

Honeywell

Honeywell 60 Series

AI IP Cameras

HC60W34R2I

HC60WC5I

HC60WB2R2I

HC60W32R2I

HC60WZ4R40WI

HC60WB4R5I

HC60W44R2I

HC60WZ4R40KI

HC60WZ8R40KI

HC60W42R2I

HC60WB4R2I

HC60WZ8R40WI

User Guide

Recommended

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

Copy Right

© 2024 Honeywell International Inc. All rights reserved. No part of this publication may be reproduced by any means without written permission from Honeywell. The information in this publication is believed to be accurate in all respects. However, Honeywell cannot assume responsibility for any consequences resulting from the use thereof. The information contained herein is subject to change without notice. Revisions or new editions to this publication may be issued to incorporate such changes. For patent information, see <https://buildings.honeywell.com/us/en/support/legal/patents>.

Revision

Issue	Date	Revisions
A	08/2023	New document.
B	11/2024	Add HC60WZ8R40KI, HC60WZ8R40WI. Update Configuring Video Analytics. Update Configuring Network. Update Configuring Storage. Update Configuring Alarm and Event.

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 COVER (OR BACK). NO USER SERVICEABLE PARTS INSIDE. REFER SERVICING TO QUALIFIED SERVICE PERSONNEL.	 THIS SYMBOL INDICATES THAT IMPORTANT OPERATING AND MAINTENANCE INSTRUCTIONS ACCOMPANY THIS UNIT.
 PRUDENCE RISQUE DE CHOC ÉLECTRIQUE NE PAS OUVRIR 	 CE SYMBOLE INDIQUE QU'UNE TENSION DANGEREUSE CONSTITUANT UN RISQUE DE CHOC ÉLECTRIQUE EST PRÉSENTE DANS L'APPAREIL
ATTENTION : POUR RÉDUIRE LE RISQUE DE CHOC ÉLECTRIQUE, NE RETIREZ PAS LE COUVERCLE (NI L'ARRIÈRE). AUCUNE RÉPARATION PAR L'UTILISATEUR NE DOIT ÊTRE EFFECTUÉE PAR UN PERSONNEL QUALIFIÉ	 CE SYMBOLE INDIQUE QUE DES INSTRUCTIONS IMPORTANTES D'UTILISATION ET D'ENTRETIEN ACCOMPAGNENT CET APPAREIL



NOTCE

IR emitted from this product.
Do not look at the operating lamp

Précautions

IR émis par ce produit.
Ne regardez pas la lampe de fonctionnement



Caution: For HC60WZ8R40WI / HC60WZ8R40KI, IR emitted from these products. Do not look at the operating lamp.



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 802.3at PoE standard. The PoE is not intended to be connected to exposed (outside plant) networks. Consult Honeywell for the recommended adapter.



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

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 instructions, 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. 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.

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

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 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.
 - It is not allowed to install the PTZ camera upside down.
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

	Cautions and Warnings	i
	Regulatory Statements	ii
	Photobiological safety	ii
	General Data Protection Regulation	ii
	FCC Compliance Statement	ii
	Manufacturer's Declaration of Conformance	iii
	Waste Electrical and Electronic Equipment (WEEE)	iii
	Check Local Waste Guidelines	iii
	Safety Instructions	iv
	Warranty and Service	iv
1	Introduction	1
	Overview	1
	Supported Browsers	1
	Browser Minimum Requirement for Hardware	2
	Key Features	2
2	Accessing the Camera	4
	Installing the Unified Tool	4
	Discovering Your Camera on the Network	6
	Initializing Cameras	8
	Assigning a New IP Address to Your Camera	9
	Configure IP Address Setting	10
	Configure DNS Server Address	10
	Upgrading the Camera's Firmware	10
	Accessing the Camera from a Web Browser	11
3	Logging in & Viewing Live Video	12
	Logging in to the Camera via the Web Client	12
	Before You Begin	12
	Logging in to the Camera	12
	Using the Main Page	15
	System Menu	16

Stream Profile.....	16
Camera Name.....	17
Live View Toolbar	17
VA Event List.....	18
Language	18
Administrator Account.....	18

4 **Configuring Camera Settings.....19**

Configuring General Settings.....	19
Configuring Video Settings	19
Mode	19
Video Stream.....	20
ROI	23
Configuring Audio Settings	24
Audio File.....	24
Configuring Image Settings	25
Mode	26
Scheme	26
Image Adjustment	26
Scene Mode.....	26
Exposure.....	27
White Balance (WB) Setting.....	27
DayNight Setting.....	28
Noise Reduction	29
Enhance Image.....	29
Zoom Focus (IPC Models)	30
Zoom Focus (PTZ Models).....	30
Configuring OSD	31
Configuring Privacy Mask.....	31

5 **Configuring Network Settings.....33**

Configuring Network General Settings.....	33
Configuring Streaming Protocols.....	34
Configuring SMTP Settings.....	38
Configuring SNMP Settings.....	40
Configuring QoS Settings	41
Configuring HTTPS Settings.....	41
HTTPS	41
Certificate Request.....	42
Upload Files	43

	Configuring IEEE 802.1x Settings.....	44
	Configuring FTP Settings.....	45
	Configuring DDNS.....	46
	Configuring Port Mapping.....	47
	Configuring System Log.....	48
	Configuring Network Discovery Protocols	52
6	Configuring Video Analytics	53
	Motion Detection.....	53
	Smart Motion	55
	Scene Change.....	57
	Intrusion Detection.....	58
	Multi Loitering.....	60
	People Counter.....	62
	Face Detection.....	66
	Line Crossing Detection	68
	Unattended Object Detection.....	70
	Missing Object Detection.....	72
	Event & Metadata Scheme	74
7	Configure Alarm and Event	75
	Configuring Alarm In and Alarm Out.....	75
	Alarm Input.....	75
	Alarm Output	77
	Configuring SD Card Alarm.....	78
	Configuring Audio Detection	79
8	Configure Storage Settings.....	81
	SD Card Management	81
	SD Card Status	82
	SD Card Format.....	82
	Content Management	83
	Searching and Viewing the Records.....	83
	Search Results	83
	Recording Settings.....	84
9	Configure System Settings	86
	Configuring System General Settings.....	86
	Configuring Maintenance Settings.....	87
	Upgrading Firmware.....	87
	Rebooting the Camera	88
	Restoring the Camera	88
	Importing/Exporting Files.....	88
	Configuring Privacy Policy.....	90

Configuring User Accounts Settings	91
Account Management	91
Configuring Access List Settings	92
10 Configuring PTZ Settings	93
Preset	93
Auto Scan Management	94
Tour	95
Pattern	96
Idle Action	97
Power Up Action	98
Intelligent Tracking	99
11 Viewing System Information	100
Logs	100
Operation Log	100
Alarm Log	100
Collect Log	101
Version	101
12 Trouble Shooting	102
Troubleshooting for Common Issues	102
13 Appendix	104
List of Symbols	104

Figures

Figure 1 Install Unified Tool.....	5
Figure 2 Select Installation Folder	5
Figure 3 Confirm Installation.....	6
Figure 4 Splash Screen	7
Figure 5 Discover Cameras	8
Figure 6 Device List.....	8
Figure 7 Initialize Page 1	9
Figure 8 Initialize Page 2.....	9
Figure 9 IP Assignment.....	10
Figure 10 Firmware Upgrade 1	11
Figure 11 Firmware Upgrade 2	11
Figure 12 Main Page	15
Figure 13 PTZ Panel.....	16
Figure 14 Live View Toolbar	17
Figure 15 General Settings	19
Figure 16 Mode Tab.....	20
Figure 17 Video Stream.....	20
Figure 18 ROI Settings	23
Figure 19 Audio Settings.....	24
Figure 20 Audio File.....	25
Figure 21 Image Settings.....	26
Figure 22 Privacy Mask.....	32
Figure 23 Network General Settings	33
Figure 24 Streaming Protocols-HTTP	35
Figure 25 Streaming Protocols-RTSP	36
Figure 26 SMTP Settings	39
Figure 27 HTTPS Settings	42
Figure 28 Certificate Request.....	43
Figure 29 IEEE 802.1x Configurations – EAP-TLS	44
Figure 30 File Transfer Protocol (FTP)	45
Figure 31 DDNS Interface.....	46
Figure 32 Port Mapping Interface.....	47
Figure 33 System Log Interface	48
Figure 34 Network Discovery Protocols	52
Figure 35 Motion Detection.....	54
Figure 36 Smart Motion.....	56
Figure 37 Scene Change	57
Figure 38 Intrusion Detection	59
Figure 39 Multi Loitering	61
Figure 40 View of Facing the Flow of People	63
Figure 41 Facing the Side Way Flow of People.....	63
Figure 42 People Counter.....	64
Figure 43 Line of People Counter.....	65
Figure 44 Number for In / Out / Stay	65
Figure 45 Face Detection.....	67
Figure 46 Line Crossing Detection	69
Figure 47 Unattended Object Detection.....	71

Figure 48 Missing Object Detection 73

Figure 49 Event & Metadata Scheme..... 74

Figure 50 Alarm Input..... 76

Figure 51 Alarm Output..... 77

Figure 52 Audio Detection..... 79

Figure 53 No SD Card 82

Figure 54 SD Card Onboard 82

Figure 55 System General Settings 86

Figure 56 Preset Settings..... 93

Figure 57 Scan Settings..... 94

Figure 58 Tour Settings 95

Figure 59 Pattern 96

Figure 60 Idle Action..... 97

Figure 61 Power Up Action..... 98

Figure 62 Intelligent Tracking 99

Tables

Table 1 Live View Toolbar Icons 17

Table 2 Cameras Resolution..... 21

Table 3 Cameras Frame Rate 21

Table 4 Port Mapping Parameters 47

Table 5 Compatible SD Card 81

Table 6 Troubleshooting for Common Issues 102

Table 7 List of Symbols 104

INTRODUCTION

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

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 surveillance applications.

The cameras offer 2megapixel resolution at up to 60 frames per second and 4 megapixel resolution 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 illumination in low-light and nighttime scenes up to 50m for dome IPC models, 60m for bullet IPC models and 500m for PTZ models. Also, all the cameras support WDR function at up to 140 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 12V DC adapter for IPC models and 24V AC for PTZ models, all the IPC cameras support Power over Ethernet (PoE) and PTZ cameras support POE+, eliminating the need for a separate power supply and associated wiring. All models also support local video storage on one Micro SD/SDHC/SDXC card slot (1TB) when network service is interrupted.

Supported Browsers

Note: *60 Series cameras support Windows desktop system and don't support mobile system.*

Chrome and Edge browsers are supported:

Browser	Version
Chrome	118.0.5993.118 (Official Build) (64-bit)
Edge	128.0.2739.54 (Official Build) (64-bit)

Browser Minimum Requirement for Hardware

Require the following hardware as a minimum for the web browser:

- Operating system: Microsoft Windows 10
- Processor: Intel Core i5 2.9 GHz or above, such as Intel Core i5-4590 Quad Core 3.3Ghz.
- System memory (RAM): 8GB, DDR3-1600
- Graphics card: 1 GB dedicated video memory, such as NVIDIA GeForce GTX 750 1 GB.
- Network card: 10 Base-T/100 Base-TX Ethernet (RJ-45)

Key Features

The key features in Honeywell Series 60 IP camera are:

Camera

- Up to 8MP (3840 x 2160) cameras
- Video parameter setup, such as electronic shutter and gain
- Video Analytics: Motion Detection, Smart Motion, Scene Change, Intrusion, Multi Loitering, People Counter, Face Detection, Line Crossing Detection, Unattended Object Detection, Missing Object Detection (Be different for different models. More details, please refer to the product datasheet.).
- True WDR (140 dB)
- True day/night mode using a removable IR cut filter
- Low-light with 2D/3D noise reduction saving storage and bandwidth together with smart codec
- For use as part of Video Systems which comply with NDAA

Storage

- Central server backup
- Series 60 camera has one SD card slot, files stored on SD card

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, QoS, SNMP, 802.1X, FTP, SFTP, UDP, ICMP, ARP, TLS

- Support the following security modes: User account and password protection, HTTPS, IP Filter, Digest authentication, TLS1.2 only (applicable for some cameras), TLS 1.2 and TLS 1.3 (applicable for some cameras. More details, please refer to product datasheet.), Stream encryption, AES128 / 256, SSH / Telnet closed, PCI-DSS compliance
- Support the following languages: Arabic, Czech, Dutch, English, French, German, Italian, Japanese, Korean, Polish, Portuguese (Brazil), Russian, Spanish, Turkish, Traditional-Chinese
- Camera configuration and management via Ethernet

Events and Analytics

- Support the following Video Analytics types: Motion Detection, Smart Motion, Scene Change, Intrusion, Multi Loitering, People Counter, Face Detection, Line Crossing Detection, Unattended Object Detection, Missing Object Detection.
- Support the following event types: Video motion detection, Alarm input, Recording notification, Scene change, Abnormal audio
- Support the following event linkage mode: Event notification using digital output, Email, FTP upload 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

ACCESSING THE CAMERA

This chapter contains the following sections:

- [Installing the Unified Tool](#), page 4
- [Discovering Your Camera on the Network](#), page 4
- [Initializing Cameras](#), page 6
- [Assigning a New IP Address to Your Camera](#), page 9
- [Upgrading the Camera's Firmware](#), page 10
- [Accessing the Camera from a Web Browser](#), page 11

Installing the Unified Tool

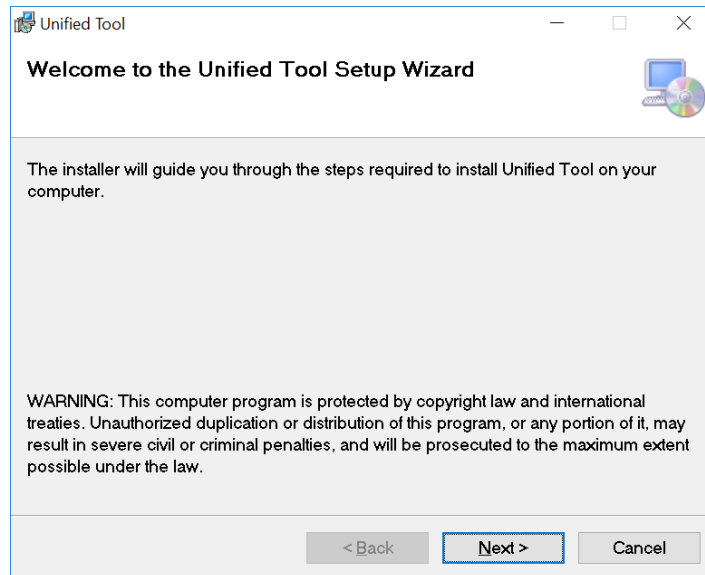
To get the installation package of Unified Tool:

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:

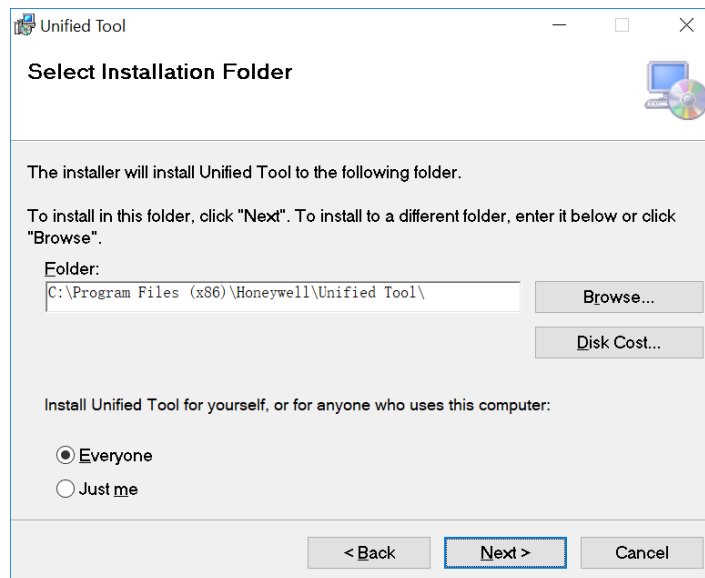
1. Double-click the installation program  in the installation package.

Figure 1 Install Unified Tool



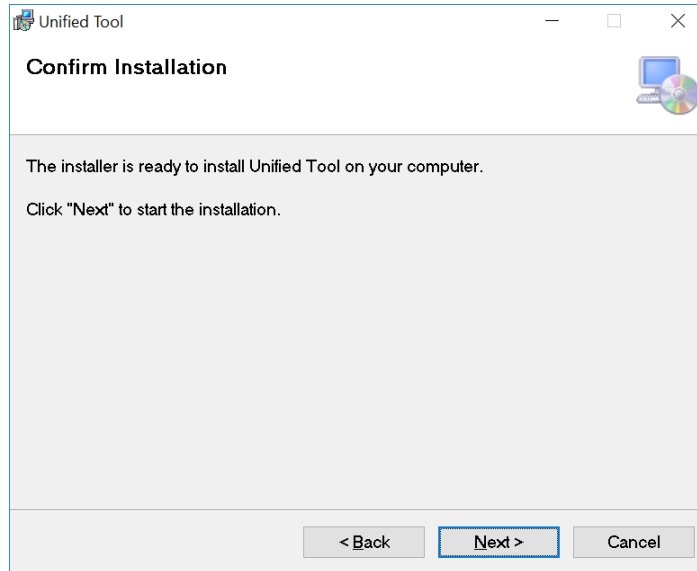
2. Click Next and the following figure is displayed:

Figure 2 Select Installation Folder



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

Figure 3 Confirm 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

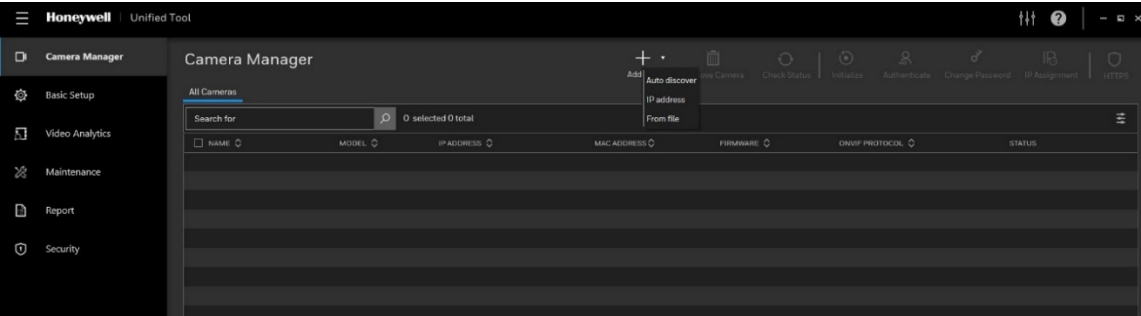
1. Double-click  on the desktop and the following figure is displayed:

Figure 4 Splash Screen



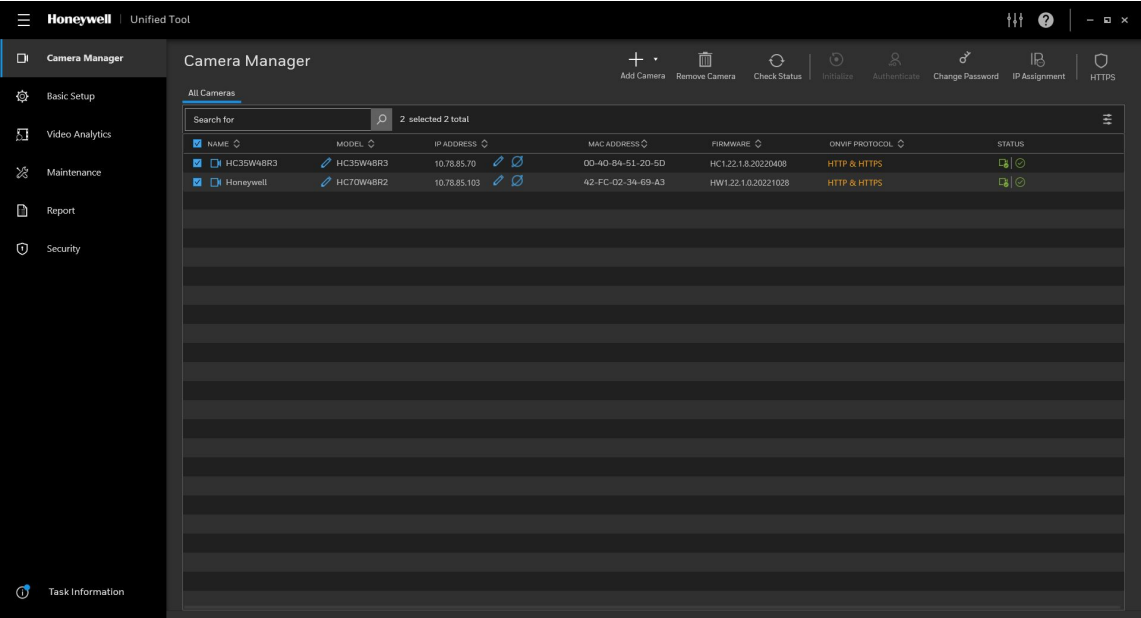
2. Select your language from the dropdown list of Language. Currently, English and traditional Chinese are supported.
3. Check Don't show the splash page on startup and this page can be skipped next time. If you want to check the splash window again, click  as shown in [Figure 6](#) and select the checkbox of Show the splash page on startup.
4. Click  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 devices will be displayed in the devices list.

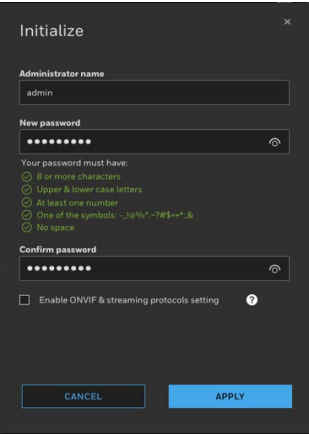
Figure 6 Device List



Initializing Cameras

It is recommended to initialize the 60 series cameras by clicking . By initialization, you can set the camera password in batch.

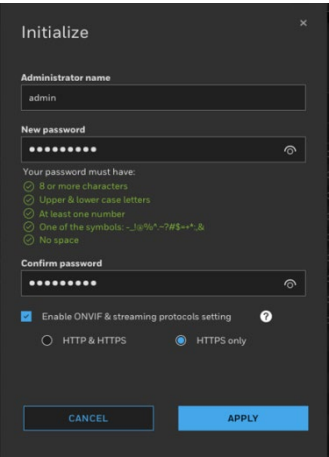
Figure 7 Initialize Page 1

A screenshot of the 'Initialize' dialog box, Page 1. It features a dark background with white text. At the top, the title 'Initialize' is followed by a close button (X). Below the title, there are two input fields: 'Administrator name' with the text 'admin' and 'New password' which is masked with dots. To the right of the 'New password' field is an eye icon. Below these fields, a list of password requirements is shown with green checkmarks: '8 or more characters', 'Upper & lower case letters', 'At least one number', 'One of the symbols: ~!@%&*~7&\$~+~.,&', and 'No space'. Below the requirements is a 'Confirm password' field, also masked with dots and having an eye icon to its right. At the bottom left is a checkbox labeled 'Enable ONVIF & streaming protocols setting' with a question mark icon to its right. At the bottom are two buttons: 'CANCEL' and 'APPLY'.

On the **Initialize** page, set **Administrator name** and **New password**. Select the checkbox to enable **ONVIF & streaming protocols setting**. Select **HTTPS only**. Click **APPLY**.

- Note:**
- *Honeywell strictly recommends to use HTTPs only and Honeywell will not hold responsible for the consequences.*
 - *ONVIF & streaming protocols setting only supports 35 & 70 series camera. Unsupported model will be skipped.*

Figure 8 Initialize Page 2

A screenshot of the 'Initialize' dialog box, Page 2. It has the same layout as Page 1, but with additional options. The 'Enable ONVIF & streaming protocols setting' checkbox is now checked. Below it are two radio button options: 'HTTP & HTTPS' and 'HTTPS only', with 'HTTPS only' being selected. The 'CANCEL' and 'APPLY' buttons remain at the bottom.

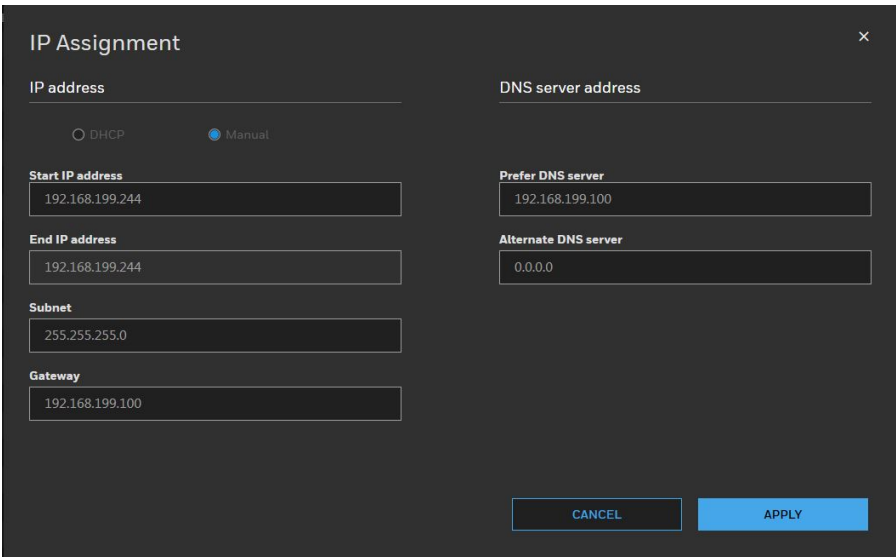
After initializing successfully, you can authenticate the camera and configure other setting.

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 6](#), click  and the following figure is displayed:

Figure 9 IP Assignment



The IP Assignment dialog box is shown with a dark background. It has a title bar with a close button (X). The dialog is divided into two main sections: IP address configuration and DNS server address configuration. In the IP address section, the 'Manual' radio button is selected. Below it, there are four text input fields: 'Start IP address' (192.168.199.244), 'End IP address' (192.168.199.244), 'Subnet' (255.255.255.0), and 'Gateway' (192.168.199.100). In the DNS server address section, there are two text input fields: 'Prefer DNS server' (192.168.199.100) and 'Alternate DNS server' (0.0.0.0). At the bottom right, there are two buttons: 'CANCEL' and 'APPLY'.

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

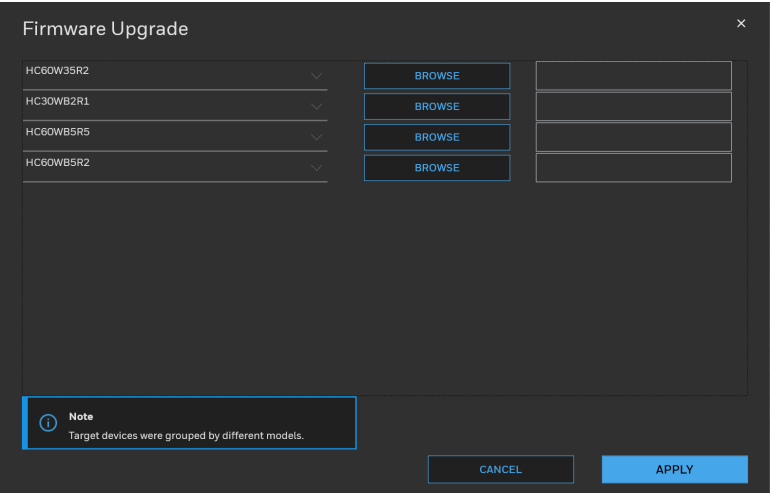
Configure the DNS server address and click **APPLY**.

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 6](#) select target device(s) and click  and the following window is displayed:

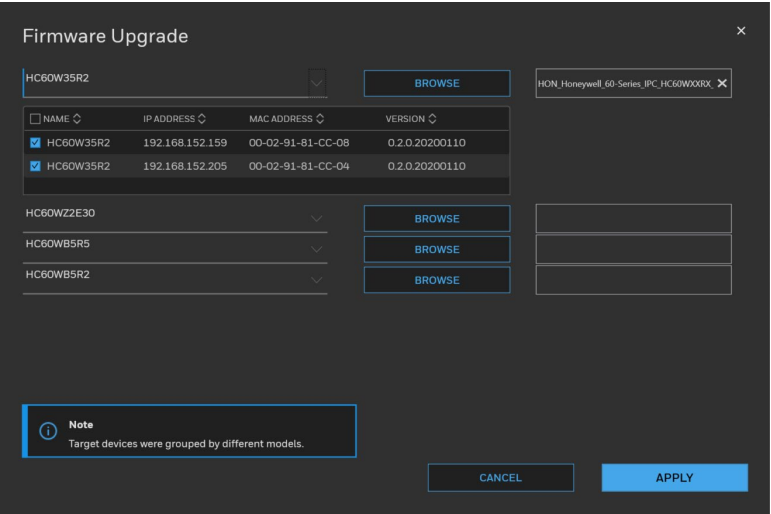
Figure 10 Firmware Upgrade 1



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 11 Firmware Upgrade 2



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

Accessing the Camera from a Web Browser

To access the camera from a web browser, click  next to the IP address of the device as shown in [Figure 6](#).

LOGGING IN & VIEWING LIVE VIDEO

This chapter contains the following sections:

- [Logging in to the Camera via the Web Client](#), page 12
- [Using the Main Page](#), page 15

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

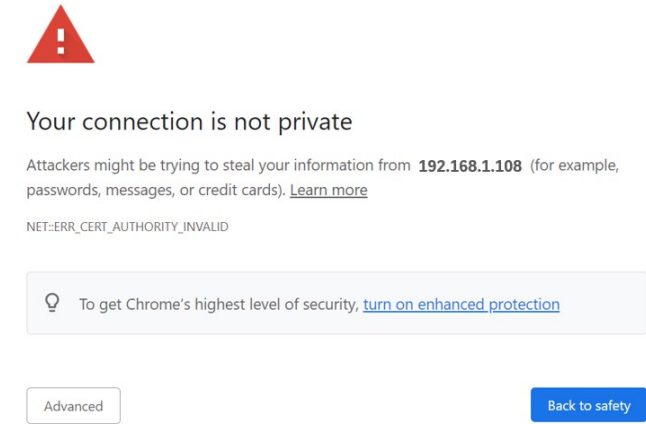
Before you log in to the web client, ensure that the following conditions are met:

- 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]").

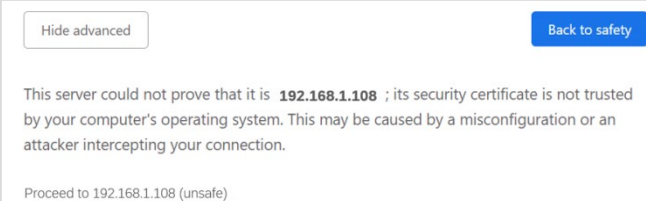
Note: *The new security enhancements do not allow pinging the camera IP address.*

Logging in to the Camera

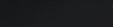
1. Open Google Chrome, type the camera's IP address in the address bar, and then click Enter. For example, if your camera's IP address is 192.168.1.108, you would type <https://192.168.1.108>.
2. The following window is displayed. Click Advanced.



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



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



Honeywell

NETWORK CAMERA

Language

English

1 - New Account Setup

User name

Password

Your password must have:

- ☒ The password must be between 8 to 20 characters
- ☒ Upper & lower case letters
- ☒ At least one number
- ☒ One of the symbols: ~!@#\$%^&*()-+=~!@#\$%^&*()-+=
- ☒ The first character must be a number or letter
- ☒ No space

Confirm password

2 - ONVIF & Streaming Protocol Setup

☒ HTTP & HTTPS(Better compatibility)

☐ HTTP only(Better cyber-security)

1 It is strongly recommended to use HTTPS only. Other protocols may not be secure and may pose a risk to your system.

SAVE

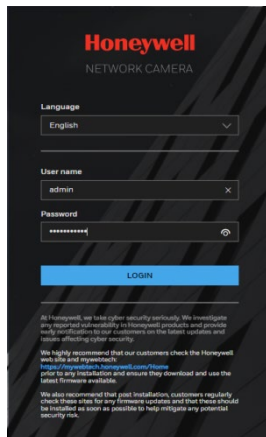
The password must be at least 8 characters in length and contain at least one uppercase letter, one lowercase letter, one number, and one special character (-_!@%^&*~?#\$.+=,;.&). The password cannot be blank. Click **SAVE**.

- ## 5. Setup ONVIF & Streaming Protocol.

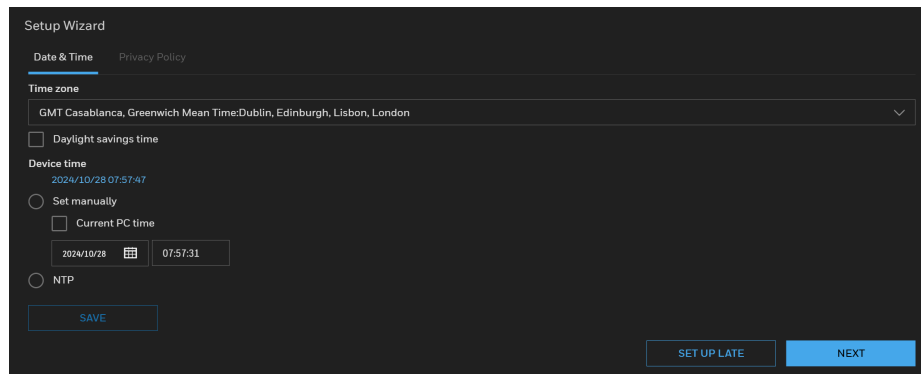
HTTP&HTTPS (better compatibility), HTTPS only (better cyber-security).

It is strongly recommended to use HTTPS only. Other protocols may not be secure and may pose a risk to your system.

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

The image shows the login interface for a Honeywell Network Camera. At the top, the Honeywell logo is displayed in red, with 'NETWORK CAMERA' in white text below it. The background is dark with a subtle pattern of diagonal lines. The login form includes a 'Language' dropdown menu set to 'English', a 'User name' field containing 'admin', and a 'Password' field with masked characters. A blue 'LOGIN' button is positioned below the password field. At the bottom, there is a small disclaimer in white text regarding security and firmware updates.

7. The pop window shows the Setup Wizard to set Date & time and Privacy Policy When the first time to login.

The image displays the 'Setup Wizard' window. It has two tabs: 'Date & Time' (active) and 'Privacy Policy'. Under 'Date & Time', there is a 'Time zone' dropdown menu set to 'GMT Casablanca, Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London'. Below this is a checkbox for 'Daylight savings time'. The 'Device time' section shows the current time as '2024/10/28 07:57:47'. There are two options: 'Set manually' (selected) and 'NTP'. Under 'Set manually', there are fields for 'Current PC time' with a date of '2024/10/28' and a time of '07:57:31'. A 'SAVE' button is at the bottom left. At the bottom right, there are two buttons: 'SET UP LATE' and 'NEXT'.

- **Date & Time**

Set the **Time Zone**, **Daylight saving time**, and **Device Time (set manually or NTP)**.

Click **SET UP LATE** to close the setup wizard. Click **NEXT** to enter the privacy policy setting interface.

- **Privacy Policy**

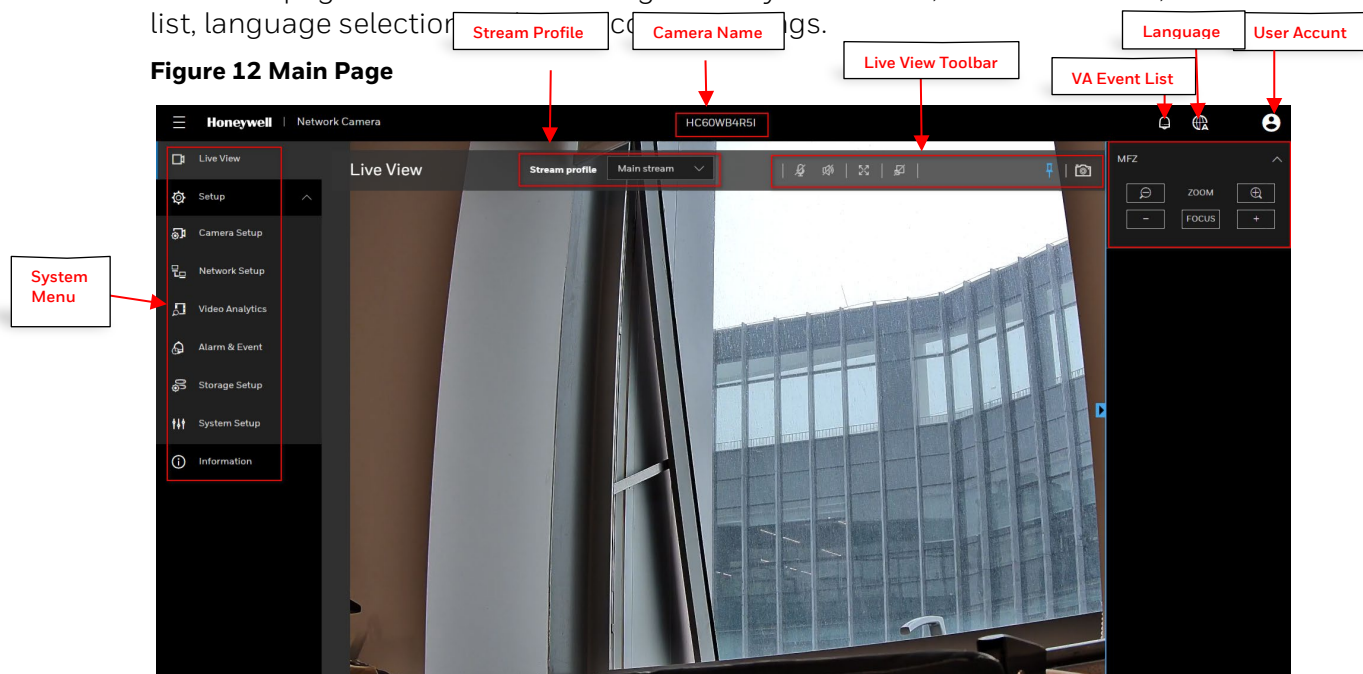
Tick **Do not remind me again** and click **Cancel**, the pop-up window will not show at next time. If untick **Do not remind me again**, the pop-up window will show every time when logging in.

If click **ADD PRIVACY POLICY**, it will go to **System Setup > Maintenance > PRIVACY POLICY** page to import the privacy policy. For details information, refer to [Configuring Privacy Policy](#).

Using the Main Page

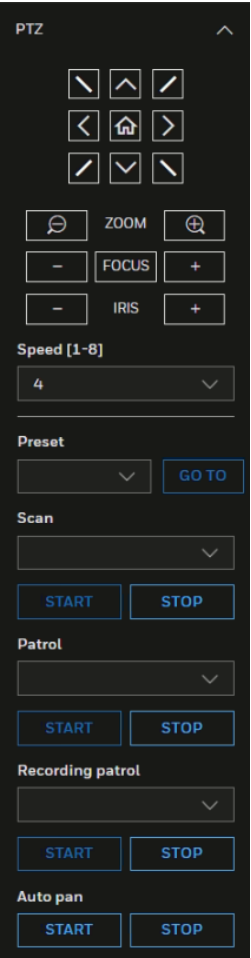
The main page includes the following areas: system menu, live view toolbar, VA event list, language selection, and user account settings.

Figure 12 Main Page



- For MFZ IPC model, an MFZ panel can be accessed by clicking  on the right as shown in [Figure 12](#).
- For PTZ model, a PTZ panel can be accessed by clicking  on the right as shown in [Figure 13](#).
- For HC60WZ4R40WI/ HC60WZ8R40WI model, you can use  in the Live View Toolbar to control the camera wiper. Each time you click , the camera wiper swipes once.

Figure 13 PTZ Panel



For details on PTZ operation, see [Configuring PTZ Settings](#) on page 93.

System Menu

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

Stream Profile

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

Main stream: Delivers high definition video for real-time monitoring, recording, and storage. Uses the most bandwidth.

Sub stream: Delivers high-definition video for real-time monitoring, recording, and storage. Uses the most bandwidth.

Third stream: Delivers low-definition video.

The properties for each stream type are configured on the **Setup > Camera Setup > Video** page (see [Configuring Video Settings](#) on page 19).

Camera Name

You can change the camera name according to your needs. For more information, see [Configuring System General Settings](#) on page 86.

Live View Toolbar

The Live View toolbar allows you to take snapshot. The following table lists the controls in more detail.

Figure 14 Live View Toolbar



Table 1 Live View Toolbar Icons

Icon	Description
	The icon can be enabled from webpage when the microphone is connected to PC or embedded in PC. Click to enable PC microphone. You can talk and the audience can listen through speakers connected to camera. Click it again to disable this option.
	The icon can be enabled from webpage when the speaker is connected to PC or embedded in PC. Click to turn on the audio to listen to the monitoring site. Click it again to turnoff the audio.
	Click to switch to the full screen mode.
	Bouding box on/ bouding box off. When the bouding box is on, it will show boxes on the objects (human or vehicle). When one of the VA alarms (alarms for human or vehicle) is enabled and the objects are in the alarm areas (for the line crossing detection and people counting, the area is full screen), the boxes are red. When the alarm is disabled, the boxes are green. For unattended object detection and missing object detection (the objects are not people or cars), the boxes are red.
	Click to Pin the live view to the toolbar. Click once again to unpin.
	Click to capture and save video images. The captured images will be displayed in a pop-up window. Right click the image and select Save pictureas to save it in JPEG (*.jpg).

Alarm for vehicles or people

VA Event List

To view the list of VA events, click the  icon on the Main Page. The icon  will be blinking when VA alarm comes in.

Note:

Max 100 VA alarms will be listed after clicking  to display event information by cycling. Please go to Information > Logs > Alarm log to see or search more alarm log records. Refer to [Alarm Log](#).

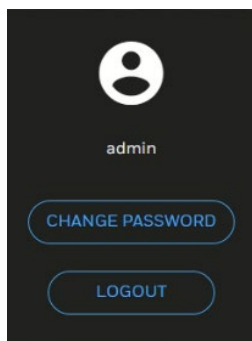
Language

To switch a language, click the  icon on the Main Page.

Administrator Account

Note: *The Administrator's account name and password is set by the user at the first login.*

To configure current login user's password or log out the current user account, click the  icon on the Main Page. The following window is displayed.



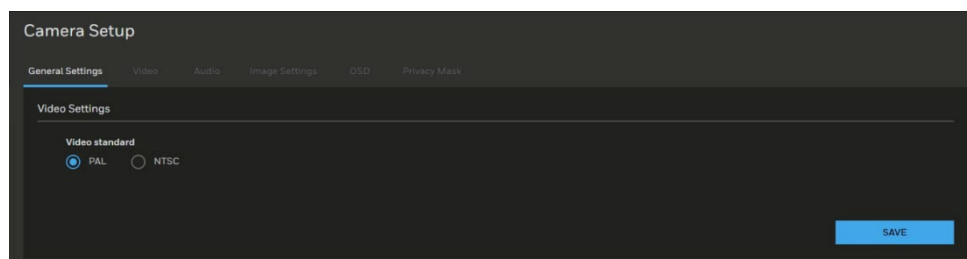
Click **CHANGE PASSWORD** to change the current login user's password.
Click **LOG OUT** to log out the current account.

CONFIGURING CAMERA SETTINGS

Configuring General Settings

Go to **Setup > Camera Setup > General Settings**.
On this page, you can configure the general video settings.
To change the video standard, select PAL or NTSC. Click **SAVE**.

Figure 15 General Settings



Configuring Video Settings

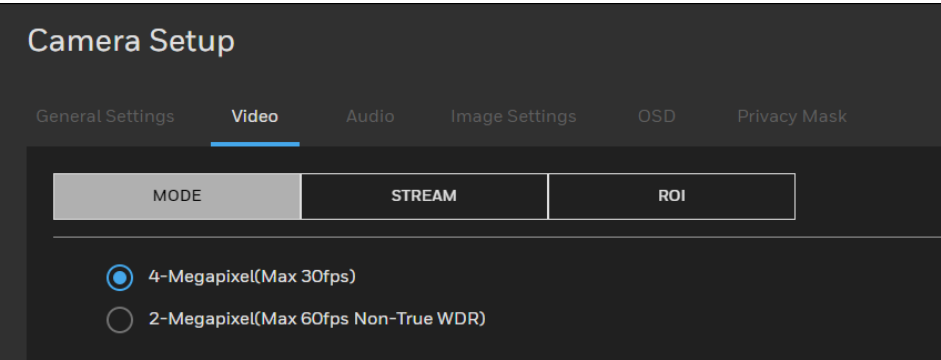
Go to **Setup > Camera Setup > Video**.
This section describes how to configure Video stream and ROI settings.

Mode

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

- Note:**
- *The Mode function is applicable for HC60WZ4R40WI/HC60WZ4R40KI/HC60WZ8R40WI / HC60WZ8R40KI.*
 - *Changing the video mode will clear the following settings: privacy mask, image setting, motion, preset position and focus window.*

Figure 16 Mode Tab



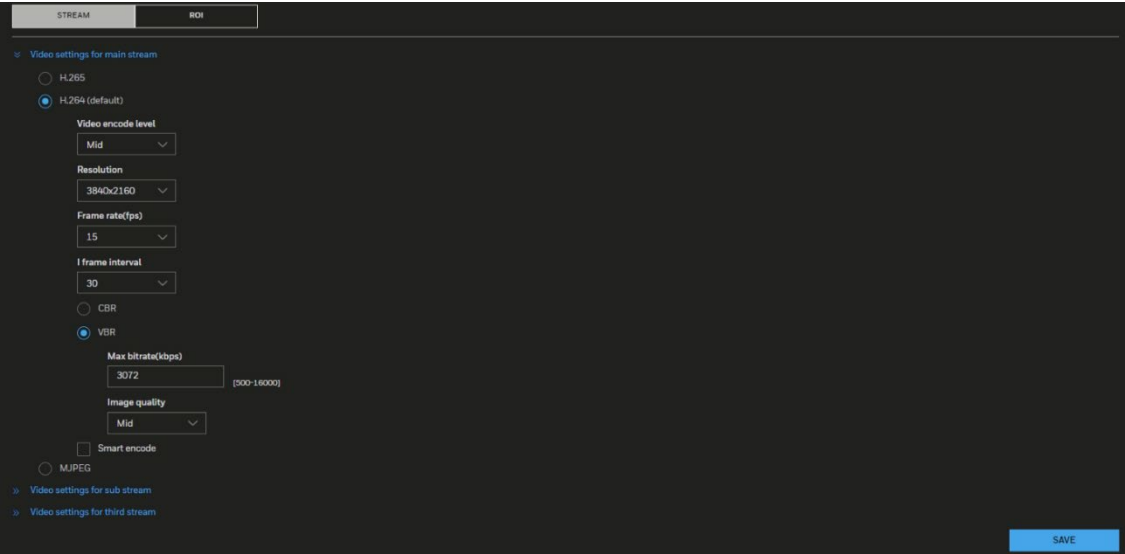
4-Megapixel (Max 30fps): Select it and the maximum resolution will be 2592x1520.

2-Megapixel (Max 60fps Non-True WDR): Select it and the maximum resolution will be 1920x1080.

Video Stream

Go to **Setup > Camera Setup > Video > STREAM**.

Figure 17 Video Stream



Select H.265, H.264(Default), or MJPEG, and apply the video settings for main stream, sub stream and third stream.

Note: *It is recommended to use camera with no more than 5 fps when MJPEG is applied as it consumes large bandwidth.*

Video encode level: Select a value from the drop-down list box.

Resolution: Select a value from the drop-down list box. A higher resolution means better image quality.

See the following table for resolution of each model:

Table 2 Cameras Resolution

Model	Main Stream	Sub Stream	Third Stream
HC60W34R2I/HC60W44R2I/HC60WB4R2I/HC60WB4R5I/HC60WC5I/	2592x1520/1920x1080/1280x720 25/30fps	1920x1080/704x576(PAL)/704x480(NTSC)/640x480/352x288(PAL)/352x240(NTSC) 25/30fps	640x480/352x288(PAL)/352x240(NTSC)/320x240 25/30fps
HC60WZ4R40WI/HC60WZ4R40KI	2592x1520/1920x1080/1280x720 25/30fps (1920x1080 50/60 fps with WDR off)	1920x1080/704x576(PAL)/704x480(NTSC)/640x480/352x288(PAL)/352x240(NTSC) 25/30fps	640x480/352x288(PAL)/352x240(NTSC)/320x240 25/30fps
HC60W32R2I/HC60W42R2I/HC60WB2R2I	1920x1080 50/60fps, 1280x720 25/30fps	1920x1080/704x576(PAL)/704x480(NTSC)/640x480/352x288(PAL)/352x240(NTSC) 25/30fps	640x480/352x288(PAL)/352x240(NTSC)/320x240 25/30fps
HC60WZ8R40KI/HC60WZ8R40WI 8MP	3840x2160 2592x1944 2592x1520 2560x1440 2304x1296 1920x1080 1280x720 25/30fps	704x480(NTSC) 704x576(PAL) 640x480 352x240(NTSC) 352x288(PAL) 25/30fps	1920x1080 1280x720 640x480 352x240(NTSC) 352x288(PAL) 320x240 25/30fps
HC60WZ8R40KI/HC60WZ8R40WI 2MP	1920x1080 1280x720 50/60 fps with WDR off	704x480(NTSC) 704x576(PAL) 640x480 352x240(NTSC) 352x288(PAL) 25/30fps	640x480 352x240(NTSC) 352x288(PAL) 320x240 25/30fps

Frame rate(fps):

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 video standard is set to **PAL**, the frame rates are selectable from 1-50 fps. If the video standard is set to **NTSC**, the frame rates are selectable from 1-60 fps.

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

See the following table for frame rate of each model:

Table 3 Cameras Frame Rate

Connection Type	Camera	Main Stream	Sub Stream	Third Stream
HTTP	HC60W34R2I HC60W44R2I HC60WB4R2I HC60WB4R5I HC60WC5I HC60WZ4R40WI	Frame rate (FPS): PAL 25/NTSC 30 I frame interval: PAL 50/NTSC 60 Bit rate (Kbps):12000	Frame rate (FPS): PAL 25/NTSC 30 I frame interval: PAL 50/NTSC 60 Bit rate (Kbps): 6000	Frame rate (FPS): PAL 25/NTSC 30 I frame interval: PAL 50/NTSC 60 Bit rate (Kbps): 1500

Connection Type	Camera	Main Stream	Sub Stream	Third Stream
	HC60WZ4R40KI			
	HC60WZ8R40KI HC60WZ8R40WI	Frame rate (FPS): PAL 25/NTSC 30 I frame interval: PAL 50/NTSC 60 Bit rate (Kbps): 16000		
	HC60W32R2I HC60W42R2I HC60WB2R2I	Frame rate (FPS): PAL 25/NTSC 30 I frame interval: PAL 50/NTSC 60 Bit rate (Kbps): 12000		
HTTPS*	HC60W34R2I HC60W44R2I HC60WB4R2I HC60WB4R5I HC60WC5I HC60WZ4R40WI HC60WZ4R40KI HC60W32R2I HC60W42R2I HC60WB2R2I	Frame rate (FPS): PAL 25/NTSC 30 I frame interval: 30 Bit rate (Kbps): 12000	Frame rate (FPS): PAL 25/NTSC 30 I frame interval: PAL 50/NTSC 60 Bit rate (Kbps): 6000	Frame rate (FPS): PAL 25/NTSC 30 I frame interval: PAL 50/NTSC 60 Bit rate (Kbps): 1500
	HC60WZ8R40KI HC60WZ8R40WI	Frame rate (FPS): PAL 25/NTSC 30 I frame interval: PAL 50/NTSC 60 Bit rate (Kbps): 16000		

- Note:**
- For encryption under HTTPS.
 - If you need to enable functions that affect performance (such as VA, SD card recording), it is recommended to reduce the corresponding parameter values instead of using the maximum parameter of above table.
 - The image parameter will be set as default value if the mode of video is changed.

I-frame interval: Determine within how many frames interval the firmware will plant and I frame. The shorter the duration, the more likely you will get better video quality, but at the cost of higher network bandwidth consumption.

CBR: Constant Bit Rate

The bit rate remains constant (recommended for low-bandwidth environments).
Required if MJPEG compression is used.

VBR: Variable Bit Rate

The bit rate changes according to the complexity of the scene.

Max bitrate(kbps): Indicates the maximal value of the bit rate. Set 500~12000 for max bitrate.

Image Quality: Select a desired quality ranging from Lowest to Highest.

- Note:**
- Selecting high compression level from MAXPRO NVR will result in low image quality in camera.
 - Selecting low compression level from MAXPRO NVR will result in high image quality in camera.

Smart encode: Check the checkbox to enable Smart Encode.

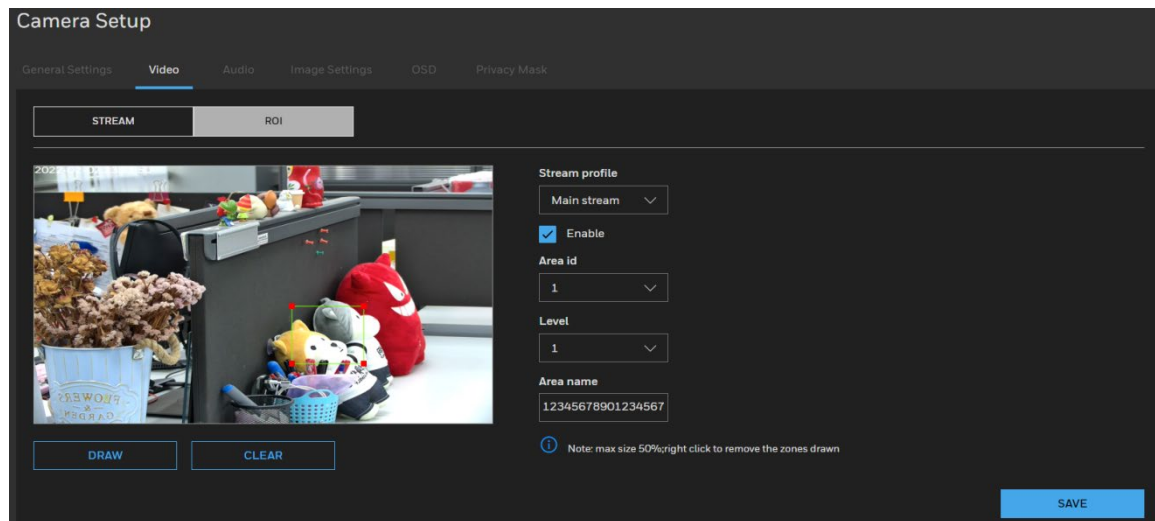
- Smart encode includes H.264 & H.265.
- The storage space will be reduced fifty percent when smart encode is enabled.
- Only main stream supports smart encode.

ROI

The ROI function allows you to configure 8 ROI windows (Region of Interest, with Foreground quality) on the screen. Areas not included in any ROI windows will be considered as the non-interested areas. The details in the ROI areas will be transmitted in a higher-quality video format. you may set up an ROI window as a privacy mask by covering a protected area using an ROI window, while the rest of the screen becomes the non-interested area.

Go to **Setup > Camera Setup > Video > ROI**.

Figure 18 ROI Settings



Stream profile: select **Main stream**, **Sub stream**, or **Third stream** to set the stream profile.

Enable: Check the checkbox to enable the ROI (Region of Interest).

Area id: Select a value from the drop-down list box to set the ROI area ID. You can add 8 areas in total.

Level: Select a value from the drop-down list box to set the visual effect of ROI. Setting as Level 1 will get the best effect for highest quality video within the interested area and the fuzziest video for non-interested areas.

Area name: Enter a customized name for areas. The maximum value cannot exceed 32 bytes.

Note: *The parameters for ROI can't been configured when the stream is selected as MJPEG or smart encode.*

Configuring Audio Settings

Go to **Setup > Camera Setup > Audio**.

Figure 19 Audio Settings

The screenshot shows the 'AUDIO' settings page. It is divided into two sections: 'Audio Input Settings' and 'Audio Output Settings'. In the 'Audio Input Settings' section, the 'Audio input' checkbox is checked. Below it, the 'Audio input type' is set to 'Microphone' via a dropdown menu. The 'Audio input volume' is represented by a slider set to 90, with a range from 0 to 100%. The 'Audio encode type' is set to 'G711ALAW' via a dropdown menu. In the 'Audio Output Settings' section, the 'Audio output' checkbox is checked. The 'Audio output type' is set to 'Internal' via a dropdown menu. The 'Audio output volume' is represented by a slider set to 80, with a range from 0 to 100%. A blue 'SAVE' button is located at the bottom right of the page.

Audio Input Settings

Audio input: Check the checkbox to enable Audio input.

Audio input type: Select the Microphone or Line-in option.

Note: *The Microphone option is only applicable for Micro Dome cameras.*

Audio input volume: Microphone gain or Line-in gain. The Microphone gain or Line-in gain option is displayed according to the Audio input option selected. Select the gain of the external audio input according to ambient conditions. Adjust the gain from 0% (least) to 100% (most).

Audio encode type: Select audio codec as **G711ALAW** and **G711ULAW** and the bit rate.

Audio Output Settings

Audio output: Check the checkbox to enable Audio output.

Audio output type: Select the Line-out option.

Audio output volume: The Line-out option is displayed according to the Audio output option selected. Select the volume of the external audio input according to ambient conditions. Adjust the volume from 0% (least) to 100% (most).

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

Audio File

Go to **Setup > Camera Setup > Audio > AUDIO FILE**

Figure 20 Audio File

Camera Setup

General Settings

Video

Audio

Image Settings

OSD

Privacy Mask

AUDIO

AUDIO FILE

Audio File

ID	FILE NAME	CYCLE NUMBER	OPERATE
1	Dangerous area. Keep away.wav	1	
2	Deep water. pay attention to safety.wav	1	
3	Do not touch valuables.wav	1	
4	Hello welcome.wav	1	
5	High altitude. No climbing.wav	1	

Schedule

SAVE

There are 3 default files, users can set the cycle number, click to test listen.

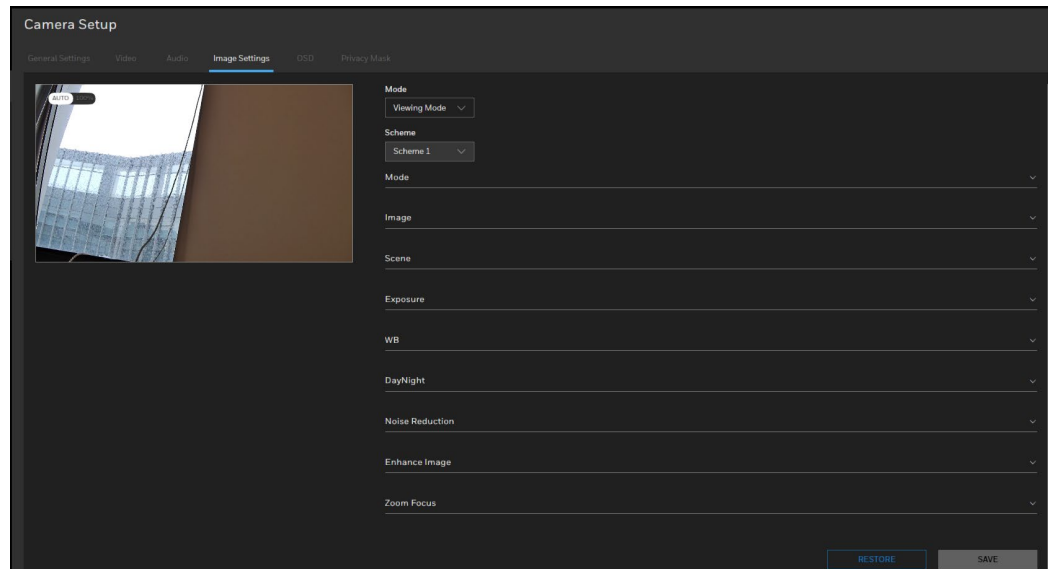
If you want to set the costumed audio Click to choose file to upload a new audio.

The file type should be WAV, size must be less than 250 Kb, the sampling rate should be 8000HZ.

Configuring Image Settings

Go to **Setup > Camera Setup > Image Settings**.
On this page, you can configure the parameters for **Mode, Scheme, Image, Scene, Exposure, WB, DayNight, Noise Reduction** and **Enhance Image**.

Figure 21 Image Settings



Mode

View Mode: Users only view the parameters of image settings.

Edit Mode: Users modify the parameters of image settings.

Scheme

When the **Mode** is edit mode, there are four schemes can be set, every scheme is independent, you can set each one for different parameters for different scene.

Image Adjustment

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

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

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

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

Scene Mode

Scene: Select indoor/outdoor to change the scene mode.

Mirror: Select Normal/Horizontal/ Vertical/ Horizontal + Vertical to mirror the image.

Aisle Mode: The image rotates 90 degrees clockwise when aisle mode is enabled.

Note: • *It will not be able to stream out when the aisle mode is enabled and sub stream or*

third stream is set on 352*240 or 320*240.

- Not all OSD will change with the image clockwise when aisle mode is enabled
- When the aisle mode is enabled, the Crowds Detection function is invalid.

Normal	Vertical	Normal	Horizontal	Normal	Horizontal + Vertical	Aisle

Exposure

Meter area is used to select the exposure area. Select Whole/Center spot/Center area for different area exposure settings.

Exposure mode: The exposure modes include:

- **Auto:** The system performs auto exposure based on the monitoring environment.
- **Manual:** Set **Shutter Setting/Iris Setting/Gain Setting** to manually adjust the exposure level for getting the best image quality.
- **Shutter priority:** you can select fixed shutter and the camera will automatically tune the gain and iris to match an optimal exposure level. Gain range will be under Max value.
- **IRIS priority:** you can select IRIS F-number and the camera will automatically tune the gain and exposure time to match an optimal exposure level. Gain range and exposure time will be under Max value.

Max shutter: The device automatically adjusts the shutter time based on the ambient light under Max value setting.

Max gain: The device automatically adjusts the gain based on the ambient light under Max value setting.

White Balance (WB) Setting

Mode: Adjust the value for the best color temperature.

- Auto: Select it and the camera will automatically adjust the color temperature.
- Tungsten/ Fluorescent/ Daylight/Shadow: Select it and the camera will change to Tungsten/ Fluorescent/ Daylight/Shadow color temperature.

Note: For PTZ models, Tungsten/Daylight color temperature is supported.

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

DayNight Setting

The day night mode settings vary based on device models.

D/N setting: It can be set to **Auto**, **Day mode**, **Night mode** or **Timing**.

- **Auto**

The camera automatically switches between day and night mode (switches on/off IR cut filter) by judging the level of ambient light directly from image light level.

For models HC60W34R2I/ HC60W44R2I/ HC60WB4R2I/ HC60WB4R5I/ HC60WZ4R40WI /HC60WZ4R40KI /HC60W32R2I/ HC60W42R2I/ HC60WB2R2I, the camera automatically switches between day and night mode to switch on/off IR cut filter by judging the level of ambient light which identified by the light dependent resistor (LDR).

- Note:**
- *The Camera will turn on the IR LED for Night mode if you select Build-in IR illuminator under Turn on illuminator in night mode.*
 - *When selecting Auto mode for D/N setting, the camera will lock to Night mode if it switches between Day mode and Night mode for 5 times within 10 minutes to adapt the ambient light changes, and it will unlock to Auto mode after 1 hour. Or you can change it as Day mode or Night mode manually to unlock it.*

Delay(s): Set the delay time for switching day to night or night to day when the camera detect to switch.

D/N switch sensitivity: Set the sensitivity for switching day to night/night to day.

- **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.

- **Timing**

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.

DTN time: After selecting **Timing** for **D/N setting**, set **DTN time** to switch time for day mode to night mode

NTD time: After selecting **Timing** for **D/N setting**, set **NTD time** to switch time for night mode to day mode

Turn on illuminator in night mode: Select **Build-in IR illuminator** to enable the IR led light. Select **None** to disable it.

IR adjustment:

- **Smart:** Select this smart IR function to control the luminance of IR lights automatically. The IR luminous intensity will be automatically adjusted according to the shooting scene. When the light received by the camera is strong, it will automatically reduce the IR luminous intensity to improve the overexposure of fill light.
- **Manual:** Select it to control the luminance of IR lights manually.

- For models HC60WB4R2I / HC60WB4R5I / HC60WC5I / HC60W42R2I / HC60WZ4R40WI / HC60WZ4R40KI / HC60WB2R2I, you can set **Near/Centre/Far** IR light distance by **Manual** configuration to drag the slider to left/right to decrease/increase the luminance of IR lights.
- For model HC60W34R2I and HC60W32R2I, you can set **Near/Far** IR light distance by **Manual** configuration.
- For other models' cameras, you can drag the slider to set the IR lights strength manually.

Note: *For HC60WZ4R40WI and HC60WZ4R40KI, the sum of the values for Near and Far is not allowed to exceed 100.*

Noise Reduction

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

2D NR/3D NR: Reduce noise of image.

Max Strength: To get better 3D noise reduction performance, please choose a higher value to set.

Note: *3D Noise Reduction is mostly applied in low-light conditions. Applying a high level 3D Noise Reduction will cause lag or motion blur in a low-light condition with fast moving objects, suggest to select a lower level of 3D Noise Reduction in this situation*

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

Enhance Image

To enhance image, you can apply the below functions to adjust the image.

Note: *The functions may vary according to different camera models.*

WDR (Wide Dynamic Range)

By lowering the brightness of the brightest area, and enhancing the brightness of the darkest area, WDR balances brightness and darkness in a scene so that both the darkest area and the lightest area can be seen clearly at the same time.

This value ranges from 1 to 100. The default value is 50.

BLC (Backlight Compensation)

The camera automatically adjusts the exposure to suit the conditions, so that the darkest area of the video can be seen.

This value ranges from 1 to 100. The default value is 50.

HLC (Highlight Compensation)

When the HLC function is enabled, the camera can lower the brightness of the brightest section of video, according to the selected HLC control level. HLC can reduce the amount of halo and lower the brightness of the entire video image.

This value ranges from 1 to 100. The default value is 50.

DeFog: Check the checkbox to enable defog. The image quality is compromised in foggy or hazy environment and defog can be used to improve image clarity.

Anti-shake: Check the checkbox to enable **Anti-shake**.

The system provides smooth video (Electronic Image Stabilization) after enabling anti-shake. The quality of the images is affected by the vibration intensity of the camera.

Note: *The Anti-shake functions is only applicable for PTZ model C60WZ4R40WI and HC60WZ4R40KI.*

Zoom Focus (IPC Models)

- Note:**
- *The Zoom Focus feature in this section is only applicable for MFZ camera models HC60W34R2I/HC60W32R2I/HC60W44R2I/HC60W42R2I/HC60WB4R2I/HC60WB2R2I/HC60WB4R5I 5.*
 - *The Zoom Focus feature in this section is not applicable for fix camera models HC60WC5I.*

Click  to zoom out the video image or click  to zoom in the video image.

Click  and  to adjust the **Focus** setting.

AUTO FOCUS ONCE: Click it to perform auto focus for one time and please wait for the auto focus completion before you decide to click it once more to perform auto focus again.

LENS INITIALIZATION: Click it to recover the lens configuration as default value.

Note: *The lens configuration needs to be recovered When there are unexpected situations that the lens configuration is messed up. Honeywell recommends not initializing the lens by yourself and if you require additional assistance, please contact Honeywell Technical Support.*

D/N auto focus: check it to enable **D/N auto focus**. Then auto focus will be triggered when a camera is switching day/night mode.

Zoom Focus (PTZ Models)

Note: *The Zoom Focus feature in this section is only applicable for PTZ models HC60WZ4R40WI and HC60WZ4R40KI.*

Digital zoom: check it to enable digital zoom. The max digital zoom is 16x.

Set **Focus mode** to **Auto**, **Manual**, **Semi-automatic** or **Focus by zoom**.

Auto: The focus is adjusted automatically whenever the scene changes.

Auto focus sensitivity: Drag the slider to set the sensitivity. When the sensitivity is high, small scene change can trigger the auto focus. When the sensitivity is low, the auto focus will not be triggered unless there's big scene change. The **Auto focus sensitivity** feature is only applicable for **Auto** mode.

Manual: The focus is adjusted manually by the user.

Click  to zoom out the video image or click  to zoom in the video image.

Click  and  to adjust the **Focus** setting.

AUTO FOCUS ONCE: Click it to perform auto focus for one time and please wait for the auto focus completion before you decide to click it once more to perform auto focus again.

Semi-automatic: The focus is triggered when pan/tilt/zoom happens.

Focus by zoom: The focus is adjusted whenever zoom happens.

The least focus distance: select the least focus distance. This value limits the focus distance. The camera will focus on objects out of the specified distance. For example, if the focus limit is set to **6m**, the camera will only focus on objects farther than 6 meters away.

Configuring OSD

Go to **Setup > Camera Setup > OSD**. The **OSD** page is displayed,

Time: Enable it to display time information in live view image. Set **Date format** and **Time format**.

Video title: Enable and enter video title to display video title in live view image.

(for PTZ model only) PTZ: Enable to display PTZ coordinates, zoom ratio, and **Preset/Scan/Patrol/Recording Patrol** label when moving PTZ.

Position: Set the OSD display position.

Font size: Set the font size of OSD display.

Configuring Privacy Mask

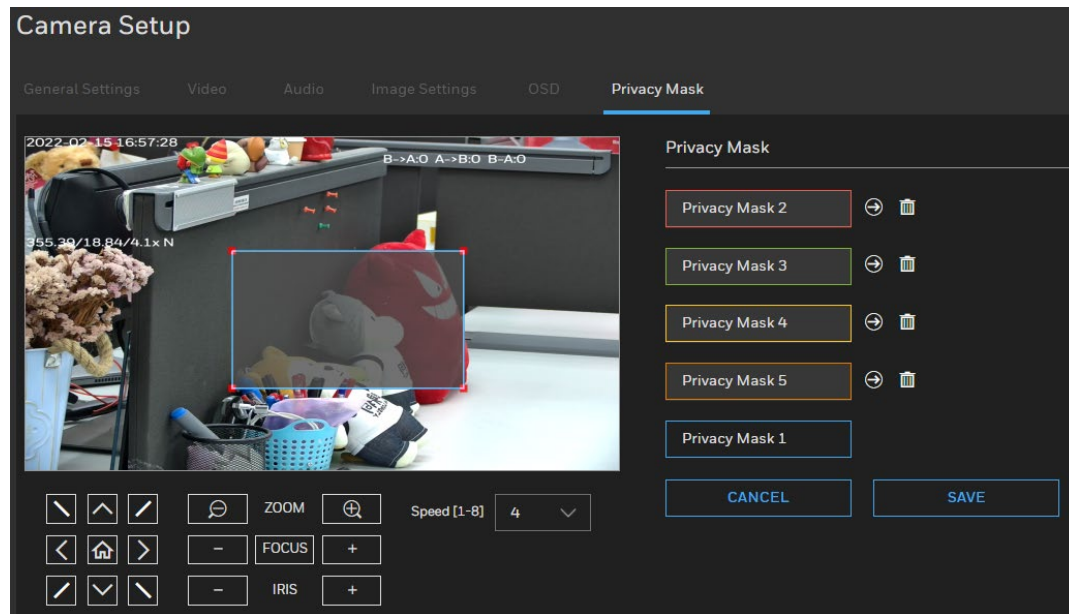
On this page, you can block out sensitive view areas to address privacy concerns. Go to **Setup > Camera Setup > Privacy Mask**.

To configure privacy masks:

1. Click **ADD MASK** to add a new privacy mask window on the video screen.
2. Drag the corner of the rectangle to create a new masking window.

3. Enter a name for the privacy mask and click SAVE to enable the setting.

Figure 22 Privacy Mask



- Note:**
- The object should be in the middle of the video screen and the setting size of privacy mask should be 1.5~2.5 times of the object size.
 - Up to 4/5 privacy mask windows for IPC/PTZ cameras can be configured on the same screen.
 - If you want to delete the privacy mask window, click  on the right side of privacy mask window name. Click  to go to the relate privacy mask position.

CONFIGURING NETWORK SETTINGS

Configuring Network General Settings

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

Go to **Setup > Network Setup > General Settings**.

Figure 23 Network General Settings

The screenshot shows the 'Network Setup' configuration page with the 'General Settings' tab selected. The 'Network Type' section is expanded, showing options for 'IP protocol' (IPv4 selected), 'DHCP' (unselected), and 'Fixed IP' (selected). Below these are input fields for 'IP address' (192.168.0.46), 'Subnet mask' (255.255.0.0), and 'Default gateway' (192.168.2.254). Further down are fields for 'Preferred DNS server' (192.168.0.1), 'Alternate DNS server' (192.168.0.2), and 'MTU(1280~1500)' (1500).

Field	Value
IP protocol	IPv4
DHCP	☐
Fixed IP	☒
IP address	192.168.0.46
Subnet mask	255.255.0.0
Default gateway	192.168.2.254
Preferred DNS server	192.168.0.1
Alternate DNS server	192.168.0.2
MTU(1280~1500)	1500

Select IPv4/IPv6 for IP protocol.

When IPv4/IPv6 is enabled, by default, the network camera will listen to router advertisements and be assigned with a link-local IPv4/IPv6 address accordingly.

DHCP: 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: 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 gateway, 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 gateway: 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.

Preferred DNS Server: The primary domain name server that translates hostnames into IP addresses.

Alternate DNS Server: Secondary domain name server that backups the Primary DNS.

MTU (1280~1500): Set the maximum value of network transmission data packets.

Configuring Streaming Protocols

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

Figure 24 Streaming Protocols-HTTP

The screenshot shows a web interface for configuring streaming protocols. At the top, there are four tabs: 'General Settings', 'Streaming Protocols' (which is active and highlighted with a blue underline), 'SMTP', and 'SNMP'. Below the tabs, there are two buttons: 'HTTP' and 'RTSP'. The 'HTTP' button is selected and highlighted in a light gray. Below these buttons, there are two sections. The first section is titled 'Authentication' and contains a dropdown menu with 'digest' selected. The second section is titled 'HTTP port' and contains a text input field with the value '80'.

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 90.

Authentication: 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.

Figure 25 Streaming Protocols-RTSP

The screenshot shows the 'Network Setup' interface with the 'Streaming Protocols' tab selected. Under the 'RTSP' sub-tab, the 'Authentication' is set to 'digest'. The 'RTP port for video' is set to '555', and the 'RTSP port' is set to '554'. A blue-bordered box contains a message: 'The port changing will take effect after restart the device' followed by RTSP URLs for Main, Sub, and Third streams using the configured ports. Below this, the 'RTCP port for video' is set to '556'. At the bottom, there are three links for multicast settings for the Main, Sub, and Third streams.

Network Setup

General Settings **Streaming Protocols** SMTP SNMP QoS HTTPS 802.1x

HTTP RTSP

Authentication

digest

RTP port for video

555

i The port changing will take effect after restart the device

RTSP port

554

i The port changing will take effect after restart the device
Main stream: rtsp://159.99.251.222:554/live1s1.sdp
Sub stream: rtsp://159.99.251.222:554/live1s2.sdp
Third stream: rtsp://159.99.251.222:554/live1s3.sdp
Or
Main stream: rtsp://159.99.251.222:554/live/1/1
Sub stream: rtsp://159.99.251.222:554/live/1/2
Third stream: rtsp://159.99.251.222:554/live/1/3

RTCP port for video

556

» Multicast settings for Main Stream

» Multicast settings for Sub Stream

» Multicast settings for Third Stream

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 90.

Authentication: Authentication provides better protection against unauthorized access.

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 one of the below RTSP URLs command to request transmission of the streaming data.

- [rtsp://IP address: Port/live1<Streaming ID>.sdp](#)

Note:

IP address: The device IP address

Port: RTSP port, default is 554

live1<Streaming ID>.sdp: liv1s1.sdp for Mainstream, liv1s2.sdp for Sub stream, liv1s3.sdp for 3rd stream.

For example: Follow below step to stream out rtsp streaming.

1. Launch an RTSP player.
2. Choose File > Open URL. A URL dialog box will pop up.
3. Type the below URL command in the text box for each stream.

The live video will be displayed in your player.

Mainstream: <rtsp://192.168.0.108:554/live1s1.sdp>

Sub stream: <rtsp://192.168.0.108:554/live1s2.sdp>

Third stream: <rtsp://192.168.0.108:554/live1s3.sdp>

- <rtsp://IP address: Port/live/Camera ID/Streaming ID>

Note:

IP address: The device IP address

Port: RTSP port, default is 554

Live: Keep Live as default.

Camera ID: 1

Streaming ID: 1 for Mainstream, 2 for Sub stream, 3 for 3rd stream.

For example: Follow below step to stream out rtsp streaming.

1. Launch an RTSP player.
2. Choose File > Open URL. A URL dialog box will pop up.
3. Type the below URL command in the text box for each stream.

The live video will be displayed in your player.

Mainstream: <rtsp://192.168.0.108:554/live/1/1>

Sub stream: <rtsp://192.168.0.108:554/live/1/2>

Third stream: <rtsp://192.168.0.108:554/live/1/3>

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

- 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 555.
- RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default, the RTSP port number is set to 554.
- 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 556.

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.

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

Multicast group address: Enter the Multicast group address.

Multicast video port: The ports can be changed to values between 1025 and 65535. The default value is 25330.

Multicast audio port: The ports can be changed to values between 1025 and 65535. The default value is 25430.

Multicast metadata port: The ports can be changed to values between 1025 and 65535. The default value is 25530.

Multicast TTL: The multicast TTL (Time To Live) is the value that tells the router the range a packet can be forwarded. The default value is 60.

Note: *Multicast is enabled by default in camera.*

Configuring SMTP Settings

If the Simple Mail Transfer Protocol (SMTP) function is enabled, the device automatically sends JPG images and alarm information to specified email addresses when an alarm is generated.

Go to **Setup > Network Setup > SMTP**.

Figure 26 SMTP Settings

The screenshot shows the 'Network Setup' page with the 'SMTP' tab selected. The page contains several input fields for configuring email settings. The fields are: 'SMTP server address' (empty), 'SMTP server port' (25, with a range of [1 ~ 65535]), 'User name' (empty), 'Password' (empty), 'Sender e-mail address1' (empty), 'Recipient e-mail address1' (empty), 'Recipient e-mail address2' (empty), 'Recipient e-mail address3' (empty), 'Recipient e-mail address4' (empty), 'Recipient e-mail address5' (empty), 'Transport mode' (No Encrypt, with a dropdown arrow), and 'Send interval' (0, with a range of [0 ~ 60s]).

SMTP server address: IP address of the SMTP server.

SMTP server port: Port number of the SMTP server.

User name: User name of the mailbox for sending emails.

Password: Password of the mailbox for sending emails.

Sender e-mail address1: Mailbox for sending emails.

Recipient_e-mail_address1: Email address of recipient 1.

Recipient_e-mail_address2: Email address of recipient 2.

Recipient_e-mail_address3: Email address of recipient 3.

Recipient_e-mail_address4: Email address of recipient 4.

Recipient_e-mail_address5: Email address of recipient 5.

Transport mode: Email encryption mode. Set this parameter based on the encryption modes supported by the SMTP server.

Send interval: The interval for sending ranges from 0 to 60 seconds. The system will not immediately send the email when the alarm occurs. When an alarm, motion detection, or other event occurs to activate an email, the system sends one email within the interval that you have specified here. This reduces the load on the email server when multiple emails are triggered simultaneously.

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.

Enable SNMPv1, SNMPv2c: Check to enable SNMPv1, SNMPv2c. SNMPv1 and SNMPv2c use communities to establish trust between managers and agents. Agents support three community names, write community, read community and trap.

Write community: Name of write community. The write community only can modify data.

Read community: Name of read community. The write community only can read data.

Trap address: IP address of the trap.

Trap port: Management port of accepting message from trap.

Trap community: community string of trap. The trap community string allows the manager to receive asynchronous information from the agent.

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

SNMPv3 uses community strings but allows for secure authentication and communication between SNMP manager and agent.

Read security name: Name of read security.

Write security name: Name of write security.

Security level: Security Level between SNMP manager and agent, includes three levels:

- Noauth: No authentication and no encryption
- Auth: Authentication but no encryption
- Priv: Authentication and encryption

Auth algorithm: Authentication Algorithm, includes MD5 and SHA.

Auth password: Authentication password.

Encry Algorithm: Encryption Algorithm, includes DES and AES.

Encry Password: Encryption password.

SNMP Port: Port of SNMP.

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.

Configuring HTTPS Settings

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 27 HTTPS Settings

Note: *Honeywell strictly recommends using HTTPS only.*

TLS (Transport Layer Security) : In the TLS (Transport Layer Security) section, the options for TLS 1.2 and TLS 1.3 are checked by default. Users can set the TLS according to their own security requirement.

Note: *HC60WZ8R40WI / HC60WZ8R40KI cameras support “TLS 1.2 & TLS 1.3” to enhance “data transportation security”.*

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.

Certificate Request

Go to **Setup > Network Setup > HTTPS > CERTIFICATE REQUEST**. You can create the certificate request here.

Figure 28 Certificate Request

The screenshot shows a web interface with three tabs at the top: "HTTPS", "CERTIFICATE REQUEST" (which is selected and highlighted), and "UPLOAD FILES". Below the tabs, there are several input fields for certificate information:

- Country**: An empty text input field.
- State or province**: An empty text input field.
- Locality**: An empty text input field.
- Organization**: An empty text input field.
- Organization unit**: An empty text input field.
- Common name**: A text input field containing the value "159.99.251.222".

Upload Files

Go to **Setup > Network Setup > HTTPS > UPLOAD FILES**. You can import the certificate from third party here.

The screenshot shows the "UPLOAD FILES" tab selected in the web interface. It contains two sections for file uploads:

- Certificate**: A section with a "CHOOSE FILE" button and the text "No file chosen".
- Key**: A section with a "CHOOSE FILE" button and the text "No file chosen".

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**.

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

Configuring IEEE 802.1x Settings

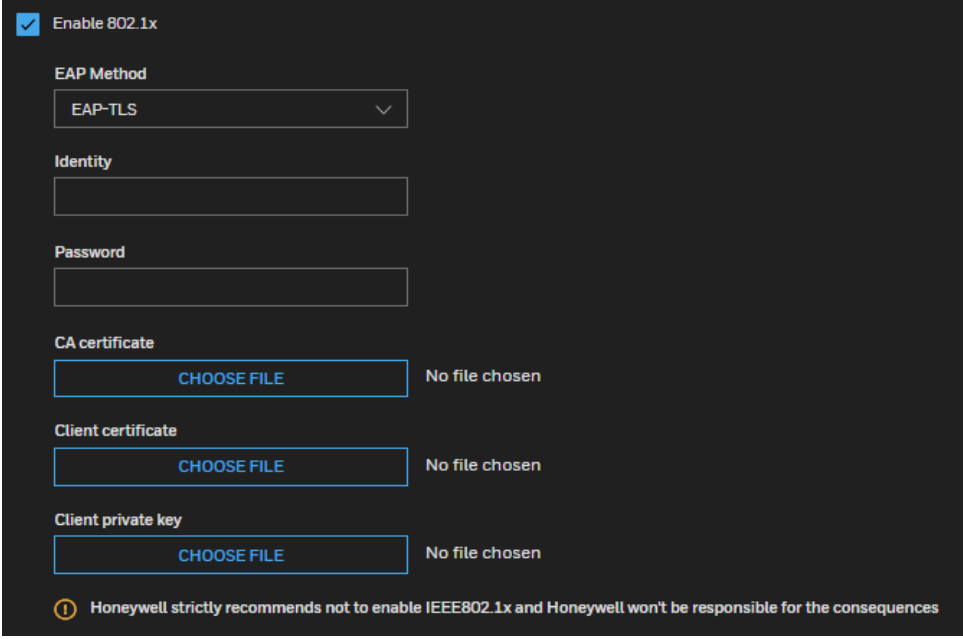
Go to **Setup > Network Setup > 802.1x**.

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 29 IEEE 802.1x Configurations – EAP-TLS



The screenshot shows the IEEE 802.1x configuration interface. At the top, there is a checkbox labeled "Enable 802.1x" which is checked. Below this, the "EAP Method" is set to "EAP-TLS" in a dropdown menu. There are three text input fields for "Identity", "Password", and "CA certificate". Below the "CA certificate" field, there is a "CHOOSE FILE" button and the text "No file chosen". Similarly, there are "CHOOSE FILE" buttons and "No file chosen" text for the "Client certificate" and "Client private key" fields. At the bottom, there is a warning icon and text: "Honeywell strictly recommends not to enable IEEE802.1x and Honeywell won't be responsible for the consequences".

Note: *Honeywell doesn't recommend enabling IEEE 802.1x.*

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

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

Configuring FTP Settings

Go to **Setup > Network Setup > FTP (File Transfer Protocol)**.

File Transfer Protocol (FTP) is a way to upload the snapshot file. Check to enable FTP upload and input the parameters of FTP which you have account in advanced.

Figure 30 File Transfer Protocol (FTP)

The screenshot shows the 'Network Setup' interface with the 'FTP' tab selected. The 'FTP' section is titled 'FTP' and contains the following settings:

- Enable FTP upload:** A checkbox that is checked.
- Mode:** A dropdown menu set to 'SFTP'.
- SFTP Address:** An empty text input field.
- SFTP Port:** A text input field containing the value '22'.
- Account:** An empty text input field.
- Password:** An empty text input field.
- SFTP Path:** An empty text input field.
- Media type:** A dropdown menu set to 'Snapshot'.
- TEST:** A button at the bottom of the form.

Enable FTP upload: Check to enable the FTP service

Mode: SFTP, FTPS, FTP

FTP (SFTP/ FTPS) Address: IP address of FTP (SFTP/ FTPS) server

FTP (SFTP/ FTPS) Port: Port of FTP server

Account: FTP server account

Password: FTP server password

FTP (SFTP/ FTPS) Path: FTP Path to save the image

Media Type: The media type of sending to FTP, snapshot or video clip

After inputting all parameters, click **TEST** to test the value. If the pop-up window shows “Test succeeded”, it means the parameters are correct. If the pop-up window shows “Test failed”, the parameters should be modified.

Click **SAVE** to save the settings.

Note: *SFTP feature is not applicable for all models camera, please refer to actual product.*

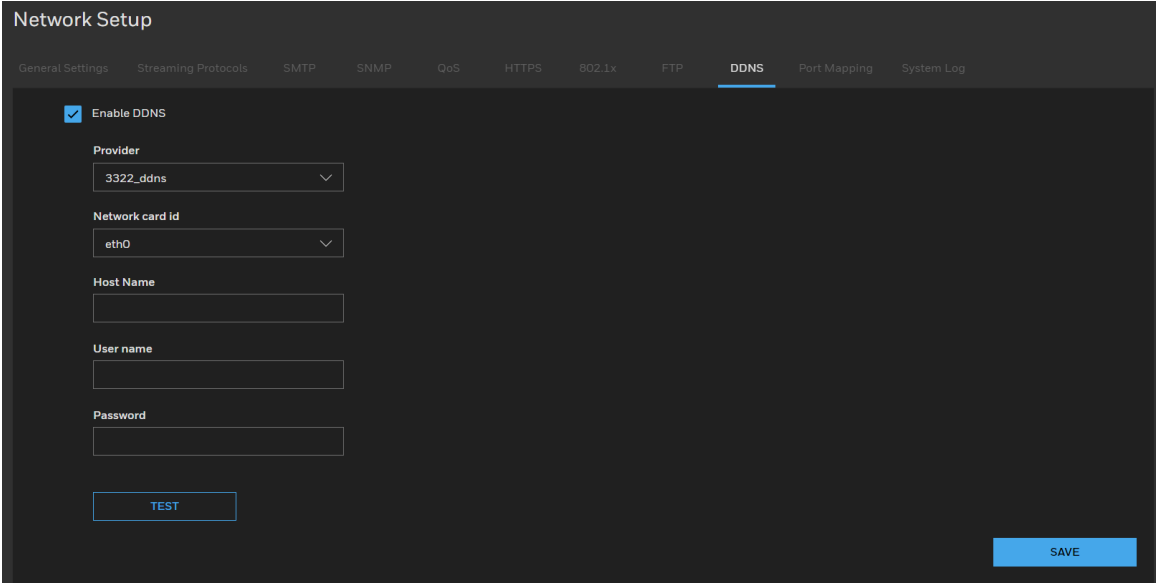
Configuring DDNS

DDNS (Dynamic Domain Name Server): User can use the DDNS account to access the NVR.

1. Go to Setup > Network Setup > DDNS.

The DDNS interface is displayed.

Figure 31 DDNS Interface



The screenshot shows the 'Network Setup' configuration page with the 'DDNS' tab selected. The 'Enable DDNS' checkbox is checked. Below it, there are several fields: 'Provider' (a dropdown menu showing '3322_ddns'), 'Network card id' (a dropdown menu showing 'eth0'), 'Host Name' (a text input field), 'User name' (a text input field), and 'Password' (a text input field). At the bottom left is a 'TEST' button, and at the bottom right is a 'SAVE' button. The top navigation bar includes links for General Settings, Streaming Protocols, SMTP, SNMP, QoS, HTTPS, 802.1x, FTP, DDNS, Port Mapping, and System Log.

2. Check Enable DDNS, choose the protocol from drop-down list, no_ip / autodns / dyndns / 3322.
3. Enter the domain name.
4. Enter the DDNS account user name and password.

5. Click APPLY to complete the settings.

Configuring Port Mapping

You can map the relationship between the LAN and the WAN to access the Device on the LAN through the IP address on the WAN.

1. Go to Setup > Network Setup > Port Mapping.

The Port Mapping interface is displayed.

Figure 32 Port Mapping Interface

Network Setup

< General Settings Streaming Protocols SMTP SNMP QoS HTTPS 802.1x FTP DDNS Port Mapping System Log Network Discovery Ph >

☒ Port Mapping

Map mode

Auto

Auto port mapping

Enable	PORTTYPE	OUTSIDEPORT	OUTSIDEIP ADDRESS	Status
☒	HTTP	80	0.0.0.0	INEFFECTIVE
☒	RTSP	554	0.0.0.0	INEFFECTIVE
☒	HTTPS	443	0.0.0.0	INEFFECTIVE

SAVE

2. Enable the function to start set the parameters.
3. You can choose auto or manual mode to set.
4. Configure the settings for the manual port parameters.

Table 4 Port Mapping Parameters

Parameter	Description
HTTP Port	The default value setting is 80. You can enter the value according to your actual situation. If you enter other value, for example, 70, and then you should enter 70 after the IP address when logging in the Device by browser.
RTSP Port	RTSP (Real-Time Streaming Protocol), the port of RTSP to access the device. The default value setting is 554.
HTTPS Port	HTTPS communication port. The default value setting is 443. You can enter the value according to your actual situation.

Note: The manual port range should be 1025-66534.

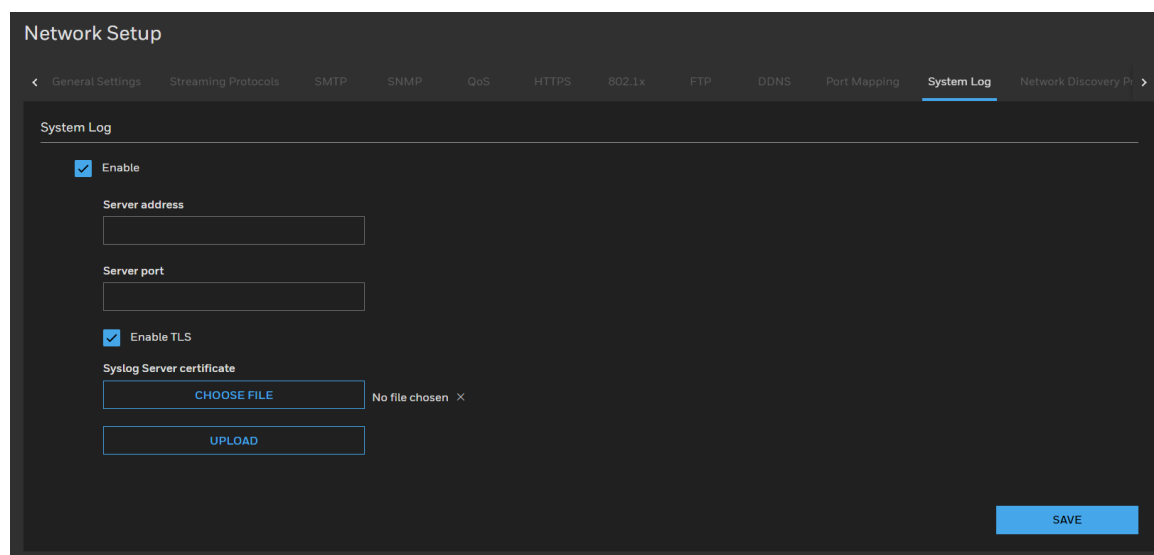
5. Click SAVE to complete the settings.
- In the browser, enter http:// IP: HTTP port. You can visit the LAN Device.

Configuring System Log

Set the parameters of 3rd-party system log server, so that the server can receive the system logs from camera and view the logs.

1. Go to Setup > Network Setup > System Log. The System Log interface is displayed.

Figure 33 System Log Interface



The screenshot shows the 'System Log' configuration page within the 'Network Setup' menu. The page has a dark theme. At the top, there's a navigation bar with tabs: General Settings, Streaming Protocols, SMTP, SNMP, QoS, HTTPS, 802.1x, FTP, DDNS, Port Mapping, System Log (selected), and Network Discovery. Below the navigation bar, the 'System Log' section is active. It contains a checkbox labeled 'Enable' which is checked. Below this are two input fields: 'Server address' and 'Server port'. Further down, there's another checkbox labeled 'Enable TLS' which is also checked. Below this is a section for 'Syslog Server certificate' with a 'CHOOSE FILE' button and a text indicator 'No file chosen'. At the bottom of this section is an 'UPLOAD' button. A large 'SAVE' button is located at the bottom right of the page.

2. Configuring the System log, user should install the software of Certificate Generation Tool. Here we take Syslog Watcher Manager and Win64OpenSSL for example.
 - a. Enable TLS is ticked, users should generate certificate file in advanced. Upload the certificate.
 - b. Install Syslog Watcher Manager and open Win64OpenSSL window.
 - c. Go to System Setup > Maintenance > IMPORT / EXPORT FILES > CA certificate to export CA certificate(cacert.crt).
 - d. Create a blank fingerprint file locally for storing the generated fingerprint information with any name, take fingerprints.txt for example.
 - e. In the Win64OpenSSL terminal interface, execute the commands to generate the relevant certificate and private key.

Execute the command to generate the root certificate and private key, where rootCA.key is the root certificate private key; rootCA.crt is the root certificate.

The detail commands are:

```
openssl genpkey -algorithm RSA -out rootCA.key -pkeyopt rsa_keygen_bits:4096
```

```
openssl req -new -key rootCA.key -out rootCA.csr -subj "/C=CN/ST= State Or Province /L= Locality /O= Organization /CN=RootCA"
```

```
openssl x509 -req -days 3650 -in rootCA.csr -signkey rootCA.key -out rootCA.crt
```

```
C:\Users\Administrator\syslog_demo>
C:\Users\Administrator\syslog_demo>openssl genkey -algorithm RSA -out rootCA.key -pkeyopt rsa_keygen_bits:4096
.....
C:\Users\Administrator\syslog_demo>openssl req -new -key rootCA.key -out rootCA.csr -subj "/C=CN/ST=StateOrProvince/L=Locality/O=Organization/CN=RootCA"
Certificate request self-signature ok
subject=C = CN, ST = StateOrProvince, L = Locality, O = Organization, CN = RootCA
```

Execute the command to generate the sub-certificate and private key, where server.key is the private key 1of the sub-certificate server.crt is the sub-certificate, and IP is the local address.

The detail commands are:

```
openssl genpkey -algorithm RSA -out server.key -pkeyopt rsa_keygen_bits:2048
```

```
openssl req -new -key server.key -out server.csr -subj "/C=CN/ST= State Or Province/L= Locality/O= Organization/CN=DeviceIP"
```

```
openssl x509 -req -days 365 -in server.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial -out server.crt
```

```
C:\Users\Administrator\demo>openssl genpkey -algorithm RSA -out server.key -pkeyopt rsa_keygen_bits:2048
.....
C:\Users\Administrator\demo>openssl req -new -key server.key -out server.csr -subj "/C=CN/ST= StateOrProvince/L= Locality/O= Organization/CN=DeviceIP"
Certificate request self-signature ok
subject=C = CN, ST = " StateOrProvince", L = " Locality", O = " Organization", CN = DeviceIP
C:\Users\Administrator\demo>
```

- f. certificate fingerprint acquisition Assume that cacert.crt is the certificate from the device.

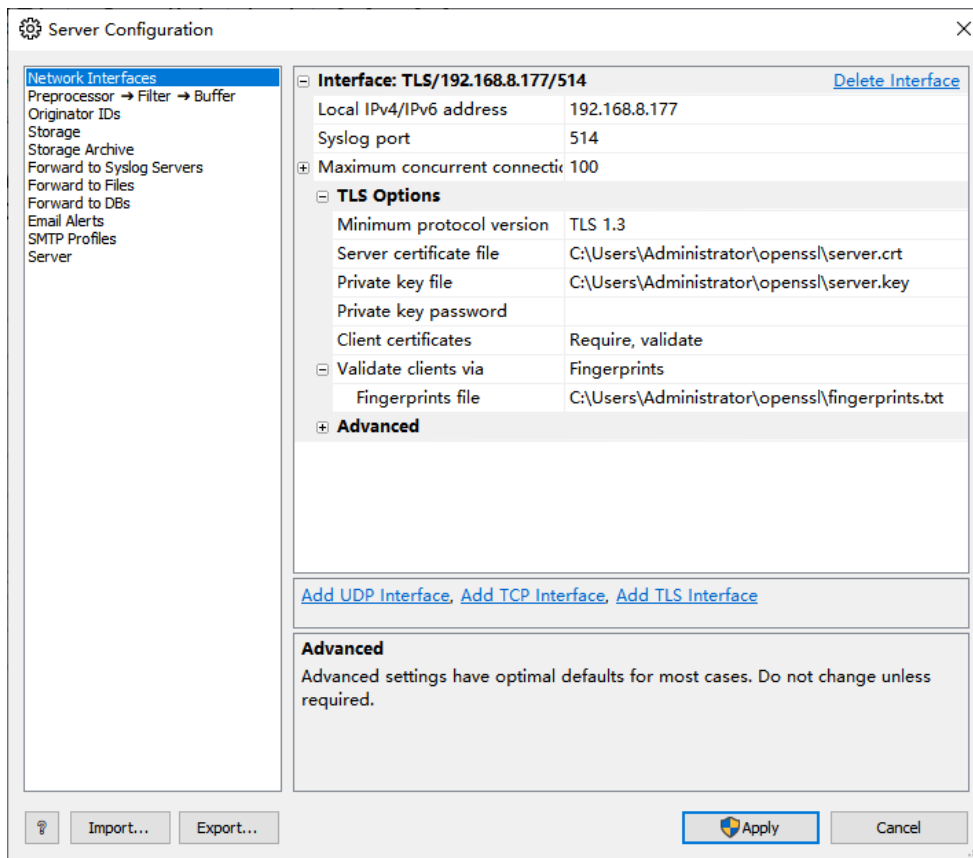
The detail command is:

```
openssl x509 -in cacert.crt -fingerprint -sha1 > fingerprints.txt
```

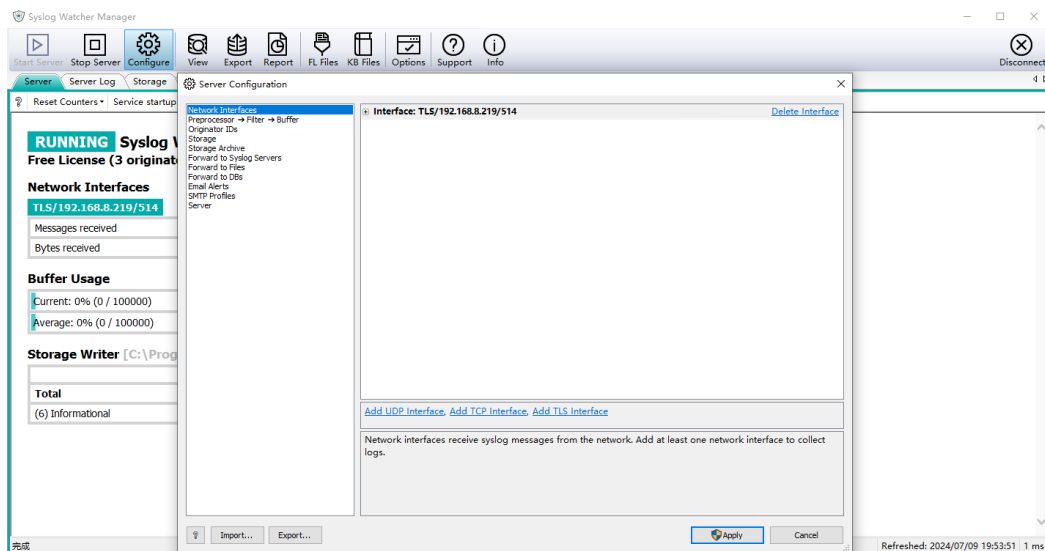
```
C:\Users\Administrator\demo>openssl x509 -in cacert.crt -fingerprint -sha1 > fingerprints.txt
```

- g. Modify the fingerprints format of the certificate fingerprints.txt.

3. Install Syslog Watcher Manager and open it.



4. Choose Add TLS Interface. Import the certificates and server.key which is generated at above.



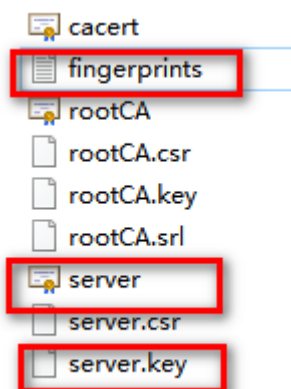
Network Interfaces

- Preprocessor → Filter → Buffer
- Originator IDs
- Storage
- Storage Archive
- Forward to Syslog Servers
- Forward to Files
- Forward to DBs
- Email Alerts
- SMTP Profiles
- Server

Interface: TLS/192.168.8.219/514 [Delete Interface](#)

Local IPv4/IPv6 address	192.168.8.219
Syslog port	514
Maximum concurrent connections	100
Drop old connections	No
TLS Options	
Minimum protocol version	TLS 1.3
Server certificate file	C:\Users\Administrator\Desktop\syslog\server.crt
Private key file	C:\Users\Administrator\Desktop\syslog\server.key
Client certificates	Require, validate
Validate clients via	Fingerprints
Fingerprints file	C:\Users\Administrator\Desktop\syslog\fingerprints.txt
Advanced	
Maximum message length	10000
Socket buffer size	1048576
'Octet counting' detection	Yes
Use CR/LF symbols to split streams	Yes
Inactive clients timeout (s)	0

Interface: TLS/0.0.0.0/514 [Delete Interface](#)



5. Set the web of camera.

System Log

☒ Enable

Server address
192.168.8.17 ← The IP of computer installing Certificate Generation Tool

Server port
514 ← Listening port

☒ Enable TLS

Syslog Server certificate

[CHOOSE FILE](#) No file chosen × Importing generated certificates server.crt

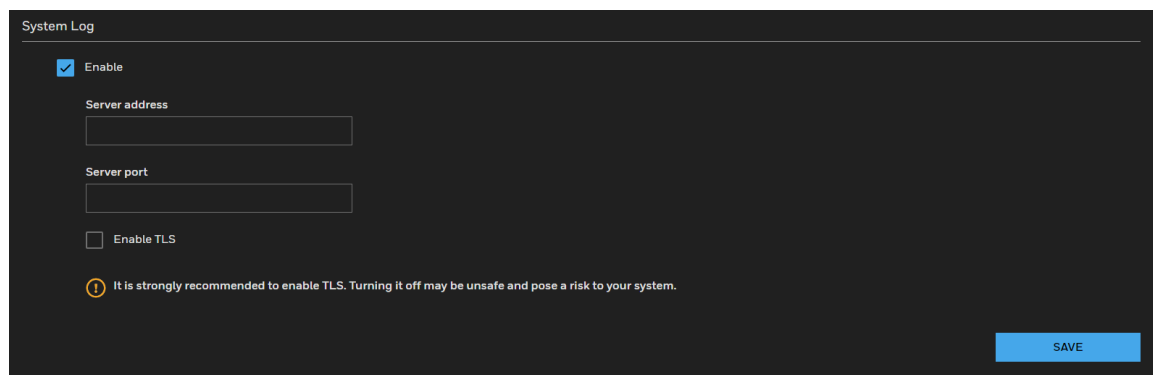
[UPLOAD](#)

6. Test the settings, the system logs are sent to Syslog Watcher Manager, it is set

succeeded. Otherwise it is failure, you should check steps.

If the TLS is disabled, there may be cyber security risk." You only need to input the **Server address** and **Server port**. Server IP the IP of computer which is installed **Syslog Watcher Manager**, the server port is the syslog port, the default is 514.

Note: It is strongly recommended to enable TLS. Turning it off may be unsafe and pose a risk to your system.



System Log

☒ Enable

Server address

Server port

☐ Enable TLS

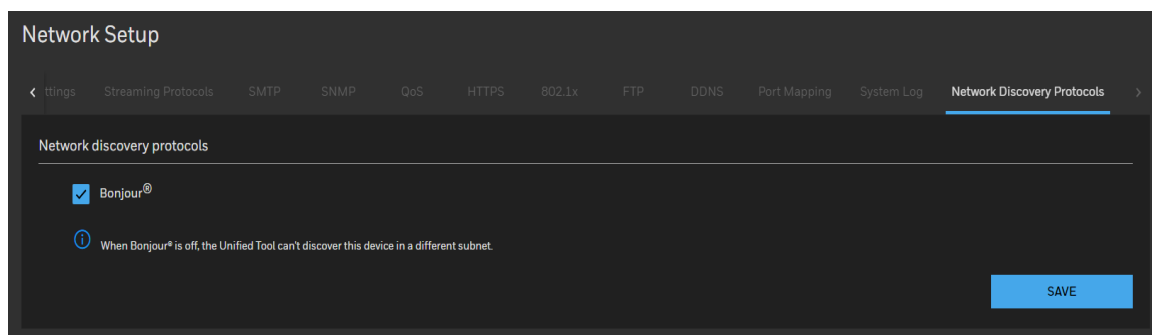
ⓘ It is strongly recommended to enable TLS. Turning it off may be unsafe and pose a risk to your system.

SAVE

Configuring Network Discovery Protocols

The Bonjour is default enabled, the Unified Tool can search all cameras at same and different subnets. When it is disabled, the Unified Tool only search the cameras at the same subnet of computer.

Figure 34 Network Discovery Protocols



Network Setup

Settings Streaming Protocols SMTP SNMP QoS HTTPS 802.1x FTP DDNS Port Mapping System Log **Network Discovery Protocols**

Network discovery protocols

☒ Bonjour®

ⓘ When Bonjour® is off, the Unified Tool can't discover this device in a different subnet.

SAVE

CONFIGURING VIDEO ANALYTICS

Video Analytics provides the following features: motion detection, smart motion, scene change, intrusion, multi loitering, people counting, face detection, line crossing detection, unattended detection, and missing object detection.

Video Analytics detects one or a group of the following objects:

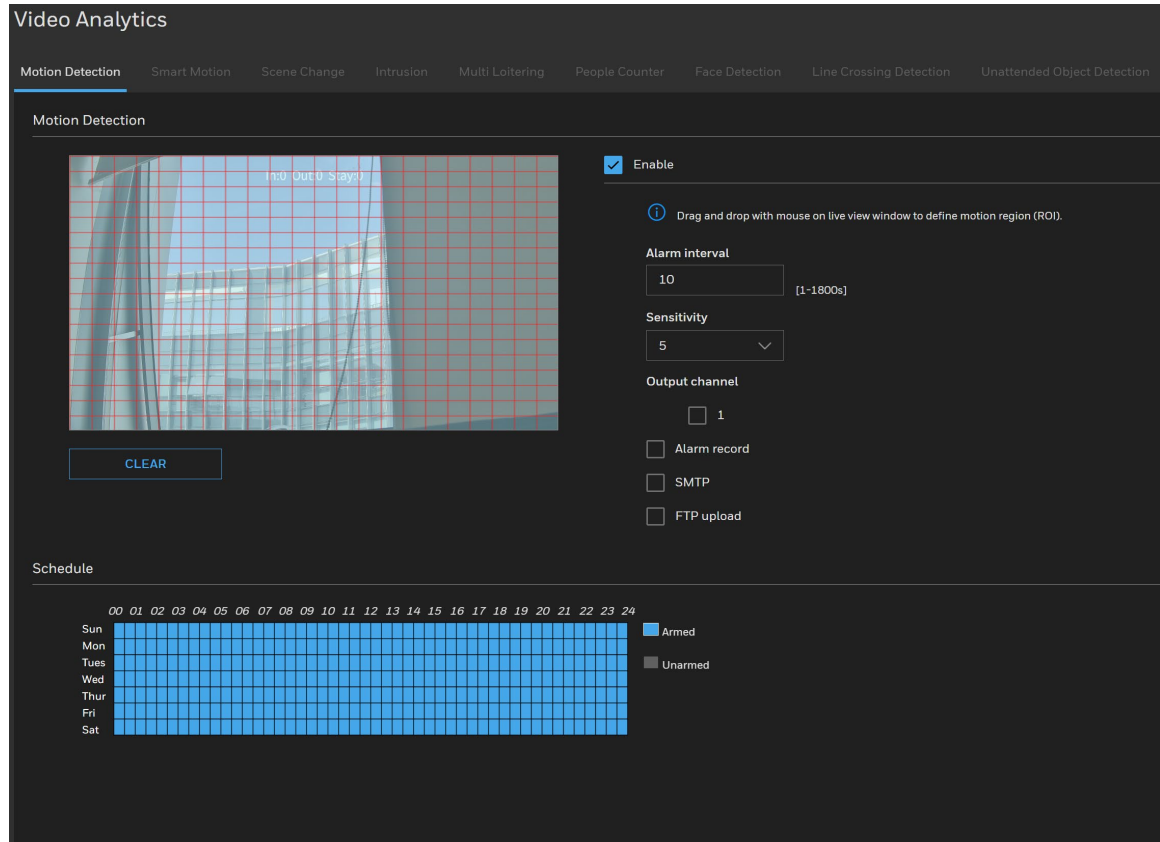
- Vehicle
- Human

Note: *On the Video Analytics page, click Open VA User Guide to open the detailed guide for Video Analytics features.*

Motion Detection

1. Go to Setup > Video Analytics > Motion Detection.

Figure 35 Motion Detection



2. Check the Enable checkbox to enable motion detection.
3. **Mode:** For High-speed cameras, users can choose mode to set, **Normal Mode** and **Preset point mode**.
Normal mode: the detection area is default set for entire area of current view. User can adjust the detection area by dragging the curse.
Preset point mode: choose one preset, which is set in advance, the lens jumps to the preset point, the detection area is set at the preset point.
4. Configure the Alarm interval and Sensitivity.
For Sensitivity, the higher the value is set, the easier the motion will be detected. But it may trigger some false alarms.
For example, 10 is the highest sensitivity value and the motion will be the easiest to be detected. But it will probably trigger some false alarms.
1 is the lowest sensitivity value and the motion will be the hardest to be detected. But it will rarely trigger false alarms.
5. Configure the detection area.
 - a) Press and hold the left mouse button, and drag in the video area to draw a detection area
 - b) Click CLEAR to delete a detection area

6. Check the linkage actions, Output channel, Alarm record, SMTP, FTP upload, and Audible alarm.

Output channel: Check the checkbox to enable **Output channel**.

Alarm record: Check the checkbox to enable the linkage action for sending alarm record to SD card so that the user can check alarm through recording video.

SMTP: Check the checkbox to enable the linkage action for sending snapshot and alarm notice information to email address which can be set in **Network Setup > SMTP**, so the user can receive the alarm timely.

FTP upload: It will send 8 alarm pictures to FTP server when alarm happened if you selected the FTP upload box.

Audible alarm: It will play the audio file to alarm when alarm happened if you selected the Audio alarm box.

7. Click SAVE.

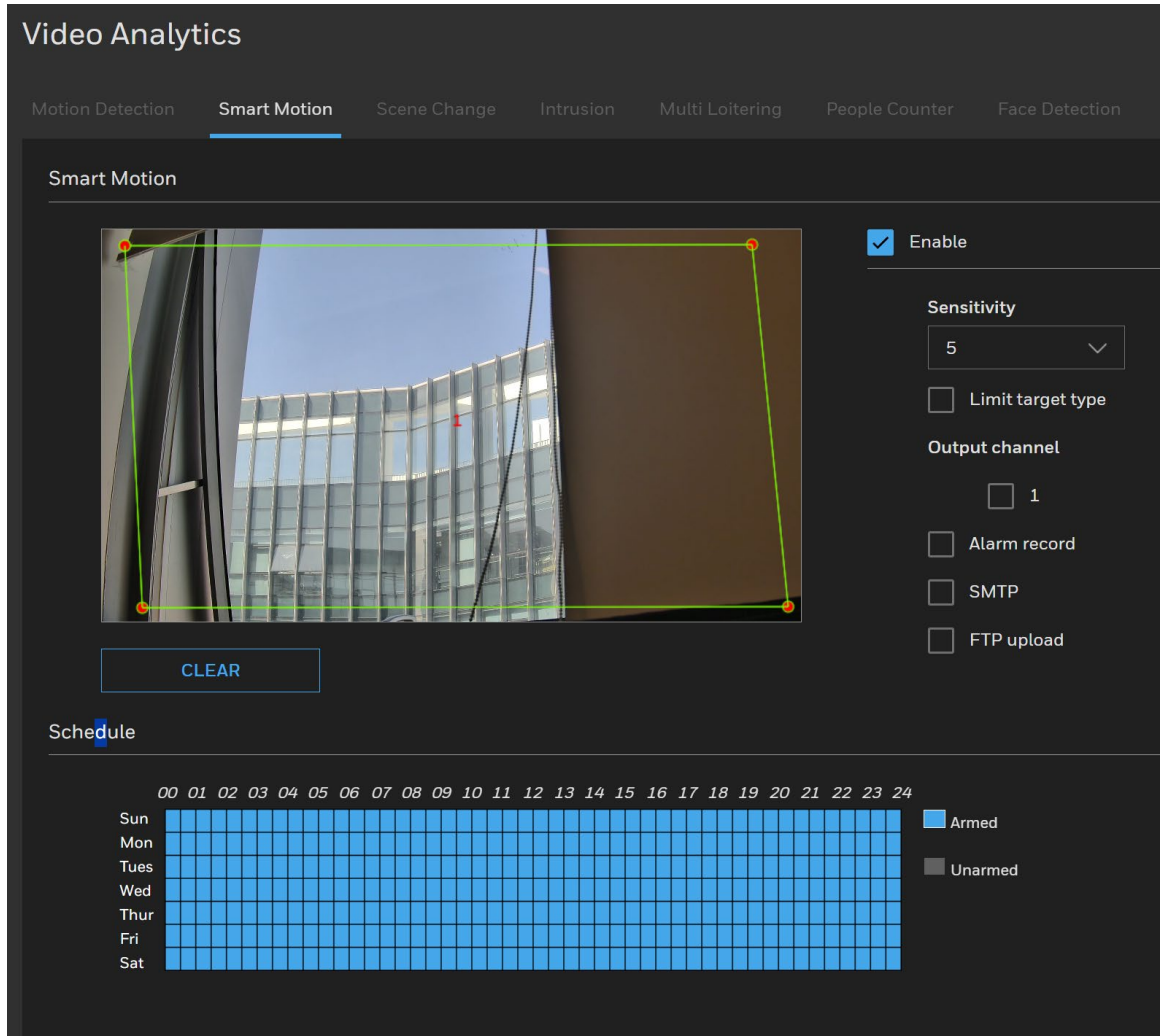
Smart Motion

After configuring an area for defense, it will generate the alarm information when someone or something intrudes in the area.

Smart Motion detection can identify 1~5 detection objects (human and cars) in the setting area. The applicable scenario to detect objects (humans or cars by selecting **Limit target type**) is in a restricted area.

1. Go to Setup > Video Analytics > Smart Motion.

Figure 36 Smart Motion



2. Check the Enable checkbox to enable smart motion detection.
3. **Mode:** For High-speed cameras, users can choose mode to set, **Normal Mode** and **Preset point mode**.
Normal mode: the detection area is set at the current scene.
Preset point mode: choose one preset, which is set in advance, the lens jumps to the preset point, the detection area is set at the preset point.
4. Configure the Sensitivity.
For Sensitivity, the higher the value is set, the easier the smart motion will be detected. But it may trigger some false alarms.
For example, 5 is the highest sensitivity value and the smart motion will be the easiest to be detected. But it will probably trigger some false alarms.
1 is the lowest sensitivity value and the smart motion will be the hardest to be detected. But it will rarely trigger false alarms.
5. Configure the detection area.

- Press and hold the left mouse button, and drag in the video area to draw a detection area
- Click CLEAR to delete a detection area.

Note: Users can set up to 6 zones for smart motion detection.

6. Select the Output channel.
7. Check the check boxes to enable Alarm record, Audible alarm and SMTP.
The detail information please refer to [Motion Detection](#) page 53
8. Click SAVE.

Scene Change

Go to **Setup > Video Analytics > Scene Change**. Set the parameters of **Scene Change**.

Figure 37 Scene Change

The screenshot shows the 'Video Analytics' configuration page with the 'Scene Change' tab selected. The interface includes a navigation bar at the top with tabs for Motion Detection, Smart Motion, Scene Change, Intrusion, Multi Loitering, People Counter, Face Detection, Line Crossing Detection, and Unattended Object Detection. The 'Scene Change' tab is active. Below the navigation bar, the 'Scene Change' configuration section is displayed. It includes a checkbox for 'Enable scene change', a 'Sensitivity' dropdown menu set to '5', an 'Output channel' section with a checkbox for '1', and three checkboxes for 'Alarm record', 'SMTP', and 'FTP upload'. A 'Schedule' dropdown menu is also present. A 'SAVE' button is located at the bottom right of the configuration area.

Enable scene change: Check the checkbox to enable the scene change.

Mode: For High-speed cameras, users can choose mode to set, **Normal Mode** and **Preset point mode**.

Normal mode: the detection area is set at the current scene.

Preset point mode: choose one preset, which is set in advance, the lens jumps to the preset point, the detection area is set at the preset point.

Sensitivity: Choose the value from the drop-down list to set the sensitivity of detecting the target.

For **Sensitivity**, the higher the value is set, the easier the scene change will be detected. But it may trigger some false alarms.

For example, 5 is the highest sensitivity value and the scene change will be the easiest to be detected. But it will probably trigger some false alarms.

1 is the lowest sensitivity value and the scene change will be the hardest to be detected. But it will rarely trigger false alarms.

Output channel: If the alarm out cable is connected to the external device such as alarm light or speaker, when scene change is triggered, the output channel will send alarm to remind user.

Alarm record: Check the checkbox to enable the linkage action for sending alarm record to SD card so that the user can check alarm through recording video.

SMTP: Check the checkbox to enable the linkage action for sending snapshot and alarm notice information to email address which can be set in **Network Setup > SMTP**, so the user can receive the alarm timely.

FTP upload: It will send 8 alarm pictures to FTP server when alarm happened if you selected the FTP upload box.

Audible alarm: It will play the audio file to alarm when alarm happened if you selected the Audio alarm box.

Note: *The scene change triggers audio playing, and the audio alarm will play just one time. It will not play repeatedly as Camera Setup > Audio > Audio File > CYCLE NUMBER.*

Schedule: Use the mouse to drag the time or click the time grid to choose time one hour by hour. The blue means armed and the gray means unarmed.

Click **SAVE**.

Intrusion Detection

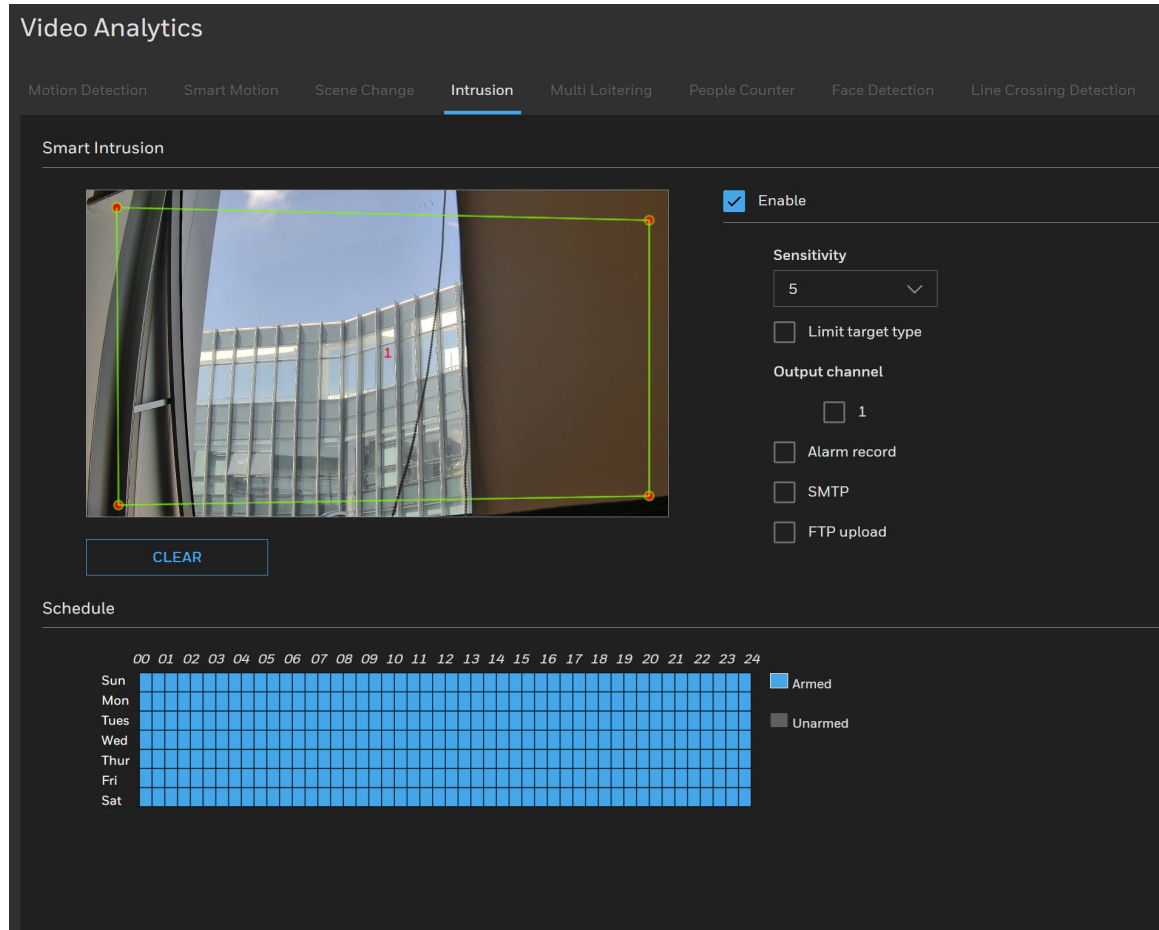
Intrusion can be used to detect 1~5 objects entering or moving in a restricted area in the camera field of view.

The applicable scenarios of this feature can be:

- Detects when a human or vehicle enters or moves in a bank or at a school after the office hours.
- Detects when a human or vehicle moves at any place that is normally forbidden to access.

1. Go to Setup > Video Analytics > Intrusion.

Figure 38 Intrusion Detection



2. Check the Enable checkbox to enable intrusion detection.
3. **Mode:** For High-speed cameras, users can choose mode to set, **Normal Mode** and **Preset point mode**.

Normal mode: the detection area is set at the current scene.

Preset point mode: choose one preset, which is set in advance, the lens jumps to the preset point, the detection area is set at the preset point.

4. Configure the Sensitivity.

For Sensitivity, the higher the value is set, the easier the intrusion will be detected. But it may trigger some false alarms.

For example, 5 is the highest sensitivity value and the intrusion will be the easiest to be detected. But it will probably trigger some false alarms.

1 is the lowest sensitivity value and the intrusion will be the hardest to be detected. But it will rarely trigger false alarms.

5. Configure the detection area.

- Press and hold the left mouse button, and drag in the video area to draw a detection area

- Click CLEAR to delete a detection area.

Note: *Users can set up one area for intrusion detection.*

6. Select the Output channel.
7. Check the check boxes to enable Alarm record, Audible Alarm and SMTP.
The detail information please refer to [Motion Detection](#) page 53.
8. Click SAVE.

Multi Loitering

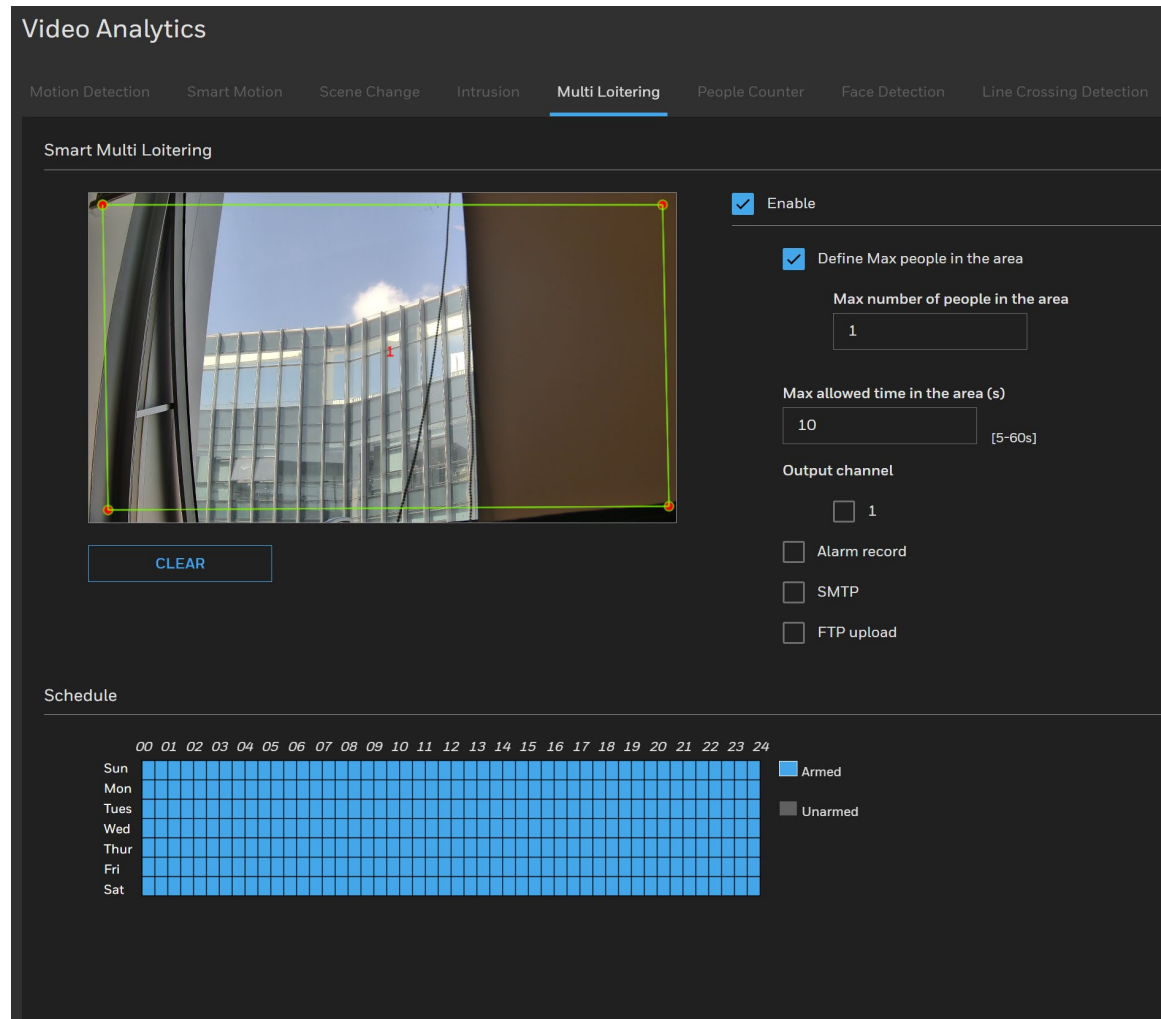
The Loitering detection can be used for a detection object or a group of detection objects lingering in an area for longer than a preset time threshold.

The applicable scenarios of this feature can be:

- Detects when a person is loitering at a walk-up of ATM lane.
- Detects when a person is loitering in a high-theft area of a store, or to prevent vandalism and break-ins.
- Detects when a person is loitering in an area that is normally not an access for visitors.

1. Go to Setup > Video Analytics > Multi Loitering.

Figure 39 Multi Loitering



2. Check the Enable checkbox to enable multi loitering detection.
3. **Mode:** For High-speed cameras, users can choose mode to set, **Normal Mode** and **Preset point mode**.

Normal mode: the detection area is set at the current scene.

Preset point mode: choose one preset, which is set in advance, the lens jumps to the preset point, the detection area is set at the preset point.

4. Check the checkbox of Define Max people in the area.
5. Configure Max number of people in the area.
6. Configure Max allowed time in the area (s).
7. Configure the detection area.
 - Press and hold the left mouse button, and drag in the video area to draw a detection area
 - Click CLEAR to delete a detection area.
8. Select the Output channel.

9. Check the check boxes to enable Alarm record, Audible Alarm and SMTP.
The detail information please refer to [Motion Detection](#) page 53
10. Click SAVE.

People Counter

People counter is used to count the persons in the field of view. It is often used to collect the number of people entering and leaving a certain area, so as to implement statistical requirements for the number of people in the area, and trigger alarms by setting thresholds.

The applicable scenarios of this feature can be:

- There are few people to pass through the view, and the movement trajectories are obvious.
- People must cross the line.

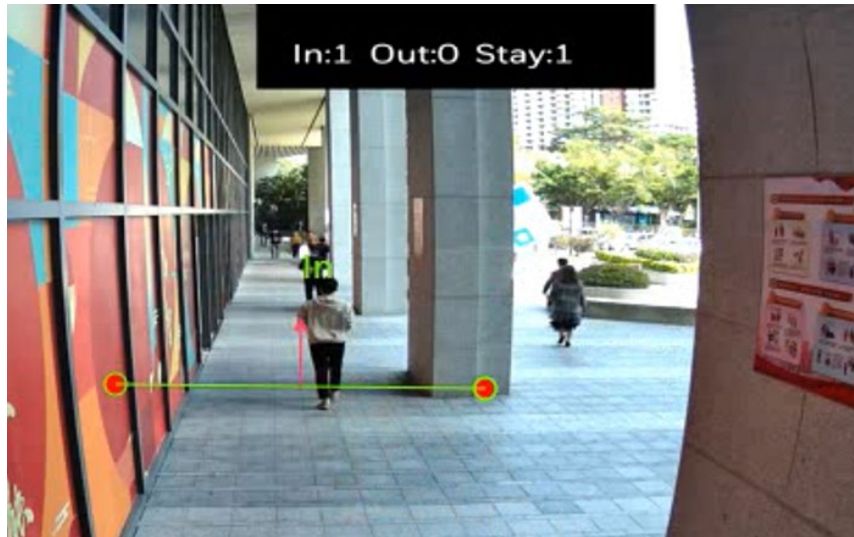
The inappropriate scene of this feature can be:

- The direction of passenger flow is complex and staggered, which seriously affects the effect.
- The horizontal distance is too far, and the target is small, which will lead to missed detection.
- The height of installation is too low, or the head is too large (people should have movement track, not too large for screen).
- Public places such as stations are crowded with people.
- At the entrance of the shopping mall, people are next to the place where people come in and out.

The below views of scenarios are suitable for the people counter:

- The camera is facing the direction of the flow of people, as shown in [Figure 40](#).

Figure 40 View of Facing the Flow of People



- The camera is facing the side way direction of the flow of people, as shown in [Figure 41](#).

Figure 41 Facing the Side Way Flow of People



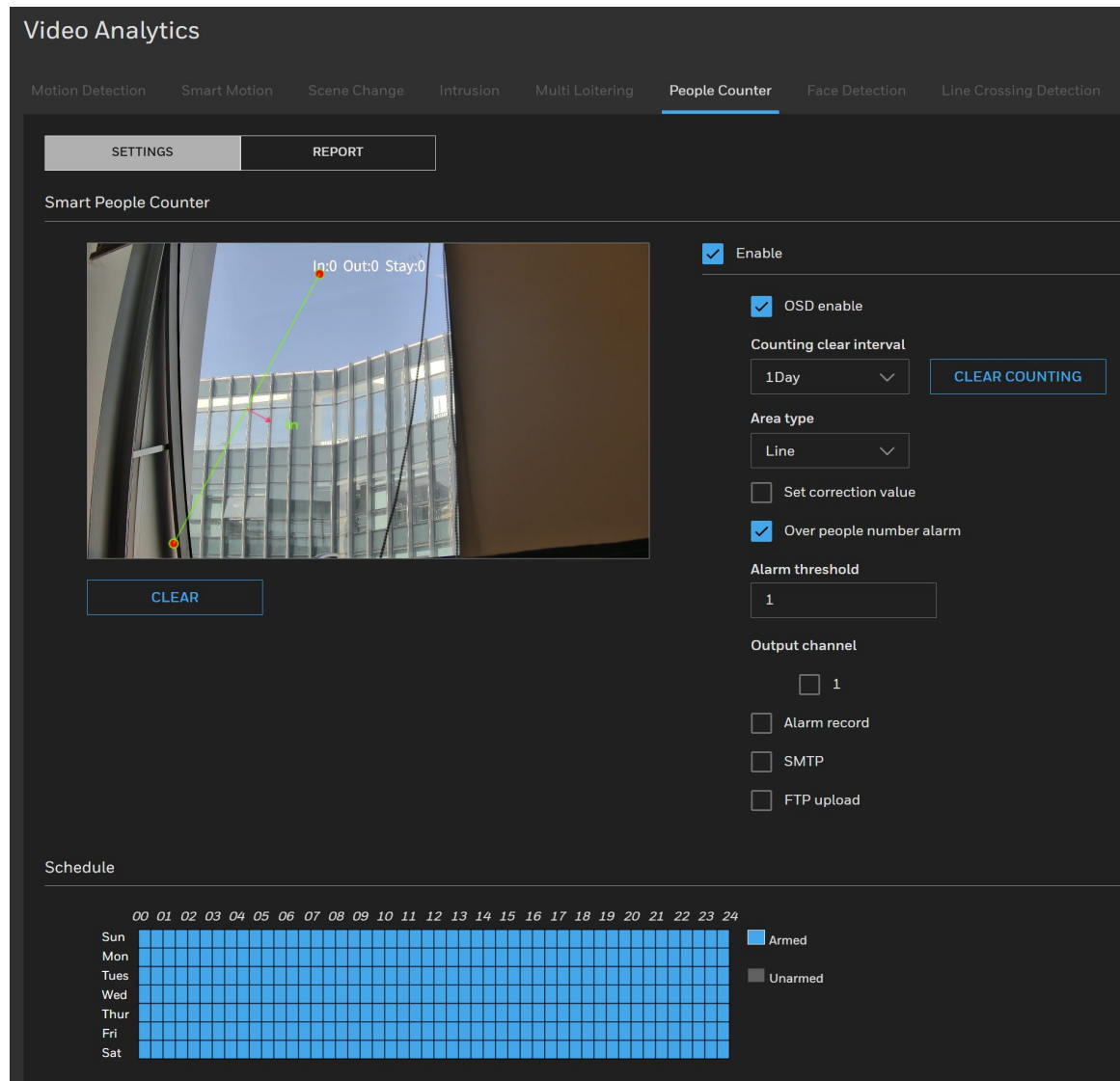
It is recommended to use the people counter function in situations below:

- The movement direction of the flow of people is relatively uniform, and there is no wandering.
- There is no interleaving and no overlapping between the flowing of people, otherwise it will affect the accuracy.
- The movement speed is not too fast, and the movement track time in the detection area is not too short.
- There are no obstructions in the visual field, try to choose a single background such as the ground and wall

- Avoid complex scenes with frequent changes in light, backlight, and direct light.
- The height and angle need to be adjusted according to the actual scene effect. The installation height is 3m~3.5m and the installation angle is 25°~45° for verification.
- The line area needs to be in the middle of the screen, and there is at least 2s for the target movement track.

Go to **Setup > Video Analytics > People Counter**. Set the parameters of People Counter.

Figure 42 People Counter



Enable: Check the checkbox to enable the people counter.

Mode: For High-speed cameras, users can choose mode to set, **Normal Mode** and **Preset point mode**.

Normal mode: the detection area is set at the current scene.

Preset point mode: choose one preset, which is set in advance, the lens jumps to the preset point, the detection area is set at the preset point.

OSD enable : Check the OSD enable checkbox to enable OSD display of people counter. The data of out and in will be showing on the live video screen.

Note: *The OSD display is only supported in Mainstream.*

Counting clear Interval: Select interval time to configure the **Counting clear interval**, the camera will clear counting numbers within every setting time interval. Click **CLEAR COUNTING** to clear current counting number.

Area Type: Draw a line on the live video screen, following the arrow direction is **In** area, reversing the arrow direction is **Out** area.

Figure 43 Line of People Counter

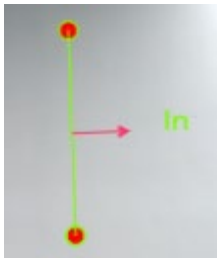
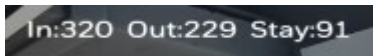


Figure 44 Number for In / Out / Stay



the **In** means people cross line into the area. Go out from the **In** area means **Out**. **Stay** means the number of **In** minus the number of **Out**.

Note: *When a correction value is set, the number for Stay will be the number of In minus the number of Out and plus the correction value.*

Set correction value: Check the enable checkbox of **Set correction value** to enable counting correction which already stay on the **In** area. Input people number which is already stay in the **In** area. If there are two people passing the line going in to the area before enabling people counter function, user can input 2 as the correction value.

Over people number alarm: Check the enable checkbox of **Over people number alarm** to enable alarm function when stay people number over the number setting in **Alarm threshold** box.

Output Channel: If the alarm out cable is connected to the external device such as alarm light or speaker, when over people number alarm is triggered, the output channel will send alarm to remind user.

Alarm record: Check the checkbox to enable the linkage action for sending alarm record to SD card so that the user can check alarm through recording video.

SMTP: Check the checkbox to enable the linkage action for sending snapshot and alarm notice information to email address which can be set in **Network Setup > SMTP**, so the user can receive the alarm timely.

Audible alarm: It will play the audio file to alarm when alarm happened if you selected the Audio alarm box.

CLEAR: Clear the line of setting. Use the mouse left-click and hold, end the draw to release the left mouse button. It is set on the corridor, or doorway.

Schedule: Use the mouse to drag the time, or click the time grid to choose time one hour by hour. The blue means armed and the gray means unarmed.

Face Detection

Face Detection is used to detect the persons appearing in the field of concern area. It is often used for warning owner that there are targets displayed and crossing the concern area.

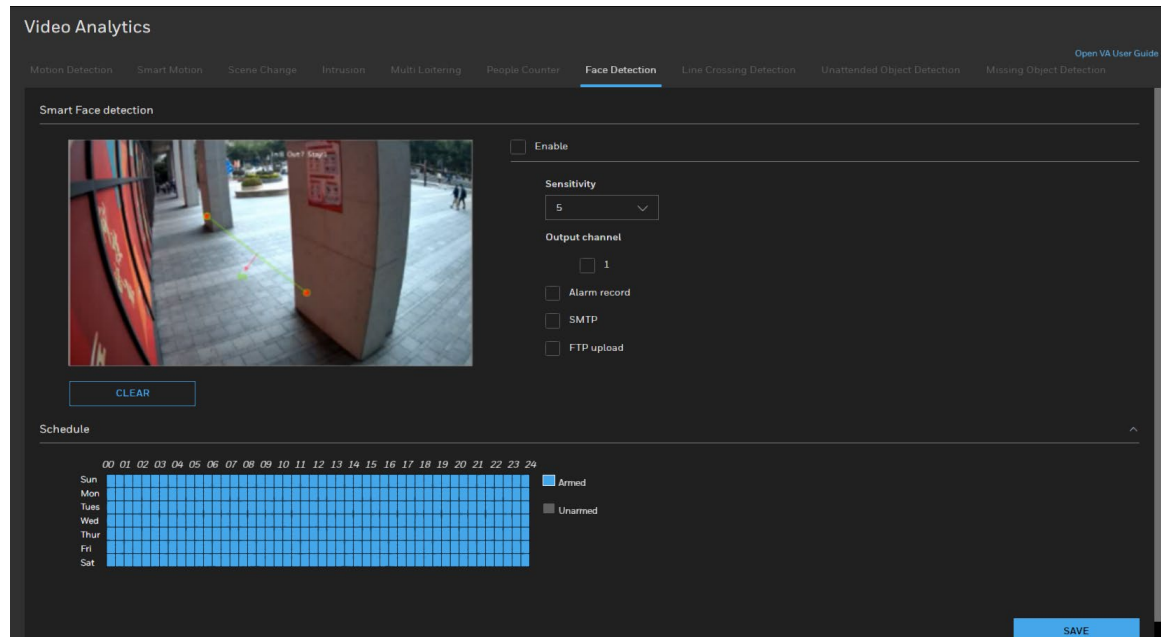
The applicable scenarios of this feature can be:

- There are few people to crossing the concern area, there are warning for owner.

The inappropriate scene of this feature can be:

- The direction of passenger flow is complex and staggered, which seriously affects the effect.
- The horizontal distance is too far, and the target is small, which will lead to missed detection.
- The height of installation is too low, or the head is too large (people should have movement track, not too large for screen).
- Public places such as stations are crowded with people
- At the entrance of the shopping mall, people are next to the place where people come in and out.

Figure 45 Face Detection



Go to **Setup > Video Analytics > Face Detection**. Set the parameters of face detection.

Enable: Check the checkbox to enable the face detection.

For **Sensitivity**, the higher the value is set, the easier the target will be detected. But it may trigger some false alarms.

For example, 5 is the highest sensitivity value and the target will be the easiest to be detected. But it will probably trigger some false alarms.

1 is the lowest sensitivity value and the target will be the hardest to be detected. But it will rarely trigger false alarms.

Mode: For High-speed cameras, users can choose mode to set, **Normal Mode** and **Preset point mode**.

Normal mode: the detection area is set at the current scene.

Preset point mode: choose one preset, which is set in advance, the lens jumps to the preset point, the detection area is set at the preset point.

Output Channel: If the alarm out cable is connected to the external device such as alarm light or speaker, when over people number alarm is triggered, the output channel will send alarm to remind user.

Alarm record: Check the checkbox to enable the linkage action for sending alarm record to SD card so that the user can check alarm through recording video.

SMTP: Check the checkbox to enable the linkage action for sending snapshot and alarm notice information to email address which can be set in **Network Setup > SMTP**, so the user can receive the alarm timely.

FTP upload: It will send 8 alarm pictures to FTP server when alarm happened if you selected the FTP upload box.

Audible alarm: It will play the audio file to alarm when alarm happened if you selected the Audio alarm box.

CLEAR: Clear the line of setting. Use the mouse left-click and hold, end the draw to release the left mouse button. It is set on the corridor, or doorway.

Schedule: Use the mouse to drag the time, or click the time grid to choose time one hour by hour. The blue means armed and the gray means unarmed.

Line Crossing Detection

Line Crossing Detection is used to set lines at a concerned position within the monitored field of view and specifies the forbidden travel direction. An alarm is generated when the targets of specified types (such as humans / vehicles) cross this line.

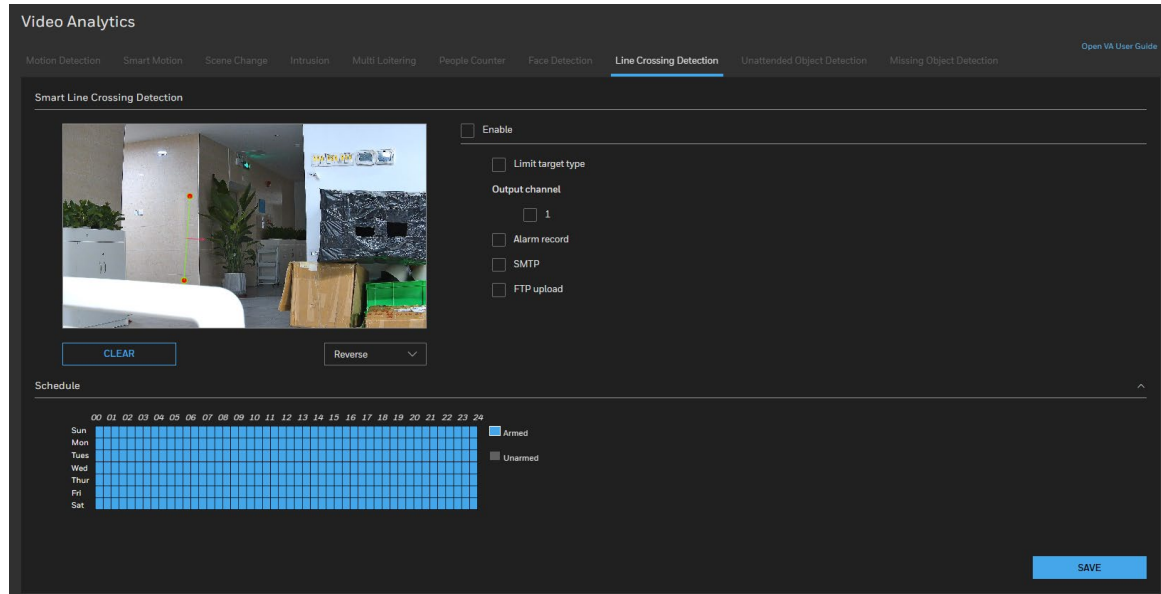
The applicable scenarios of this feature can be:

- There are specifies scene that forbidden humans / vehicles crossing the detection line.

The inappropriate scene of this feature can be:

- The direction of passenger flow is complex and staggered, which seriously affects the effect.
- The horizontal distance is too far, and the target is small, which will lead to missed detection.
- The height of installation is too low, or the head is too large (people should have movement track, not too large for screen).
- Public places such as stations are crowded with people.
- At the entrance of the shopping mall, people are next to the place where people come in and out.
- When the camera is perpendicular to the ground.

Figure 46 Line Crossing Detection



Go to **Setup > Video Analytics > Single Line Crossing**. Set the parameters of single line crossing.

Enable: Check the checkbox to enable the single line crossing.

Mode: For High-speed cameras, users can choose mode to set, **Normal Mode** and **Preset point mode**.

Normal mode: the detection area is set at the current scene.

Preset point mode: choose one preset, which is set in advance, the lens jumps to the preset point, the detection area is set at the preset point.

Limit target type: Check the checkbox to enable Limit target type and choose the type from the pull-down list: Human or vehicle / Human / Vehicle. The smart detection only used for chosen type.

Output Channel: If the alarm out cable is connected to the external device such as alarm light or speaker, when over people number alarm is triggered, the output channel will send alarm to remind user.

Alarm record: Check the checkbox to enable the linkage action for sending alarm record to SD card so that the user can check alarm through recording video.

SMTP: Check the checkbox to enable the linkage action for sending snapshot and alarm notice information to email address which can be set in **Network Setup > SMTP**, so the user can receive the alarm timely.

FTP upload: It will send 8 alarm pictures to FTP server when alarm happened if you selected the FTP upload box.

Audible alarm: It will play the audio file to alarm when alarm happened if you selected the Audio alarm box.

Draw detection lines on live video. And choose type of line, such as **Bidirectional**, **Reverse**, or **Positive**.

CLEAR: Clear the line of setting. Use the mouse left-click and hold, end the draw to release the left mouse button. It is set on the corridor, or doorway.

Schedule: Use the mouse to drag the time, or click the time grid to choose time one hour by hour. The blue means armed and the gray means unarmed.

Unattended Object Detection

The **Unattended Object Detection** function refers to that an alarm is generated when the dwelling time of an object within the deployment area meets the set shortest dwelling time.

The applicable scenarios of this feature can be:

- Object Detection is used to detecting there are some objects appeared on concern area and not displayed in view before, such as bags, chairs and so on.

The inappropriate scene of this feature can be:

- The direction of passenger flow is complex and staggered, which seriously affects the effect.
- The horizontal distance is too far, and the target is small, which will lead to missed detection.
- The height of installation is too low, or the head is too large (people should have movement track, not too large for screen).
- Public places such as stations are crowded with people
- At the entrance of the shopping mall, people are next to the place where people come in and out.

Figure 47 Unattended Object Detection

The screenshot shows the 'Unattended Object Detection' configuration page within a 'Video Analytics' menu. The page has a dark theme. At the top, there's a navigation bar with various analytics options: Motion Detection, Smart Motion, Scene Change, Intrusion, Multi-Clustering, People Counter, Face Detection, Line Crossing Detection, **Unattended Object Detection** (highlighted), and Missing Object Detection. An 'Open VA User Guide' link is on the far right. The main content area is titled 'Unattended Object Detection'. It features a video preview window on the left showing a scene with green bounding boxes around objects. Below the preview is a 'CLEAR' button. To the right of the preview are configuration options: an 'Enable' checkbox, a 'The Shortest Dwelling Time (s)' input field set to '5' with a range '[5-60s]', an 'Output channel' section with a radio button for '1' and checkboxes for 'Alarm record', 'SMTP', and 'FTP upload'. At the bottom is a 'Schedule' section with a 7x24 grid for days of the week (Sun-Sat) and hours (00-24). A legend indicates blue for 'Armed' and grey for 'Unarmed'. A 'SAVE' button is at the bottom right.

Go to **Setup > Video Analytics > Unattended Object Detection**. Set the parameters of object detection.

Enable: Check the checkbox to enable the object detection function.

Mode: For High-speed cameras, users can choose mode to set, **Normal Mode** and **Preset point mode**.

Normal mode: the detection area is set at the current scene.

Preset point mode: choose one preset, which is set in advance, the lens jumps to the preset point, the detection area is set at the preset point.

Shortest Dwelling Time: The number must from 5 to 60 with unit for second.

Output Channel: If the alarm out cable is connected to the external device such as alarm light or speaker, when over people number alarm is triggered, the output channel will send alarm to remind user.

Alarm record: Check the checkbox to enable the linkage action for sending alarm record to SD card so that the user can check alarm through recording video.

SMTP: Check the checkbox to enable the linkage action for sending snapshot and alarm notice information to email address which can be set in **Network Setup > SMTP**, so the user can receive the alarm timely.

FTP upload: It will send 8 alarm pictures to FTP server when alarm happened if you selected the FTP upload box.

Audible alarm: It will play the audio file to alarm when alarm happened if you selected the Audio alarm box.

Draw detection area on live video. Left-click on the live view to start drawing the area and right-click to end setting the smart detection areas.

- Note:**
- *This VA function is only applicable for HC60WZXR40WI/ HC60WZXR40KI.*
 - *There is no detection area ID/channels numbers shows in live-view alarm information.*

CLEAR: Clear the line of setting. Use the mouse left-click and hold, end the draw to release the left mouse button. It is set on the corridor, or doorway.

Schedule: Use the mouse to drag the time, or click the time grid to choose time one hour by hour. The blue means armed and the gray means unarmed.

Missing Object Detection

The **Missing Object Detection** function refers to that an alarm is generated when the removing time of an object within the deployment area meets the set shortest removing time.

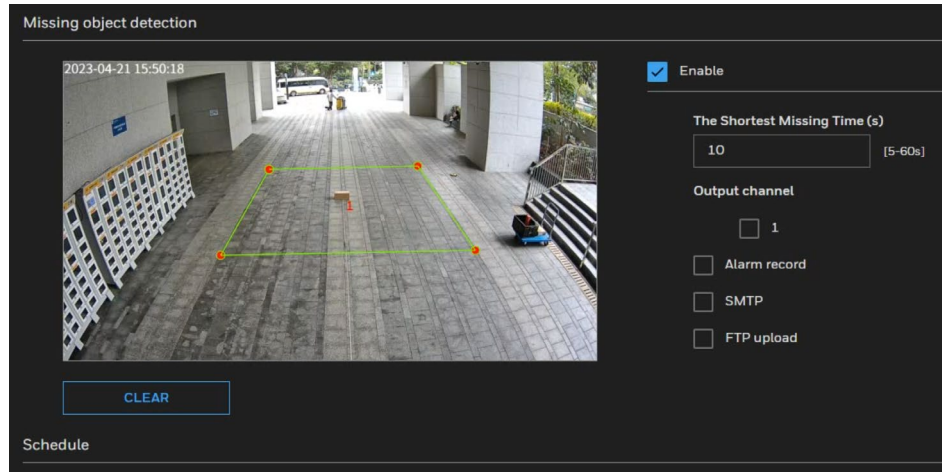
The applicable scenarios of this feature can be:

- It is used to detecting there are some objects disappeared on concern area.

The inappropriate scene of this feature can be:

- The direction of passenger flow is complex and staggered, which seriously affects the effect.
- The horizontal distance is too far, and the target is small, which will lead to missed detection.
- The height of installation is too low, or the head is too large (people should have movement track, not too large for screen).
- Public places such as stations are crowded with people
- At the entrance of the shopping mall, people are next to the place where people come in and out

Figure 48 Missing Object Detection



Go to **Setup > Video Analytics > Missing Object Detection**. Set the parameters of object removed.

Enable: Check the checkbox to enable the object removed function.

Mode: For High-speed cameras, users can choose mode to set, **Normal Mode** and **Preset point mode**.

Normal mode: the detection area is set at the current scene.

Preset point mode: choose one preset, which is set in advance, the lens jumps to the preset point, the detection area is set at the preset point.

Shortest Dwelling Time: The number must from 5 to 60 with unit for second.

Output Channel: If the alarm out cable is connected to the external device such as alarm light or speaker, when over people number alarm is triggered, the output channel will send alarm to remind user.

Alarm record: Check the checkbox to enable the linkage action for sending alarm record to SD card so that the user can check alarm through recording video.

SMTP: Check the checkbox to enable the linkage action for sending snapshot and alarm notice information to email address which can be set in **Network Setup > SMTP**, so the user can receive the alarm timely.

FTP upload: It will send 8 alarm pictures to FTP server when alarm happened if you selected the FTP upload box.

Audible alarm: It will play the audio file to alarm when alarm happened if you selected the Audio alarm box.

Draw detection area on live video. Left-click on the live view to start drawing the area and right-click to end setting the smart detection areas.

- Note:**
- *This VA function is only applicable for HC60WZXR40WI/ HC60WZXR40KI.*
 - *There is no detection area ID/channels numbers shows in live-view alarm information.*

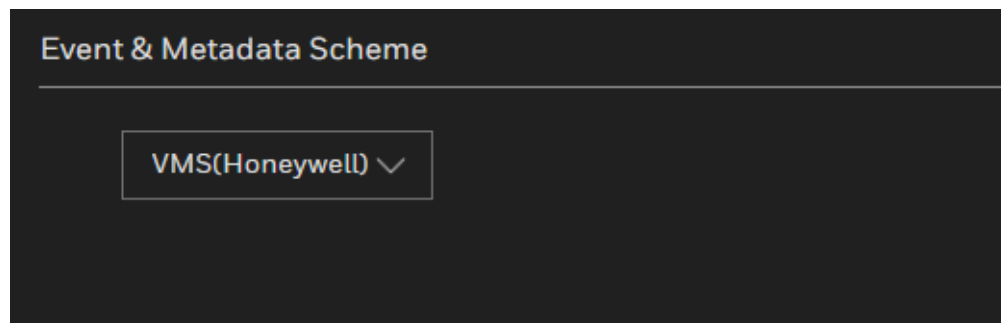
CLEAR: Clear the line of setting. Use the mouse left-click and hold, end the draw to release the left mouse button. It is set on the corridor, or doorway.

Schedule: Use the mouse to drag the time, or click the time grid to choose time one hour by hour. The blue means armed and the gray means unarmed.

Event & Metadata Scheme

The Event & Metadata Scheme function support different VA data transmission. You must choose a correct method link to third platform such as MaxPro or genetic. The third platform will not receive VA information if choose incorrect connection.

Figure 49 Event & Metadata Scheme



Go to **Setup > Video Analytics > Event & Metadata Scheme**.

VMS(Honeywell): The ONVIF message topic format based on Honeywell definition, applicable for Honeywell VMS, such as Maxpro.

VMS(3rd-party): The ONVIF message topic format based universal ONVIF definition, applicable for 3rd-party VMS, such as Genetec.

- Note:**
- *Motion Detection/Smart Motion/Scene Change not limited by this feature.*
 - *When the stream of camera is switched to http&https or https only, the signal will be interrupted for 3min, then it will be recovered automatically.*

7

CONFIGURE ALARM AND EVENT

This section describes the alarm and event settings.

Configuring Alarm In and Alarm Out

Alarm Input

Go to Setup > Alarm & Event > Alarm In and Alarm Out.

Figure 50 Alarm Input

The image shows a configuration interface for two alarm inputs, labeled 'Alarm Input1' and 'Alarm Input2'. Each input has a set of configuration options:

- Alarm input:** A checkbox to enable the alarm input.
- Name:** A text input field for naming the alarm.
- Current mode:** A dropdown menu currently set to 'Low'.
- Output channel:** Two checkboxes, '1' and '2', to select the output channel.
- Alarm record:** A checkbox to enable alarm recording.
- SMTP:** A checkbox to enable SMTP notifications.
- PTZ linkage:** A checkbox to enable PTZ linkage.
- Schedule:** A grid for configuring the alarm schedule. The grid has 24 columns representing hours (00 to 24) and 7 rows representing days of the week (Sun to Sat). A legend indicates that blue squares represent 'Armed' status and grey squares represent 'Unarmed' status.

In the screenshot, the 'Alarm input' checkbox is checked for both inputs. The 'Name' field is empty. The 'Current mode' is set to 'Low'. The 'Output channel' checkboxes '1' and '2' are unchecked. The 'Alarm record', 'SMTP', and 'PTZ linkage' checkboxes are unchecked. The 'Schedule' grid shows all cells as blue, indicating the alarm is armed for all days and times.

Alarm input: Check the checkbox of Alarm input.

Name: Enter the alarm input name.

Current mode: Select the current mode from the drop-down list box.

Schedule: Configure the schedule by using one of the methods below.

- Click left mouse button to select any time point within 0:00-24:00 from Monday to Sunday.
- Hold down the left mouse button, drag and release mouse to select the schedule within 0:00-24:00 from Monday to Sunday.

Output channel: Select the Output channel.

Alarm record/SMTP/FTP upload: Check the check boxes to enable Alarm record, SMTP and FTP upload.

PTZ linkage: Check the check boxes to enable **PTZ linkage**.

After the event is triggered, the system will run or stop the movement of the corresponding type according to the settings.

- **PTZ type:** Select **Preset/Scan/Patrol/Recording Patrol**.
- **Value:** Select the value.
- **Operate:** Select **Invoke/Pause/Continue** when PTZ type is **Patrol**.
 - **Invoke:** Call related PTZ linkage for running **Patrol**.
 - **Pause:** Pause related PTZ linkage **Patrol**.
 - **Continue:** Continue related PTZ linkage running **Patrol**.

Note: *PTZ linkage function is only applicable for PTZ models HC60WZ4R40WI / HC60WZ4R40KI / HC60WZ8R40WI / HC60WZ8R40KI.*

Alarm Output

Go to Setup > Alarm & Event > Alarm In and Alarm Out.

Figure 51 Alarm Output

The screenshot displays the 'Alarm Output' configuration page. It features two identical sections for 'Alarm Output1' and 'Alarm Output2'. Each section includes a text input for 'Name', a dropdown menu for 'Current signal' (currently set to 'Grounded'), and two buttons labeled 'OPEN' and 'CLOSE' under the 'Manual control' heading. At the bottom of the page, there is a checkbox labeled 'Timing alarm output' which is currently unchecked.

Name: Alarm output name

Current Signal: Select **Grounded** or **Open** to define normal status for the alarm output. Connect the output cable to an external device, the camera will report the current signal output status according to alarm event setting.

- **Grounded:** Camera alarm relay is **Normal Open**. It will turn to **Grounded/Closed** when an alarm event is generated to trigger it.
- **Open:** Camera alarm relay is **Normal Closed (Grounded)**. It will turn to **Open** state when an alarm event is generated to trigger it.

Note: *The signal status will take effect after one alarm out is triggered.*

Manual control: If alarm out signal is coming, click **Close** to disable alarm out or click **Open** to keep alarm out status.

If alarm out signal is not coming, it is opposite with above.

Timing alarm output: Enable **Timing alarm output** and set time for alarm out. The device will continue trigger alarm out during the selecting time slot.

Note: *For 2M/4M models (HC60W34R2I/ HC60W32R2I /HC60W44R2I / HC60W42R2I / HC60WB4R2I/HC60WB2R2I/HC60WB4R5I/HC60WC5I), two alarm inputs and an alarm output can be configured.
For PTZ model HC60WZ4R40WI/HC60WZ4R40KI, alarm input1~7, and alarm output1/output2 can be configured.*

Configuring SD Card Alarm

Go to Setup > Alarm & Event > SD Card Alarm.

SD card alarm: Check the checkbox to enable **SD card alarm**.

Alarm threshold(used space): The camera will alarm when used space achieves the alarm threshold.

Alarm interval: Set the interval.

Output channel: Check the checkbox to set the Output channel.

SMTP/FTP upload: Check the check boxes to enable SMTP and FTP upload.

Note: *For the event recording clips edge sync, current firmware version can only support no more than 1000 recording clips in the SD card within 1 month ahead the current searching timestamp.*

Configuring Audio Detection

Go to Setup > Alarm & Event > Audio Detection.

When the camera detects a sudden rise or fall in audio, it will send alarm messages.

Figure 52 Audio Detection

Alarm & Event

Alarm In And Alarm Out SD Card Alarm **Audio Detection**

Audio Detection

☐ Enable

☐ Sudden rise

Rise sensitivity
5 [1 - 100]

Rise threshold
70 [1 - 100]

☐ Sudden drop

Drop sensitivity
5 [1 - 100]

Drop threshold
70 [1 - 100]

Output channel
☐ 1

☐ Alarm record ☐ SMTP ☐ FTP upload

Real Time Volume

Schedule

Sun Mon Tues Wed Thur Fri Sat

00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

Armed
Unarmed

SAVE

Enable: Check the checkbox to enable the audio detection.

Sudden rise/ Sudden drop: Check the checkbox of sudden rise/drop. Set the rise/drop sensitivity (1-100) and rise/drop threshold (1-100).

For Sensitivity, the higher the value is set, the easier the sudden rise will be detected. But it may trigger some false alarms.

For example, 100 is the highest sensitivity value and the sudden rise/drop will be the easiest to detect. But it will probably trigger some false alarms.

1 is the lowest sensitivity value and the sudden rise/drop will be the hardest to detect. But it will rarely trigger false alarms.

Rise / Drop Threshold: The volume of detecting sound. Its range is 1-100 dB.

Output channel: Select the Output channel.

Alarm record/SMTP/FTP upload: Check the check boxes to enable Alarm record, SMTP and FTP upload.

Real Time Volume: Show the volume of camera receiving at real time.

Schedule: Configure the schedule by using one of the methods below.

- Click left mouse button to select any time point within 0:00-24:00 from Monday to Sunday.
- Hold down the left mouse button, drag and release mouse to select the schedule within 0:00-24:00 from Monday to Sunday.

CONFIGURE STORAGE SETTINGS

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 5 Compatible SD Card

SD Card Brand	Model	Size
SanDisk	microSDHC A1 C10	16 GB
Kingston	microSDHC V10	16 GB
SanDisk	microSDHC V30	32 GB
SanDisk	microSDXC V30	64 GB
SanDisk	microSDXC V30	128 GB
Toshiba	microSDXC M303 V30	128 GB
Micron	microSDXC A2 C10	128 GB
Samsung	microSDXC C10	256 GB
Kingston	microSDXC V30	256 GB
SanDisk	microSDXC C10	256 GB
SanDisk	microSDXC UHS-I	1TB

- 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 82.*

SD Card Status

This tab shows the status and reserved space of your SD card. 60 Series camera supports only one SD card.
Remember to format the SD card when using it for the first time, see [SD Card Format](#) on page 82.

Figure 53 No SD Card

SD Card Status			
SD Card Status :	N/A	Total size :	0 MBytes
Free size :	0 MBytes	Used size :	0 MBytes
Alarm threshold(%) :	100%		

Figure 54 SD Card Onboard

SD Card Status			
SD Card Status :	Usable	Total size :	7360 MBytes
Free size :	2880 MBytes	Used size :	4480 MBytes
Alarm threshold(%) :	50%	File system :	Ext4

SD Card Format	
SD card(s):	SD Card 1

SD Card Format

To format the SD Card, select the SD card and click FORMAT.
Insert/detach SD Card
The following instructions apply while inserting and detaching the SD card from the camera.



Caution: Do not detach the SD card while the formatting is going on.



Warning: Check if any recording such as continuous recording is running and disable the event or recording rule before detaching the SD card. The SD card has unformatted status after reinserting into the camera if the recording was on while you removed it from the camera.

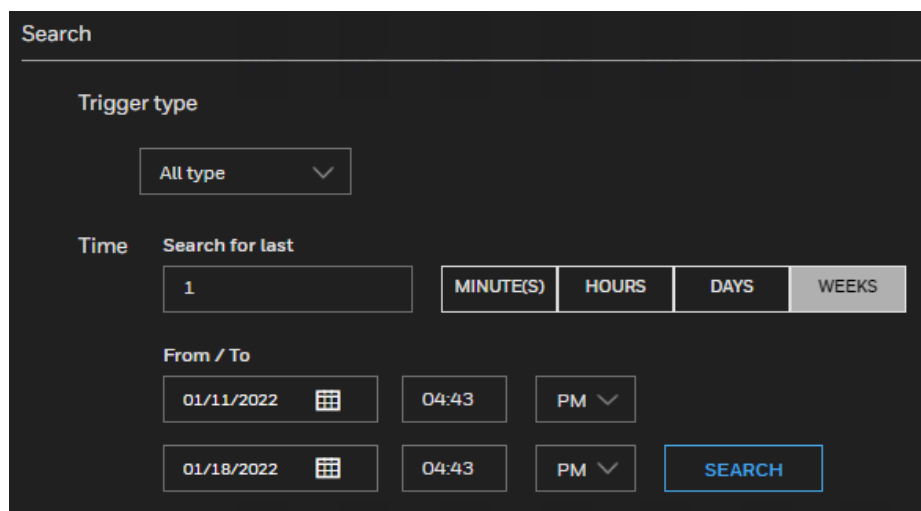
Content Management

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.



The screenshot shows a 'Search' tab with the following fields and controls:

- Trigger type:** A dropdown menu currently set to 'All type'.
- Time:** A section titled 'Search for last' containing a text input field with the value '1' and four buttons: 'MINUTE(S)', 'HOURS', 'DAYS', and 'WEEKS'.
- From / To:** Two rows of date and time selection fields. The first row shows '01/11/2022' and '04:43 PM'. The second row shows '01/18/2022' and '04:43 PM'. Each date field has a calendar icon, and each time field has a dropdown arrow.
- SEARCH:** A blue button located at the bottom right of the form.

- **Trigger type:** Select one or more triggers from Backup, System boot, Alarm input, Motion, Network failure, Recording notification, Periodically, Tampering detection, and VADP.
- **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

To sort the search results, click each column header.

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.

Storage Setup

SD Card Management **Content Management** Recording Settings

Search

Trigger type
All type

Time Search for last
1 MINUTES HOURS DAYS WEEKS

From / To
02/01/2022 11:21 AM
03/31/2022 11:21 PM **SEARCH**

Search Results

	Device	Trigger type	Starting time	Ending time
☐	SD	Periodically	02/25/2022 02:34 PM	02/25/2022 03:04 PM
☐	SD	Periodically	02/25/2022 03:04 PM	02/25/2022 03:34 PM
☐	SD	Periodically	02/25/2022 03:34 PM	02/25/2022 03:38 PM
☐	SD	Periodically	02/25/2022 03:41 PM	02/25/2022 03:44 PM
☒	SD	Alarm record	03/01/2022 11:20 AM	03/01/2022 11:21 AM
☐	SD	Alarm record	03/03/2022 11:19 AM	03/03/2022 11:20 AM

Items per page: 999 << 1 / 1 >> **DOWNLOAD**

Note: The alarm records sorted in Trigger type are alarm type recording, not periodically recording. It includes Motion alarm, I/O alarm, Intrusion alarm, Multi loiter alarm, Smart motion alarm, Camera tamper alarm, Personnel count threshold alarm.

Recording Settings

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

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

General Setup

Alarm post record
10 [0-86400s]

☐ Record audio

Record rule
Cycle store

Stream profile
Main stream

Schedule record

☒ Schedule record

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Sun	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed
Mon	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed
Tues	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed
Wed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed
Thur	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed
Fri	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed
Sat	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed

☐ Network failure record

Network Failure Record

NVR IP address Time
 5 [5-12s]

Schedule record: Enables schedule record that you can configure the time policy.

Alarm post record: Recording duration (in seconds) after an alarm is generated.

Record audio: Indicates whether to record audios together with videos.

Record rule: Rule for saving recordings. The options are as follows:

Cycle Store: Saves recordings in cycles.

Save Days: Duration (in days) for saving a recording. The duration can be a maximum of 99999 days.

The value 0 indicates that recordings are not overwritten.

Stream profile: Select from the dropdown list: Main stream, Sub stream, Third stream.

Network Failure Record: Enable **Network failure record**. Fill in the NVR IP address and continuation time. The camera will keep detecting the connection status that the IPC accessed to NVR.

If the time is set as 5, when the NVR is disconnected, the camera's SD card will wait for 5s then start to record. When NVR is restoring recording, the SD card will go on recording for 5s, then stop to record.

- Note:**
- *The settings above are applied to all video recording behaviors globally.*
 - *The Network Failure Record function depends on ONVIF server detection. When the IP camera disconnection lasts for more than 15 sec, the Network Failure Record function will go working.*
 - *The time for Network Failure Record means the time that the IP camera continues recording video in SD card after the IP camera is recovered for connecting to the NVR.*
 - *For Network Failure Record function, the camera can only support the pre-recording buffer with fixed 15MB. It needs about 18~20S to detect the abnormal RTSP disconnection to start the recording and storage in SD card. To make the backfill cover the recording gap on end-head side, it is recommended to configure it with low bitrate.*

Schedule: Left-click or drag the mouse to select any time within 0:00-24:00 from Monday to Sunday.

CONFIGURE SYSTEM SETTINGS

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 55 System General Settings

System Setup

Camera name
HC35WE5R3 **SAVE NAME**

System Time

Time zone
GMT Casablanca, Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

☐ Daylight savings time

SAVE

Device time
2000/01/05 01:12:08

Current PC time
2022/01/18 16:59:47 **SYNCHRONIZE**

Set manually
2000/1/5 01:11:26 **SYNCHRONIZE**

☐ NTP

SAVE

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

Time zone: Select the appropriate time zone from the dropdown list.

Daylight savings time: Check the checkbox to enable Daylight savings time and specify the DST start time and end time.

- When the DST start time arrives, the device time automatically goes forward one hour.
- When the DST end time arrives, the device time automatically goes backward one hour.

Device time: Device display time. It is recommended to use NTP to make sure the time is correct, otherwise the device time maybe inaccurate.

Current PC time: Time on the current PC.

Set manually: Enables you to manually set the device time.

NTP: IP address or domain name of the NTP server. Check the checkbox to enable NTP.

NTP server addr: The NTP server IP.

NTP Port: Port number of the NTP server.

Check the time interval(at least 10 s): Set time interval to check if the device time synchronizes with the NTP server time.

Configuring Maintenance Settings

Go to **Setup > System Setup > Maintenance**.

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

The screenshot shows the 'Maintenance' settings page. It features two tabs at the top: 'GENERAL SETTINGS' and 'IMPORT/EXPORT FILES'. The 'Upgrade firmware' section includes a 'Firmware file' label, a 'CHOOSE FILE' button, and the text 'No file chosen'. An 'UPGRADE' button is positioned to the right. The 'Reboot' section has a 'REBOOT' button. The 'Restore' section contains a checkbox for 'Reserve IP setting' and a 'RESTORE' button.

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.
- 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 82.
- 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 33).

Daylight Savings Time: Check to retain the Daylight Savings Time settings (see [Importing/Exporting Files](#) on page 88).

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

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

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

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

Importing/Exporting Files

Export / Upload daylight savings time rules, custom language file, configuration file, and server status report.

The screenshot shows the 'EXPORT/EXPORT FILES' tab in the Honeywell web client. It is divided into two main sections: 'Export Files' and 'Upload Files'. In the 'Export Files' section, there are two 'EXPORT' buttons, one for the 'CA certificate' and one for the 'Export configuration file'. Below these is a text input field for the 'Password for exporting configuration file'. The 'Upload Files' section contains a 'CHOOSE FILE' button, the text 'No file chosen', and an 'UPLOAD' button. Below these is a text input field for the 'Password for uploading configuration file'. At the bottom, a status message with an information icon states: 'The configuration upload is successful, the device will restart'.

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. 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

Click **EXPORT** to export all parameters for the camera and user-defined scripts.

Note: *User needs to specify the password before exporting the configuration file.*

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 Privacy Policy

Go to **Setup > System Setup > Maintenance > PRIVACY POLICY**.

“admin” User can upgrade the privacy policy file to web, so that other users can understand the privacy policy and make sure that.

System Setup

General Settings **Maintenance** User Accounts Access List

GENERAL SETTINGS IMPORT/EXPORT FILES **PRIVACY POLICY**

Import Privacy Policy

Privacy Policy

Now privacy notice is not imported.
Please note that this is an on-premise video system. By purchasing, installing and running the system you acknowledge and agree that you are the controller of any information collected, shared or processed in this system and that you are solely and completely liable to upload a valid privacy notice, to provide notices of any recordings and to obtain any legally required consents in your use of this system.

CLEAR UPGRADE

Administrator User can clear the default policy, edit the new privacy policy, click UPGRADE to save. When other users login the web, they should tick “I have read and accepted the Privacy Policy.” and accepted.

Note: *The default policy is “Please note that this is an on-premise video system. By purchasing, installing and running the system you acknowledge and agree that you are the controller of any information collected, shared or processed in this system and that you are solely and completely liable to upload a valid privacy notice, to provide notices of any recordings and to obtain any legally required consents in your use of this system.”*

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

Account Management

— New user —

User name

Password

Confirm password

Privilege

Administrators

DELETE ADD UPDATE

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.
2. Make necessary changes and click UPDATE to enable the setting or click DELETE to delete the account.

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.

IP filter: Check this item and click SAVE to enable the IP 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 filter address.

- 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 operation on page [33](#).*
 - *The Range rule only applies to IPv4 addresses.*

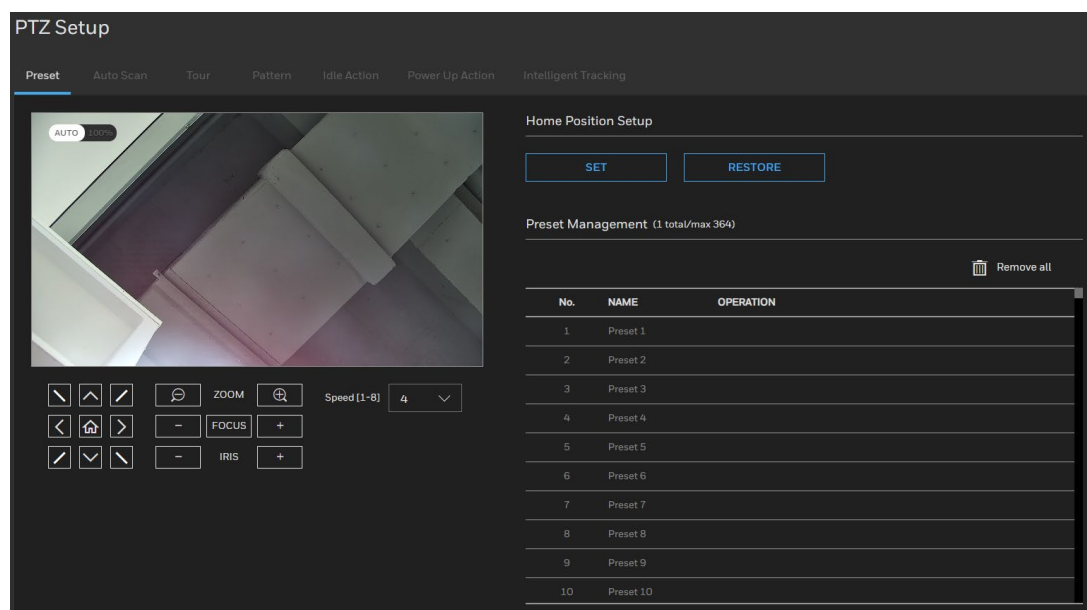
This section describes how to control the camera's Pan/Tilt/Zoom operation.

Note: The functions in this section are applicable for PTZ cameras only.

Preset

Go to **Setup** → **PTZ Setup** → **Preset**.

Figure 56 Preset Settings



: Click the buttons to move the video image up/right/down/left/45-degree tilt and click  to return to the home location.

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

FOCUS: Click  and  to adjust the **Focus** setting.

IRIS: Click  and  to adjust the **IRIS** setting.

Speed [1-8]: Select the movement speed for camera view. The speed range is 1 to 8 and the default setting is 5.

Home Position Setup

- **SET:** Click to set the current position as the home location.
- **RESTORE:** Click to restore the home position to default.

Preset Management

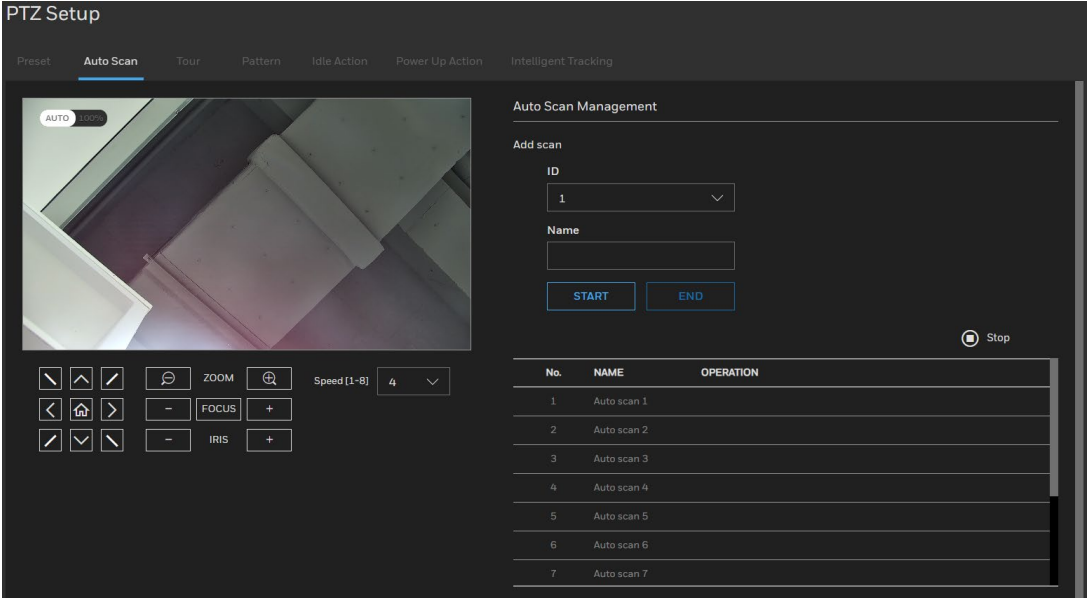
- Click Remove all to delete all the preset list.
- Click  to go to this preset.
- Click  to replace this preset with current position.
- Click  to remove the preset.

Note: Preset point 80~115 are reserved for special presets. And calling special preset 103 will run wiper once.

Auto Scan Management

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

Figure 57 Scan Settings



PTZ Setup

Preset **Auto Scan** Tour Pattern Idle Action Power Up Action Intelligent Tracking

Auto Scan Management

Add scan

ID: 1

Name:

START END

Stop

No.	NAME	OPERATION
1	Auto scan 1	
2	Auto scan 2	
3	Auto scan 3	
4	Auto scan 4	
5	Auto scan 5	
6	Auto scan 6	
7	Auto scan 7	



: Click the buttons to move the video image up/right/down/left/45-degree tilt and click  to return to the home location.

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

FOCUS: Click  and  to adjust the **Focus** setting.

IRIS: Click  and  to adjust the **IRIS** setting.

Speed [1-8]: Select the movement speed for camera view. The speed range is 1 to 8 and the default setting is 5.

Scan Management

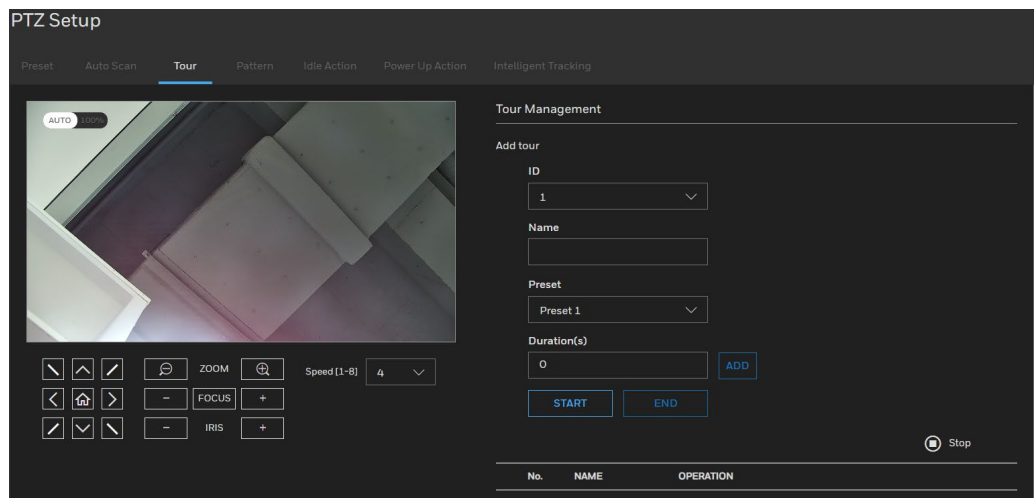
Add scan: Set the scan ID and name. Click **START** to start record. Click **END** to end record.

- Click  to start this scan.
- Click  to stop the scan setting.
- Click  to remove the scan.

Tour

Go to **Setup** → **PTZ Setup** → **Tour**.

Figure 58 Tour Settings



: Click the buttons to move the video image up/right/down/left/45-degree tilt and click  to return to the home location.

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

FOCUS: Click  and  to adjust the **Focus** setting.

IRIS: Click  and  to adjust the **IRIS** setting.

Speed [1-8]: Select the movement speed for camera view. The speed range is 1 to 8 and the default setting is 5.

Tour Management

Add tour: Set the tour ID/Name/Preset/Duration(s). Click **START** to start record. Click **END** to end record.

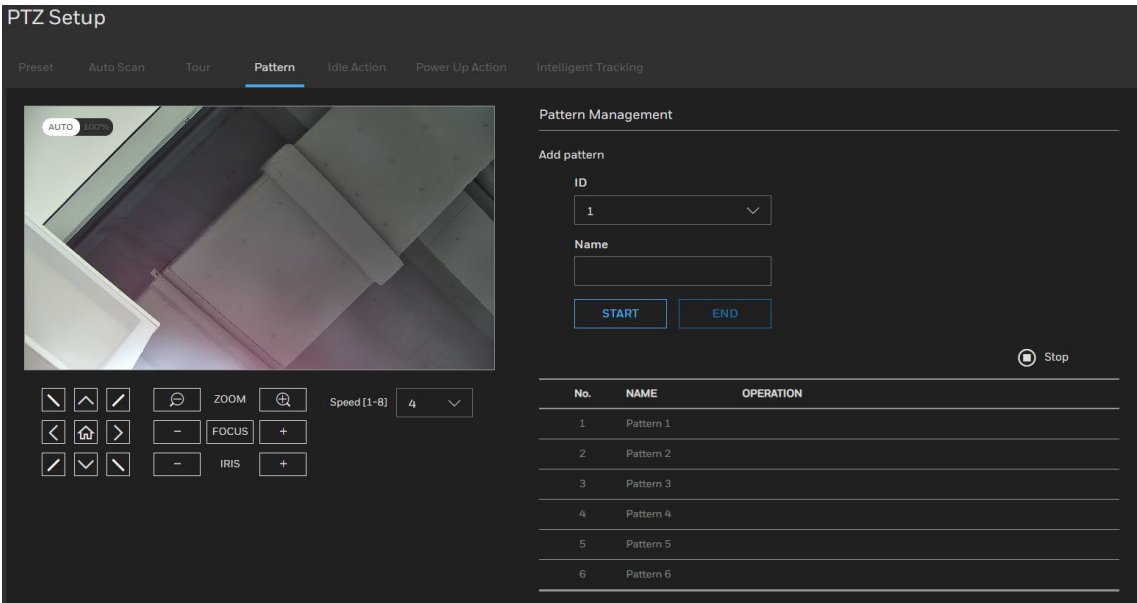
- Click  review your recorded tour.
- Click  to stop the tour review.
- Click  to remove the tour.

This Tour list displays the configured patrols. Note that only one Tour can be applied at a time.

Pattern

Go to **Setup** → **PTZ Setup** → **Pattern**.

Figure 59 Pattern



: Click the buttons to move the video image up/right/down/left/45-degree tilt and click  to return to the home location.

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

FOCUS: Click  and  to adjust the **Focus** setting.

IRIS: Click  and  to adjust the **IRIS** setting.

Speed [1-8]: Select the movement speed for camera view. The speed range is 1 to 8 and the default setting is 5.

Pattern Management

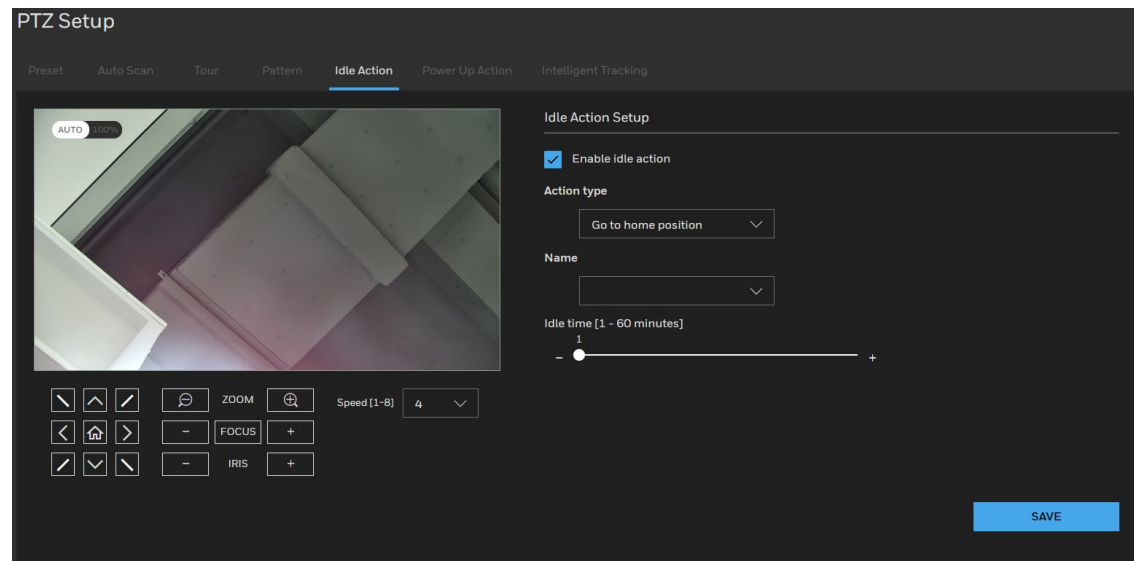
Add pattern: Set the pattern ID and Name. Click **START** to start record. Click **END** to end record.

- Click  review your pattern.
- Click  to stop the pattern review.
- Click  to remove the pattern.

Idle Action

Go to **Setup** → **PTZ Setup** → **Idle Action**.

Figure 60 Idle Action



Click the buttons to move the video image up/right/down/left/45-degree tilt and click  to return to the home location.

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

FOCUS: Click  and  to adjust the **Focus** setting.

IRIS: Click  and  to adjust the **IRIS** setting.

Speed [1-8]: Select the movement speed for camera view. The speed range is 1 to 8 and the default setting is 5.

Action type: The action includes go to home position/preset/auto scan/pattern/tour.

Name: The name of linkage action. For example, the preset name.

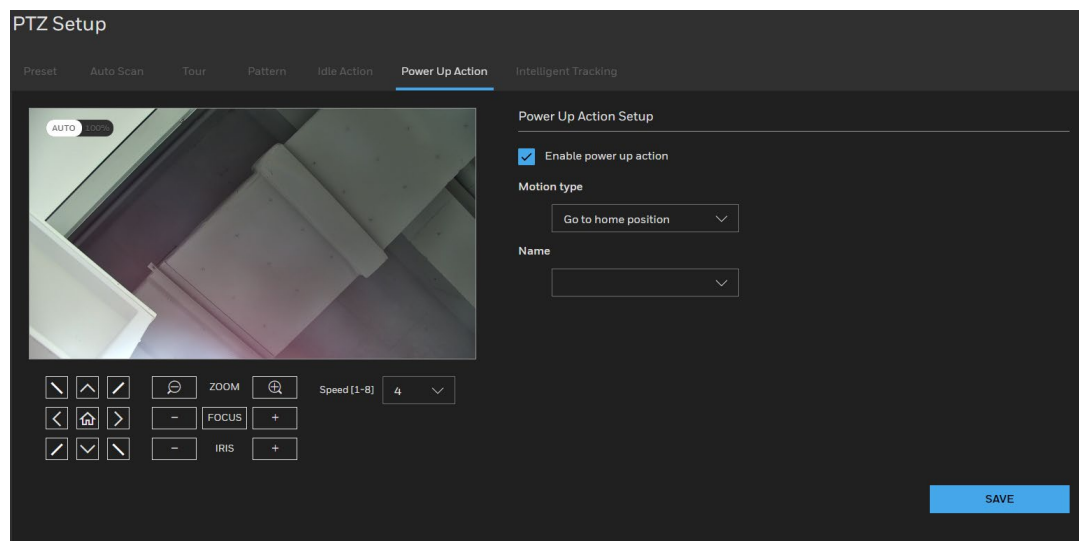
Idle time: The wait time for return to idle action.

Check the checkbox to enable idle action. Set the idle time. Click **SAVE**.

Power Up Action

Go to **Setup** → **PTZ Setup** → **Power Up Action**.

Figure 61 Power Up Action



Click the buttons to move the video image up/right/down/left/45-degree tilt and click  to return to the home location.

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

FOCUS: Click  and  to adjust the **Focus** setting.

IRIS: Click  and  to adjust the **IRIS** setting.

Speed [1-8]: Select the movement speed for camera view. The speed range is 1 to 8 and the default setting is 5.

Motion type: The action includes go to home position/preset/auto scan/pattern/tour.

Name: The name of linkage action. For example, the preset name.

Check the checkbox to enable power up action. Click **SAVE**.

Intelligent Tracking

Go to **Setup > PTZ Setup > Intelligent Tracking**.

Figure 62 Intelligent Tracking

The screenshot shows the 'PTZ Setup' window with the 'Intelligent Tracking' tab selected. The 'Intelligent Tracking Settings' section includes a checked checkbox for 'Enable intelligent tracking'. Below it are three sliders: 'Calibration coefficient' (range 1 to 30), 'Trace magnify' (range 1 to 30), and 'Time of duration(s)' (range 1 to 300, currently set at 120). There are two dropdown menus: 'Start point' (set to 'None') and 'Tracking type' (set to 'Person'). A blue 'SAVE' button is located at the bottom right.

Calibration coefficient: It is equivalent to a control coefficient, and real-time tracking doubling rate nonlinear positive correlation; Usually the higher the installation height, the greater the calibration coefficient value. Drag the slider to adjust the value among 1 to 30.

Trace magnify: It is the value of lens zoom, which has a large influence on the real-time tracking magnification. Drag the slider to adjust the value among 1 to 30.

Time of duration (s): The maximum time of a tracking period, Drag the slider to adjust the value among 1 to 300 s.

Start point: Choose preset or none to set the start point of the tracking. The preset should be set in advanced.

Tracking type: Choose the tracking type, human or vehicle.

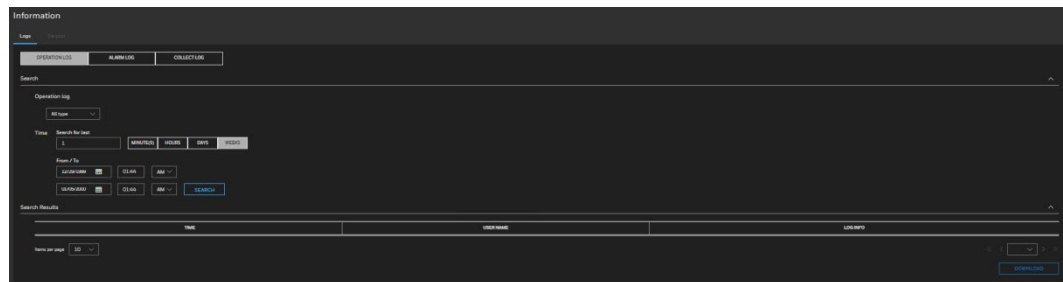
Check the checkbox to enable intelligent tracking. Click **SAVE**.

Logs

Go to **Setup > Information > Logs**.

Operation Log

Operation logs record user operations and scheduled task commands during the running of the device. Operation logs can be classified into the following types: permission management, system maintenance, device configuration, recording operation, video control, and real-time video.



1. Select the type of operation logs to be queried from the drop-down list box.
2. Set the start time and end time as required.
3. Click **SEARCH**.
The operation logs are displayed.
4. Click **Download** on the right of the page to download the operation logs.

Alarm Log

An alarm log records information about an alarm generated on a device, including the security, disk, and recording alarms.

1. Select the type of alarm logs to be queried from the drop-down list box.

2. Set the start time and end time as required.
3. Click **SEARCH**.
4. The alarm logs are displayed.
5. Click **Download** on the right of the page to download the operation logs.

Collect Log

You can collect logs about a device, which help you analyze and solve possible problems occurring on the device with one click.

1. Click **COLLECT**, the download page is displayed.
2. Select the path to save the logs.

Version

Go to **Setup > Information > Version**.

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

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 6 Troubleshooting for Common Issues

Issues	Solutions
<i>Power supply is unstable.</i>	Use of a UPS power supply is strongly recommended.
<i>Camera webpage has abnormal display.</i>	Clear the cache of browser. - If the pc screen width is 1366px, it is recommended to zoom the browser to 80%. - If the pc screen width is 1920px, it is recommended to zoom the browser to 100%.
<i>VA reference accuracy is up to 92% (only one VA is enabled). If the accuracy is lower than it, please refer the situations and solutions in the right column.</i>	1. Whether the height and angle of the camera meet the requirements 2. Whether the focus state of the camera is optimal, and the lens front cover is dusty 3. Whether the arming area is drawn on the border of the image 4. Whether the color of the item is similar to the background color (for the function of detecting removing leftover items) 5. Whether the camera is in a backlight environment which will affect the detection of the target and the effect of VA 6. Whether the target is appearing at the boundary of the area which will affect the judgment 7. Whether there is an obstruction near the target, in some cases, the target ID will change, which will affect the VA detection effect (such as the warning line) 8. If multiple targets are in the front and back positions (there will be partial occlusion and overlap), the number of detection targets is subject to the image and algorithm 9. If the accuracy rate is low, you can open the bounding box to check whether the target is detected normally

<i>The edge browser doesn't support H265 live view.</i>	1.Open the edge browser, input "edge://gpu". 2.Find "Media Foundation Rendering Capabilities", make sure the "HEVC installed " and "HEVC activatable" is true. a) If they are false, you need to download the HEVC Video Extensions. b) input "https://www.microsoft.com/store/productId/9N4WGH0Z6VHQ?ocid=dpshare" to download HEVC Video Extensions , click "Install" to jump to Microsoft store, download the Extension and install. 3.Reopen the edge browser after Finishing the installation.
<i>The Chrome browser doesn't support H265 live view.</i>	Need chrome 118.0.5993.118 or higher version.

List of Symbols

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

Table 7 List of Symbols

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.
	Eurasian Conformity (EAC) RoHS

Building Automation – Security Americas (Head Office)

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

Building Automation – 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

Building Automation – 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

Building Automation – Security Europe/South Africa

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

Building Automation – Security Northern Europe

Stationsplein Z-W 961, 1117 CE Schiphol-Oost, Netherlands
Tel: +31 (0) 299 410 200

Building Automation – Security Deutschland

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

Building Automation – Security France

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

Building Automation – Security Italia SpA

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

Building Automation – Security España

Josefa Valcárcel, 24
28027 – Madrid, España
Tel: +34 902 667 800

Building Automation – Security Asia Pacific

Building #1, 555 Huanke Road,
Zhang Jiang Hi-Tech Park Pudong New Area,
Shanghai, 201203, China
Tel: 400 840 2233

Building Automation – 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

Building Automation – 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

Building Automation – 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 600-60UG02 Rev B– 11/2024