Honeywell

Honeywell

Bi-Spectrum Cameras

HC35TB5R1JT07 HC35TB5R4JT10 HC35TE5R3JT21 HC35TE5R4JT35

User Guide

Recommended

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

Copy Right

Revision

Issue	Date	Revisions
A	03/2025	New document.

Cautions and Warnings

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

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

Regulatory Statements

Photobiological safety

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

General Data Protection Regulation

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

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

Further details can be found on the GDPR website of the EU

FCC Compliance Statement

Information to the User: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help. Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. This Class A digital apparatus complies with Canadian ICES-003.

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

Manufacturer's Declaration of Conformance

North America

The equipment supplied with this guide conforms to UL 62368-1 and CSA C22.2 No. 62368-1.

Europe

The manufacturer declares that the equipment supplied with this guide is compliant with the European Parliament and Council Directive on the Restrictions of the use of certain hazardous substances in electrical and electronic equipment (2011/65/EU) as Amended by RoHS 3 (2015/863), and the essential requirements of the EMC Directive (2014/30/EU), conforming to the requirements of standards EN 55032 for emissions, EN 50130-4 for immunity, and EN 62368 for electrical equipment safety.

Waste Electrical and Electronic Equipment (WEEE)

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

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

Check Local Waste Guidelines

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

Safety Instructions

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

1. HEED WARNINGS - Adhere to all warnings on the unit and in the operating instructions.
2. INSTALLATION

- Install in accordance with the manufacturer's instructions.
- Installation and servicing should be performed only by qualified and experienced technicians to conform to all local codes and to maintain your warranty.
- Any wall or ceiling mounting of the product should follow the manufacturer's instructions and use a mounting kit approved or recommended by the manufacturer.
- It is not allowed to install the PTZ camera upside down.

3. POWER SOURCES - This product should be operated only from the type of power source indicated on the marking label. If you are not sure of the type of power supplied to your facility, consult your product dealer or local power company.
4. MOUNTING SYSTEM - Use only with a mounting system recommended by the manufacturer or sold with the product.
5. ATTACHMENTS/ACCESSORIES - Do not use attachments/accessories not recommended by the product manufacturer as they may result in the risk of fire, electric shock, or injury to persons.
6. CLEANING - Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning.
7. SERVICING - Do not attempt to service this unit yourself. Refer all servicing to qualified service personnel.
8. REPLACEMENT PARTS - When replacement parts are required, be sure the service technician has used replacement parts specified by the manufacturer or

have the same characteristics as the original part. Unauthorized substitutions may result in fire, electric shock or other hazards. Using replacement parts or accessories other than the original manufacturers may invalidate the warranty.

Warranty and Service

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

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

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

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

TABLE OF CONTENTS

Figures

Tables

CHAPTER

1 INTRODUCTION

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

Overview

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

The cameras offer 4 mega pixel resolution at up to 30 frames per second and use video compression technology to save bandwidth and storage while ensuring maximum video quality.

Each camera comes with configurable motion detection and camera tamper detection and supports up to 4 user-defined privacy mask areas.

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: *Bi-spectrum cameras support Windows desktop system and don't support mobile system.*
H.265 rendering need GPU supporting, if not it will transfer to rendering I frame.

Chrome and Edge browsers are supported:

Browser	Version
Chrome	91.0.4472.164 (Official Build) (64-bit)
Edge	92.0.902.7 (Official Build) (64-bit)

Browser Minimum Requirement for Hardware

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

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

Key Features

The key features in Honeywell Series Bi-spectrum IP camera are:

Camera

- Up to 2880×1620 for optical
- Up to 256×192 for thermal
- Video parameter setup, such as electronic shutter and gain
- Video Analytics: Motion Detection, Smart Motion, Scene Change, Intrusion, Multi Loitering, People Counter, Face Detection, Line Crossing Detection, Unattended Object Detection, Missing Object Detection (Be different for different models. More details, please refer to the product datasheet.).
- True WDR
- True day/night mode using a removable IR cut filter
- Low-light with 2D/3D noise reduction saving storage and bandwidth together with smart codec
- For use as part of Video Systems which comply with NDAA

Storage

- Camera has one SD card slot, files stored on SD card

Network

- Up to 10 connections
- Compatible with the following network protocols: IPv4, IPv6, TCP/IP, HTTP, HTTPS, RTSP/RTP/RTCP, IGMP/Multicast, SMTP, DHCP, NTP, DNS, QoS, SNMP, 802.1X, FTP, SFTP, UDP, ICMP, ARP, TLS
- Support the following security modes: User account and password protection, HTTPS, IP Filter, Digest authentication, TLS1.2 only (applicable for some cameras), TLS 1.2 and TLS 1.3 (applicable for some cameras), Stream encryption, AES128 / 256, SSH / Telnet closed, PCI-DSS compliance
- Support the following languages: Arabic, Czech, Dutch, English, French, German,

Italian, Japanese, Korean, Polish, Portuguese (Brazil), Russian, Spanish, Turkish, Traditional-Chinese

- Camera configuration and management via Ethernet

Events and Analytics

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

User Management

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

System Management

- Log function
- Support controlling access permission by verifying the client PC's IP address

CHAPTER 2

ACCESSING THE CAMERA

This chapter contains the following sections:

Installing the Unified Tool

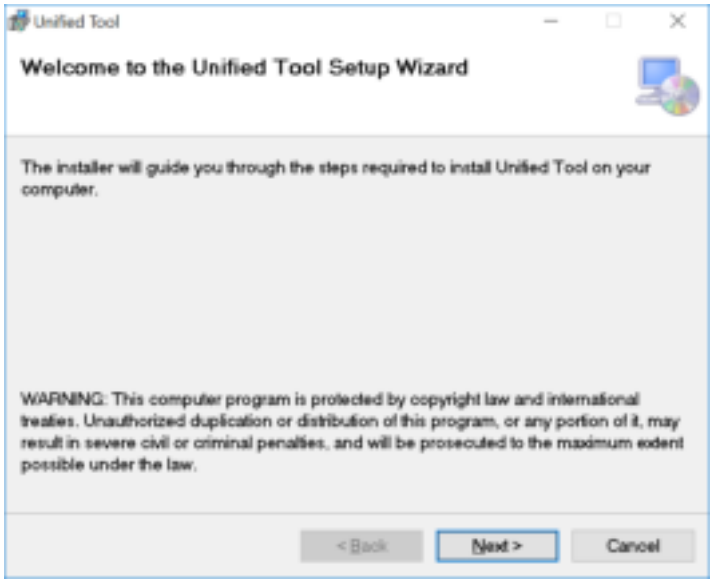
To get the installation package of Unified Tool:

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

To install the Unified Tool:

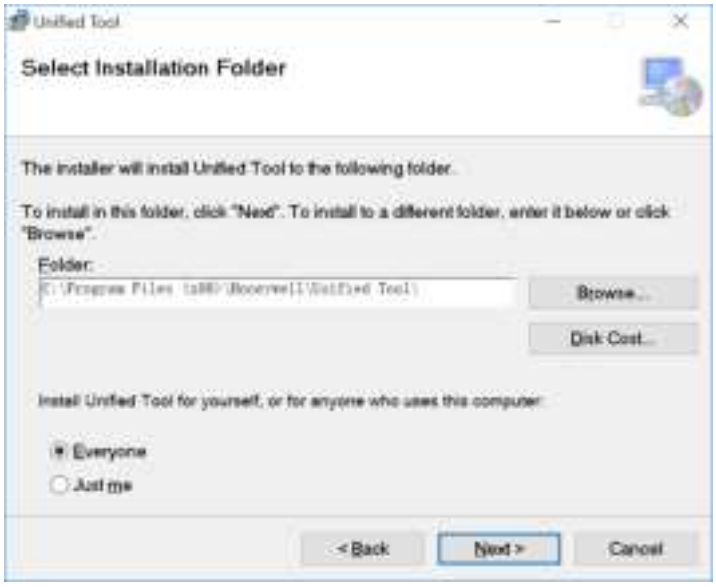
1. Double-click the installation program  in the installation package.

Figure 1 Install Unified Tool



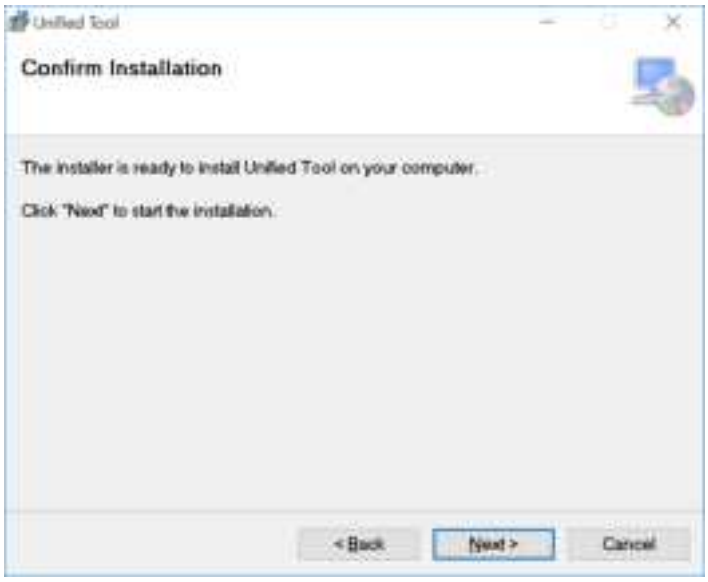
2. Click Next and the following figure is displayed:

Figure 2 Select Installation Folder



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

Figure 3 Confirm Installation



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

Discovering Your Camera on the Network

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

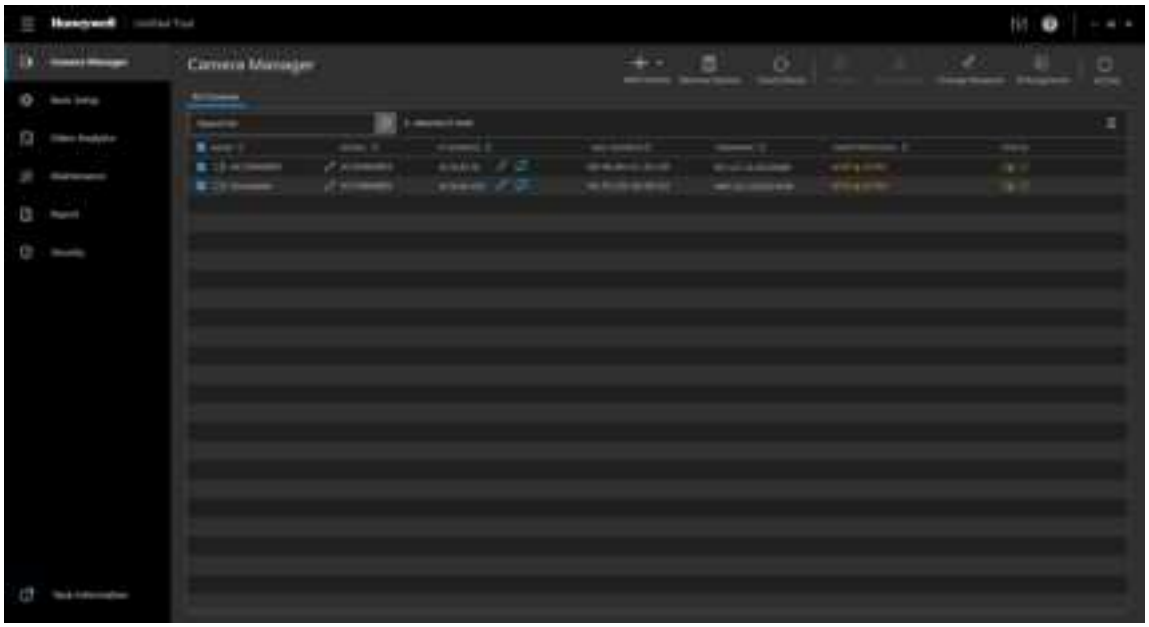
Figure 4 Splash Screen

2. Select your language from the dropdown list of Language. Currently, English and traditional Chinese are supported.
3. Check Don't show the splash page on startup and this page can be skipped next time. If you want to check the splash window again, click as shown in Figure 6 and select the checkbox of Show the splash page on startup.
4. Click on the main page and select Auto discover/IP address/From file on the drop list to discover the cameras.

Figure 5 Discover Cameras

After the discovering, all devices will be displayed in the devices list.

Figure 6 Device List



Initializing Cameras

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

Figure 7 Initialize Page 1

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

Note:
- *Honeywell strictly recommends to use HTTPs only and Honeywell will not hold responsible for the consequences.*

Figure 8 Initialize Page 2

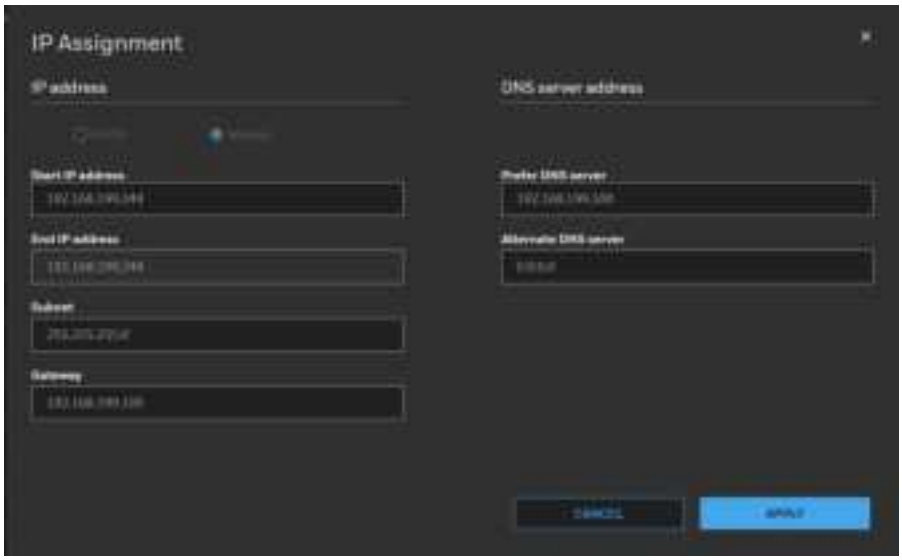
After initializing successfully, you can authenticate the camera and configure other setting.

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



Configure IP Address Setting

- To obtain IP address, subnet mask, and default gateway settings automatically, select the check box of **DHCP**.
- To configure IP address, subnet mask, and default gateway settings manually, select the check box of

Manual and enter the settings. If you enter the start IP address, the system can calculate the end IP address automatically according to the number of your selected device(s).

- After all settings are completed, click **APPLY**.

Configure DNS Server Address

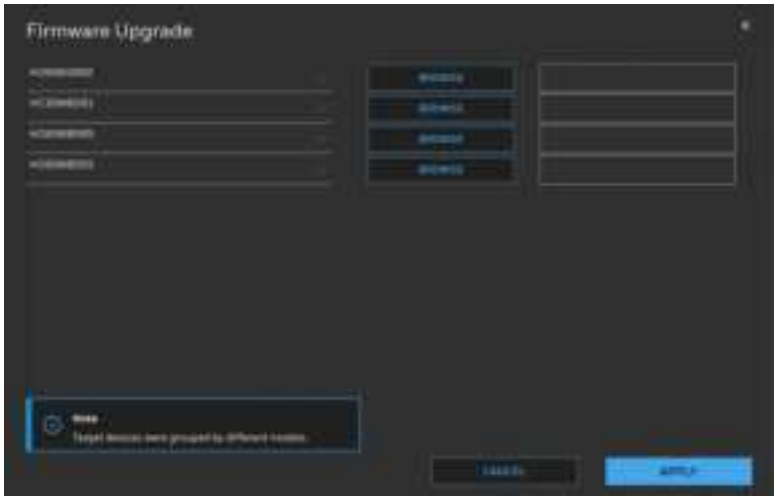
Configure the DNS server address and click **APPLY**.

Upgrading the Camera's Firmware

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

Select the **Maintenance** tab from the left pane as shown in Figure 6 select target device(s) and click  and the following window is displayed:

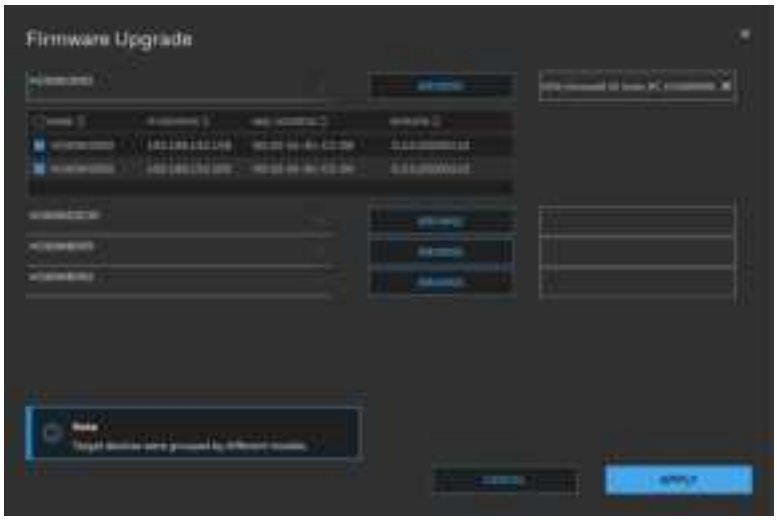
Figure 10 Firmware Upgrade 1



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

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

Figure 11 Firmware Upgrade 2



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

Accessing the Camera from a Web Browser

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

CHAPTER

3 LOGGING IN & VIEWING LIVE VIDEO

This chapter contains the following sections:

Logging in to the Camera via the Web Client

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

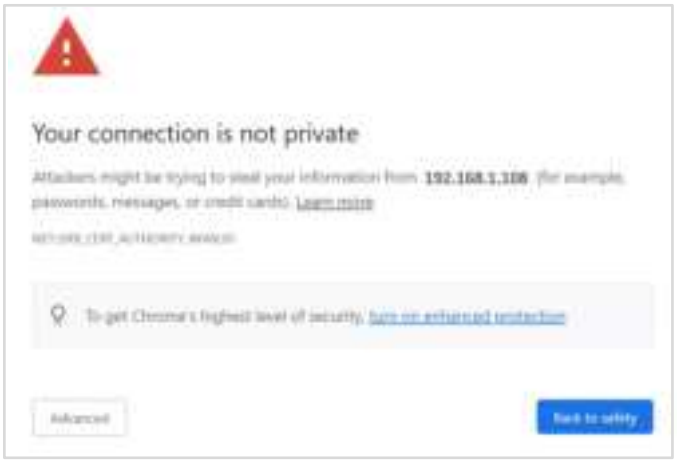
Before You Begin

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

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

Logging in to the Camera

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.

7. The pop window shows “privacy policy not imported” When the first time to login.

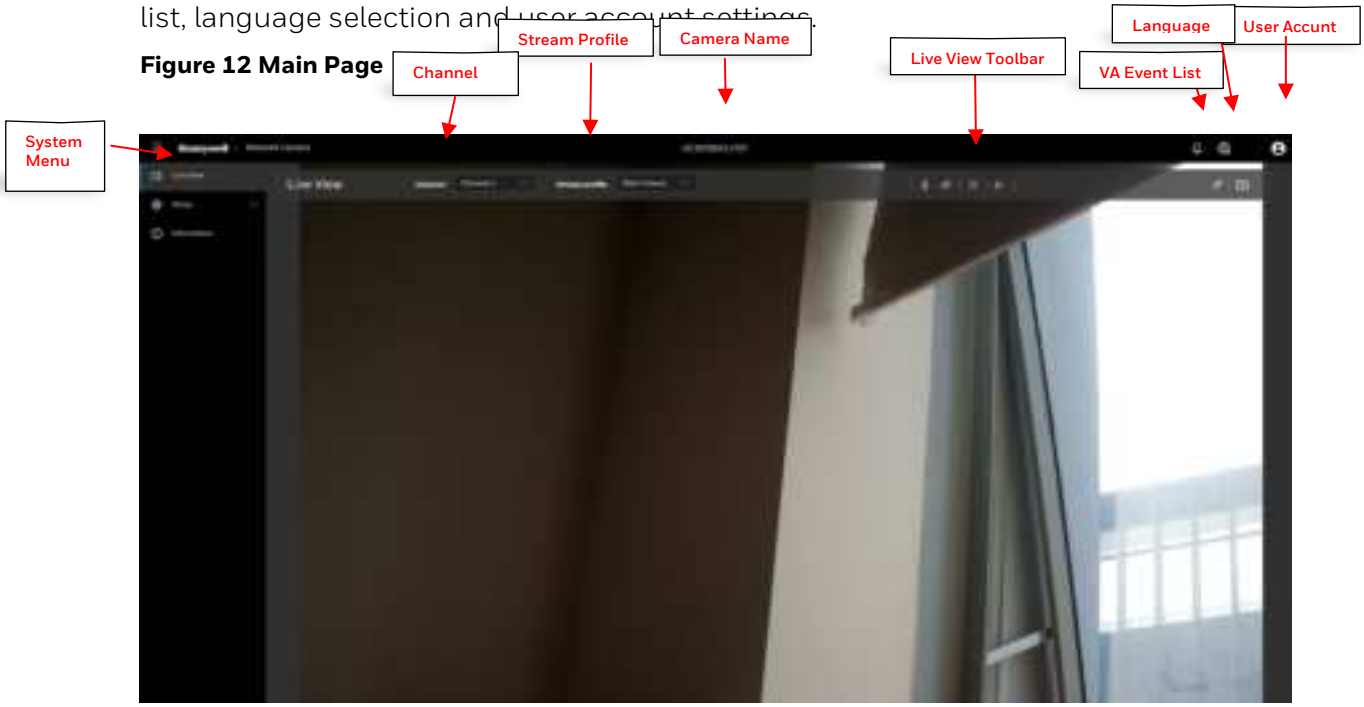
Tick **Do not remind me again** and click **Cancel**, the pop-up window will not show at next time. If untick **Do not remind me again,** the pop-up window will show every time when logging in.

If click **ADD PRIVACY POLICY,** it will go to **System Setup > Maintenance > PRIVACY POLICY** page to import the privacy policy. For details information, refer to Configurating 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



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**.

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.

The properties for each stream type are configured on the **Setup > Camera Setup > Video** page (see Configuring Video Settings on page 17).

Camera Name

You can change the camera name according to your needs. For more information, see Configuring System General Settings on page 89.

Live View Toolbar

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

Figure 13 Live View Toolbar

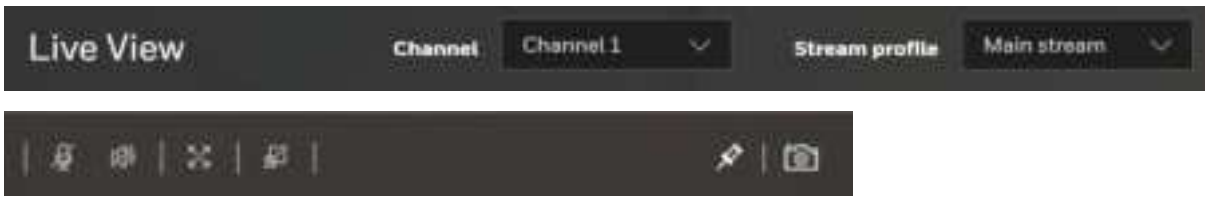


Table 1 Live View Toolbar Icons

Icon	Description
Channel	Channel 1 is optical channel; Chanel 2 is thermal channel; Switch the channel to view the different channels real-time video.
Stream profile	Main stream, or sub stream to view real-time video. The detail stream is set at **Setup > Camera Setup > Video.**
	The icon can be enabled from webpage when the microphone is connected to PC or embedded in PC. Click to enable PC microphone. You can talk and the audience can listen through speakers connected to camera. Click it again to disable this option.

	The icon can be enabled from webpage when the speaker is connected to PC or embedded in PC. Click to turn on the audio to listen to the monitoring site. Click it again to turnoff the audio.
	Click to switch to the full screen mode.
	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 human or vehicle), the boxes are red.
	Click to Pin the live view to the toolbar. Click once again to unpin.
	Click to capture and save video images. The captured images will be displayed in a pop-up window. Right click the image and select Save pictureas to save it in JPEG (*.jpg).

VA Event List

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

Note:

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

Language

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

Administrator Account

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

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

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

CHAPTER 4

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

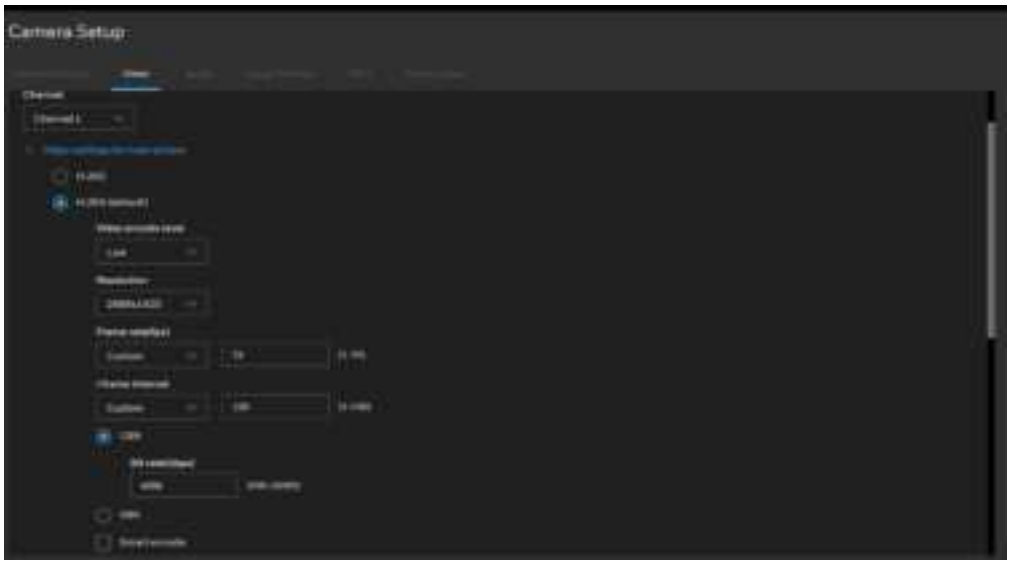
Configuring Video Settings

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

Video Stream

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

Figure 15 Video Stream



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

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

Video encode level: Select a value from the drop-down list box.
Resolution: Select a value from the drop-down list box. A higher resolution means better image quality.
See the following table for resolution of each model:

Table 2 Cameras Resolution

Model	Main Stream	Sub Stream
HC35TE5R3JT21 HC35TE5R4JT35 HC35TB5R1JT07 HC35TB5R4JT10	2880x1620 2560x1440 2304x1296 1920x1080 Bit rate (Kbps):12000 1280x720 Bit rate (Kbps):8000	1920x1080 Bit rate (Kbps):12000 1280x720 Bit rate (Kbps):8000 704x480(576) Bit rate (Kbps):3000 640x480 Bit rate (Kbps):1500
Thermal channel	704x480(576)	704x480(576) Bit rate (Kbps):3000 352x288 256x192 Bit rate (Kbps):1500

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 1-25 fps. If the video standard is set to **NTSC**, the frame rates are selectable from 1-30 fps.

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

See the following table for frame rate of each model:

Table 3 Cameras Frame Rate

Connection Type	Camera	Main Stream	Sub Stream
HTTP	HC35TE5R3JT21 HC35TE5R4JT35 HC35TB5R1JT07 HC35TB5R4JT10	Frame rate (FPS): PAL 25/NTSC 30 (Support custom) I frame interval: PAL 100/NTSC 120 Bit rate (Kbps):12000	Frame rate (FPS): PAL 25/NTSC 30 I frame interval: PAL 100/NTSC 120 Bit rate (Kbps): 1500
	Thermal channel	Frame rate (FPS): PAL 25/NTSC 30(Support custom) I frame interval: PAL 100/NTSC 120 Bit rate (Kbps): 6000	
HTTPS*	HC35TE5R3JT21 HC35TE5R4JT35 HC35TB5R1JT07 HC35TB5R4JT10	Frame rate (FPS): PAL 25/NTSC 30 (Support customization) I frame interval: PAL 100/NTSC 120 Bit rate (Kbps): 12000	Frame rate (FPS): PAL 25/NTSC 30 I frame interval: PAL 100/NTSC 120 Bit rate (Kbps): 1500
	Thermal channel	Frame rate (FPS): PAL 25/NTSC 30(Support custom) I frame interval: PAL 100/NTSC 120 Bit rate (Kbps): 6000	

Note:
- *For encryption under HTTPS. The limitation of encryptions:*
  *Channel1-MainStream:2880*1620@30fps, I frame 5fps, 8Mbps*
  *Channel1-SubStream:1920*1080@30fps, I frame 5fps, 4Mbps*
  Channel2-MainStream:D1 @30fps. I frame 5fps, 2Mbps
  Channel2-SubStream:D1 @30fps. I frame 5fps, 2Mbps"
  *Channel1-MainStream:2688*1520@30fps, I frame 5fps, 12Mbps*
  *Channel1-SubStream:1920*1080@30fps, I frame 5fps, 6Mbps*
  Channel2-MainStream:1920x1080 @30fps. I frame 5fps, 6Mbps
  Channel2-SubStream:D1 @30fps. I frame 5fps, 2Mbps"
- *If you need to enable functions that affect performance (such as VA, SD card recording), it is recommended to reduce the corresponding parameter values instead of using the maximum parameter of above table.*
- *The image parameter will be set as default value if the mode of video is changed.*

I-frame interval: Determine within how many frames interval the firmware will plant and I frame. The shorter the duration, the more likely you will get better video quality, but at the cost of higher network bandwidth consumption.
CBR: Constant Bit Rate
The bit rate remains constant (recommended for low-bandwidth environments). Required if MJPEG compression is used.
VBR: Variable Bit Rate
The bit rate changes according to the complexity of the scene.
Max bitrate(kbps): Indicates the maximal value of the bit rate. Set 500~12000 for max bitrate.
Image Quality: Select a desired quality ranging from Lowest to Highest.

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

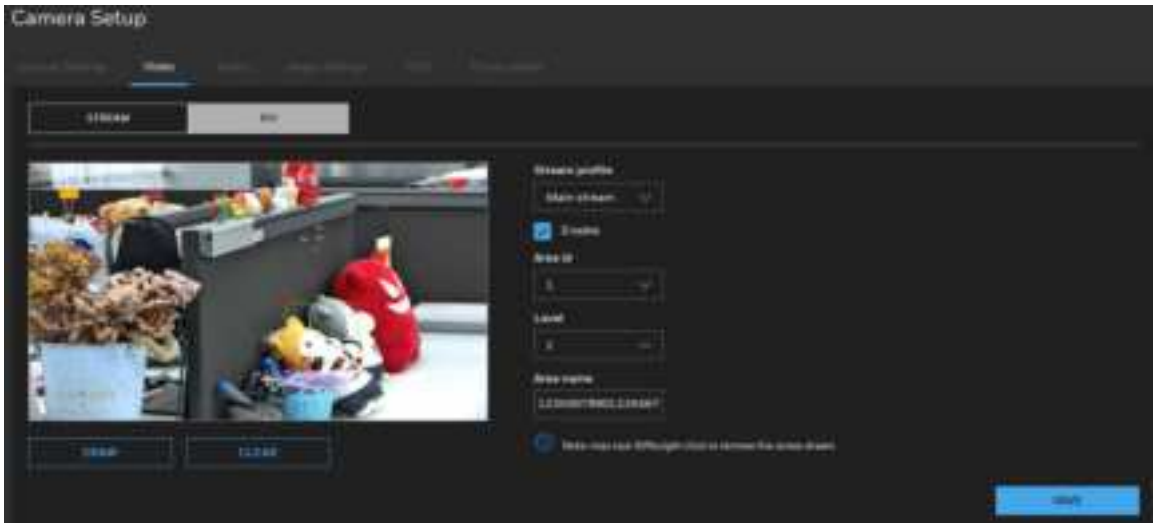
- *Selecting low compression level from MAXPRO NVR will result in high image quality in camera.*

Smart encode: Check the checkbox to enable Smart Encode.
- Smart encode includes H.264 & H.265.
- The storage space will be reduced fifty percent when smart encode is enabled.
- Only main stream supports smart encode.

ROI

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

Figure 16 ROI Settings



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

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

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

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

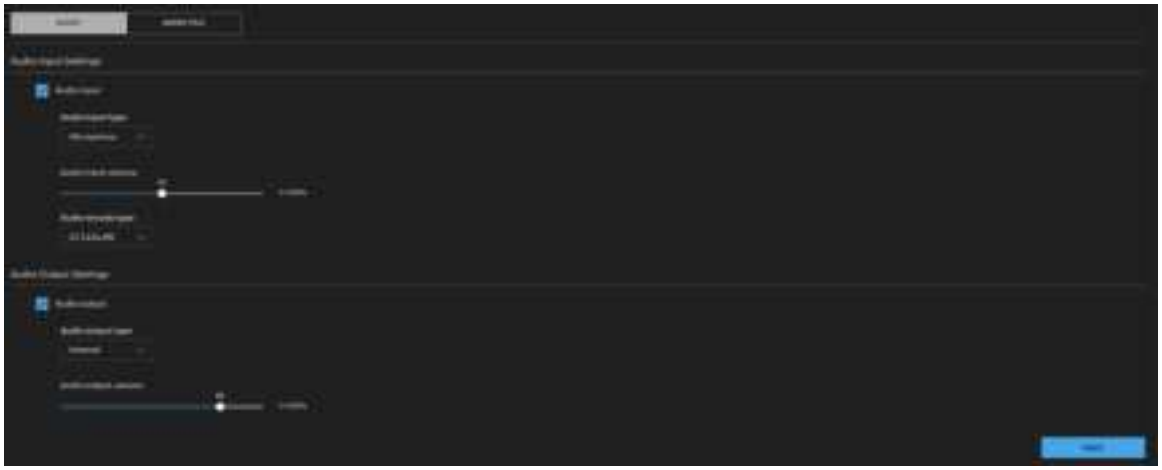
Area name: Enter a customized name for areas. The maximum value cannot exceed 32 bytes.

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

Configuring Audio Settings

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

Figure 17 Audio Settings



Audio Input Settings
Audio input: Check the checkbox to enable Audio input.
Audio input type: Select the Microphone or Line-in option.

Note: *When integrated with the platform, the camera only supports one audio backchannel connection at the same time.*

Audio input volume: Microphone gain or Line-in gain. The Microphone gain or Line-in gain option is displayed according to the Audio input option selected. Select the gain of the external audio input according to ambient conditions. Adjust the gain from 0% (least) to 100% (most).
Audio encode type: Select audio codec as **G711ALAW** and **G711ULAW** and the bit rate.
Audio Output Settings
Audio output: Check the checkbox to enable Audio output.
Audio output type: Select the Line-out option.
Audio output volume: The Line-out option is displayed according to the Audio output option selected. Select the volume of the external audio input according to ambient conditions. Adjust the volume from 0% (least) to 100% (most).
After you complete the settings on this page, click **SAVE** to enable the settings.

Audio File

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

Figure 18 Audio File

There are 17 default files, users can set the cycle number, click  to test listen. If the playing time is over the alarm interval, the audio cycle number will be interrupted.

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

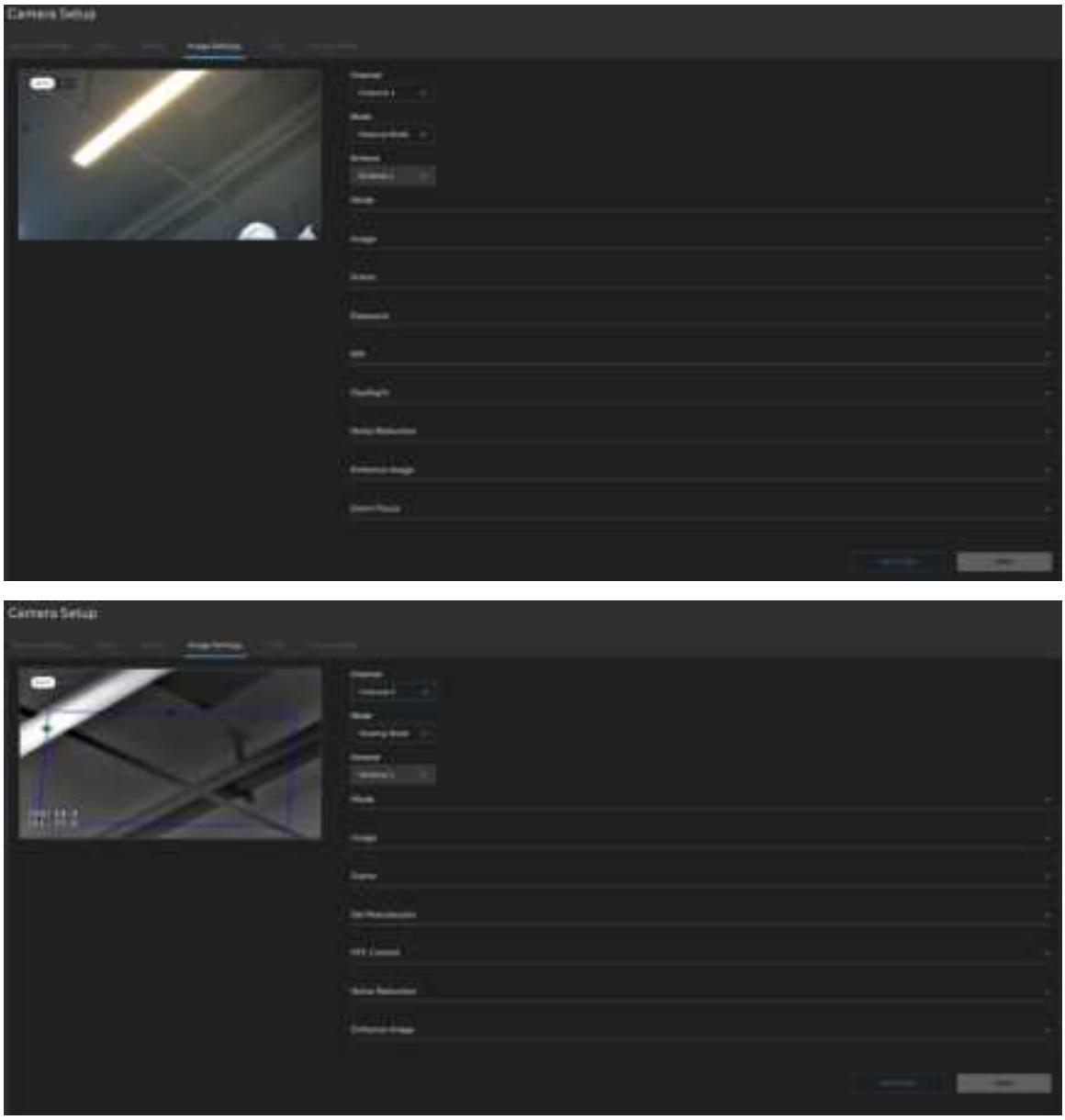
The file type should be WAV, size must be less than 250 Kb, the sampling rate should be 8000Hz.

Configuring Image Settings

Go to **Setup > Camera Setup > Image Settings**.
On the Channel drop-down list, choose a channel to set the image settings of optical or thermal channel.

- On channel 1 (optical channel) page, you can configure the parameters for **Mode, Scheme, Image**, **Scene**, **Exposure**, **WB**, **DayNight**, **Noise Reduction** and **Enhance Image**. For motorized lens camera, you can set **Zoom Focus**.
- On channel 2 (thermal channel) page, you can configure the parameters for **Mode, Scheme, Image, Scene, Set Pseudocolor, FFC Control, Noise Reduction** and **Enhance Image**.

Figure 19 Image Settings



Mode

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

Scheme

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

Image Adjustment

Brightness: Adjust the image brightness level (0 to 100).
Saturation: Adjust the image saturation level (0 to 100).
Contrast: Adjust the image contrast level (0 to 100).
Sharpness: Adjust the image sharpness level (0 to 100).
Detail enhancement: For thermal channel, adjust the details and edges of higher temperature image (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.

Normal	Vertical	Normal	Horizontal	Normal	Horizontal + Vertical
					

Exposure

Meter area is used to select the exposure area. Select Whole/Center spot/Center area for different area exposure settings.
Exposure mode: The exposure modes include:

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

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

White Balance (WB) Setting

Mode: Adjust the value for the best color temperature.

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

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

DayNight Setting

The day night mode settings vary based on device models.
D/N setting: It can be set to **Auto**, **Day mode**, **Night mode** or **Timing**.

- **Auto**

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

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

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

- **Day mode**

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

- **Night mode**

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

- **Timing**

The camera switches between day mode and night mode based on a specified schedule. Enter the start and end time for day mode. The time format is [hh:mm] and is expressed in 24-hour clock time. By default, the start and end time of day mode are set to 07:00 and 18:00.
DTN time: After selecting **Timing** for **D/N setting**, set **DTN time** to switch time for day mode to night mode
NTD time: After selecting **Timing** for **D/N setting**, set **NTD time** to switch time for night mode to day mode
Turn on illuminator in night mode: Select **Build-in IR illuminator** to enable the IR led light. Select **None** to disable it.
IR adjustment:

- **Manual**: Select it to control the luminance of IR lights manually. You can drag the slider to set the IR lights strength manually.

Noise Reduction

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

2D NR/3D NR: Reduce noise of image.
Max Strength: To get better 3D noise reduction performance, please choose a higher value to set.

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

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

Enhance Image

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

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

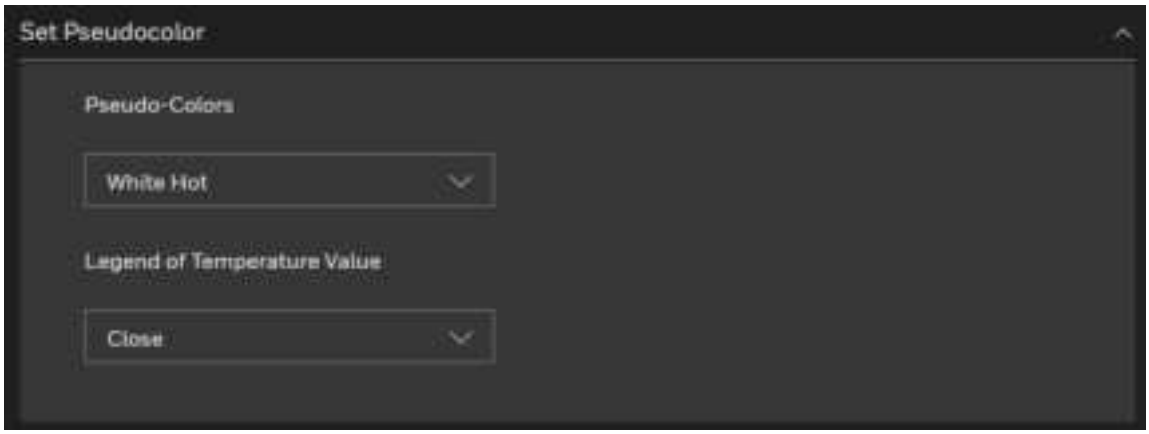
WDR (Wide Dynamic Range)
By lowering the brightness of the brightest area, and enhancing the brightness of the darkest area, WDR balances brightness and darkness in a scene so that both the darkest area and the lightest area can be seen clearly at the same time.
This value ranges from 1 to 100. The default value is 50.
BLC (Backlight Compensation)
The camera automatically adjusts the exposure to suit the conditions, so that the darkest area of the video can be seen.
This value ranges from 1 to 100. The default value is 50.
HLC (Highlight Compensation)
When the HLC function is enabled, the camera can lower the brightness of the brightest section of video, according to the selected HLC control level. HLC can reduce the amount of halo and lower the brightness of the entire video image.
This value ranges from 1 to 100. The default value is 50.
DeFog: Check the checkbox to enable defog. The image quality is compromised in foggy or hazy environment and defog can be used to improve image clarity.

Set Pseudocolor

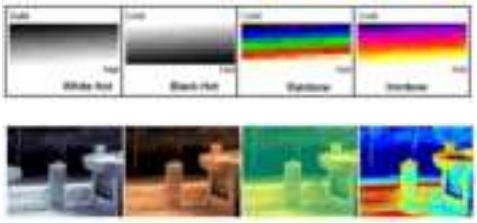
Go to **Setup > Camera Setup > Image Settings** and on the Channel drop-down list, choose channel 2. You can set pseudocolor on this page.

You can set pseudo-colors, legend on this page.

Figure 20 Set Pseudocolor



Pseudo-Colors: the temperatures of the temperature fields detected by the thermal imaging camera are separately mapped to values ranging from 0 to 255 by the algorithm. In the black/white display mode, this range is converted to the grayscale tones. For example, 0 indicates completely black, and 255 indicates completely white. The temperature field of the scene is converted to images by using the grayscale ranging from 0 to 255. Different polarity modes can be converted to different display images. The most common setting is white hot (a hotter object is displayed brighter than a colder object) or black hot (a hotter object is displayed darker than a colder object). The difference between two modes lies in that the temperatures corresponding to the darker one and the lighter one is reversed. Other modes include rainbow, ironbow, HSV, autumn, bone and so on.

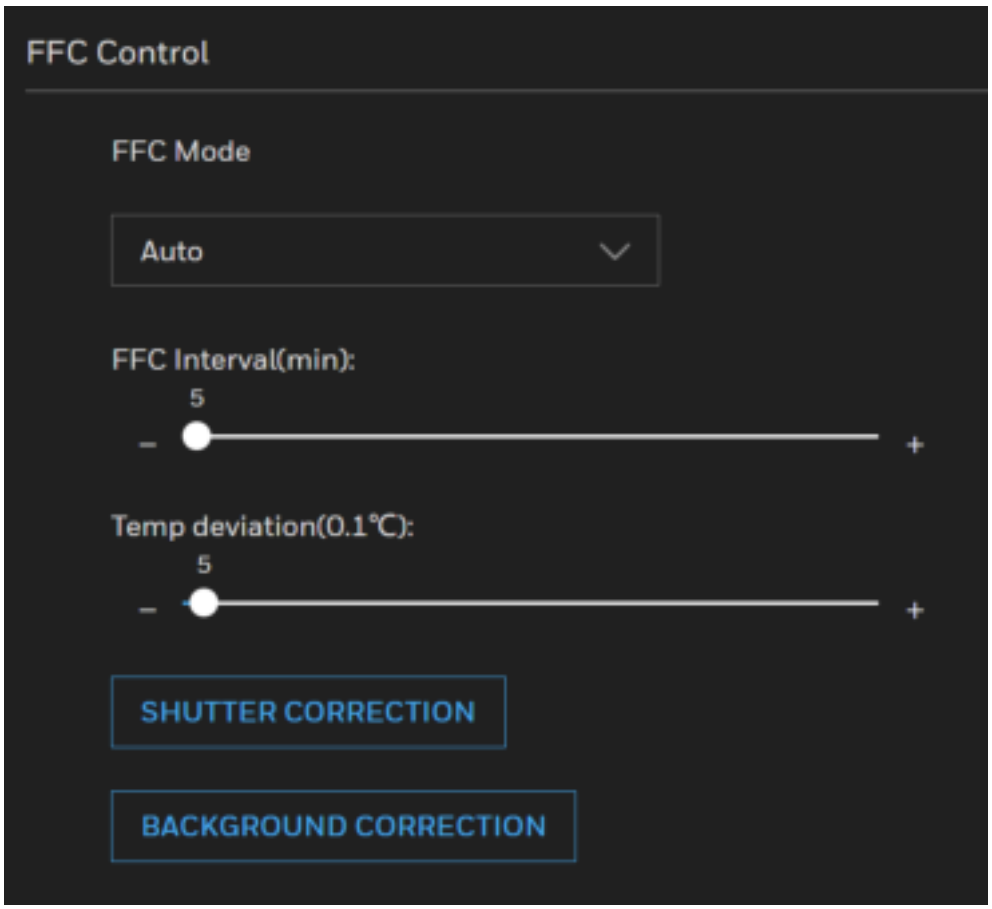


Legend of Temperature Value: If it is on, the Temperature bar will show in live video, otherwise there is no legend.

FFC Control

Go to **Setup > Camera Setup > Image Settings** and on the Channel drop-down list, choose channel 2. You can set **FCC Control** on this page.
The internal of the thermal imaging camera may comprise the mechanical action correction mechanism that can periodically improve the image quality. This component is called **flat field correction (FFC)**. When controlling the FFC, the FFC shields the sensor array, so that each portion of the sensor can collect uniform temperature fields (flat field).
By means of FFC, the camera can update the correction coefficients to output more uniform images. Throughout the FFC process, the video image is frozen for two seconds and a static-frame image is displayed. After the FFC is complete, the image is automatically recovered. Repeated FFC operations can prevent the grainy and image degradation problems. The FFC is especially important when the temperature of the camera changes. For example, after the camera is powered on or the ambient temperature is changed, you should immediately perform the FFC.

Figure 21 FFC Control

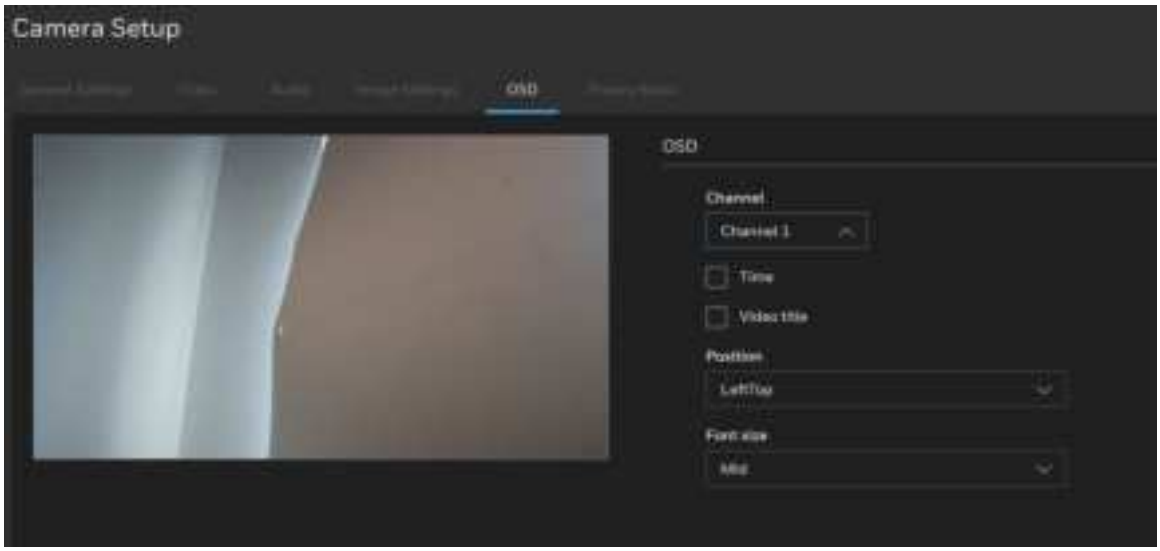


Auto: In the Automatic FFC mode, the camera performs FFC whenever its temperature changes by a specified amount or at the end of a specified period of time (whichever comes first). When this mode is selected, the FFC interval (minutes) ranges from 5 to 30 minutes. The temperature change of the camera is based on the temperatures collected by the internal temperature probe. The temperature of the camera sharply changes when the camera is powered on. The FFC is relatively frequent, which is normal.
Manual: In the manual FFC mode, the camera does not automatically perform the FFC based on the temperature change or the specified period. You can press the Do FFC button to select the manual FFC mode. When you feel that the image is obviously degraded but the automatic FFC is not performed, you can use the manual FFC function to check whether the image quality can be improved.
FFC Interval (min): In the automatic FFC mode, the FFC interval ranges from 5 to 255 minutes.

Temper deviation(0.1℃): In the automatic FFC mode, the FFC deviation range is from 0.2 to 25.5 centigrade.
SHUTTER CORRECTION: Click it to adjust exposure immediately.
BACKGROUND CORRECTION: Click it and cover the camera with something to adjust image. Remove the thing to finish adjustment.

Configuring OSD

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



Choose channel to set OSD.

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

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

Note: *At low resolution mode, if there are too many OSD characters it may be displayed incompletely.*

Position: Set the OSD display position.

Font size: Set the font size of OSD display.

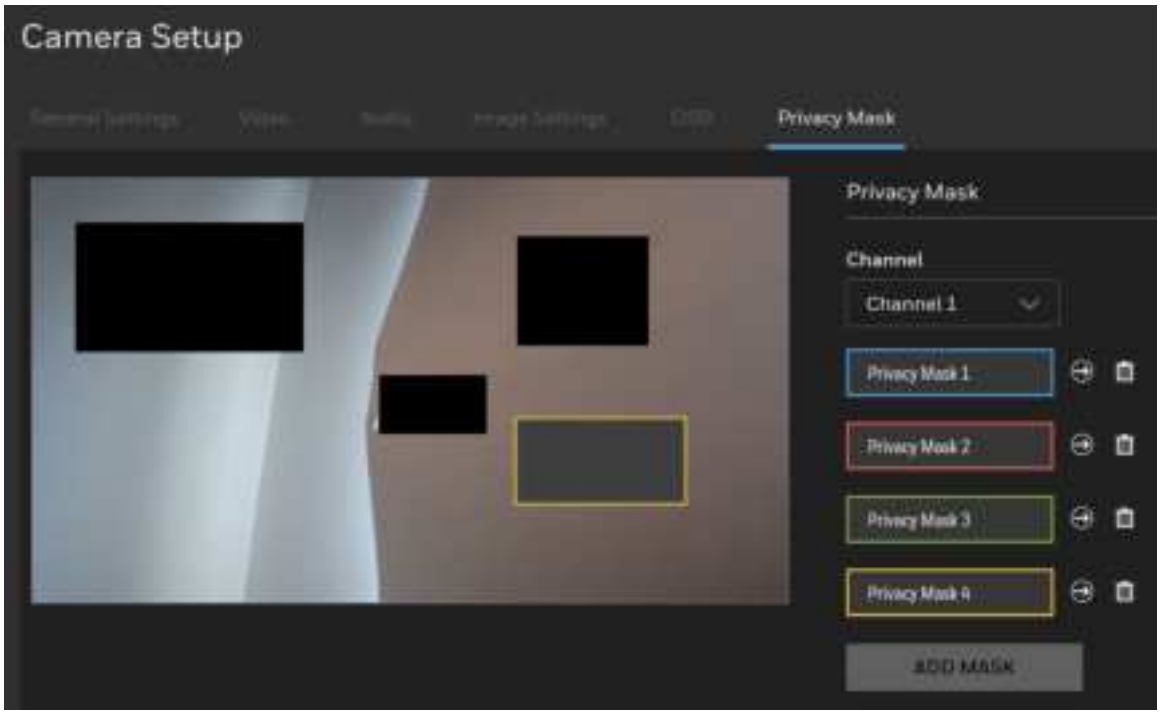
Configuring Privacy Mask

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

To configure privacy masks:

1. Choose channel to set privacy mask.
2. Click ADD MASK to add a new privacy mask window on the video screen.
3. Drag the corner of the rectangle to create a new masking window.
4. Enter a name for the privacy mask and click SAVE to enable the setting.

Figure 22 Privacy Mask



Note:

- *The object should be in the middle of the video screen and the setting size of privacy mask should be 1.5~2.5 times of the object size. (only for PTZ)*
- *If you want to delete the privacy mask window, click*  *on the right side of privacy mask window name. Click*  *to go to the relate privacy mask position.*
- *It supports up to 4 privacy masks.*

CHAPTER

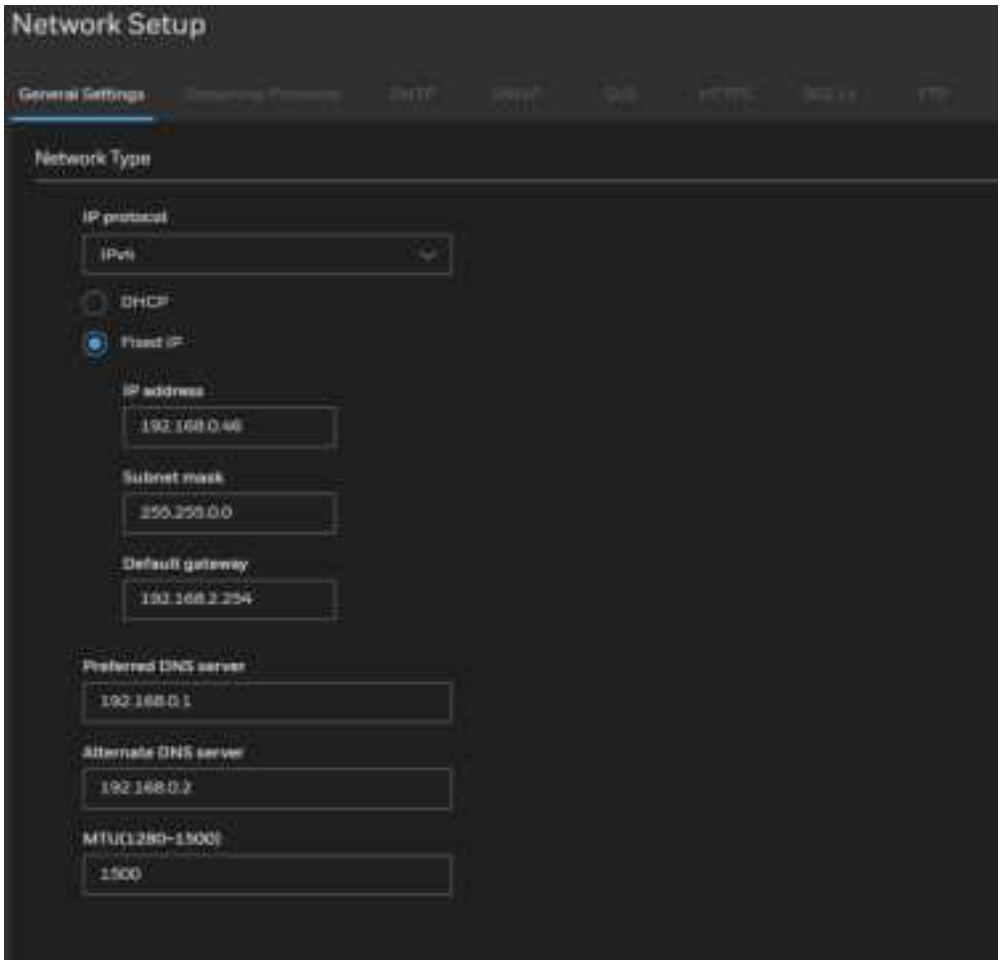
5 CONFIGURING NETWORK SETTINGS

Configuring Network General Settings

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

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

Figure 23 Network General Settings



Select IPv4/IPv6 for IP protocol.

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

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

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

IP address:

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

Enter the Static IP, Subnet mask, Default gateway, and Primary DNS provided by your ISP or network administrator.

Subnet mask: This is used to determine if the destination is in the same subnet. The default value is “255.255.255.0”.

Default gateway: This is the gateway used to forward frames to destinations in a different subnet. Invalid router setting will disable the transmission to destinations across different subnets.

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

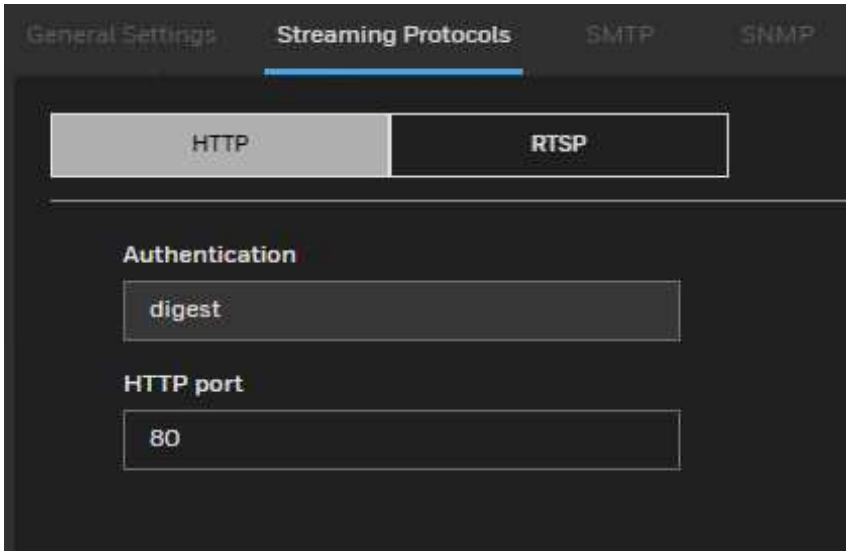
Alternate DNS Server: Secondary domain name server that backups the Primary DNS.

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

Configuring Streaming Protocols

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

Figure 24 Streaming Protocols-HTTP

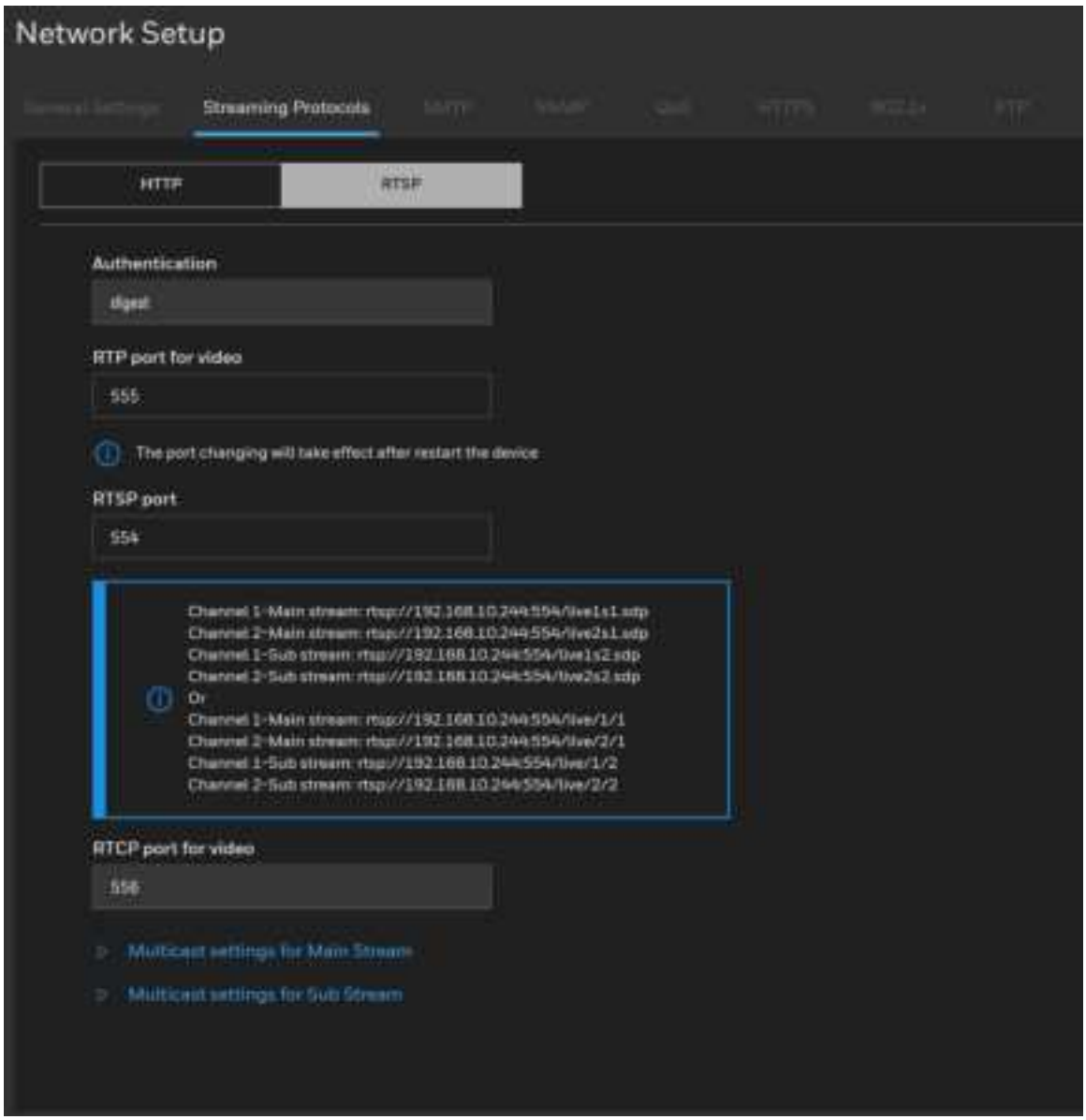


To utilize **HTTP** authentication, make sure that you have set a password for the camera first.

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

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

Figure 25 Streaming Protocols–RTSP



To utilize RTSP streaming authentication, make sure that you have set a password for controlling the access to video stream first.

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/live1/1<Streaming ID>.sdp*
- *rtsp://IP address: Port/live1/2<Streaming ID>.sdp*

Note: *IP address: The device IP address*
Port: RTSP port, default is 554
live1s1<Streaming ID>.sdp: liv1s1.sdp for Mainstream, liv1s2.sdp for Sub

stream.1 is optical channel, 2 is thermal channel.

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

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

   The live video will be displayed in your player.

   Channel 1-Main stream: *rtsp://192.168.10.244:554/live1s1.sdp*

   Channel 2-Main stream: *rtsp://192.168.10.244:554/live2s1.sdp*

   Channel 1-Sub stream: *rtsp://192.168.10.244:554/live1s2.sdp*

   Channel 2-Sub stream: *rtsp://192.168.10.244:554/live2s2.sdp*

- ***rtsp://IP address: Port/live/Camera ID/1/Streaming ID***
- ***rtsp://IP address: Port/live/Camera ID/2/Streaming ID***

Note: *IP address: The device IP address*
Port: RTSP port, default is 554
Live: Keep Live as default.
Camera ID: 1
1 is optical channel, 2 is thermal channel
Streaming ID: 1 for Mainstream, 2 for Sub stream.

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

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

   The live video will be displayed in your player.

   Channel 1-Main stream: rtsp*://192.168.10.244:554/live/1/1*

   Channel 2-Main stream: rtsp*://192.168.10.244:554/live/2/1*

   Channel 1-Sub stream: rtsp*://192.168.10.244:554/live/1/2*

   Channel 2-Sub stream: rtsp*://192.168.10.244:554/live/2/2*

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

- The RTP (Real-time Transport Protocol) is used to deliver video data to the clients. By default, the RTP port for video is set to 555.
- RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default, the RTSP port number is set to 554.
- The RTCP (Real-time Transport Control Protocol) allows the camera to transmit the data by monitoring the Internet traffic volume. By default, the RTCP port for video is set to 556.

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

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

Multicast group address: Enter the Multicast group address.

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

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

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

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

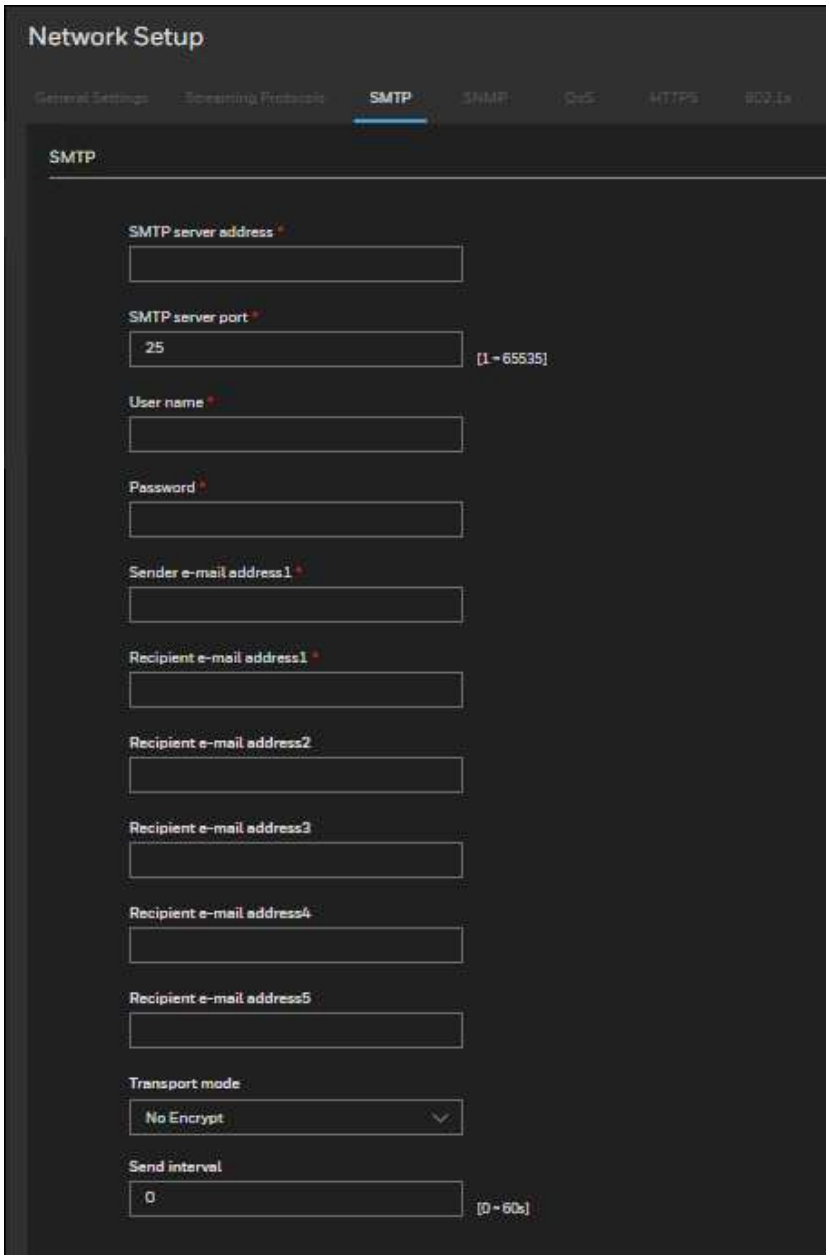
Note: *Multicast is enabled by default in camera.*

Configuring SMTP Settings

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

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

Figure 26 SMTP Settings



SMTP server address: IP address of the SMTP server.

SMTP server port: Port number of the SMTP server.

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

Password: Password of the mailbox for sending emails.

Sender e-mail address1: Mailbox for sending emails.

Recipient_e-mail_address1: Email address of recipient 1.

Recipient_e-mail_address2: Email address of recipient 2.

Recipient_e-mail_address3: Email address of recipient 3.

Recipient_e-mail_address4: Email address of recipient 4.

Recipient_e-mail_address5: Email address of recipient 5.

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

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

Configuring SNMP Settings

Go to **Setup > Network Setup > SNMP**.

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

The SNMP consists of the following three key components:

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

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

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

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

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

Trap address: IP address of the trap.

Trap port: Management port of accepting message from trap.

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

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

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

Read security name: Name of read security.

Write security name: Name of write security.

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

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

Auth algorithm: Authentication Algorithm, includes MD5and SHA.

Auth password: Authentication password.

Encry Algorithm: Encryption Algorithm, includes DES and AES.

Encry Password: Encryption password.

SNMP Port: Port of SNMP.

Configuring QoS Settings

Go to **Setup > Network Setup > QoS**.

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

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

- All network switches and routers in the network must include support for QoS.
- The network video devices used in the network must be QoS-enabled.

Configuring HTTPS Settings

HTTPS

Go to **Setup > Network Setup > HTTPS > HTTPS**.

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

Figure 27 HTTPS Settings

Note: *Honeywell strictly recommends using HTTPS only.*

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

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

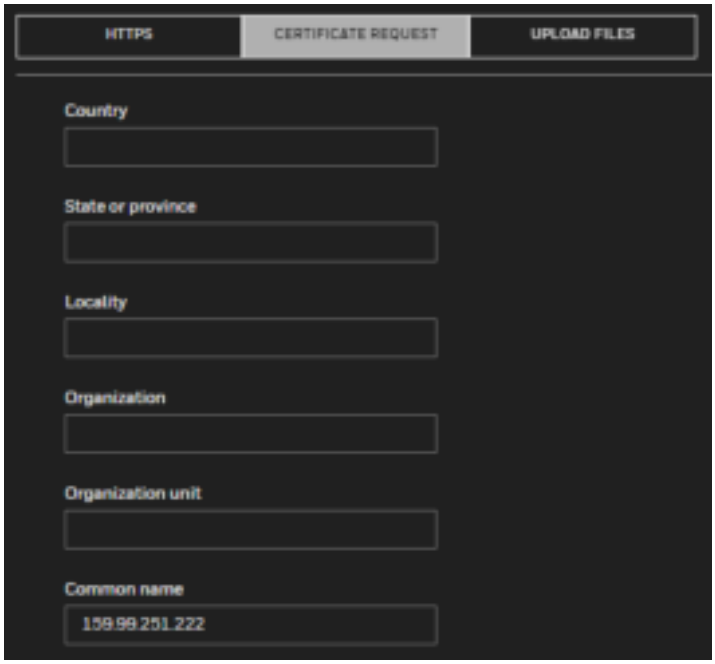
HTTPS only: Select it and the web browser can only be accessed via HTTPS with higher security level.

Note: *When the stream of camera is switched to http&https or https only, the signal will be interrupted for 3min, then it will be recovered automatically.*

Certificate Request

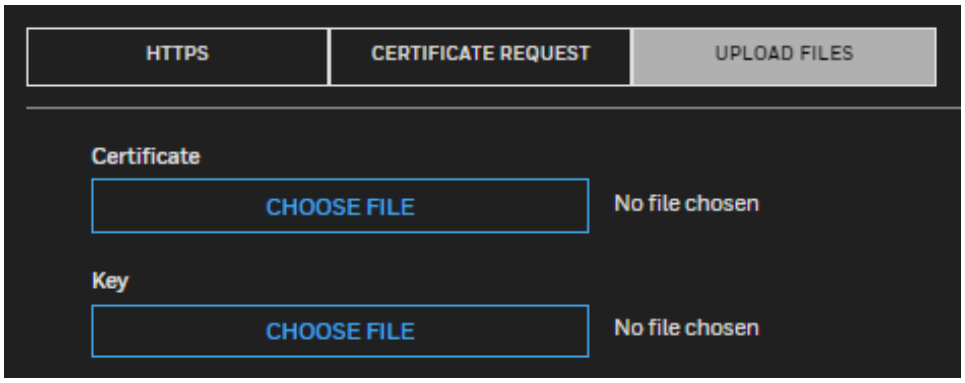
Go to **Setup > Network Setup > HTTPS > CERTIFICATE REQUEST**. You can create the certificate request here.

Figure 28 Certificate Request



Upload Files

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



To import the certificate from third party:

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

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

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

  Supported Key format: PEM format.

Configuring IEEE 802.1x Settings

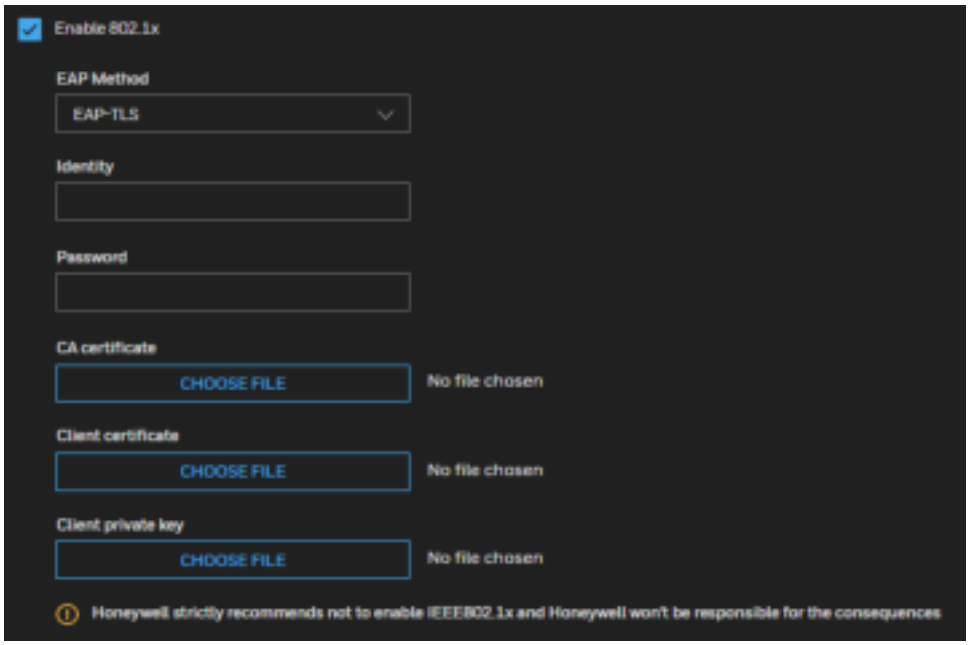
Go to **Setup > Network Setup > 802.1x**.

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

To configure IEEE 802.1x settings:

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

Figure 29 IEEE 802.1x Configurations – EAP-TLS



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

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

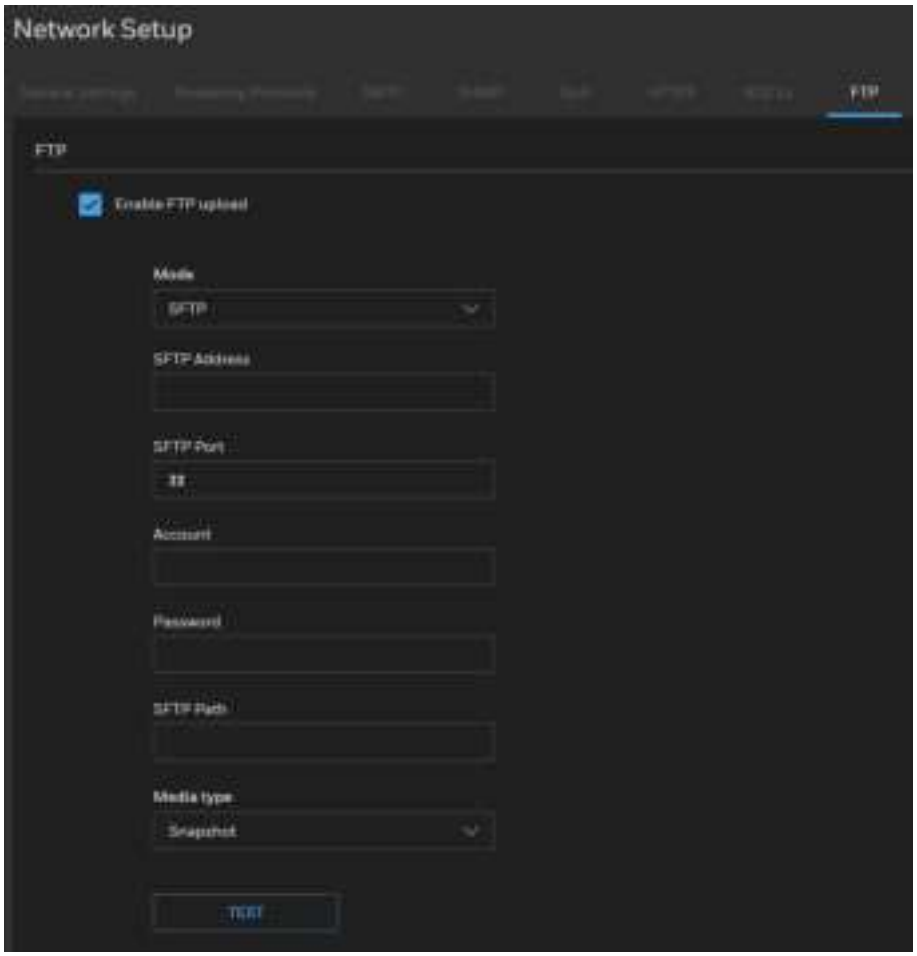
3. When all settings are complete, move the camera to the protected LAN by connecting it to an 802.1x enabled switch. The devices will then start the authentication automatically.

Configuring FTP Settings

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

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

Figure 30 File Transfer Protocol (FTP)



Enable FTP upload: Check to enable the FTP service

Mode: SFTP, FTPS, FTP

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

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

Account: FTP server account

Password: FTP server password

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

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

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

Click **SAVE** to save the settings.

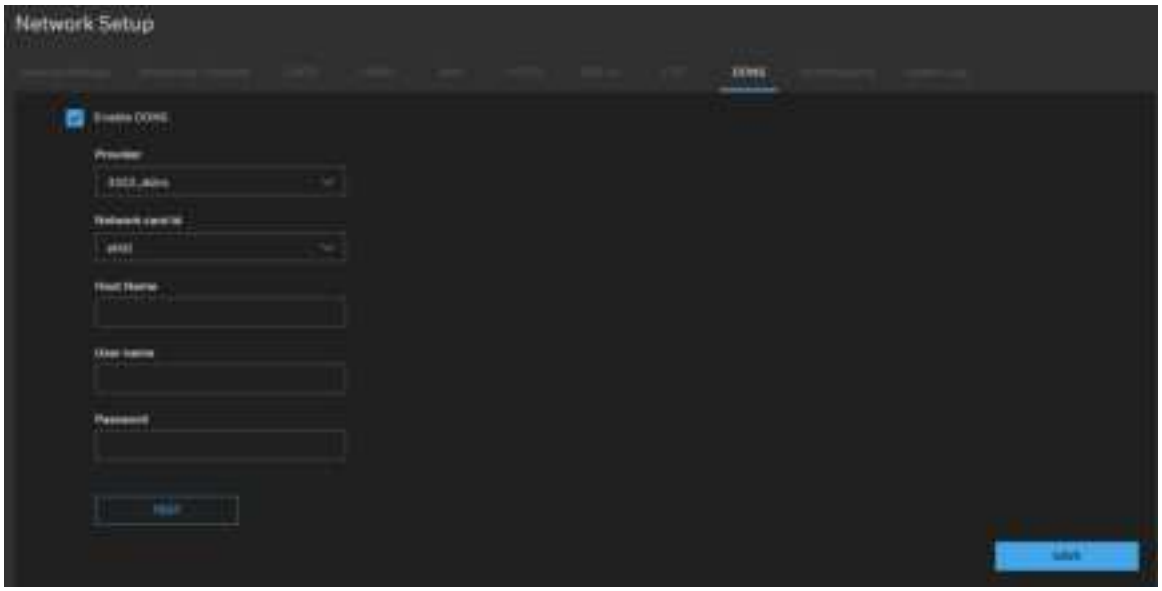
Configuring DDNS

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

1. Go to Setup > Network Setup > DDNS.

   The DDNS interface is displayed.

Figure 31 DDNS Interface



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

Configuring Port Mapping

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

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

   The Port Mapping interface is displayed.

Figure 32 Port Mapping Interface

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

Table 4 Port Mapping Parameters

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

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

5. Click SAVE to complete the settings.

   In the browser, enter http:// IP: HTTP port. You can visit the LAN Device.

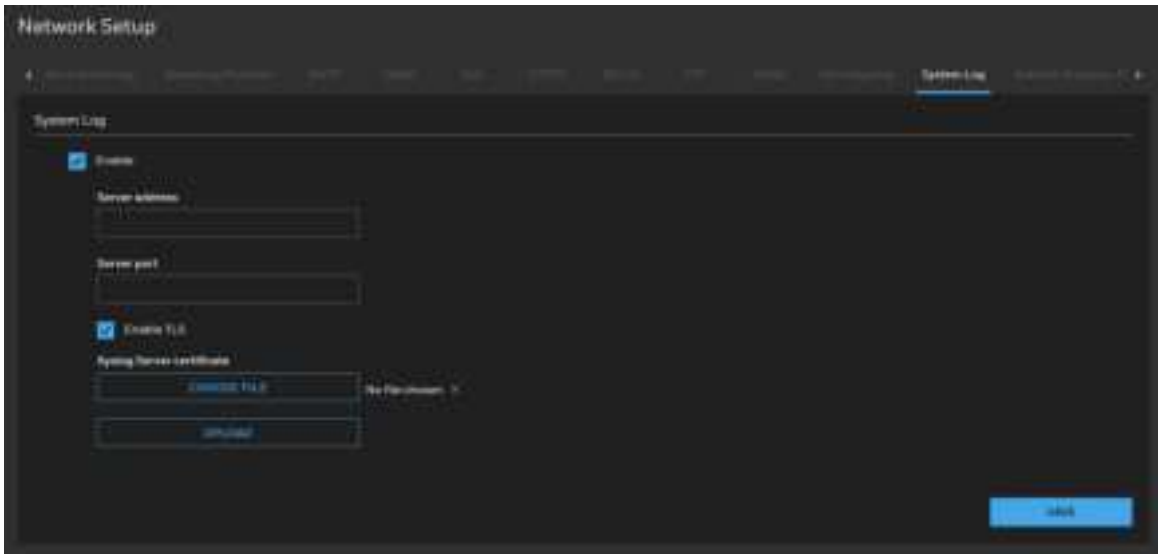
Configuring System Log

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

1. Go to Setup > Network Setup > System Log.

   The System Log interface is displayed.

Figure 33 System Log Interface



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

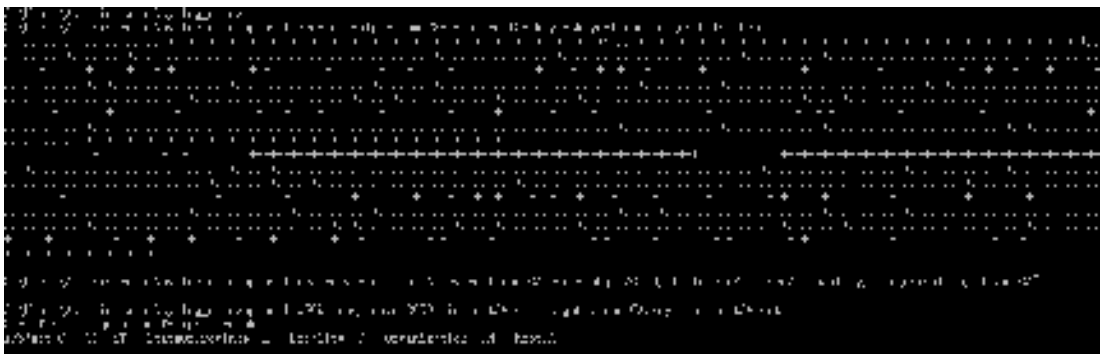
Execute the command to generate the root certificate and private key, where rootCA.key is the root certificate private key; rootCA.crt is the root certificate.

The detail commands are:

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

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

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



   f) Execute the command to generate the sub-certificate and private key,

where server.key is the private key 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

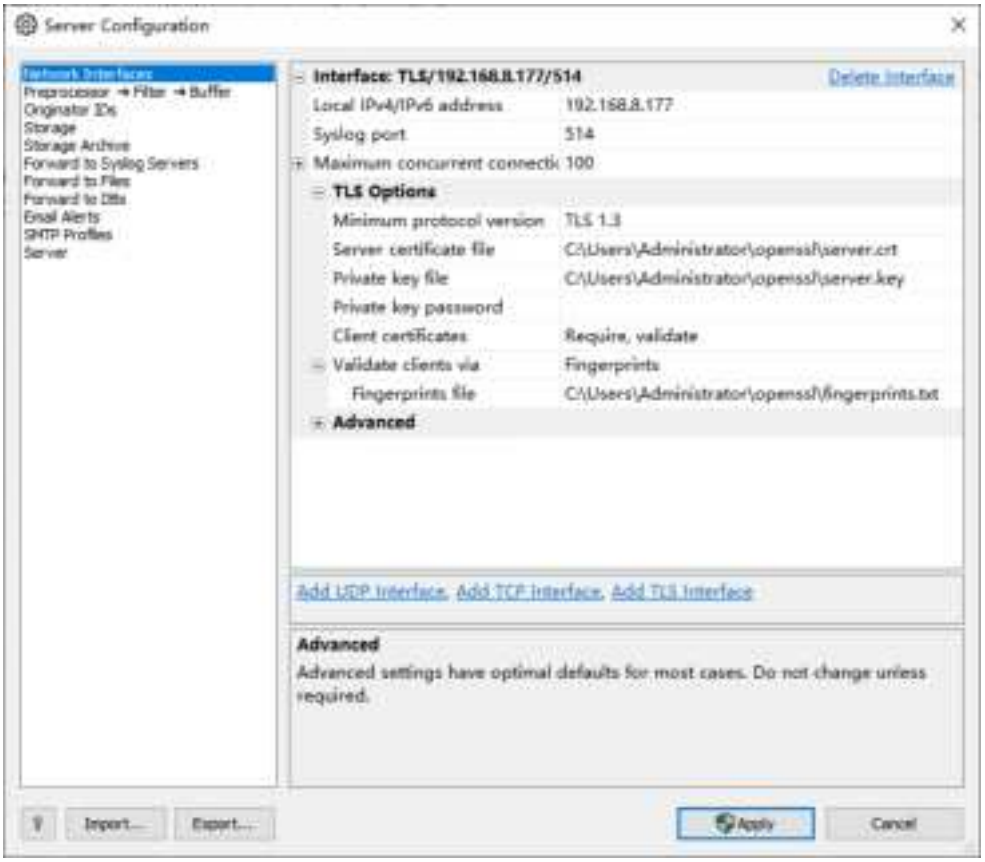
g) certificate fingerprint acquisition Assume that cacert.crt is the certificate from the device.

The detail command is:

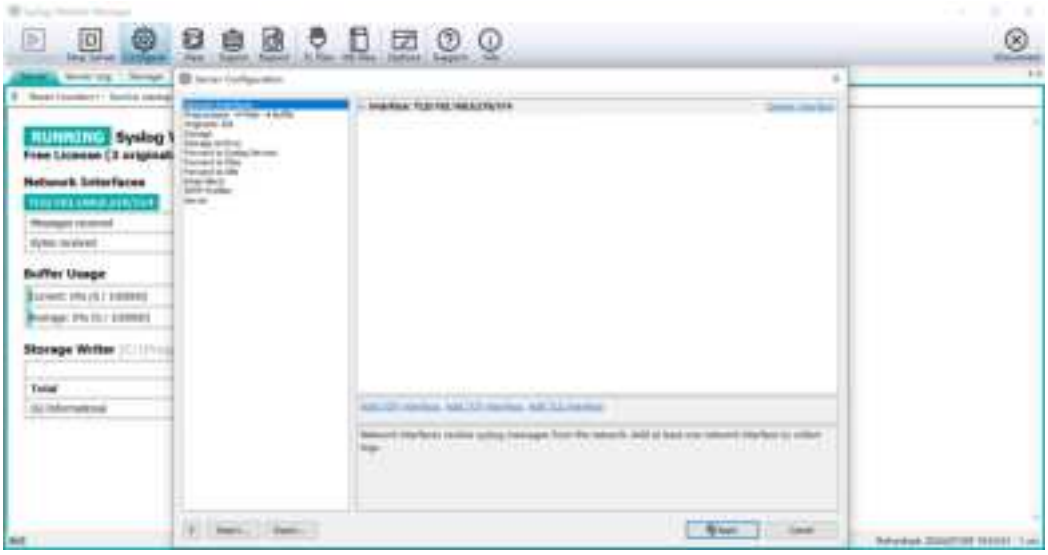
openssl x509 -in cacert.crt -fingerprint -sha1 > fingerprints.txt

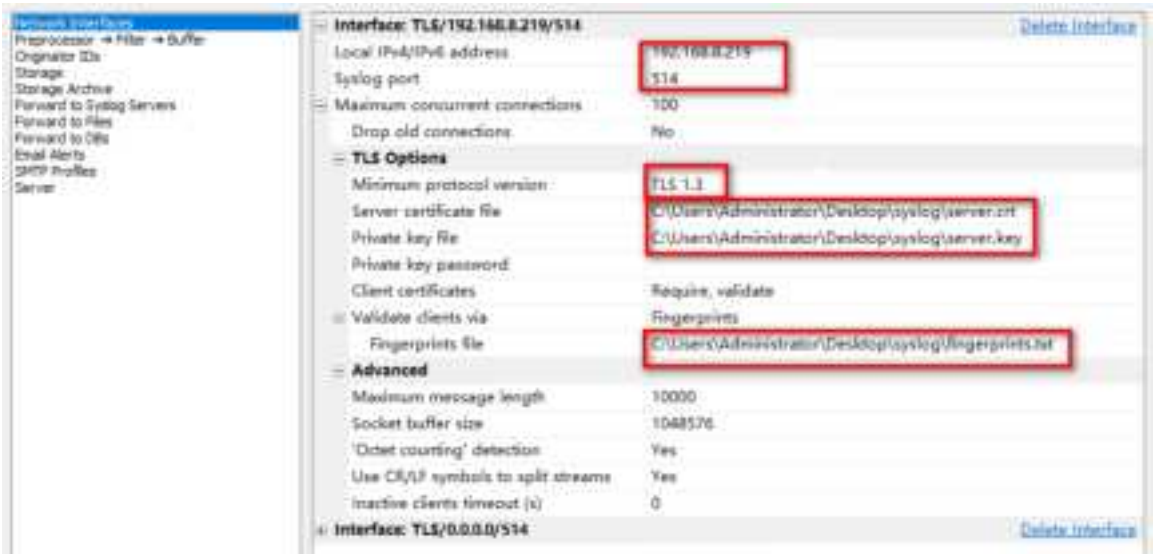
Modify the fingerprints format of the certificate fingerprints.txt

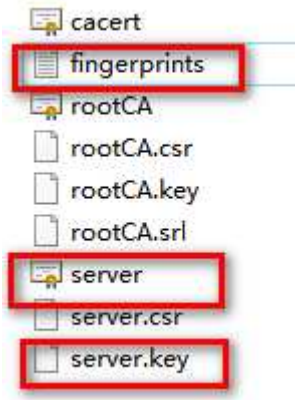
3. Install Syslog Watcher Manager and open it.



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







5. Set the web of camera.

6. Test the settings, the system logs are sent to Syslog Watcher Manager, it is set succeeded. Otherwise it is failure, you should check steps.

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

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

Configuring Network Discovery Protocols

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

Figure 34 Network Discovery Protocols

CHAPTER

6 CONFIGURING VIDEO ANALYTICS

Video Analytics provides the following features: motion detection, smart motion, scene change, intrusion, multi loitering, people counting, face detection, line crossing detection, unattended detection, and missing object detection. Video Analytics detects one or a group of the following objects:

- Vehicle
- Human

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

Installation Instruction

Model	Detection distance of optical channel	Detection distance of thermal channel
HC35TE5R3JT21	Face: 3~4 m Human: 3 ~27 m Vehicle: up to 90 m	Human: 2~16 m Vehicle: up to 42m Smoker: 2-10 m
HC35TE5R4JT35	Face: 3~4 m Human: 3 ~27 m Vehicle: up to 165 m	Human: 4~16m Vehicle: up to 90m Smoker: 3.5 ~12.5m
HC35TB5R1JT07	Face: 9~10 m Human: 9~38 m Vehicle: up to 195 m	Human: 10~32 m Vehicle: up to 140m Smoker: 8-15 m
HC35TB5R4JT10	Face: 9~10 m Human: 9~38 m Vehicle: up to 195 m	Human: 11~ 38 m Vehicle: up to 210m Smoker: 11-18 m

Figure 35 Installation (human)

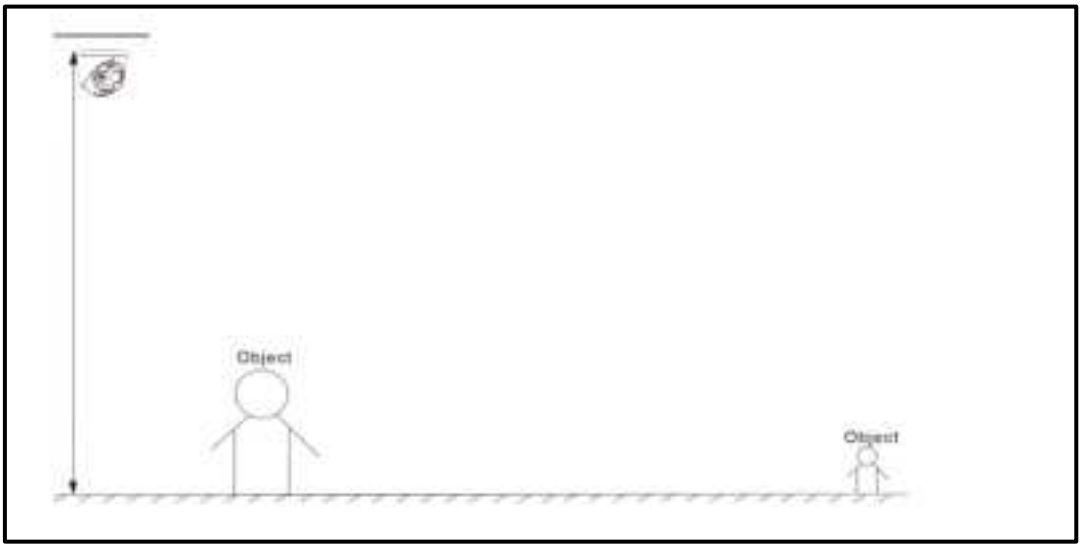


Figure 36 Installation (vehicle)

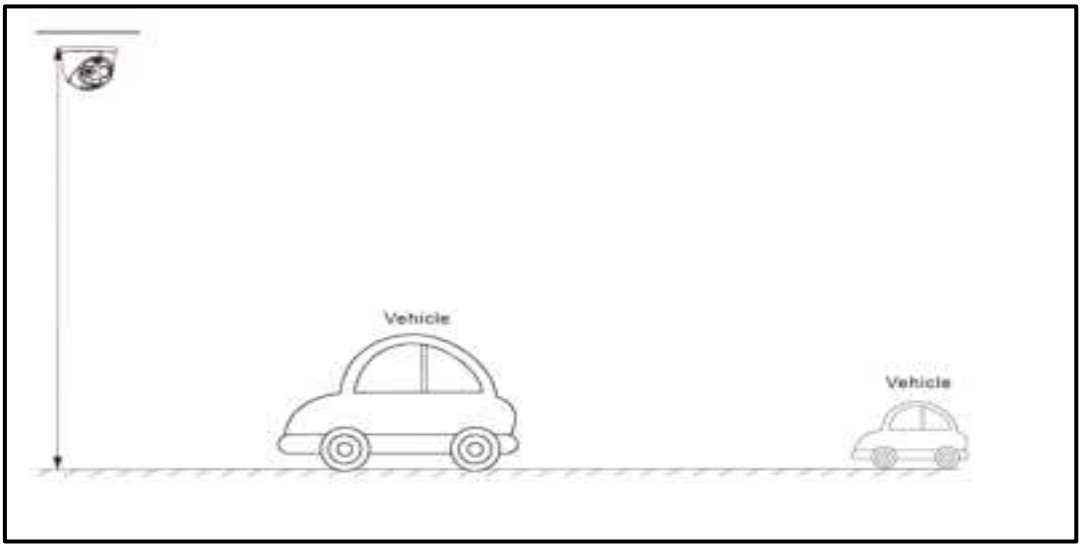
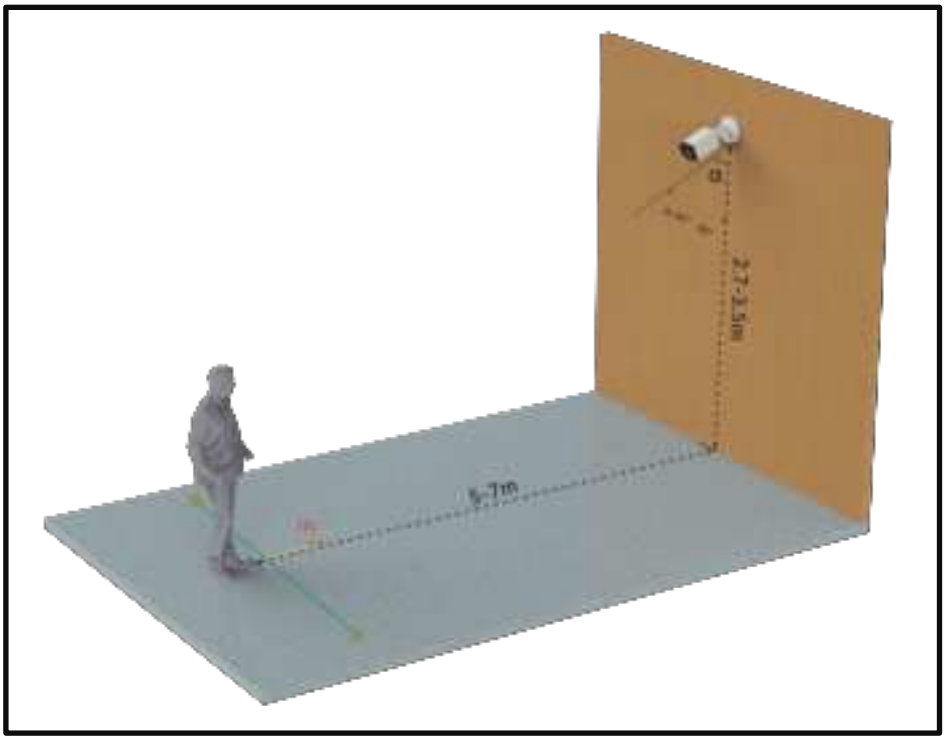


Figure 37 Installation Angle (For People Counter)



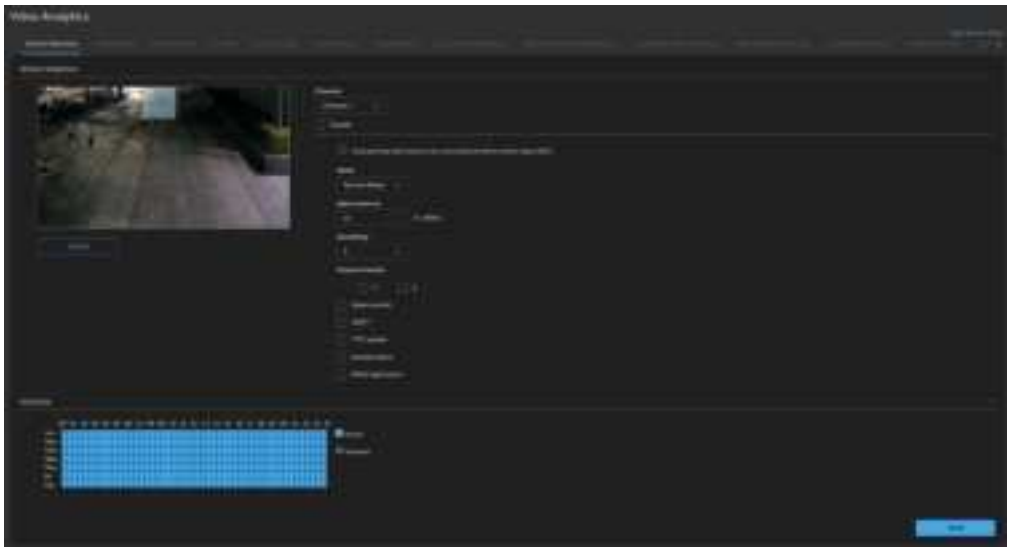
Motion Detection

When the motion detection function is enabled, the camera detects that an object moves into the motion detection area within the schedule time, the camera generates an alarm and triggers linkage alarm output.

Both of the two channels support it.

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

Figure 38 Motion Detection



2. Choose the channel from the drop-down list. Channel 1 is optical channel; Channel 2 is thermal channel.
3. Check the Enable checkbox to enable motion detection.
4. Set Mode.

   For 35 series cameras, users can choose mode to set, **Normal Mode** and **Preset point mode.**

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

   Preset point mode: choose one preset, which is set in advance, the lens jumps to the preset point, the detection area is set at the preset point.
5. Configure the Alarm interval and Sensitivity.

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

   For example, 10 is the highest sensitivity value and the motion will be the easiest to be detected. But it will probably trigger some false alarms.

   1 is the lowest sensitivity value and the motion will be the hardest to be detected. But it will rarely trigger false alarms.
6. Configure the detection area.
   a) Press and hold the left mouse button, and drag in the video area to draw a detection area
   b) Click CLEAR to delete a detection area
7. Select the Output channel.
8. Check the linkage actions Alarm record, SMTP, FTP upload, Audible alarm and White light alarm.

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

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

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

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

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

   White light alarm: it will be flashing to alarm when alarm happened if you selected the white light alarm. The light will be always on when alarm duration, at **Thermal > Led Control > Lighting mode** is set **Alarm on**.
9. Set 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.
10. Click SAVE.

Smart Motion

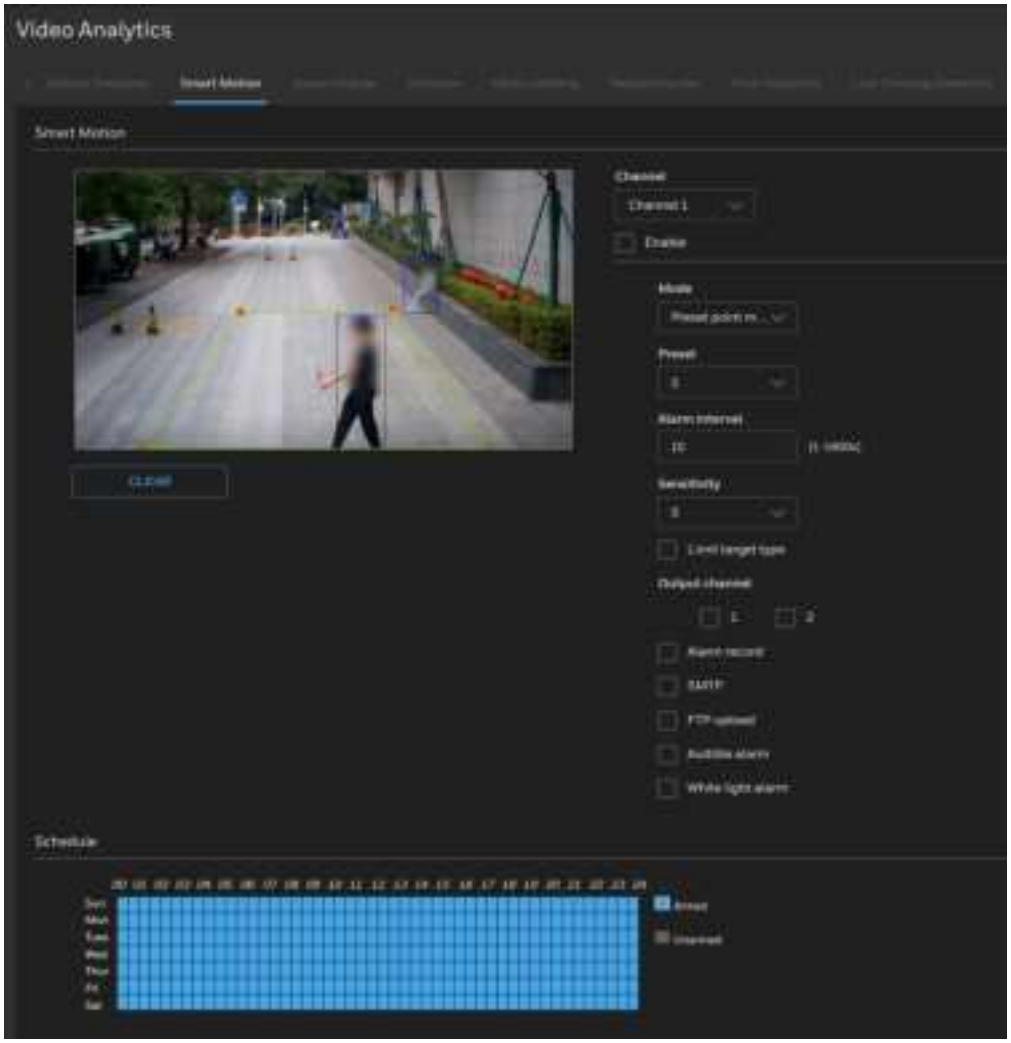
After configuring an area for defense, it will generate the alarm information when someone or something intrudes in the area.

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

Both of the two channels support it.

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

Figure 39 Smart Motion



2. Choose the channel from the drop-down list. Channel 1 is optical channel; Channel 2 is thermal channel.
3. Check the Enable checkbox to enable smart motion detection.
4. Set **Mode**.

   For 35 series cameras, users can choose mode to set, **Normal Mode** and **Preset point mode.**

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

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

5. Configure the Sensitivity.

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

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

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

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

Note: *Users can set up to 6 zones for smart motion detection.*
The smart detection can't be triggered by human on thermal channel, becaus the human is too large for thermal lens, they will be filtered.

7. Select the Output channel.
8. Check the check boxes to enable Alarm record, SMTP, FTP upload, Audible alarm and White light alarm.

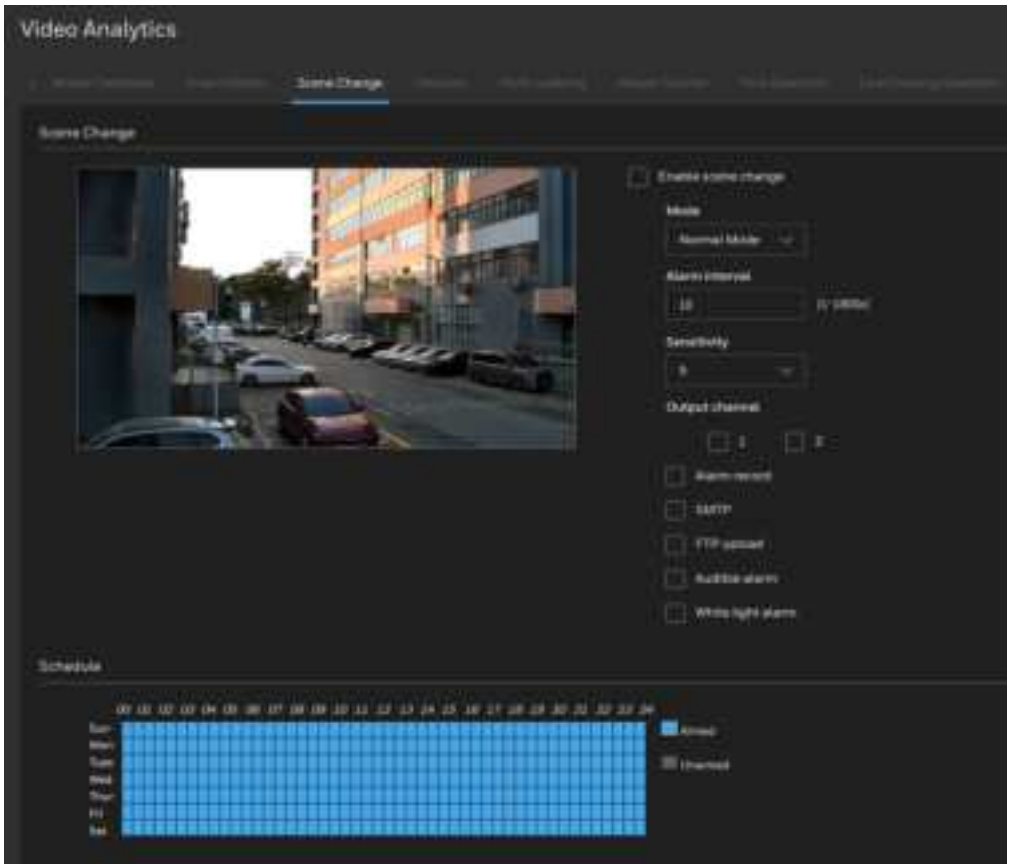
   The detail information please refer to Motion Detection, page 52.
9. Set Schedule. Use the mouse to drag the time or click the time grid to choose time one hour by hour. The blue means armed, and the gray means unarmed.
10. Click SAVE.

Scene Change

Note: *This VA function is only supported for optical channel.*

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

Figure 40 Scene Change



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

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

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

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

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

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

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

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

2. Select the Output channel.
3. Check the check boxes to enable Alarm record, SMTP, FTP upload, Audible alarm and White light alarm.

   The detail information please refer to Motion Detection, page 52.

Note: *The scene change triggers audio playing, and the audio alarm will play just one time. It*

will not play repeatedly as Camera Setup > Audio > Audio File > CYCLE NUMBER.
The scene change need cover at least 10s to trigger

4. Set 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.

5. Click SAVE.

Intrusion Detection

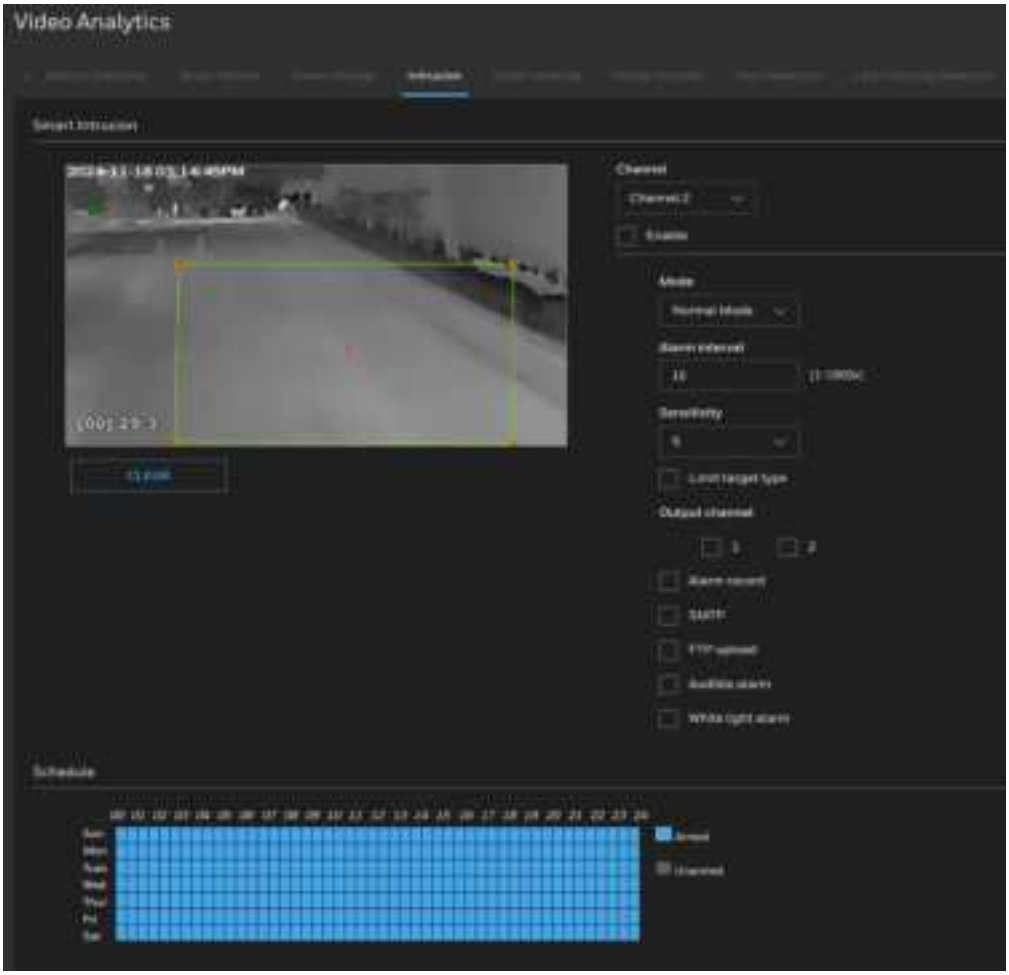
Intrusion can be used to detect 1~5 objects entering or moving in a restricted area in the camera field of view.

The applicable scenarios of this feature can be:

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

1. Go to Setup > Video Analytics > Intrusion.

Figure 41 Intrusion Detection



2. Choose the channel from the drop-down list. Channel 1 is optical channel; Channel 2 is thermal channel.
3. Check the Enable checkbox to enable intrusion detection.
4. Mode: For 35 series cameras, users can choose mode to set, Normal Mode and Preset point mode.

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

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

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

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

   1 is the lowest sensitivity value and the intrusion will be the hardest to be detected. But it will rarely trigger false alarms.
6. Configure the detection area.
   a) Press and hold the left mouse button, and drag in the video area to draw a detection area
   b) Click CLEAR to delete a detection area.

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

7. Select the Output channel
8. Check the check boxes to enable Alarm record, SMTP, FTP upload, Audible alarm and White light alarm.

   The detail information please refer to Motion Detection, page 52.
9. Set 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.
10. Click SAVE.

Multi Loitering

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

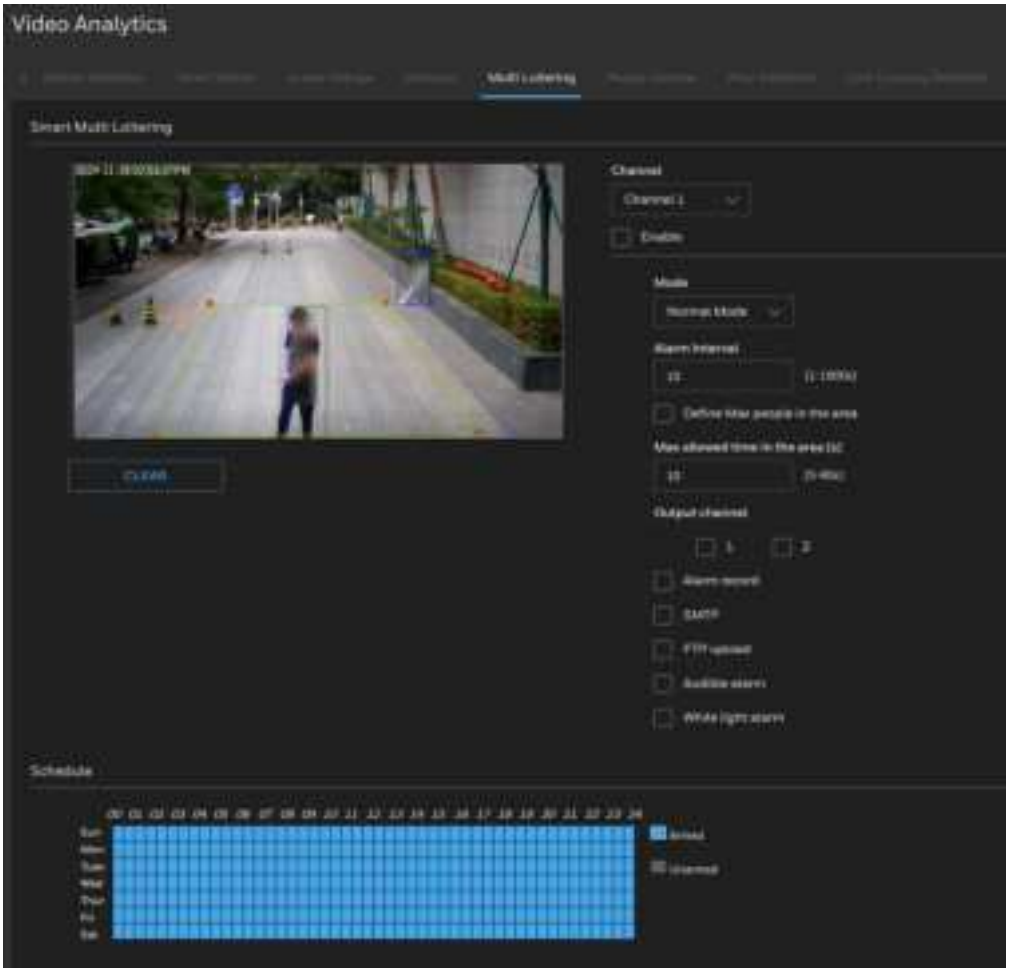
The applicable scenarios of this feature can be:

- Detects when a person is loitering at a walk-up of ATM lane.
- Detects when a person is loitering in a high-theft area of a store, or to prevent vandalism and break-ins.

- Detects when a person is loitering in an area that is normally not an access for visitors.

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

Figure 42 Multi Loitering



2. Choose the channel from the drop-down list. Channel 1 is optical channel; Channel 2 is thermal channel.
3. Check the Enable checkbox to enable multi loitering detection.
4. **Set Mode**. For 35 series cameras, users can choose mode to set, **Normal Mode** and **Preset point mode.**

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

   Preset point mode: choose one preset, which is set in advance, the lens jumps to the preset point, the detection area is set at the preset point.
5. Check the checkbox of Define Max people in the area.
6. Configure Max number of people in the area.
7. Configure Max allowed time in the area (s).
8. Configure the detection area.
   a) Press and hold the left mouse button, and drag in the video area to draw a detection area
   b) Click CLEAR to delete a detection area.

9. Select the Output channel.
10. Check the check boxes to enable Alarm record, SMTP, FTP upload, Audible alarm and White light alarm.

    The detail information please refer to Motion Detection, page 52.
11. Set 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.
12. Click SAVE.

People Counter

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

The applicable scenarios of this feature can be:

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

The inappropriate scene of this feature can be:

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

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

- The camera is facing the direction of the flow of people, as shown in Figure 43 .

Figure 43 View of Facing the Flow of People

- The camera is facing the side way direction of the flow of people, as shown in Figure 44.

Figure 44 Facing the Side Way Flow of People

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

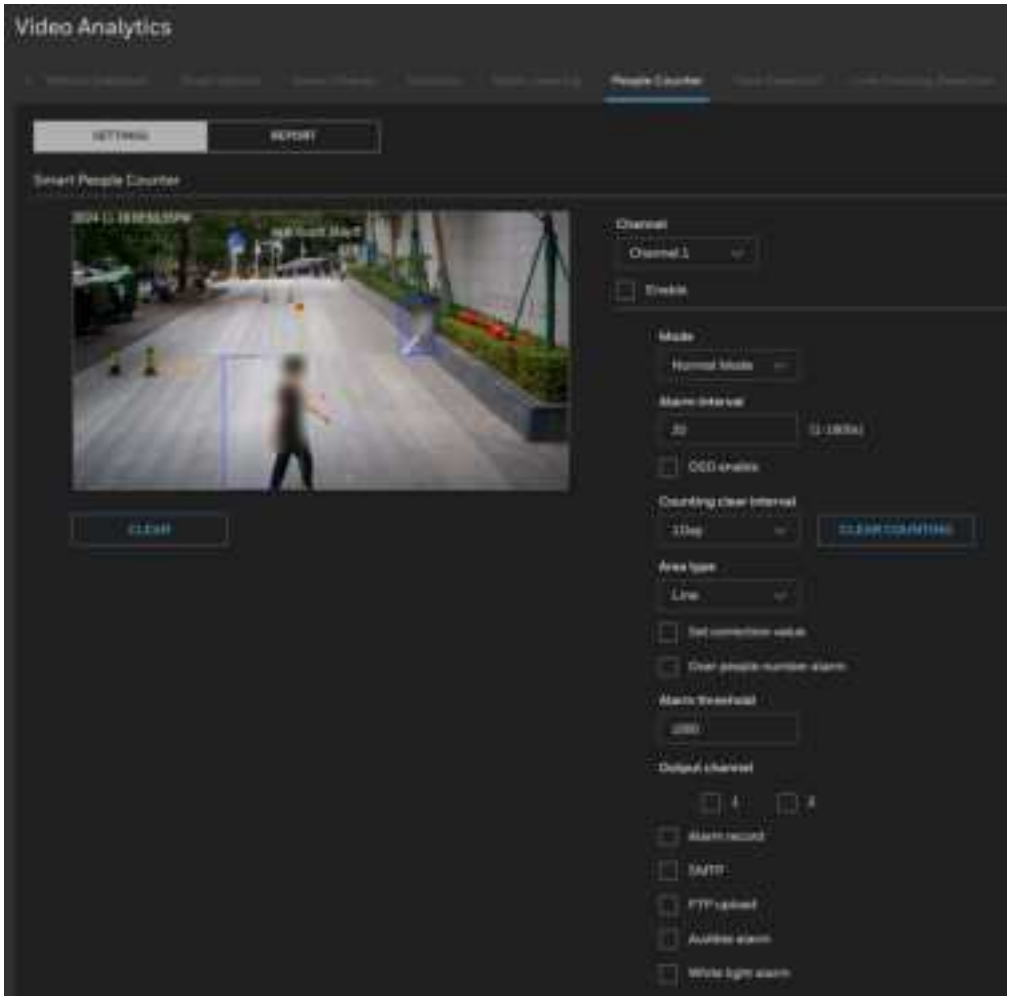
- The movement direction of the flow of people is relatively uniform, and there is no wandering.
- There is no interleaving and no overlapping between the flowing of people, otherwise it will affect the accuracy.
- The movement speed is not too fast, and the movement track time in the detection area is not too short.
- There are no obstructions in the visual field, try to choose a single background such as the ground and wall
- Avoid complex scenes with frequent changes in light, backlight, and direct light.
- The height and angle need to be adjusted according to the actual scene effect. The installation height is 3m~3.5m and the installation angle is 25°~45° for

verification.

- The line area needs to be in the middle of the screen, and there is at least 2s for the target movement track.

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

Figure 45 People Counter



Choose the channel from the drop-down list. **Channel 1** is optical channel; **Channel 2** is thermal channel.

Enable: Check the checkbox to enable the people counter.

Mode: For 35s cameras, users can choose mode to set, **Normal Mode** and **Preset point mode.**

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

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

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

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

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

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

Figure 46 Line of People Counter

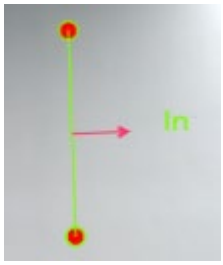
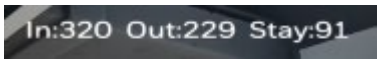


Figure 47 Number for In / Out / Stay



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

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

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

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

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

Check the check boxes to enable **Alarm record, SMTP, FTP upload, Audible alarm** and **White light alarm.**

The detail information please refer to **Motion Detection**, page **52.**

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

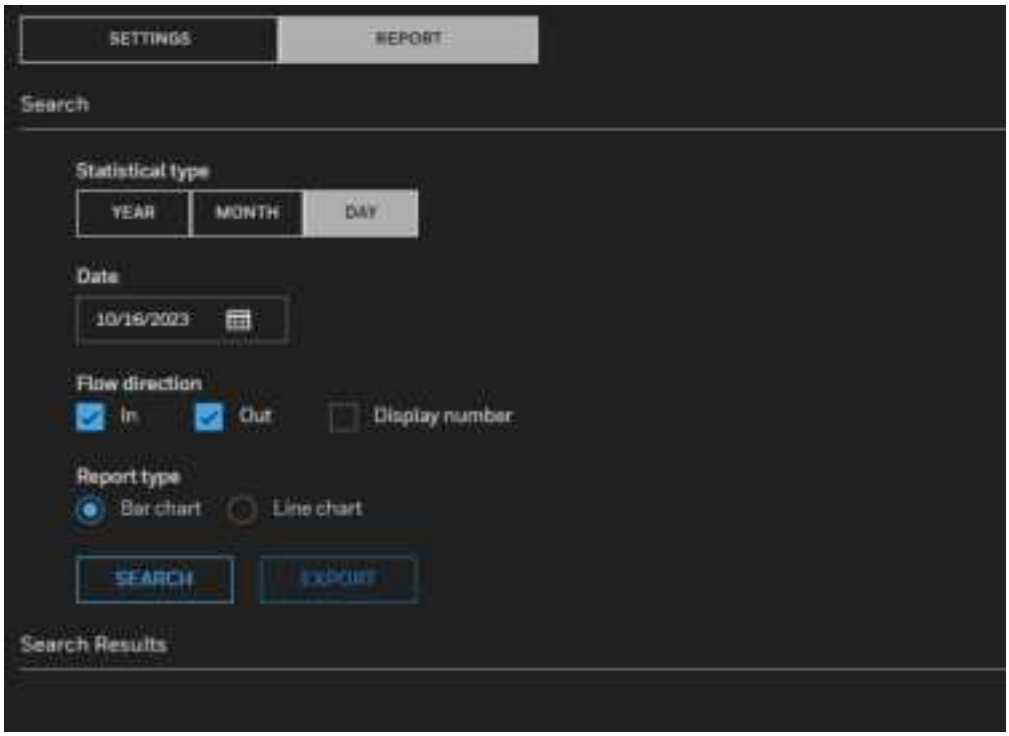
It is set on the corridor, or doorway.

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

Report

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

Figure 48 People Counter-REPORT



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

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

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

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

Users can search the statistic or export the results to local folder. The search results can show on the page directly.

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

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

Face Detection

Note: *This VA function is only supported for optical channel.*

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

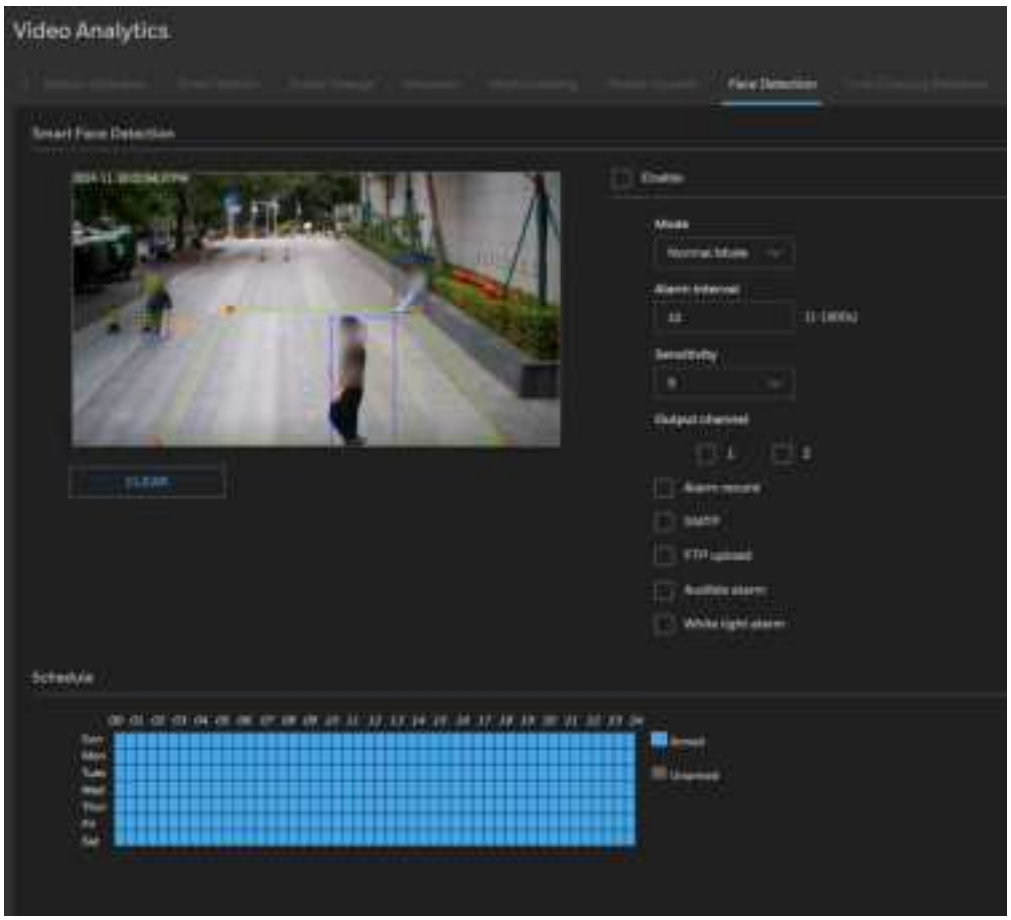
The applicable scenarios of this feature can be:

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

The inappropriate scene of this feature can be:

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

Figure 49 Face Detection



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

Choose the channel from the drop-down list. **Channel 1** is optical channel; **Channel 2** is thermal channel.

Enable: Check the checkbox to enable the face detection.

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

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

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

Mode: For 35s cameras, users can choose mode to set, **Normal Mode** and **Preset point mode.**

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

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

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

Check the check boxes to enable **Alarm record, SMTP, FTP upload, Audible alarm** and **White light alarm.**

The detail information please refer to **Motion Detection,** page **52.**

CLEAR: Clear the areas of setting. Use the mouse left-click and hold, end the draw to release the left mouse button.

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

Line Crossing Detection

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

The applicable scenarios of this feature can be:

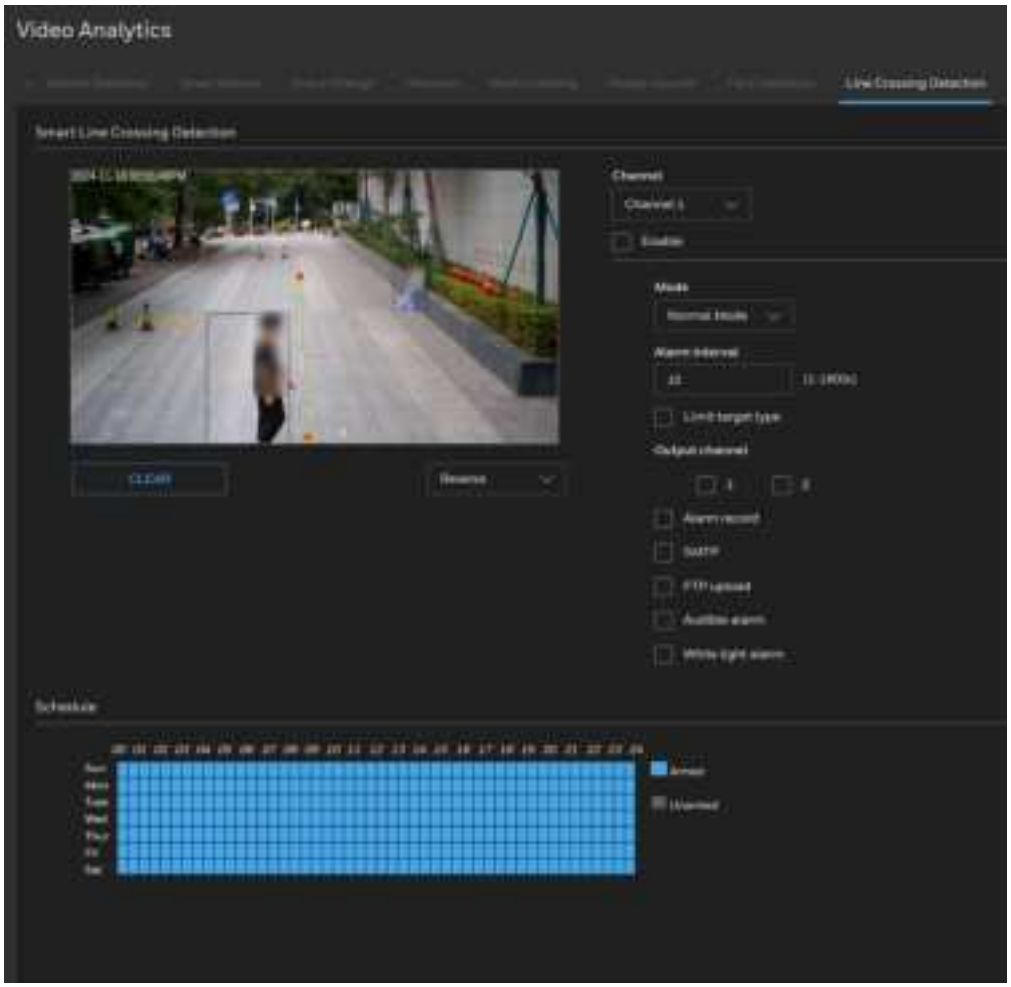
- There are specifies scene that forbidden humans / vehicles crossing the detection line.

The inappropriate scene of this feature can be:

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

- When the camera is perpendicular to the ground.

Figure 50 Line Crossing Detection



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

Choose the channel from the drop-down list. **Channel 1** is optical channel; **Channel 2** is thermal channel.

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

Mode: For 35s cameras, users can choose mode to set, **Normal Mode** and **Preset point mode.**

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

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

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

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

Check the check boxes to enable **Alarm record, SMTP, FTP upload, Audible alarm** and **White light alarm.**

The detail information please refer to **Motion Detection**, page **52.**

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

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

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

Double Line Crossing Detection

Double Line Crossing Detection is used to two lines that are set at a concerned special position within the field of view and specify the forbidden travel direction. when target objects (such as humans / vehicles) move along the set travel direction and cross these lines in a certain order (line 1 followed by line 2).

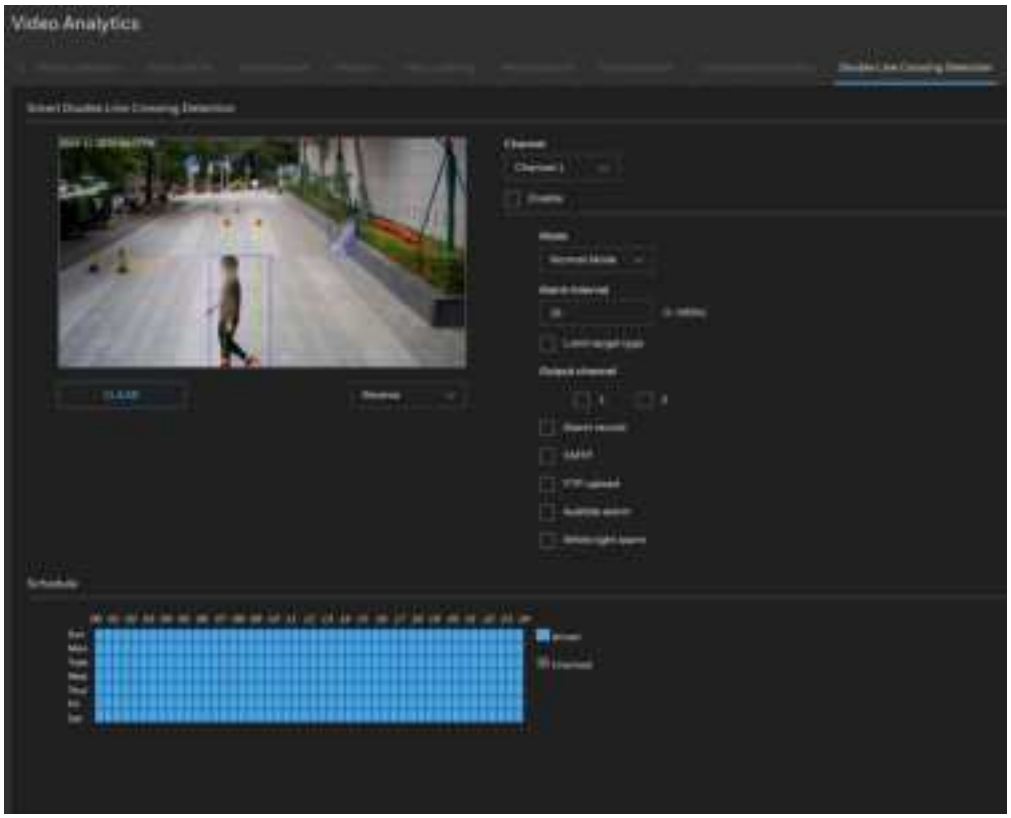
The applicable scenarios of this feature can be:

- There are specifies scene that forbidden humans / vehicles stay for long time at the detection lines.

The inappropriate scene of this feature can be:

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

Figure 51 Double Line Crossing Detection



Go to **Setup > Video Analytics > Double Line Crossing Detection**. Set the parameters of double line crossing.

Choose the channel from the drop-down list. **Channel 1** is optical channel; **Channel 2** is thermal channel.

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

Mode: For 35s cameras, users can choose mode to set, **Normal Mode** and **Preset point mode.**

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

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

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

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

Check the check boxes to enable **Alarm record, SMTP, FTP upload, Audible alarm** and **White light alarm.**

The detail information please refer to **Motion Detection,** page **52.**

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

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

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

Unattended Object Detection

Note: *This VA function is only supported for optical channel.*

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

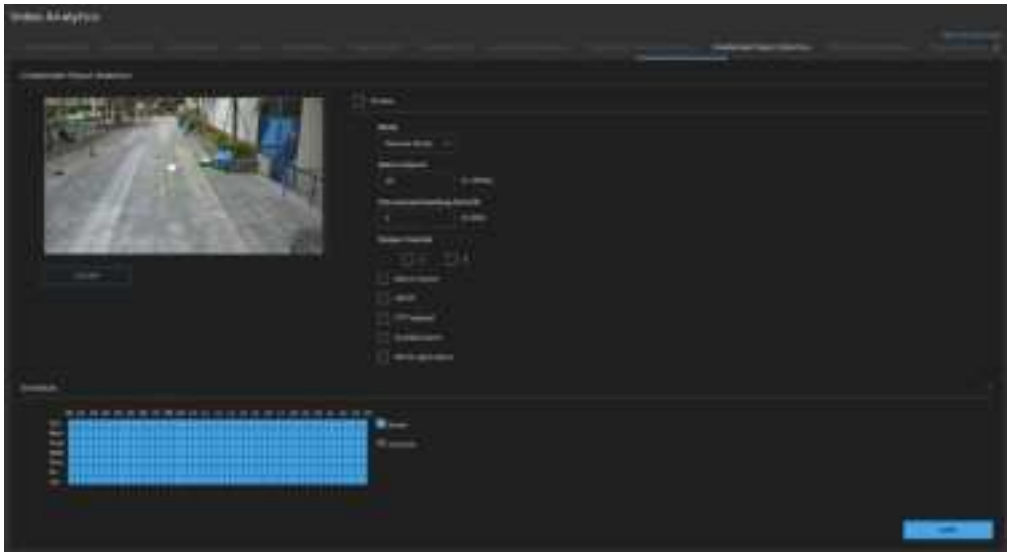
The applicable scenarios of this feature can be:

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

The inappropriate scene of this feature can be:

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

Figure 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.

Mode: For 35s cameras, users can choose mode to set, **Normal Mode** and **Preset point mode.**

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

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

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

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

Check the check boxes to enable **Alarm record, SMTP, FTP upload, Audible alarm** and **White light alarm.**

The detail information please refer to **Motion Detection**, page **52.**

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

Note: *The alarm information about ID area, it only shows from ID 1 even if the alarm is from other ID areas.*

CLEAR: Clear the area of setting. Use the mouse 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.

Missing Object Detection

Note: *This VA function is only supported for optical channel.*

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

The applicable scenarios of this feature can be:

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

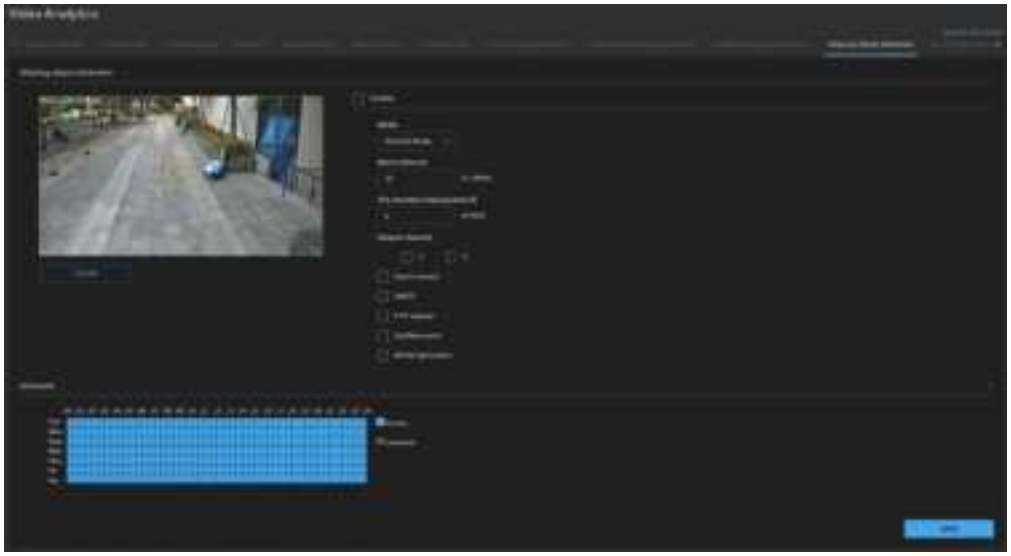
The inappropriate scene of this feature can be:

- The direction of passenger flow is complex and staggered, which seriously affects the effect.
- The horizontal distance is too far, and the target is small, which will lead to missed detection.
- The height of installation is too low, or the head is too large (people should have movement track, not too large for screen).

- Public places such as stations are crowded with people

  At the entrance of the shopping mall, people are next to the place where people come in and out

Figure 53 Missing Object Detection



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

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

Mode: For 35s cameras, users can choose mode to set, **Normal Mode** and **Preset point mode.**

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

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

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

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

Check the check boxes to enable **Alarm record, SMTP, FTP upload, Audible alarm** and **White light alarm.**

The detail information please refer to **Motion Detection,** page **52.**

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

Note: *The alarm information about ID area, it only shows from ID 1 even if the alarm is from other ID areas.*

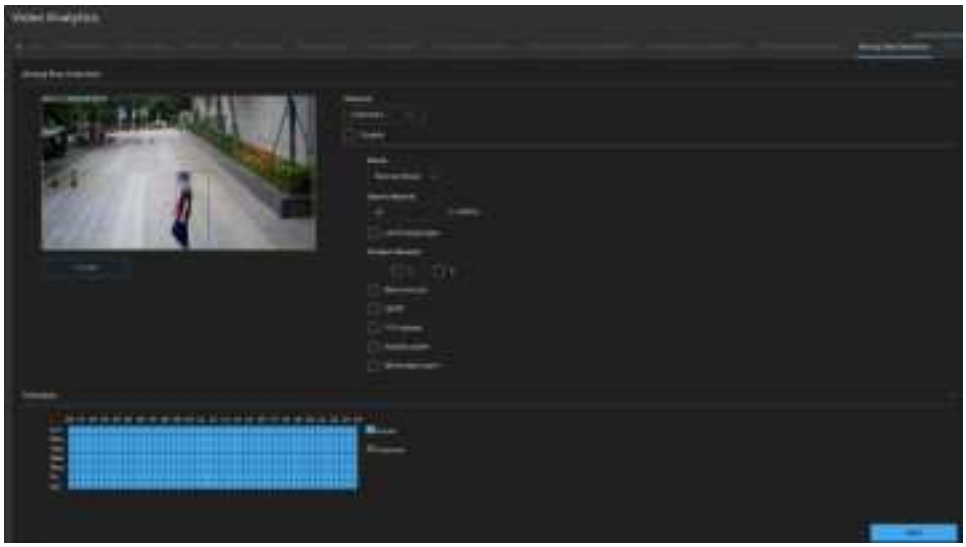
CLEAR: Clear the area of setting. Use the mouse left-click on the screen to start drawing polygon and right-click to end setting the smart detection areas, you can set several areas to detect.

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.

Wrong Way Detection

The **Wrong Way Detection** function refers to that an alarm is generated when an object is moving towards the opposite direction within the deployment area.

Figure 54 Wrong Way Detection



Go to **Setup > Video Analytics > Wrong Way Detection**. Set the parameters of double line crossing.

Choose the channel from the drop-down list. **Channel 1** is optical channel; **Channel 2** is thermal channel.

Enable: Check the checkbox to enable the wrong way detection.

Mode: For 35s cameras, users can choose mode to set, **Normal Mode** and **Preset point mode.**

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

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

Alarm Interval: During the interval, the same alarm will only be sent once.

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

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

Check the check boxes to enable **Alarm record, SMTP, FTP upload, Audible alarm** and **White light alarm.**

The detail information please refer to Motion Detection, page 52.

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

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

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

Smoker Detection

Note: *This VA function is only supported for thermal channel.*

The smoker detection function refers to that an alarm is generated when someone is smoking or generating spark at the deployment area.

The applicable scenarios of this feature can be:

- Detects when a human smoking in a warehouse or at gasoline station.
- Detects when someone smoking in mountain to prevention to avoid fire.

Go to **Setup > Video Analytics > Smoker Detection** to access the **Smoker Detection** interface.

Figure 55 Smoker Detection Interface

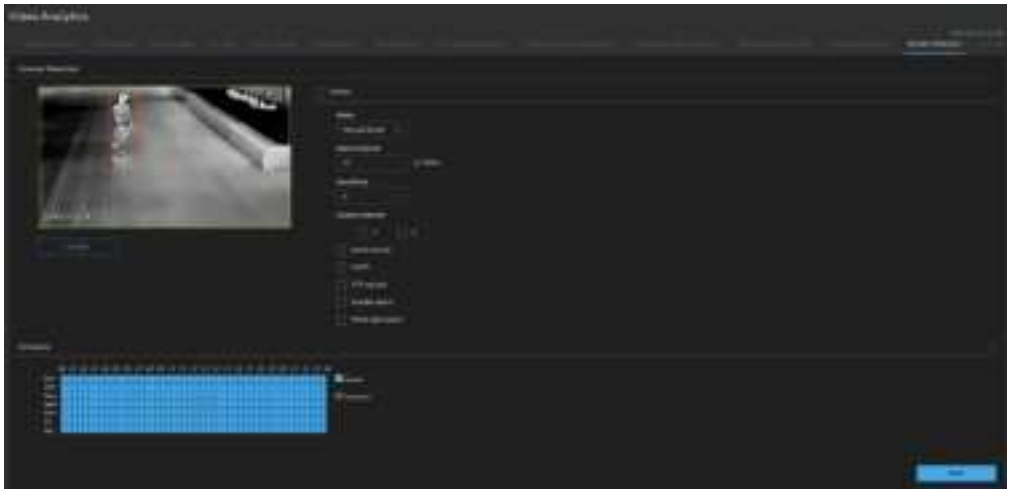


Figure 56 Setting Area

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

Mode: For 35s cameras, users can choose mode to set, **Normal Mode** and **Preset point mode.**

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

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

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

Check the check boxes to enable **Alarm record, SMTP, FTP upload, Audible alarm** and **White light alarm.**

The detail information please refer to **Motion Detection,** page **52.**

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 area of setting. Use the mouse 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.

Note: *People drink hot tea or coffee at smoke forbidden area will trigger smoker alarm. Set the low sensitivity to decrease the false alarms.*

Smoke and Flame Detection

Note: *This VA function is only supported for optical channel.*

The smoke flame detection function refers to that an alarm is generated when something is smoking or generating flame at the deployment area.

The applicable scenarios of this feature can be:

- Detects when the object is burning and producing smoke and flame in a warehouse or at gasoline station.
- Detect the object at Customs or ports to find the fire in time.

Go to **Setup > Video Analytics > Smoke and Flame Detection** to access the Smoke and Flame Detection interface.

Figure 57 Smoke and Flarm Detection

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

Mode: For 35s cameras, users can choose mode to set, **Normal Mode** and **Preset point mode.**

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

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

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

Check the check boxes to enable **Alarm record, SMTP, FTP upload, Audible alarm** and **White light alarm.**

The detail information please refer to **Motion Detection,** page **52.**

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 area of setting. Use the mouse 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.

Table 5 Test pixel of smoke and flame

Model	Test distance (m)	Test effect pixel
The object size is 1.2m*0.65m		
HC35TE5R3JT21	2	225*148
HC35TE5R4JT35	2	338*227
HC35TB5R1JT07	4	312*259
HC35TB5R4JT10	4	316*260

Fire Spot Detection

Note: *This VA function is only supported for thermal channel.*

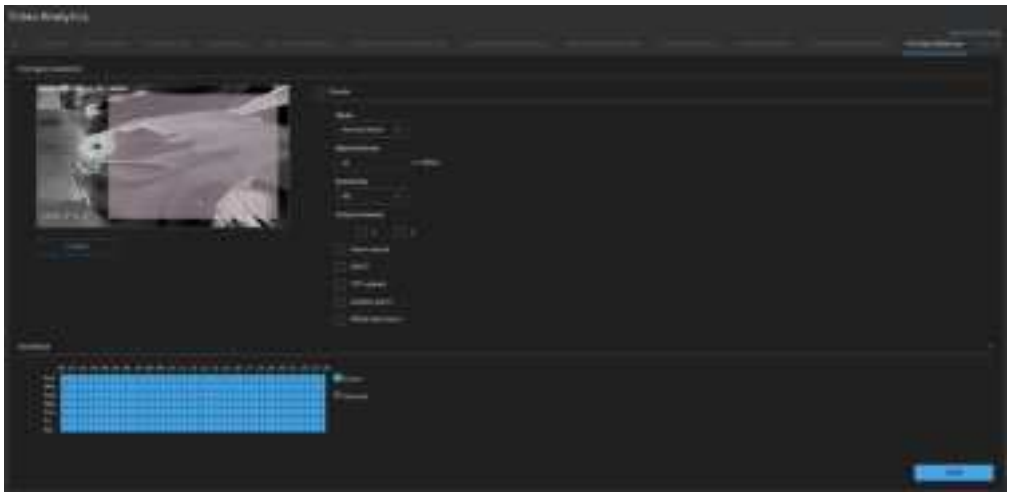
The fire spot detection function refers to that an alarm is generated when something is on fire at the deployment area.

The applicable scenarios of this feature can be:

- Detects when the object is burning and having fire spot in a warehouse or at gasoline station.
- Detect the object at Customs or ports to find the fire in time.

Go to Setup > Video Analytics > Fire Spot Detection to access the **Fire Spot Detection** interface.

Figure 58 Fire Spot Detection



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

Figure 59 Fire Spot Detection

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

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

Mode: For 35s cameras, users can choose mode to set, **Normal Mode** and **Preset point mode.**

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

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

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

Check the check boxes to enable **Alarm record, SMTP, FTP upload, Audible alarm** and **White light alarm.**

The detail information please refer to **Motion Detection,** page **52.**

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.

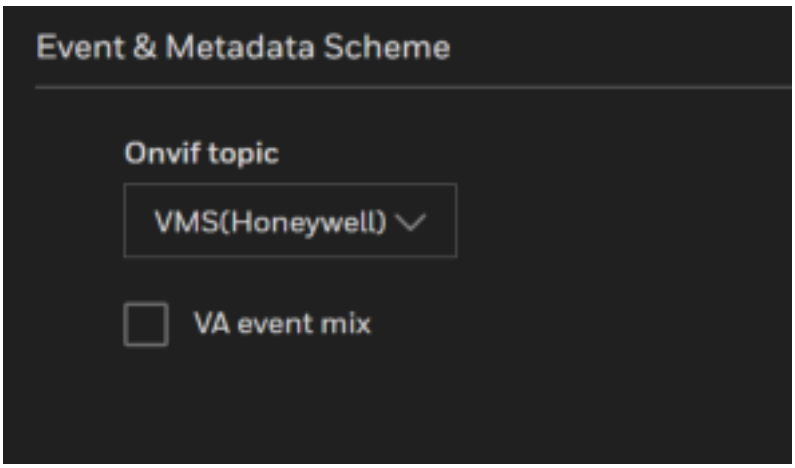
Table 6 Test distance of fire spot

Model	Test distance (m)
Test environment: the diameter of blackbody is 16cm, the temperature is 120℃	
HC35TE5R3JT21	10
HC35TE5R4JT35	13
HC35TB5R1JT07	25
HC35TB5R4JT10	30

Event & Metadata Scheme

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

Figure 60 Event & Metadata Scheme



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

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

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

VA event mix: if checked, when one channel is triggered the alarm, no matter channel 1 or channel 2, it will send messages of channel 1 and channel 2 via ONVIF at the same time.

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

7 CONFIGURE ALARM AND EVENT

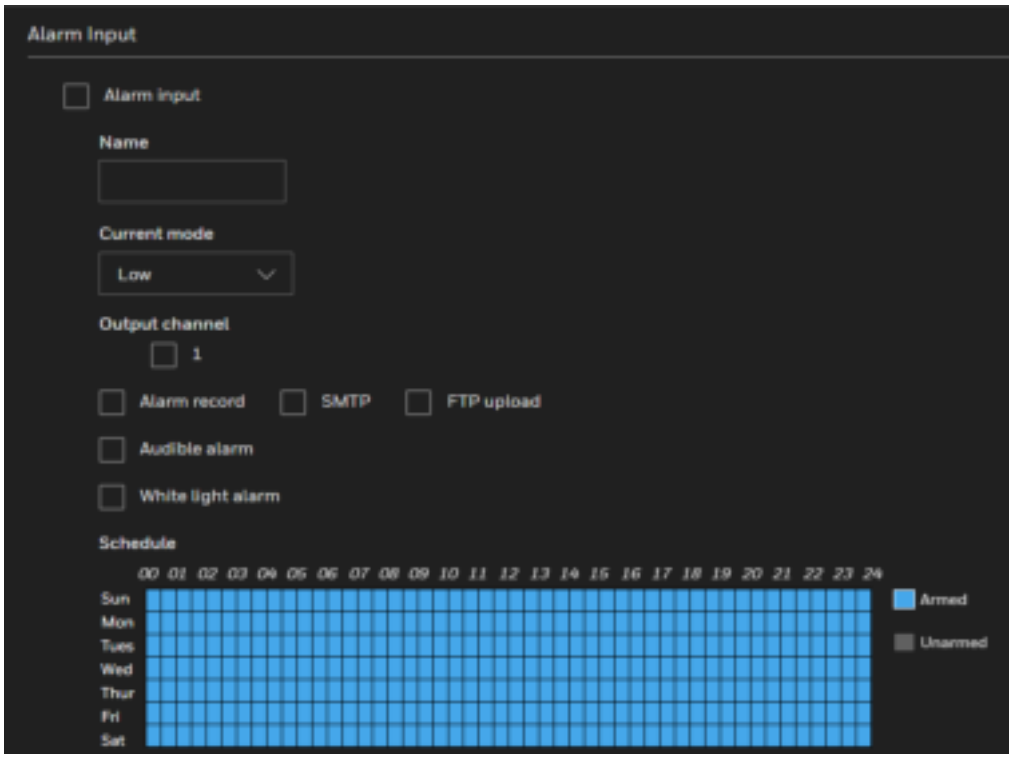
This section describes the alarm and event settings.

Configuring Alarm In and Alarm Out

Alarm Input

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

Figure 61 Alarm Input



Alarm input: Check the checkbox of Alarm input.

Name: Enter the alarm input name.

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

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

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

Output channel: Select the Output channel.

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

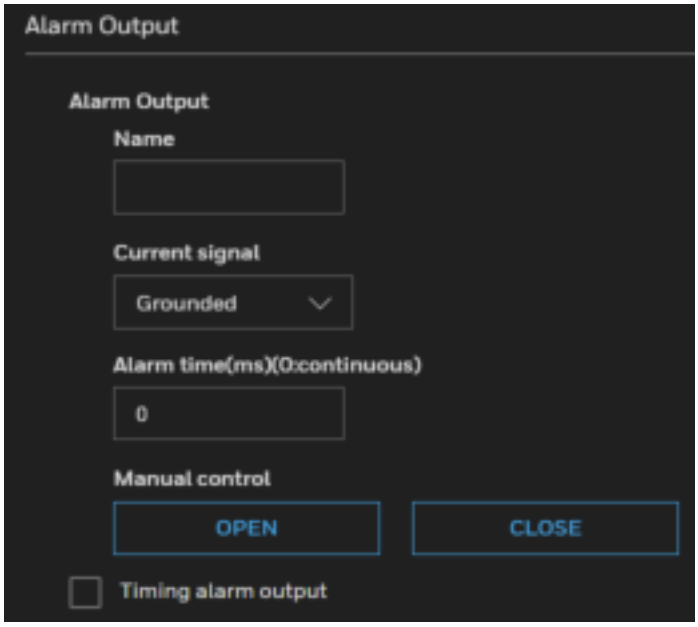
After the event is triggered, the system will run or stop the movement of the corresponding type according to the settings.

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

Alarm Output

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

Figure 62 Alarm Output



Name: Alarm output name

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

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

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

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

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

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

Note: *Two alarm inputs and an alarm output can be configured.*

Configuring SD Card Alarm

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

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

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

Alarm interval: Set the interval.

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

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

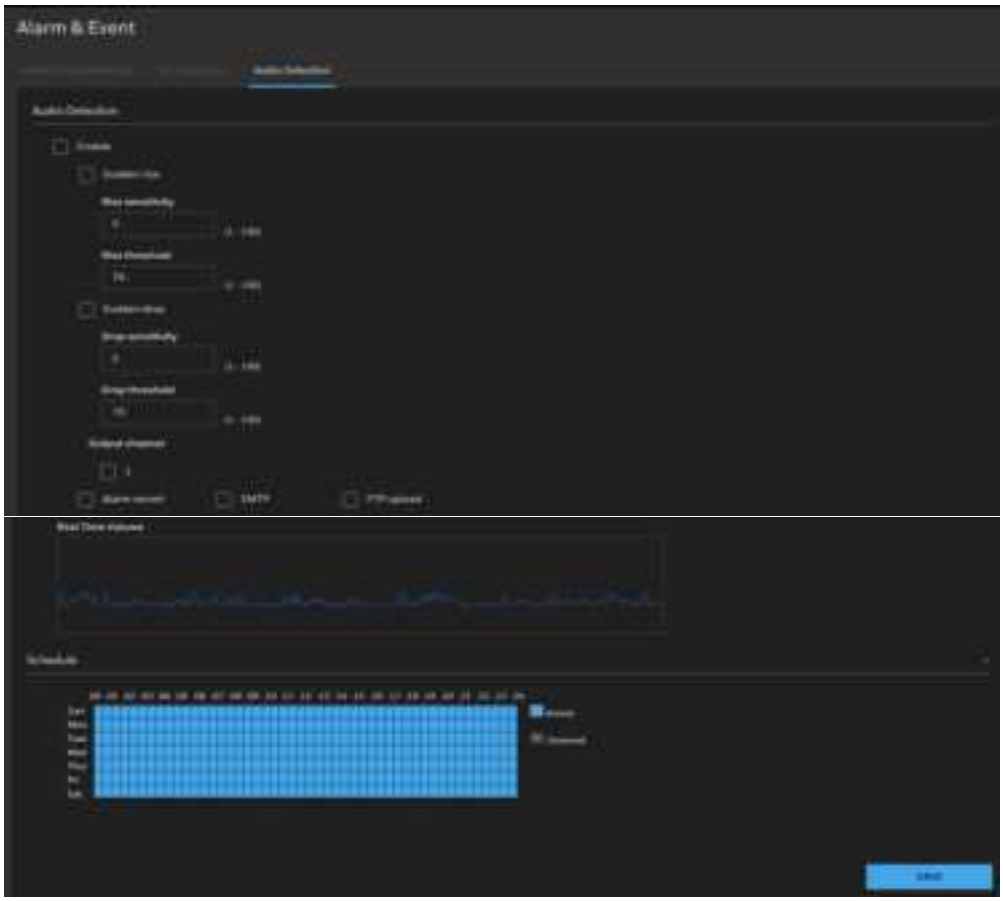
Note: *For the event recording clips edge sync, current firmware version can only support no more than 1000 recording clips in the SD card within 1 month ahead the current searching timestamp.*

Configuring Audio Detection

Go to Setup > Alarm & Event > Audio Detection.

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

Figure 63 Alarm Input



Enable: Check the checkbox to enable the audio detection.

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

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

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

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

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

Output channel: Select the Output channel.

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

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

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

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

CHAPTER
8 CONFIGURE STORAGE SETTINGS

SD Card Management

Go to **Setup > Storage Setup > SD Card Management**.
This section describes how to manage the local storage on the camera. Here you can view SD card status, and implement SD card control.
See the following table for compatible SD Card.

Table 7 Compatible SD Card

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

Note:
- *It is recommended to turn OFF the recording activity before you remove an SD card from the camera.*
- *The lifespan of an SD card is limited. Regular replacement of the SD card can be necessary.*
- *Camera file system takes up several megabytes of memory space. The storage space cannot be used for recording.*
- *Using an SD card that already contains data recorded by another device should not be used in this camera.*
- *Do not modify or change the folder names in the SD card. That may result in camera malfunctions.*
- *If you want to use the SD card in another camera, format the SD card in another camera first. For how to format the SD card, see* SD Card Format *on page* 85*.*

SD Card Status

This tab shows the status and reserved space of your SD card. Bi-spectrum 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 85.

Figure 64 No SD Card

Figure 65 SD Card Onboard

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.

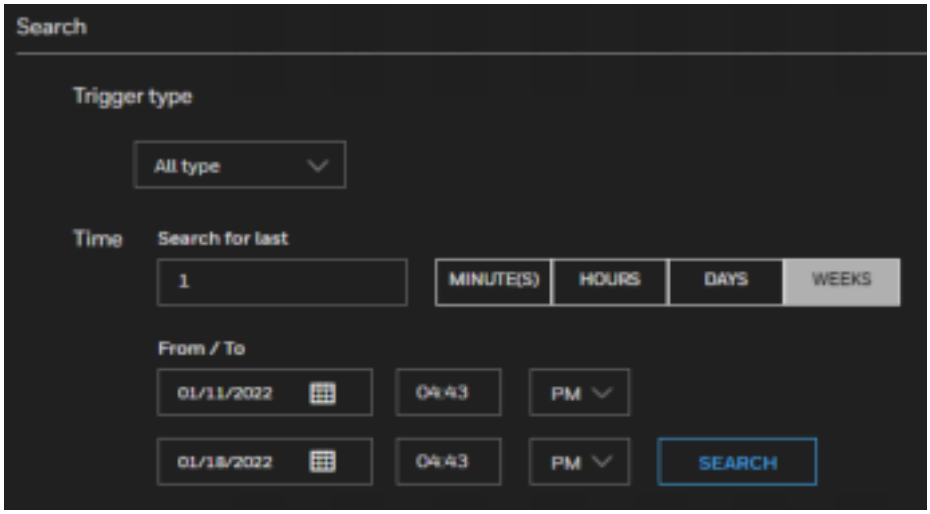
Warning: Check if any recording such as continuous recording is running anddisable the event or recording rule before detaching the SD card. The SD card has unformatted status after reinserting into the camera if the recording was on while you removed it from the camera.

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.

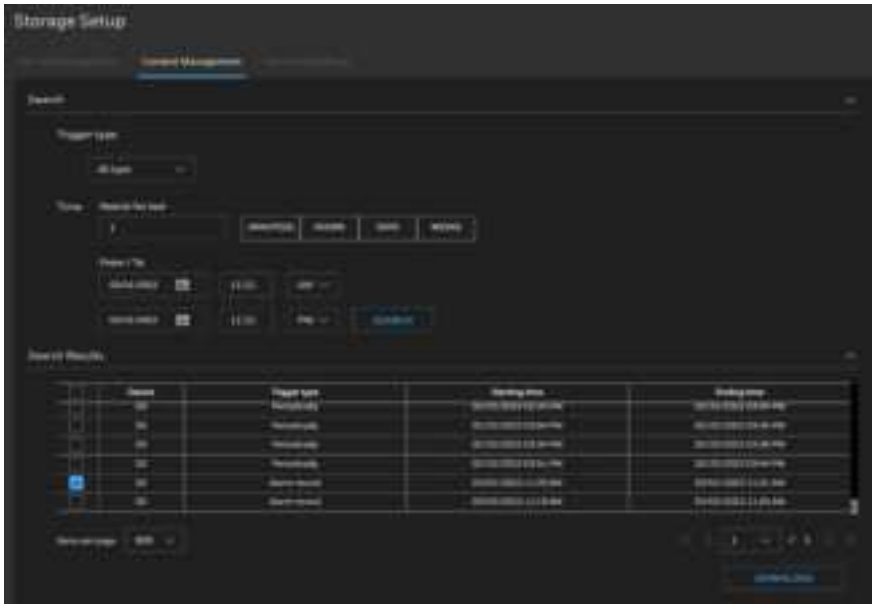


- **Trigger type:** Select one or more triggers from All types, Periodically Motion detection alarm I/O alarm, Intrusion alarm, Multi loitering alarm, Smart motion alarm, Scene change alarm People counter alarm, Unattended object detection alarm Missing object detection alarm, Line crossing detection alarm, Double line crossing detect alarm, Wrong way detect alarm Audio detection alarm, Face detection alarm Smoke and flame detection alarm (channel 1). For channel 2, All types Periodically, Motion detection alarm, I/O alarm Intrusion alarm, Multi loitering alarm, Smart motion alarm, People counter alarm, Line crossing detection alarm, Double line crossing detect alarm, Wrong way detect alarm, Audio detection alarm, Smoker detection alarm, Fire spot detection alarm, Temperature threshold warning, Temperature threshold alarm, Temperature difference warning, Temperature difference alarm, Temperature section alarm, Temperature rise warning.
- **Time**: Manually enter the time range you want to search for contents created at a specific point in time.

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

Search Results

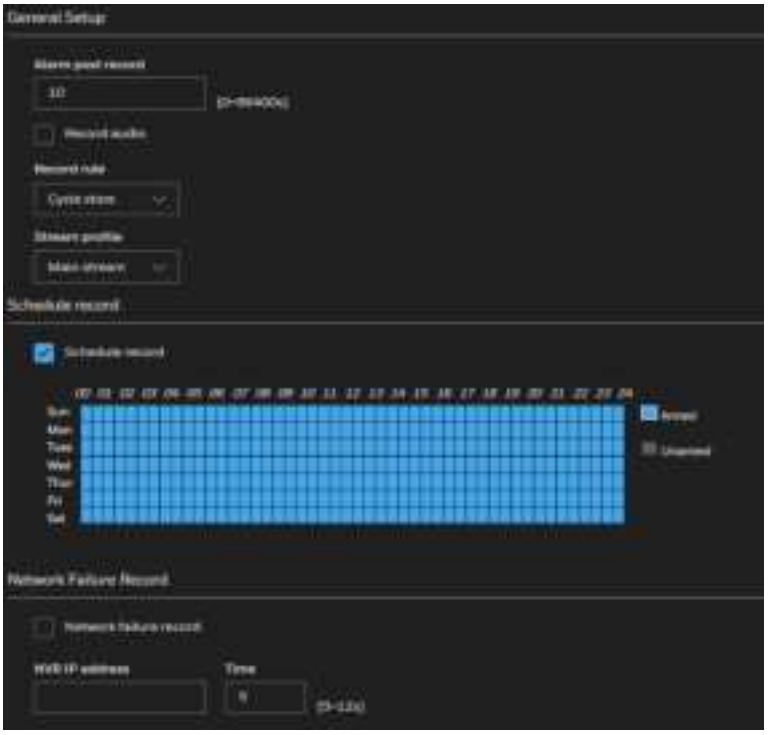
To sort the search results, click each column header.
Download: Click on a search result and click **DOWNLOAD**, and a file download window will pop up for you to save the file. You can play the video clip by VLC player.



Note: *The alarm records sorted in Trigger type are alarm type recording, not periodically recording.*
For Optical, it includes All types, Periodically, Motion detection alarm, I/O alarm, Intrusion alarm, Multi loitering alarm, Smart motion alarm, Scene change alarm, People counter alarm, Unattended object detection alarm, Missing object detection alarm, Line crossing detection alarm, Double line crossing detect alarm, Wrong way detect alarm, Audio detection alarm, Face detection alarm, Smoke and flame detection alarm.
For Thermal, it includes All types, Periodically, Motion detection alarm, I/O alarm, Intrusion alarm, Multi loitering alarm, Smart motion alarm, People counter alarm, Line crossing detection alarm, Double line crossing detect alarm, Wrong way detect alarm, Audio detection alarm, Smoker detection alarm, Fire spot detection alarm, Temperature threshold warning, Temperature threshold alarm, Temperature difference warning, Temperature difference alarm, Temperature section alarm, Temperature rise warning, Temperature rise alarm.

Recording Settings

Go to **Setup > Storage Setup > Recording Settings**.
This section describes how to configure the recording settings for the camera.



Schedule record: Enables schedule record that you can configure the time policy.
Alarm post record: Recording duration (in seconds) after an alarm is generated.
Record audio: Indicates whether to record audios together with videos.
Record rule: Rule for saving recordings. The options are as follows:
Cycle Store: Saves recordings in cycles.
Save Days: Duration (in days) for saving a recording. The duration can be a maximum of 99999 days.
The value 0 indicates that recordings are not overwritten.
Stream profile: Select from the dropdown list: Main stream, Sub stream.
Network Failure Record: Enable **Network failure record**. Fill in the NVR IP address and continuation time. The camera will keep detecting the connection status that the IPC accessed to NVR.
If the time is set as 5, when the NVR is disconnected, the camera's SD card will wait for 5s then start to record. When NVR is restoring recording, the SD card will go on recording for 5s, then stop to record.

Note:

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

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

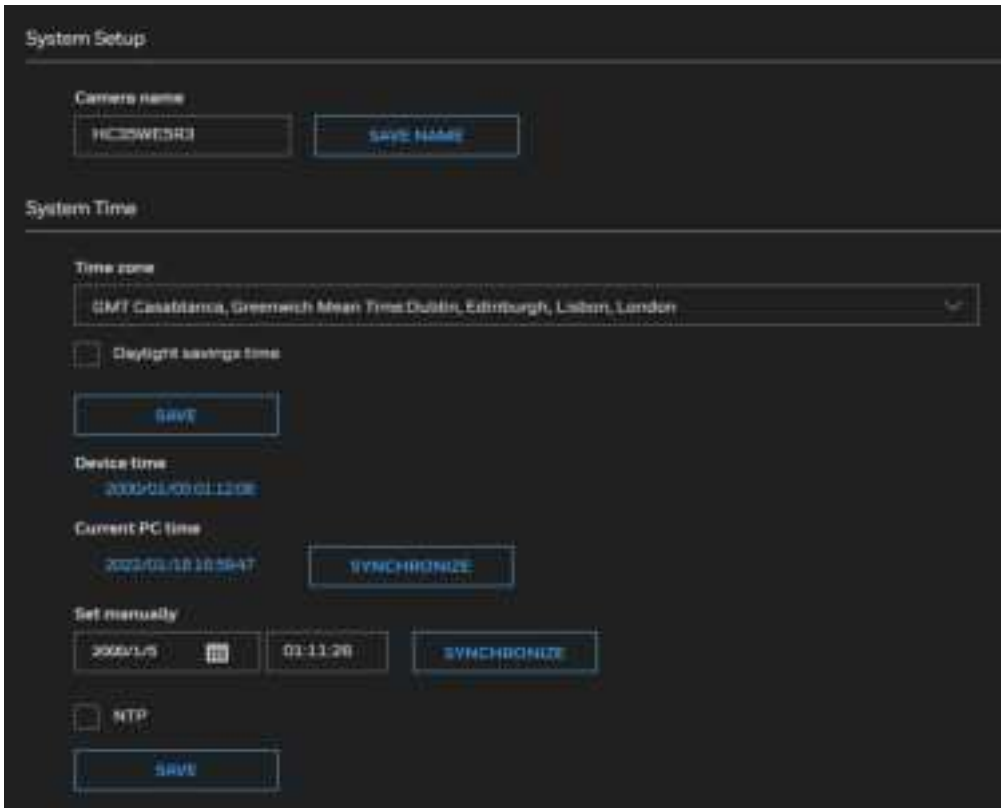
CHAPTER

9 CONFIGURE SYSTEM SETTINGS

Configuring System General Settings

Go to **Setup > System Setup > General Settings**.
This section explains how to configure the basic settings for the camera, such as the host name and system time.

Figure 66 System General Settings



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.

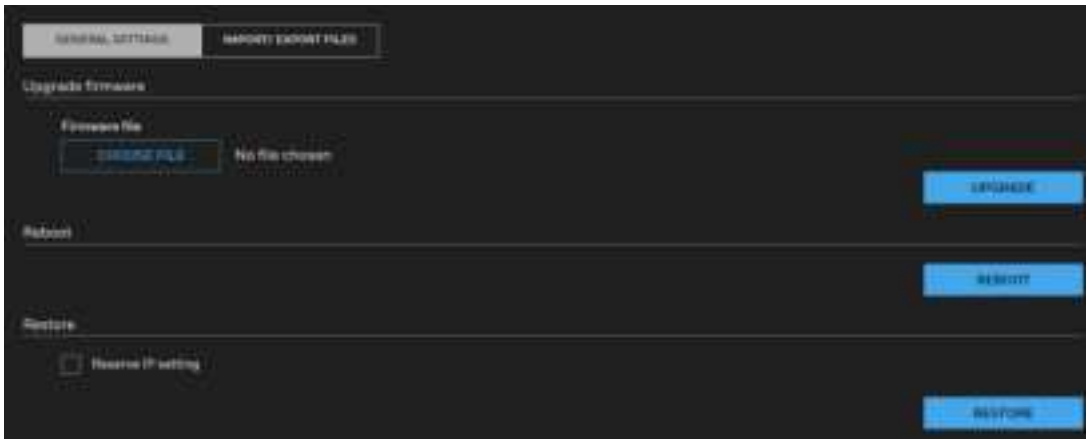
- When the DST start time arrives, the device time automatically goes forward one hour.
- When the DST end time arrives, the device time automatically goes backward one hour.

Device time: Device display time.

Current PC time: Time on the current PC.
Set manually: Enables you to manually set the device time.
NTP: IP address or domain name of the NTP server. Check the checkbox to enable NTP.
NTP server addr: The NTP server IP.
NTP Port: Port number of the NTP server.
Check the time interval(at least 10 s): Set time interval to check if the device time synchronizes with the NTP server time.

Configuring Maintenance Settings

Go to **Setup > System Setup > Maintenance**.
This chapter describes how to restore the camera to factory default, upgrade firmware version, etc.



Upgrading Firmware

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

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

Follow the steps below to upgrade the firmware:

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

- If an SD card is used in your camera, it will be formatted automatically after the upgrade. The formatting may take 5 to 20 minutes.
- After the SD card is formatted, it will be encrypted and its content cannot be read on other cameras.
- If you want to use the SD card in another camera, format the SD card in another

camera first. For how to format the SD card, see SD Card Format on page 85.

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

Rebooting the Camera

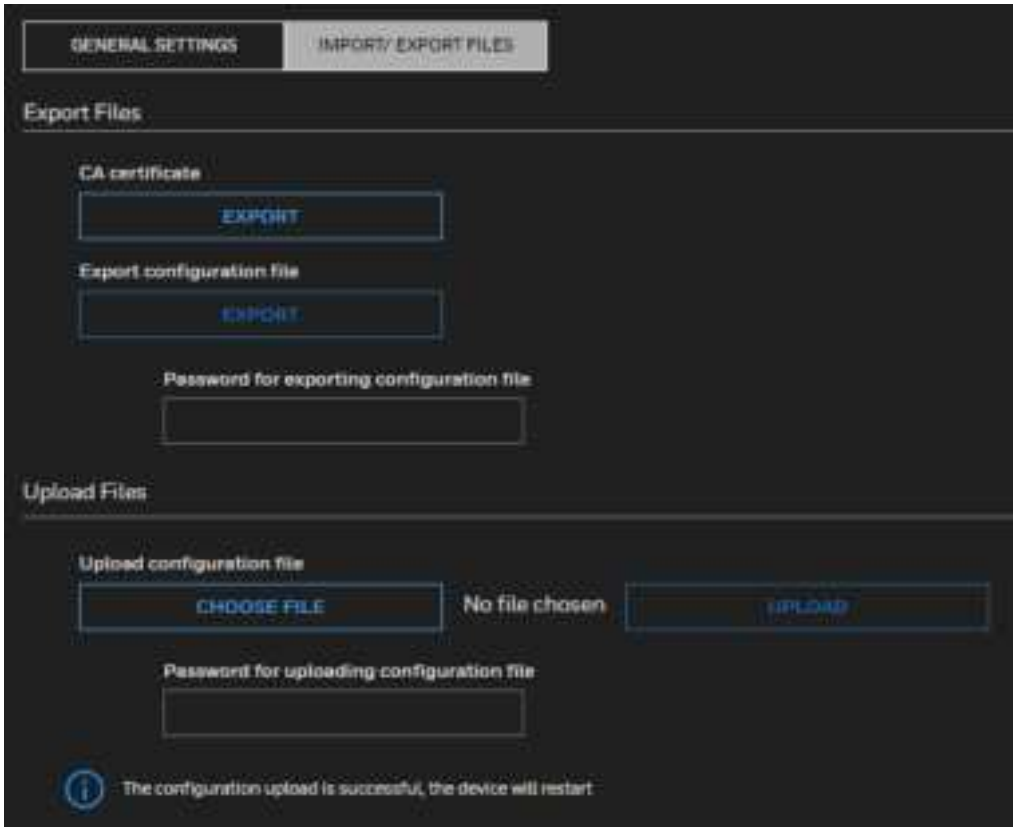
On this page, you can reboot the camera. It takes about one minute to complete.
After it is completed, the live video page will be displayed in your browser.
If the connection fails after rebooting, manually enter the IP address of the camera in the address field to resume the connection.

Restoring the Camera

Restore the camera to factory default settings.
Network Setup: Check to retain the Network Type settings (see Configuring Network General Settings on page 31).
Daylight Savings Time: Check to retain the Daylight Savings Time settings (see Importing/Exporting Files on page 91).
Focus position: Check to retain the lens focus position using the previously saved position parameters.
If none of the options is selected, all settings will be restored to factory default. Click RESTORE and the camera will be rebooted.
After it is completed, the live video page will be displayed in your browser.
If the connection fails after rebooting, manually enter the IP address of the camera in the address field to resume the connection.

Importing/Exporting Files

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



Export CA Certificate

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

1. Click Export to save the root certificate (ca.crt) on your local computer.
2. Go to the directory where you saved the certificate and double-click the certificate. The Certificate window opens.
3. In the Certificate window, on the General tab, click Install Certificate to open the Certificate Import Wizard.
4. Click Next to continue.
5. Click Place all certificates in the following store, click Browse, click Trusted Root Certification Authorities, and then click OK.
6. Click Next, and then click Finish to close the Certificate Import Wizard. A confirmation dialog box appears with the message "The import was successful."
7. Click OK, and then click OK to close the Certificate window. And now your browser will not display a warning that the connection is not private/ secure.

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

Export Configuration File

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

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

Upload Configuration File

Follow the steps below to upload a configuration file:

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

The model and firmware version of the device should be the same as the configuration file. If you have set up a fixed IP or other special settings for your device, it is not suggested to update a configuration file.
If the power is disconnected during firmware upgrade or if there is unknown reason causing abnormal LED status, and a Restore cannot recover normal working condition, you can perform the following steps to activate the camera with its backup firmware:

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

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

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

Configurating Privacy Policy

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

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

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

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

Configuring User Accounts Settings

Go to **Setup > System Setup > User Accounts**.
This section describes how to create multiple accounts and grant privileges to these accounts.

Account Management

The administrator account name is “admin”, which is permanent and cannot be deleted.
The administrator can create up to 20 user accounts. To create a new user:

1. Select New user from the

dropdown list.

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

The privilege levels are listed below:

Role	Privilege
Administrator	Full control
Viewer	Live, Language

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

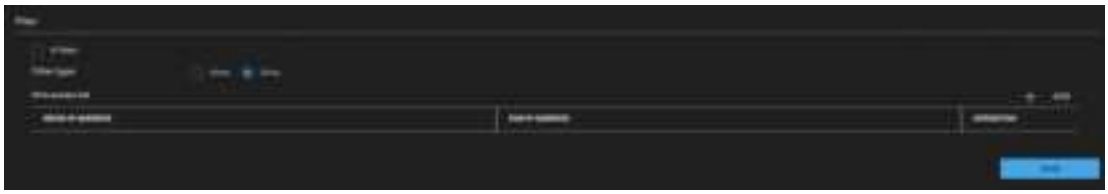
To change a user's access rights or delete user accounts:

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

Configuring Access List Settings

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

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



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

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

Click **ADD** and you can add a filter address.

Note:
- *The IPv6 access list column will not be displayed unless you enable IPv6 on the Network page. For more information about IPv6 Settings, see operation on page 31.*
- *The Range rule only applies to IPv4 addresses.*

CHAPTER

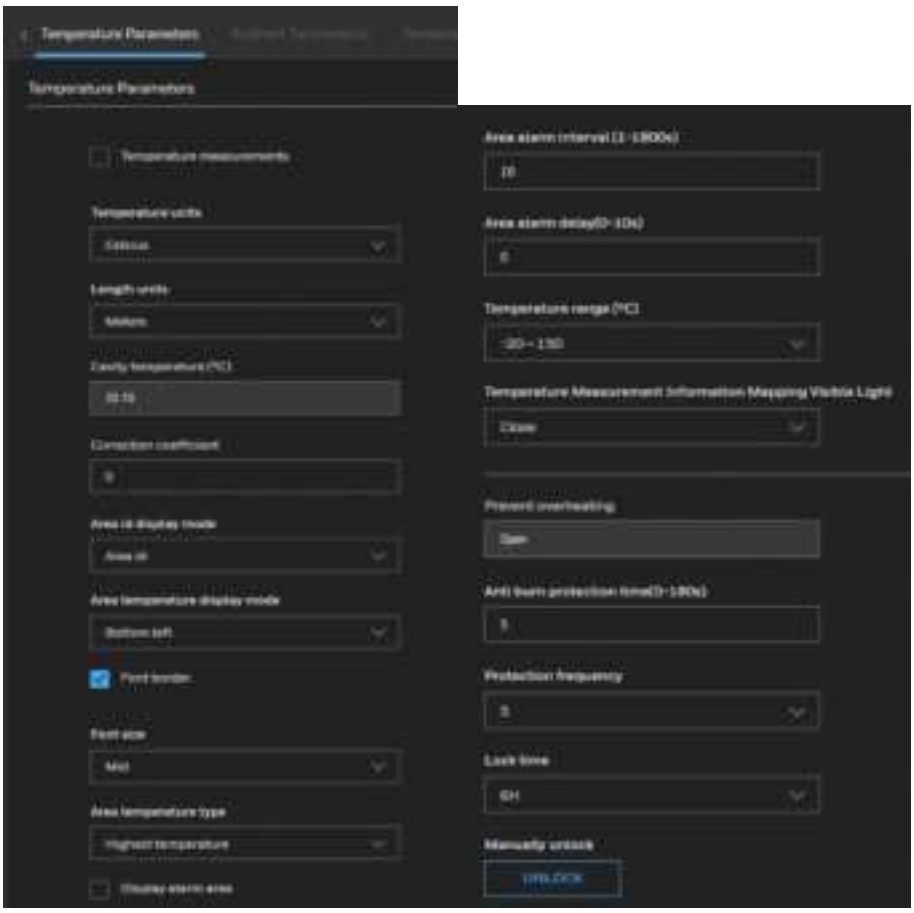
10 CONFIGURING THERMAL SETTINGS

In this chapter, users can set the parameters about thermal, such as temperature parameters, ambient temperature, temperature alarm, schedule linkage, thermal mapping, defect pixel correction, led control, box display and so on.

Temperature Parameters

Go to **Setup > Thermal > Temperature Parameters**.

Figure 67 Temperature Parameters Settings



Set the parameters follows the table.

Table 8 Temperature parameters

Parameter	Description	Setting
Temperature measurements	It is ticked by default to enable measuring the temperature. If it is unticked, the device is invalid temperature measurement.	[Default value] **Tick**
Temperature Unit	Celsius and Fahrenheit temperature units are available.	[Setting method] Select a value from the drop-down list box. [Default value] **Celsius**
Length units	Meters and feet length units are available.	[Setting method] Select a value from the drop-down list box. [Default value] Meters
Cavity Temperature	The cavity temperature of camera refers to the internal temperature of the camera body	No need to configure.
Correction Coefficient	Correction coefficient is referring to the deviation of measured object temperature and actual temperature, is offset value. For example: 1. The measured object temperature is 20, and actual temperature is 20.5, so the correction coefficient should be 0.5. 2. The measured object temperature is 20, and actual temperature is 19.5, so the correction coefficient should be -0.5.	[Setting method] Enter a value manually. It ranges from -100 to 100 [Default value] **0.00**
Area ID display mode	There are two modes to display, area ID and area name. 	[Setting method] Select a value from the drop-down list box. [Default value] **Area ID**
Temperature Consume Mode	Transmission of temperature values or picture to third party platforms via Modbus protocol. It can be supported via Ethernet. There three modes can be chosen, close/ jpeg +temperature/ temperature.	[Setting method] Select a value from the drop-down list box. [Default value] **Close**

Parameter	Description	Setting
Area Temperature Display Mode	The display position of temperature information on the live-video image. 	[Setting method] Select a value from the drop-down list box. [Default value] **Low left**
Font Border	Enable to bold the font	[Setting method] Enable or disable [Default value] **Disable**
Font size	There are three font size can be chosen, small/mid/big	[Setting method] Enable or disable [Default value] **Mid**
Area Temperature Type	There are three types of area temperature: Highest temperature, Highest temperature &Lowest temperature, Highest temperature&Lowest temperature&Average temperature	[Setting method] Select a value from the drop-down list box. [Default value] **Highest Temperature**
Display Alarm Area	Check to display the setting alarm area on live video. When alarm is triggered in the area, the alarm detection area of the object will be drawing the frame to reminder. The corresponding information is only displayed in the thermal main stream.	[Setting method] Enable or disable [Default value] **Untick**
Area Alarm Interval (1-1800s)	During the interval, the same alarm will only be sent once.	[Setting method] Enter a value manually ranges from 1 to 1800. [Default value] **10**
Area Alarm delay (0-10S)	The area alarm information will delay for setting time.	[Setting method] Enter a value manually ranges from 1 to 10. [Default value] **0**
Temperature range	-20°C to 150°C (-4°F to 302°F)	[Setting method] Select a value from the drop-down list.

Parameter	Description	Setting
Prevent Overheating	Open, if temperature of the testing area is too high, the camera will be automatic triggered prevent over heat function. The shutter will be closed to keep the detector safe. The live video will show tip “The current temperature has exceeded the maximum temperature! Please wait...”	[Setting method] Open
Anti burn protection time(5-60 S)	When the prevent overheating takes effect, the shutter will close for the setting time.	[Setting method] Enter a value manually ranging from 5 to 60.
Protection frequency	When the overheating time is over this setting value, the shutter will be lock for the setting lock time. The Never means the shutter cannot be locked. The next trigger time is over 20s, the frequency will be cleared, and recount.	[Setting method] Select a value from the drop-down list.
Lock time	The shutter will be locked during the time, or users can click the button to unlock manually. The live video will show tip “The shutter is closed. Please wait for time or manual unlock”	[Setting method] Select a value from the drop-down list.
Temperature Measurement Information Mapping Visible Light	If it is open, the live video of thermal channel will be mapping with optical channel. The effect will show on optical channel. It is only applicable for optical main stream.	[Setting method] Select a value from the drop-down list box.

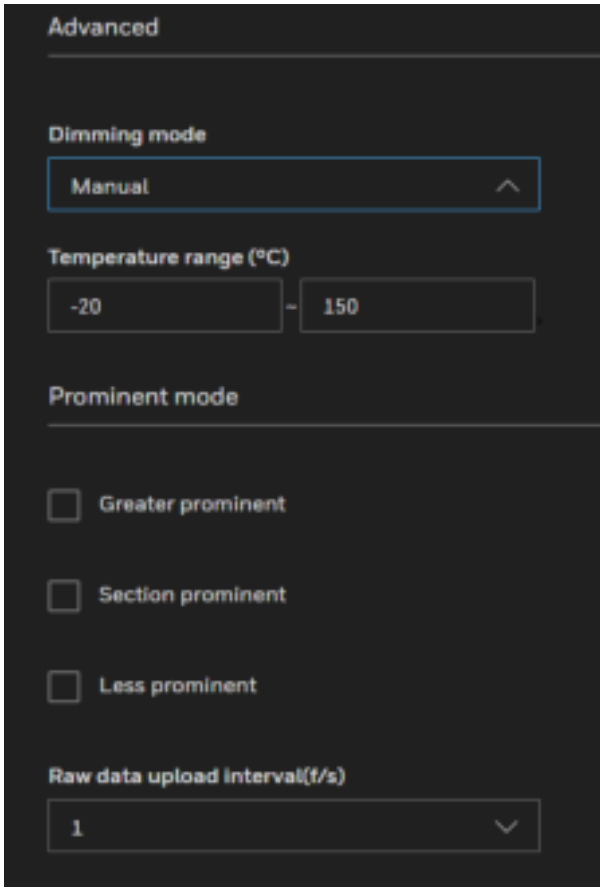

Advanced
Dimming mode
Manual
Temperature range (°C)
-20
~
150
Prominent mode
Greater prominent
Section prominent
Less prominent
Raw data upload interval(f/s)
1

Table 9 Advanced Parameters

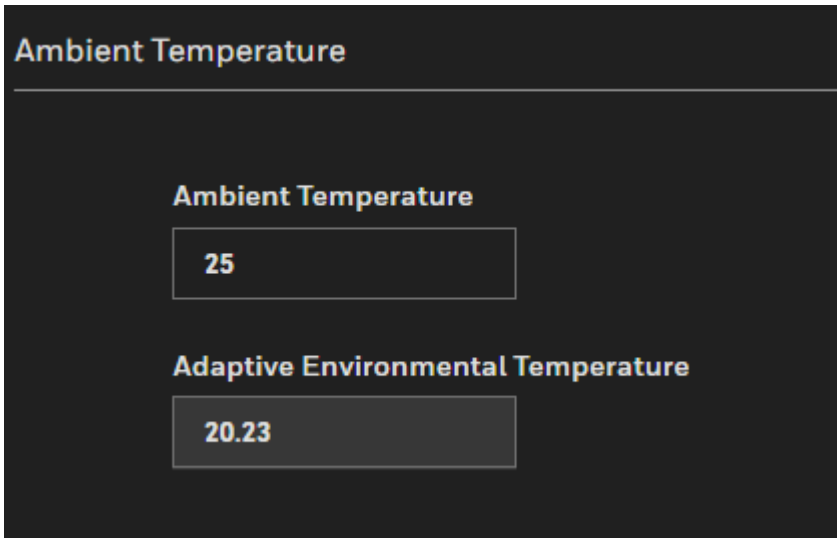
Parameter	Description	Setting
Dimming Mode	The temperature range is divided into 256 colors, the larger the temperature range the less obvious the color contrast, the smaller the temperature range the more obvious the color contrast. There are auto and manual modes. **Auto**: The device automatically adjusts the brightness and contrast of the image based on the highest and lowest temperature of the current scene.  **Manual**: The device adjusts according to the manually configured temperature range to achieve the expected image brightness and contrast. 	[Setting method] Select a value from the drop-down list box. [Default value] **Auto**
Greater Prominent	Enable that, the image will show the setting color if the temperature is higher than set value.	[Setting method] Enter a value manually. Choose one color to show.
Section Prominent	Enable that, the image will show the setting color if the temperature is between minimum and maximum temperature.	[Setting method] Enter a value manually. Choose one color to show.
Less Prominent	Enable that, the image will show the setting color if the temperature is lower than set value.	[Setting method] Enter a value manually. Choose one color to show.

Click **SAVE.**

Ambient Temperature

Go to **Setup > Thermal > Ambient Temperature**.

Figure 68 Ambient Temperature Settings



Ambient Temperature:
Usually, no customer configuration is required. The current ambient temperature needs to be configured only when the device has just been powered on but the user needs to measure the temperature immediately.
Adaptive Environmental Temperature: the camera will get the value automatically.

Click **SAVE.**

Temperature Alarm

1. Go to **Setup > Thermal > Temperature Alarm.**

Figure 69 Temperature Alarm

2. Set the temperature alarm parameters following the table.

Table 10 Advanced Parameters

Parameter	Description	Setting
Enable	Tick the check box of ID to enable the area measuring.	[Setting method] Tick

Parameter	Description	Setting
Name	Area name of temperature area.	[Setting method] Enter a value manually.
Type	Type of temperature area. ID 0 is default rectangle area, which is full screen. It cannot be modified. Other IDs can be set as point, line, or polygon.	[Setting method] Select a value from the drop-down list box. [Default value] **Rectangle/Point**
Alarm Type	**Temperature difference alarm:** when the area's temperature difference (Highest temperature minus Average temperature) is over the setting value (Warning temperature or Alarm temperature), it will generate the alarm. **Temperature rise alarm:** In the duration time. If the rising temperature value is more than the set value (Warning temperature or Alarm temperature), it will generate the alarm. **Temperature threshold alarm:** when the temperature is higher than threshold, the alarm will be triggered. **Section Alarm:** if the temperature value is among the set temperature range, it will generate the alarm.	[Setting method] Select a value from the drop-down list box. [Default value] **Threshold alarm**
Warning Value	Camera will trigger warning alarm when the object temperature reaches the warning value. The value can be set when selecting Section alarm.	[Setting method] Enter a value manually. [Default value] **48**
Alarm Value	Camera will alarm when the object temperature reaches the alarm value.	[Setting method] Enter a value manually. [Default value] **50**
Maximum Alarm Value	At section alarm type, the device would not alarm when the temperature is higher than maximum alarm value.	[Setting method] Enter a value manually. [Default value] **60.00**

Parameter	Description	Setting
Duration (1-10S)	If the highest temperature rises by the set value within the set duration time range, a temperature rise alarm will be triggered For example: The maximum temperature in the target area is 30 ℃. if we set the alarm threshold to 50 ℃, and set the duration to 10 seconds, when the highest temperature in the temperature measurement area rises by 50 ℃ (i.e. the temperature in the target area is higher than 80 ℃) within 10 seconds, a temperature alarm will be triggered.	[Setting method] Enter a value manually. [Default value] **1.00**
Emission Rate	The emission rate is the capability of an object to emit or absorb energy. The emission rate should be set only when the target is special material. The detail please refer to ***Table 5 Common Emission Rate*** .	[Setting method] Enter a value manually. [Default value] **0.95**
Distance(M)	The distance between camera and target.	[Setting method] Enter a value manually. [Default value] **15** NOTE Enter actual distance when the distance between camera and target is less than 15m.Enter 15 when the distance between camera and target is great than or equal to 15m.
Reflection temperature on	When there are some high temperature objects on scene, and the temperature reflect to the other object, you can enable this function to calibrate the temperature.	[Setting method] Tick to enable
Reflect Temperature	The temperature of high temperature object.	[Setting method] Enter a value manually. [Default value] **50.00**
Ignore Object	Enable to shield the temperature of area capturing AI object. Users can choose None/ human/ vehicle/ all type (Human + Vehicle).	[Setting method] Select a value from the drop-down list box.
Alarm	Enable or disable the alarm output and linkage of area.	[Setting method] Tick to enable alarm.

Parameter	Description	Setting
Masking	Enable, the device will shield this area's temperature.	[Setting method] Tick to shield.
Group ID	Different areas can be divided into the same group. The same group's areas will be merger calculated temperature difference alarm. The ID can be chosen into one of six groups, or no group. The group will be alarm following as the next rules: A=The highest temperature of groups (the highest temperature of N regions is the largest) B=Average temperature of groups (average temperature of N regions) WA=Warning value AA=Alarm value a. If A-B >= WA, a temperature difference warning signal is generated ---> (the one with the largest difference between the N areas and the average temperature is the alarm area flashing) b. If A-B >= AA, a temperature difference alarm signal is generated ---> (the one with the largest difference between the N areas and the average temperature is the alarm area flashing) c. If the warning and alarm conditions are met at the same time, the alarm signal will be generated first.	[Setting method] Select a value from the drop-down list box.

Note: *The temperature OSD will be shown as the Group ID' sequence if the group ID is not None.*

Table 11 Common Emission Rate

Materials	Temperature (℃/℉)	Emissivity
Gold (High-purity)	227/440	0.02
Aluminum foil	27/81	0.04
Aluminum sheet	27/81	0.18
Aluminum used for families (flat)	23/73	0.01
Aluminum plate (98.3% purity)	227/440	0.04
	577/1070	0.06
Aluminum plate (rough)	26/78	0.06
Aluminum (oxidized @ 599℃)	199/390	0.11
	599/1110	0.19

Materials	Temperature (℃/℉)	Emissivity
Polished aluminum	38/100	0.22
Tin (light tinned Iron sheet)	25/77	0.04
Nickel wire	187/368	0.1
Lead (99.9% purity, No oxidized)	127/260	0.06
Copper	199/390	0.18
Cobalt	599/1110	0.19
Steel	199/390	0.52
	599/1110	0.57
Tinned iron sheet (Light)	28/82	0.23
Brass (High-polish)	247/476	0.03
Brass (Tough rolled, polished metal wire)	21/70	0.04
Tinned Iron (Light)	-	0.13
Iron plate (Rust eaten)	20/68	0.69
Rolled steel sheet	21/71	0.66
Ferric oxide	100/212	0.74
Wrought-iron	21/70	0.94
Fused iron	1299-1399/3270-2550	0.29
Copper (Polished)	21-117/70-242	0.02
Copper(Polished, not reflected)	22/72	0.07
Copper (Heavy oxide Board)	25/77	0.78
Enamel (Fuse on iron)	19/66	0.9
Formica Plate	27/81	0.94
Frozen soil	-	0.93
Brick (Red, rough)	21/70	0.93
Brick (Unglazed, rough)	1000/1832	0.8
Carbon (T - carbon 0.9% ash)	127/260	0.81
Concrete	-	0.94
Glass (Glossy)	22/72	0.94
Granite (Surfaced)	21/70	0.85
Ice	0/32	0.97
Marble (I Polished, grey)	22/72	0.93
Asbestos board	23/74	0.96
Asbestos paper	38/100	0.93
	371/700	0.95
Asphalt (Paving the road)	4/39	0.97
Paper (Black tar)	-	0.93
Paper (White)	-	0.95
Plastic (White)	-	0.91

3. Set **temperature area**.

a. Tick the name checkbox, then set the name.

b. Choose the type (point, line, polygon)

c. Press and hold the left mouse button, and drag in the video area to draw a temperature area. Right-click to finish the area selected.

4. Click **SAVE**.

Note: *ID 0 is the full screen; The area cannot be changed.*

 *: the lowest temperature of the full screen.*

 *: the highest temperature of the full screen.*

 *: the lowest temperature of the area.*

 *: the highest temperature of the area.*

Schedule Linkage

Go to **Setup > Thermal > Schedule Linkage.**

There are seven type alarm linkage, threshold alarm, threshold warning, temperature difference alarm, temperature difference warning, temperature section alarm, temperature rise alarm, temperature rise warning.

The signal of alarm is set at **Temperature Alarm** page.

Figure 70 Schedule Linkage

Check the checkbox to enable linkage action.

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

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

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

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

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

White light alarm: it will flash the white light to alarm when alarm happened if you selected the white light alarm.

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.**

Thermal Mapping

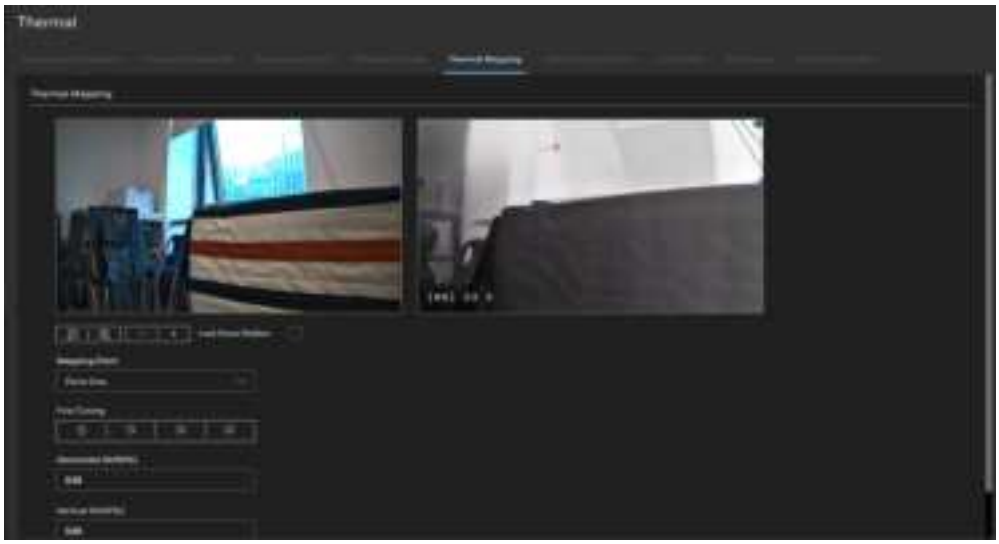
When the temperature measurement areas of the optical channel and thermal channel don't match, user can use this function to adjust.

If Temperature Measurement Information Mapping Visible Light is enabled and the temperature measurement area seen in optical channel does not match the temperature measurement area in thermal channel, the Thermal Mapping needs to be adjusted.

Firstly, user can use the **Mapping points** to adjust. If there are still minor inconsistencies for the temperature measurement areas, user can use **Fine turning**, **Horizontal shift(%)** and **Vertical shift(%)** to adjust in detail.

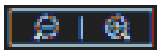
1. Go to **Setup > Thermal > Thermal Mapping.**

Figure 71 Thermal Mapping



2. Set the parameters of thermal mapping following the table.

Table 12 Thermal Mapping Parameters

Parameter	Description	Setting
	Zoom out / zoom in	[Setting method] Click
	Far focus / Near focus	[Setting method] Click
Lock focus position	Users adjust the position for mapping to lock this position. Zoom and Focus can't be operated when enabling this function	[Setting method] Enable

Parameter	Description	Setting
Mapping point	You need to map three points for two channels. Points are corresponding of each other. Point one + (green cross) Point two: + (red cross). Point three: + (blue cross) blue cross. Steps: a. Choose mapping point one, the green cross shows on two channel images, and choose the same position on two channels as for point one. b. Choose mapping point two and point three in a time, follow the previous step. c. Click APPLY and check if the temperature measurement area of optical is consistent with that of thermal channel.  **Note:** It is best to cover the temperature measurement area with three mapping points and form a triangular pattern. The three mapping points should not be too close.	[Setting method] Select from drop list.
Fine turning	Click the icon to adjust the position trifle. When measure area on optical channel is deviate the thermal channel's, you can adjust it. The temperature area of optical channel will be moved.	[Setting method] Click
Horizontal shift(%)	Adjust horizontal position of area which is on visual image. The effect is same as the fine tuning, it is another method to adjust.	[Setting method] Input value
Vertical shift(%)	Adjust vertical position of area which is on visual image. The effect is same as the fine tuning, it is another method to adjust.	[Setting method] Input value

3. Zoom and focus the optical channel, so that the two channels are at the same field view. Then lock focus position.
4. Choose the point in turn to set the three mapping points, the detail information please see the previous table.

5. The point is not match up perfectly, adjust trimming by click the arrows of fine turning.
6. Click **SAVE**.

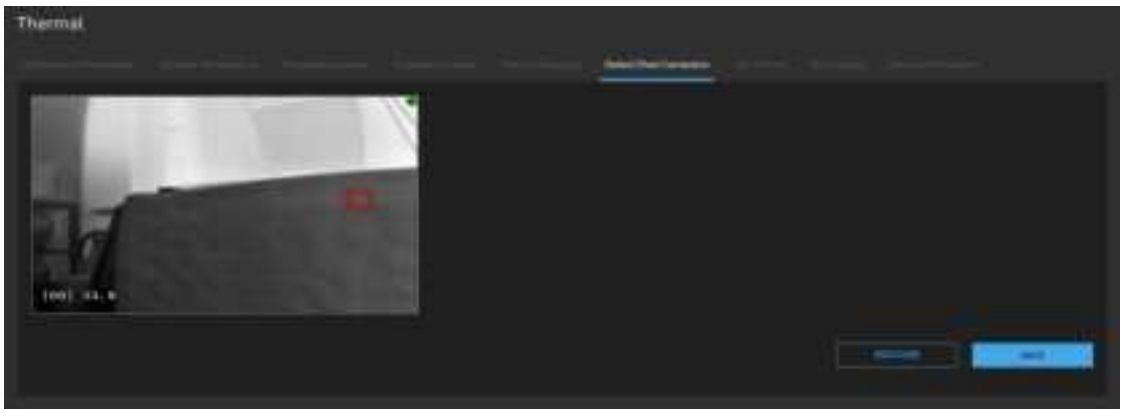
Defect Pixel Correction

1. Go to **Setup > Thermal > Defect Pixel Correction**.

If the image has a white or special dot as shown in Figure 73, users can use the function to recover the defect pixel.

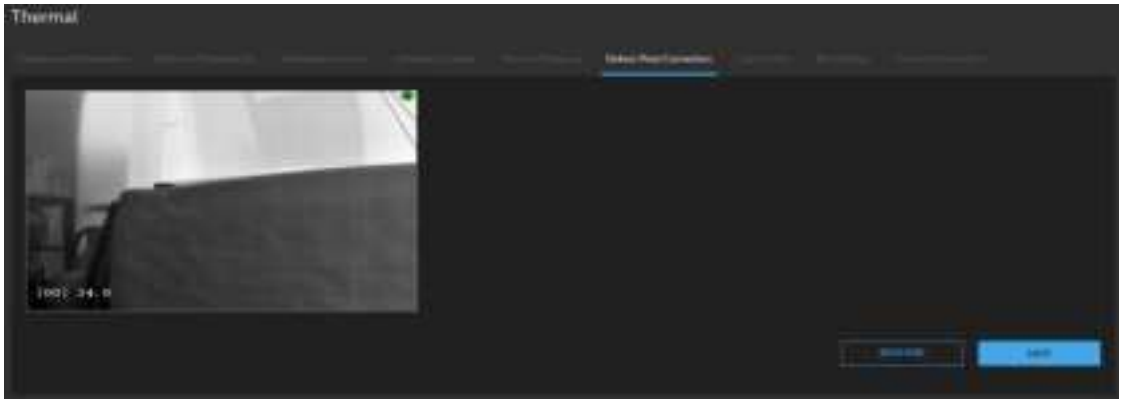
Note: *Users should connect the technical support at this condition to make sure to apply.*

Figure 72 Defect Pixel Correction



2. Click the white point at image, click RESTORE to recover the defect pixel, as shown in Figure 74 .

Figure 73 Recover Defect Pixel

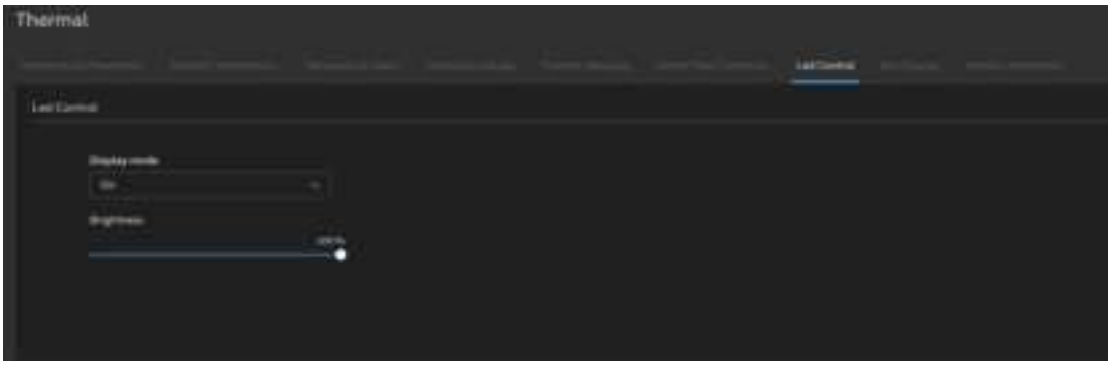


3. Click **SAVE**.

Led Control

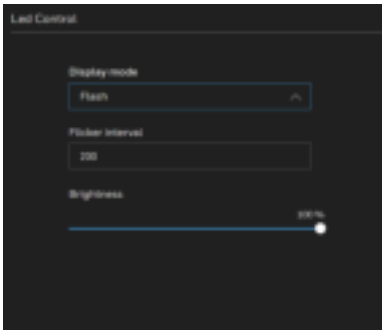
Set the display mode and brightness of LED, as shown in Figure 74. It is the white light alarm settings.

Figure 74 Led Control



Display Mode: There are five modes can be chosen.

- **On:** the LED is always lighting.
- **Off:** the LED is closed.
- **Flash:** set the flicker interval, the LED will flicker as the set.



- **Timing on:** the LED will be lighting at the set time.

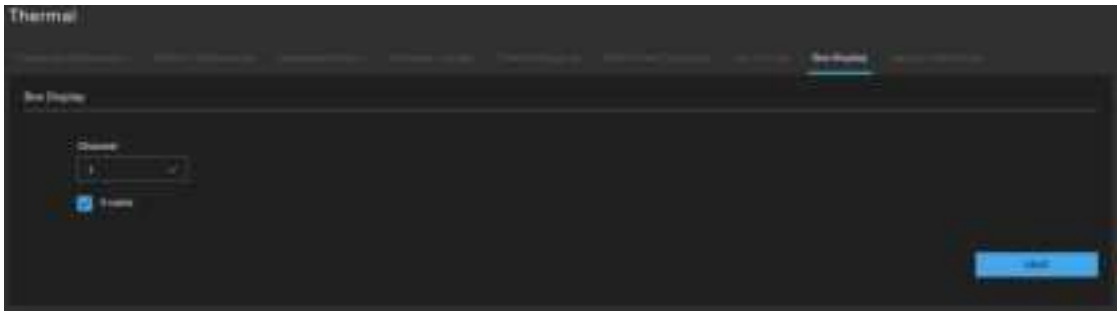
- **Alarm on:** the LED will be lighting at the alarm time.

Brightness: the LDE's brightness. 100% is the brightest.

Box Display

The blue box shows on web when the human body is detected. This is embedded bounding Box in streaming. The box will show blue when human body or vehicle is detected. Box will show red when VA alarm happened.

Figure 75 Box Display

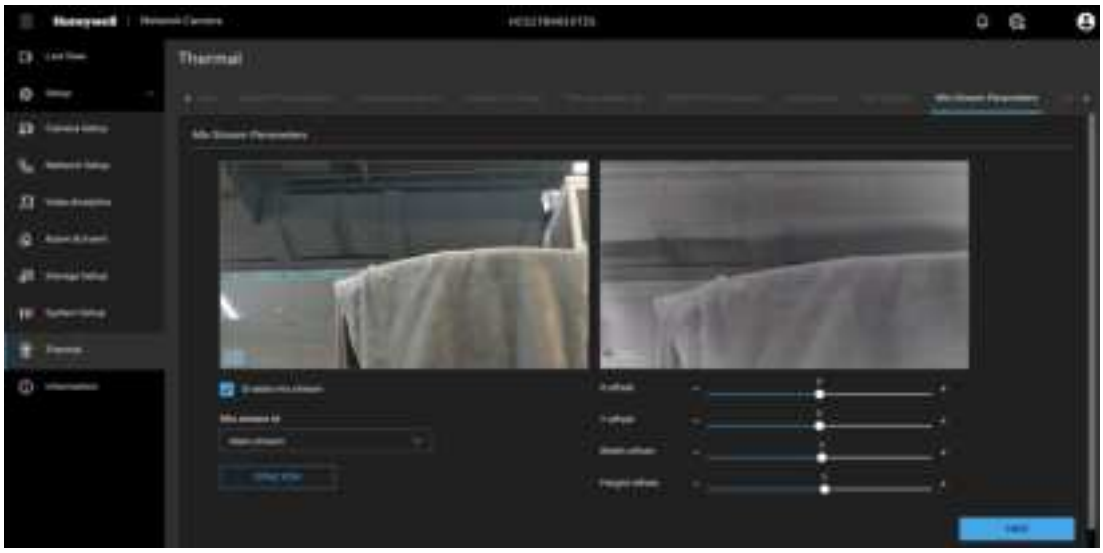


Choose the channel to enable. The default is enabling for two channels.

Mix Stream Parameters

The mix stream is that the optical channel's image is mixed to thermal channel, the thermal channel's image has both channels information.

Figure 76 Mix Stream Parameters



Stream ID: the mix stream image shows on which stream of thermal channel, all / stream 1 /stream 2.

SYNC FOV: Click the button, the field view of optical channel will be sync with thermal channel's.

X Offset and **Y Offset**: The mix stream mode is open. The thermal image and optical-light image are mixed, if the positions of two channel isn't mapping, you can set the offset to move optical channel image. X offset is adjusting left and right direction. Y offset is adjusting up and down direction.

Width Offset and **Height Offset:** Adjust the aspect ratio.

Version Information

The version information about the device, so that we can track products.

CHAPTER

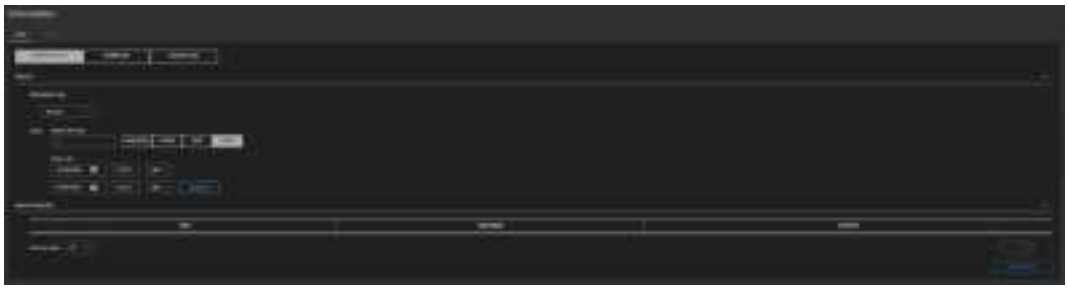
11 VIEWING SYSTEM INFORMATION

Logs

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

Operation Log

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



1. Select the type of operation logs to be queried from the drop-down list box.
2. Set the start time and end time as required.
3. Click SEARCH.

   The operation logs are displayed.
4. Click Download on the right of the page to download the operation logs.

Alarm Log

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

1. Select the type of alarm logs to be queried from the drop-down list box.
2. Set the start time and end time as required.
3. Click SEARCH.

4. The alarm logs are displayed.
5. Click Download on the right of the page to download the operation logs.

Collect Log

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

1. Click **COLLECT**, the download page is displayed.

2. Select the path to save the logs.

Version

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

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

CHAPTER

12 TROUBLE SHOOTING

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 13 Troubleshooting for Common Issues

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

The edge browser doesn't support H265 live view.	1.Open the edge browser, input "edge://gpu". 2.Find "Media Foundation Rendering Capabilities", make sure the "HEVC installed " and "HEVC activatable" is true. a) If they are false, you need to download the HEVC Video Extensions. b) input "https://www.microsoft.com/store/productId/9N4WGH0Z6VHQ?ocid=pdpshare" to download HEVC Video Extensions , click "Install" to jump to Microsoft store, download the Extension and install. 3.Reopen the edge browser after Finishing the installation.
The temperature is inaccurate.	1.Check the ambient temperature, reset it, at **Setup > Thermal > Ambient Temperature** page. 2. Check the distance, reset it, at **Setup > Thermal > Temperature parameter** page. 3. Check the emission reset it, at **Setup > Thermal > Temperature parameter** page**.**
When the ambient temperature is the same as the target temperature, the target will not be detected.	
When the surface temperature of the object is close to the ambient temperature, the thermal imaging VA has a high probability of failing to identify the vehicle.	Adjust the sensitivity.
Fire spots detection sometimes be incorrectly triggered by other heat sources.	Adjust the sensitivity.
There is no audio file output when two-way audio is ongoing.	Disable two-way audio.

CHAPTER

13 APPENDIX

List of Symbols

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

Table 14 List of Symbols

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

	The protective earth (ground) symbol. This symbol indicates that the marked terminal is intended for connection to the protective earth/grounding conductor.
	Eurasian Conformity (EAC) RoHS

Building Automation – Security Americas (Head Office)
Honeywell Commercial Security
715 Peachtree St. NE
Atlanta, GA 30308
Tel: +1 800 323 4576

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

Building Automation – Security Middle East/N. Africa
Emaar Business Park, Building No. 2, Sheikh Zayed Road
P.O. Box 232362
Dubai, United Arab Emirates
security_meta@honeywell.com
Tel: +971 4 450 5800

Building Automation – Security Europe/South Africa
Building 5 Carlton Park,
King Edward Avenue
Narborough, Leicester, LE19 0LF
United Kingdom
Tel: +44 (0) 1163 500714

Building Automation – Security Northern Europe
Stationsplein Z-W 961, 1117 CE Schiphol-Oost, Netherlands
Tel: +31 (0) 299 410 200

Building Automation – Security Deutschland
Johannes-Mauthe-Straße 14
D-72458 Albstadt
Germany
Tel: +49 (0) 7431 801-0

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

Building Automation – Security Italia SpA
Via Achille Grandi 22,
20097 San Donato Milanese (MI), Italy

Building Automation – Security España
Josefa Valcárcel, 24
28027 – Madrid, España
Tel.: +34 902 667 800

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

Building Automation – Security and Fire (ASEAN)
Honeywell International Sdn Bhd
Level 25, UOA Corp Tower, Lobby B
Avenue 10, The Vertical, Bangsar South City
59200, Kuala Lumpur, Malaysia
Email: buildings.asean@honeywell.com
Technical support (Small & Medium Business):

Vietnam: +84 4 4458 3369
Thailand: +66 2 0182439 Indonesia: +62 21 2188 9000
Malaysia: +60 3 7624 1530
Singapore: +65 3158 6830
Philippines: +63 2 231 3380

Honeywell Home and Building Technologies (India)
HBT India Buildings
Unitech Trade Centre, 5th Floor,
Sector – 43, Block C, Sushant Lok Phase – 1,
Gurgaon – 122002, Haryana, India
Email: HBT-IndiaBuildings@honeywell.com
Toll Free Number: 000 800 050 2167
Tel: +91 124 4975000

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

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

Honeywell

https://buildings.honeywell.com/security
+1 800 323 4576 (North America only)
Document 600-35UG03 Rev A– 03/2025