

Honeywell

Honeywell 60 Series

Cameras

HC60WB5R2P
HC60W45R2P

HC60WB5R5P
HC60W45R4P

HC60W35R4P
HC60WFCR1

HC60W35R2P

User Guide

Recommended

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

Copy Right

© 2025 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	08/2025	New document.

Cautions and Warnings

 CAUTION RISK OF ELECTRIC SHOCK DO NOT OPEN 	 THIS SYMBOL INDICATES THAT DANGEROUS VOLTAGE CONSTITUTING A RISK OF ELECTRIC SHOCK IS PRESENT WITHIN THE UNIT.
CAUTION: TO REDUCE THE RISK OF ELECTRIC SHOCK, DO NOT REMOVE 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



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 the 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 this owner's ("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, according 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 under 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 the receiver.
- Connect the equipment to 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 following 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 an identified Return Merchandise Authorization (RMA) number may be refused.**

TABLE OF CONTENTS

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	10
	Configure IP Address Setting	10
	Configure DNS Server Address.....	10
	Upgrading the Camera's Firmware	11
	Accessing the Camera from a Web Browser	12
3	Logging in & Viewing Live Video.....	13
	Logging in to the Camera via the Web Client.....	13
	Before You Begin.....	13
	Logging in to the Camera	13
	Using the Main Page.....	16
	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	25
Configuring Audio Settings	26
Audio File.....	27
Configuring Image Settings	27
Mode	28
Scheme	28
Image Adjustment	28
Scene Mode.....	28
Exposure.....	29
White Balance (WB) Setting.....	29
DayNight Setting.....	30
Noise Reduction	31
Enhance Image.....	31
Zoom Focus (IPC Models)	32
Configuring OSD	32
Configuring Privacy Mask.....	33
5 Configuring Network Settings.....	34
Configuring Network General Settings.....	34
Configuring Streaming Protocols	35
Configuring SMTP Settings.....	39
Configuring SNMP Settings.....	41
Configuring QoS Settings	42
Configuring HTTPS Settings.....	42
HTTPS	42
Certificate Request.....	43
Upload Files	44
Configuring IEEE 802.1x Settings.....	45
Configuring FTP Settings.....	46
Configuring DDNS	47
Configuring Port Mapping.....	48
Configuring System Log.....	49
Configuring Network Discovery Protocols	53
6 Configuring Video Analytics	54
Object Analytics	56
Smart Motion	58

Scene Change.....	60
Intrusion Detection.....	62
Multi Loitering Detection.....	64
Face Detection.....	66
People Counter.....	67
Settings.....	67
Report.....	71
Line Crossing Detection.....	72
Unattended Object Detection.....	74
Missing Object Detection.....	76
Best Snapshot.....	77
Heat Map.....	78
Heat Map Set.....	78
Heat map.....	79
Report.....	80
Event & Metadata Scheme.....	81
License Plate Detection.....	82
License Plate Detection.....	82
List Management.....	83
List Event.....	84
Motion Detection.....	85
7 Configure Alarm and Event.....	88
Configuring Alarm In and Alarm Out.....	88
Alarm Input.....	88
Alarm Output.....	89
Configuring SD Card Alarm.....	91
Configuring Audio Detection.....	91
Configuring Illegal Access Alarm.....	92
Configuring Wiegand.....	93
8 Configure Storage Settings.....	94
SD Card Management.....	94
SD Card Status.....	95
SD Card Format.....	95
Content Management.....	95
Searching and Viewing the Records.....	96
Search Results.....	96
Recording Settings.....	98
9 Configure System Settings.....	100
Configuring System General Settings.....	100

Configuring Maintenance Settings.....	101
Upgrading Firmware.....	101
Rebooting the Camera.....	102
Restoring the Camera.....	102
Importing/Exporting Files.....	102
Configuring Privacy Policy.....	104
Configuring User Accounts Settings.....	105
Account Management.....	106
Configuring Access List Settings.....	106
10 Viewing System Information.....	108
Logs.....	108
Operation Log.....	108
Alarm Log.....	108
Collect Log.....	109
Version.....	109
Privacy Policy.....	109
11 Troubleshooting.....	111
Troubleshooting for Common Issues.....	111
12 Appendix.....	113
List of Symbols.....	113

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	16
Figure 13 Live View Toolbar	17
Figure 14 General Settings	19
Figure 15 Mode Tab	20
Figure 16 Video Stream	20
Figure 17 ROI Settings	25
Figure 18 Audio Settings	26
Figure 19 Audio File	27
Figure 20 Image Settings	28
Figure 21 Privacy Mask	33
Figure 22 Network General Settings	34
Figure 23 Streaming Protocols-HTTP	36
Figure 24 Streaming Protocols-RTSP	37
Figure 25 SMTP Settings	40
Figure 26 HTTPS Settings	43
Figure 27 Certificate Request	44
Figure 28 IEEE 802.1x Configurations – EAP-TLS	45
Figure 29 File Transfer Protocol (FTP)	46
Figure 30 DDNS Interface	47
Figure 31 Port Mapping Interface	48
Figure 32 System Log Interface	49
Figure 33 Network Discovery Protocols	53
Figure 34 Video Analytics Interface	55
Figure 35 Package Management Interface	55
Figure 36 License Activation	56
Figure 37 Smart Motion	59
Figure 38 Set A Detection Area	60
Figure 39 Scene Change	61
Figure 40 Intrusion Detection	62
Figure 41 Set Intrusion Area	63
Figure 42 Multi Loitering	64
Figure 43 Set Multi Loitering Area	65
Figure 44 Face Detection	66
Figure 45 View of Facing the Flow of People	68
Figure 46 Facing the Side Way Flow of People	69
Figure 47 People Counter	70
Figure 48 Line of People Counter	70
Figure 49 Number for In / Out / Stay	70
Figure 50 People Counter-REPORT	72
Figure 51 Single Line Crossing	73

Figure 52 Unattended Object Detection..... 75

Figure 53 Missing Object Detection 76

Figure 54 Best Snapshot Set..... 77

Figure 55 Heat Map Set..... 79

Figure 56 Event & Metadata Scheme 79

Figure 57 Event & Metadata Scheme 80

Figure 58 Event & Metadata Scheme 81

Figure 59 Basic Settings..... 82

Figure 60 List Management Interface 83

Figure 61 Add Plate..... 83

Figure 62 List Event—White List/Black List..... 84

Figure 63 List Event—Visitor 85

Figure 64 Motion Detection Interface 86

Figure 65 Set A Detection Area 87

Figure 66 Alarm Input..... 88

Figure 67 Alarm Output..... 90

Figure 68 Audio Detection..... 91

Figure 69 Illegal Access Alarm 92

Figure 70 Wiegand 93

Figure 71 No SD Card 95

Figure 72 SD Card Onboard 95

Figure 73 Play Recording..... 97

Figure 74 System General Settings 100

Tables

Table 1 Live View Toolbar Icons 17

Table 2 Cameras Resolution..... 21

Table 3 Cameras Frame Rate 23

Table 4 Port Mapping Parameters 48

Table 5 Compatible SD Card 94

Table 6 Troubleshooting for Common Issues 111

Table 7 List of Symbols 113

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 with traditional camera and network video technology and combine video data collection and transmission. These flexible, fully featured cameras are the ideal choice for a wide range of surveillance applications.

The cameras include 5 MP indoor / outdoor dome cameras, 5 MP outdoor bullet cameras and a 12 MP fisheye camera. 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), 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 systems and don't support mobile systems.*

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 of the Honeywell 60 Series IP camera are:

Camera

- Up to 5 MP (2592x1944) for indoor / outdoor dome cameras and outdoor bullet cameras and 12 MP (3552 x 3552) for fisheye camera cameras
- Video parameter setup, such as electronic shutter and gain
- 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 (applicable for HC60W35R4P / HC60W35R2P / HC60W45R2P / HC60W45R4P / HC60WB5R2P / HC60WB5R5P)
- 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 the 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, UDP, ICMP, ARP, TLS, FTP/SFTP, DDNS

- Support the following security modes: User account and password protection, HTTPS, IP Filter, Digest authentication, TLS1.2&TLS1.3, Stream encryption, AES128 / 256, SSH / Telnet closed, PCI-DSS compliance, Built-In encryption chipset
- Support the following languages: Arabic, Czech, Dutch, English, French, German, Italian, Japanese, Korean, Polish, Portuguese (Brazil), 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, License Plate Detection (Be different for different models. More details, please refer to the product datasheet)
- Support the following event types: Alarm input, SD card alarm, Abnormal sound alarm, Illegal Access Alarm
- Support the following event linkage mode: Event notification using digital output, FTP/SFTP, Email, Micro SD card recording and audio output

User Management

- Each user belongs to a 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 10
- [Upgrading the Camera's Firmware](#), page 11
- [Accessing the Camera from a Web Browser](#), page 12

Installing the Unified Tool

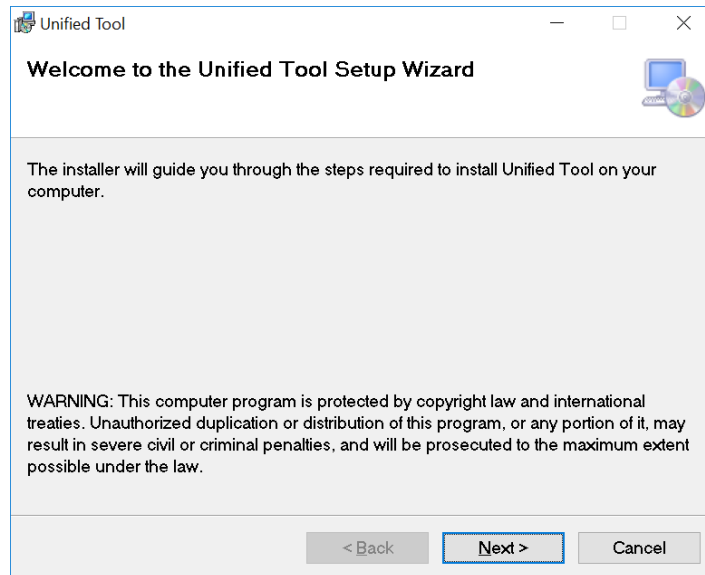
To get the installation package of Unified Tool:

Go to <https://myhoneywellbuildingsuniversity.com> and log in. 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:

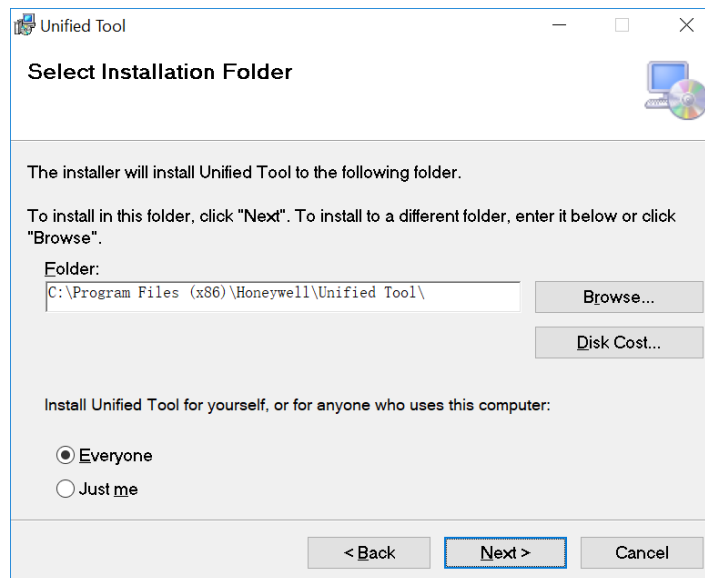
1. Double-click the installation program  in the installation package.

Figure 1 Install Unified Tool



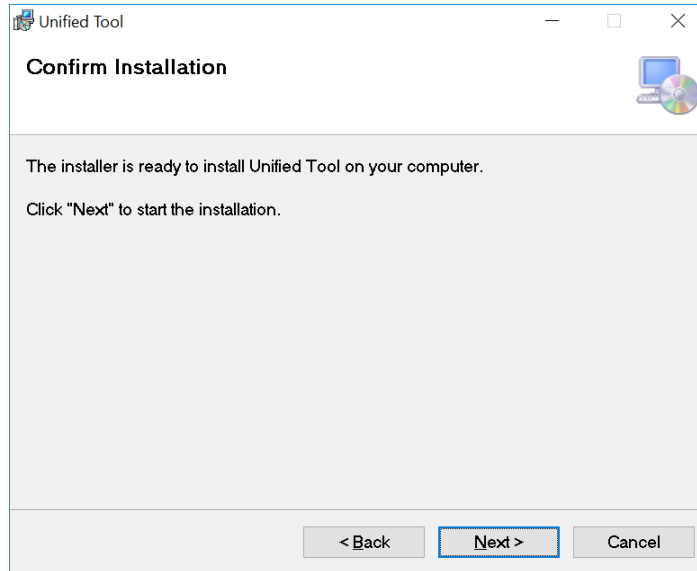
2. Click Next and the following figure is displayed:

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

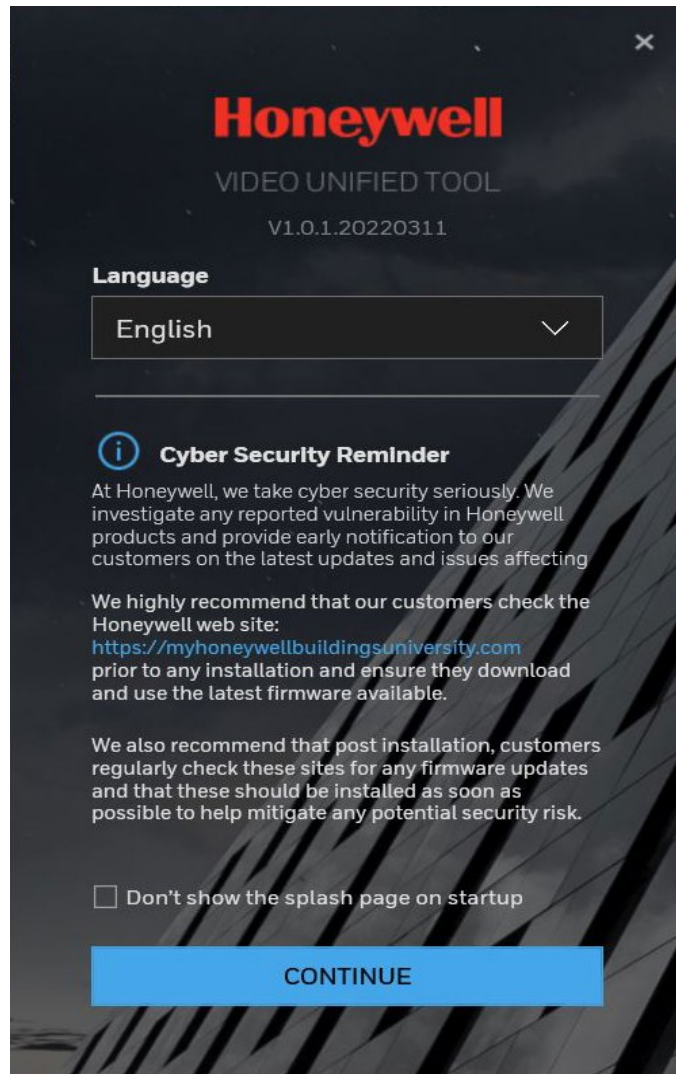


4. Click Next. When the installation is completed, click Close. A shortcut of Unified Tool will be displayed on your desktop.

Discovering Your Camera on the Network

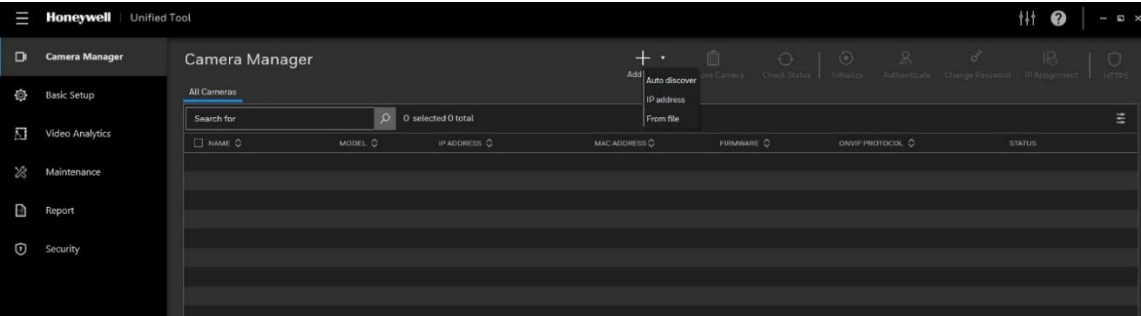
1. Double-click  on the desktop and the following figure is displayed:

Figure 4 Splash Screen



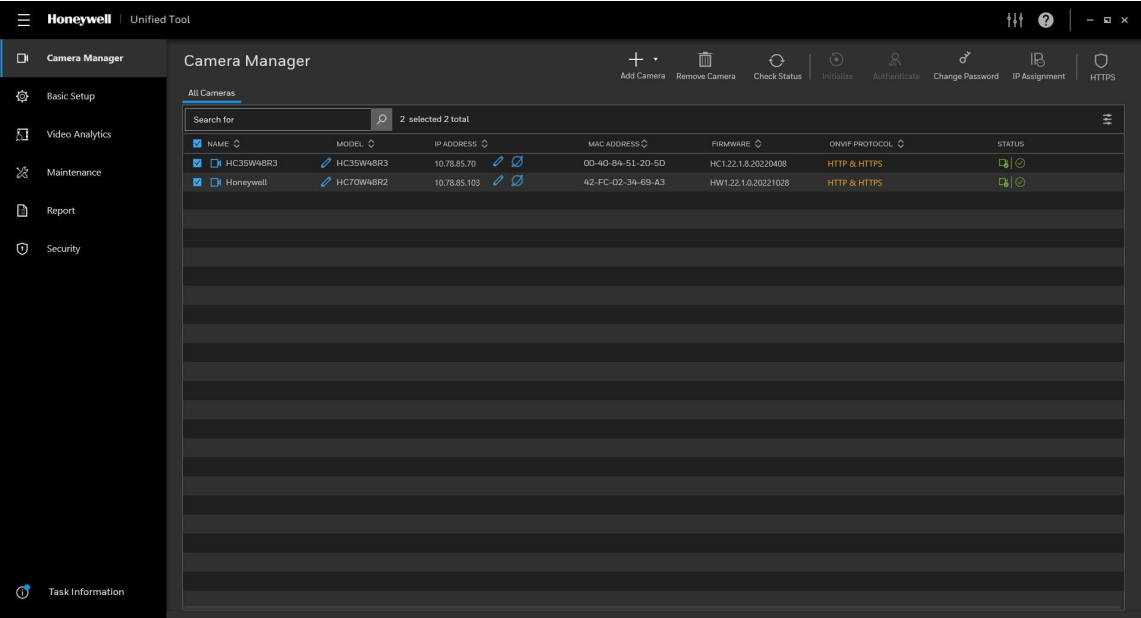
2. Select your language from the dropdown list of Language. Currently, English and traditional Chinese are supported.
3. Check Don't show the splash page on startup and this page can be skipped next time. If you want to check the splash window again, click  as shown in [Figure 6](#) and select the checkbox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

Figure 6 Device List



Initializing Cameras

It is recommended to initialize the 35 Series cameras by clicking . By initialization, you can set the camera password in batch.

Figure 7 Initialize Page 1

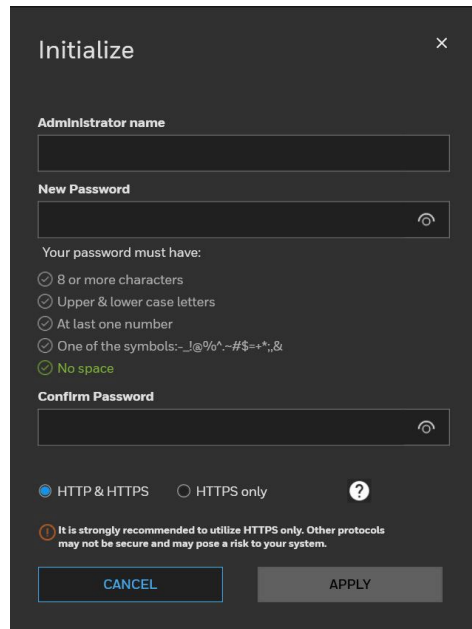
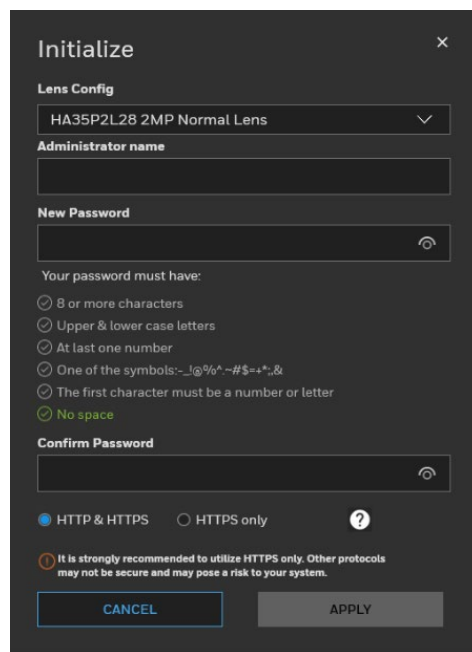
A screenshot of the 'Initialize' dialog box, Page 1. It features a dark background with white text. At the top is the title 'Initialize' and a close button (X). Below the title are two input fields: 'Administrator name' and 'New Password'. The 'New Password' field has a toggle icon on the right. Underneath the password field, a list of requirements is shown with checkmarks: '8 or more characters', 'Upper & lower case letters', 'At last one number', 'One of the symbols: _!@%&^*~#\$+=*~&', and 'No space' (highlighted in green). Below this is a 'Confirm Password' field with a toggle icon. At the bottom, there are two radio buttons: 'HTTP & HTTPS' (selected) and 'HTTPS only'. A help icon (?) is next to the 'HTTPS only' option. A warning message states: 'It is strongly recommended to utilize HTTPS only. Other protocols may not be secure and may pose a risk to your system.' At the very bottom are two buttons: 'CANCEL' and 'APPLY'.

Figure 8 Initialize Page 2

A screenshot of the 'Initialize' dialog box, Page 2. It features a dark background with white text. At the top is the title 'Initialize' and a close button (X). Below the title is a 'Lens Config' section with a dropdown menu showing 'HA35P2L28 2MP Normal Lens'. Below this are the same 'Administrator name' and 'New Password' fields as in Figure 7. The password requirements list is identical, with 'No space' highlighted in green. Below the password fields are the same 'HTTP & HTTPS' (selected) and 'HTTPS only' radio buttons, along with the same warning message and 'CANCEL'/'APPLY' buttons at the bottom.

For split pin hole cameras, lens can be selected on the Initialize page, please refer to [Figure 8](#).

On the **Initialize** page, please set **Administrator name** and **New password**. Select **HTTP & HTTPS** or **HTTPS only**. Click **APPLY**.

- Note:**
- *Honeywell strictly recommends to use HTTPs only and Honeywell will not hold responsible for the consequences.*
 - *For ONVIF & streaming protocols setting, unsupported model will be skipped.*

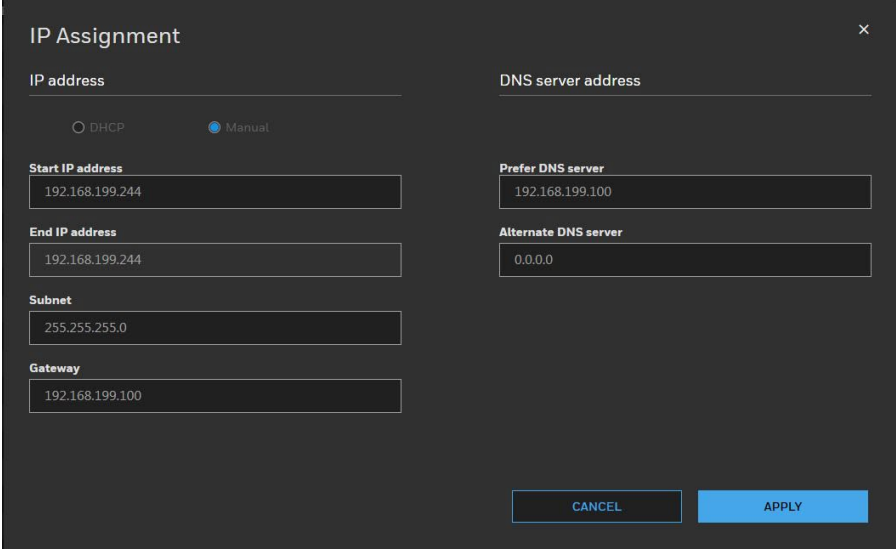
After initializing successfully, you can authenticate the camera and configure other setting.

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 'IP Assignment' and a close button. The dialog is divided into two main sections. The left section is titled 'IP address' and contains two radio buttons: 'DHCP' (unselected) and 'Manual' (selected). Below the radio buttons 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). The right section is titled 'DNS server address' and contains 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 the IP address, subnet mask, and default gateway settings automatically, select the check box of **DHCP**.
- To configure the 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

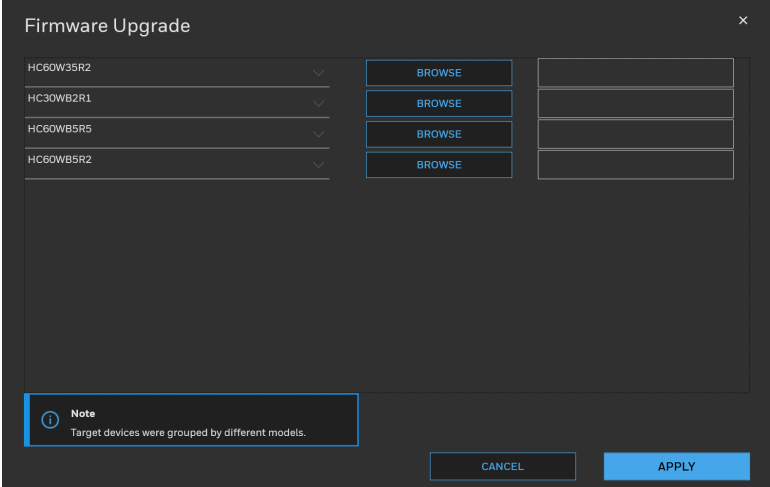
Configure the DNS server address and click **APPLY**.

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

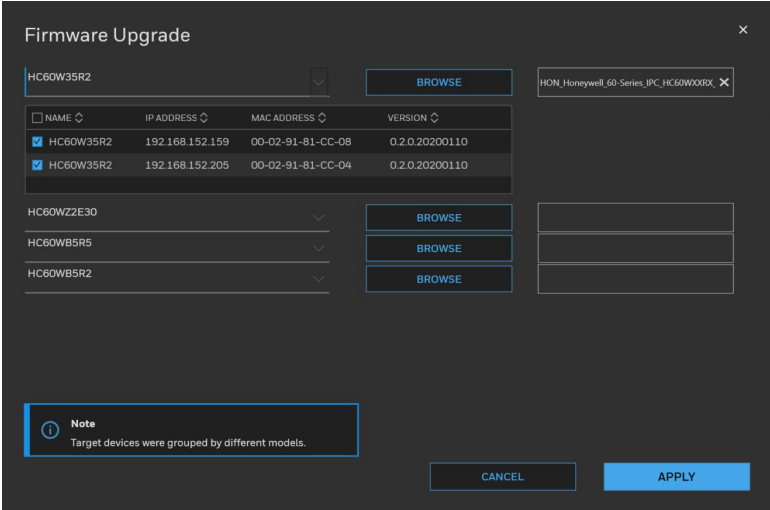


The dialog box titled "Firmware Upgrade" contains a list of camera models on the left: HC60W35R2, HC30WB2R1, HC60WB5R5, and HC60WB5R2. Each model has a dropdown arrow to its right. To the right of the list are four "BROWSE" buttons, one for each model. At the bottom left, there is a "Note" box with an information icon and the text "Target devices were grouped by different models." At the bottom right are "CANCEL" and "APPLY" buttons.

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



The dialog box titled "Firmware Upgrade" shows the "HC60W35R2" model selected in the dropdown. The "BROWSE" button next to it is active, and a file path "HC60W35R2_Honeywell_60-Series_IPC_HC60W35R2" is displayed in the adjacent text box. Below the model list, a table shows the selected devices:

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

Below the table, the other camera models (HC60W22E30, HC60WB5R5, HC60WB5R2) are still listed with their respective "BROWSE" buttons. The "Note" box and "CANCEL/APPLY" buttons remain at the bottom.

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 13
- [Using the Main Page](#), page 16

Logging in to the Camera via the Web Client

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

Before You Begin

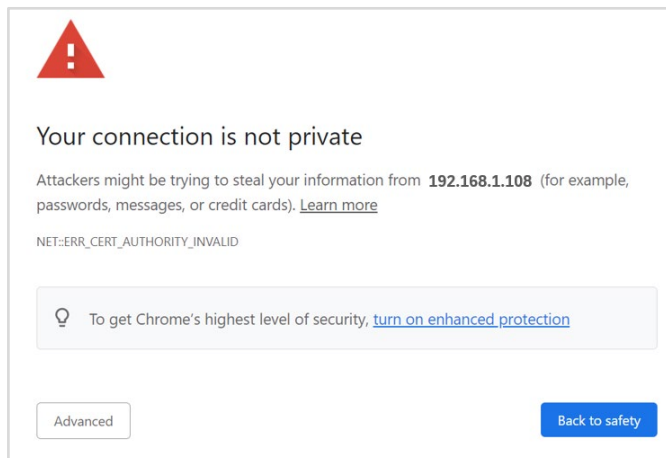
Before you log in to the web client, ensure that the following conditions are met:

- 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]").

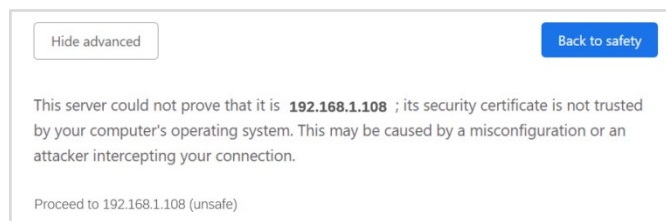
Note: *The new security enhancements do not allow pinging the camera IP address.*

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.

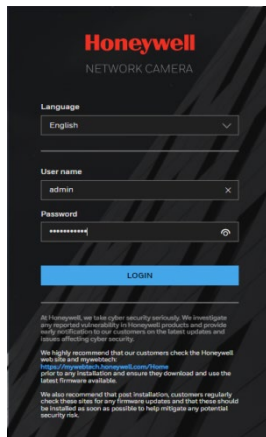
The password must be at least 8 characters in length and contain at least one uppercase letter, one lowercase letter, one number, and one special character (-_!@%^.~?#\$.+*.,&). The password cannot be blank. Click **SAVE**.

5. Setup ONVIF & Streaming Protocol.

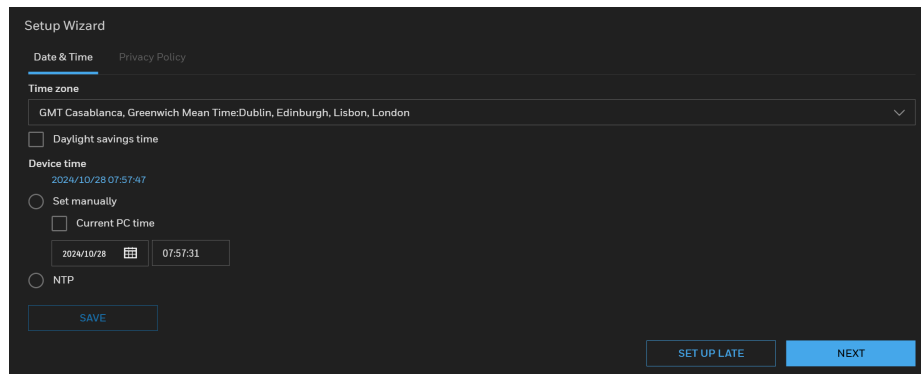
HTTP&HTTPS (better compatibility), HTTPS only (better cyber-security).

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 below it. The interface is dark-themed. There are three input fields: 'Language' with a dropdown menu showing 'English', 'User name' with 'admin' entered, and 'Password' with masked characters. A blue 'LOGIN' button is positioned below the password field. At the bottom, there is a small white text block containing security disclaimers and recommendations.

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

The image shows the 'Setup Wizard' window, specifically the 'Date & Time' tab. The window has a dark background. The 'Time zone' is set to 'GMT Casablanca, Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London'. There is a checkbox for 'Daylight savings time' which is currently unchecked. The 'Device time' is shown as '2024/10/28 07:57:47'. Below this, there are two options: 'Set manually' (selected) and 'NTP'. Under 'Set manually', there are input fields for 'Current PC time' showing '2024/10/28' and '07:57:31'. A 'SAVE' button is at the bottom left, and 'SET UP LATE' and 'NEXT' buttons are at the bottom right.

- **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**

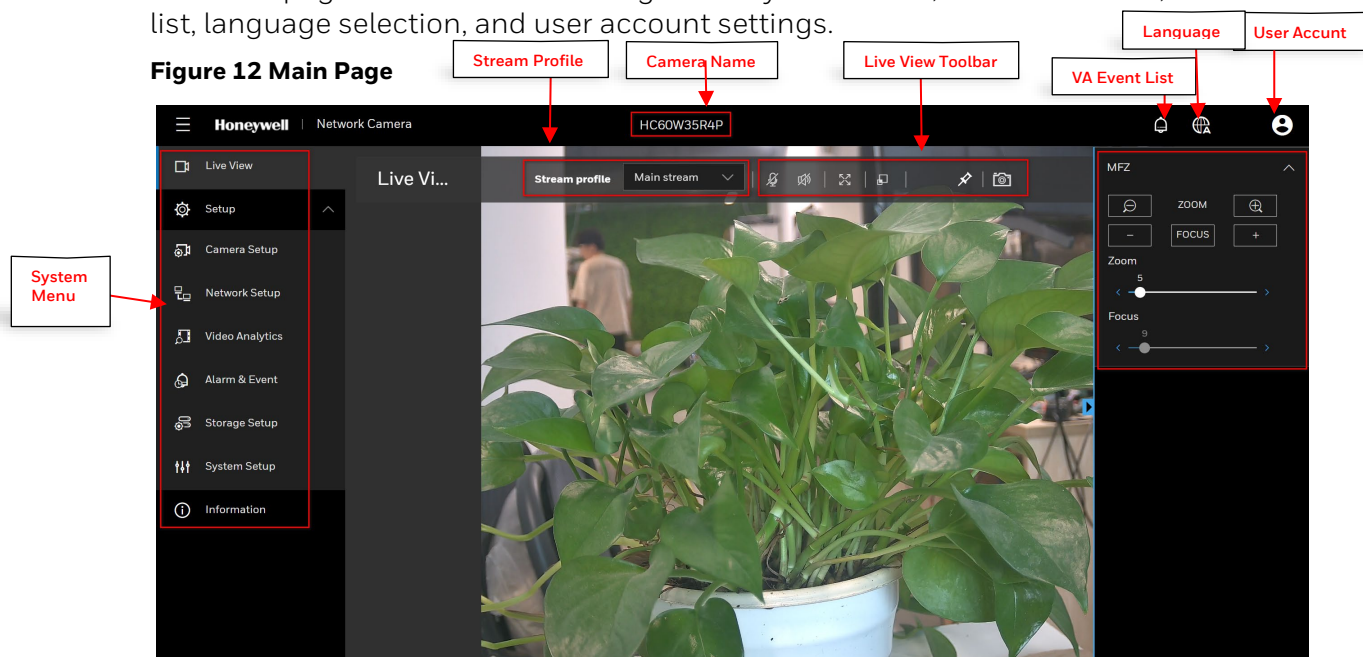
Tick **Do not remind me again** and click **Cancel**, the pop-up window will not show at next time. If untick **Do not remind me again**, the pop-up window will show whenever logging in.

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 the MFZ IPC model, an MFZ panel can be accessed by clicking  on the right as shown in [Figure 12](#).

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 100.

Live View Toolbar

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

Figure 13 Live View Toolbar



Table 1 Live View Toolbar Icons

Icon	Description
	The icon can be enabled from the webpage when the microphone is connected to the PC or embedded in the PC. Click to enable the PC microphone. You can talk and the audience can listen through speakers connected to the camera. Click it again to disable this option.
	The icon can be enabled from the webpage when the speaker is connected to the PC or embedded in the 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.
	Bounding box on/ bounding box off. When the bounding 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 Picture 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 the 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 for more alarm log records. Refer to the [Alarm Log](#).

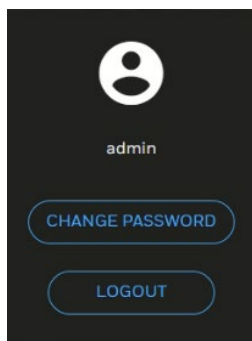
Language

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

Administrator Account

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

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



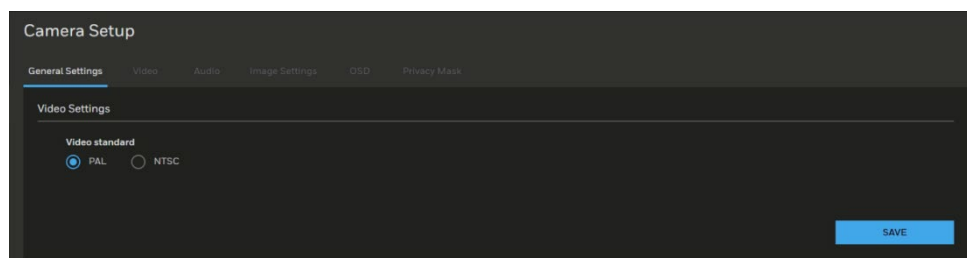
Click **CHANGE PASSWORD** to change the current login user's password.
Click **LOG OUT** to log out of the current account.

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 14 General Settings



Configuring Video Settings

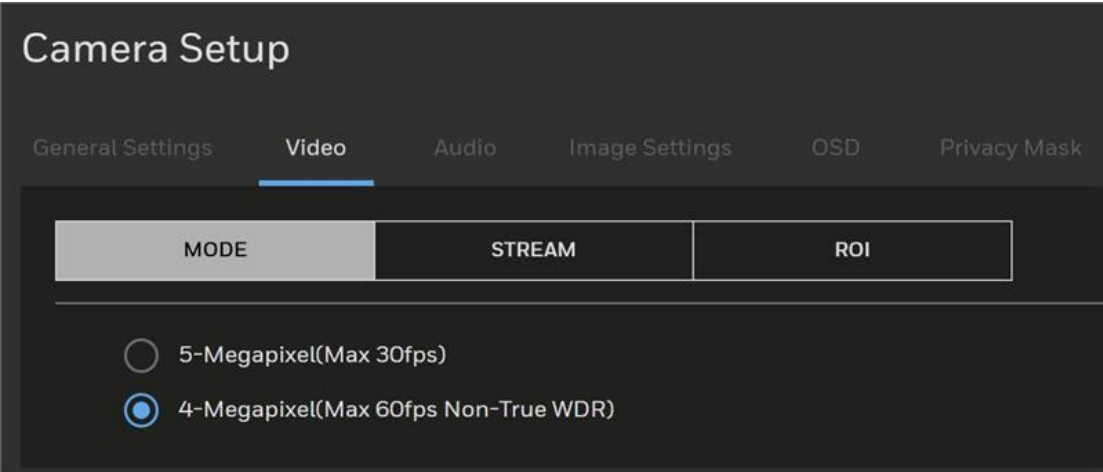
Go to **Setup > Camera Setup > Video**.
This section describes how to configure Video stream and ROI settings.

Mode

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

- Note:**
- *The Mode function is applicable for HC60W35R4P / HC60W35R2P / HC60W45R2P / HC60W45R4P / HC60WB5R2P / HC60WB5R5P.*
 - *Changing the video mode will clear the following settings: privacy mask, image setting, motion, preset position, and focus window.*

Figure 15 Mode Tab



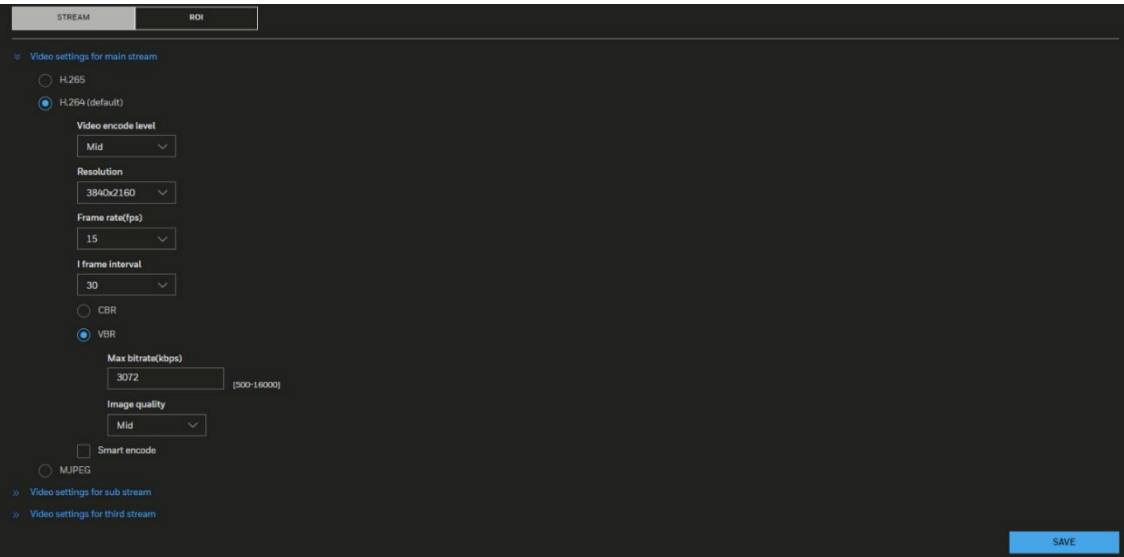
5-Megapixel (Max 30fps): Select it and the maximum resolution will be 2592x1944.

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

Video Stream

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

Figure 16 Video Stream



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

Note: *It is recommended to use the 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 the resolution of each model:

Table 2 Cameras Resolution

Model	Main Stream	Sub Stream	Third Stream
HC60WB5R2P/HC60WB5R5P/HC60W35R4P/HC60W35R2P/HC60W45R2P/HC60W45R4P	2592 x 1944 2688 x 1520 2560 x 1440 2304 x 1296 1920 x 1080 1280 x 720 25/30fps	2592 x 1944 1920 x 1080 704 x 576 640 x 480 352 x 288 25/30fps	2592 x 1944 640 x 480 352 x 288 320 x 240 25/30fps
HC60WB5R2P/HC60WB5R5P/HC60W35R4P/HC60W35R2P/HC60W45R2P/HC60W45R4P 60 fps	2560 x 1440 2304 x 1296 1920 x 1080 1280 x 720 50/60 fps	2560 x 1440 2304 x 1296 1920 x 1080 1280 x 720 704 x 480 640 x 480 352 x 240 50/60 fps	1920 x 1080 1280 x 720 640 x 480 352 x 240 320 x 240 50/60 fps
HC60WFCR1 One-Channel Fisheye	3552 x 3552 2560 x 2560 1520 x 1520 1280 x 1280 25/30fps	640 x 640 480 x 480 25/30fps	1520 x 1520 704 x 480/704 x 576 640 x 640 480 x 480 352 x 240/352 x 288 25/30fps
HC60WFCR1 One-Channel Double Panorama (1:1)	3552 x 3552 2560 x 2560 1520 x 1520 1280 x 1280 25/30fps	640 x 640 480 x 480 25/30fps	640 x 640 480 x 480 25/30fps
HC60WFCR1 One-Channel Double Panorama (4:3)	4000 x 3000 3552 x 2664 2592 x 1944 1280 x 960	640 x 480 320 x 240 25/30fps	640 x 480 320 x 240 25/30fps
HC60WFCR1 One-Channel Double Panorama (16:9)	3840 x 2160 2880 x 1620 2560 x 1440 1280 x 720 25/30fps	640 x 360 25/30fps	640 x 360 25/30fps
HC60WFCR1、 One-Channel 4 PTZ (1:1)	3552 x 3552 2560 x 2560 1520 x 1520 1280 x 1280 25/30fps	640 x 640 480 x 480 25/30fps	640 x 640 480 x 480 25/30fps
HC60WFCR1、 One-Channel 4 PTZ (4:3)	4000 x 3000 3552 x 2664 2592 x 1944 1280 x 960	640 x 480 320 x 240 25/30fps	640 x 480 320 x 240 25/30fps

Model	Main Stream	Sub Stream	Third Stream
HC60WFCR1、 One-Channel 4 PTZ (16:9)	3840 x 2160 2880 x 1620 2560 x 1440 1280 x 720 25/30fps	640 x 360 25/30fps	640 x 360 25/30fps
HC60WFCR1 One-Channel Single Panorama (4:1) Mounting mode: Ceiling/Desktop	4096 x 1024 2560 x 640 1920 x 480	1920 x 480 960 x 240	1920 x 480 960 x 240
HC60WFCR1 One-Channel Single Panorama (16:3) Mounting mode: Ceiling/Desktop	4096 x 768 2560 x 480 1920 x 360	1920 x 360 1280 x 240	1920 x 360 1280 x 240
HC60WFCR1 One-Channel Single Panorama (4:3) Mounting mode: Walling	4000 x 3000 3552 x 2664 2592 x 1944 1280 x 960	640 x 480 320 x 240	640 x 480 320 x 240
HC60WFCR1 One-Channel Single Panorama (16:9) Mounting mode: Walling	3840 x 2160 2880 x 1620 2560 x 1440 1280 x 720	640 x 360	640 x 360
HC60WFCR1 One-Channel 1Fisheye+3PTZ	3552 x 3552 2560 x 2560 1520 x 1520 1280 x 1280	640 x 640 480 x 480	640 x 640 480 x 480
HC60WFCR1 Multi-Channel 4PTZ (1:1)	1776 x 1776 1520 x 1520 1280 x 1280 1280 x 960 720 x 720	640 x 640 704 x 480 352 x 240 320 x 240	1520 x 1520 1280 x 1280 640 x 640 704 x 480 352 x 240
HC60WFCR1 Multi-Channel 4PTZ (4:3)	2048 x 1536 1280 x 960	640 x 480 320 x 240	640 x 480 320 x 240
HC60WFCR1 Multi-Channel 4PTZ (16:9)	2304 x 1296 1280 x 720	640 x 360	640 x 360
HC60WFCR1 Multi-Channel 1Fisheye+3PTZ Fisheye	3552 x 3552 1776 x 1776 1520 x 1520 1280 x 1280 1280 x 960 720 x 720	640 x 640 704 x 480/704 x 576 352 x 240/352 x 288 320 x 240	1520 x 1520 1280 x 1280 640 x 640 704 x 480/704 x 576 352 x 240/352 x 288

Model	Main Stream	Sub Stream	Third Stream
HC60WFCR1 Multi-Channel 1Fisheye+3PTZ PTZ	1776 x 1776 1520 x 1520 1280 x 1280 1280 x 960 720 x 720	640 x 640 704 x 480/704 x 576 352 x 240/352 x 288 320 x 240	1520 x 1520 1280 x 1280 640 x 640 704 x 480/704 x 576
HC60WFCR1 Multi-Channel 1Fisheye+6PTZ Fisheye	3552 x 3552 1776 x 1776 1520 x 1520 1280 x 1280 1280 x 960 720 x 720	640 x 640 704 x 480/704 x 576 352 x 240/352 x 288 320 x 240	N/A
HC60WFCR1 Multi-Channel 1Fisheye+6PTZ PTZ	1776 x 1776 1520 x 1520 1280 x 1280 1280 x 960 720 x 720	640 x 640 704 x 480/704 x 576 352 x 240/352 x 288 320 x 240	N/A

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 the frame rate of each model:

Table 3 Cameras Frame Rate

Connection Type	Camera	Main Stream	Sub Stream	Third Stream
HTTP	HC60WB5R2P/H C60WB5R5P/HC 60W35R4P/HC60 W35R2P/HC60W 45R2P/HC60W45 R4P	Frame rate (FPS): PAL 25/NTSC 30 I frame interval: PAL 50/NTSC 60 Bit rate (Kbps):16000	Frame rate (FPS): PAL 25/NTSC 30 I frame interval: PAL 50/NTSC 60 Bit rate (Kbps): 16000	Frame rate (FPS): PAL 25/NTSC 30 I frame interval: PAL 50/NTSC 60 Bit rate (Kbps): 16000
	HC60WFCR1 One-Channel Fisheye Double Panorama 4 PTZ	Frame rate (FPS): PAL 25/NTSC 30 I frame interval: PAL 50/NTSC 60 Bit rate (Kbps): 16000	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): 1200
	HC60WFCR1 One-Channel/ 1Fisheye+3PTZ Multi-Channel 1Fisheye+3PTZ/Fi sheye/1Fisheye+6 PTZ/Fisheye	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): 8000	Frame rate (FPS): PAL 25/NTSC 30 I frame interval: PAL 50/NTSC 60 Bit rate (Kbps): 12000

Connection Type	Camera	Main Stream	Sub Stream	Third Stream
HTTPS*	HC60WB5R2P/H C60WB5R5P/HC 60W35R4P/HC60 W35R2P/HC60W 45R2P/HC60W45 R4P	Frame rate (FPS): PAL 25/NTSC 30 I frame interval: PAL 50/NTSC 60 Bit rate (Kbps):16000	Frame rate (FPS): PAL 25/NTSC 30 I frame interval: PAL 50/NTSC 60 Bit rate (Kbps): 16000	Frame rate (FPS): PAL 25/NTSC 30 I frame interval: PAL 50/NTSC 60 Bit rate (Kbps): 16000
	HC60WFCR1 One-Channel Fisheye Double Panorama 4 PTZ	Frame rate (FPS): PAL 25/NTSC 30 I frame interval: PAL 50/NTSC 60 Bit rate (Kbps): 16000	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): 12000
	HC60WFCR1 One-Channel/ 1Fisheye+3PTZ Multi-Channel 1Fisheye+3PTZ/Fi sheye/1Fisheye+6 PTZ/Fisheye	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): 8000	Frame rate (FPS): PAL 25/NTSC 30 I frame interval: PAL 50/NTSC 60 Bit rate (Kbps): 12000

- Note:**
- For encryption under HTTPS.
 - If you need to enable functions that affect performance (such as VA, and SD card recording), it is recommended to reduce the corresponding parameter values instead of using the maximum parameter of the above table.
 - The image parameter will be set as the default value if the mode of the 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. Choose the custom, you can input the value ranges from 1 to 100 in the table.

I frame interval

Custom ^

50

[1-100]

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 a high compression level from MAXPRO NVR will result in low image quality in the camera.
 - Selecting a low compression level from MAXPRO NVR will result in high image

quality in the camera.

Smart Encode: Check the checkbox to enable Smart Encode.

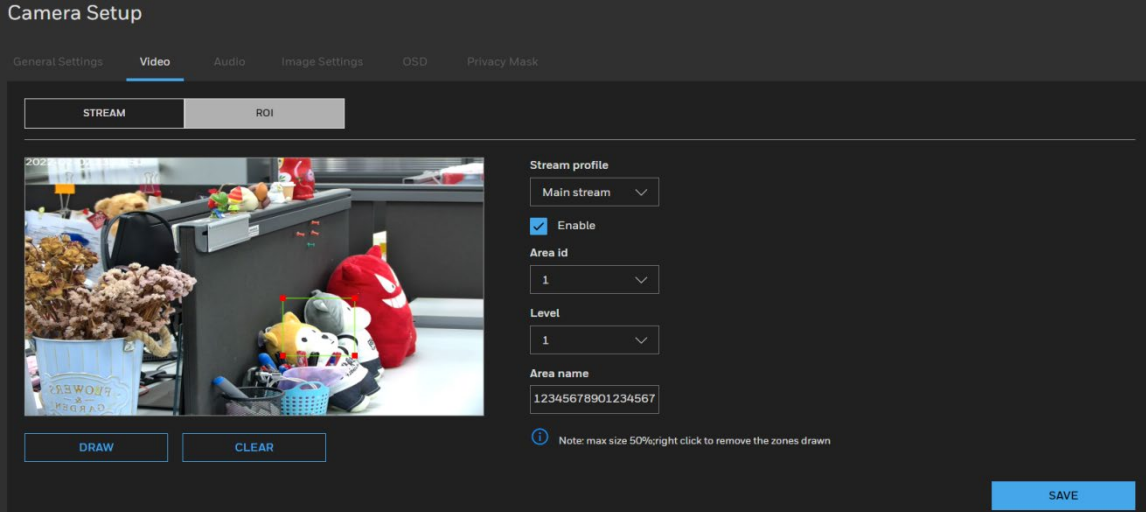
- Smart encode includes H.264 & H.265.
- The storage space will be reduced fifty percent when smart encode is enabled.
- Only mainstream supports smart encode.

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 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 17 ROI Settings



The screenshot shows the 'Camera Setup' window with the 'Video' tab selected. Under the 'Video' tab, the 'ROI' sub-tab is active. On the left, a live video feed shows a desk with various items, and a red rectangular ROI box is drawn over a portion of the desk. Below the video feed are 'DRAW' and 'CLEAR' buttons. On the right, the 'Stream profile' is set to 'Main stream'. The 'Enable' checkbox is checked. The 'Area id' is set to '1', and the 'Level' is set to '1'. The 'Area name' field contains the text '12345678901234567'. A note at the bottom right states: 'Note: max size 50%;right click to remove the zones drawn'. A 'SAVE' button is located at the bottom right of the settings panel.

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 the 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 be configured when the stream is selected as MJPEG or smart encode.*

Configuring Audio Settings

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

Figure 18 Audio Settings

The screenshot shows the 'AUDIO' settings page. At the top, there are two tabs: 'AUDIO' and 'AUDIO FILE'. Below the tabs, the page 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' dropdown menu is set to 'Line in'. The 'Audio input volume' slider is positioned at 50, with a range from 0 to 100%. The 'Audio encode type' dropdown menu is set to 'G711ALAW'. In the 'Audio Output Settings' section, the 'Audio output' checkbox is checked. Below it, the 'Audio output type' dropdown menu is set to 'External'. The 'Audio output volume' slider is positioned at 50, with a range from 0 to 100%. A blue 'SAVE' button is located in the bottom right corner of the settings area.

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**, **G711ULAW**, or **G726**.

Audio Output Settings

Audio output: Check the checkbox to enable Audio output.

Audio output type: Select the Line-out option.

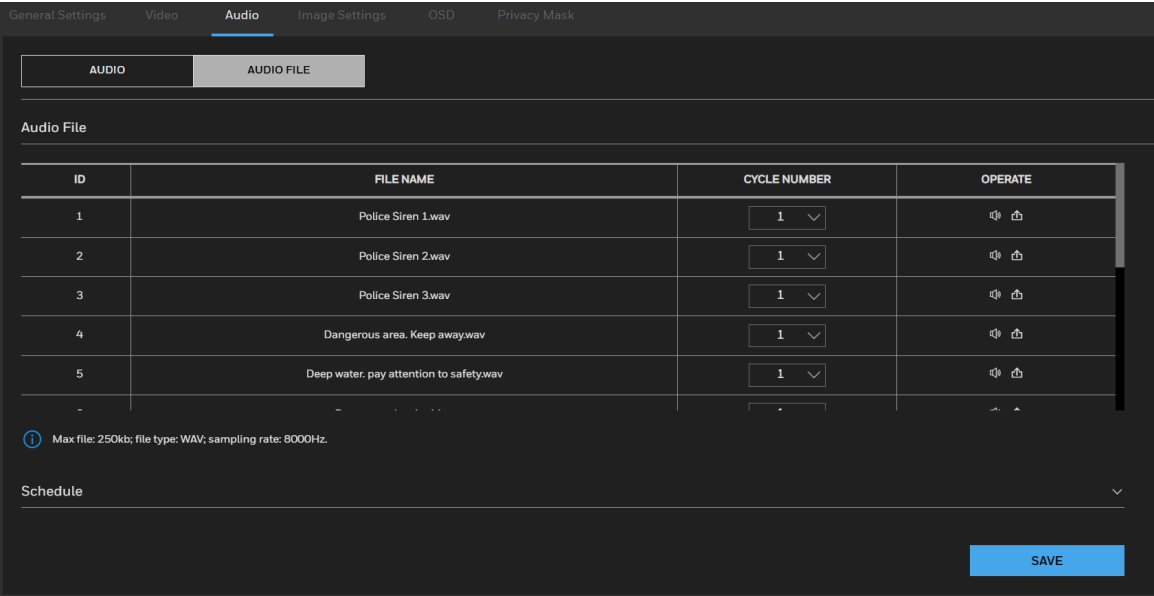
Audio output volume: The Line-out option is displayed according to the Audio output option selected. Select the volume of the external audio input according to ambient conditions. Adjust the volume from 0% (least) to 100% (most).

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 19 Audio File



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

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

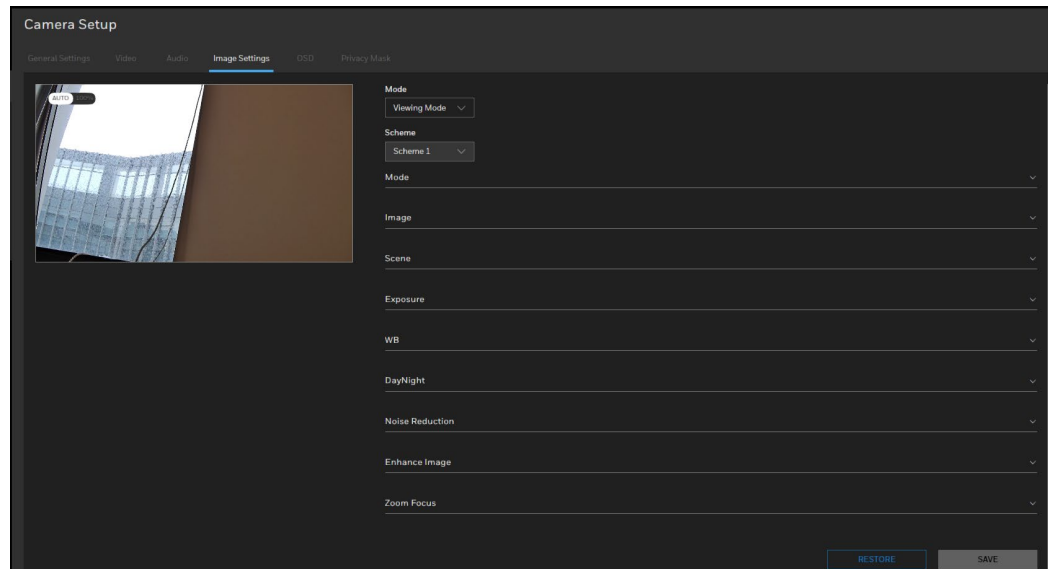
The file type should be WAV, the size must be less than 250 KB, and the sampling rate should be 8000HZ.

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 20 Image Settings



Auto: It shows all the images of the lens.

100%: It shows the section of the scene, drag the border bar to adjust.

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 editing mode, four schemes can be set, every scheme is independent, and you can set each one for different parameters for different scenes.

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 the 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

The 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 to get 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. The gain range will be under the maximum 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 the maximum value.

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

Max gain: The device automatically adjusts the gain based on the ambient light under the 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 the 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 the 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 to the ambient light changes, and it will unlock to Auto mode after 1 hour. Or you can change it to 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 detects 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 modes 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 HC60WB5R2P/HC60WB5R5P, 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 models HC60W35R2P and HC60W35R4P, you can set **Near/Far** IR light distance by **Manual** configuration.
- For other models' cameras, you can drag the slider to set the IR light strength manually.

Note: *For HC60WB5R2P/HC60WB5R5P, 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 the noise of the 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, suggesting to select a lower level of 3D Noise Reduction in this situation.*

All changes made to image settings are directly shown on the screen. To recall the original settings without incorporating the changes, click **RESTORE**. After you complete 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 the 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 environments and defog can be used to improve image clarity.

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 fixed camera models HC60WC5I.*

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

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

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

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

Note: *The lens configuration needs to be recovered When there are unexpected situations in which the lens configuration is messed up. It is not recommended to initialize the lens by yourself and if additional assistance is needed, please contact Honeywell Technical Support.*

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

Configuring OSD

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

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

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

Position: Set the OSD display position.

Font size: Set the font size of the OSD display.

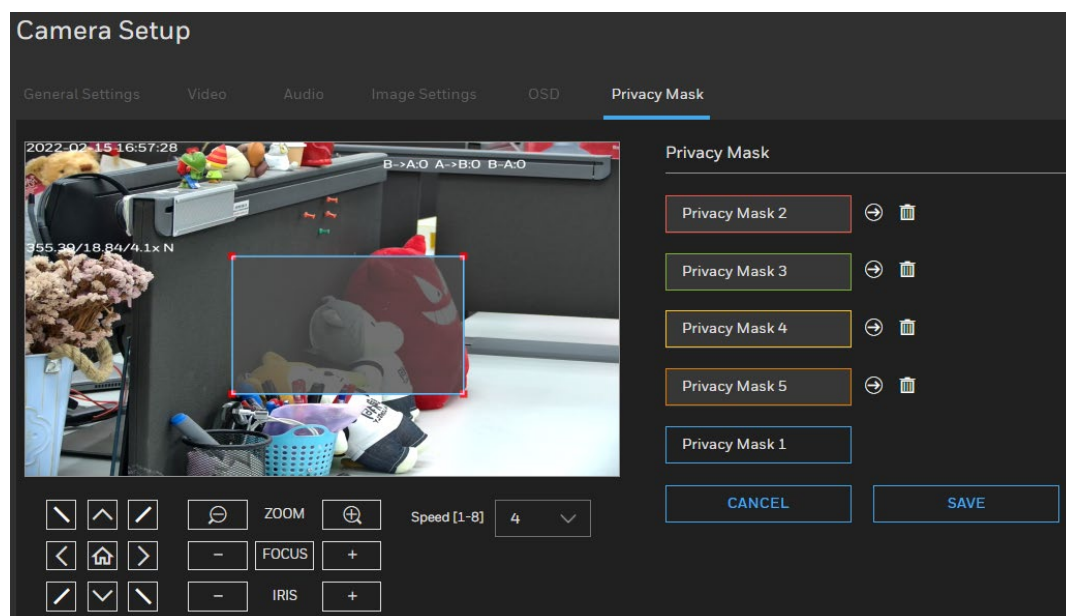
Configuring Privacy Mask

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 21 Privacy Mask



- Note:**
- The object should be in the middle of the video screen and the setting size of the privacy mask should be 1.5~2.5 times the object size.
 - Up to 4 privacy mask windows for IPC cameras can be configured on the same screen.
 - If you want to delete the privacy mask window, click  on the right side of the privacy mask window name. Click  to go to the related 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 22 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 the IP protocol.

When IPv4/IPv6 is enabled, by default, the network camera will listen to router advertisements and be assigned 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 settings will disable the transmission to destinations across different subnets.

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

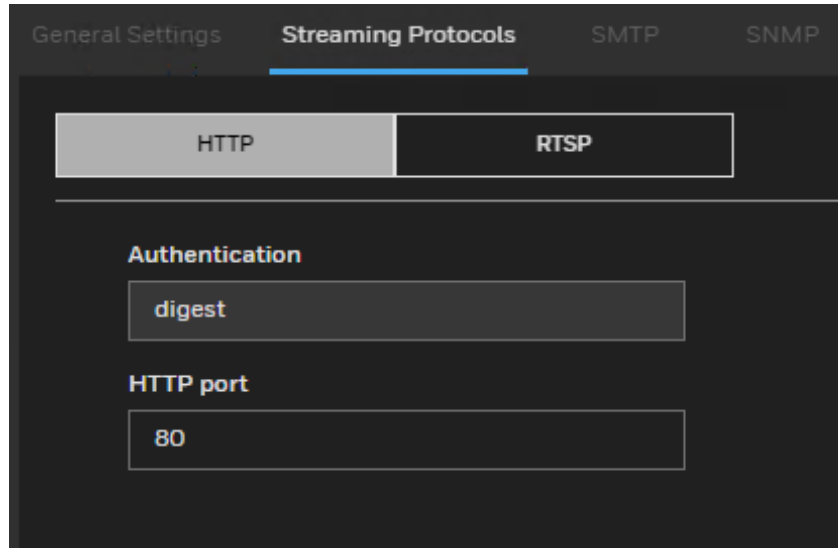
Alternate DNS Server: Secondary domain name server that backs up the Primary DNS.

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

Configuring Streaming Protocols

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

Figure 23 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 [104](#).

Authentication: User credentials are encrypted with MD5 algorithm which provides 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 24 Streaming Protocols-RTSP

The screenshot shows the 'Network Setup' interface with the 'Streaming Protocols' tab selected. Under this tab, the 'RTSP' sub-tab is active. The 'Authentication' dropdown is set to 'digest'. The 'RTP port for video' is set to '555', with a note below it stating 'The port changing will take effect after restart the device'. The 'RTSP port' is set to '554'. A large information box contains the following text: 'The port changing will take effect after restart the device', followed by three RTSP stream URLs for Main, Sub, and Third streams using the new port 554, and an 'Or' followed by the same three URLs using the default port 554. Below this, the 'RTCP port for video' is set to '556'. At the bottom, there are three expandable links: 'Multicast settings for Main Stream', 'Multicast settings for Sub Stream', and 'Multicast settings for Third Stream'.

To utilize RTSP streaming authentication, make sure that you have set a password for controlling the access to the video stream first. For more information, see [Configuring User Accounts Settings](#) on page 104.

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's 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 the 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's 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 the 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 the 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 25 SMTP Settings

Network Setup

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

SMTP

SMTP server address *

SMTP server port *
25 [1 ~ 65535]

User name *

Password *

Sender e-mail address1 *

Recipient e-mail address1 *

Recipient e-mail address2

Recipient e-mail address3

Recipient e-mail address4

Recipient e-mail address5

Transport mode
No Encrypt

Send interval
0 [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 that executes applications that monitor and control managed devices.
- **Agent:** A network-management software module on a managed device that 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 for accepting messages from the 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 the SNMP manager and agent.

Read security name: Name of read security.

Write security name: Name of write security.

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

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

Auth algorithm: The 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.

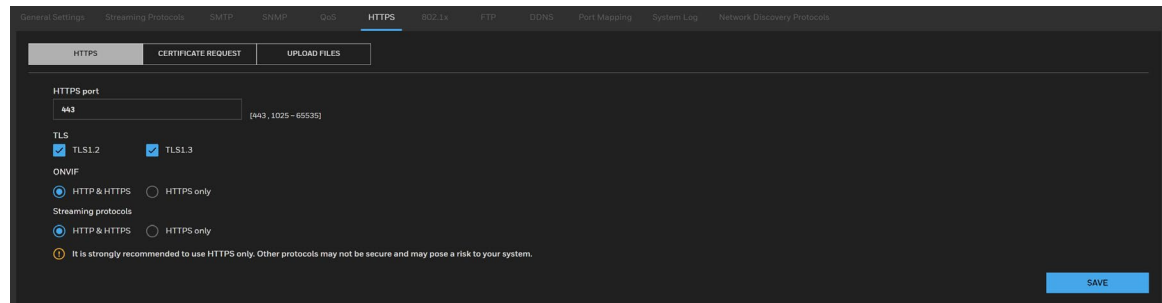
Configuring HTTPS Settings

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 a higher security level.

Figure 26 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 security requirements.

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

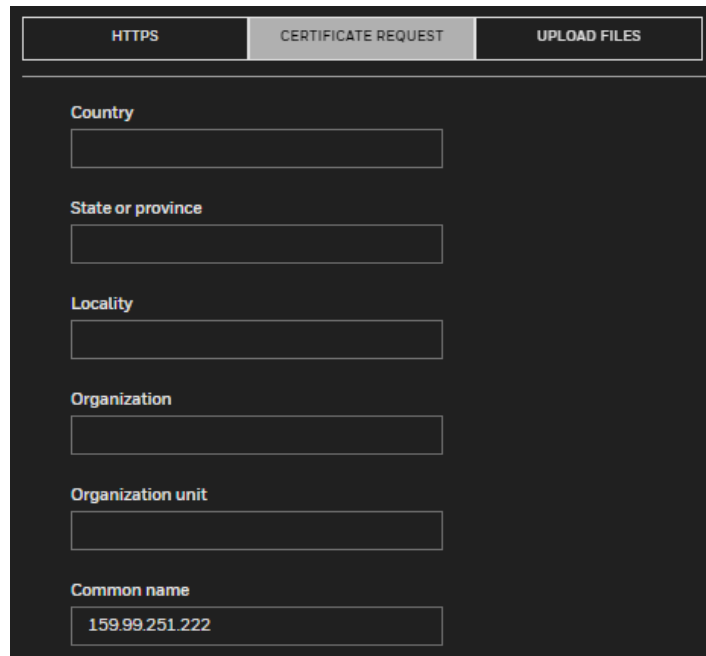
HTTP & HTTPS: Select it and the web browser can be accessed via HTTP or HTTPS.

HTTPS only: Select it and the web browser can only be accessed via HTTPS with a higher security level.

Certificate Request

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

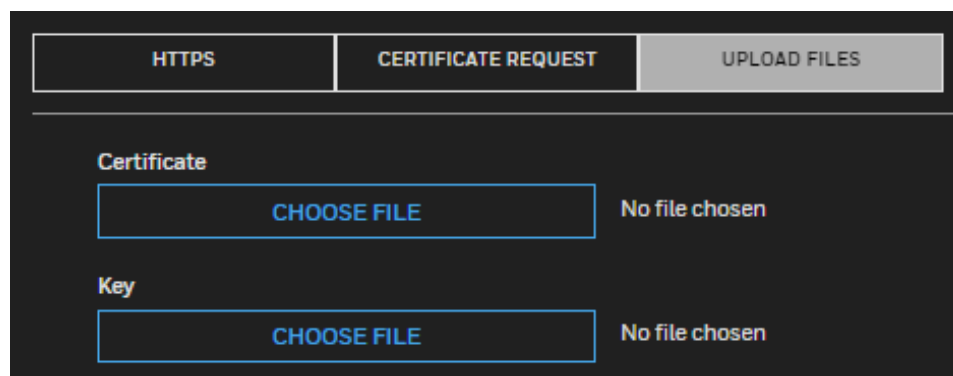
Figure 27 Certificate Request



The screenshot shows a web interface with three tabs: "HTTPS", "CERTIFICATE REQUEST", and "UPLOAD FILES". The "CERTIFICATE REQUEST" tab is active. Below the tabs, there are several input fields with labels: "Country", "State or province", "Locality", "Organization", "Organization unit", and "Common name". The "Common name" field contains the text "159.99.251.222".

Upload Files

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



The screenshot shows a web interface with three tabs: "HTTPS", "CERTIFICATE REQUEST", and "UPLOAD FILES". The "UPLOAD FILES" tab is active. Below the tabs, there are two sections: "Certificate" and "Key". Each section has a "CHOOSE FILE" button and a "No file chosen" status indicator.

To import the certificate from a 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 the 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

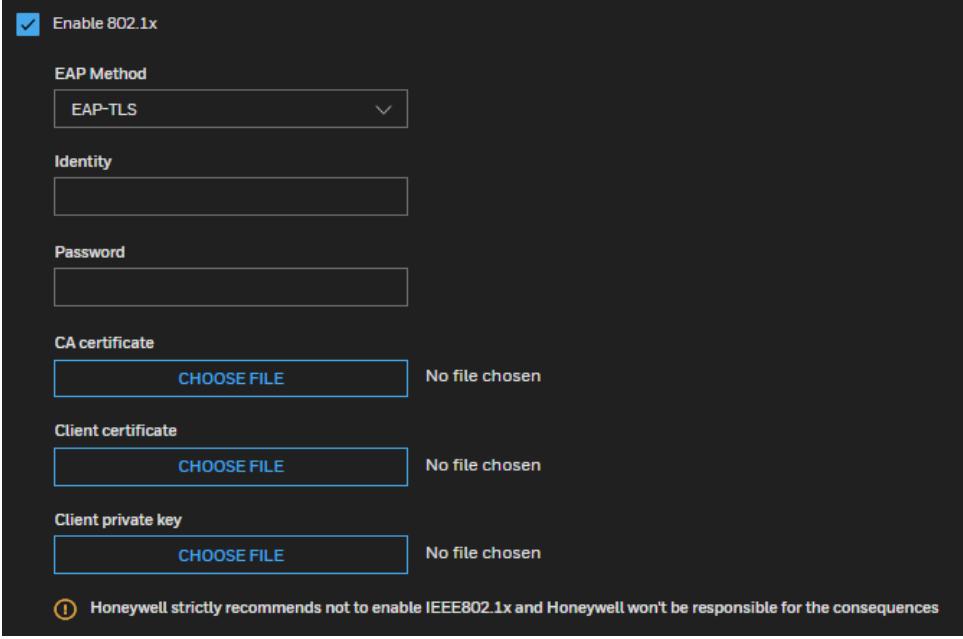
Go to **Setup > Network Setup > 802.1x**.

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 28 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 input fields for "Identity" and "Password". Below these are three sections for certificates and keys: "CA certificate", "Client certificate", and "Client private key". Each section has a "CHOOSE FILE" button and a status indicator "No file chosen". 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 the 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 for which you have an account in advance.

Figure 29 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, the default mode is SFTP.

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.

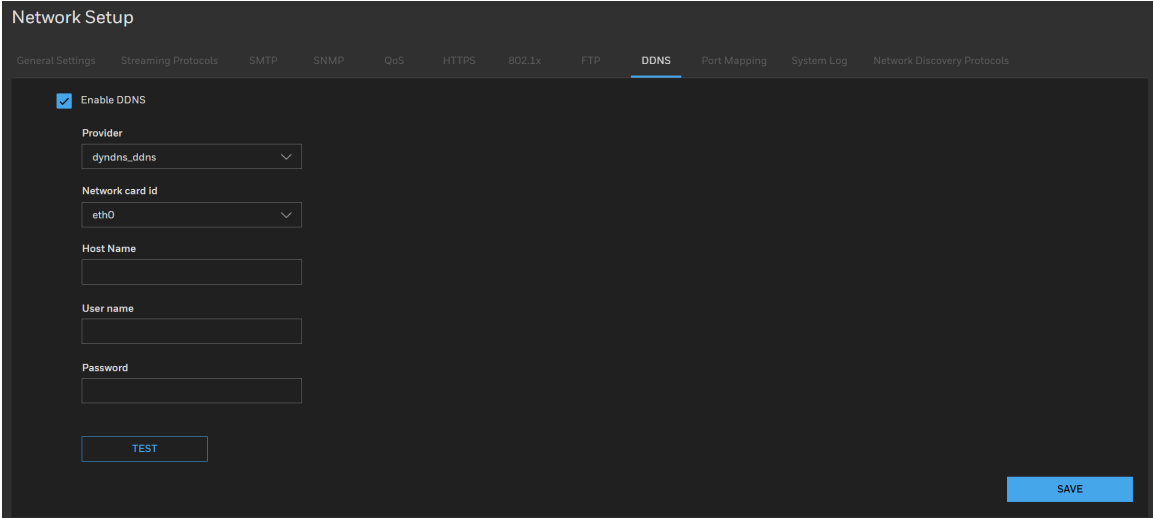
Configuring DDNS

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

1. Go to Setup > Network Setup > DDNS.

The DDNS interface is displayed.

Figure 30 DDNS Interface



The screenshot shows the 'Network Setup' window with the 'DDNS' tab selected. The 'Enable DDNS' checkbox is checked. Below it, there are several fields: 'Provider' (a dropdown menu showing 'dyndns_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.

2. Check Enable DDNS, choose the protocol from drop-down list, no-ip_ddns / auto_ddns / freedns_ddns / dynu_ddns.
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 31 Port Mapping Interface

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

2. Enable the function to start setting 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 another value, for example, 70, then you should enter 70 after the IP address when logging in to the Device by browser.
RTSP Port	RTSP (Real-Time Streaming Protocol), is 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 the 3rd-party system log server, so that the server can receive the system logs from the camera and view the logs.

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

Figure 32 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 contains the following options: 'Enable' (checked), 'Server address' (text input), 'Server port' (text input), 'Enable TLS' (checked), and 'Syslog Server certificate' (with a 'CHOOSE FILE' button and 'No file chosen' text). At the bottom right, there is a 'SAVE' button.

2. Configuring the System log, the 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 advance. 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 genpkey -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. The key is the private key 1 of 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 detailed command is:

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

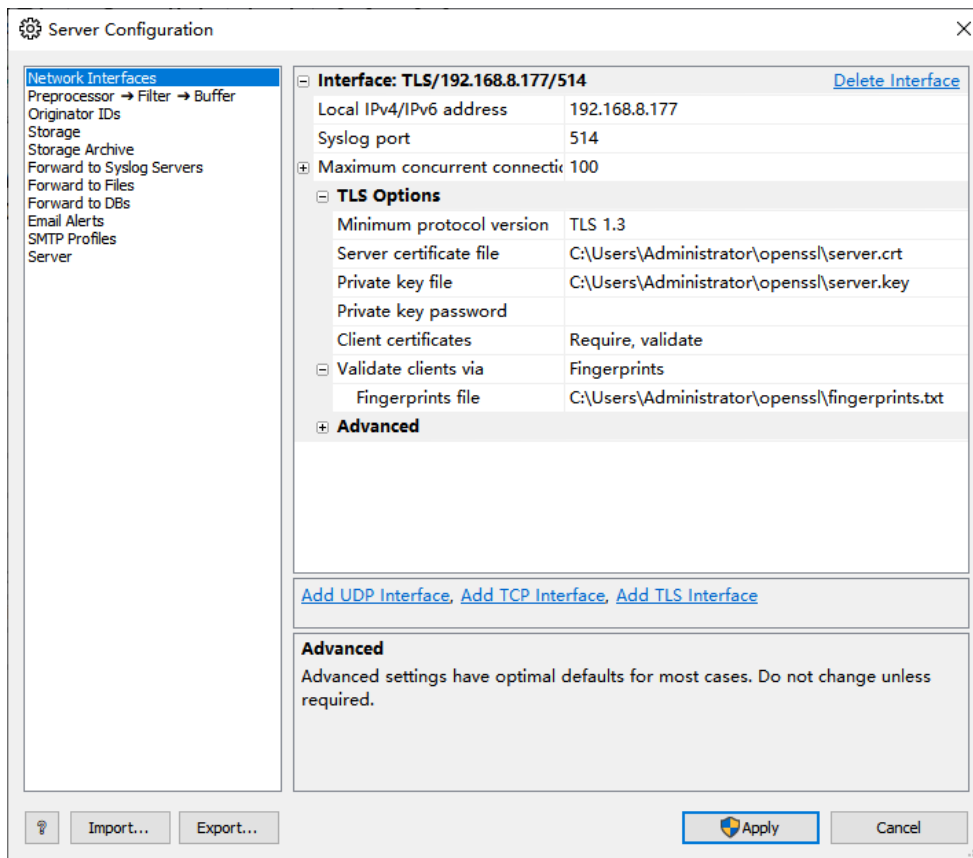
```

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

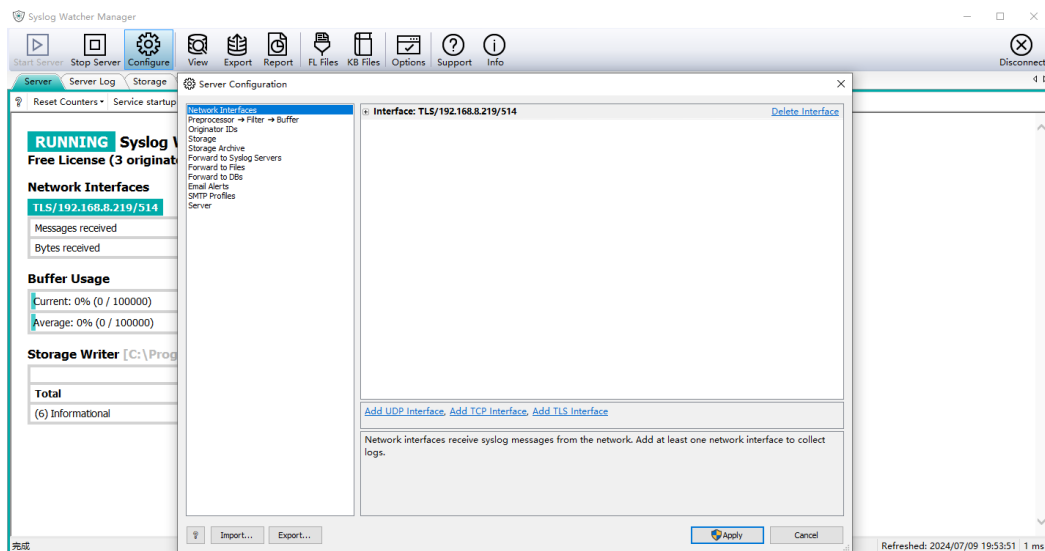
```

- g. Modify the fingerprint 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 above.



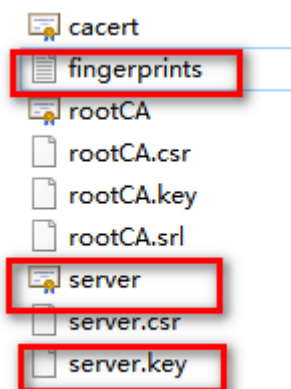
Network Interfaces

- 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
Private key password	
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 the 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

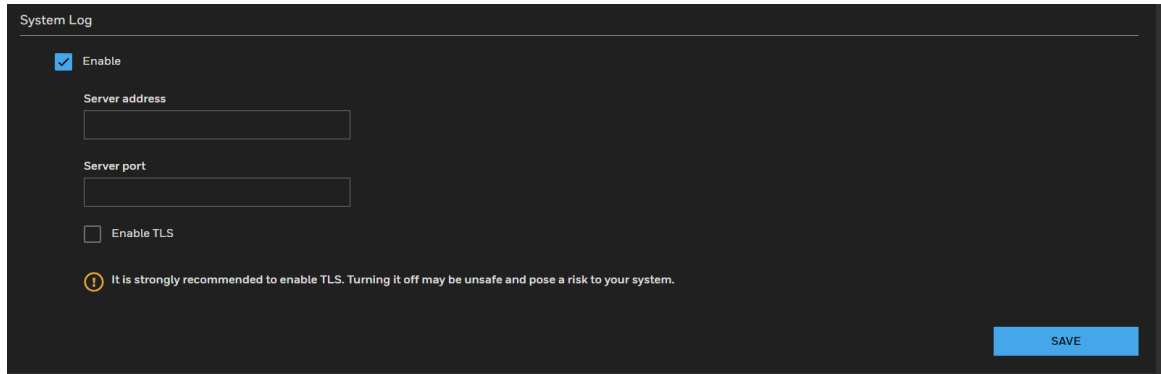
[UPLOAD](#)

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

succeed. Otherwise, it is failure, you should check the 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 is the IP of the computer that 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

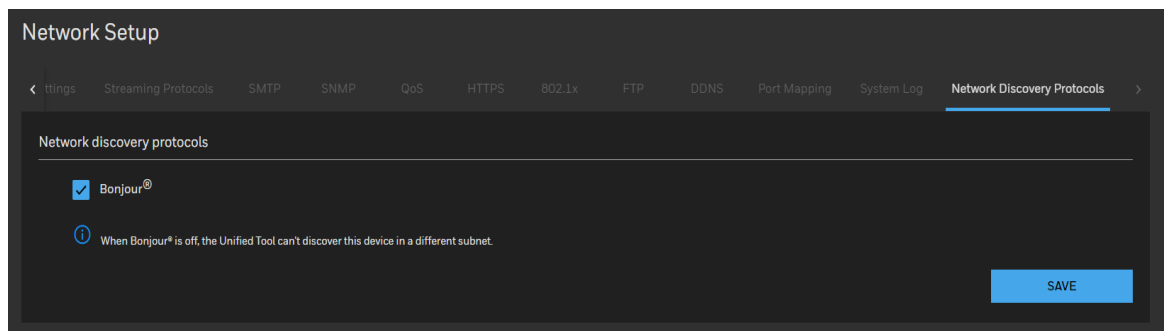
ⓘ It is strongly recommended to enable TLS. Turning it off may be unsafe and pose a risk to your system.

SAVE

Configuring Network Discovery Protocols

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

Figure 33 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 includes Package Management and Motion detection. The Package Management page shows the System Resource (Update information every 10 seconds) and Package Management.

The package management includes basic analytics and license plate detection. The basic analytics provides the following features, Smart motion, Scene change, Intrusion detection, Multi loitering detection, People counter, Face detection, Line crossing detection, Unattended object detection, Missing object detection, Heat map, and event & metadata scheme.

Note: *The basic analytics and license plate detection are incompatible, only one type can be enabled at the same time.
On the Video Analytics page, click Open VA User Guide to open the detailed guide for Video Analytics features.*

Figure 34 Video Analytics Interface

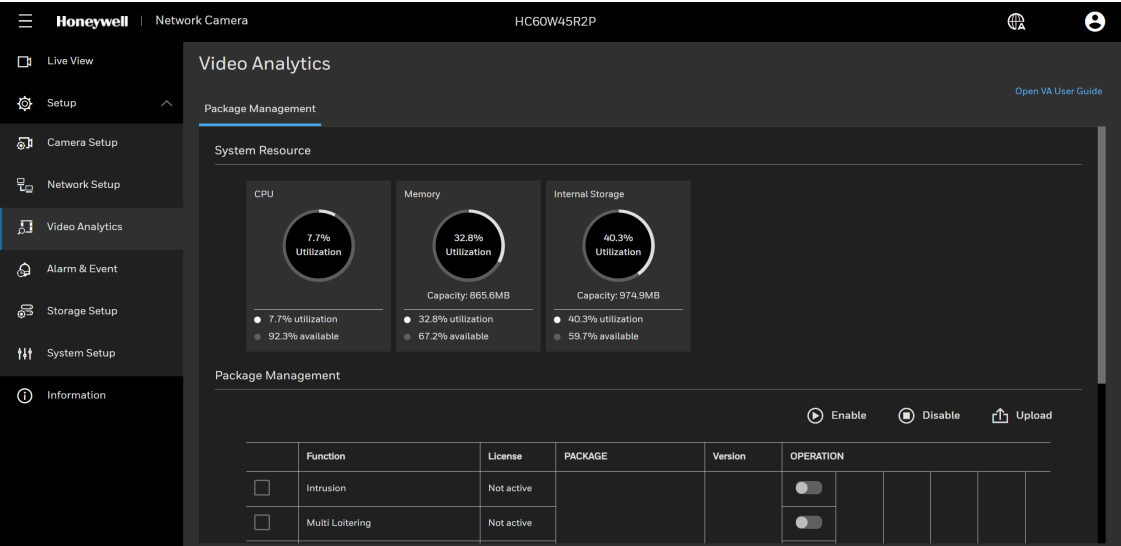
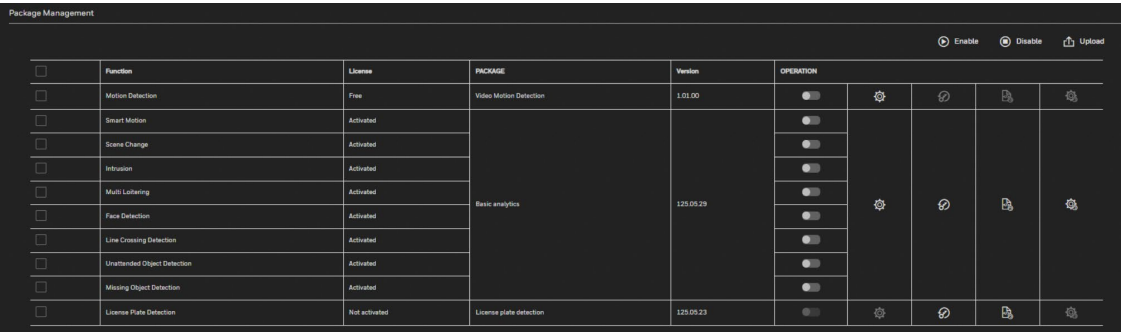


Figure 35 Package Management Interface



Enable: Enable the batch analytics action, tick some functions, click the icon to enable. The license plate detection and basic analytics cannot be enabled simultaneously.

Disable: Disable the batch analytics action.

Upload: Upload the algorithm software package, the package will be updated on Honeywell's website.

: Click to set the detailed information.

: License Activation. There are basic analytics and license plate detection license activation.

: Algorithm reset: click the button and the version of algorithm will be recovery to the factory version.

: Settings reset: click the button and the settings of VA will be reset.

Figure 36 License Activation

License Activation

Status

Basic analytics is not activated

Activation

Hardware ID: 006020145237 [COPY]

Activation code: []

[CLOSE] [ACTIVATE]

License Activation

Status

License plate detection is not activated

Activation

Hardware ID: 00A084805F01 [COPY]

Activation code: []

[CLOSE] [ACTIVATED]

Activation will turn off other algorithms.

The Hardware ID is the MAC address of the camera, the activation code please connect with **Honeywell**. Input the activation code, and click **ACTIVATED** to activate the algorithm.

Note: *On the Video Analytics page, click Open VA User Guide to open the detailed guide for Video Analytics features.
The supported VA function list may be different for each SKU. Please find the supported VA function list in the datasheet for each SKU.*

Object Analytics

For cameras: HC60WB5R2P/ HC60WB5R5P/ HC60W35R4P/ HC60W35R2P/ HC60W45R2P/ HC60W45R4P, support to recognize the target attribute as car/ gender/ masking/ age/ colors of car.

Car: Car/ Truck/ Motorcycle/ Bus.

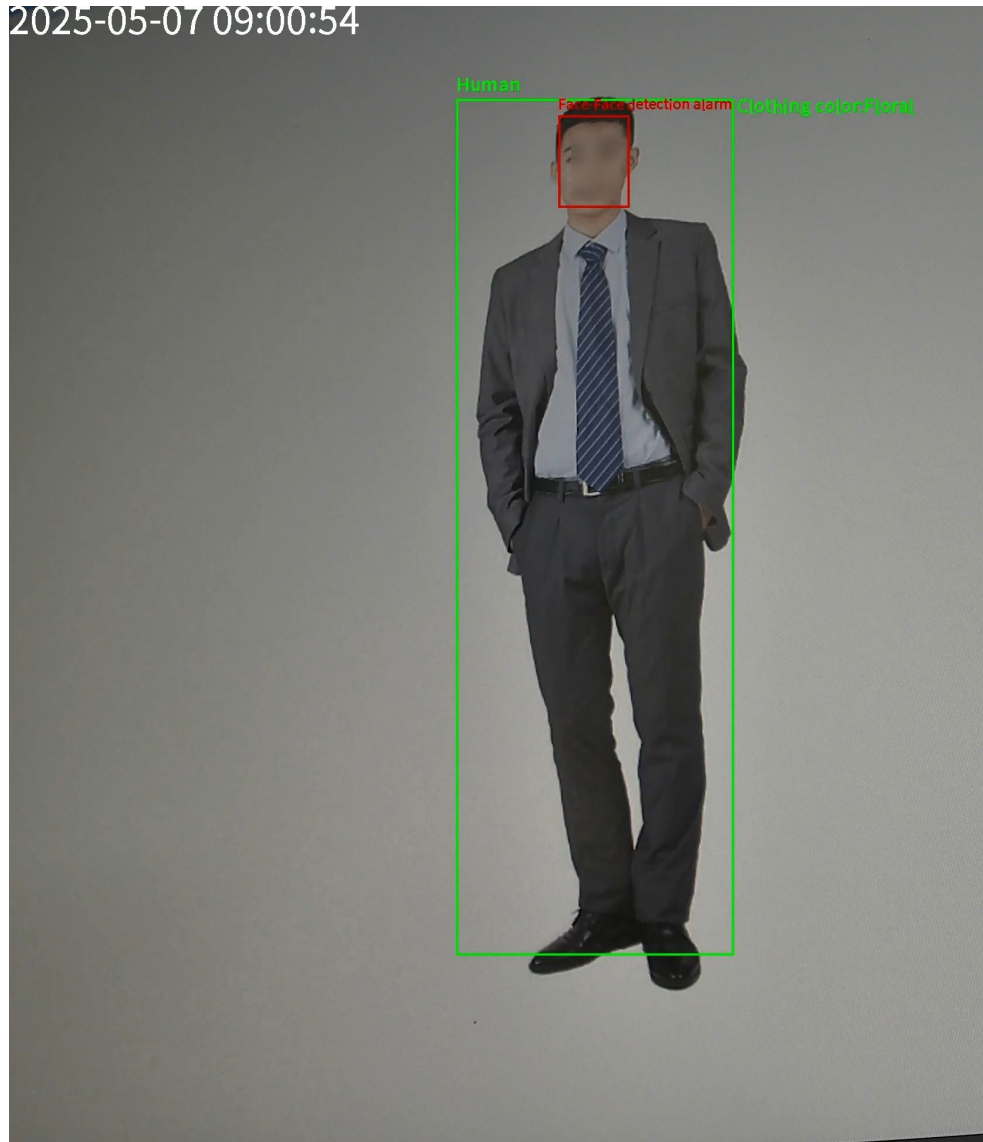
Gender: Male/ Female.

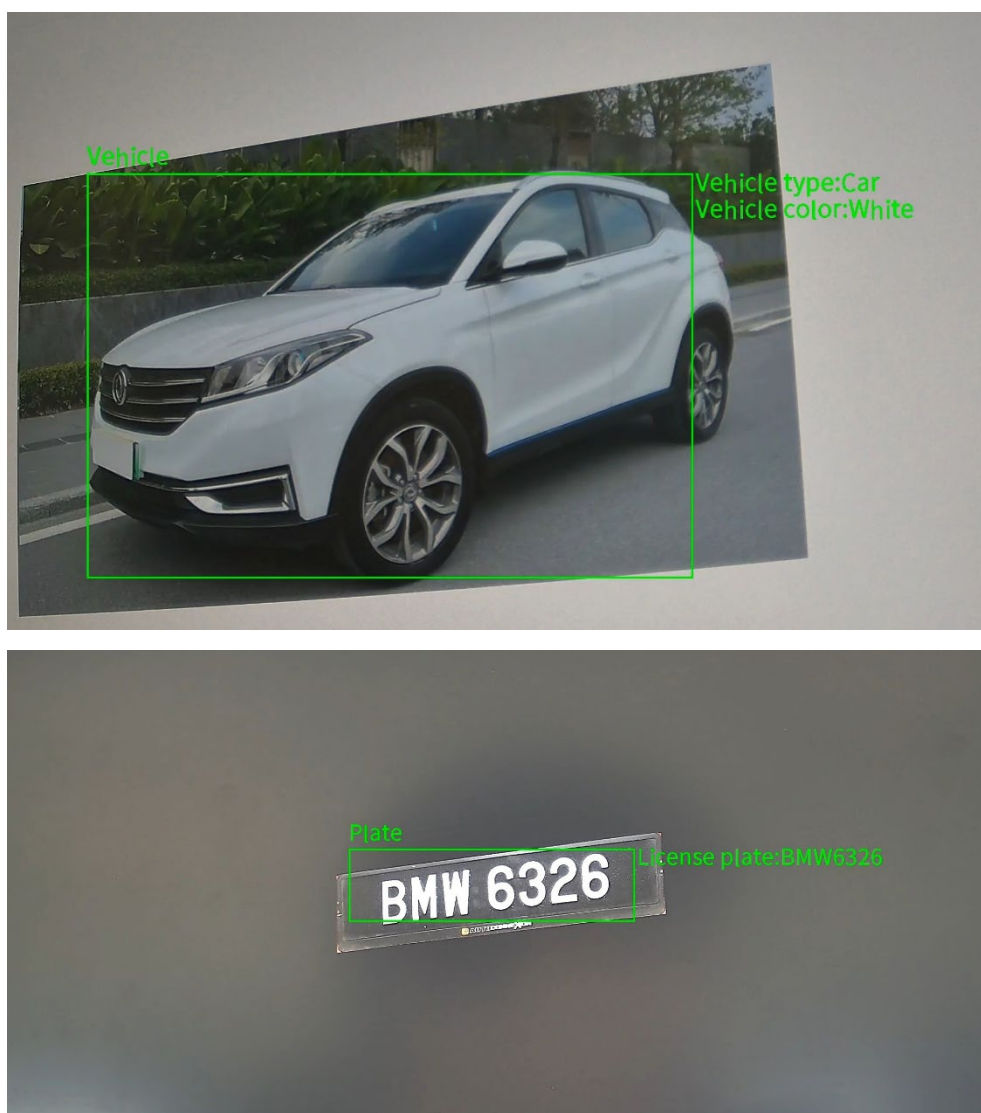
Masking: Wearing / Not wearing.

Age: Young/ Adult/ Middle Age/ Senior.

Colors of car or personal clothing: Blue/ Yellow/ Black/ White/ Green/ Red/ Gray/ Purple/ Pink /Brown /Teal / Colorful / Beige/ Gold/ Orange/ Silvery/ Floral.

2025-05-07 09:00:54





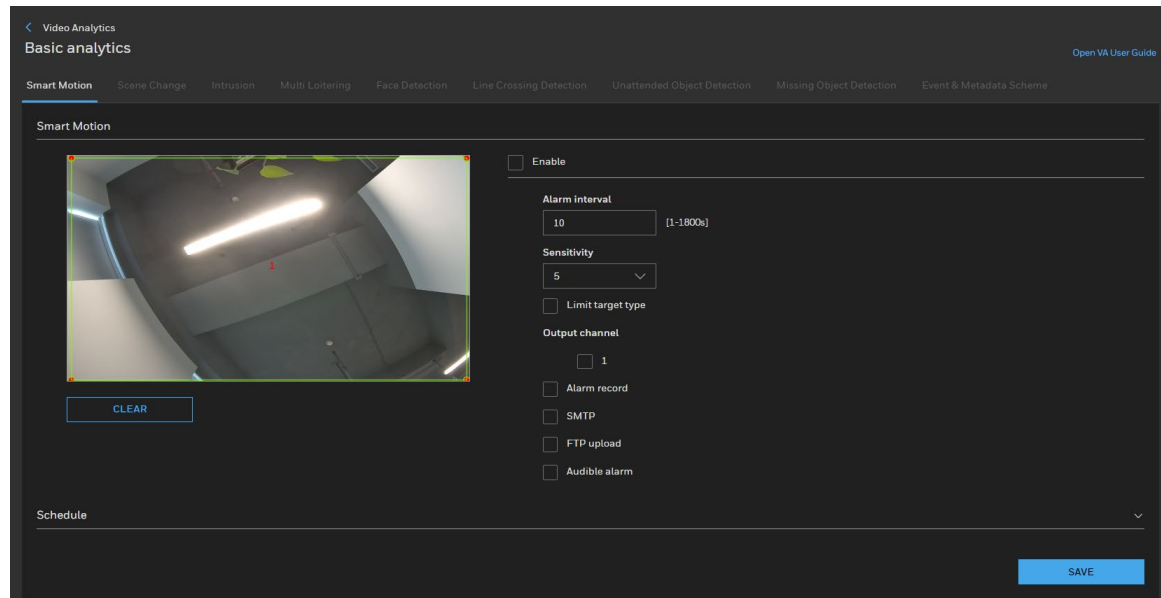
Smart Motion

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 vehicle) in the setting area. The applicable scenario to detect objects (humans or vehicles by selecting **Limit target type**) is in a restricted area.

Go to **Setup > Video Analytics > Smart Motion**. Set the parameters of smart detection.

Figure 37 Smart Motion



Enable: Check the checkbox to enable the **Smart Motion**.

Alarm interval: It will only send one alarm during the configured interval time.

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 motion will be detected. But it may trigger some false alarms.

For example, 5 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.

Limit target type: Check the checkbox to enable Limit target type and choose the type from the pull-down list: Human / Vehicle / All types.

Output channel: Check the checkbox to enable Output channel.

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

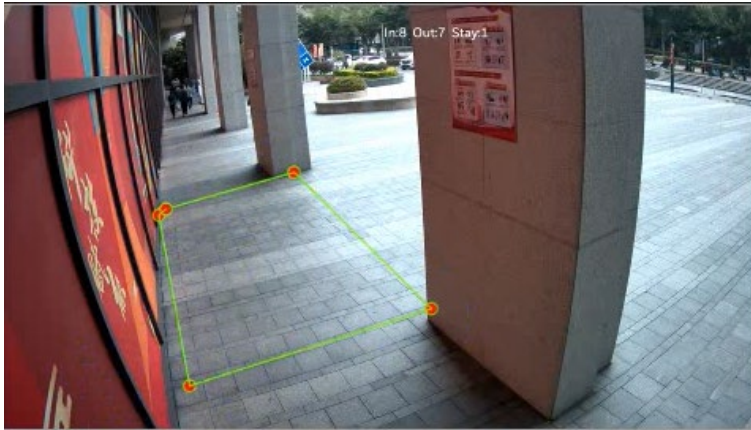
SMTP: Check the checkbox to enable the linkage action for sending snapshot and alarm notice information to the email address which can be set in **Network Setup > SMTP**, so the user can receive the alarm timely.

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

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

Left-click on the live view to start drawing the polygon and right-click to end setting the smart detection areas. You can set several areas to detect.

Figure 38 Set A Detection Area



CLEAR: Clear the area of the setting. Use the mouse to left-click on the screen to start drawing the polygon and right-click to end setting the smart detection areas, you can set several areas to detect.

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

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** to save the settings.

Scene Change

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

Figure 39 Scene Change

The screenshot shows the 'Scene Change' configuration page in the Honeywell 60 Series Cameras User Guide. The page is titled 'Scene Change' and is part of the 'Basic analytics' section. It features a video preview on the left and configuration options on the right. The configuration options include a checkbox for 'Enable scene change', an 'Alarm interval' field set to 10 (with a range of 1-1800s), a 'Sensitivity' dropdown menu set to 5, an 'Output channel' checkbox, and several alarm action checkboxes: 'Alarm record', 'SMTP', 'FTP upload', and 'Audible alarm'. A 'Schedule' section is visible at the bottom, and a 'SAVE' button is located in the bottom right corner.

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

Alarm interval: It will only send one alarm during the configured interval time.

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 motion will be detected. But it may trigger some false alarms.

For example, 5 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.

Output channel: Check the checkbox to enable Output channel.

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

SMTP: Check the checkbox to enable the linkage action for sending snapshot and alarm notice information to the 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 the FTP server when the alarm happens if you select the FTP upload box.

Audible alarm: It will play the audio file to alarm when the alarm happens if you select the Audio alarm box. 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** to save the settings.

Intrusion Detection

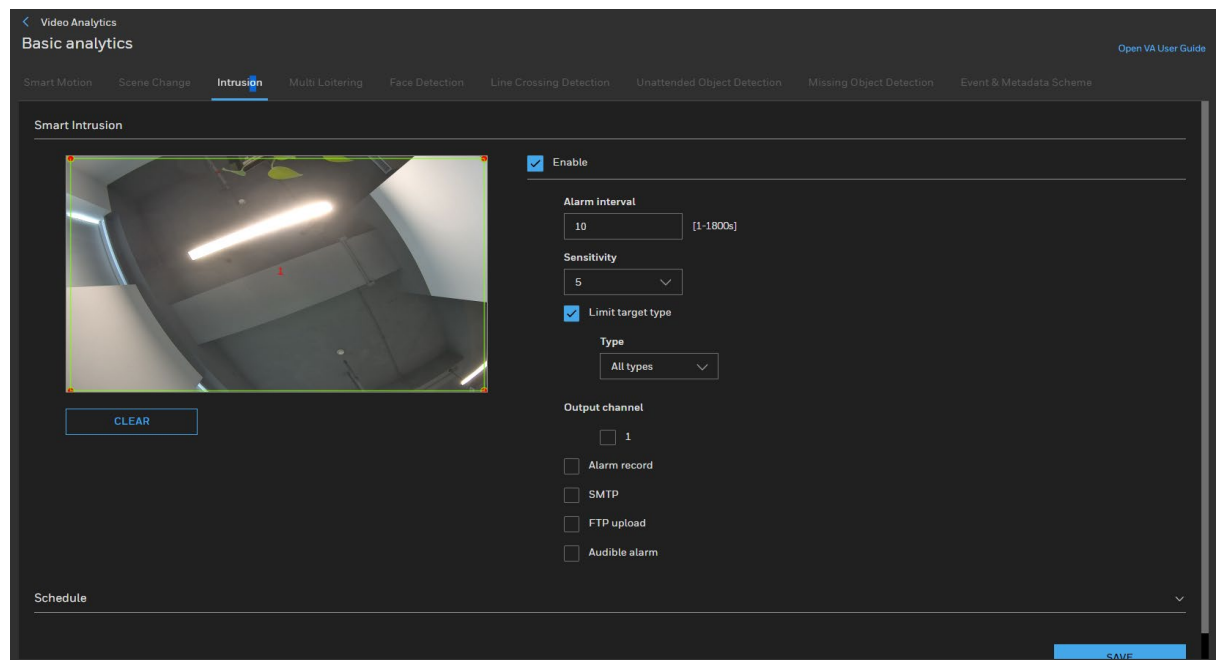
Intrusion Detection can be used to detect people entering or leaving a virtual area in the camera field of view.

The applicable scenarios of this feature can be:

- Detects when a person enters a bank vault or school after office hours.
- Detects when a person leaves an emergency exit fire escape, or any place that is normally forbidden from access.

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

Figure 40 Intrusion Detection



Enable: Check the checkbox to enable the Intrusion detection.

Alarm interval: It will only send one alarm during the configured interval time.

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 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.

Limit target type: Check the checkbox to enable Limit target type and choose the type from the pull-down list: Human / Vehicle / All types.

Output channel: Check the checkbox to enable Output channel.

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

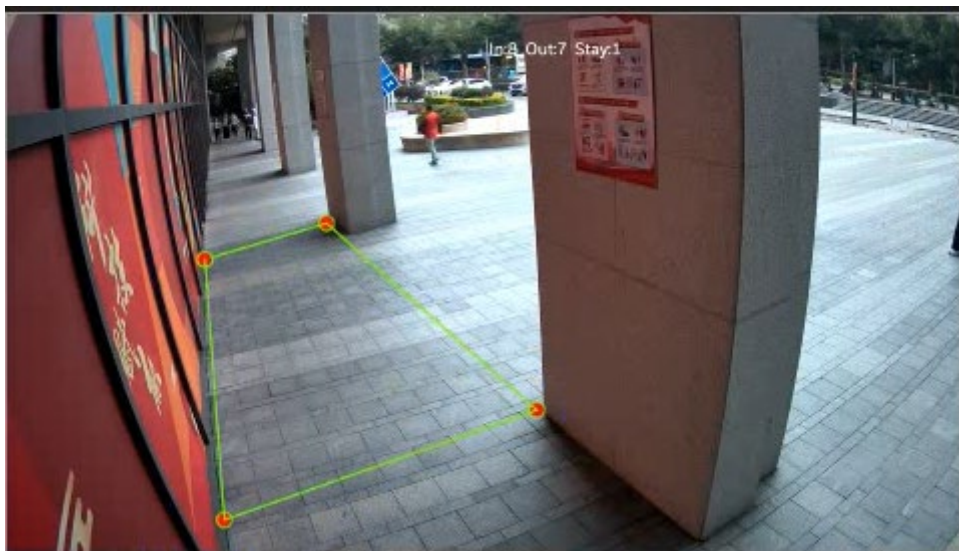
SMTP: Check the checkbox to enable the linkage action for sending snapshot and alarm notice information to the email address which can be set in **Network Setup > SMTP**, so the user can receive the alarm timely.

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

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

Left-click on the live view to start drawing the polygon and right-click to end setting the smart detection areas, you can set several areas to detect.

Figure 41 Set Intrusion Area



CLEAR: Clear the area of the setting. Use the mouse to left-click on the screen to start drawing the polygon and right-click to end setting the smart detection areas, you can set several areas to detect.

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

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** to save the settings.

Multi Loitering Detection

The Multi Loitering detection can be used to detect a group of people 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 or some human are loitering in an area that is normally not accessible to visitors.

Go to **Setup > Video Analytics > Multi Loitering**. Set the parameters of multi loitering.

Figure 42 Multi Loitering

The screenshot displays the 'Multi Loitering' configuration page within a video analytics software. The top navigation bar includes 'Video Analytics' and 'Basic analytics'. The 'Multi Loitering' tab is selected. The interface is divided into two main sections: a video preview on the left and a configuration panel on the right. The video preview shows a camera feed of an interior space with a 'CLEAR' button below it. The configuration panel includes an 'Enable' checkbox, an 'Alarm interval' dropdown set to '10' with a range of '[1-1800s]', a 'Max allowed time in the area (s)' dropdown set to '10' with a range of '[5-60s]', an 'Output channel' dropdown set to '1', and checkboxes for 'Alarm record', 'SMTP', 'FTP upload', and 'Audible alarm'. A 'SAVE' button is located at the bottom right of the configuration panel.

Enable: Check the checkbox to enable the multi loitering detection.

Max allowed time in the area (s): Set the max allowed time that people can loiter in the area. When the number of people is more than the number and the time is more than the preset shortest time, it will send an alarm.

Note: For HC60WB5R2P /HC60WB5R5P /HC60W35R4P /HC60W35R2P /HC60W45R2P /HC60W45R4P, the max allowed time in the area function does not apply to these models.

Output channel: If the alarm out cable is connected to the external device such as a buzzer.

Alarm interval: It will only send one alarm during the configured interval time.

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 motion will be detected. But it may trigger some false alarms.

For example, 5 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.

Output channel: Check the checkbox to enable Output channel.

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

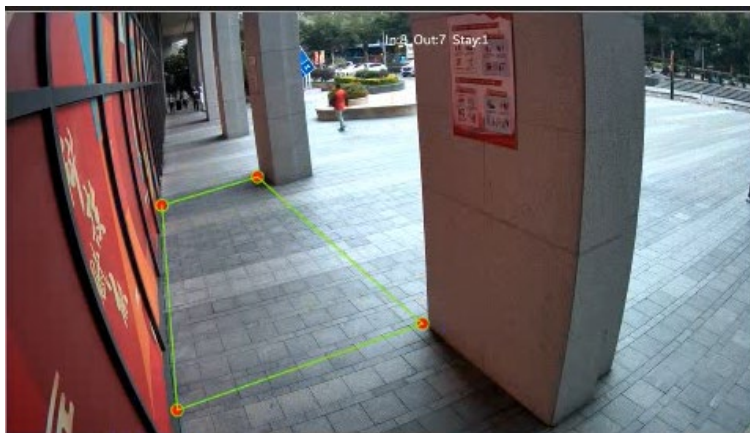
SMTP: Check the checkbox to enable the linkage action for sending snapshot and alarm notice information to the email address which can be set in **Network Setup > SMTP**, so the user can receive the alarm timely.

FTP upload: It will send 8 alarm pictures to the FTP server when an alarm happens if you select the FTP upload box.

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

Left-click on the live view to start drawing the polygon and right-click to end setting the smart detection areas, you can set several areas to detect.

Figure 43 Set Multi Loitering Area



CLEAR: Clear the area of the setting. Use the mouse to left-click on the screen to start drawing polygon and right-click to end setting the smart detection areas, you can set several areas to detect.

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** to save the settings.

Face Detection

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

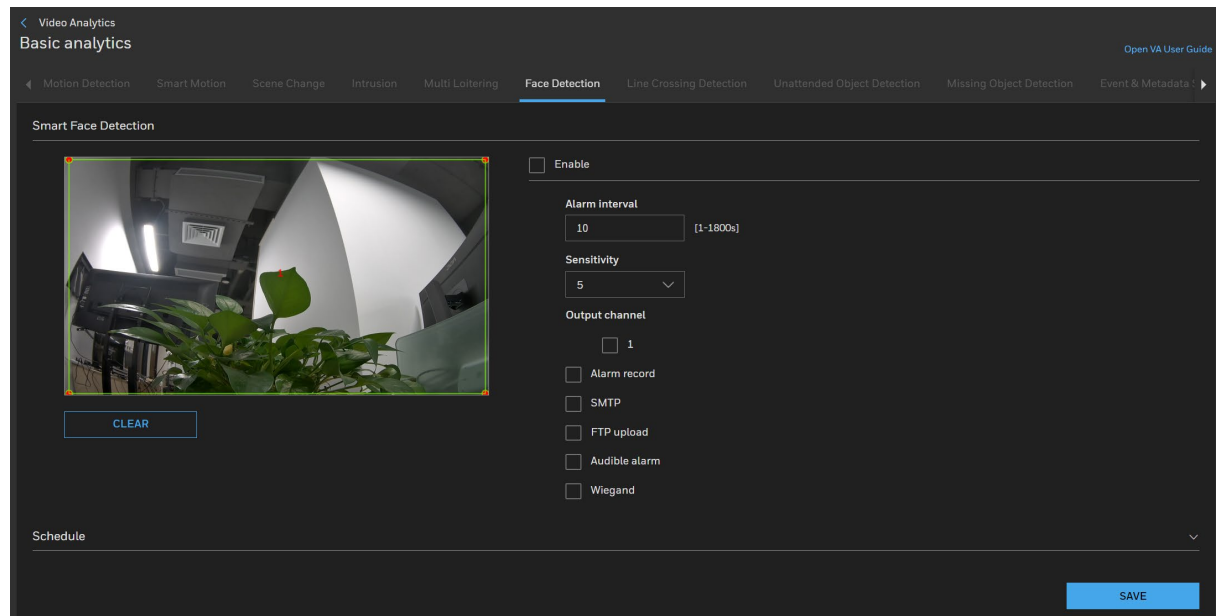
The applicable scenarios of this feature can be:

- Few people are crossing the concerned area, there are warnings for owners.

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 the installation is too low, or the head is too large (people should have a movement track, not too large for the 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 44 Face Detection



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

Enable: Check the checkbox to enable face detection.

Alarm interval: It will only send one alarm during the configured interval time.

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 motion will be detected. But it may trigger some false alarms.

For example, 5 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.

Output channel: Check the checkbox to enable Output channel.

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

SMTP: Check the checkbox to enable the linkage action for sending snapshot and alarm notice information to the 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 the FTP server when an alarm happens if you select the FTP upload box.

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

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

Click **SAVE** to save the settings.

People Counter

Note: *This feature is only applicable for model HC60WFCR1*

Settings

The 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, to implement

statistical requirements for the number of people in the area, and to 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 the installation is too low, or the head is too large (people should have a movement track, not too large for the 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 45](#).

Figure 45 View of Facing the Flow of People



- The camera is facing the sideways direction of the flow of people, as shown in [Figure 46](#).

Figure 46 Facing the Side Way Flow of People

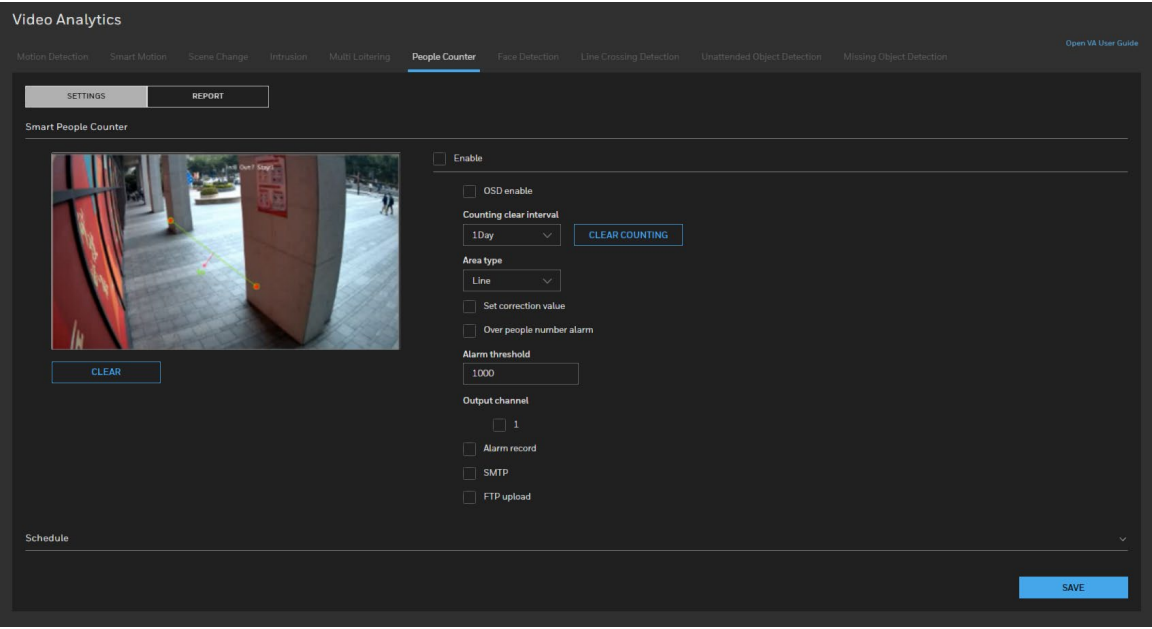


It is recommended to use the people counter function in the situations below:

- 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 should be at least 2s for the target movement track.

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

Figure 47 People Counter



Enable: Check the checkbox to enable the people counter.

Alarm interval: It will only send one alarm during the configured interval time.

OSD enable: Check the OSD enable checkbox to enable the OSD display of people counters. The data of out and in will be shown 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 the 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 48 Line of People Counter

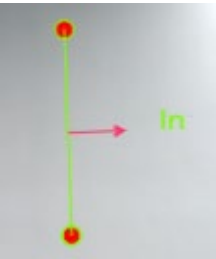
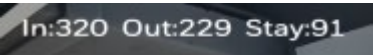


Figure 49 Number for In / Out / Stay



The **In** means people cross the line into the area. Going 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 plus the correction value.*

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

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

Output channel: Check the checkbox to enable Output channel.

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

SMTP: Check the checkbox to enable the linkage action for sending snapshot and alarm notice information to the 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 the FTP server when an alarm happens if you select the FTP upload box.

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

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

Report

Go to **Setup > Video Analytics > People Counter > REPORT**. Report the statistics of People Counter.

Figure 50 People Counter-REPORT

SETTINGS REPORT

Search

Statistical type

YEAR MONTH DAY

Date

10/16/2023

Flow direction

☒ In ☒ Out ☐ Display number

Report type

☒ Bar chart ☐ Line chart

SEARCH EXPORT

Search Results

Statistical type: choose the type of statistic to report, **YEAR / MONTH / DAY**.

Date: choose the detailed time from the calendar to report.

Flow direction: choose the flow direction to report statistics, **In / Out / Display number**.

Report type: two types can be chosen, **Bar chart / Line chart**.

Users can search the statistics or export the results to the local folder. The search results can be shown on the page directly.

SEARCH: click the search button, and the search results based on the search criteria will be displayed in the Search Results area.

EXPORT: support click the EXPORT button to export the people counter data.

Line Crossing Detection

Line Crossing Detection is a line that is set 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 human / vehicle) cross this line.

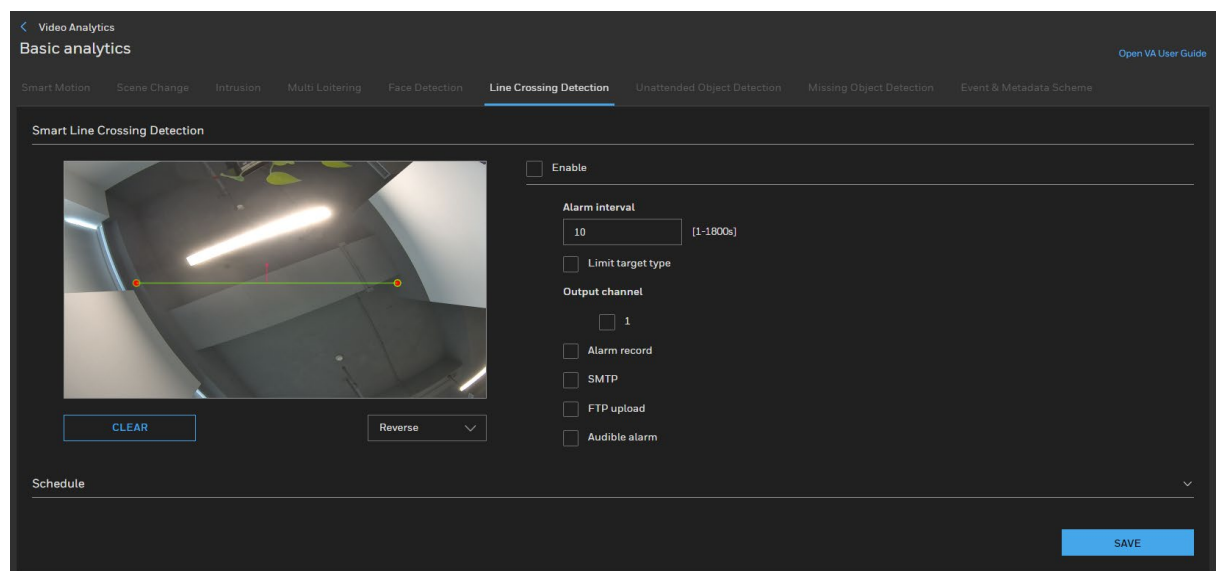
The applicable scenarios of this feature can be:

- There are specific scenes that forbid persons/vehicles from 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 the installation is too low or the head is too large (people should have a movement track, not too large for the 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 51 Single Line Crossing



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.

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.

Alarm interval: It will only send one alarm during the configured interval time.

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 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.

Limit target type: Check the checkbox to enable Limit target type and choose the type from the pull-down list: Human / Vehicle / All types.

Output channel: Check the checkbox to enable Output channel.

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

SMTP: Check the checkbox to enable the linkage action for sending snapshot and alarm notice information to the 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 the FTP server when an alarm happens if you select the FTP upload box.

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

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

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

Click **SAVE** to save the settings.

Unattended Object Detection

The Unattended Object Detection function refers to an alarm 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:

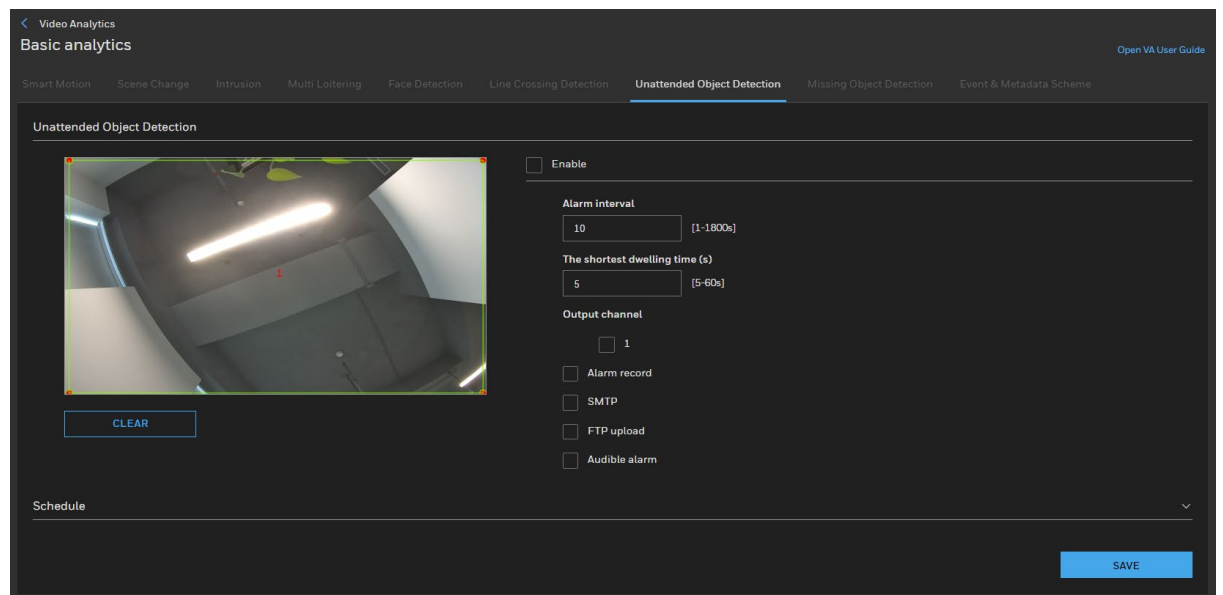
- Object Detection is used to detect some objects that appeared in the concern area and were not displayed in view before, such as bags, chairs, and so on.

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 the installation is too low, or the head is too large (people should have a movement track, not too large for the 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 52 Unattended Object Detection



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

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

Shortest Dwelling Time: The number must be from 5 to 60, in seconds.

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

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

SMTP: Check the checkbox to enable the linkage action for sending snapshot and alarm notice information to the 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 the FTP server when an alarm happens if you select the FTP upload box.

Audible alarm: It will play the audio file to alarm when the alarm happens if you select 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.

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

Click **SAVE** to save the settings.

Missing Object Detection

The Missing Object Detection function refers to an alarm 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 detect some objects disappeared in the concerned 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 the installation is too low or the head is too large (people should have a movement track, not too large for the 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 53 Missing Object Detection

The screenshot shows the 'Missing Object Detection' configuration page. On the left, there is a video preview window showing a person walking, with a red dot indicating the detection point. Below the preview is a 'CLEAR' button. On the right, there are several settings: an 'Enable' checkbox, an 'Alarm interval' set to 10 (range [1-1800s]), 'The shortest missing time (s)' set to 5 (range [5-60s]), and an 'Output channel' section with checkboxes for '1', 'Alarm record', 'SMTP', 'FTP upload', and 'Audible alarm'. At the bottom right is a 'SAVE' button.

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

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

Shortest Dwelling Time: The number must be from 5 to 60, in seconds.

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

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

SMTP: Check the checkbox to enable the linkage action for sending snapshot and alarm notice information to the 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 the FTP server when an alarm happens if you select the FTP upload box.

Audible alarm: It will play the audio file to alarm when the alarm happens if you select 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.

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

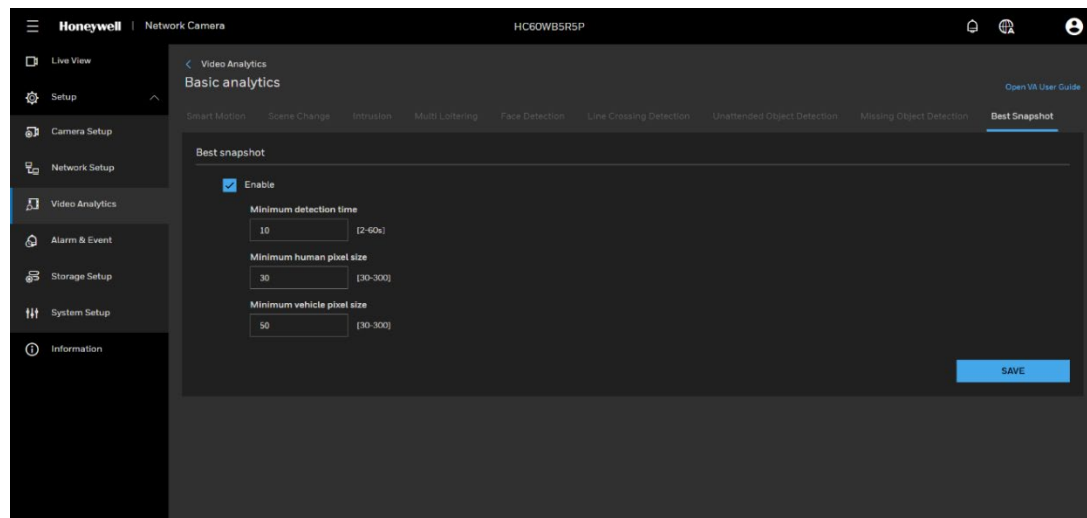
Schedule: Use the mouse to drag the time, or click the time grid to choose time one hour by hour. The blue means armed and the gray means unarmed.

Click **SAVE** to save the settings.

Best Snapshot

The best snapshot is for all basic analytics setting. This feature captures the best still cuts of the classified objects (Humans and Vehicles). Enable to set the following parameters.

Figure 54 Best Snapshot Set



Minimum detection time: The object enters the detection area for more than the minimum set time.

Minimum human pixel size: If the height pixel size of the human body exceeds this minimum size, the object can be photographed.

Minimum vehicle pixel size: If the height pixel size of the vehicle exceeds this minimum size, the object can be captured.

The object needs to conform to the set time and size, the camera will choose the best one to display during the start time to the leaving time.

The object needs to conform to the set time and size, and the camera will select the best one to display during the start time and the departure time.

Note: *This feature is only applicable for Milestone with Honeywell Plugin.*

Heat Map

Note: *The heat map function is only applicable for HC60WFCR1.*

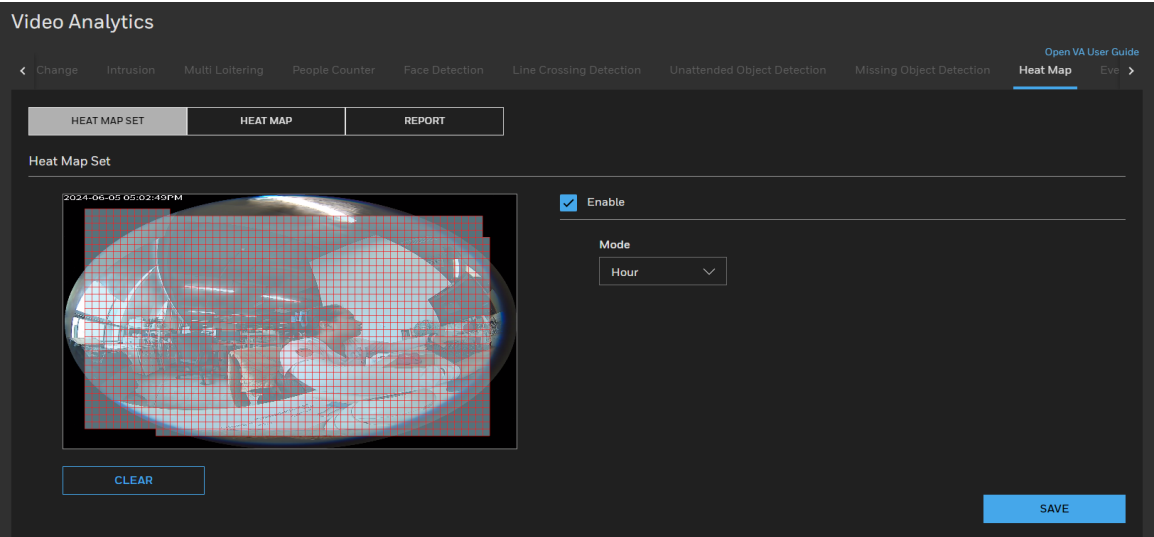
Heat Map Set

The heat map is a method of data analysis, statistics, and intuitive display, displaying customers' regions, targets, and geographical locations in a specially highlighted form.

After the camera enables the heat map, it will automatically detect and count the flow of people in the detection area, and identify the relative frequency of flow activities through different colors.

Go to **Setup > Video Analytics > Heat Map > Heat Map Set**.

Figure 55 Heat Map Set



Enable the heat map function. This function is disabled by default and needs to be manually enabled.

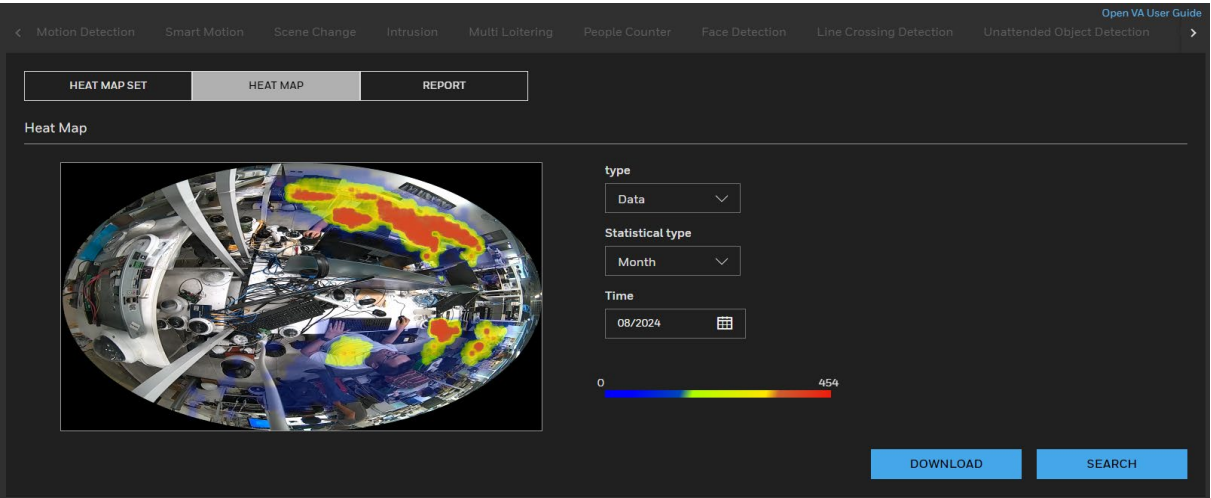
Set **Mode**, is a statistical type, Hour (there are 24 pieces of data per day) or Day (there is 1 piece of data per day); The original data will be cleared when the type is switched. Please operate with caution.

Click **SAVE** to save the settings.

Heat map

Go to **Setup > Video Analytics > Heat Map > Heat Map**.

Figure 56 Event & Metadata Scheme



Type: Choose Data or Picture. Data is presented in numerical form to download; The picture is displayed in different areas with different colors on the downloaded picture.

Statistics type: Year / Month / Day / Hour can be chosen.

Time: Select a retail time to search or download heat map data.

Heat map bar Distinguish different degrees by different colors.

The maximum value is the maximum data of a single area in the heat map at the current set time.

Click **DOWNLOAD** to download the statistics to the local folder.

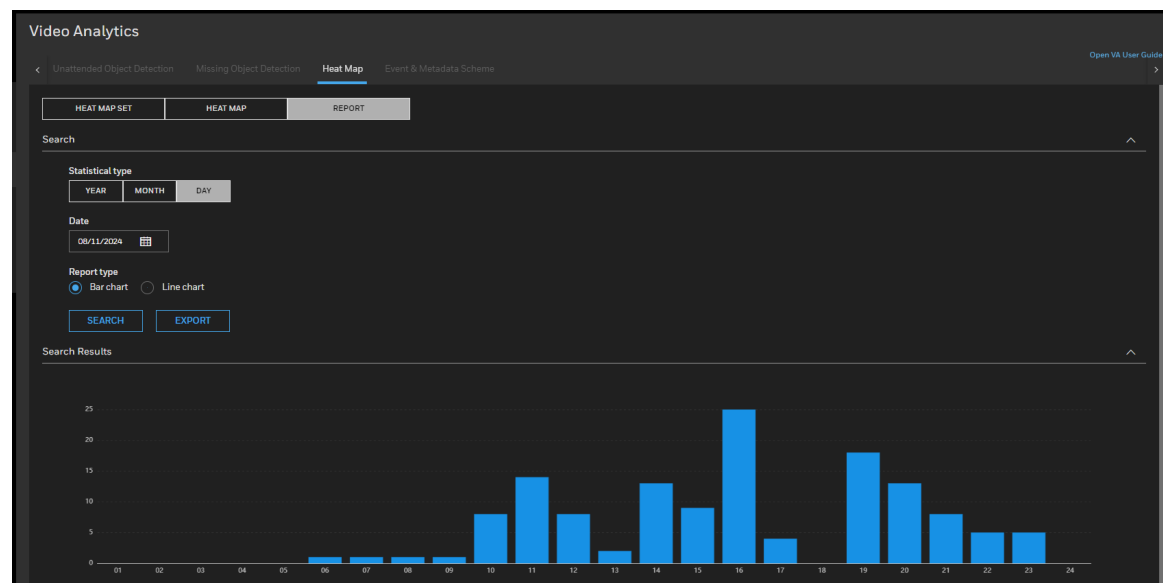
Click **SEARCH** to view the result on the current page.

Note: *The download file of the year shows the data for 12 months.
The download file of the month shows the data for all days of this month.
The download file of the day shows the data for 24 hours.*

Report

Go to **Setup > Video Analytics > Heat Map > Report**.

Figure 57 Event & Metadata Scheme



Set **Statistical Type** (Hour, Day, Month, Year),

Start time and End time (set detailed time according to the statistical method).

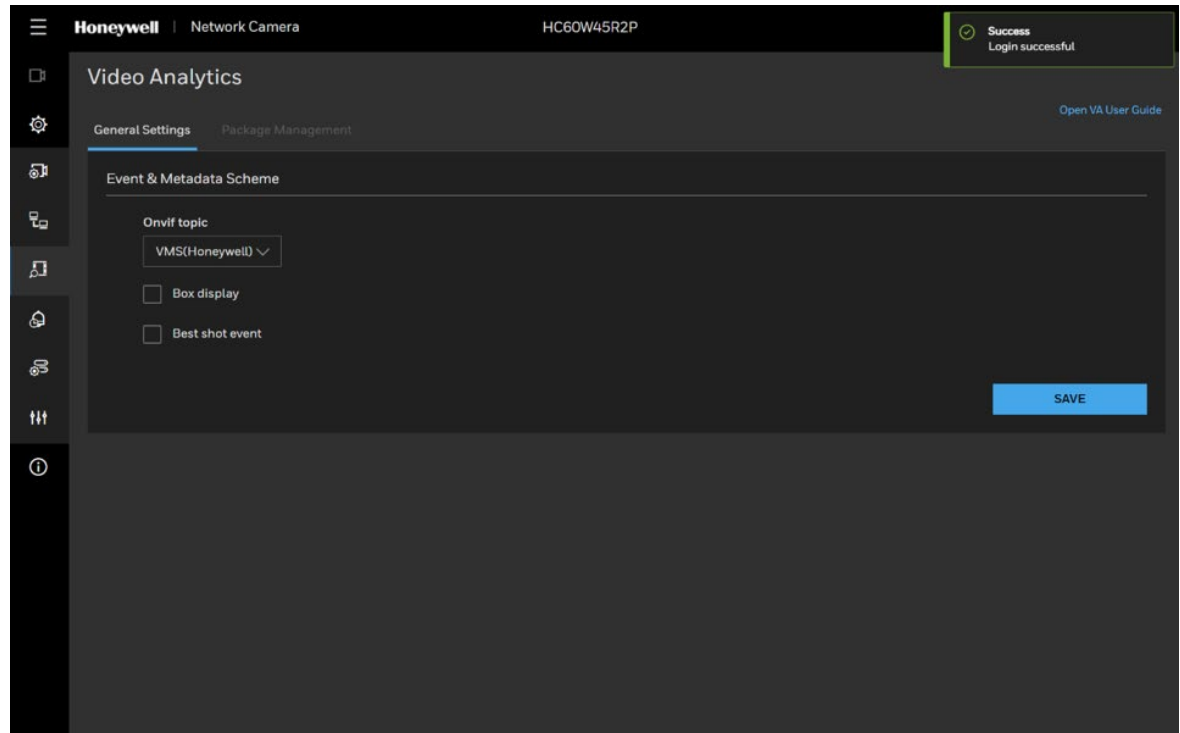
Set the chart type (Bar chart or Line chart).

Click **SEARCH** or **EXPORT** the relevant heat map statistic.

Event & Metadata Scheme

The Event & Metadata Scheme function supports different VA data transmissions. You must choose a correct method link to a third platform such as MaxPro or Genetic. The third platform will not receive VA information if chooses an incorrect connection.

Figure 58 Event & Metadata Scheme



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

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

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

Box display: The bounding box shows on main streaming when the target is detected.

Best shot event: When it is enabled, the ONVIF will send one message when the best shot event is triggered.

Note: *Motion Detection / Smart Motion / Scene Change features are not limited by this feature.*

License Plate Detection

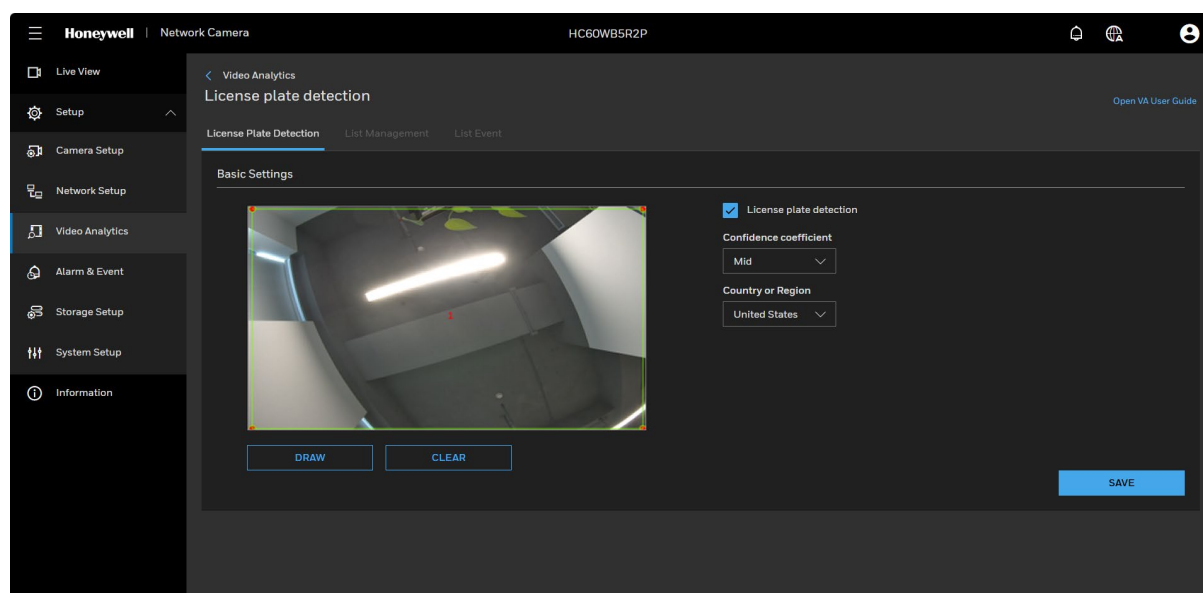
Note: *The License Plate Detection function is only applicable for HC60WB5R2P /HC60WB5R5P /HC60W35R4P /HC60W35R2P/HC60W45R2P /HC60W45R4P.*

On the Video Analytics interface, click  on the License plate detection item to enter the settings page.

Users can set the license plate detection, list management, and list events at the license plate detection interface.

License Plate Detection

Figure 59 Basic Settings



License plate detection: Check the checkbox to enable the License plate detection.

Confidence coefficient: Choose the value from the drop-down list to set the sensitivity of detecting the target, Low, Mid, or High. The higher the confidence, the better the snapshot quality and the fewer snapshots.

Country: Choose the country or region to detect, the different regions have different license plate algorithms.

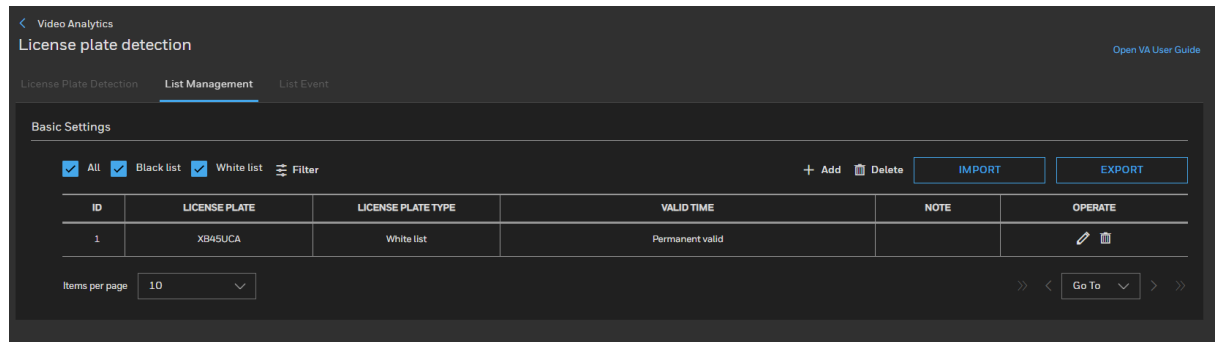
Schedule: Use the mouse to drag the time, or click the time grid to choose time one hour by hour. The blue means armed and the gray means unarmed.

Click **SAVE** to save the settings.

List Management

Go to **License plate detection > List Management** interface, and set the license plate to white list or blacklist.

Figure 60 List Management Interface



The user can add the plates one by one, or import the plates file to the camera. Import file type you can export the file advanced, and follow the example to input the data.

Note: *The size of the imported file can be more than 250KB, and the number of license plates is up to 4000. The imported file will cover all the data. If not, you need to export the file and add the new license plates into this file, and then import this new file to the device.*
When importing the license plates, you must choose the corresponding country, otherwise the character may be imported with error.

Figure 61 Add Plate

The 'Add Plate' dialog box contains the following fields and options:

- License plate:** A text input field.
- Type:** A dropdown menu with 'White list' selected.
- Valid time:** A dropdown menu with 'Permanent' selected.
- Note:** A text input field.
- Tip:** A section with the following text:
 - Wiegand 26 Card ID: There are a total of 8 digits, with the first 5 digits ranging from 00001 to 65535 and the last 3 digits ranging from 001 to 255
 - Wiegand 34 Card ID: Maximum 10 digits, range: 1~2147483647
- Buttons:** 'CANCEL' and 'SAVE' buttons at the bottom.

Input the license plate, choose the type (white list or blacklist), set the valid time, and choose the Wiegand. If needed, you can add a note to remark something.

Note: *The Wiegand is applicable for HC60WB5R2P /HC60WB5R5P.*

Tick the type of license to show in the list, you can set the filter to show a detailed license plate.

Click  to edit the current license plate. Click  to delete.

Items per page

Choose the items per page, 10/25/50/100 can be chosen.

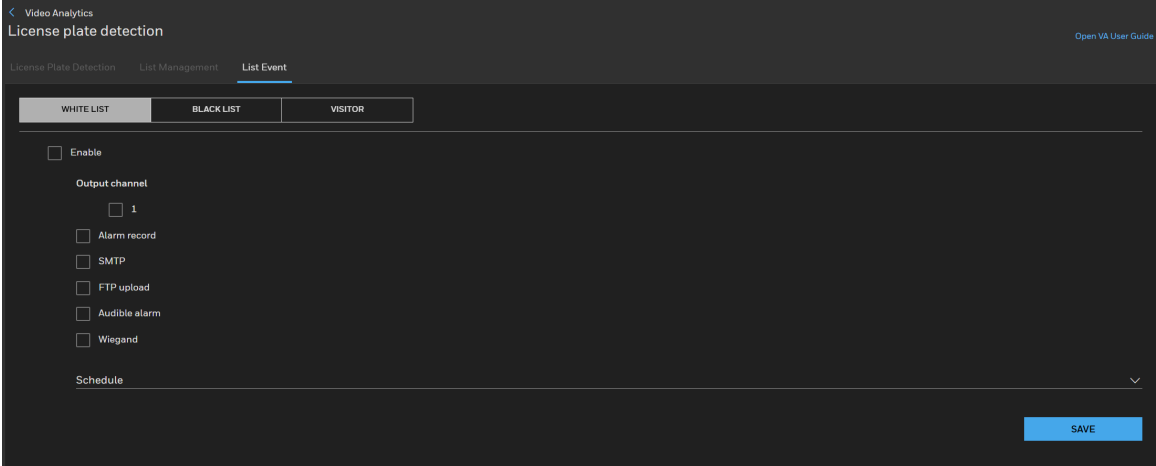
Go To

Go to the other page to view license plates quickly.

List Event

Go to **License plate detection > List Event** interface, and set the linkage action when the camera detects the license plate of the list. The white list, black list, and visitor are the same method to set.

Figure 62 List Event—White List/Black List



Enable: Check the checkbox to enable the license plate detection function.

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

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

SMTP: Check the checkbox to enable the linkage action for sending snapshot and alarm notice information to the 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 the FTP server when an alarm happens if you select the FTP upload box.

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

Wiegand: When the plate of the whitelist is captured, it will send signal to the Wiegand device.

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** to save the settings.

Figure 63 List Event—Visitor

WHITE LIST BLACK LIST VISITOR

☐ Enable

Output channel

☐ 1

☐ Alarm record

☐ SMTP

☐ FTP upload

☐ Audible alarm

☐ Wiegand

Wiegand ID

Schedule

SAVE

Note: For Visitor plates, tick the Wiegand, users should input the Wiegand ID for alarming.

Motion Detection

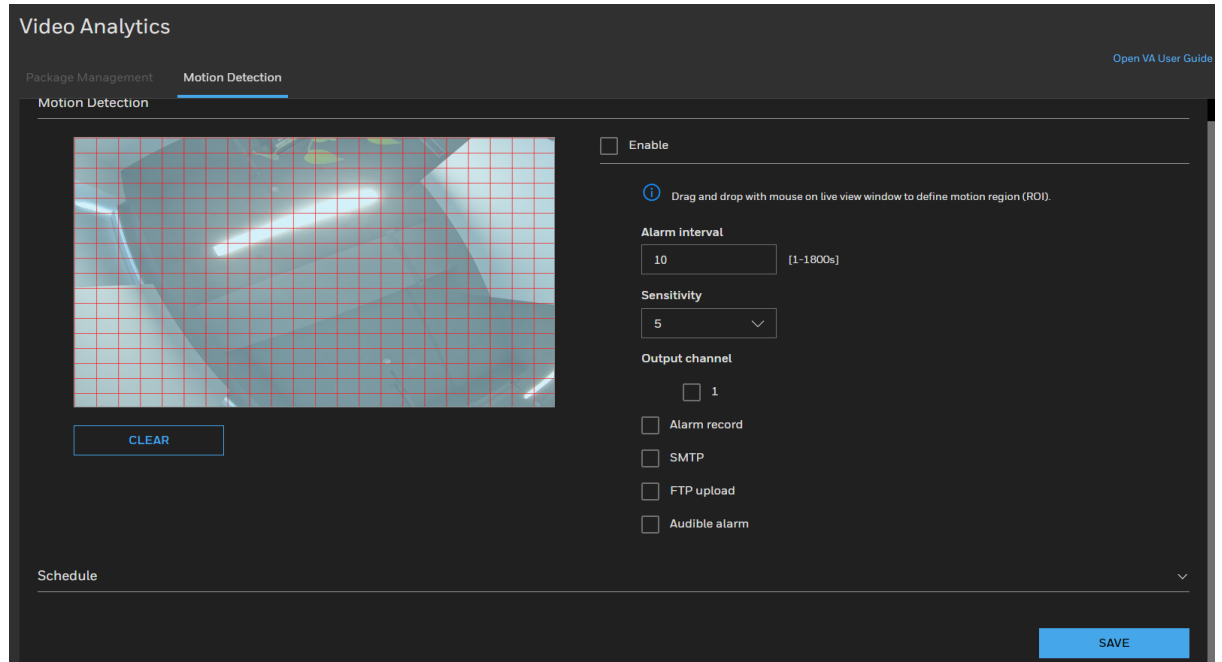
Motion Detection can be used to detect the motions of humans and things in the defense time at the drawing areas.

The applicable scenarios of this feature can be:

- Detects when a human enters the warehouse after office hours.
- Detects when an object is moved at a fixed place.

Log in a camera and go to **Setup > Video Analytics > Motion Detection**, as shown in [Figure 64](#).

Figure 64 Motion Detection Interface



Enable: Check the checkbox to enable the Motion Detection.

Alarm interval: It will only send one alarm during the configured interval time.

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 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.

Output channel: Check the checkbox to enable Output channel.

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

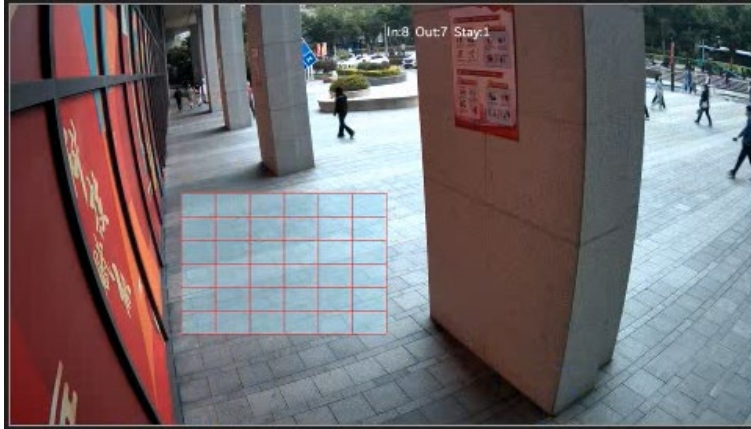
SMTP: Check the checkbox to enable the linkage action for sending snapshot and alarm notice information to the email address which can be set in **Network Setup > SMTP**, so the user can receive the alarm timely.

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

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

Drag and drop with your mouse to draw detection areas on the live video to define motion region (ROI). You can set several areas to detect.

Figure 65 Set A Detection Area



CLEAR: Clear the area of the setting. Use the mouse on the screen to draw the rectangle to set the motion detection areas. You can set several areas to detect.

Schedule: Use the mouse to drag the time or click the time grid to choose time hour by hour. The blue means armed and the gray means unarmed, as shown in [Figure 64](#).

The defense area consists of grids. You can draw the mouse to choose, or click to choose. It is better to choose the center area in the picture. The far distance should set the higher value sensitivity and more area to cover.

The area can cover all pictures, it also can be set in a small area such as a cabinet.

Click **SAVE** to save the settings.

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 66 Alarm Input

Alarm Input1

☐ Alarm input

Name

Current mode
Low

Output channel
☐ 1

☐ Alarm record ☐ SMTP ☐ FTP upload

☐ Audible alarm

Schedule

	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

Armed
Unarmed

Alarm Input2

☐ Alarm input

Name

Current mode

Output channel

☐ Alarm record ☐ SMTP ☐ FTP upload

☐ Audible alarm

Schedule

	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																									
Mon																									
Tues																									
Wed																									
Thur																									
Fri																									
Sat																									

☐ Armed
☐ Unarmed

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 the left mouse button to select any time point between 0:00-24:00 from Monday to Sunday.
- Hold down the left mouse button, drag and release the 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/Audible alarm: Check the checkboxes to enable Alarm record, SMTP, FTP upload, and Audible alarm.

Alarm Output

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

Figure 67 Alarm Output

Alarm Output

Alarm Output

Name

Current signal

Grounded ^

Alarm time(ms)(0:continuous)

0

Manual control

OPEN CLOSE

☐ Timing alarm output

Name: Alarm output name

Current Signal: Select **Grounded** or **Open** to define the 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 the alarm event setting.

Alarm time: Specifies the duration of alarm signal output. 0: Indicates continuous alarm (no automatic termination).

- **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 an alarm out signal is coming, click **Close** to disable the alarm out or click **Open** to keep the alarm out status.

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

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

Note: *For HC60WB5R2P/ HC60WB5R5P/ HC60W35R4P/ HC60W35R2P /HC60W45R2P /HC60W45R4P, two alarm inputs and one alarm output can be configured.
For HC60WFCR1, two alarm inputs and two alarm outputs can be configured.*

Configuring SD Card Alarm

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

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

Alarm threshold (used space): The camera will alarm when the 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 checkboxes to enable SMTP and FTP upload.

Note: *For the event recording clips edge sync, the current firmware version can only support no more than 1000 recording clips in the SD card within 1 month ahead of 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 68 Audio Detection

The screenshot shows the 'Alarm & Event' configuration page with the 'Audio Detection' tab selected. The page has a dark theme. At the top, there are tabs for 'Alarm In And Alarm Out', 'SD Card Alarm', 'Audio Detection' (active), 'Illegal Access Alarm', and 'Wiegand'. Below the tabs, the 'Audio Detection' section contains several settings: an 'Enable' checkbox, four alarm type checkboxes ('Glass break alarm', 'Scream alarm', 'Gunshot alarm', 'Loud sound alarm'), an 'Alarm interval' field set to '10' with a range '[10 ~ 86400s]', an 'Output channel' section with a '1' checkbox, and three checkboxes for 'Alarm record', 'SMTP', and 'FTP upload'. At the bottom, there is a 'Schedule' section with a dropdown arrow and a blue 'SAVE' button.

Enable: Check the checkbox to enable the audio detection. And then tick the following alarms.

Glass break alarm/Scream alarm/Gunshot alarm/Loud sound alarm: Check the checkbox to enable.

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

Alarm interval: Set the interval.

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

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

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

Note: *For the Audio Detection, the detection value is a theoretical value for reference only and may differ from the actual detection value. It is only recommended to use as an auxiliary detection method, not as the only basis for detection.*

Configuring Illegal Access Alarm

Go to Setup > Alarm & Event > Illegal Access Alarm.

If the user enters an incorrect password five times in a row, the camera will be locked for five minutes, and an alarm notification will be sent.

Figure 69 Illegal Access Alarm

The screenshot shows the 'Alarm & Event' configuration page with the 'Illegal Access Alarm' tab selected. The 'Illegal access alarm' section has an 'Enable' checkbox. Below it is a 'Schedule' section with a grid for selecting armed/unarmed times. The grid has columns for hours (00-24) and rows for days of the week (Sun-Sat). A legend indicates blue for 'Armed' and grey for 'Unarmed'. A 'SAVE' button is at the bottom right.

	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

Enable: Check the checkbox to enable the illegal access alarm.

SMTP: Check the checkboxes to enable SMTP.

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

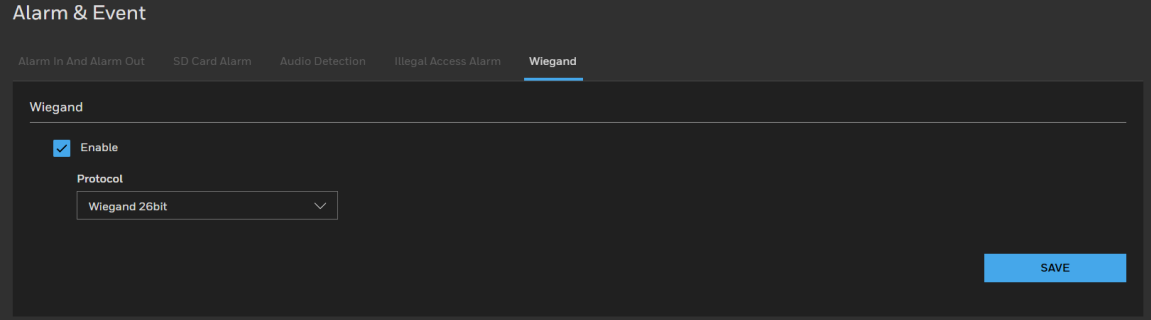
- Click the left mouse button to select any time point between 0:00-24:00 from Monday to Sunday.
- Hold down the left mouse button, drag and release the mouse to select the schedule within 0:00-24:00 from Monday to Sunday.

Configuring Wiegand

Go to Setup > Alarm & Event > Wiegand.

The LPR camera can enable Wiegand, and when the camera detected the license plate of the whitelist or blacklist, it will send the signal to the Wiegand device.

Figure 70 Wiegand



The screenshot shows the 'Alarm & Event' configuration page with the 'Wiegand' tab selected. Under the 'Wiegand' section, there is a checkbox labeled 'Enable' which is checked. Below it is a 'Protocol' dropdown menu currently set to 'Wiegand 26bit'. A blue 'SAVE' button is located at the bottom right of the configuration area.

Enable: Check the checkbox to enable the Wiegand

Protocol: Select Wiegand protocol as **Wiegand 26bit**, and **Wiegand 34bit**.

Note: *The protocol type should correspond with the Wiegand ID, otherwise, the signal send failed.*

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 cards.

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.*
 - *The 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 on 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 95.*

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 95.

Figure 71 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 72 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.

Search

Trigger type

All type

Time

Search for last

1

MINUTE(S)

HOURS

DAYS

WEEKS

From / To

01/11/2022

04:43

PM

01/18/2022

04:43

PM

SEARCH

- **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 content created at a specific point in time.

Click **SEARCH** and the recorded data corresponding to the search criteria will be listed in the **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 clips with the 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 recordings, not periodically recording. It includes Motion detection alarm, I/O alarm, Intrusion alarm, Multi loitering alarm, Smart motion alarm, Scene change alarm, Unattended detection alarm, Missing object detection alarm, Line crossing detection alarm, Audio detection alarm, Face detection alarm, and Camera tamper alarm.
For HC60WFCR1, it supports the personnel count threshold alarm.

Click the result to play the recording.

Figure 73 Play Recording

Storage Setup

SD Card Management **Content Management** Recording Settings

Play

← BACK TO SEARCH



◀ || ▶ ⛶

Search Results

2 Items total (Max 1000)

	Device	Trigger type	Starting time	Ending time
☐	SD	Motion detection alarm	03/27/2025 10:18:26 AM	03/27/2025 10:18:45 AM
☐	SD	Motion detection alarm	03/27/2025 10:18:54 AM	03/27/2025 10:19:45 AM

Items per page: 10

1 / 1

DOWNLOAD

It will play all the recording. Click ◀ to play the previous recording, click || to pause playing, and click ▶ to play the next recording. Click ⛶ to play the recording in full screen.

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
Mon
Tues
Wed
Thur
Fri
Sat

☒ Armed
☐ Unarmed

Network Failure Record

☐ Network failure record

NVR IP address **Time**
5 [5~12s]

Schedule record: Enables schedule record so 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 audio 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 work.
 - The time for Network Failure Record means the time that the IP camera continues recording video in the SD card after the IP camera is recovered for connecting to

the NVR.

- *For the Network Failure Record function, the camera can only support the pre-recording buffer with a fixed 15MB. It takes about 18~20S to detect the abnormal RTSP disconnection to start the recording and storage in the SD card. To make the backfill cover the recording gap on the end-head side, it is recommended to configure it with a 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 hostname and system time.

Figure 74 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 may be inaccurate.

Current PC time: Time on the current PC.

Set manually: This 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 a 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 the firmware version, etc.

GENERAL SETTINGS IMPORT/EXPORT FILES

Upgrade firmware

Firmware file

CHOOSE FILE No file chosen

UPGRADE

Reboot

REBOOT

Restore

☐ Reserve IP setting

RESTORE

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 is completed.
- 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 95.
- A new SD card inserted into the 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 into the camera, wait for the SD card formatting to complete.

Rebooting the Camera

On this page, you can reboot the camera. It takes about one minute to complete. After it is completed, the live video page will be displayed in your browser. If the connection fails after rebooting, manually enter the IP address of the camera in the address field to resume the connection.

Restoring the Camera

Restore the camera to factory default settings.

Network Setup: Check to retain the Network Type settings (see [Configuring Network General Settings](#) on page 34).

Daylight Savings Time: Check to retain the Daylight Savings Time settings (see [Importing/Exporting Files](#) on page 102).

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 reports.

The screenshot shows the 'EXPORT/EXPORT FILES' tab in the Honeywell 60 Series Cameras web client. It is divided into two main sections: 'Export Files' and 'Upload Files'.

Export Files:

- CA certificate:** A button labeled 'EXPORT'.
- Export configuration file:** A button labeled 'EXPORT'.
- Password for exporting configuration file:** A text input field.

Upload Files:

- Upload configuration file:** A button labeled 'CHOOSE FILE'.
- No file chosen:** A status indicator.
- UPLOAD:** A button.
- Password for uploading configuration file:** A text input field.

Message: A blue information icon followed by the text: '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 into 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 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: *The 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 as the password of the configuration file you set for exporting, or the uploading will fail. 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.

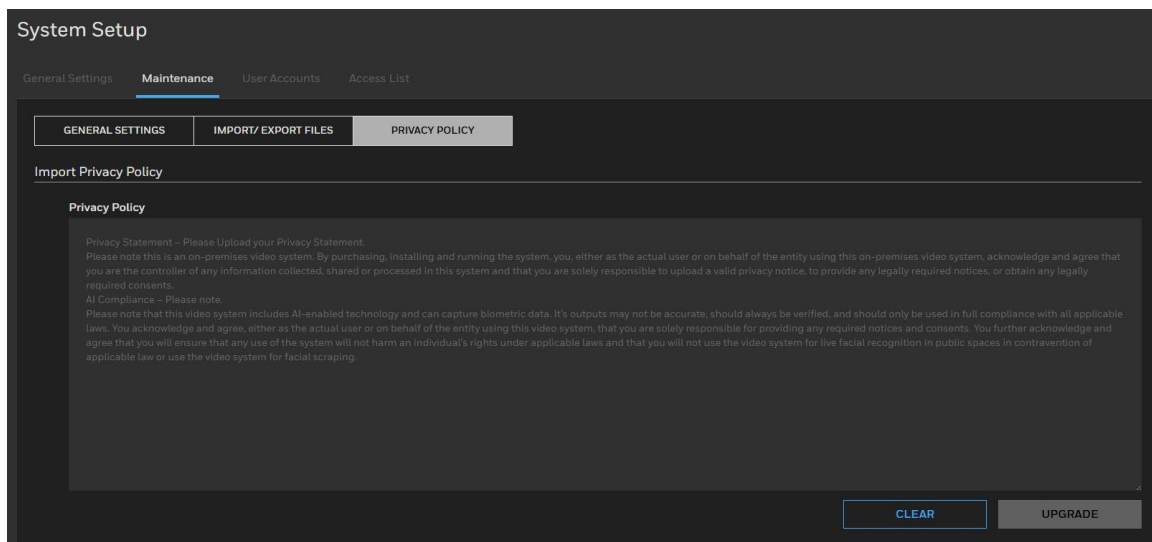
If the power is disconnected during a firmware upgrade or if there is an unknown reason causing abnormal LED status, and a Restore cannot recover normal working condition, you can perform the following steps to activate the camera with its backup firmware:

- 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 hangs. (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 the web so that other users can understand the privacy policy and make sure that.



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

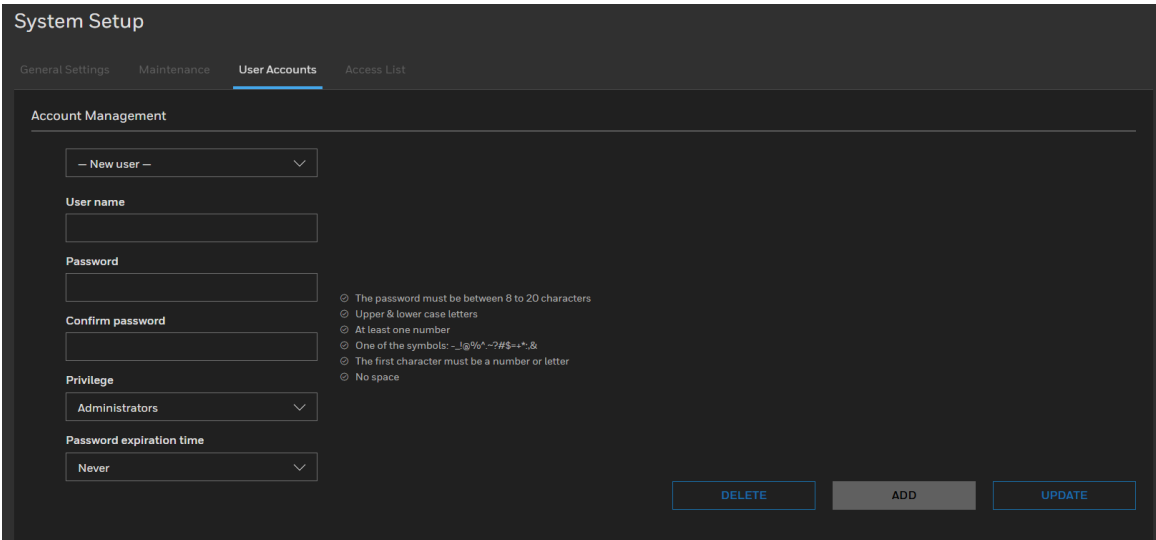
Note: *The default policy is “Privacy Statement – Please Upload your Privacy Statement. Please note this is an on-premises video system. By purchasing, installing, and running the system, you either as the actual user or on behalf of the entity using this on-premises video system, acknowledge and agree that you are the controller of any information collected, shared, or processed in this system and that you are solely responsible to upload a valid privacy notice, to provide any legally required notices, or obtain any legally required consents. AI Compliance- Please note. Please note that this video system includes AI-enabled technology and can capture biometric data. It's outputs may not be accurate should always be verified and should only be used in full compliance with all applicable laws. You acknowledge and agree, either as the actual user or on behalf of the entity using this video system, that you are solely responsible for providing any required notices and consents. You further acknowledge and agree that you will ensure that any use of the system will not harm an individual's rights under applicable laws and that you will not use the video system for live facial recognition in public spaces in contravention of applicable law or use the video system for facial scraping.”*

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



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:

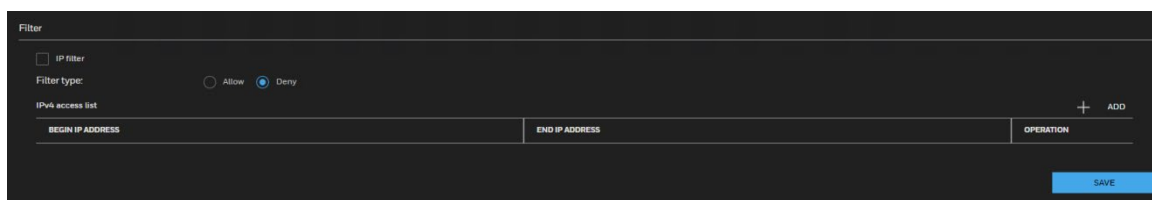
1. Select an existing account.
2. Make necessary changes and click UPDATE to enable the setting or click DELETE to delete the account.

For safety and the users’ level, the user should set the password expiration time, select 1 day /2 days/3 days/1 week/3 weeks/ 1 month/2 months / 3 months/ 6 months/ 1 year/ Never.

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.

The screenshot shows a web interface for configuring IP filtering. At the top, there's a 'Filter' section with a checkbox for 'IP filter'. Below it, 'Filter type:' has two radio buttons: 'Allow' and 'Deny', with 'Deny' selected. Underneath is the 'IPv4 access list' section, which contains a table with three columns: 'BEGIN IP ADDRESS', 'END IP ADDRESS', and 'OPERATION'. To the right of the table is a '+ ADD' button. At the bottom right of the interface is a blue 'SAVE' button.

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.

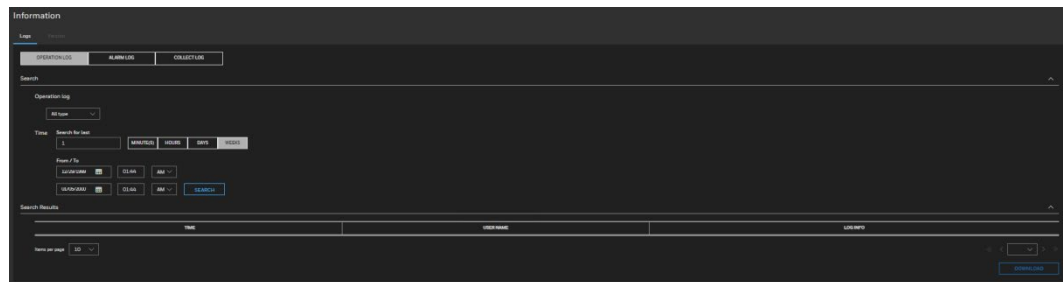
- Note:**
- *The IPv6 access list column will not be displayed unless you enable IPv6 on the Network page. For more information about IPv6 Settings, see operation on page [34](#).*
 - *The Range rule only applies to IPv4 addresses.*

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 helps you analyze and solve possible problems occurring on the device with one click.

1. Click **COLLECT**, and 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.

Privacy Policy

Go to **Setup > Information > Privacy Policy**.

On the **Privacy Policy** page, the non-admin user accounts accept the privacy policy.

Information

Logs Version Privacy Policy

PURPOSE:

There is a camera monitoring here!

☐ I have read and accepted the Privacy Policy.

ACCEPTED

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>The power supply is unstable.</i>	The use of a UPS power supply is strongly recommended.
<i>The camera webpage has an abnormal display.</i>	Clear the cache of the 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 that, please refer to the situations and solutions in the right column.</i>	- Whether the height and angle of the camera meet the requirements - Whether the focus state of the camera is optimal, and the lens front cover is dusty - Whether the arming area is drawn on the border of the image - Whether the color of the item is similar to the background color (for the function of detecting and removing leftover items) - Whether the camera is in a backlight environment which will affect the detection of the target and the effect of VA - Whether the target appears at the boundary of the area which will affect the judgment - 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) - 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 - If the accuracy rate is low, you can open the bounding box to check whether the target is detected normally

Issues	Solutions
<i>The Edge browser doesn't support H265 live view.</i>	1. Open the Edge browser, and input "edge://gpu". 2. Find "Media Foundation Rendering Capabilities", and make sure the "HEVC installed " and "HEVC activatable" are true. a) If they are false, you need to download the HEVC Video Extensions. b) Input "https://www.microsoft.com/store/productId/9N4WGH0Z6VHQ?ocid=dpdshare" to download HEVC Video Extensions, click "Install" to jump to the 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.

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 600-60UG04 Rev A– 08/2025