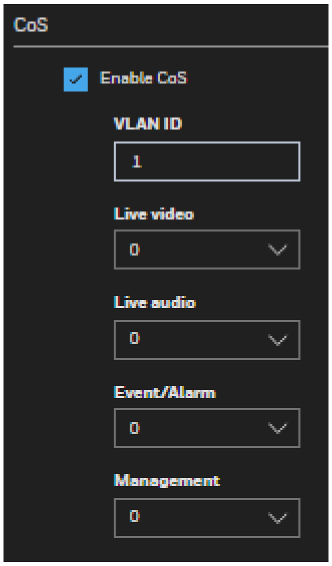
To utilize QoS in a network environment, the following requirements must be met:

- 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 39 Cos



CoS

☑ Enable CoS

VLAN ID

1

Live video

0

Live audio

0

Event/Alarm

0

Management

0

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.

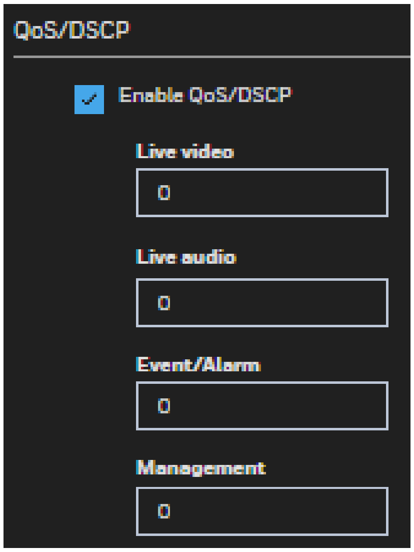
Note:

- *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 40 QoS/DSCP



QoS/DSCP

☑ Enable QoS/DSCP

Live video: 0

Live audio: 0

Event/Alarm: 0

Management: 0

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

Configuring SNMP Settings

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

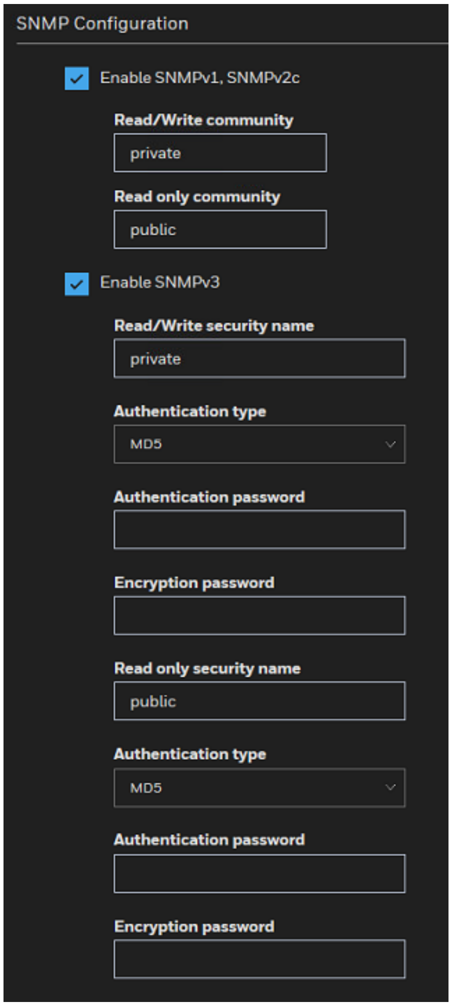
SNMP (Simple Network Management Protocol) is a protocol for collecting, organizing, and exchanging management information between managed devices on a network.

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 41 SNMP Configurations



SNMP Configuration

☑ Enable SNMPv1, SNMPv2c

Read/Write community
private

Read only community
public

☑ Enable SNMPv3

Read/Write security name
private

Authentication type
MD5

Authentication password

Encryption password

Read only security name
public

Authentication type
MD5

Authentication password

Encryption password

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

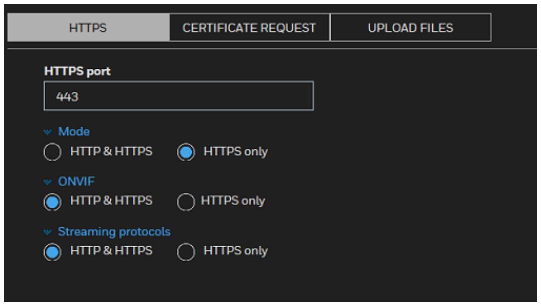
Go to **Setup** →**Network Setup** → **HTTPS**.

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 42 HTTP



HTTPS port: 443

Mode: ○ HTTP & HTTPS ● HTTPS only

ONVIF: ● HTTP & HTTPS ○ HTTPS only

Streaming protocols: ● HTTP & HTTPS ○ HTTPS only

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.

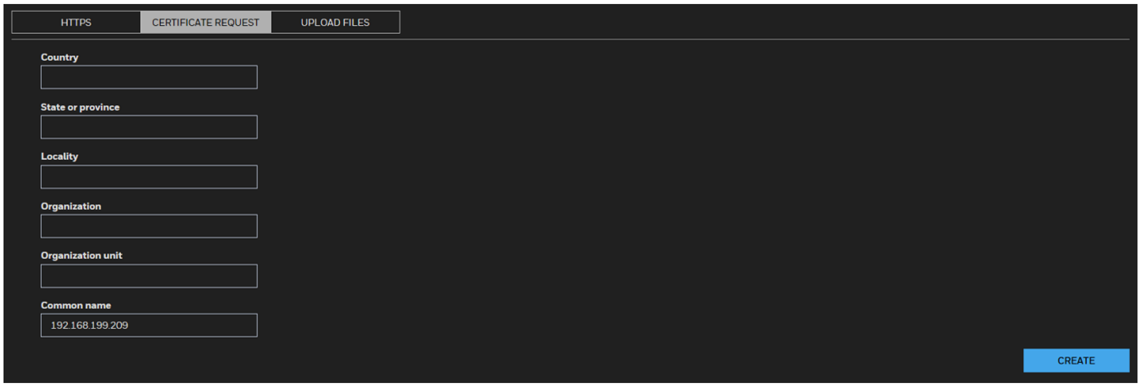
Note: *Honeywell strictly recommends using HTTPS only.*

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 43 Certificate Request



Country:

State or province:

Locality:

Organization:

Organization unit:

Common name: 192.168.199.209

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.

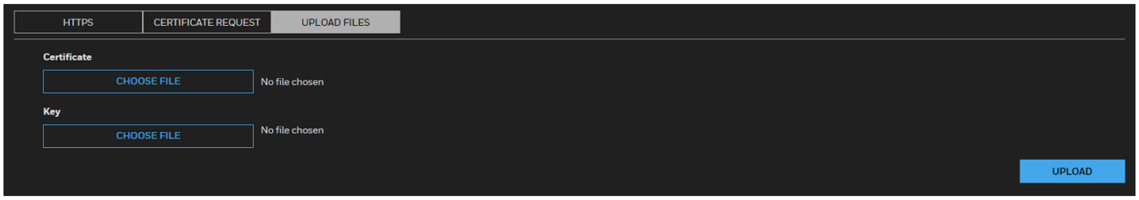
After the certificate file is uploaded successfully, if you want to remove the certificate, click **REMOVE**.

Upload files

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

You can import the certificate from third party here.

Figure 44 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.

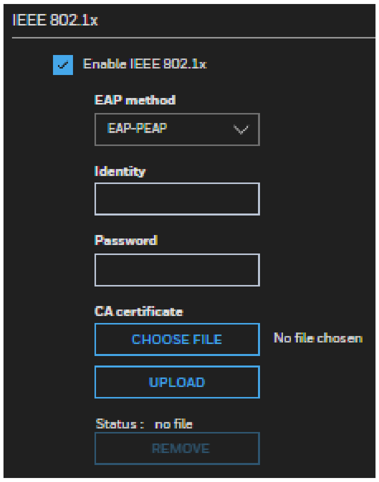
To configure IEEE 802.1x settings:

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 45 IEEE 802.1X Configurations – EAP-PEAP



IEEE 802.1x

☑ Enable IEEE 802.1x

EAP method: EAP-PEAP

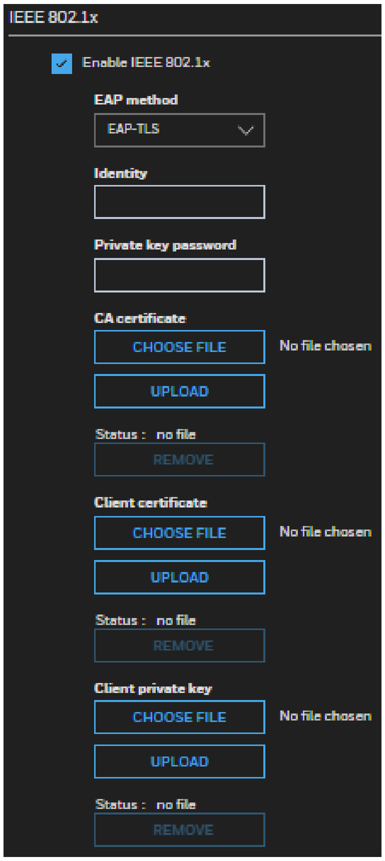
Identity

Password

CA certificate

Status : no file

Figure 46 IEEE 802.1X Configurations – EAP-TLS



IEEE 802.1x

☑ Enable IEEE 802.1x

EAP method: EAP-TLS

Identity

Private key password

CA certificate

Status : no file

Client certificate

Status : no file

Client private key

Status : no file

3. 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).

4. 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.

CHAPTER

6 CONFIGURING VIDEO ANALYTICS

This chapter contains the following sections:

Configuring Motion Detection Settings

Go to **Setup →Video Analytics → Motion Detection**. Select Channel information with Channel 1/2/3/4. Each channel is independent, and can be configured with different settings as below.

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

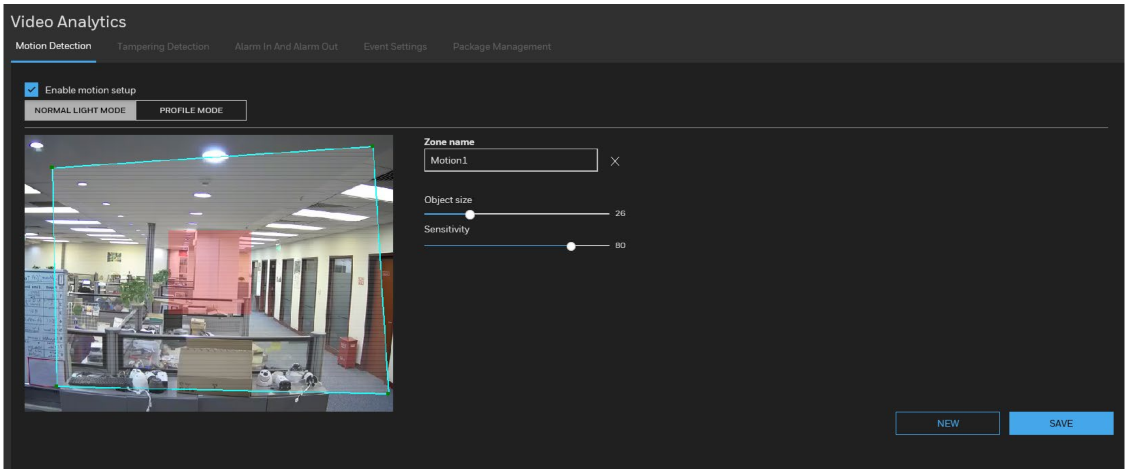
change the shape of the detection area by dragging the corner points.

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 47 Configuring Motion Detection Settings



☑ Enable motion setup

Zone name: Motion1 ✕

Object size: 26

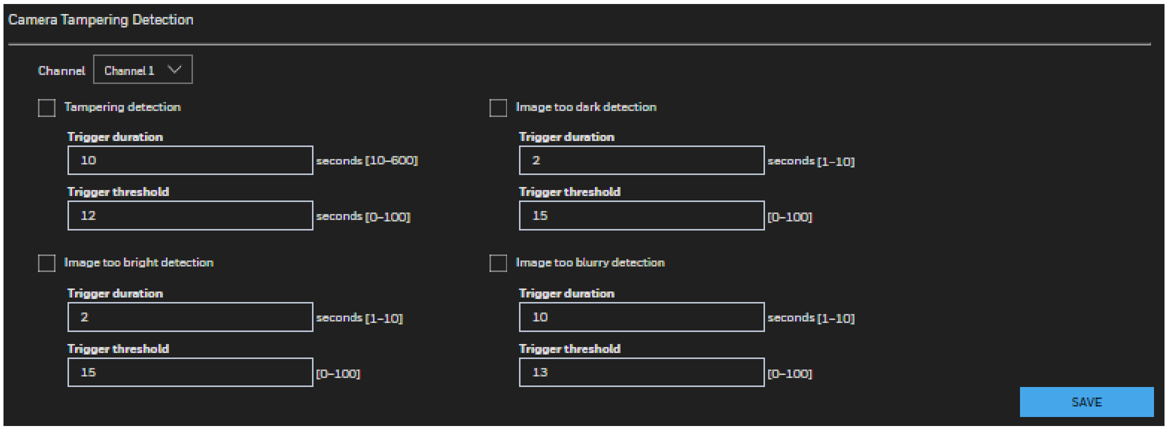
Sensitivity: 80

Configuring Tampering Detection Settings

Go to **Setup →Video Analytics → Tampering Detection**. Select Channel information with Channel 1/2/3/4. Each channel is independent, and can be configured with different settings as below.

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

Figure 48 Tampering Detection Configurations



Camera Tampering Detection

Channel: Channel 1

□ Tampering detection

Trigger duration: 10 seconds [10-600]

Trigger threshold: 12 seconds [0-100]

□ Image too dark detection

Trigger duration: 2 seconds [1-10]

Trigger threshold: 15 [0-100]

□ Image too bright detection

Trigger duration: 2 seconds [1-10]

Trigger threshold: 15 [0-100]

□ Image too blurry detection

Trigger duration: 10 seconds [1-10]

Trigger threshold: 13 [0-100]

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.

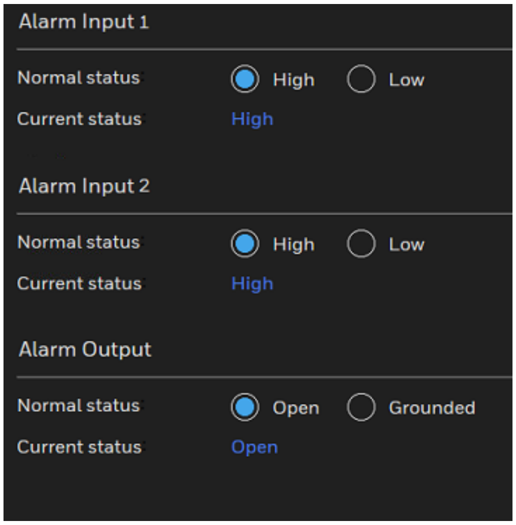
Trigger threshold: It determines how sensitive the tamper detection setting is. The lower the threshold value, the easier the detection is triggered.

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 55.

Configuring Alarm In and Alarm Out

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

Figure 49 Alarm In and Alarm Out



Alarm Input 1

Normal status ● High ○ Low

Current status High

Alarm Input 2

Normal status ● High ○ Low

Current status High

Alarm Output

Normal status ● Open ○ Grounded

Current status Open

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 55.

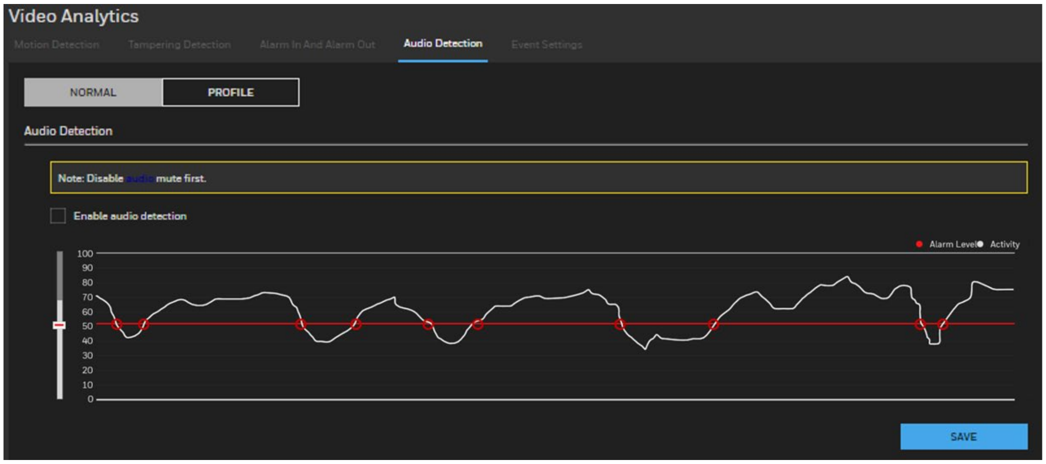
Configuring Audio Detection

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

Audio detection, along with video motion detection, is applicable in the following scenarios:

- Detection of activities not covered by camera view, e.g., a loud input by gun shots or breaking a door/ window.
- A usually noisy environment, such as a factory, suddenly becomes quiet due to a breakdown of machines.
- Dark environments where video motion detection may not function well.

Figure 50 Audio Detection: NORMAL Tab



Note: Disable audio mute first.

☐ Enable audio detection

The red circles indicate where the audio alarms can be triggered when exceeding or falling below the preset threshold.

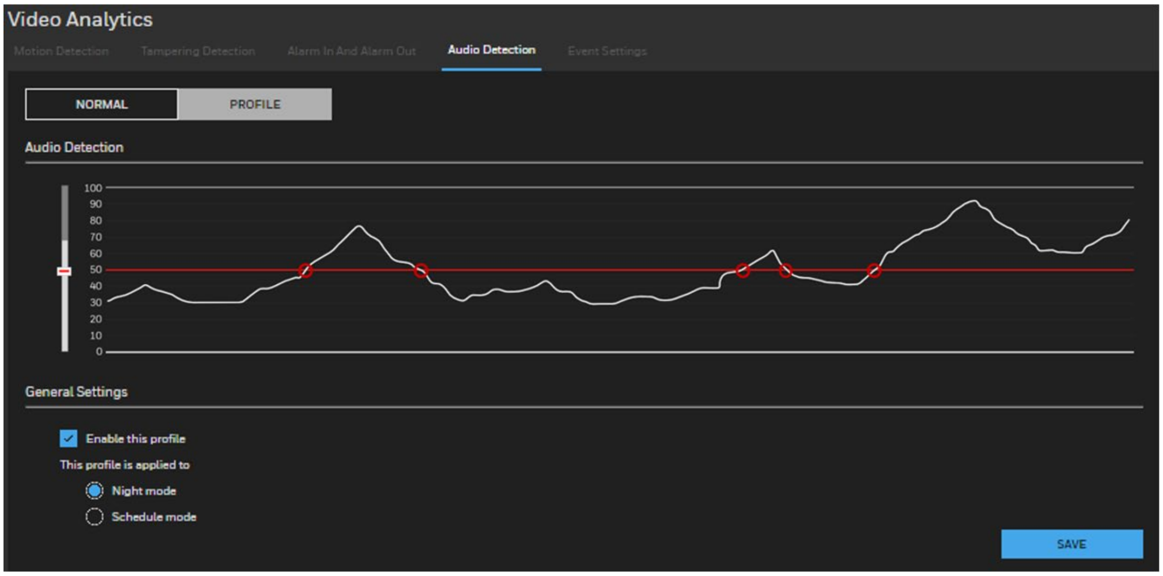
Perform the following steps to configure Audio detection in the **NORMAL** tab:

1. Once the Audio detection window is opened, the current sound input will be interactively indicated by a fluctuating white wave diagram.
2. Drag the Alarm level slider to a preferred location on the left slide bar.
3. Check Enable audio detection and click SAVE.

Note:

- *The volume numbers (0~100) on the left side of wave diagram does not represent decibel (dB). Sound intensity level has already been mapped to preset values. You can, however, use the real-world inputs at your installation site that are shown on the wave diagram to configure an alarm level.*
- *To configure this feature, you must unmute the audio in Setup →Camera Setup → Audio. After unmuting, sometimes you need to refresh the page to make the audio detection page settings take effect. The default of the camera can be muted due to the lack of an internal microphone. An external microphone is provided by users.*

Figure 51 Audio Detection: PROFILE Tab



☑ Enable this profile

This profile is applied to

● Night mode

○ Schedule mode

You can configure a different audio detection setting in the **PROFILE tab**. For example, a place can be noisy in the day time and become very quiet in the night.

1. Check Enable this profile. Once the Audio detection window is opened, the current sound input will be interactively indicated by a fluctuating white wave diagram.
2. Drag the Alarm level slider to a preferred location on the left slide bar.
3. Check the Night mode or Schedule mode. You may also manually configure a period of time during which this profile will take effect.
4. Click SAVE.

Note:

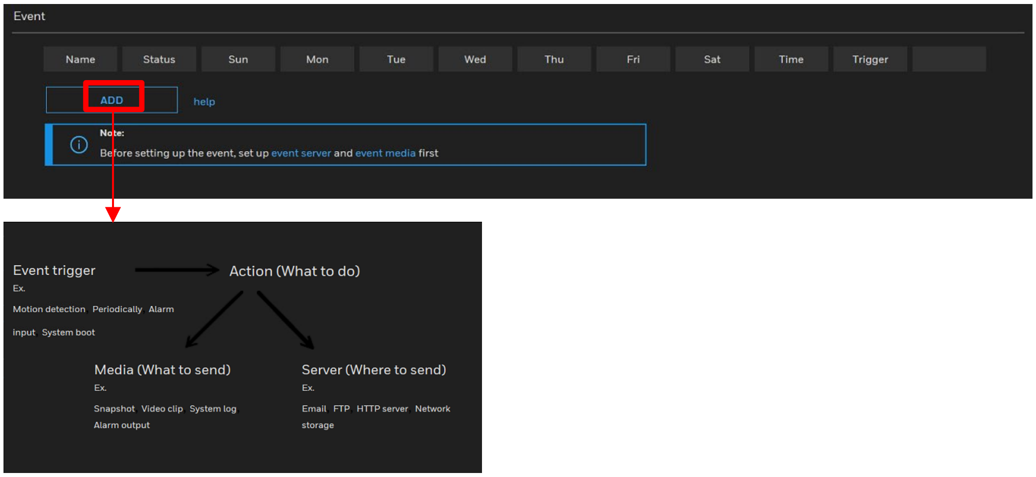
- *If the Alarm level and the received volume are set within a range of 20% on the wave diagram, frequent alarms will be triggered. It is recommended to set the Alarm level farther apart from the detected sound level.*
- *To configure and enable this feature, you must not configure video stream #1 into Motion JPEG. If an external microphone input is connected and recording of audio stream is preferred, audio stream is transmitted between camera and viewer/recording station along with stream #1.*

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 52 Event Settings



Note:
Before setting up the event, set up event server and event media first

Event trigger → Action (What to do)

Ex.
Motion detection Periodically Alarm input System boot

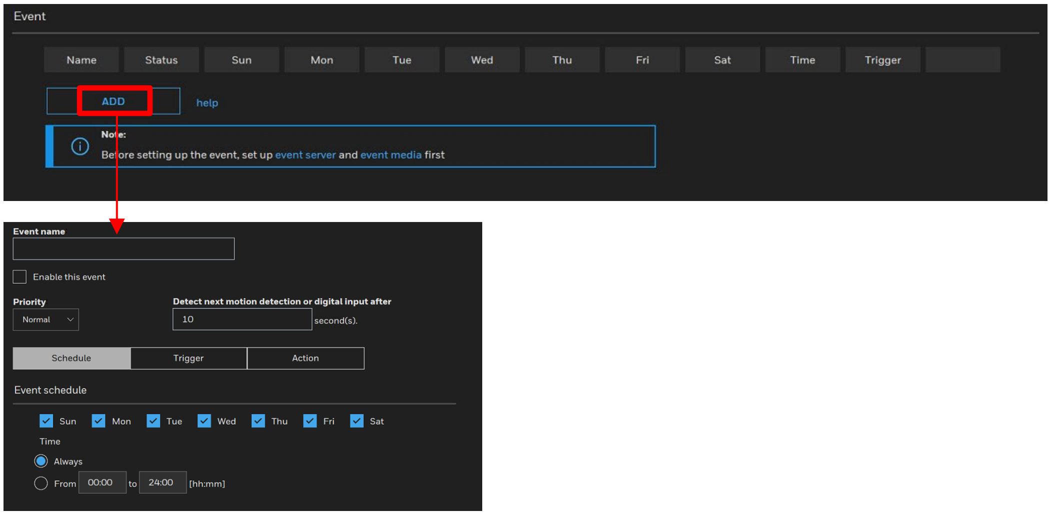
Media (What to send)
Ex.
Snapshot Video clip System log Alarm output

Server (Where to send)
Ex.
Email FTP HTTP server Network storage

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 53 Event



Note:
Before setting up the event, set up event server and event media first

Event name

□ Enable this event

Priority: Normal

Detect next motion detection or digital input after 10 second(s).

Event schedule

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time

● Always

○ From 00:00 to 24:00 [hh:mm]

- **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

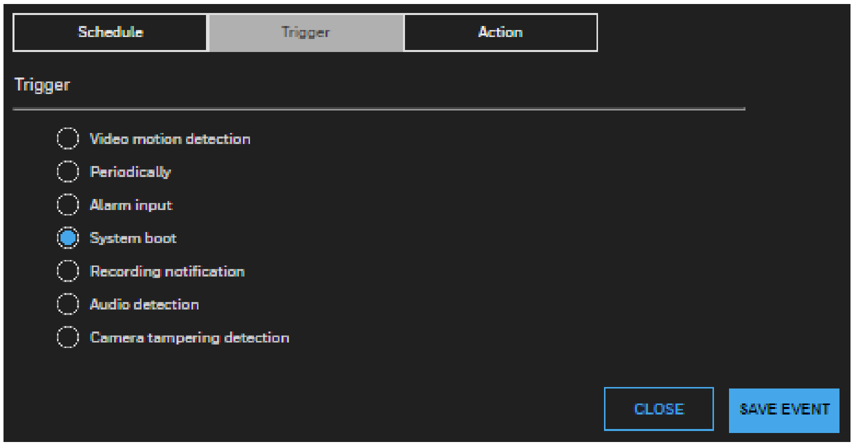
Specify the period of time during which the event trigger will take effect. Select the days of a week and the time in a day (in 24-hr time format) for the event triggering schedule. For example, you may prefer an event to be triggered only during the off-office hours.

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 54 Trigger Sources



Trigger

○ Video motion detection
○ Periodically
○ Alarm input
● System boot
○ Recording notification
○ Audio detection
○ Camera tampering detection

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 48.

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.

Audio detection

This option allows the camera to trigger when the audio detection exceeding the preset threshold.

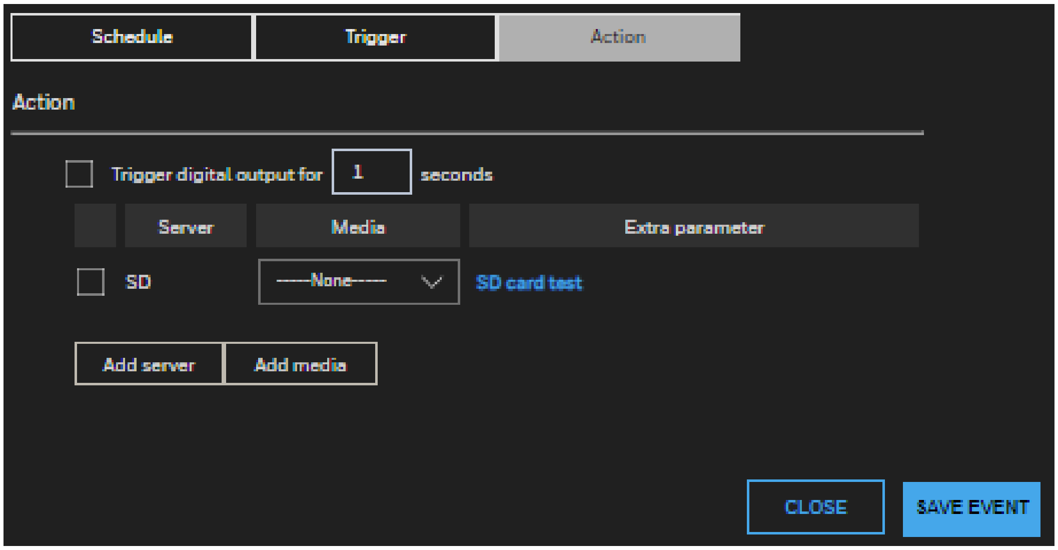
Camera tampering detection

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 49.

Action

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

Figure 55 Action



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

SD card 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 63.

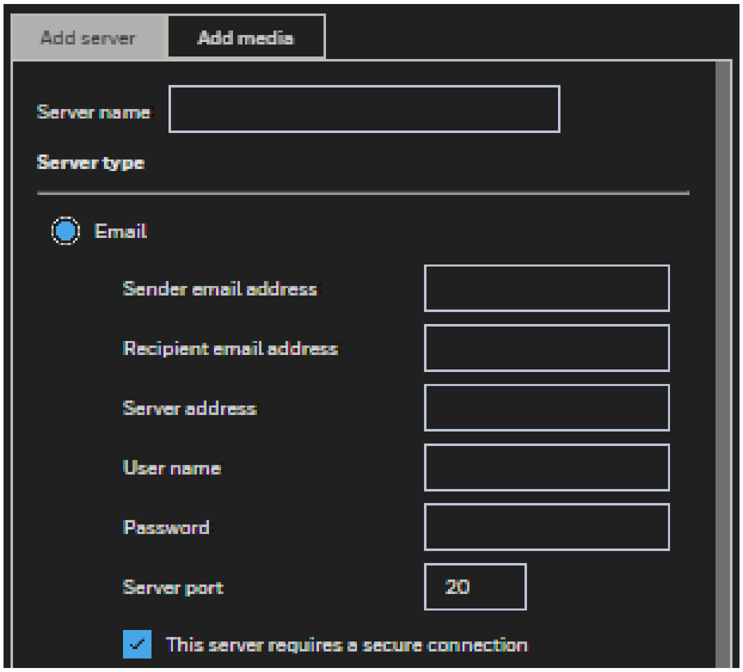
Add Server

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 56 Add Server



Server name

Server type

● Email

Sender email address

Recipient email address

Server address

User name

Password

Server port 20

☑ This server requires a secure connection

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.

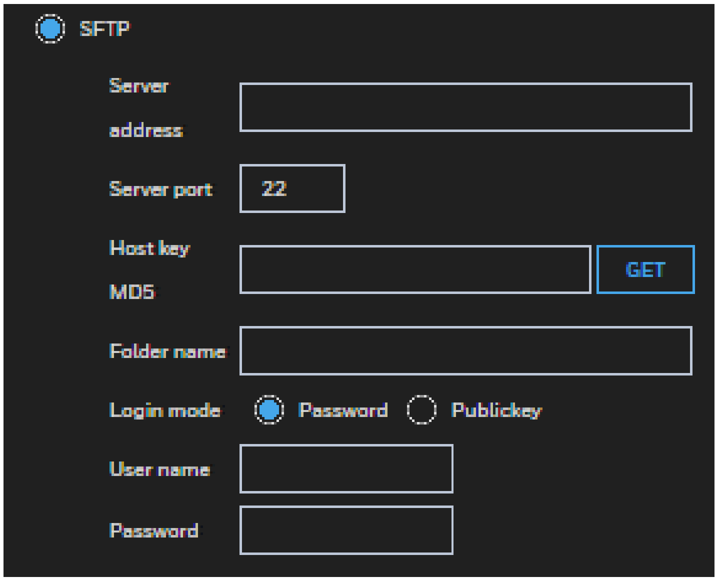
Click **SAVE SERVER** to enable the settings.

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 – SFTP

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

Figure 57 Server type – SFTP



● SFTP

Server address

Server port: 22

Host key MD5

Folder name

Login mode: ● Password ○ Publickey

User name

Password

- Server name: Enter a name for the server setting.
- Server address: server address
- Server port: server port
- Host key MD5: Server fingerprint(MD5). You can get it by calculate server host key(public) md5.
- Folder name: Login path on server
- Login mode:

  authentication method

  passwd = password authentication. You have to setup sftp_passwd for this login mode to work.

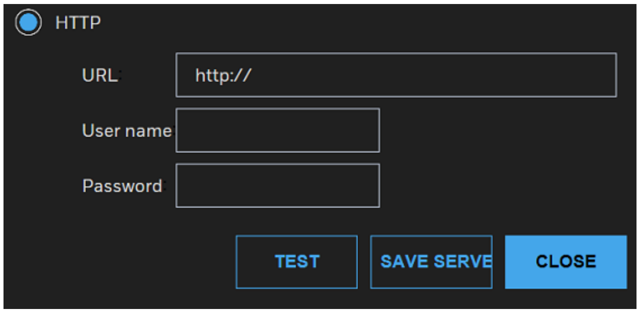
  publickey = Public key authentication is more secure than password authentication.User name: Enter the user name if necessary.
- User name: Enter the user name if necessary.
- Password: Enter the password if necessary.

To verify if the SFTP 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 SFTP server.

Server type - HTTP

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

Figure 58 Server type – HTTP



● HTTP

URL: http://

User name

Password

- 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.

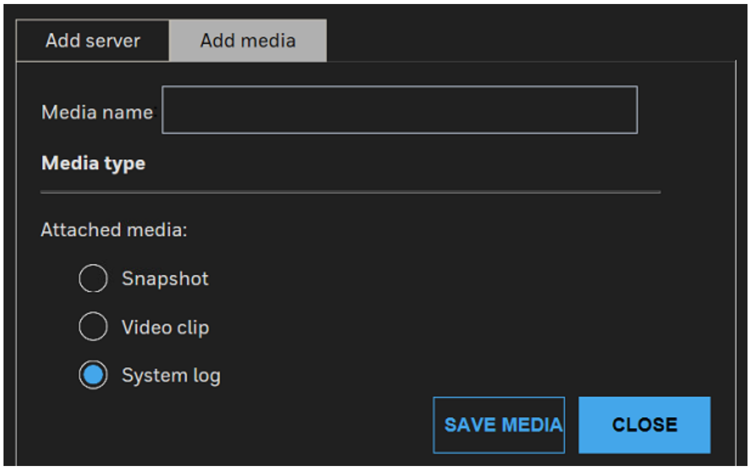
To verify if the HTTP settings are correctly configured, click **TEST**. The result will be shown in a pop-up window. If successful, you will receive a test.txt file on the HTTP server.

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 59 Add Media



Media name

Media type

Attached media:

○ Snapshot

○ Video clip

● System log

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.

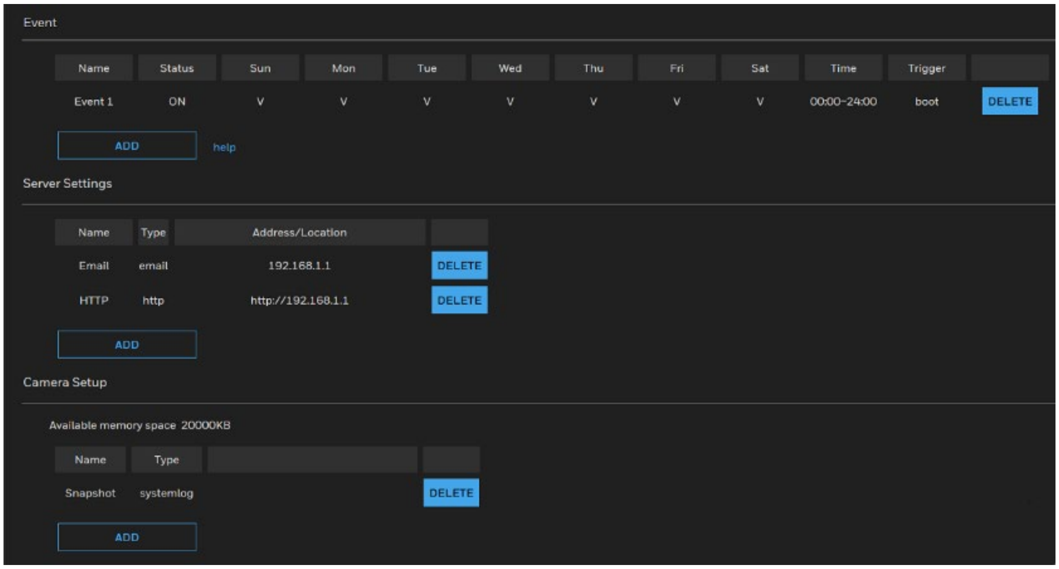
Click **SAVE MEDIA** to enable the settings, and then click **CLOSE** to exit the page.

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 60 Event Settings Examples



Event

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Trigger	
Event 1	ON	V	V	V	V	V	V	V	00:00-24:00	boot	DELETE

Server Settings

Name	Type	Address/Location	
Email	email	192.168.1.1	DELETE
HTTP	http	http://192.168.1.1	DELETE

Camera Setup

Available memory space 20000KB

Name	Type		
Snapshot	systemlog		DELETE

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.

CHAPTER

7

CONFIGURING STORAGE SETTINGS

This chapter contains the following sections:

- SD Card Management, page 62
- Content Management, page 64
- Recording Settings, page 66

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 4 Compatible SD Card

SD Card Brand	Model	Size
Western Digital	SC QD101 microSD Card	1TB
Micron	microSD card	1TB
Sandisk	MicroSDXC USH-I Card	512G
Toshiba	MicroSDXC USH-I Card	256G
SONY	MicroSDXC U1	128G
Samsung	MicroSDXC EVO PLUS U1	64G

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*

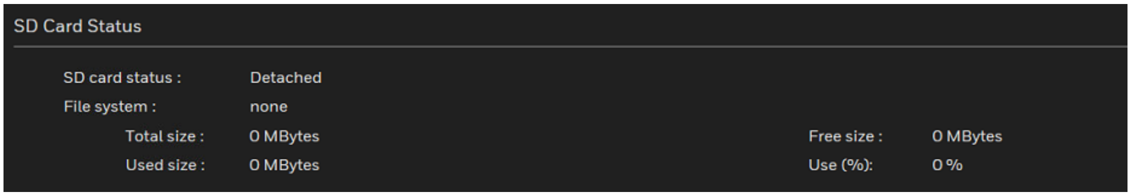
in camera malfunctions.

- *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* 63*.*

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 63.

Figure 61 No SD Card



SD Card Status

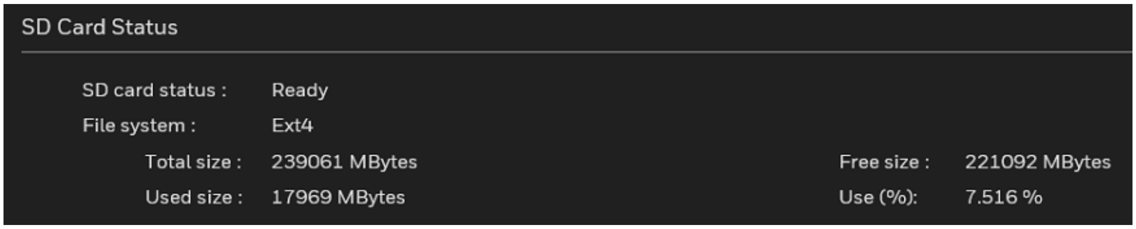
SD card status : Detached

File system : none

Total size : 0 MBytes   Free size : 0 MBytes

Used size : 0 MBytes   Use (%): 0 %

Figure 62 SD Card Onboard



SD Card Status

SD card status : Ready

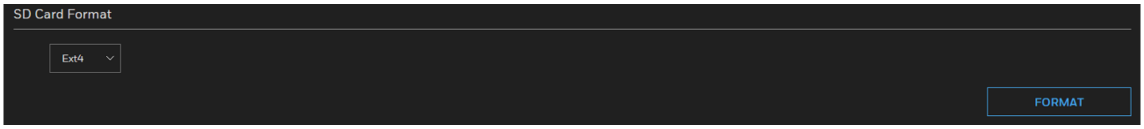
File system : Ext4

Total size : 239061 MBytes   Free size : 221092 MBytes

Used size : 17969 MBytes   Use (%): 7.516 %

SD Card Format

Figure 63 SD Card Format



SD Card Format

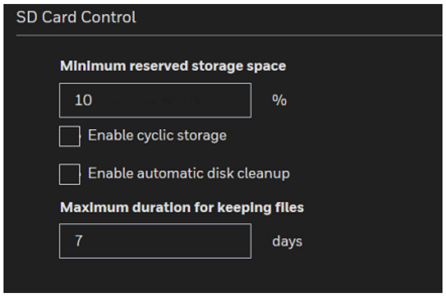
Ext4

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

Note: *SD card encryption by LUKS (Linux Unified Key Setup).*

SD Card Control

Figure 64 SD Card Control



SD Card Control

Minimum reserved storage space

10 %

□ Enable cyclic storage

□ Enable automatic disk cleanup

Maximum duration for keeping files

7 days

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

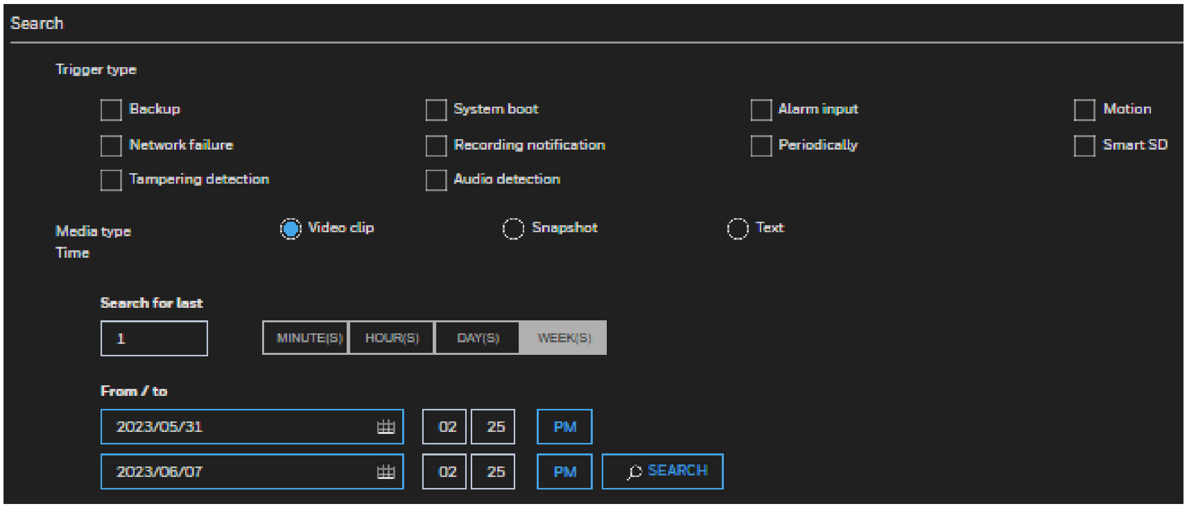
Go to **Setup →Storage Setup →Content Management**.

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 65 Search



Search

Trigger type

□ Backup	□ System boot	□ Alarm input	□ Motion
□ Network failure	□ Recording notification	□ Periodically	□ Smart SD
□ Tampering detection	□ Audio detection		

Media type ● Video clip ○ Snapshot ○ Text

Time

Search for last

1 MINUTE(S) HOUR(S) DAY(S) [✓ WEEK(S)]

From / to

2023/05/31 02 25 PM

2023/06/07 02 25 PM SEARCH

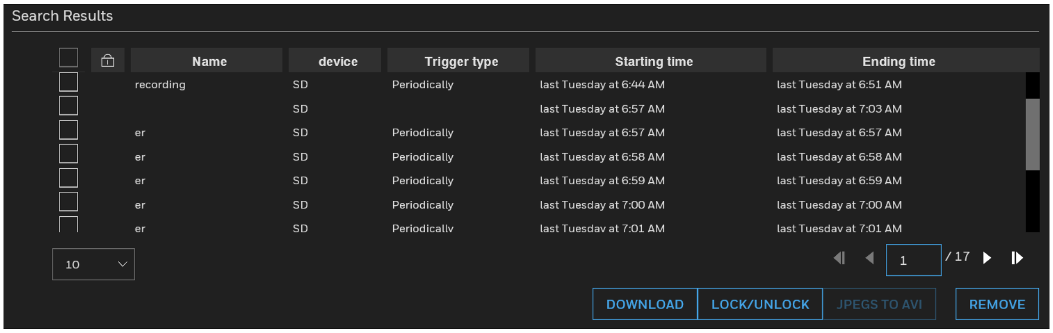
- Trigger type: Select one or more trigger types.
- Media type: Select a media type (Video clip, snapshot or text).
- Time: Manually enter the time range you want to search for contents created at a specific point in time.

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 66 Search Results

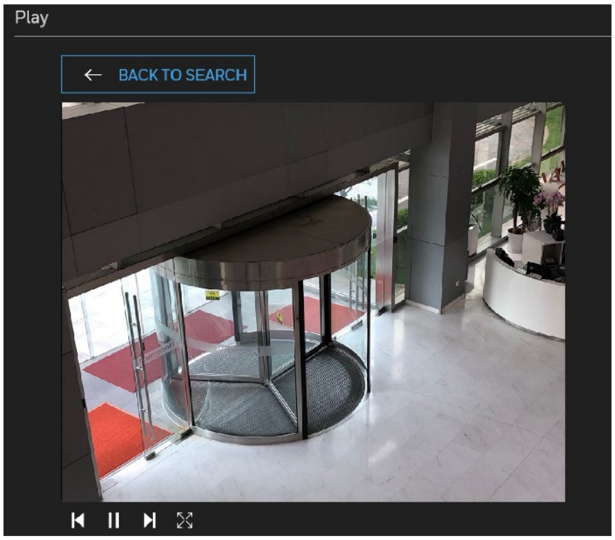


Search Results

□		Name	device	Trigger type	Starting time	Ending time
□		recording	SD	Periodically	last Tuesday at 6:44 AM	last Tuesday at 6:51 AM
□			SD		last Tuesday at 6:57 AM	last Tuesday at 7:03 AM
□		er	SD	Periodically	last Tuesday at 6:57 AM	last Tuesday at 6:57 AM
□		er	SD	Periodically	last Tuesday at 6:58 AM	last Tuesday at 6:58 AM
□		er	SD	Periodically	last Tuesday at 6:59 AM	last Tuesday at 6:59 AM
□		er	SD	Periodically	last Tuesday at 7:00 AM	last Tuesday at 7:00 AM
□		er	SD	Periodicallv	last Tuesdav at 7:01 AM	last Tuesdav at 7:01 AM

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

Figure 67 Play Search Result



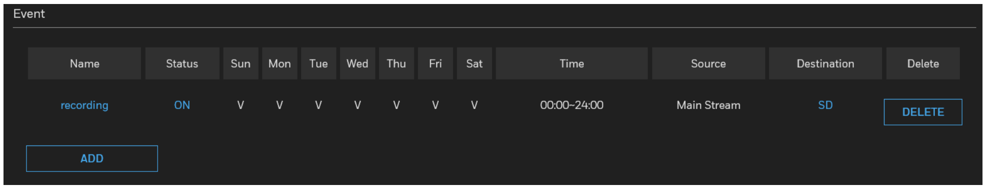
- **DOWNLOAD**: Click on a search result and click **DOWNLOAD**, and a file download window will pop up for you to save the file. You can play the video clip by VLC player.
- **LOCK/UNLOCK**: Select the checkbox in front of a desired search result, then click **LOCK/UNLOCK**. The selected items will become Locked, which will not be deleted during cyclic recording. You can click again to unlock the selections.
- **JPEGS TO AVI**: This function 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.
- **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 68 Recording Settings



Event

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Source	Destination	Delete
recording	ON	V	V	V	V	V	V	V	00:00~24:00	Main Stream	SD	DELETE

ADD

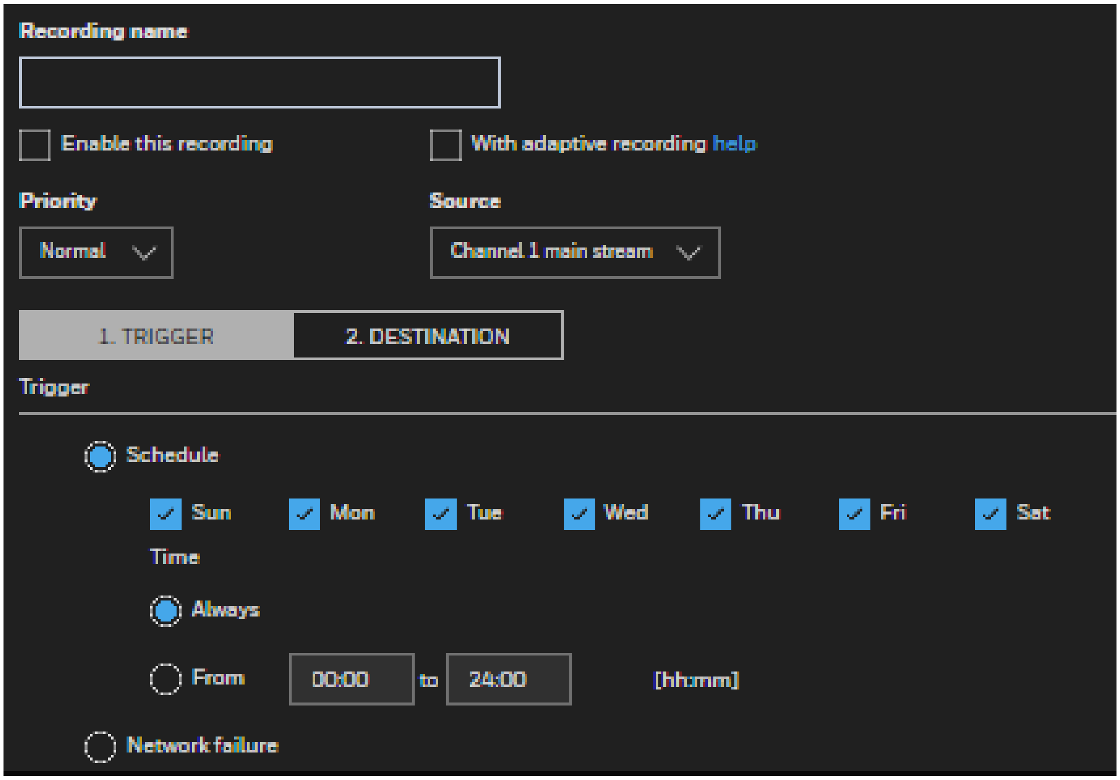
SD Test: Insert the SD card and click here to test.

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 63.*

Adding a Recording Setting

Click **ADD** as shown in Figure 68 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 69 Recording Settings Details



Recording name

□ Enable this recording

□ With adaptive recording help

Priority: Normal

Source: Channel 1 main stream

1. TRIGGER | 2. DESTINATION

Trigger

● Schedule

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time

● Always

○ From 00:00 to 24:00 [hh:mm]

○ Network failure

- **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.

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 51.*
- *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 51.*

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).

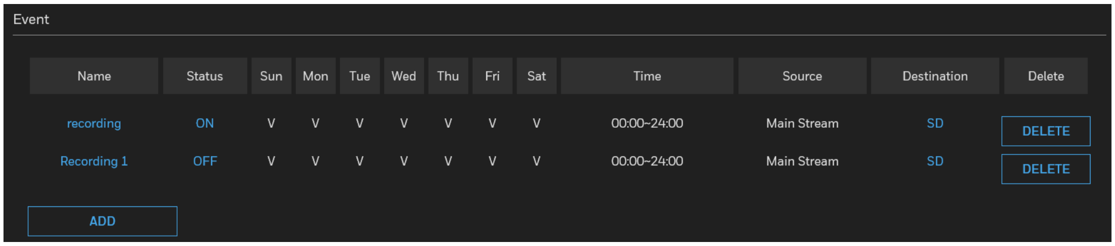
2. Set a destination (SD) for the recorded video files.

- 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 51.

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 70 Recording 1



Event

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Source	Destination	Delete
recording	ON	V	V	V	V	V	V	V	00:00~24:00	Main Stream	SD	DELETE
Recording 1	OFF	V	V	V	V	V	V	V	00:00~24:00	Main Stream	SD	DELETE

ADD

- 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.

CHAPTER

8 CONFIGURING SYSTEM SETTINGS

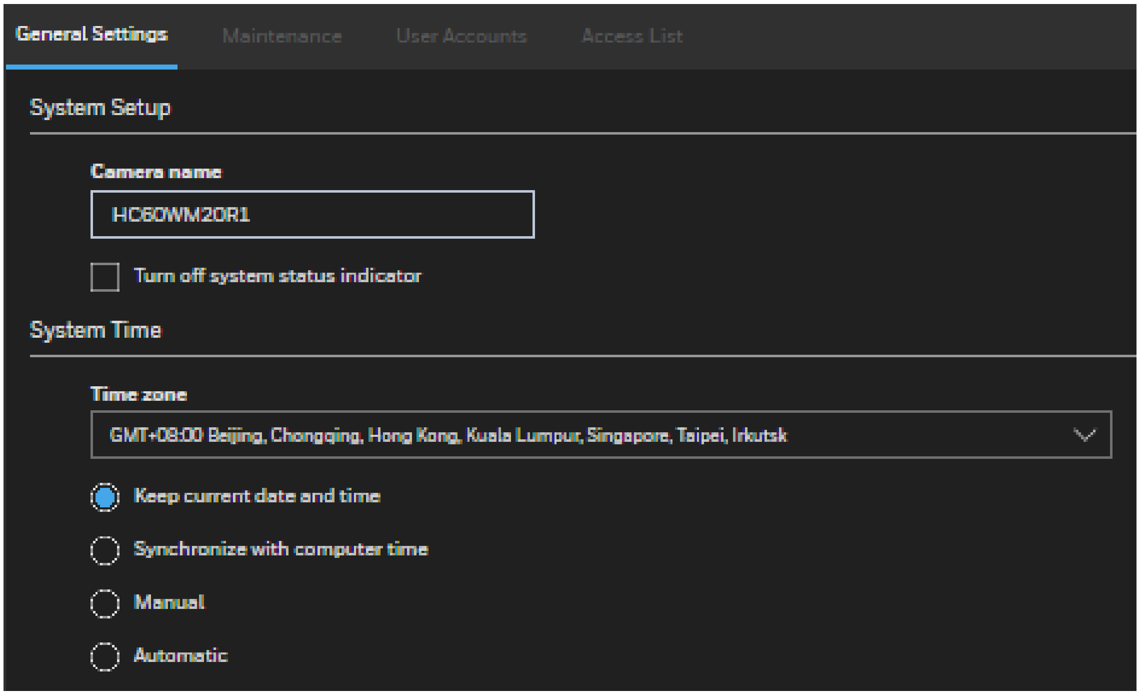
This chapter contains the following sections:

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 71 Configuring System General Settings



System Setup

Camera name

HC60WM20R1

□ Turn off system status indicator

System Time

Time zone

GMT+08:00 Beijing, Chongqing, Hong Kong, Kuala Lumpur, Singapore, Taipei, Irkutsk

● Keep current date and time

○ Synchronize with computer time

○ Manual

○ Automatic

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

Turn off system status indicator: 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 70.

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.

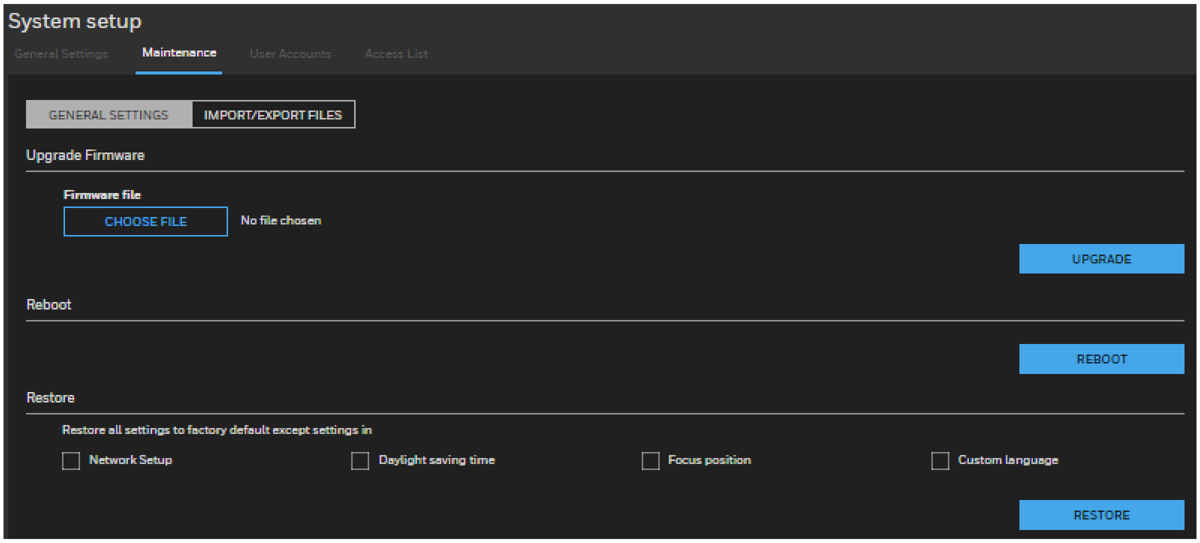
- NTP server: Assign the IP address or domain name of the time-server. Leaving the text box blank connects the camera to the default time servers. The precondition is that the camera must have the access to the Internet.
- Update interval: Select to update the time using the NTP server on an hourly, 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 72 Maintenance



Restore all settings to factory default except settings in

□ Network Setup □ Daylight saving time □ Focus position □ Custom language

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 63.*
- *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 34).

Daylight Saving Time: Check to retain the **Daylight Saving Time** settings (see Importing /Exporting Files on page 72).

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

Custom language: Check this option to retain the custom language settings.

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

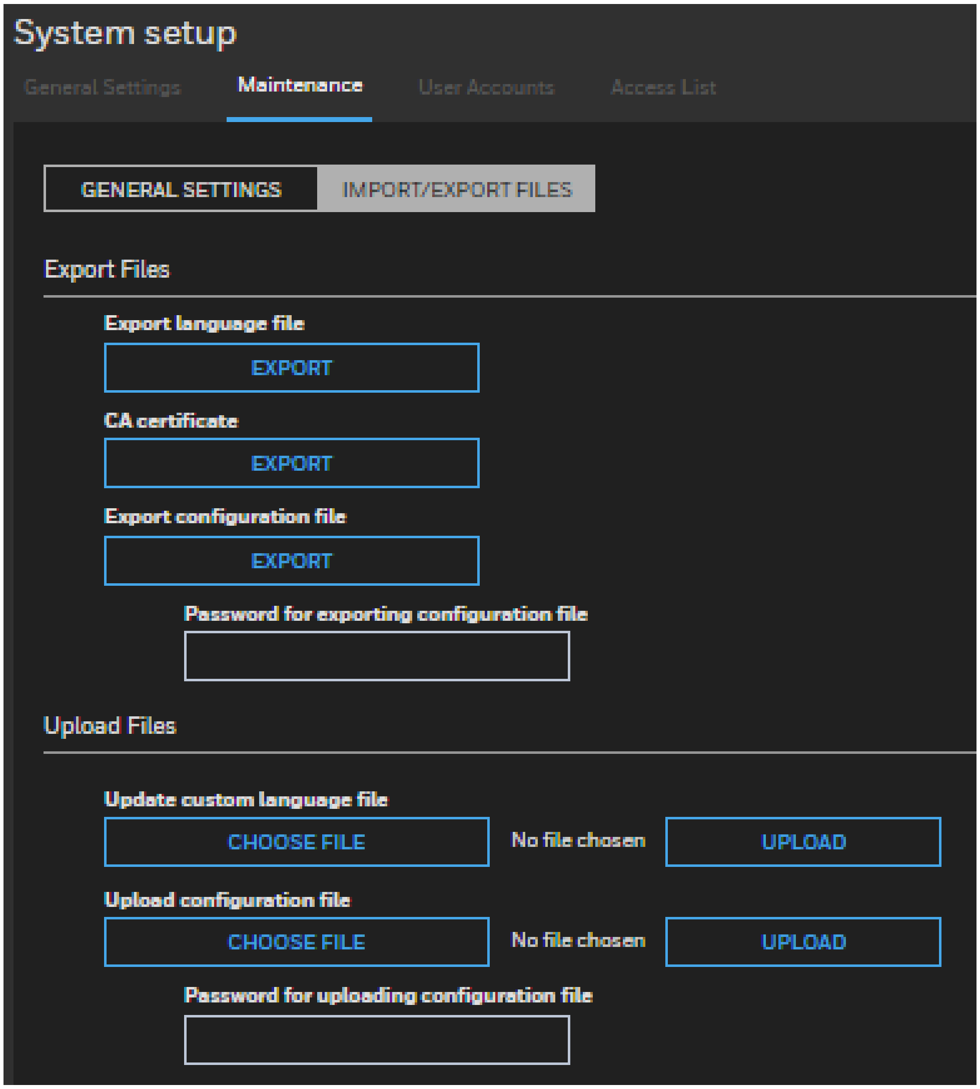
After it is completed, the live video page will be displayed in your browser.

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 73 Import/Export Files



Export language file

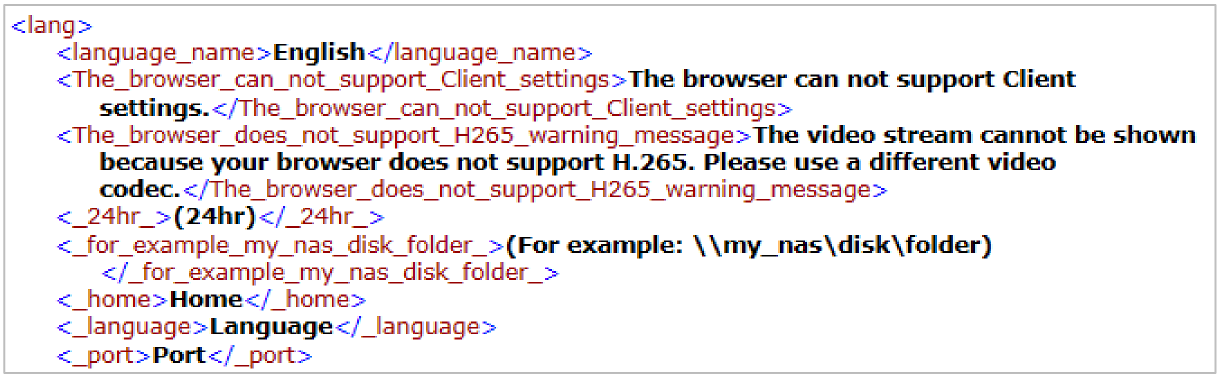
Follow the steps below to export language file

The camera supports the following languages: English, German, Spanish, French, Italian, Japanese, Portuguese, Russian and traditional Chinese. If your language is not listed, perform the following steps to customize the camera language.

Taking the English language file for example:

1. Click EXPORT to export the export_translator.xml file.
2. Save and open the export_translator.xml file.
3. Replace all English string value in bold black (see Figure 74) into your own language and save the file. The following figure is a sample segment.

Figure 74 Editing Language String



```
<lang>
    <language_name>English</language_name>
    <The_browser_can_not_support_Client_settings>The browser can not support Client
        settings.</The_browser_can_not_support_Client_settings>
    <The_browser_does_not_support_H265_warning_message>The video stream cannot be shown
        because your browser does not support H.265. Please use a different video
        codec.</The_browser_does_not_support_H265_warning_message>
    <_24hr_>(24hr)</_24hr_>
    <_for_example_my_nas_disk_folder_>(For example: \\my_nas\disk\folder)
        </_for_example_my_nas_disk_folder_>
    <_home>Home</_home>
    <_language>Language</_language>
    <_port>Port</_port>
```

4. Upload the updated export_translator.xml file to your system. See Update custom language file. on page 75.

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 custom language file

Follow the steps below to update custom language file:

1. Click CHOOSE FILE under Update custom language file.
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.

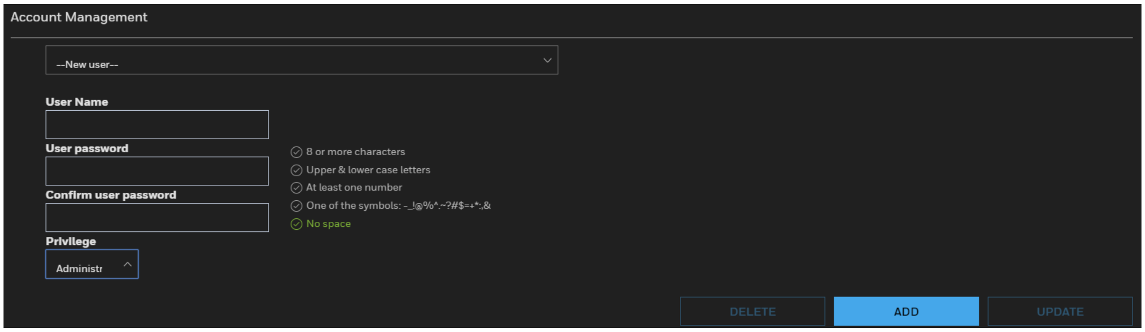
Configuring User Accounts Settings

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

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

Account Management

Figure 75 Account Management



Account Management

--New user--

User Name

User password

Confirm user password

Privilege

Administr

✓ 8 or more characters

✓ Upper & lower case letters

✓ At least one number

✓ One of the symbols: -_!@%^.~?#$=+*:,&

✓ No space

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:

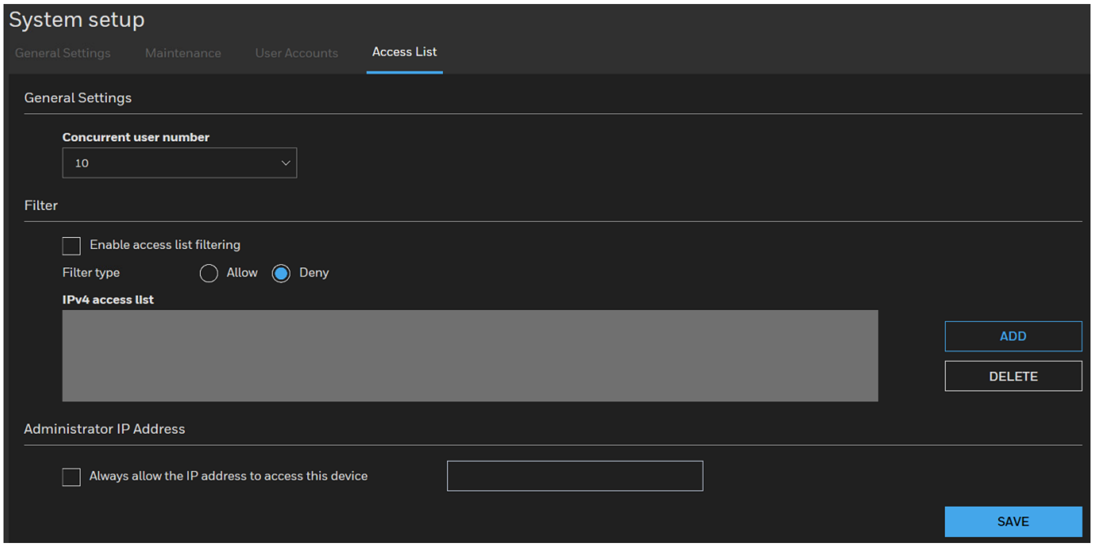
1. Select an existing account to modify.
2. Make necessary changes and click UPDATE or DELETE to enable the setting.

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 76 Access List



System setup

General Settings | Maintenance | User Accounts | Access List

General Settings

Concurrent user number: 10

Filter

□ Enable access list filtering

Filter type ○ Allow ● Deny

IPv4 access list

ADD

DELETE

Administrator IP Address

□ Always allow the IP address to access this device

SAVE

General Settings

Concurrent user number: Simultaneous live viewing for 1~20 clients (including main stream to third stream). The default value is 20.

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 36.*
- *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.

CHAPTER

9 VIEWING SYSTEM INFO

This chapter contains the following sections:

- Log, page 79
- Version, page 80

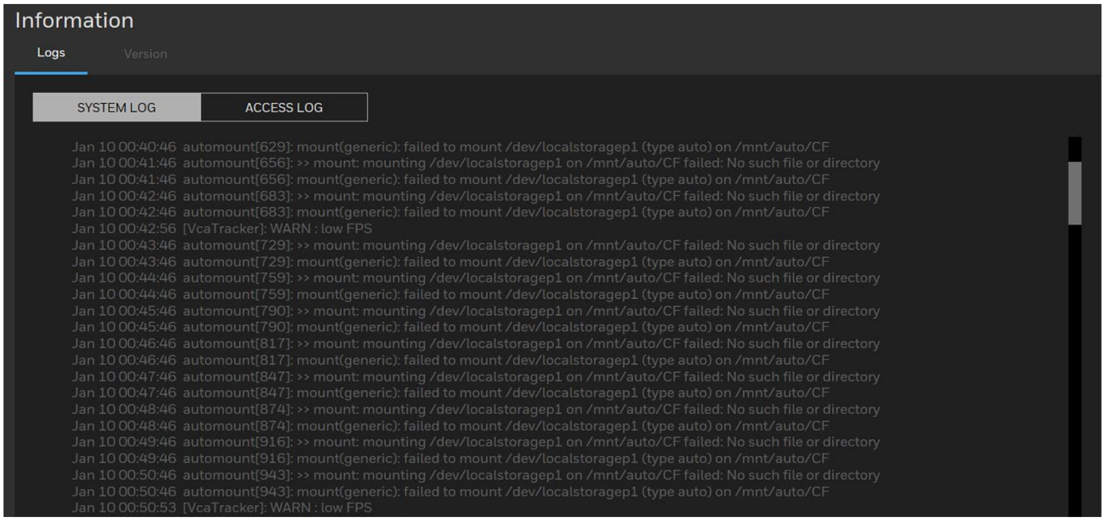
Log

Go to **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 77 System Log

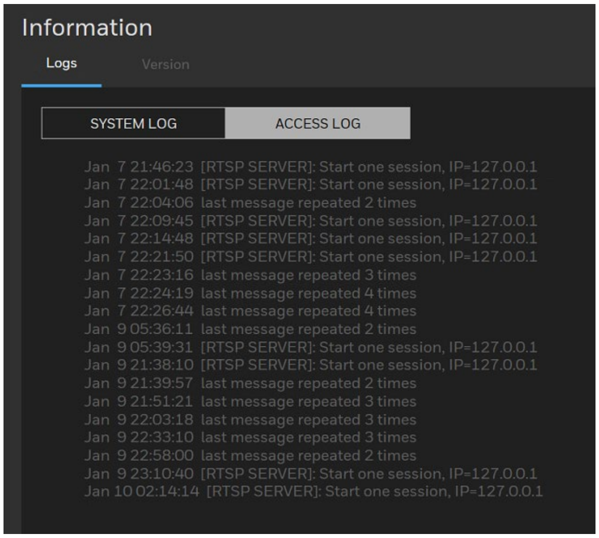


```
Jan 10 00:40:46  automount[629]: mount(generic): failed to mount /dev/localstoragep1 (type auto) on /mnt/auto/CF
Jan 10 00:41:46  automount[656]: >> mount: mounting /dev/localstoragep1 on /mnt/auto/CF failed: No such file or directory
Jan 10 00:41:46  automount[656]: mount(generic): failed to mount /dev/localstoragep1 (type auto) on /mnt/auto/CF
Jan 10 00:42:46  automount[683]: >> mount: mounting /dev/localstoragep1 on /mnt/auto/CF failed: No such file or directory
Jan 10 00:42:46  automount[683]: mount(generic): failed to mount /dev/localstoragep1 (type auto) on /mnt/auto/CF
Jan 10 00:42:56  [VcaTracker]: WARN : low FPS
Jan 10 00:43:46  automount[729]: >> mount: mounting /dev/localstoragep1 on /mnt/auto/CF failed: No such file or directory
Jan 10 00:43:46  automount[729]: mount(generic): failed to mount /dev/localstoragep1 (type auto) on /mnt/auto/CF
Jan 10 00:44:46  automount[759]: >> mount: mounting /dev/localstoragep1 on /mnt/auto/CF failed: No such file or directory
Jan 10 00:44:46  automount[759]: mount(generic): failed to mount /dev/localstoragep1 (type auto) on /mnt/auto/CF
Jan 10 00:45:46  automount[790]: >> mount: mounting /dev/localstoragep1 on /mnt/auto/CF failed: No such file or directory
Jan 10 00:45:46  automount[790]: mount(generic): failed to mount /dev/localstoragep1 (type auto) on /mnt/auto/CF
Jan 10 00:46:46  automount[817]: >> mount: mounting /dev/localstoragep1 on /mnt/auto/CF failed: No such file or directory
Jan 10 00:46:46  automount[817]: mount(generic): failed to mount /dev/localstoragep1 (type auto) on /mnt/auto/CF
Jan 10 00:47:46  automount[847]: >> mount: mounting /dev/localstoragep1 on /mnt/auto/CF failed: No such file or directory
Jan 10 00:47:46  automount[847]: mount(generic): failed to mount /dev/localstoragep1 (type auto) on /mnt/auto/CF
Jan 10 00:48:46  automount[874]: >> mount: mounting /dev/localstoragep1 on /mnt/auto/CF failed: No such file or directory
Jan 10 00:48:46  automount[874]: mount(generic): failed to mount /dev/localstoragep1 (type auto) on /mnt/auto/CF
Jan 10 00:49:46  automount[916]: >> mount: mounting /dev/localstoragep1 on /mnt/auto/CF failed: No such file or directory
Jan 10 00:49:46  automount[916]: mount(generic): failed to mount /dev/localstoragep1 (type auto) on /mnt/auto/CF
Jan 10 00:50:46  automount[943]: >> mount: mounting /dev/localstoragep1 on /mnt/auto/CF failed: No such file or directory
Jan 10 00:50:46  automount[943]: mount(generic): failed to mount /dev/localstoragep1 (type auto) on /mnt/auto/CF
Jan 10 00:50:53  [VcaTracker]: WARN : low FPS
```

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 deleted after the camera is rebooted.

Figure 78 Access Log



```
Jan  7 21:46:23  [RTSP SERVER]: Start one session, IP=127.0.0.1
Jan  7 22:01:48  [RTSP SERVER]: Start one session, IP=127.0.0.1
Jan  7 22:04:06  last message repeated 2 times
Jan  7 22:09:45  [RTSP SERVER]: Start one session, IP=127.0.0.1
Jan  7 22:14:48  [RTSP SERVER]: Start one session, IP=127.0.0.1
Jan  7 22:21:50  [RTSP SERVER]: Start one session, IP=127.0.0.1
Jan  7 22:23:16  last message repeated 3 times
Jan  7 22:24:19  last message repeated 4 times
Jan  7 22:26:44  last message repeated 4 times
Jan  9 05:36:11  last message repeated 2 times
Jan  9 05:39:31  [RTSP SERVER]: Start one session, IP=127.0.0.1
Jan  9 21:38:10  [RTSP SERVER]: Start one session, IP=127.0.0.1
Jan  9 21:39:57  last message repeated 2 times
Jan  9 21:51:21  last message repeated 3 times
Jan  9 22:03:18  last message repeated 3 times
Jan  9 22:33:10  last message repeated 3 times
Jan  9 22:58:00  last message repeated 2 times
Jan  9 23:10:40  [RTSP SERVER]: Start one session, IP=127.0.0.1
Jan 10 02:14:14  [RTSP SERVER]: Start one session, IP=127.0.0.1
```

Version

Go to **Information →Version**.

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

CHAPTER

10 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 5 Troubleshooting

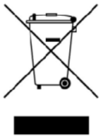
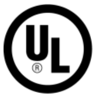
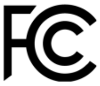
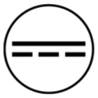
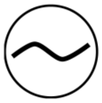
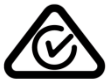
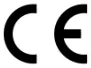
Issues	Solutions
Cannot install/log in to web client.	• Ensure that your browser's security settings allow ActiveX controls. • Ensure that you have a valid network setup and that you are using the correct login username and password.
Power supply is unstable.	Use of a UPS power supply is strongly recommended.
Camera webpage has abnormal display.	• Clear the cache of browser. • Prefer 75% zoom in browser for low resolution (< 1366*768) display.
The audio will not stop automatically when switching from live page to settings page.	Manually turn off the audio on live page.
RS485 Default configuration.	Protocol: Pelco-D Id: 1 Baudrate: 2400 Databit: 8 Paritybit: none Stopbit: 1

CHAPTER

11 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 EAC	Eurasian Conformity (EAC) RoHS

Honeywell Building Technologies – Security Americas (Head Office)

Honeywell Commercial Security
715 Peachtree St. NE
Atlanta, GA 30308
Tel: +1 800 323 4576

Honeywell Building Technologies – Security Mexico

Mexico: Av. Santa Fe 94, Torre A, Piso 1, Col. Zedec,
CP 012010, CDMX, México.
Colombia: Edificio Punto 99, Carrera 11a.
98-50, Piso 7, Bogota, Colombia.
Tel: 01.800.083.59.25

Honeywell Building Technologies – Security Middle East/N. Africa

Emaar Business Park, Building No. 2, Sheikh Zayed Road
P.O. Box 232362
Dubai, United Arab Emirates
security_meta@honeywell.com
Tel: +971 4 450 5800

Honeywell Building Technologies – Security Europe/South Africa

Building 5 Carlton Park,
King Edward Avenue
Narborough, Leicester, LE19 0LF
United Kingdom
Tel: +44 (0) 1163 500714

Honeywell Building Technologies – Security Northern Europe

Stationsplein Z-W 961, 1117 CE Schiphol-Oost, Netherlands

Tel: +31 (0) 299 410 200

Honeywell Building Technologies – Security Deutschland

Johannes-Mauthe-Straße 14
D-72458 Albstadt
Germany
Tel: +49 (0) 7431 801-0

Honeywell Building Technologies – Security France

Immeuble Lavoisier
Parc de Haute Technologie
3-7 rue Georges Besse
92160 Antony, France
Tel: +33 (0) 1 40 96 20 50

Honeywell Building Technologies – Security Italia SpA

Via Achille Grandi 22,
20097 San Donato Milanese (MI), Italy

Honeywell Building Technologies – Security España

Josefa Valcárcel, 24

28027 – Madrid, España

Tel.: +34 902 667 800

Honeywell Building Technologies – Security Россия и СНГ

121059 Moscow,
Ul, Kiev 7
Russia
Tel: +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
Tel: 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
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
Email: HBT-IndiaBuildings@honeywell.com
Toll Free Number: 000 800 050 2167
Tel: +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
Email: info.security@honeywell.com
Customer support: HSG-CS-KR@honeywell.com; +82 1522-8779
Tel: +82-2-799-6114

Honeywell Building Technologies – Security & Fire (Pacific)

Honeywell Ltd
9 Columbia Way
BAULKHAM HILLS NSW 2153
Email: hsf.comms.pacific@Honeywell.com
Technical support:
Australia: 1300 220 345
New Zealand: +64 9 623 5050

Honeywell

https://buildings.honeywell.com/security
+1 800 323 4576 (North America only)
Document 600-60UG01 Rev A – 10/2023