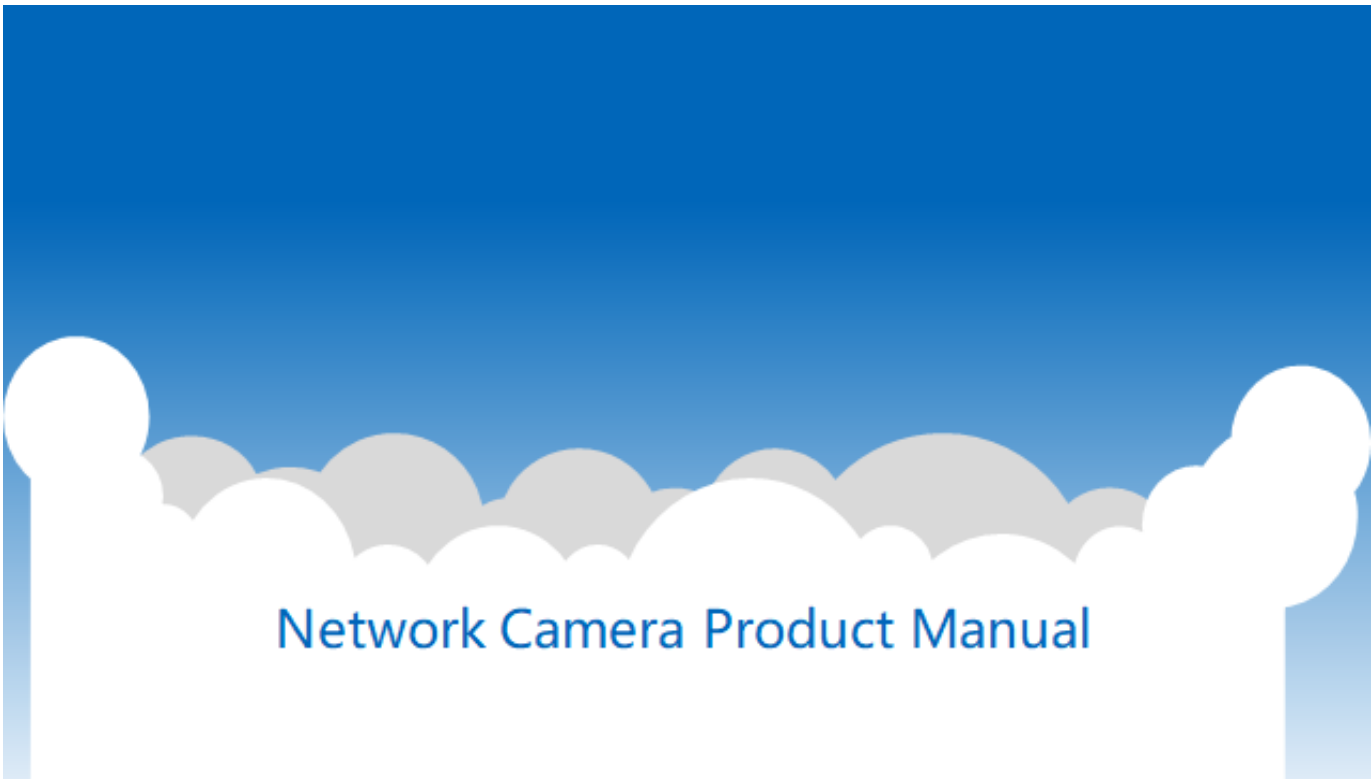
Network Camera

Product Manual



V1.0.2

Preface

This document details the fucntions of the product and its configuration. Please read the content carefufully before using the product and keep this document safely for future reference.

Key Symbols

The following symbols may appear in this document and their meanings are as follows:

symbol	description
	This indicates a moderate- or low-level potential risk that, if not avoided, could result in minor or moderate injuries to the user.
	This indicates a potential risk that, if ignored, could lead to the damage of the device, data loss, reduced device performance, or unpredictable results.
	This indicates additional information to support the main text by providing further emphasis or complementary information.

Update History

Version number	Update Contents	Release date
V1.0.2	Add WIFI function	2024.12
V1.0.1	Update the function of Disarming Update the function of Auto Upload	2024.09
V1.0.0	First release	2024.04

Declaration

This product manual applies to all of our smart IP camera product lines.

Please refer to the actual product, the product manual should be only used as reference.

This product manual may contain technical inaccuracies or typographical errors.

The product and/or software described in the product manual may be improved or updated at any time and are subject to upgrade without notice.

The screenshots in this product manual are not from the same machine, and are for illustrative purposes only.

If you have any inquiries regarding the latest procedures and supplementary documentation, please contact the company's after-sales service department.

Safety Precautions

The following are the requirements for the correct use of the product.In order to prevent any risks and property damage, please read the product manual carefully before using the product and strictly follow the instructions provided.

Shipping Requirements

Caution

- Please transport the device under the permissible humidity and temperature conditions.
- Please ship the device with its factory packaging or equivalent materials.
- Do not handle the device with heavy pressure, harsh vibrations or soak the device during shipment.

Storage Requirements

Caution

- Please store the device under the permissible humidity and temperature conditions.
- Avoid placing the device under conditions that are moist, dusty, extremely hot or cold, under strong electromagnetic radiation or under unstable lighting conditions.
- Do not handle the device with heavy pressure, harsh vibrations or soak the device during storage.

Installation requirements

Warning

- Please strictly follow your local electrical safety standards and confirm that the power supply is correctly set up before the equipment is put into operation.
- Please strictly follow the following power supply requirements.
- When selecting a power adapter, please use a power supply that meets the SELV(Safe Extra Low Voltge) standards and supplies power according to the standard rated voltage of GB8898(IEC60065) or GB4943.1(IEC60950-1 or IEC62368-1 for Limited Power Source).The specific power supply requirements are based on the equipment label.
- If the device arrives with a power adapter, it is recommended to use the included power adapter.
- Unless otherwise specified, do not provide two or more power supply methods to the device simultaneously, otherwise the device may incur damages.
- The equipment should be installed in a place only accessible by professionals (the professionals need to clearly understand the safety precautions for using this equipment). Non-professionals accessing the equipment installation area while the equipment is in use may incur accidental injuries.

Caution

- Do not handle the device with heavy pressure, harsh vibrations or soak the device during installation.
- Please install an easy-to-use mechanism (or device) when instaliing the wiring so that an emergency power-off can be performed when necessary.
- It is recommended to use this device with lightning protection to improve the lightning protection effect. Any outdoor use must also meet the lightning protection specifications.
- The dome is an optical device and should not be directly touched when wiping its surface during installation.

Operational Requirements

Warning

- To prevent burns, please avoid touching the device cooling vents.

Caution

- Please use the device under the permissible humidity and temperature conditions.
- Ordinary equipment should not be used in environments containing corrosive substances (e.g. chloride, SO2, etc.) such as seashores and chemical plants to prevent any damage to the appearance or function of the equipment.
- Do not focus the device on strong light sources (e.g. direct lighting, sunlight, etc.), otherwise it may cause an over-brightness or light pulling (which is not a malfunction), which may also affect the life of the photosensitive CMOS (Complimentary Metal Oxide Semi-conductor) sensor
- When using the laser device, avoid exposing the surface of the device to the radiation from the laser beam.
- Do not inject liquids into the device to avoid internal damages to the device.
- Do not expose the indoor equipment to rain or moisture to avoid fire hazards or an electric shock.
- To avoid heat accumulation, do not block the device's cooling vents. Protect the plug from being stepped on or pressed, especially at plugs, electrical outlets and other contacts leading from the unit.
- Do not touch the CMOS directly; instead, use an air gun to remove dust or dirt from the surface od the lens. The dome is an optical device, therefore do not touch the surface of the dome directly.
- Please ensure the protection of your network, device data and personal information, including but not limited to the use of strong passwords, the regular change of passwords, updating firmware to the latest version and isolating computer networks. For some of the older versions of IP camera firmware, the ONVIF (Open Network Video Interface Forum) password will not be automatically changed after the system's master password is changed. You will either need to update the camera's firmware or manually update the ONVIF password.

Maintenance and Repare Requirements

Caution

- Please strictly refer to this document for the disassembling of the equipment. Illegal disassembly may result to leakage or malfunctioning of the equipment.Ensure that the sealing ring is flat and in the mounting groove before closing the cover of the equipment involved in the disassembly operation.
- Please use the parts or accessories specified by the manufacturer and have them installed and repaired by professional service personnel.
- Clean the device with a clean, soft cloth. If the dirt is difficult to remove, gently wipe it off with a small amount of neutral detergent using a clean soft cloth, and then wipe dry, Do not use volatile solvents such as alcohol, benzene or thinner, or strong, abrasive cleaners, as this may damage the surface coating or reduce the performance of the equipment.
- The dome is an optical device. Dirt such as dust, grease or fingerprints can be gently wiped with a little ether or a clean soft cloth (or a soft cloth dampened with water). Dirt can also be gently wiped off with an air gun.
- It is normal for stainless steel cameras to rust on the surface after being used in a strong corrosive environments (eg. Seasides, chemical plants, etc.), for a period of time. You can use a soft cloth with mild abrasiveness dipped in a small amount of acidic solution (vinegar is recommended) to gently wipe the rust off and then dry.

Table of Contents

1 Product Overview

1.1 Product Introduction

IPC (IP Camera, Newtork Camera) is a combination of traditional cameras and network technology, and users can remotely connect to network cameras through a remote network connection for configuration and management.

Network connection

Before accessing the IP camera through the network, you need to first get its IP address; users can search for the IP address via the Quick Configuration Tool. Simultaneously, you need to set up the IP address, subnet mask and gateway for the computer host. Make sure that the IP camera is correctly connected to the network and check the local network status of the PC.

1.2 Functional Classification

The functions supported by different network cameras may vary slightly; please refer to the actual situation.

1.2.1 Basic Feautures

Real-time Monitoring

- Supports real-time previews of the device monitoring screen.
- Supports the preview screen to simulatenously open the sound and voice intercom, and to timely contact the monitoring site, so as to quickly deal with anomalies.
- Supports capturing abnormal situations on screen through snapshots or triple captures, which is

convenient for subsequent and handling of anomalies.

- Supports recording of abnormal situations occurring during monitioring, which is convenient for subsequent viewing and handling of anomalies.
- Supports setting coding parameters and adjusting the preview screen.
- Supports the real-time monitoring of intelligent alarms and displays alarm capture information while previewing.

Video

- Supports automatic recording, in accordance with the selected recording schedule.
- Supports video/picture playback to view valuable video clips or captured pictures.
- Supports video/pictire downloads as the basis for judgement.
- Supports alarm linkage recording when the alarm occurs i.e.linkage to the corresponding channel records.

Account Management

- Supports adding, modifying and deleting user groups, and managing the permissions assigned to each user group.
- Supports adding, modifying and deleting users, and setting user permissions.
- Supports changing the user password.

1.2.2 Smart Features

Alarm

- Supports setting alarm prompts or sounds according to the alarm type.
- Supports viewing the alarm push information.

Video detection

- Supports motion detection, video detection, video color cast, video blur focus, and scene change detection.
- Supports linkage recording alarm output, sending emails, caputuring pictures, etc. when an alarm occurs.

Intelligent Dynamic Inspection

- Supports intelligent dynamic detection used to detect the movement range of people, non-motor vehicles or motor vehicles on the screen.
- Supports linkage recording, linkage audio, alarm output, sending emails, capturing pictures, etc. when an alarm occurs.

Perimeter Protection

- Supports tripwire intrusion, area intrusion, people gathering, people wandering, items left behind, moving items, parking detection and other intelligent perimeter functions.
- Supports linkage tracking, linkage recording, linkage audio, alarm output, sending emails, capturing pictures, etc. when an alarm occurs

Face detection

- Supports displaying face detection information such as face-related attributes on the preview interface.
- Supports linkage tracking, linkage recording, linkage audio, alarm output, sending emails, capturing pictures, etc. when an alarm occurs.

Video Structuring

- Supports the detection of people, motor vehicles, and non-motor vehicles in the captured video, and displays the relevant attribute features in the preview interface.
- When an alarm occurs, it supports linkage alarm output.

People Counting

- Provides statistics based on the flow of people entering and exiting the detection area and outputs statistical reports.
- An alarm will be triggered when the number of counted people meet the people limit or the stay time exceeds the preset time.
- Supports linkage recording, alarm output, sending email, audio and capturing when an alarm occurs.

Heatmap

- Supports the counting of cumulative density of target movements and displays the heat values wih different colors.
- Supports viewing heatmap reports.

Alarm Settings

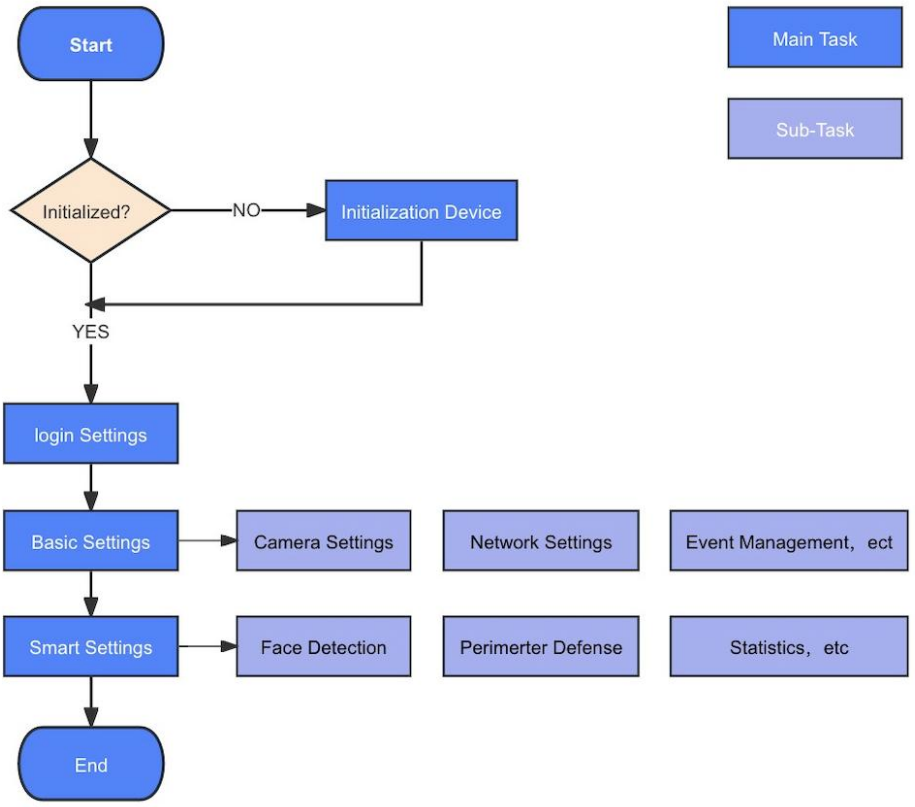
- Triggers an alarm when an external alarm input device generates an alarm.
- Supports linkage recording, alarm output, sending emails, PTZ operation and capturing images when an alarm occurs.

Anomaly Handling

- Supports SD card anomalies, network anomalies, illegal access detection and security anomly detection.
- Supports linkage alarm output and sending emails when an alarm occurs for an SD card anomaly, unauthorized access, or security anomalies,
- Supports linkage recording, alarm output and sending emails when a network anomaly alarm occurs.

2 Configuration Process

Please refer to the relevant configuration process to complete the configuration based according to the actual requirements.



Configuration process

configuration	Description	Reference Chapters
evice initialization	When using the device for the first time or after restoring factory configurations, the user needs to complete the initialization process (such as setting a password) before accessing the device normally.	Chapter 3 Device Initialization
Device Sign-In	Enter the device IP address into a PC (computer) browser to log in to the web interface. The default IP address of the device is 192.168.1.86.	
Setting Up Basic	Basic features include setting up camera	

Functions	properties, setting up IP addresses, managing events, managing local storage, and more.	
Setting Up Smart Features	Setting up detection rules for intelligent events	

Instruction

3 Device Initialization

After using the device for the first time or after restoring the factory configurations, the user needs to initialize the device (for example, setting the password for the admin user).This article uses the WEB operation as an example to introduce the initialization process. The user can also use the ConfigTool or NVR (Network Hard Disk Recorder) to initialize the device.

Instructions

1、To ensure the security of the device, please keep the admin password properly after the device is initialized, and remember to change it regularly.

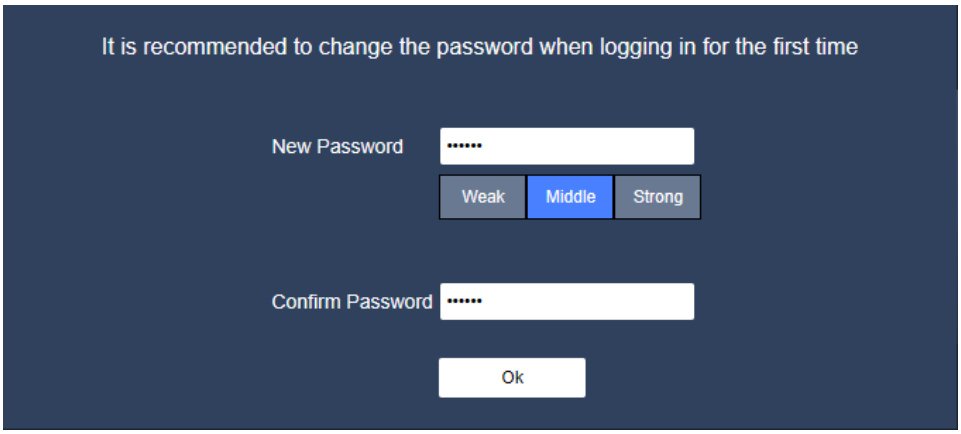
2、When initializing the device, ensure the IP address of the PC is on the same network as the IP address of the device.

3、The browsers Internet Explorer 11 and Google Chrome are recommended.

Procedure

Step 1: Open a browser, enter the IP address in the address bar (the default IP address is 192.168.1.86), and press enter

Step 2: Set the log-in password for the admin account. This is as shown in the figure below.



Log-In Initialization

Parameters	Description
Password	Set the passwsord for the admin user account; the password must be set to 6-32 non-empty characters consisting of numbers, letters and common characters (with the exception of quotation marks, spaces and Chinese characters). Set a high-security password according to the password strength prompt.
New Password	

Description of the password setting parameters

Step 3: Click “Ok”

4 Basic Features

This section describes the basic functions of the device, including the device log-in, camera settings, network settings, event management, system management and system information.

4.1 Device Log-In

Log in to the device web interface through the recommended browsers, Internet Explorer 11 or Google.

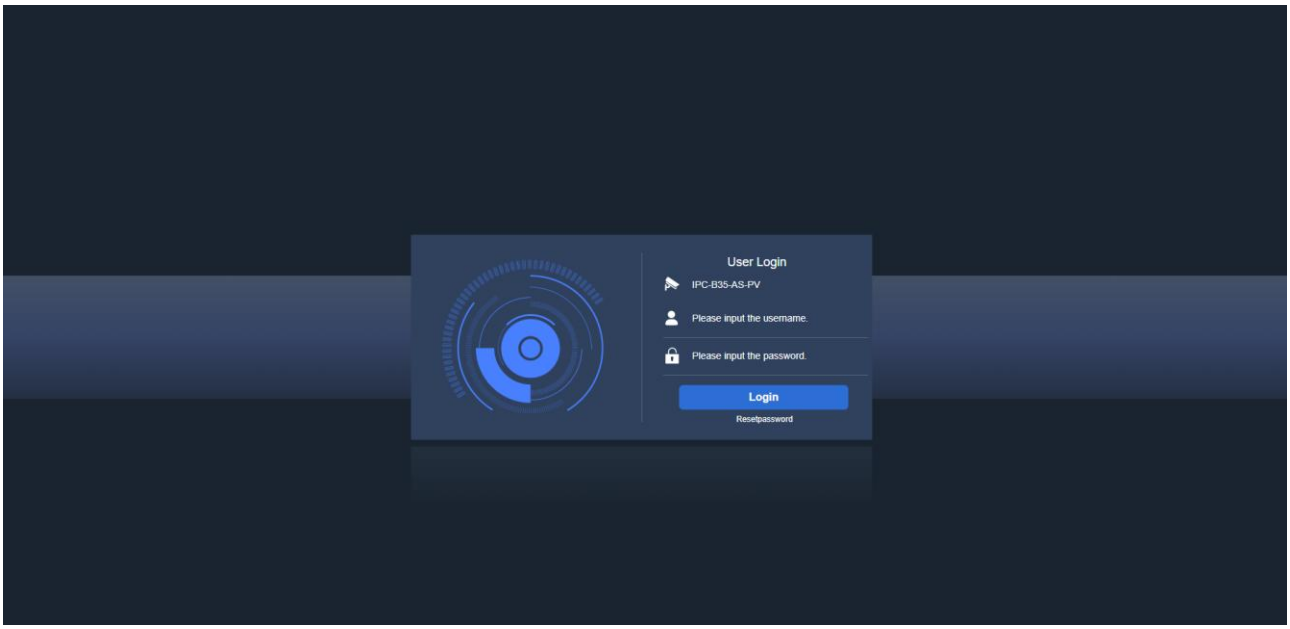
Please complete the device initialization and re-log in to the web interface (see Chapter 3 Device Initialization for further details).

When a user signs in to the device, ensure that the PC’s IP address is on the same network as the device’s IP address.

Procedure

Step 1: Open a browser, enter the device's IP address in the address bar (the default IP address is 192.168.1.86), and press Enter.

Step 2: Enter the username and password; the default user name of the device is "admin".



Log-In

Step 3: When logging in to the device for the first time, the sytem will pop up a "Change Password" prompt. Please change the administrator password on time and safe-keep it.

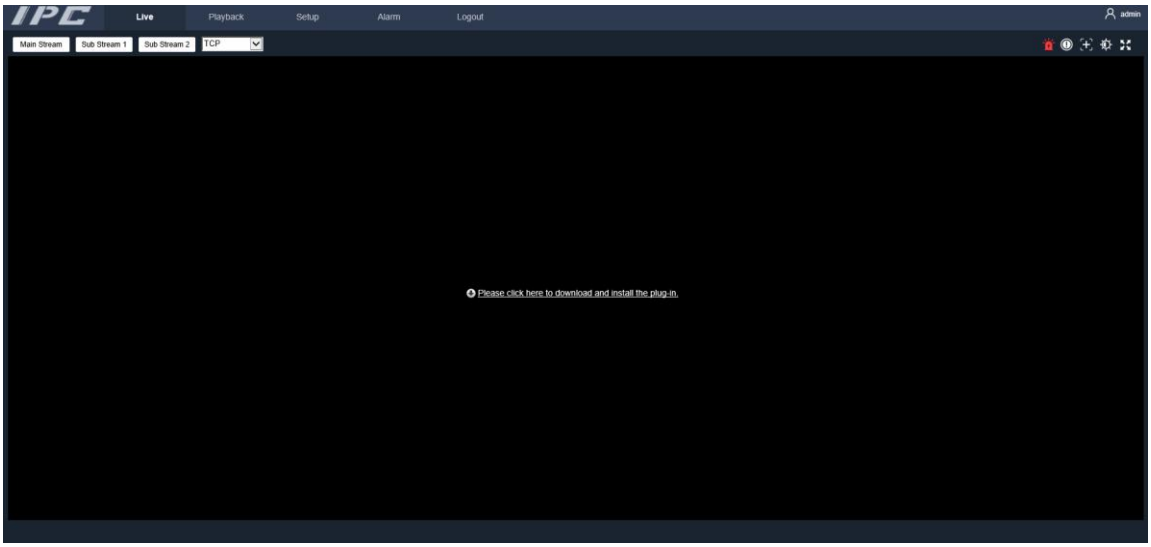
Modifying the password

Instructions

Reset Password: If the user forgets the password, click Reset Password to get a key. After the customer sends this key to our technician, our technician will generate a new decoding key for the user, and the password will be reset to the default password "123456".

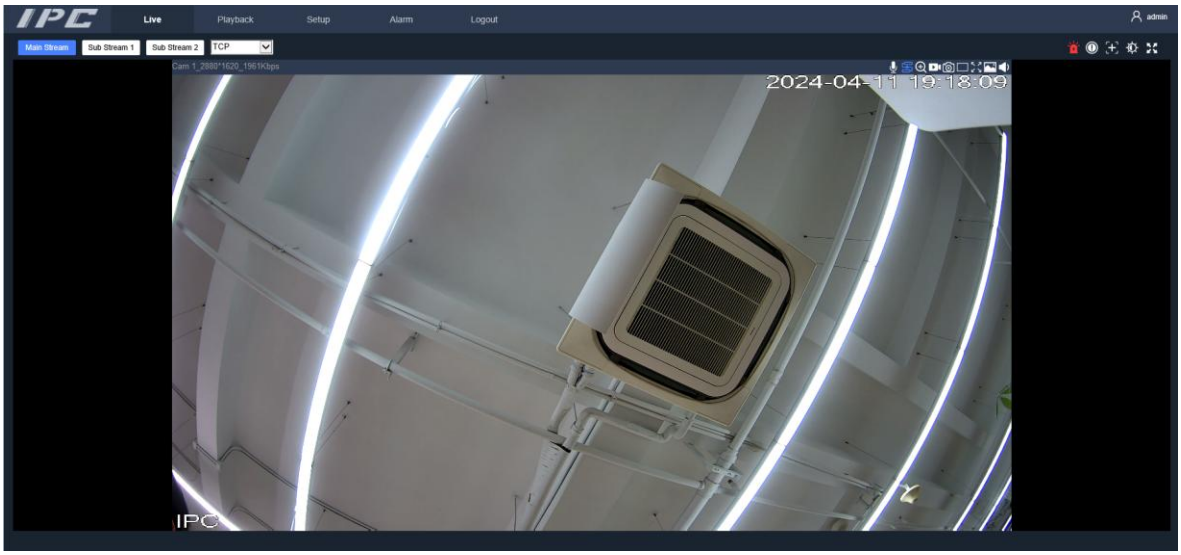
Note: The device should not be powered off or restarted during this operation, otherwise the generated key will be invalid.

Step 4: Click Login. After logging in, the system will display preview interface by default and afterward the “Please click here to download the plug-in” prompt link will appear. Click it to install the plug-in as show in the figure below.



Downloading the plug-in

Step 5: After installation, restart the browser and log in. On the main interface of the IP camera, one can preview, playback, parameter settings, alarm and other functions, as show in Figure 3-4:



3-4 Real-time preview

4.2 Camera Settings

This chapter decribes the settings of the camera parameters, including video configuration, image configuration and audio configuration.

4.2.1 Video Parameter Configuration

Set video parameters, including video streaming, capture configuration, video overlay and region of interest.

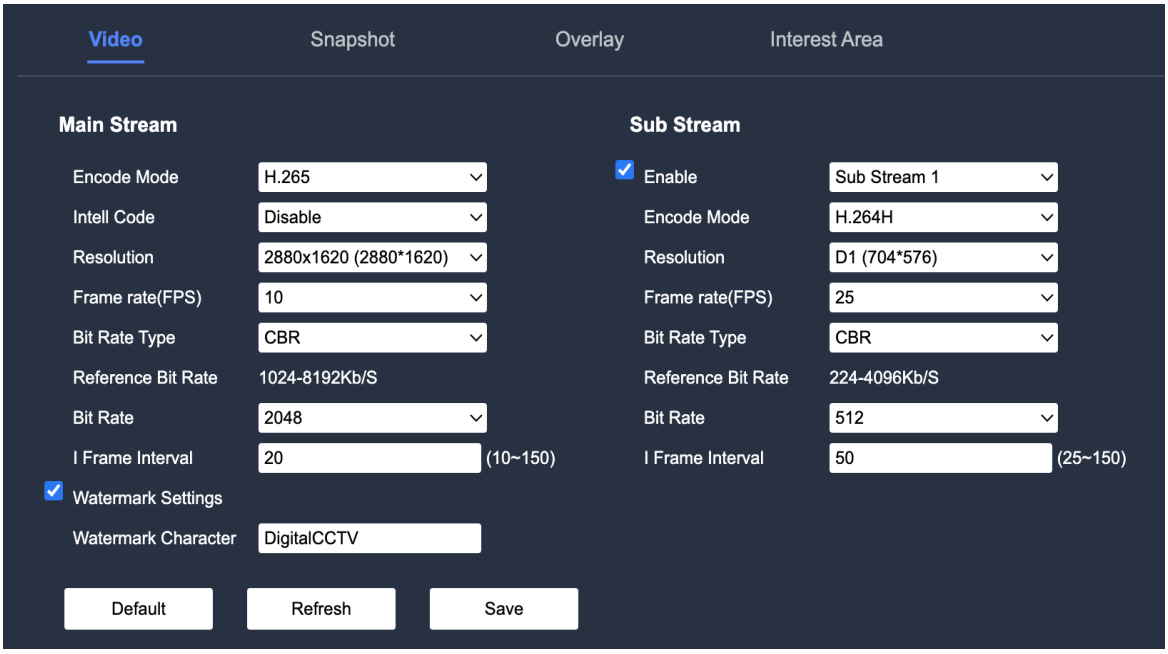
4.2.1.1 Video Stream Set Up

Set the video streaming parameters according to the network bandwidth, including stream type, enconding mode, resolution, frame rate, stream control, stream rate, frame interval, watermark settings, etc.

Procedure

Step 1: click “setup” in the upper right corner of the interface, and choose Camera-video config-Video.

Step 2: Set the parameters.



Video Stream Set Up

Parameter	Description
Auxillary Code Stream	Select “Enable” to enable secondary streaming, which is enabled by default. The device can support multiple secondary streams at the same time.
Smart Encoding	Enable Smart Encoding to improve image compression performance and reduce the storage space required for images.
Encoding Mode	Select the encoding mode based on the network bandwidth • H.264: including H.264B (Baseline Profile encoding mode), H.264M(Main Profile encoding mode) and H.264H(High Profile encoding model, all three equal in image quality. The bsndwidth occupied by the three decreases sequentially at the same quality. • H.265: Main Profile encoding mode, even under same image quality, the bandwidth is smaller that that of the H.264
Resolution	The higher the value of the video image, the clearer the image but, the larger the occupied bandwidth.
Frame Rate (FPS)	FPS is the number of frames per second that the video contains. The higher the frame rate, the more realistic and smoother the image will be.
Bitstream control	This represents how the bitstream is controlled when the video data is transmitted. • Fixed Stream: The bitrate varies around the set bitrate value, which may result in unclear images when the scene is complex and wasted bandwidth when the scene is simple. • Varied bitrate: The bitrate automatically adjusts with the change of complexity of the monitoring scene in order to maintain the scene’s complexity and clarity; clearer images when the scene is complex, and smaller bandwidth when the scene is simple.
Quality	This parameter is supported when “Bitrate Control” is set to to “Varied Bitrate. The better the video quality, the more the bandwidth occupied.
Reference Bitstream	The optimal range of bitstream values recommended to the user is

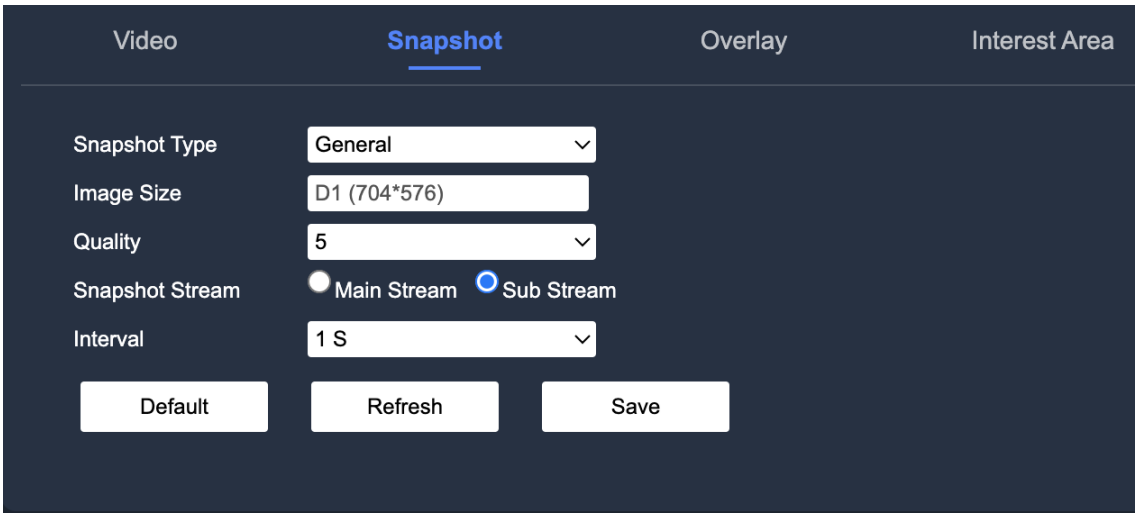
	based on the resolution and frame rate set by the user.
	1、When “Bitstream Control” is set to “Fixed Bitrate”. Based on the actual scenario and the recommended Reference Bitstream value, select the appropriate stream value in the Stream drop-down list. 2、When “Bitstream Control” is set to “Varied Stream”. Select the upper limit of the bitrate according to the Reference Bitstream value; the bitrate will automatically adjust with the complexity of the monitoring scene. However, the maximum bitrate value will change towards the set upper limit of the bitrate value.
I-Frame Interval	For the number of P-frames between 2 I-frames, the smaller the value the lower the number of P-frames and the higher the quality of the image. The range of the I-frame interval varies with the frame rate. It is recommended to set the I-frame interval to 2 times the frame rate.
Watemark Settings	After setting a watermark for video stream, the user can check whether the video has been tampered with by checking the watermark characters • Check “Watermark Settings” to enable the watermark feature. • Enter the watermark characters/symbols, the default is DigitalCTTV
Watermark Characters	

Step 3； Click “Save” to complete the video stream.

4.2.1.2 Snapshot Configuration

Step 1: Click “setup” in the upper right cornwe of the interface, and select Camera-video Config-Snapshot

Step 2: Set Snapshot parameters



Snapshot Configuration

Parameter	Description
Snapshot Type	This includes both normal and triggered captures. • Normal Capture: A normal capture is a snapshot that takes a picture within the range set by the schedule. • Trigger capture: Refers to the capture sets of images when a video detects intelligent events snd alarms.
Image Size	The resolutions of main and secondary streams are the same, but cannot be modified.
Image Quality	Sets the image capture quality by the grades: lowest, lower, lowest, medium, higher and highest.
Snapshot Stream	Sets the type of capture stream. The types are main stream and secondary stream, in which the secondary stream is the default.
Snapshot Speed	Sets the drawing frequency of the image.

Step 3: Click “Save” to complete the snapshot configuration.

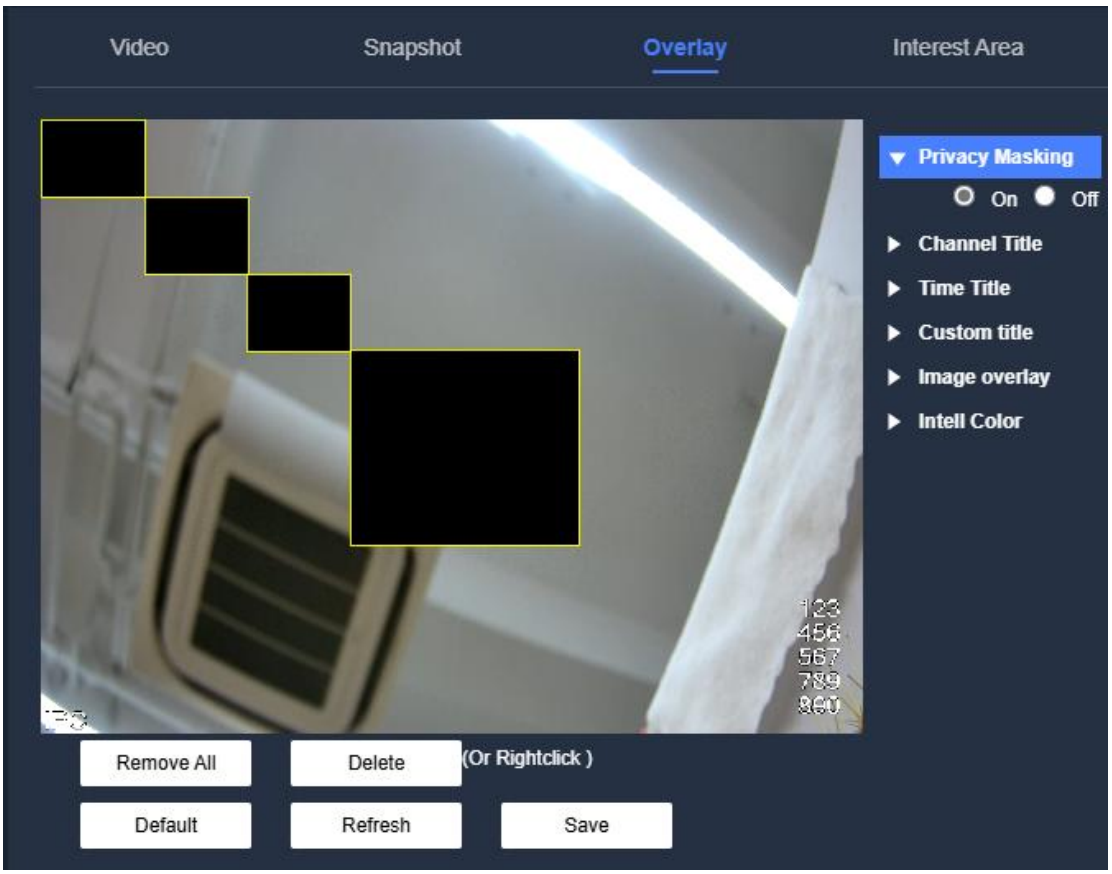
4.2.1.3 Video Overlay Settings

Set the video overlay information and the preview page displays the corresponding overlay information.

Procedure

Step 1: Click “setup” in the upper right corner of the interface and select “Camera-video Config Overlay to display the video overlay interface.

Step 2: Set up area overrides. When it is necessary to protect the privacy of a particular area on the video screen, the user can set the area override. Select “Enable” and drag the region box to the privacy area and to protect the privacy area.



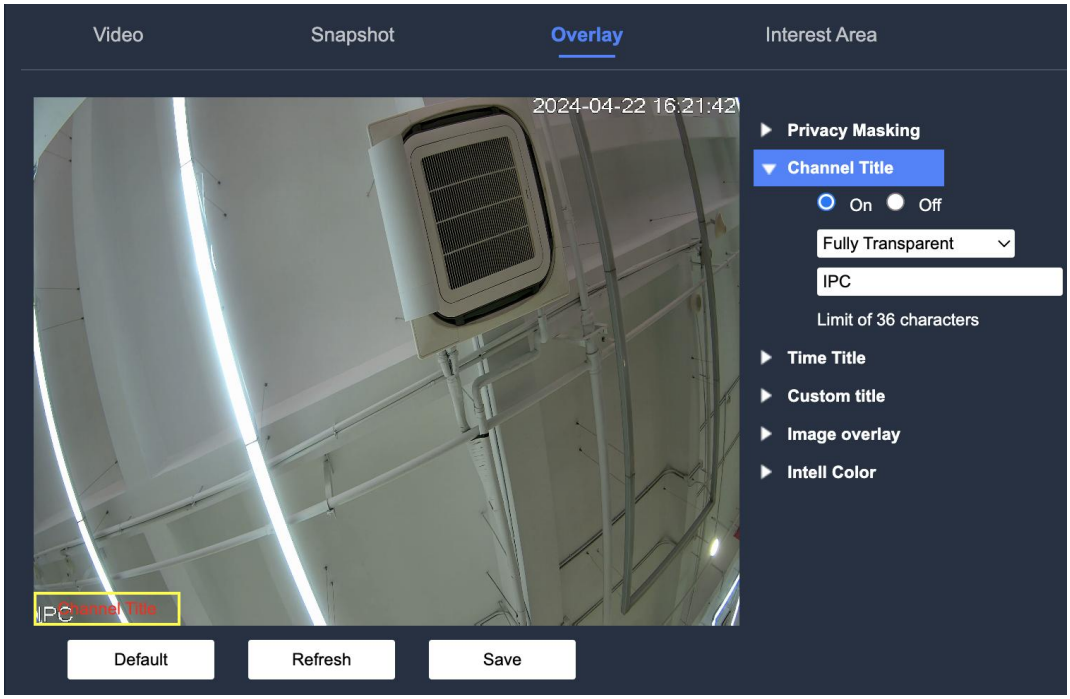
Instructions

1、Privacy masking frames are automatically generated on the screen, and up to 4 privacy masking frames can be added.

2、Click “Clear” to delete all privacy occlusion frames, select “Privacy Occlusion Frame” and click Delete to delete the corresponding privacy occlusion frame. The area coverage box is resizeable.

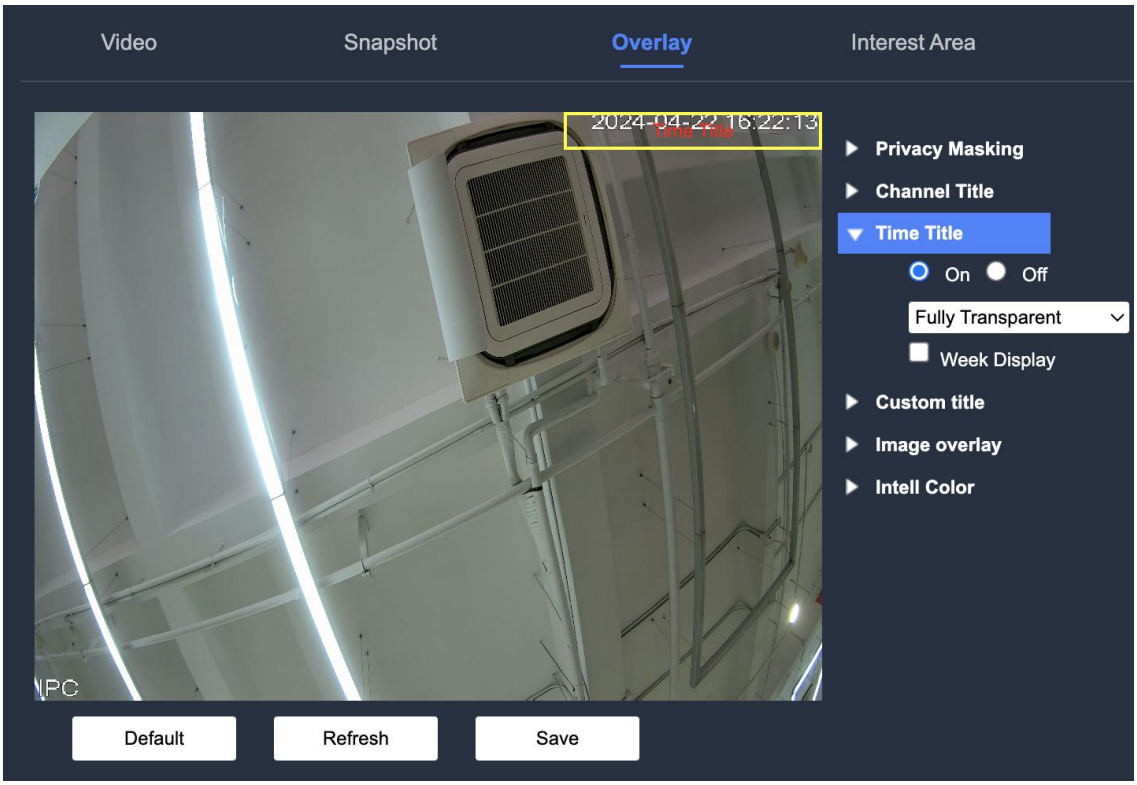
Step 3: Set the channel title needed to be displayed on the video screen.

1、Click “Channel Title” to display the channel title interface, as shown in the following figure:



2、Select “On” and set the channel title. The channel title will be displayed on the video screen. The user can drag the channel title of the animation surface and place it in the appropriate.

Step 4: Sets the time title when it is preferred to display the time information on the video screen. Click “Time Title” to display the time title page, as shown in the following figure:

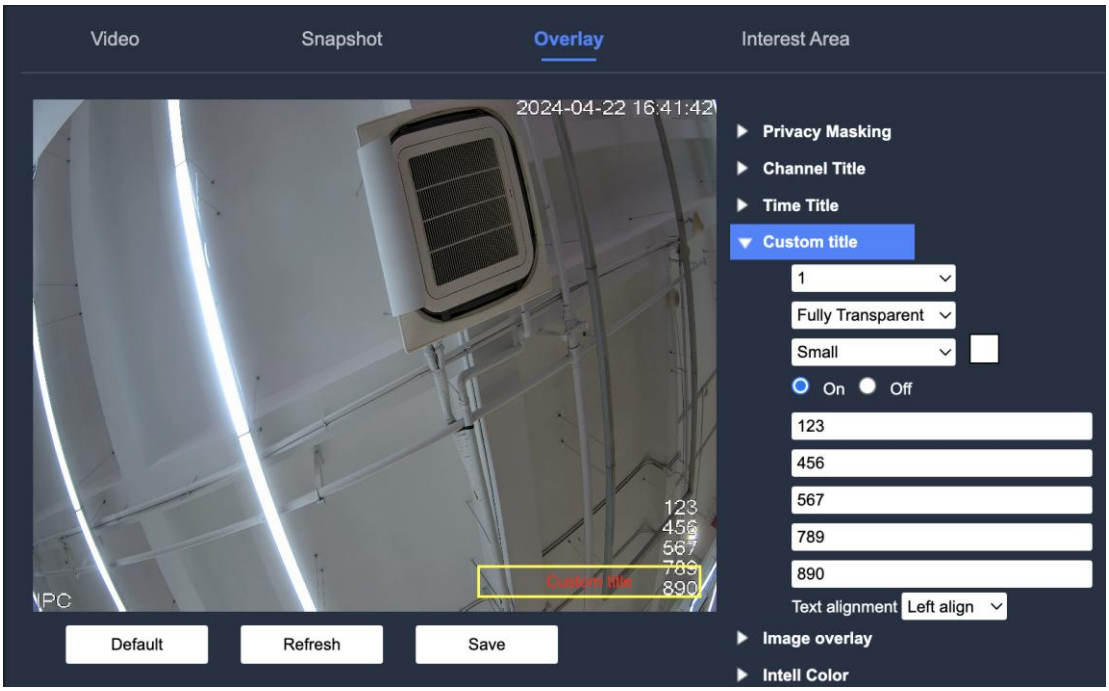


1、Select “Enable”, the time will be displayed on screen and the user can drag the time title of the animation interface and put it in a suitable position.

2、Select “Show Day” to display the day of the week on the video screen.

Step 5: Sets a custom title when needed to display other information on the video screen

1、Click “Custom title” to display the custom title interface, as shown in the following figure:



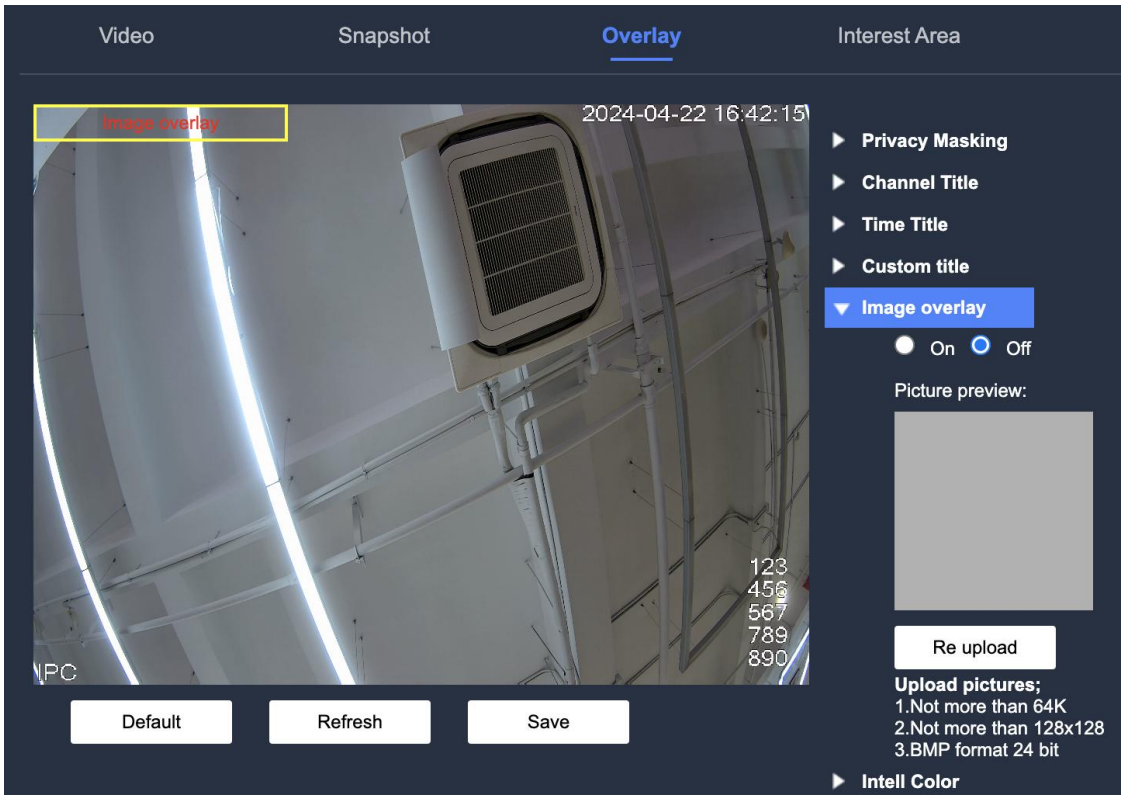
2、Select “On” and the custom title information will be displayed on the video screen. Sets the custom overlay, alignment, font size and transparency and drags the custom title of the animation surface and places it in the appropriate postion.

Instructions

Supports the set up of upto 4 sets of custom overlay

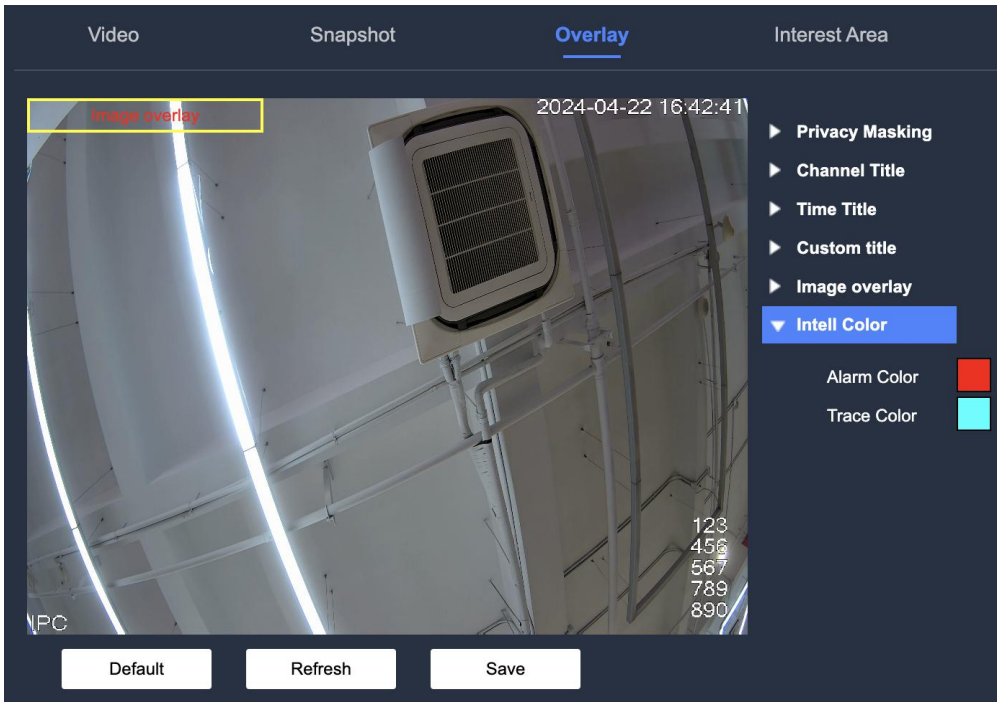
Step 6: Set the image overlay. When necessary to display image information on the video screen, the user can set the image overlay.

1、Click “Image Overlay” to display the image the overlay page, as shown in the following figure:



2、Select “On”, click “Upload”, select the image to be overlayed and the overlayed image will appear on the video screen. Position the image in the preferred position and click “Save”.

Step 7: Set the colors of the smart box and alarm box, and click “Save” when done as illustrated in the figure below:

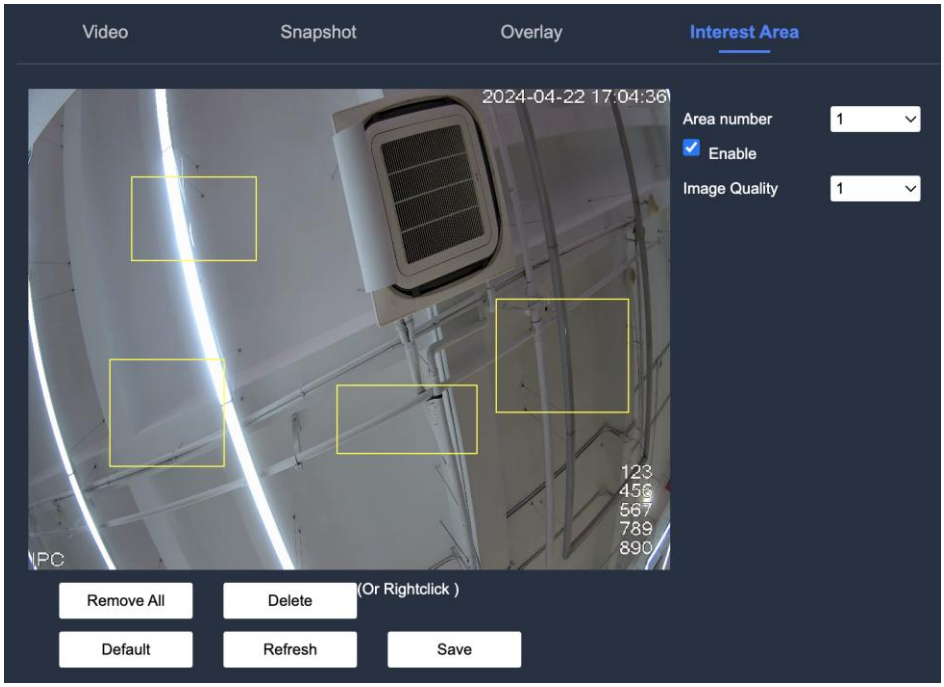


4.2.1.4 Intrest Area Settings

Set the Interest Area in the picture and set the image quality of the region of interest. The picture of the region of interest will be displayed according to the image quality.

Procedure

Step 1: Click “setup” on the upper right corner of the interface, and select Camera-video config-Interest Area. The Interest Area interface will be displayed as follows:



Step 2: Select “Enable”, drag the region box to the area of interest and set the image quality of thr Interest Area.

Instructions

1、Supports up top 4 Interest Areas

2、The higher the image quality value , the better the image quality

3、Click “Clear” to delete all region boxes, select a region box, click “Delete”or right-click to delete th region box.

4.2.2 Image Configuration

Adjust the camera’s image, exposure, day/night transition, backlight, white balance, image

enhancement and other attributes according to the actual environment. Improves the clarity of the monitoring scene by adjusting the camera parameters to ensure that the monitoring is normal, as shown in the picture below:

Instructions

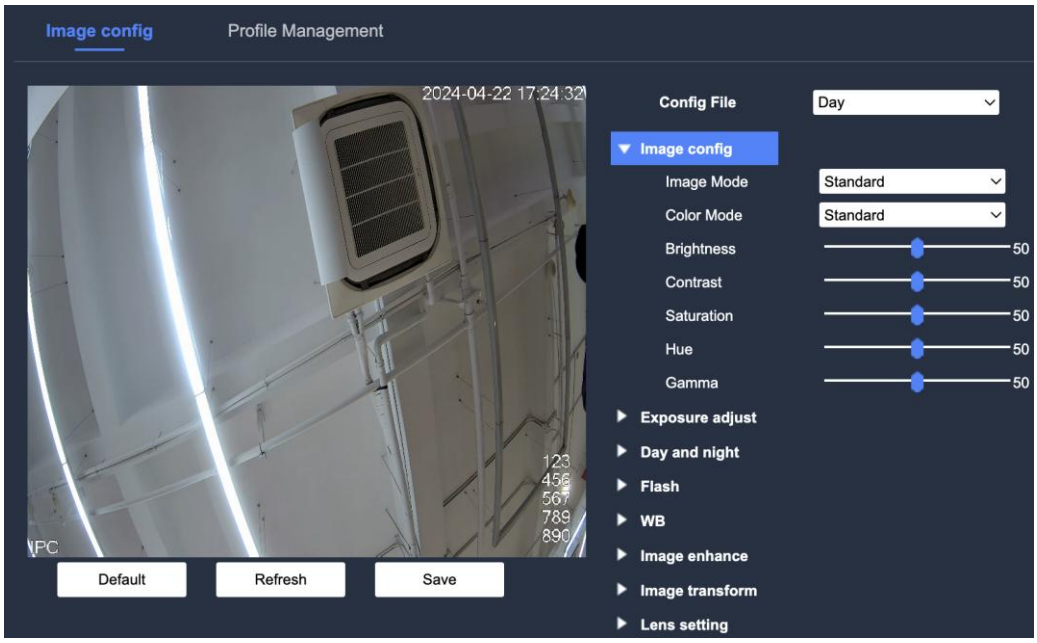
The camera parameters may vary from model to model, please set them according to the product model.

4.2.2.1 Image Adjustment

The user can adjust the image parameters according to the environment's requirements.

Procedure

Step 1: Select Settings-Camera Settings-Image Configuration-Image Adjustment to display the image configuration interface as shown in the figure below:



Step 2: Parameter setting, see the table below.

Parameters	Description
Image Mode	Sets the image mode to either transparency mode or real mode. The user can set it according to the scene's requirements.
Color Mode	Sets the color mode to either the standard mode or brilliant mode. The user can set it according to the scene's requirements.
Brightness	Sets the brightness and darkness of the image. The higher the value, the brighter the image and vice versa. If the value is too large, the screen will turn white.
Contrast	Sets the ratio of black to white in an image (i.e contrast).The larger the value, the richer the colors on the image and vice versa. If the value is too large, the darker parts of the image will get too dark and the brighter parts will overwhelm the image. And if the value is too small, the image will gray.
Saturation	Sets the vividness of the image. The higher the value, the more vivid the image and vive versa. Adjusting the saturation does not affect the overall brightness of the image.
Chroma	Changes the color space and adjust the color bias to the same direction.
Gamma	Changes the brightness and contrast of the image via non-linear adjustment. The higher the value, the brighter the image and vice versa.

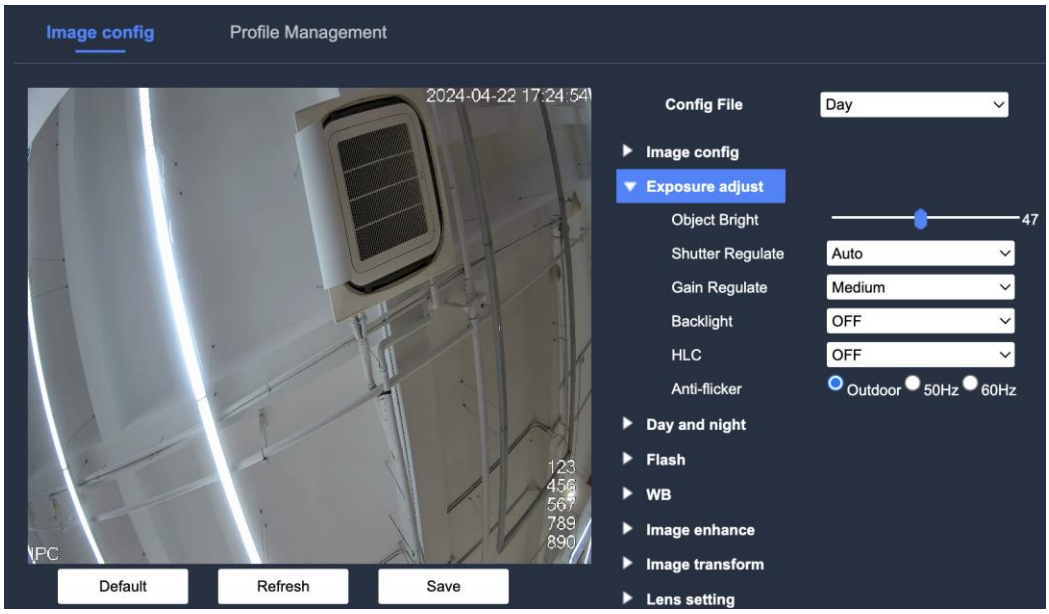
Step 3: Click "Save" to complete the configuration the camera image adjustment parameters**.**

4.2.2.2 Exposure Adjustment

The image can become much clearer by adjusting the lens aperture, shutter, etc.

Procedure

Step 1: Select Settings – Camera Settings – Image Configuration - Exposure Adjustment; the Exposure Adjustment interface will appear as follows:



Step 2: Parameter settings, see the table below.

Parameters	**Description**
Target Brightness	Adjusts the brightness of the video frama
Shutter Adjustment	Sets effective exposure time. The lower the value, the shorter the exposure time. The longer the exposure time, the brighter the video.
Gain Adjustment	Adjusts the gain upper limit, and the user can select different gain levels depending on the actual requirements.
Backlight Compensation	Sets the backlight compensation function. Turning on backlight compensartion in a backlit environment can prevent silhouettes on the darker parts of the subject of the video.
Glare Suppression	Sets the glare suppression of a video. When an extremely strong light is present in the environment, turning on strong light suppression will suppress the brightness of the highlighted area of the image, reduce the size of the halo area, reduce the brightness of the whole image and capture the details of facial attributes and license plates in dark environments. The higher the value, the more obvious the light suppression.
Anti-flicker	There are three anti-flicker modes: 50Hz, 60Hz and outdoor.

	• 50Hz: When the mains power is 50Hz, the exposure automatically adjusts according to brightness of the scene to ensure that the image does not appear in horizontal streaks. • 60Hz: When the mains power is 60Hz, the exposure automatically adjusts according to the brightness of the scene to ensure that the image does not appear in horizontal streaks. • Outdoor: When Outdoor is selected, the exposure mode can be set to “Gain Priority” and “Shutter Priority”. Different devices support different exposure modes.

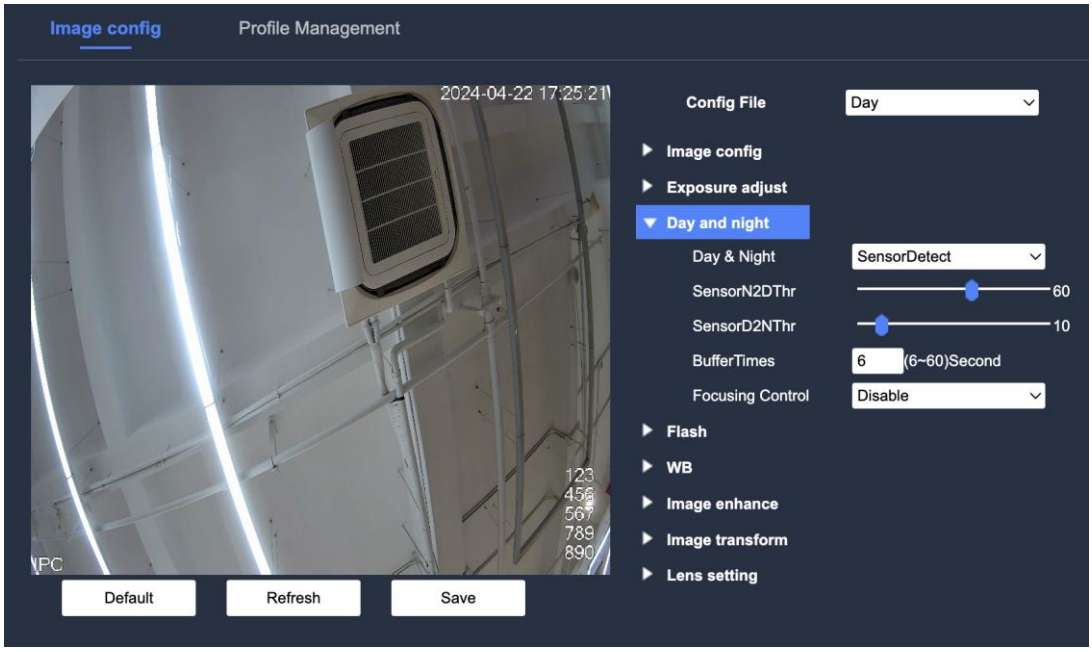
Step 3: Click “Save” to complete the configuration of the camera exposure adjustment parameters.

4.2.2.3 Day and Night

Sets the image display to black and white, multi-color or switches between mutli-color and black and white depending on the environment’s requirements.

Procedure

Step 1: Select Settings – Camera Settings – Image Configuration – Day and Night, and the Day and Night Switching interface will appear, as shown in the image below:



Step 2: Parameter setting, see the table below

Parameter	Description

Day and Night Mode	Sets the device image display to black and white, multi-color or sensitivity switching. • Black & White: The image is displayed in black and white. • Color: The image is displayed as a color image. • Sensitivity Switching: The device automatically selects a color mode or black-and-white mode according to the brightness of the environment. **Instructions** The day/night mode settings are not affected by the "Profile Management" settings.
Black-to-color Threshold	This configuration can be set when the day-and-night mode is set to sensitivity switching. The higher the setting, the brighter the ambient light required to be switched to color and vice versa.
Color-to-black Threshold	This configuration can be set when the day-and-night mode is set to sensitivity switching. The larger the value, the darker the ambient light required to switch to black-and-white, and vice and versa.
Buffer Time	This configuration can be set when the day-and-night mode is set to sensitivity switching. When the ambient illumination exceeds the threshold (black-to-color threshold and color-to-black threshold), wait for the response time and then switches between day and night.
Focus Fine-tuning	For motorized zoom lens devices, the device will fine-tune the focal length of the picture between day and night to ensure day and night confocal after checking.

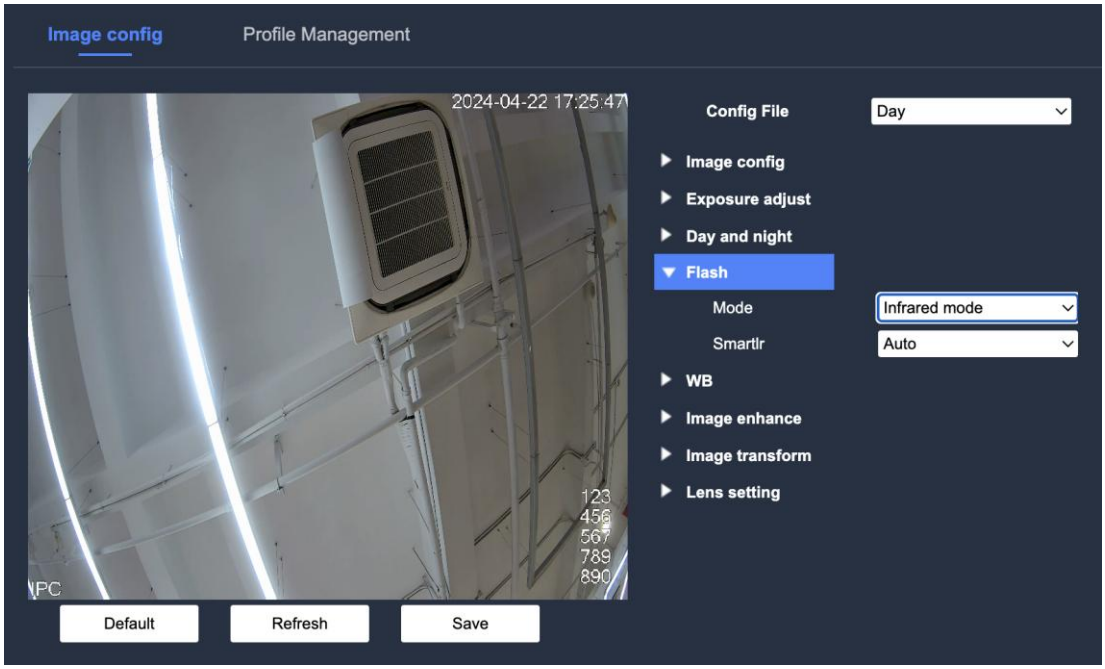
Step 3: Click "Save" to complete the configuration of the camera's day/night switching settings.

4.2.2.4 Fill Light

When the device comes with a fill light, the user can set the fill light mode. Common fill lights are divided into infared fill lights and white fill lights. Different models of equipment support different types of fill lights; therefore, configurations may vary, please refer to the actual situation.

Procedure

Step 1: Select Settings – Camera Settings – Image Configuration- Flash to display the day-and-night switching interface, as shown in the figure below:



Step 2: Parameter settings, see the table below.

Parametes	Description
Mode Configuration	When the device comes with a fill light, the user can set a preferred fill light scheme, including infrared mode, white light mode and smart mode. Infrared Mode: only turns on the infrared light, and can only capture black and white pictures. • White Light Mode: only turns on the white light and captures the scene clearly. • Smart Mode: When the device triggers the smart alarams, white light fills the light and image gets clearly captured
Smart Infrared	Automatic: The system automatically adjusts the brightness of the fill light according to the actual scene.
	Manual: Manually sets the brightness of the fill light and the system will fill the image according to the set value. Smart mode does not support manual configuration. Smart Infrared Value: Sets the smart Infrared value, the larger the value, the brighter the fill light, and vice versa.The user should set the

	appropriate value according to the actual requirements.
	Off: Turns off the fill light.
Delay Time	The delay time for the smart alarm can be set in Smart mode. The corresponding delay time can be set according to the actual requirements.

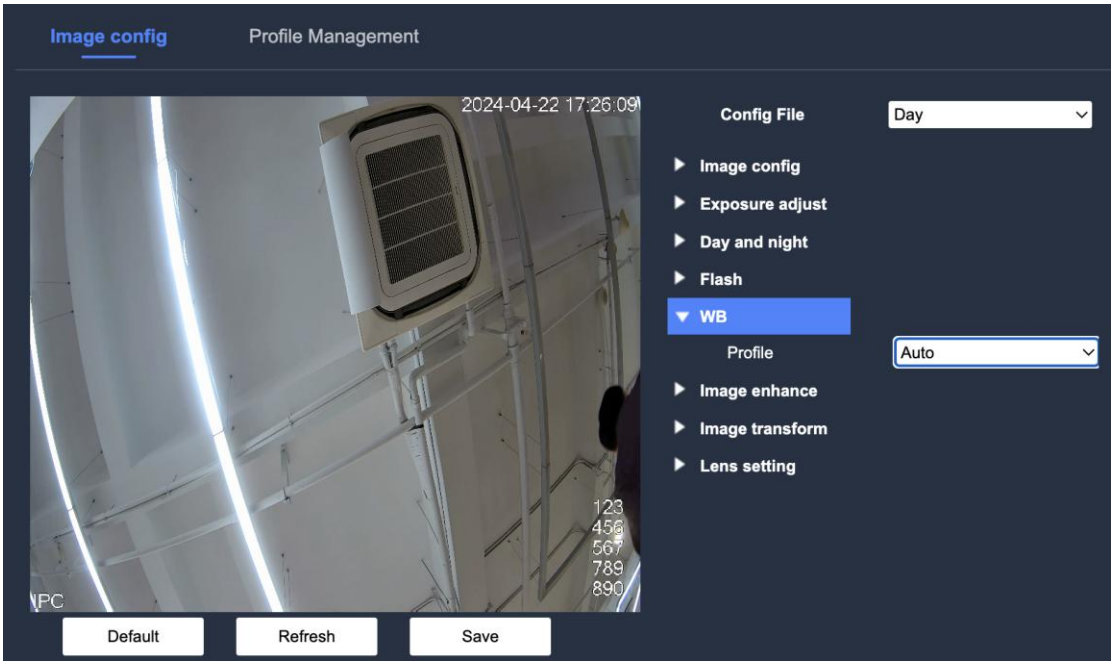
Step 3: Click β to complete the configuration of the camera fill light parameters.

4.2.2.5 White Balance

The white balance function can correct color deviations in an image caused by light, so that the white objects in the image still appear white even in different color environments.

Procedure

Step 1: Select Settings - Camera Settings - Image Settings - White Balance, to display the White Balance configuration interface as shown below



Step 2: Parameter settings, see the table below.

Parameters	Description	
	Automatic	The system automatically compensates for the white balance for different color temperatures, so that the image color is normal.
	White Balance Lock	The system only automatically fixes the color temperature to make the image color normal.

Scenario Mode	Fluorescent Light	The system automatically compensates for the white balance of the fluorescent lamp environment, so that the image color is normal.
	Incadescent Lamp	The system automatically compensates for the white balance of the incandescent lamp environment, so the image color is normal.
	Ultra-violet Lamp	The system automatically compensates for the white balance of the ultra-violet light environment, so that the image color is normal.
	Manual	Manually sets the red gain value and blue gain value, and the system will compensate for different color temperatures in the environment according to those settings

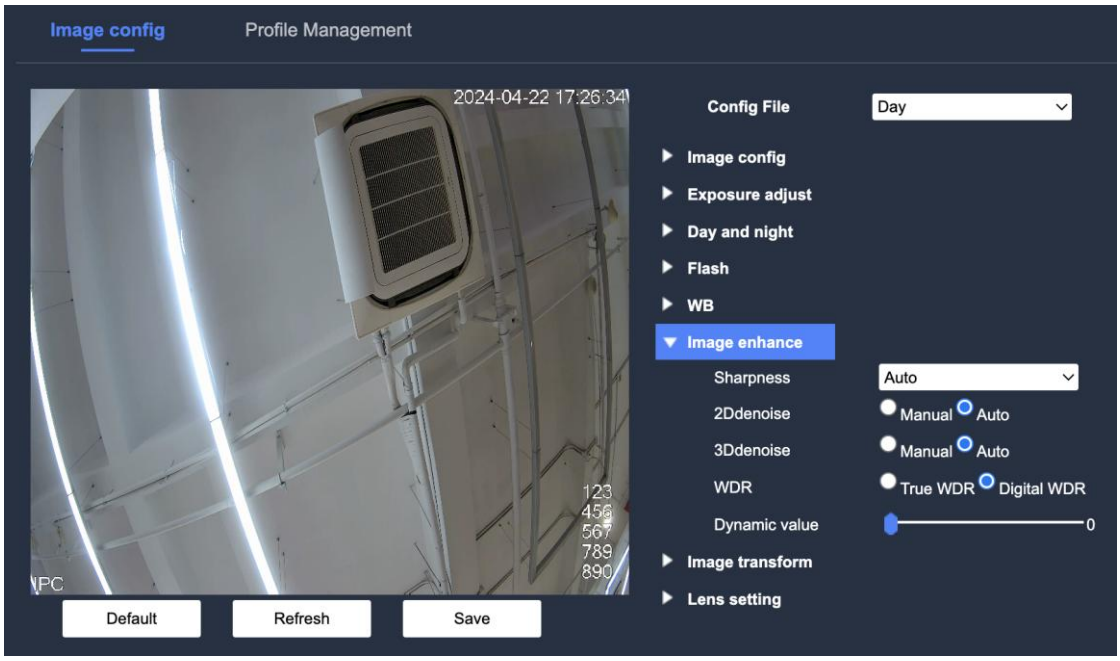
Step 3: Click “Save” to complete the configuration of the white balance parameters.

4.2.2.6 Image Enhancement

Sets image sharpness, noise reduction, wide dynamic range and other functions.

Procedure

Step 1: Select Settings – Camera Settings – Image Configuration – Image enhancement to display the image enhancement configuration interface, as shown in the image below:



Step 2: Parameter settings, see table below.

Parameter	Description	
Sharpness	Automatic	Automatically configures the sharpness value (i.e. how sharp the edges of the image are) based on the environment's requirements.
	Manual	Manually configures the sharpness value; the larger the value setting, the clearer the image and vice versa. With larger values, the image is prone to noise.
2D denoise	Automatic	The pixels within a single frame are averaged with other surrounding pixels to reduce image noise. This configuration reduces noise automatically according to the environment's requirement
	Manual	The pixels within a single frame are averaged with other surrounding pixels to reduce image noise. The noise reduction value can be manually set according to the requirements of the scene; the larger the value, the better the noise reduction effect.
	2D denoise Value	
3D denoise	Automatic	3D noise reduction is done automatically according to the requirements of the scene.
	Manual	For multi-frame (at least 2 frames) images, noise reduction is performed by utilizing the inter-frame information between the front and back frames of the video. The higher the value, the
	3D denoise Level	

		better the noise reduction effect, but the greater the picture drag.
WDR	True WDR	Turns on True WDR. The system reduces the brightness of high-brightness areas and increases the brightness of low brightness areas according to the requirements of the scene. The larger the value, the stronger the effect; the brighter the dark areas, the greater the noise.
	Digital WDR	Turns on Digital WDR. Enhances the brightness of the video screen.
Dynamic value	Adjusts the dynamic values of digital WDR and true WDR	

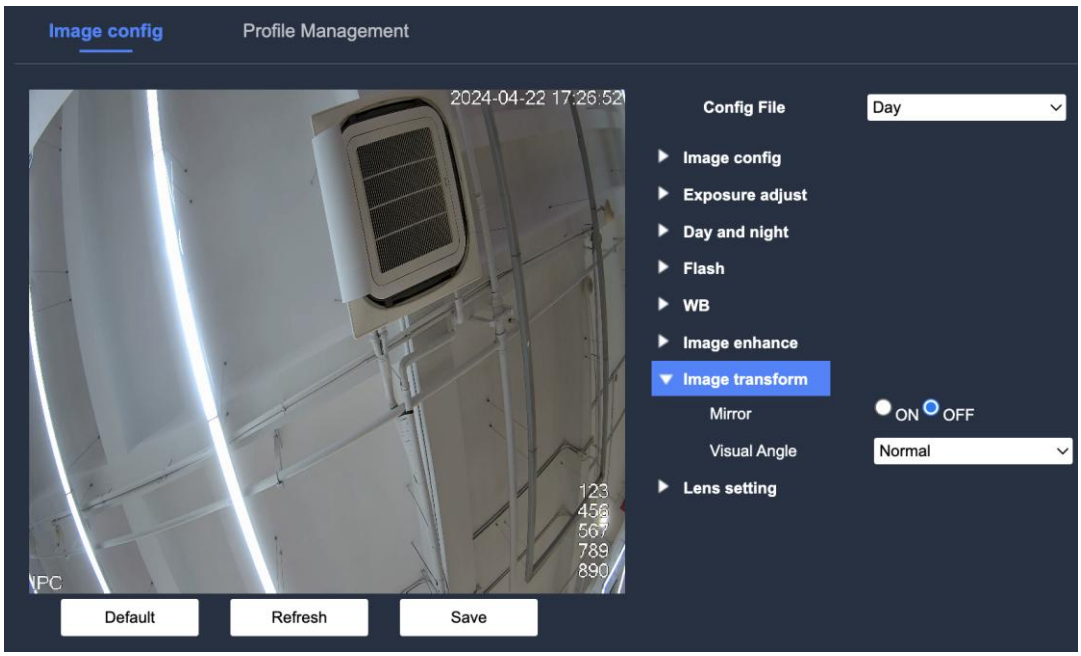
Step 3: Click “Save” to complete the configuration white balance configuration parameters.

4.2.2.7 Image Transformation

The image transformation function can flip and mirror the image.

Procedure

Step 1: Select Settings – Camera Settings – Image Configuration – Image Transform and the Image Transform configuration interface is displayed, as show in the figure below:



Step 2: Parameter settings, see the table below.

Parameter	Description	
Mirror	When Mirror is enabled, the image is flipped left and right.	
Visual	Normal	Displays the screen normally.

Angle	Corridor Mode 1	Displays the screen angled at 90 degrees clockwise.
	Invert	Displays the video flipped upside down.
	Corridor Mode 2	Displays the screen angled at 90 degrees counterclockwise

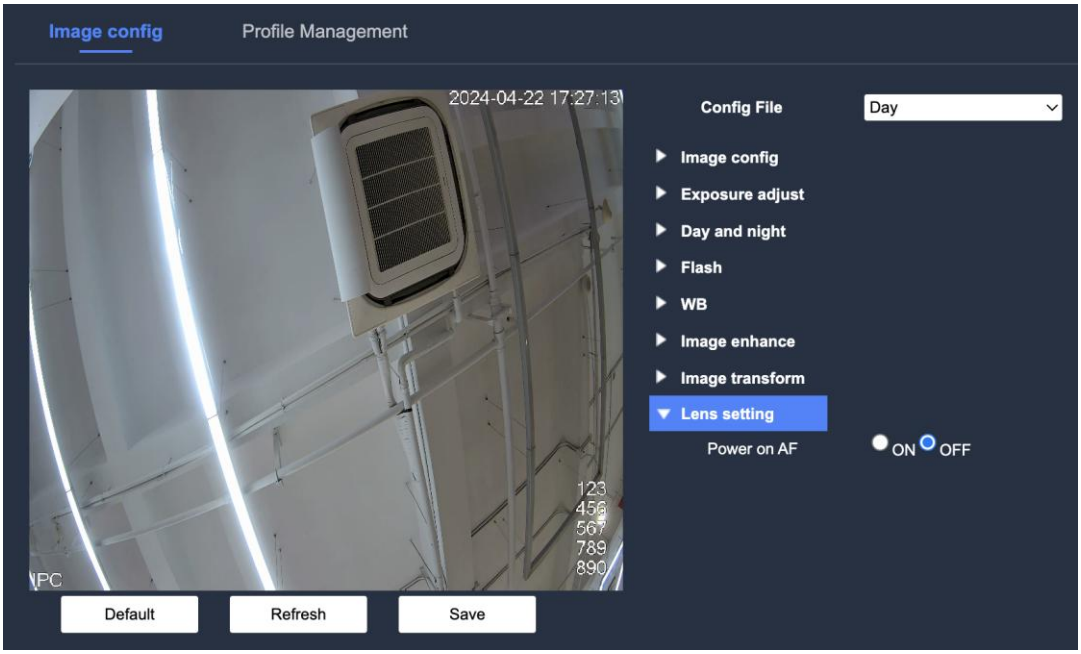
Steo 3: Click “Save” to complete the configuration of the camera image correction parameters.

4.2.2.8 Power-on Correction

Motorized zoom device power-up correction function.

Procedure

Step 1: Select Settings – Camera Settings – Image Configuration – Lens Setting- Power-On Correction to display the Power-on Correction configuration interface, as shown in the image below:



Step 2: Parameter settings. When the power-on correction function is enabled, the device will automatically focus towards the clearest position of the image when restarted. When the power-on correction function is turned off, the device will not be automatically focus on the video when the device is restarted.

Instructions

The power-on correction function is only available for motorized zoom cameras.

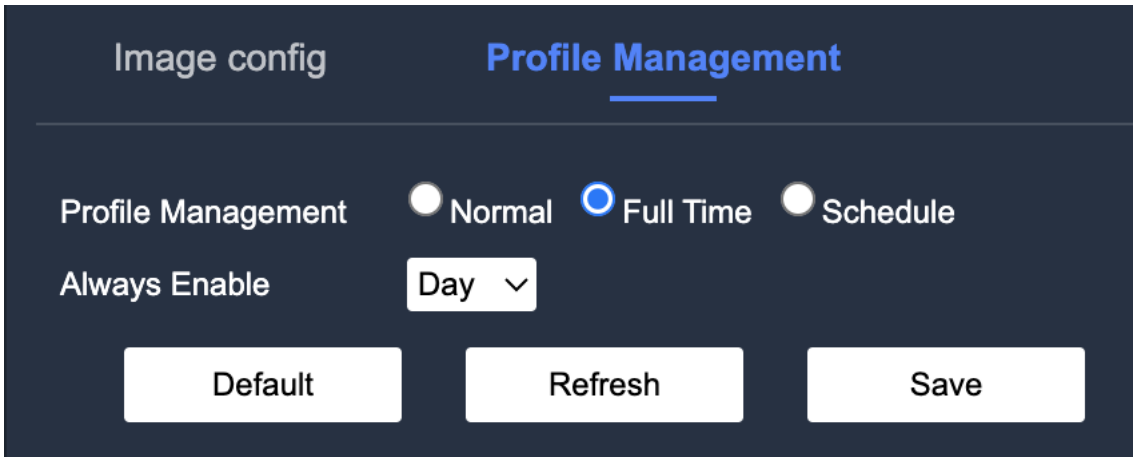
Step 3: Click “Save” to complete the configuration of the camera power-on correction parameters.

4.2.2.9 Profile Management

The user can select from 94 configuration file types such as “Normal”, “Day”, “Night’, and “Switch by Time”, and can set and view the configuration parameters and effects under the corresponding types after selecting the profile type.

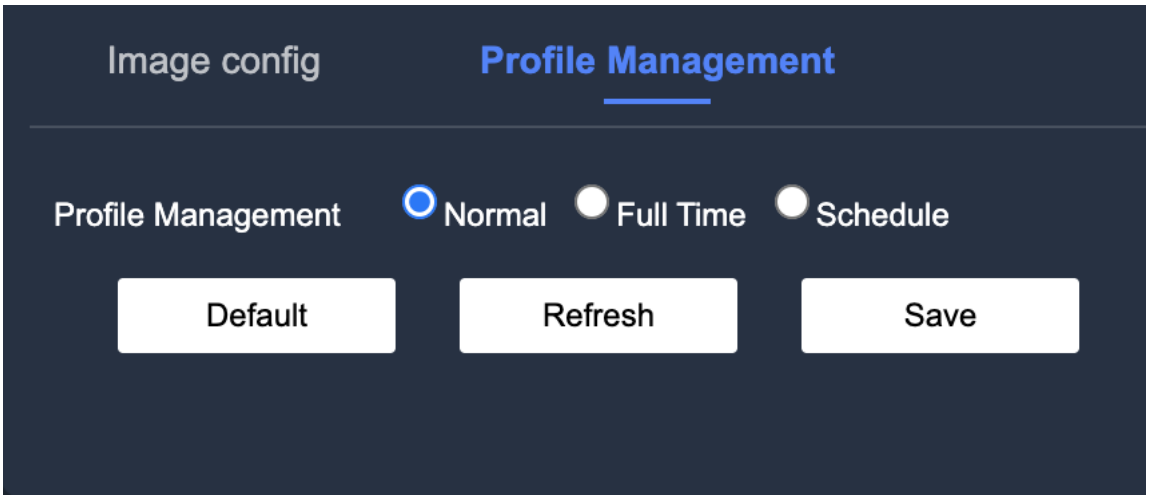
Procedure

Step 1: Select Settings – Camera Settings – Image Configuration – Profile Management, and the Profile Management configuration interface is displayed, as shown in the figure below:



Step 2: Set up the profile.

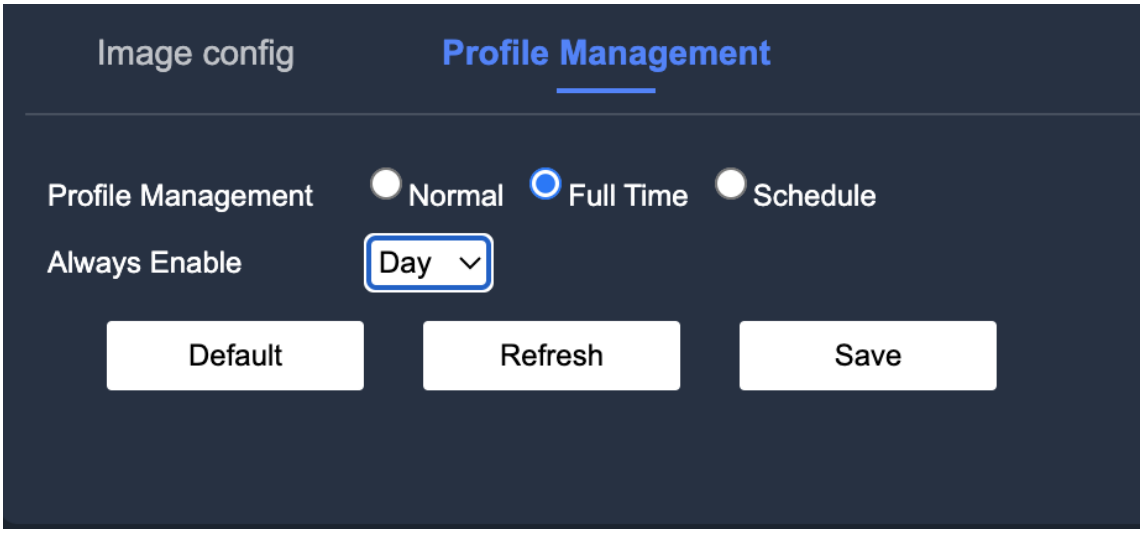
When the “Profile Management” is set to “Normal”, the system monitors the device based on the normal mode configuration. The settings are as follows:



Normal Settings

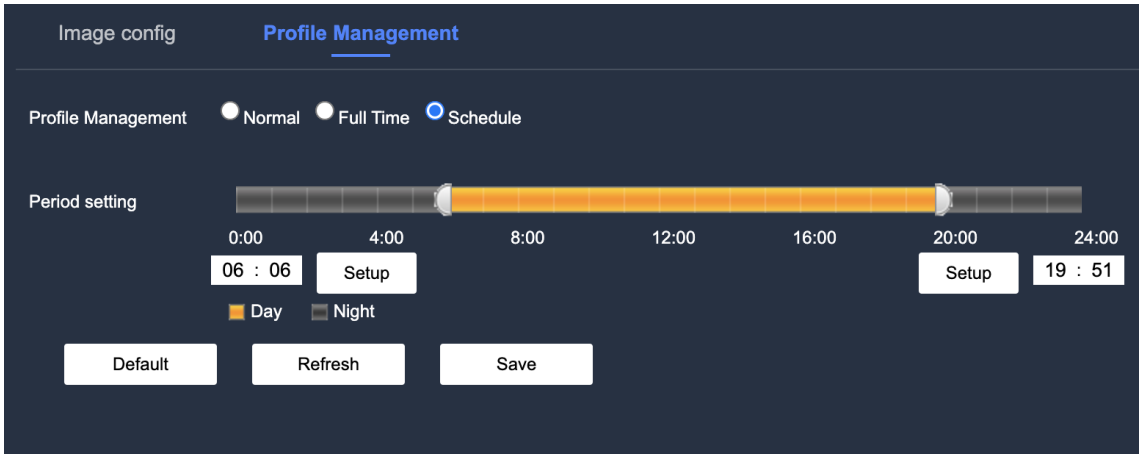
When “Profile Management” is set to “Full Time”, the user can either choose to always use the

"Daytime" or "Nighttime" modes for monitoring according to the always-on configuration. The settings are as follows:



Full Time Settings

When "Profile Management" is set to "Switch by Time", the user can set a specific period of time to daytime and another to night, for example, set 6:00～18:00 to daytime and 18:00～6:00 to nighttime. The system uses the corresponding configurations to monitor at different times. The settings are as follows:



Switch by Time Settings

Step 3: Click "Save" to complete the profile setup.

4.2.3 Audio Configuration

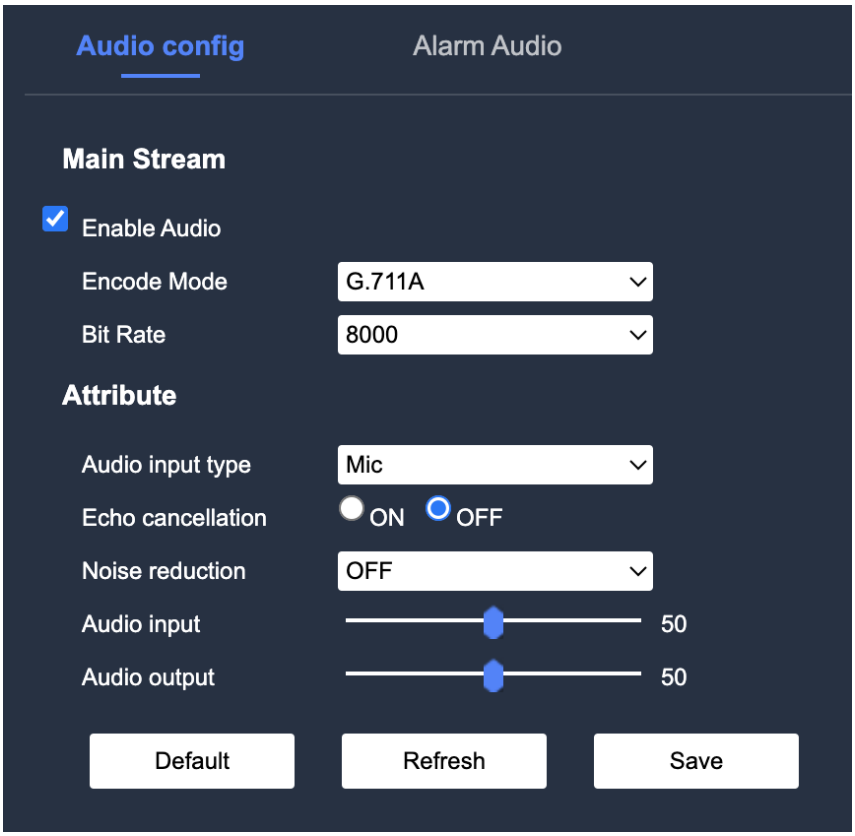
Audio and Alarm Audio set up

4.2.3.1 Audio Configuration

Sets the device's audio input type, volume, etc., and when audio encoding is enabled, the stream transmitted over the network is only a composite audio-video stream, otherwise only the video images will be included.

Procedure

Step 1: Select Settings – Camera Settings – Audio Configuration, and the audio configuration interface will appear as shown in the image below:



Step 2: Select Enable Audio; the device only supports the mainstream audio settings. The parameter settings are as follows:

Parameter	Description
Enable Audio	Enables Audio. Select Enable Audio Encoding.
Encode Mode	Sets the audio encoding mode and it takes effect for both audio and voice intercom. It is recommended to use the default value.
Bit Rate	This is the number of samples per second from the audio signal. The higher the sampling frequency, the more samples per unit

	time, and the more accurate the restored audio signal.
Audio Input Type	Displays the audio input source type. • Line: The device collects audio signals through external devices. • Mic: The device collects audio signals through its built-in mic.
Echo Cancellation	When echo cancellation is enabled, the system automatically cancels out echoes in the environment
Noise Reduction	When noise reduction is enabled, the system automatically filters out any noise in the environment.
Audio input	Adjusts the volume of the microphone
Adio output	Adjusts the volume of the speaker or talkback.

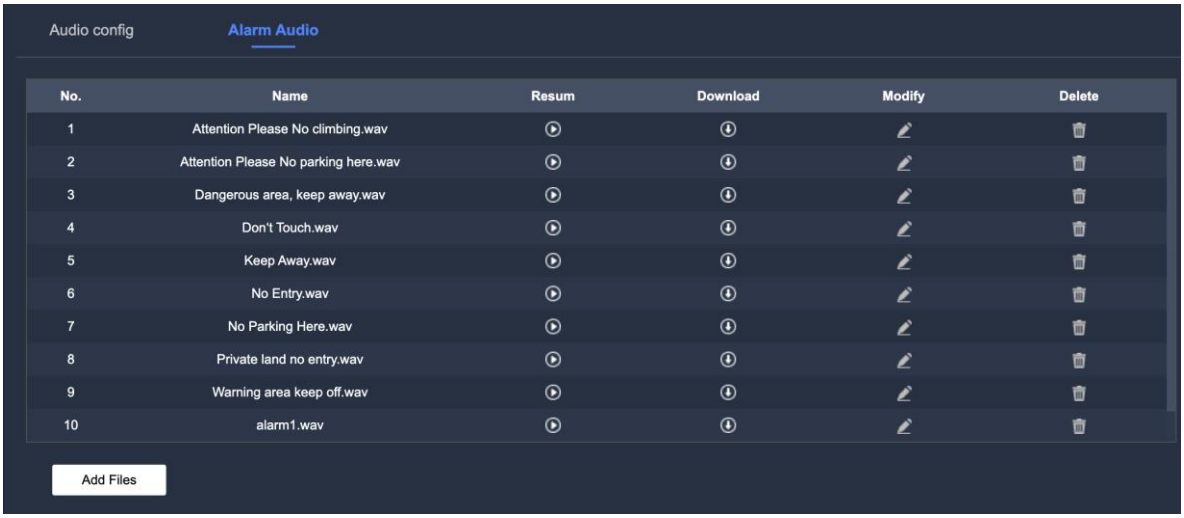
Step 3: Click “Save” to complete the audio encoding configurations.

4.2.3.2 Alarm Audio Configuration

Sets the alarm sound; when the alarm occurs, the device plays the corresponding alarm sound, and supports uploading the local alar audio file.

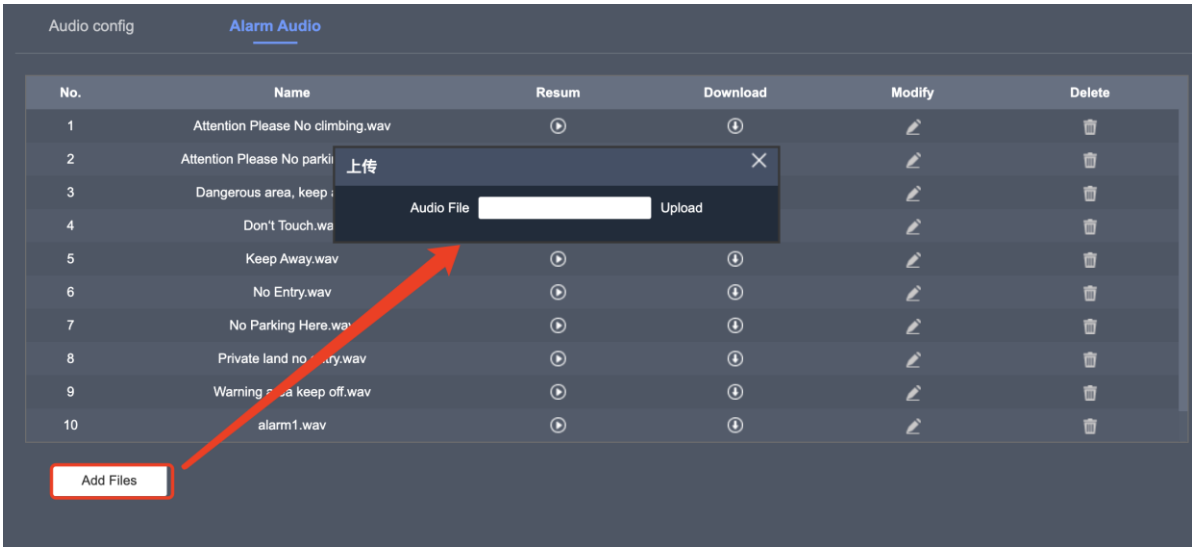
Procedure

Step 1: Select Settings – Camera Settings – Audio Configuration – Alarm Audio, and the Alarm Audio interface will appear as shown in the figure below. The audio displayed on the interface is the default audio of the device.



Step 2: Click “Add Audio File” to add audio and click “Upload. Then, select the audio file to be

uploaded and the file will be added successfully.



Instructions

1、Only audio files in WAV format can be uploaded

2、Uploaded audio files can be modified and deleted, but built-in audio files can not.

4.3 Network Settings

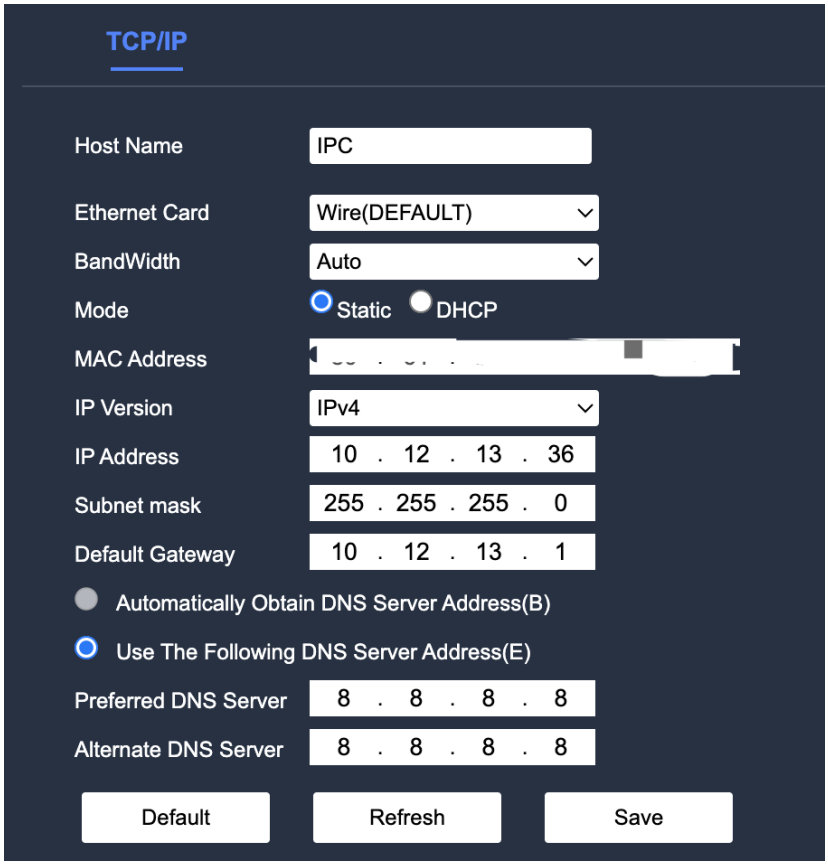
This section describes the device network configuration process and settings.

4.3.1 TCP/IP Settings

Sets the device IP address, DNS (Domain Name System) server and other information according to the to the network set-up,to ensure that the device and other devices in the network are connected normally.

Procedure

Step 1: Select Settings – Network Settings – TCP/IP to display the TCP/IP interface as shown in the figure below.



TCP/IP Settings

Step 2: Choose the device's network mode and set the IP address, DNS and other information as described in the following table.

Parameter	**Description**
Host Name	This is the name of the device; it should have a maximum length of 15 characters.
Network Card	Select the Network card to be configured; the default is set to wired.
Bandwidth	Select the preferred broadband which are, 10M, 100M and automatic; the default is set to automatic.
Mode	Set the mode that fetches the device IP address. Static: Manually set the IP address, Subnet Mask and Gateway. Click "save" and the webpage will automatically jump to the log-in page where the IP is newly set. DHCP: For a DHCP server in the network, select "DHCP". The device will automatically obtain the dynamic IP address and other information.
MAC address	Displays the device's MAC address

IP version	Select IPV4 or IPV6 address format
IP address	When the mode is set to “Static”, enter the device IP address, subnet mask and default gateway according to the network plan **Instructions** IPV6 version does not have a subnet mask The IP address and default gateway need to be on the same network segment.
Subnet Mask	
Default Gateway	
Preferred DNS Servers	The DNS server IP address
Alternate DNS Server	Alternate DNS server IP address

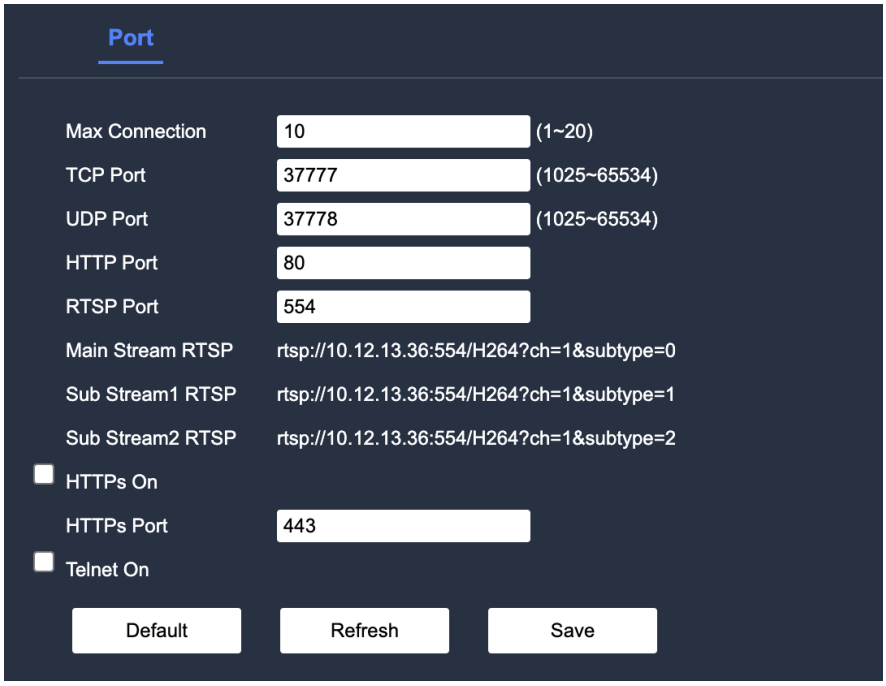
Step 3: Click OK to complete the configuration of the TCP/IP parameters

4.3.2 Port Settings

These settings set the maximum number of users (including web clients, platform clients, mobile clients, etc.) that can connect to devices at the same time and each port number.

Procedure

Step 1: Select Settings - Network Settings – Ports, to display the port configuration interface. Refer to the figure below:



Step 2: Set the parameters; refer to the following table

Parameter	**Description**
Max Connection	The number of clients (such as web client, platform client and mobile client) that can be logged in at the same time is 10 by default.
TCP Port	The default TCP communications port is set to 3777
UDP Port	The user packet protocol is set to 37778 by default.
HTTP Port	The HTTP communicatioms port; the default is set to 80. If set to other values, the modified port number needs to be added after the IP address when logging in with a browser.
RTSP Port	The RTSP port is set to 554 by default; the following formats mainstream RTSP, substream RTSP, and substream 2RTS can be used to play live video using a browser or VLC (Multimedia player)
Mainstream RTSP	Displays the mainstream RTSP URL format
Substream RTSP	Displays the sub-stream RTSP URL format
Substream 2RTSP	Displays the sub-stream 2RTSP URL format.
HTTPs Port	The HTTPS protocol port is set to 443 by default.

Step 3: Click “save” to complete the configuration of the Port parameters.

4.3.3 PPPoE Settings

PPPoE is one of the ways the devices can access a network. Establish a network connection via PPPoE dial up and the device automatically fetches the dynamic IP address over the public network after the connection is successful.

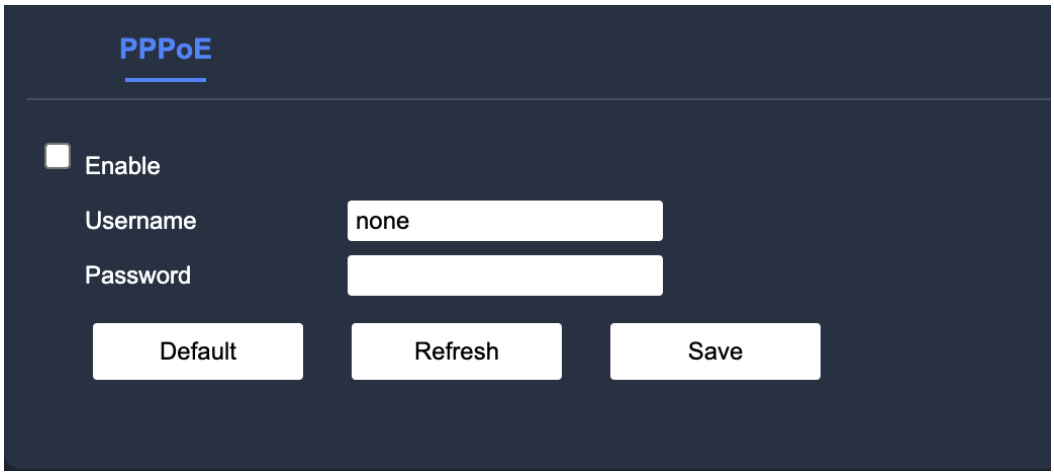
- The device is already connected to the internet.
- Already obtained the PPPoE username and password provided by the ISP.

Procedure

Step 1: Click Settings – Network Settings – PPPoE, to display the PPPoE configuration interface.

Step 2: Check “Enable”

Step 3: Input the PPPoE user account name and password as shown in the figure below:



PPPoE Settings

Step 4: Click Save to complete the PPPoE configuration, and the system will prompt that the PPPoE configurations are successfully saved and will display IP address in real time. Users will be able to acess the device through this IP address.

Instructions

When PPPoE dial-up is enabled, disable the UPnP function to avoid affecting the PPPoE dial-up.

After a successful PPPoE dial-up, the device IP address can no longer be modified through the WEB interface.

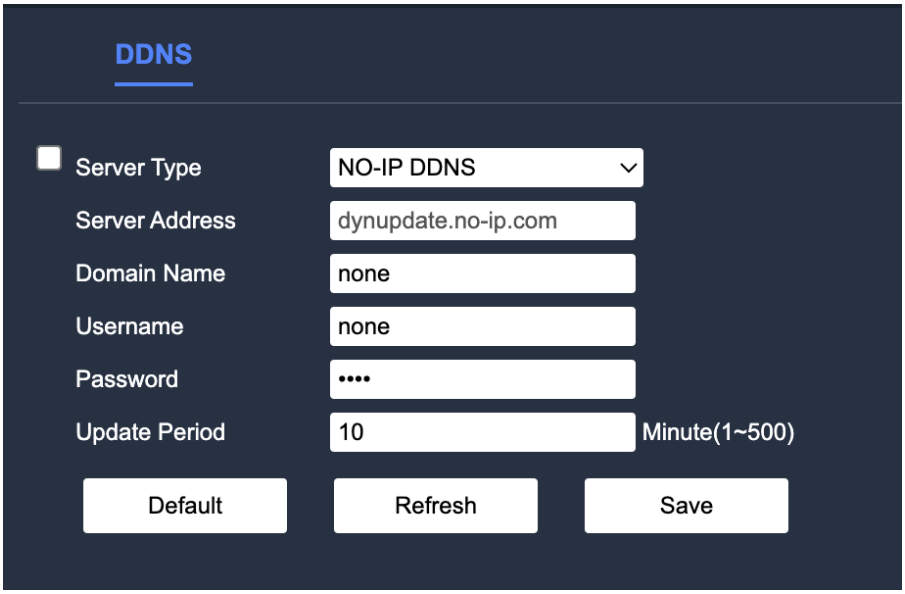
4.3.4 DDNS Settings

After setting the DDNS parameters, when the device's IP address changes frequently, the system dynamically updates the relationship between the domain name and IP address on the DNS server, so that you can directly use the domain name to remotely access the device without having to record the constantly changing IP address.

Confirm that the device supports the DNS server.

Procedure

Step 1: Select Settings – Network Settings – DDNS, to display the DDNS configuration interface as shown in the figure below.



DDNS Settings

Step 2: Select a type and set the DDNS parameters described in the following table as needed.

Parameters	Description
Server Type	The name and address of the DDS server vendor are mapped as follows: • The NO-IP DDNS server address is dynupdate.no-ip.com • The Dyndns DDNS server address is members.dyndns.org
Server Address	

	• The FNT DDNS server address is main.faceaip.net
Domain Name	Enter the domain name that is registered on the DDNS server provider website
Username	Enter the username gotten from the DDNS service provider
Password	Enter the password gotten from the DDNS service provider
Update Period	The update cycle to and from the device and server is 10 minutes by default.

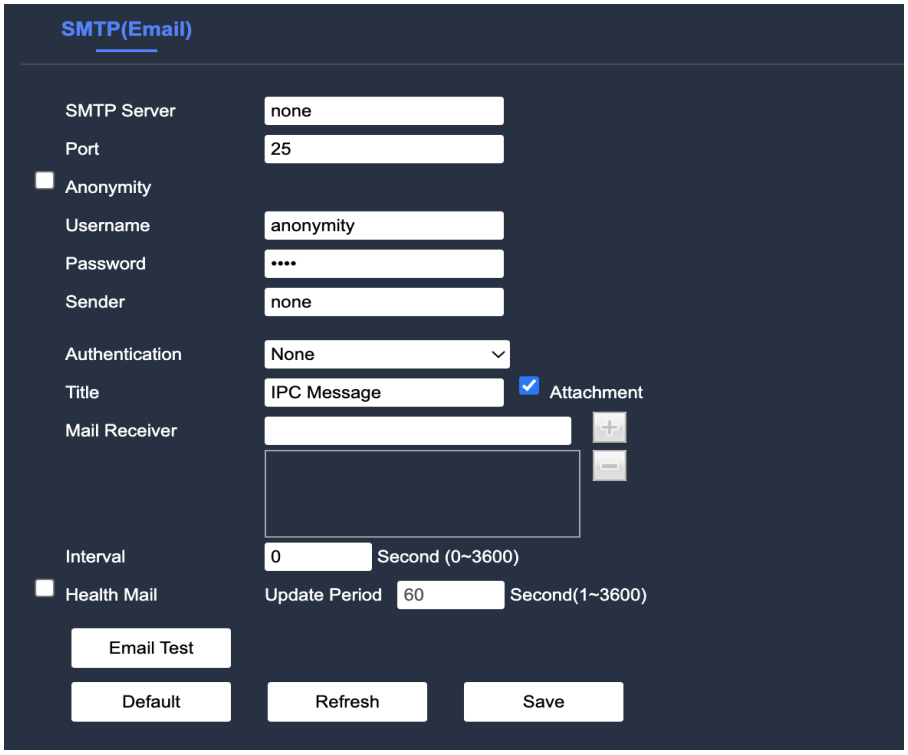
Step 3: Click “save” to complete the configuration of DDNS parameters, then enter the domain name in the PC web browser to log in to the WEB interface.

4.3.5 SMTP (Email) Settings

After enabling the “Send Email” alarm linkage function, the system will send an email to the specified recipient when an alarm is triggered.

Procedure

Step 1: Select Settings – Network Settings – SMTP (Email), to display the SMTP (Email) configuration interface as shown in the figure below.



Step 2: Set the parameters; refer to the following table.

Parameters	Description
SMTP Server	SMTP server address
Port	SMTP server port
Anonymity	Select “Anonymity” and the message received by the user will not display the sender’s information.
Username	SMTP server username
Password	SMTP server password
Sender	Sender’s email address
Encryption	Select an encryption method. Options include: None, SSL and TLS.
Title	Supports the input of Chinese, English and Arabic characters.
Attachments	Select “Attachments” to allow attachments to be sent.
Mail Reciever	Enter the recipient’s email address, click “+” to add an email address. Only adding up to 3 receiving addresses is supported.
Interval	Set the email sending interval between 0～3600 seconds
Health Email	Determines whether the email link is successful or not through the test email sent by the system. Select “Health Mail”, and set the email test message according to the interval time.The range of time intervals allowed for sending health mail is 1～3600 seconds.
Update period	
Email Test	

Step 3: Click “Save” to complete the configuration of the SMTP (Email) parameters.

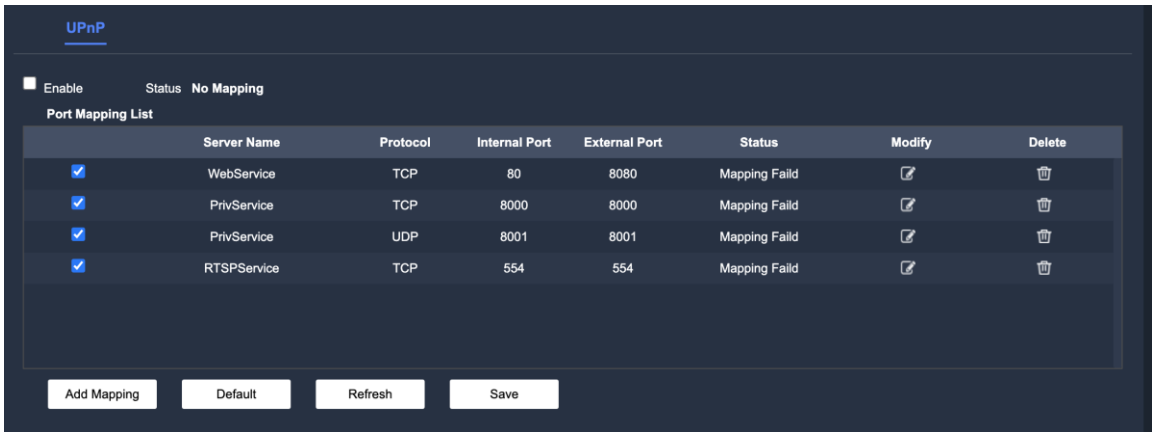
4.3.5 UPNP Settings

The UPnP protocol is used to establish a mapping relationship between the internal network and the external network; the users on the external network can use the public IP address to directly access the decvice on the internal network.

- Please make sure that the UPnP network service is installed on your PC
- Log in to the router and set the IP address of the router’s WAN port to access the internet.
- The router enables the UPnP feature.
- Connect the device to the router’s LAN port and connect it to the private network.
- Select Network Settings – TCP/IP to set the private IP address of the router or DHCP to automatically obtain the IP address.

Procedure

Step 1: Select Settings – Network Settings – UpnP, to display the UPnP configuration interface as shown in the figure below.



Step 2: Select “UpnP”to enable the UPnP function.

Step 3: Select the corresponding service name and select the unoccupied port to automatically complete the port mapping; the user cannot modify port mapping.

Step 4: Click “Save” to complete the configuration of the UPnP parameters. Enter “http://external IP address: external port number” in the browser to access the private network device with the corresponding port number in the router.

4.3.6 Wi-Fi Setting

By Adding a wireless network, the device can be connected to the network, realize the wireless connection between the device and other devices in the same network.reduce the difficulty of the device connection, and facilitate the device movement.

4.3.6.1 WIFI

Procedure

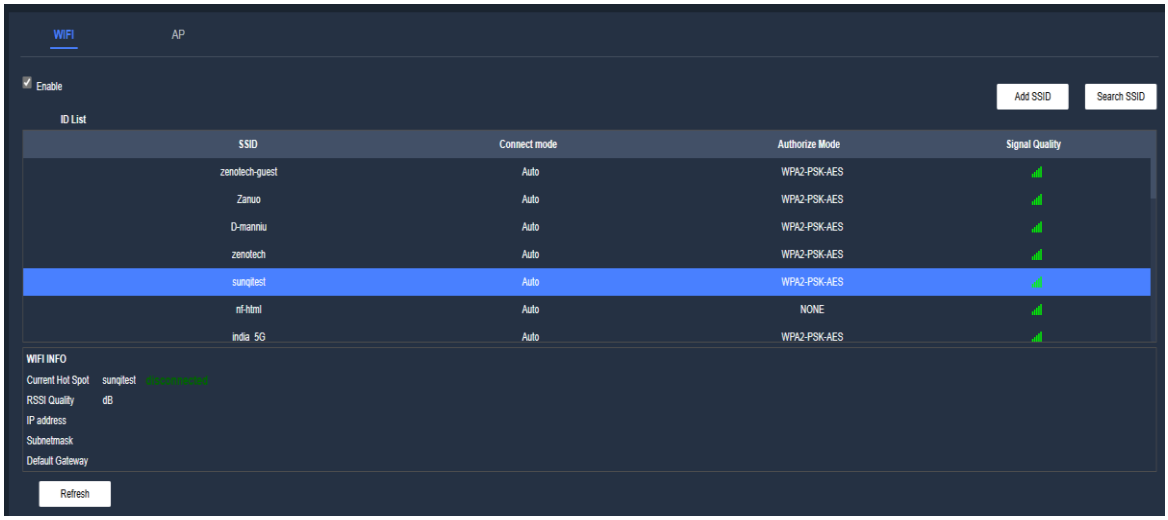
Step 1: Select Settings – Network Settings –WIFI-WIFI

Step 2 ：Select “enable”

Step 3 ：connect to a wireless network

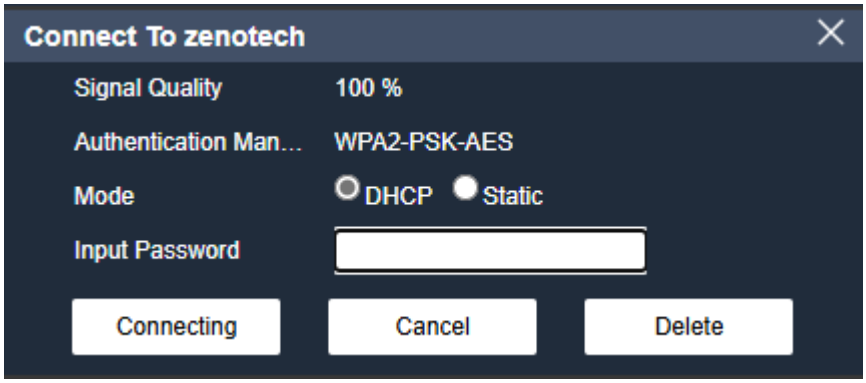
- Add wireless network by searching

1. Click “Search SSID”
2. Click the network you want to connect



Add wireless network(Search add)

3. Input WIFI password.If not input password, direct click “connecting”.

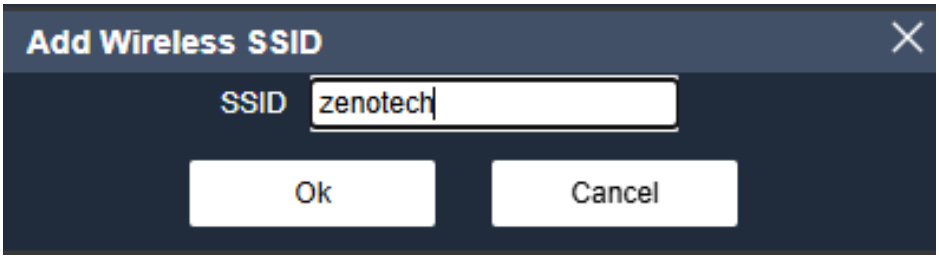


Connect to WIFI(Search add)

4. Click “connecting”

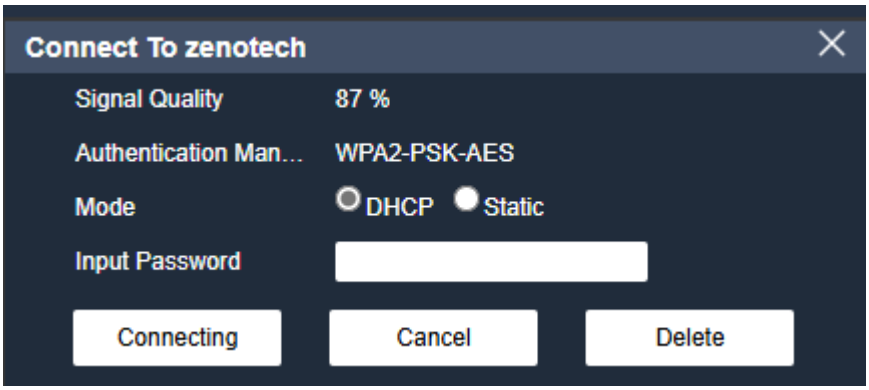
- Add wireless network manually

1. Click “Add SSID”.
2. Input SSID, click “OK”.



Input SSID

3. Input WIFI password.If not input password, direct click “connecting”.



Input Wi-Fi password

4. Click “connecting”

Step 4：Click “Refresh”, acquire connection status, the setting is complete.

4.3.6.2 AP

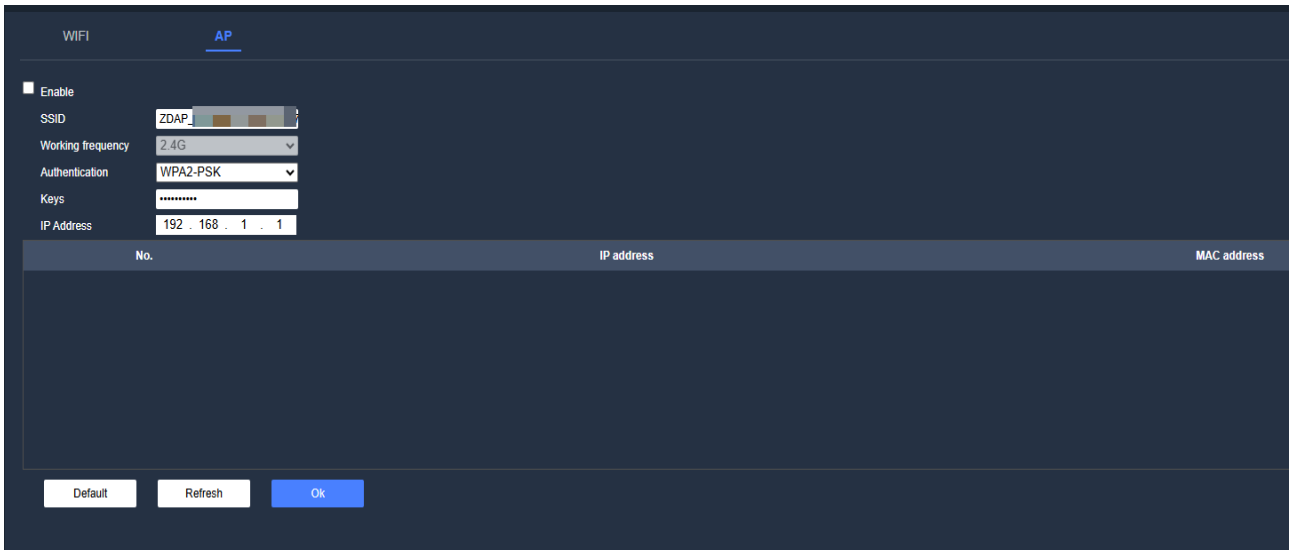
Use the device as a wireless Access Point (AP). Other wireless terminal device (such as moble phones) can connect to the device by searching for the AP name of the device, and then we can log in the device through browser. The AP and wifi function can not be enable at the same time. The AP function is disabled by default.

Procedure

Step 1: Select Settings – Network Settings –WIFI-AP

Step 2：Select “enable”, enable the AP function

Step 3：Set AP parameters



AP parameter

Step 3: Set the parameters; refer to the following table.

Parameter	Description
Enable	Select Enable to enable “AP”features
SSID	The default network name is “ZDAP_DN”
Working frequency	Support 2.4GHz working frequency by default
Authentication	The default is WAP2 PSK, can not modify
Keys	Set connection password.When other wireless terminals connect to the device, need to input the password.AP default password is “zdap+the last eight bits of DN”
IP Address	Displays the IP adress of the AP

Step 4: click “Save” to complete the configuration of the AP.

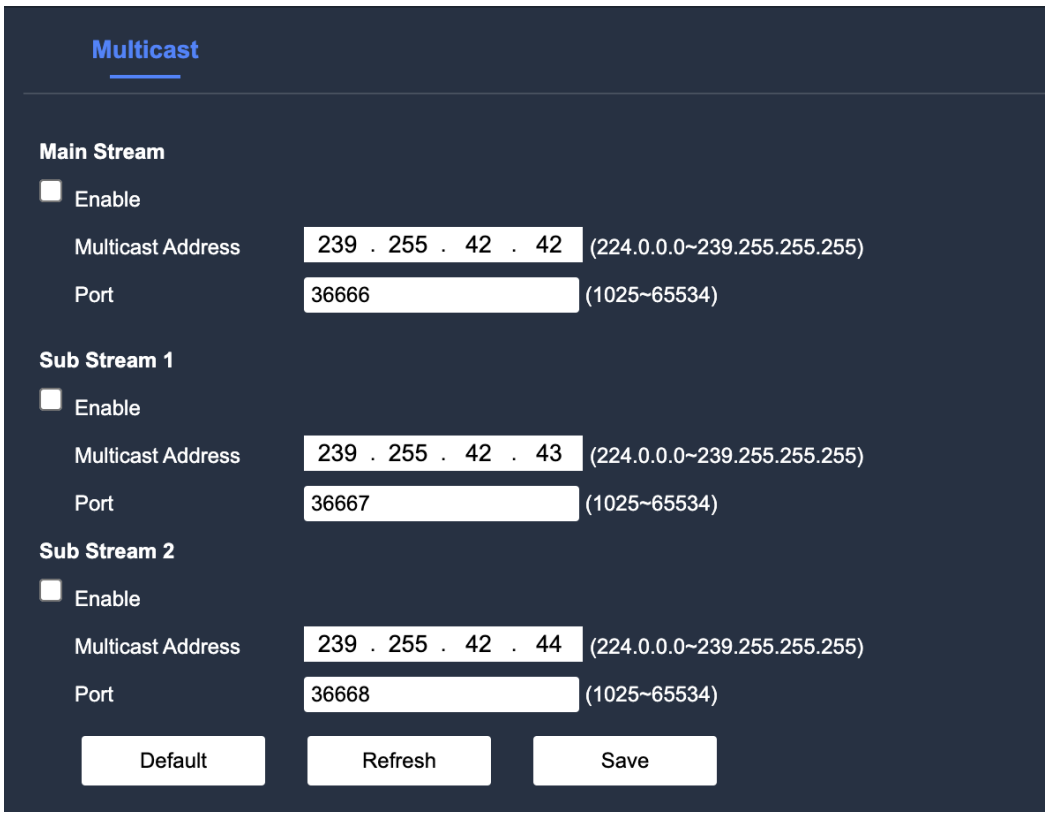
4.3.7 Multicast Setting

When multiple users try to preview the device video screen through the network at the same time, the preview may not be possible due to network bandwidth limitations. It is recommended to set up a multicast IP (224.0.0.0~239.255.255.255) for the device to solve this problem by using multicast protocol access.

Procedure

Step 1: Select Settings – Network Settings – Multicast, to display the Multicast configuration

interface as shown in the figure below.



Step 2: Set the parameters; refer to the following table.

Parameter	Description
Enable	Check Enable to enable Multicast features
Multicast Address	The default multicast address of the mainstream/substream 1/substream 2 is 239.255.42.42 and the value range is 224.0.0.0~ 239.255.255.255.
Port	The value range of the multicast ports is 1025~65500 • The main stream is 36666 • Sub-stream 1 is 36667 • Sub-stream 2 is 36668

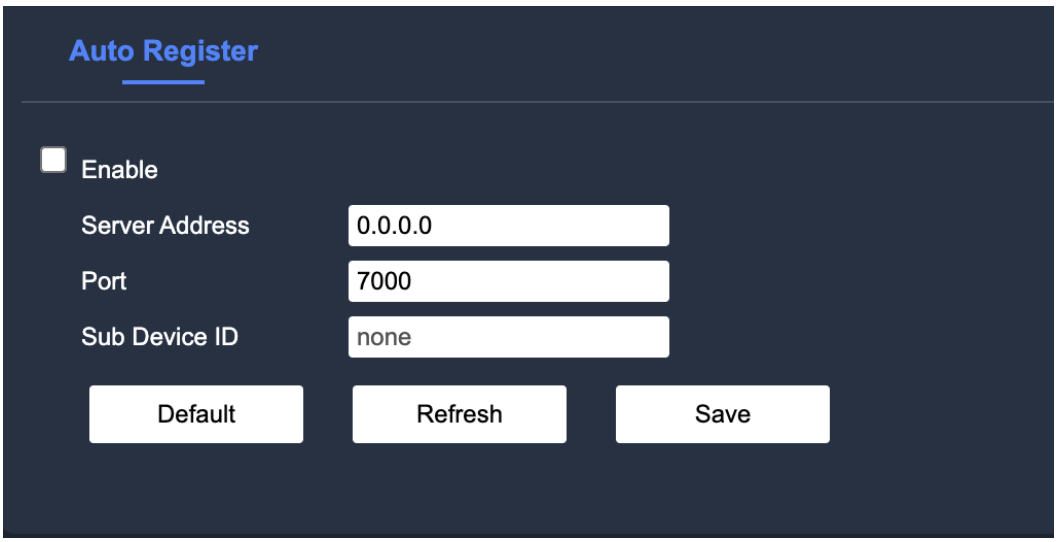
Step 3: Click “Save” to complete the configuration of the Multicast parameters.

4.3.8 Active Register

The device is actively registered with the proxy server designated by the user, and the proxy server acts as a relay function, so that the client software can visit the device through the proxy server to preview and monitor the device.

Procedure

Step 1: Select Settings – Network Settings – Auto Register, to display the Auto Register configuration interface is displayed as shown in the figure below.



Step 2: Set the parameters; refer to the following table.

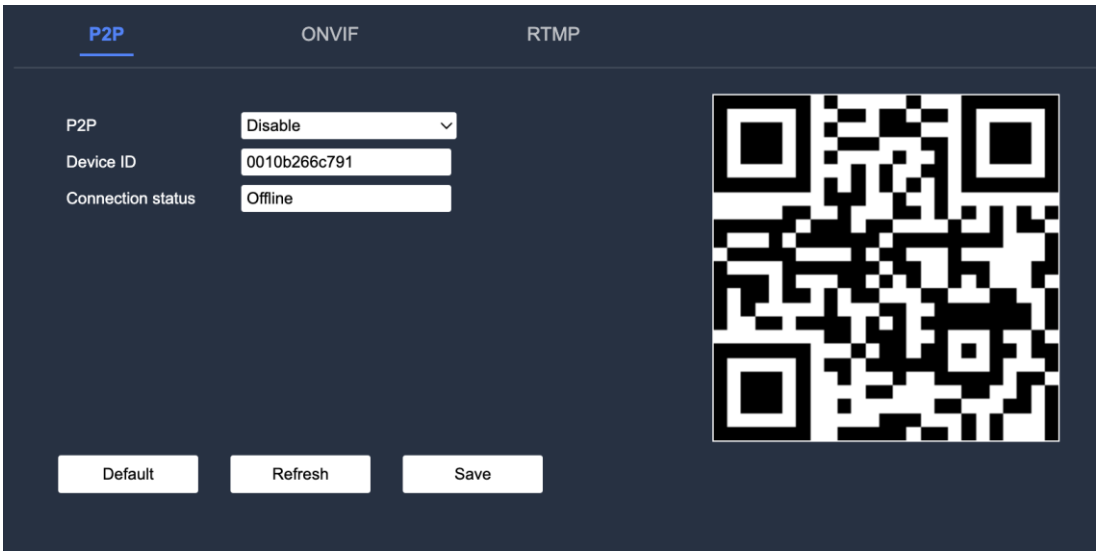
Parameters	Description
Enable	Check Enable to enable the Auto Register features
Server Address	The user needs to register the IP address or domain name of the server.
Port	The port number used by the server for auto-registration
Sub Device ID	The ID used by the device; it is automatically generated by the device.

Step 3: Click “Save” to complete the configuration of the Auto Register paramters.

4.3.9 Platform Access

4.3.9.1 P2P Settings

Select “Enable” to enable the P2P function. Connect the device to the internet, and after the connection status displays “Online”, connect to the device through the mobile client as shown in the figure below.



Step 1: Select Settings – Network Settings – Platform Access– P2P, to display the P2P configuration interface.

Step 2: Select enable P2P; it is turned off by default.

Step 3: Log in to VESTA ADVANCED on the mobile app. Click "+" on the home page to add a device, and complete the configuration according to the prompts on the mobile interface.

Instructions

Please ensure that your mobile phone has downloaded, installed and registered with VESTA ADVANCED. If not, please go to the mobile app store to search and download the app.

Connection:

- Add by adding the device ID number of this device.
- Add by scanning the QR code pictured above.

4.3.9.2 ONVIF Setttings

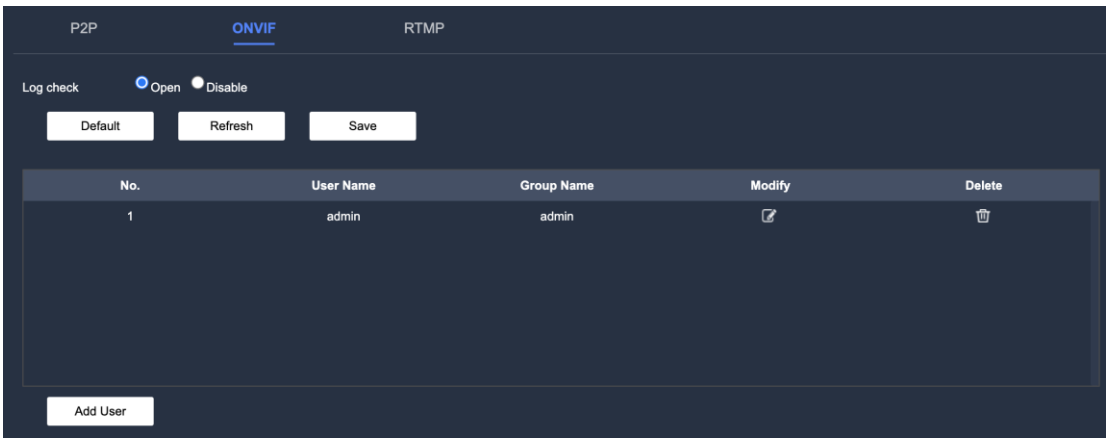
With ONVIF enabled, devices can communicate with other vendors' network video products (including front-ends and recording equipment) through the ONVIF protocol.

Procedure

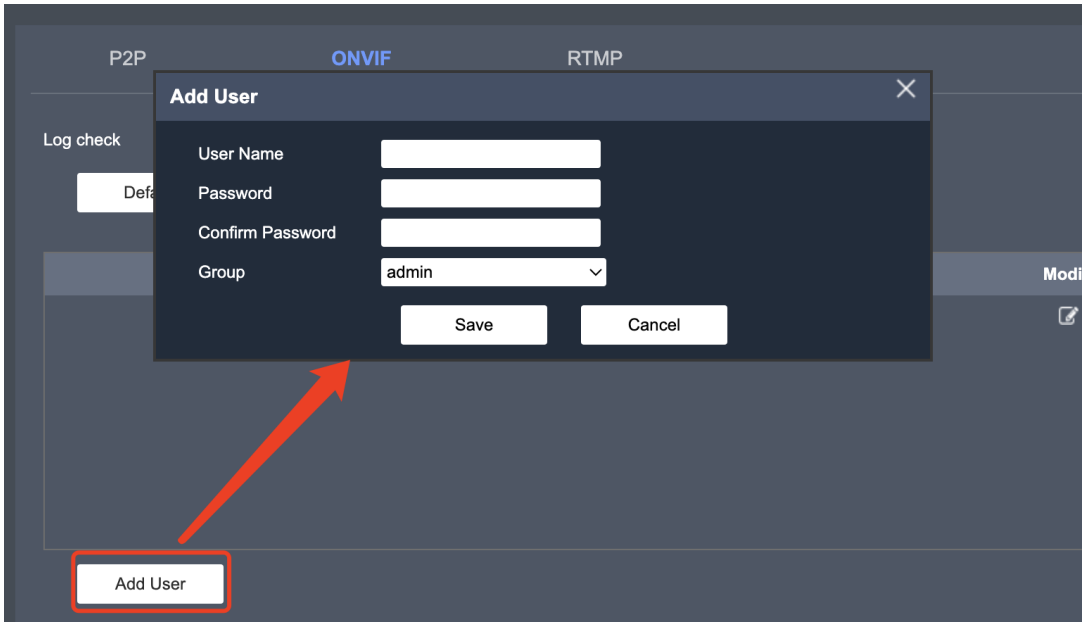
Step 1: Select Settings – Network Settings – Platform Access – ONVIF, to display the ONVIF configuration interface.

Step 2: Select "ONVIF" to enable the ONVIF feature

Step 3: Select “Log Check”, and enable the log-in verification as illustrated in the figure below.



Step 4: To add an ONVIF user, enter the username, password, password confirmation and select the user group. Click “Save”, as shown in the figure below.



4.3.9.3 RTMP Settings

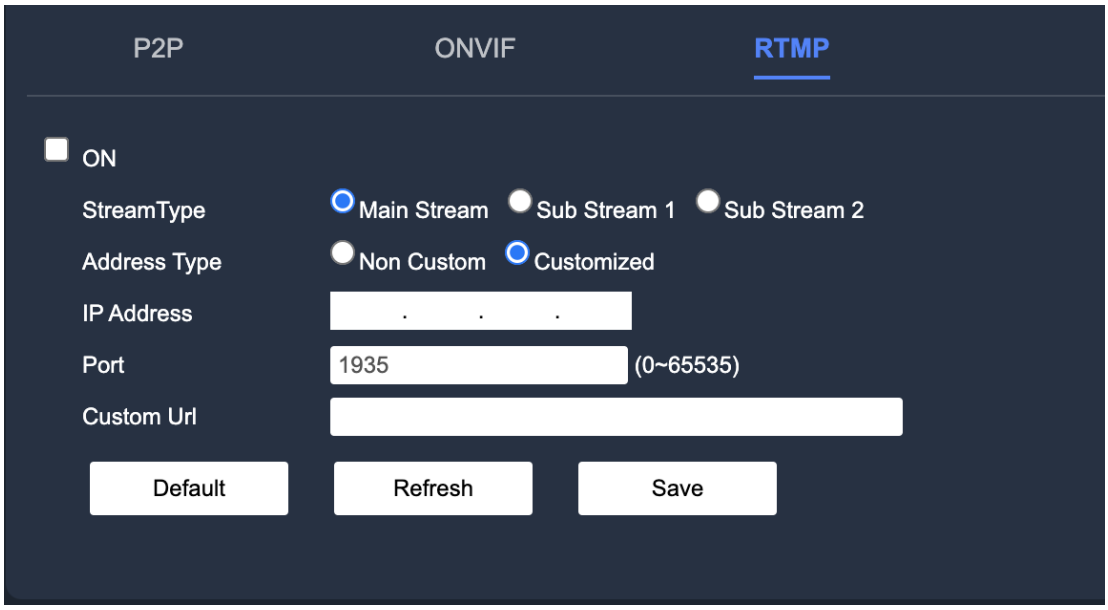
The device can connect to third-party platforms through the RMTP protocol to achieve live video streaming.

- Only the admin account can configure the RMTP
- RMTP only supports H.264, H.264B and H.264H video formats as well as AAC audio formats.

Procedure

Step 1: Select Settings – Network Settings – Platform Access – RMTP, to display the RMTP

configuration interface



Step 2: Set the parameters; refer to the following table.

Parameter	Description
Enable	Select Enable to enable “RTMP”features
Stream Type	Choose the preferred stream type for the live stream, which includes: main stream, substream 1 and substream 2. Ensure that the video encoding mode of the chosen stream is H.264, H.264B or H.264H, and that the audio encoding mode is AAC.
Address Type	Consists of Customized and Non-Custom • Non-Custom: Enter the server IP • Customized: Fill in the path assigned by the server.
IP Address	If the Non-Custom option is chosen,then the user must enter the IP address and port number of the server. IP Address: Enter the IP address of the server Port: Enter the port number; it is recommended to use the default value.
Port	
Custom Address	When the Customized option is chosen, the user needs to enter the path assigned by the server.

Step 3: Click “Save” to complete the configuration of the RTMP parameters.

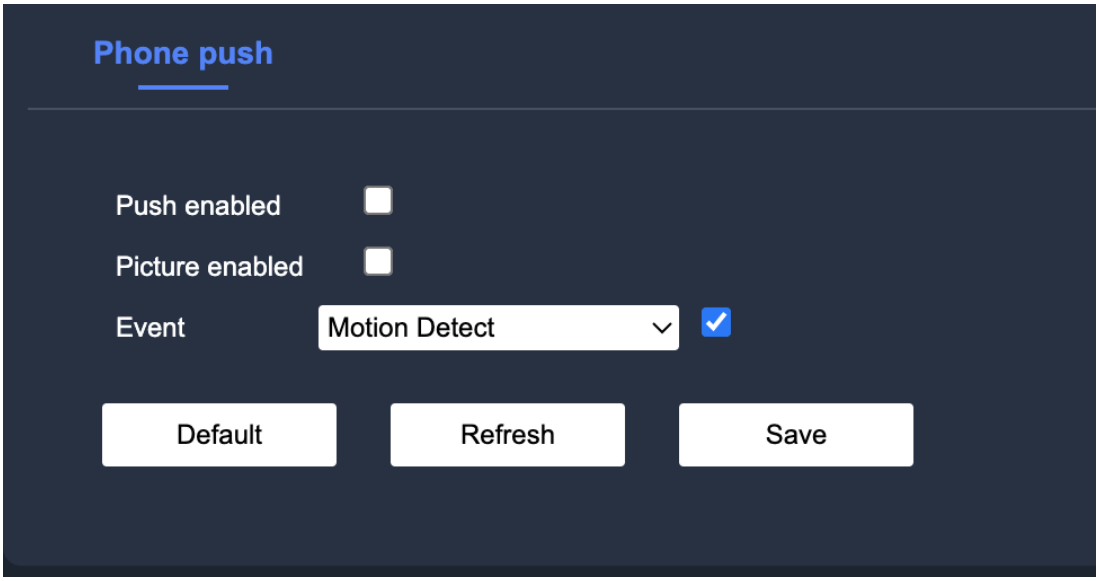
4.3.10 Phone Push

Phone Push allows a mobile phone to receive ordinary or smart alarm information and pictures

from the cameras via our VESTA ADVANCED app.

Procedure

Step 1: Select Settings- Network Settings – Phone Push, to display the Phone Push configuration interface.



Step 2: Set the parameter; refer to the following table.

Parameters	Description
Push Enabled	If “Push Enabled” is checked, the device will push the alarm information selected in the event to the mobile app.
Picture Enabled	If “Picture Enabled” is checked, the device will push the alarm type picture selected from the event to the mobile app.
Event	Alarm Events: The alarm types are Smart Alaram, VQD alarm and motion detection. The user can select the alarm type preffered to be pushed to the mobile app as needed

Step 3: Click “Save” to complete the configuration of the Phone Push parameters.

4.4 Event Management

Configure functions such as video detection, smart alarm, alarm settings and anomaly handling.

4.4.1 Video Detecte

By analyzing the video image,this checks whether there is a sufficient degree of change within the image. When the image changes to a significant degree (such as moving objects, blurred video images, etc.) the system performs an alarm linkage.

4.4.1.1 Motion Detection Settings

After setting up dynamic detection, when a moving target aapears on the monitoring screen and the moving speed reaches the preset sensitivity, the system will execute an alarm.

Procedure

Step 1: Select Settings - Event Management - Video Detection – Motion Detection, to display the Motion Detection configuration interface as shown below.

Step 2: Check “Enable” to enable Motion Detection features.

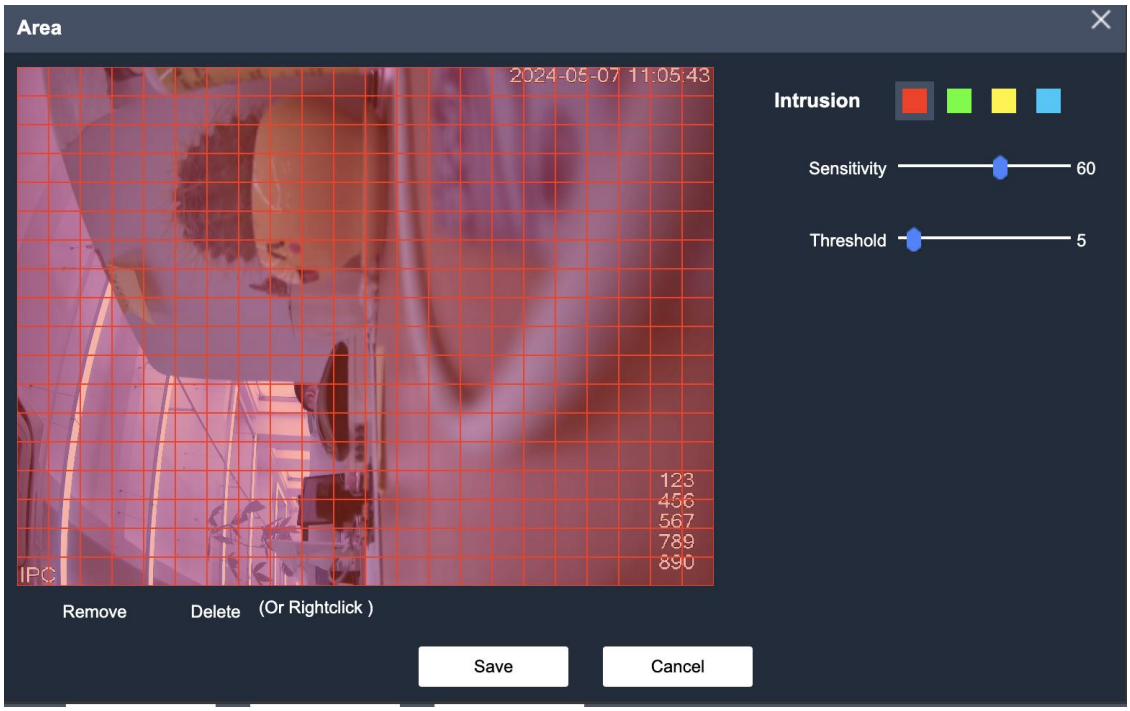
Step 3: Set the motion detection area.

1、Click “Settings” after “Area Settings”.

2、Select the area color block, set the effective area of motion detection. and set the sensitivity and area threshold as needed.

- By default, the entire video screen is the effective motion detection area, and the user can set different color blocks to cover different detection areas for different regions of the video.
- Sensitivity: The degree of sensitivity to external changes; the larger the sensitivity value, the easier it is to trigger the alarm.
- Threshold: The area threshold of the activated motion detection area; the smaller the threshold, the easier it is to trigger the alarm.

3、Click “Save” to complete the configuration of the Area parameters.



Step 4: Dynamically detects the set parameter; refer to the following table

Parameter	Description
Enable	Check “Enable” to enable “Motion Detection” features. Motion Detection is enabled by default.
Period	After setting the time period for the alarm, the alarm event will only start within the specified time range.
Anti-Dither	Only one motion detection alarm is recorded during the dejitter period.
Record	If “Record”is selected, the system will automatically record the alarm when an alarm occurs. When the alarm ends, the alarm recording will extend for a period
Record Delay	

	of time (according to the set time) then halted.
Alarm Output	Check “Alarm Output” to enable the alarm linkage output feature; when an alarm occurs, the system links the corresponding alarm to the output device. When the alarm ends, the alarm recording extends for a period of time (according to the set time) then halted.
Alarm Delay	
Send Email	If “Send Email”is checked, the system will send an email to notify the user when an alarm occurs.
Snapshot	Check “Snapshot”, and when an alarm occurs, the sytem will automatically capture the alarm.

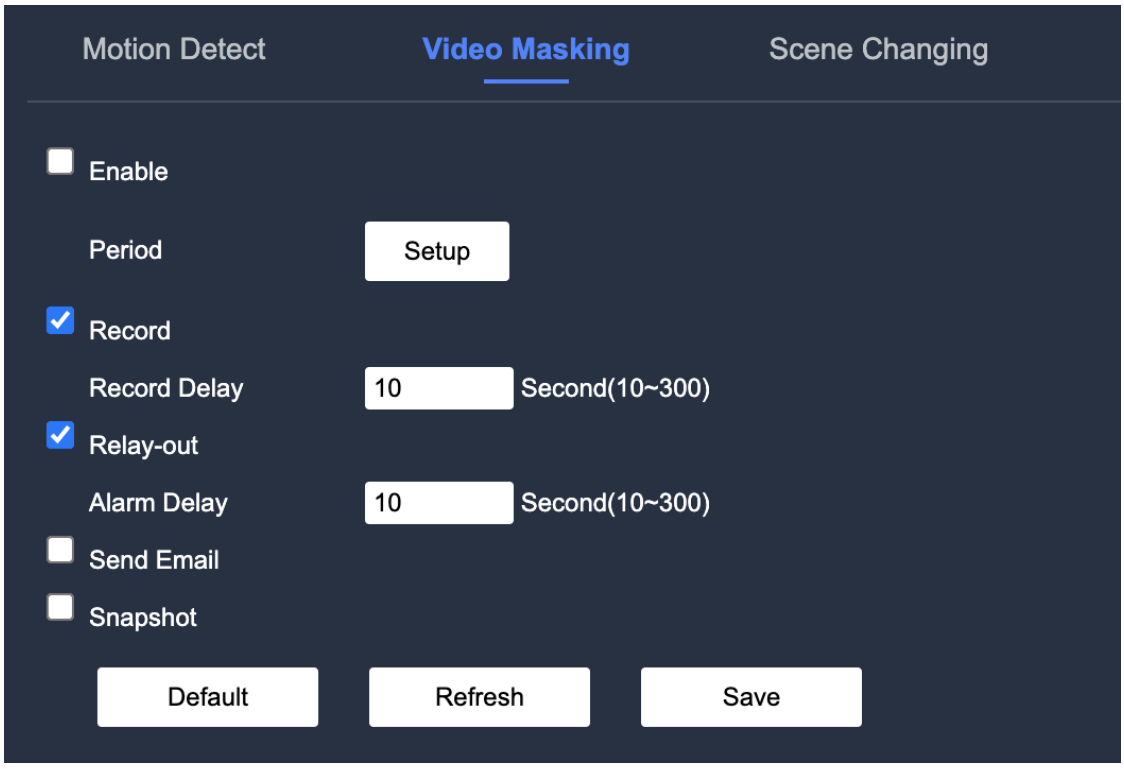
Step 5: Click “Save” to complete the configuration of the Motion Detection parameters.

4.4.1.2 Video Masking Settings

After Video Masking is set up, the system will execute an alarm linkage action whenever the lens is blocked or the video outputs a single-color frame due to light or other reasons.

Procedure

Step 1: Select Settings – Event Management – Video Detection – Video Masking, to display the Video Masking interface as shown in the figure below.



Step 2: Set the parameters; refer to the following table.

Parameters	Description
Enable	Check “Enable” to enable Video Masking features.
Period	After setting the time period for the alarm, the alarm event will only start within the specified time range
Record	If “Record”is selected, the system will automatically record the alarm when an alarm occurs. When the alarm ends, the alarm recording will extend for a period of time (according to the set time)then halted.
Record Delay	
Alarm Output	Check “Alarm Output” to enable the alarm linkage output; when the alarm occurs, the system links the corresponding alarm to the output device. When the alarm ends, the alarm recording extends for a period of time (according to the set time) then halted.
Alarm Delay	
Send Email	If “Send Email”is checked, the system will send an email to notify the user when an alarm occurs
Snapshot	Check “Snapshot”, and when an alarm occurs, the sytem will automatically capture the alarm.

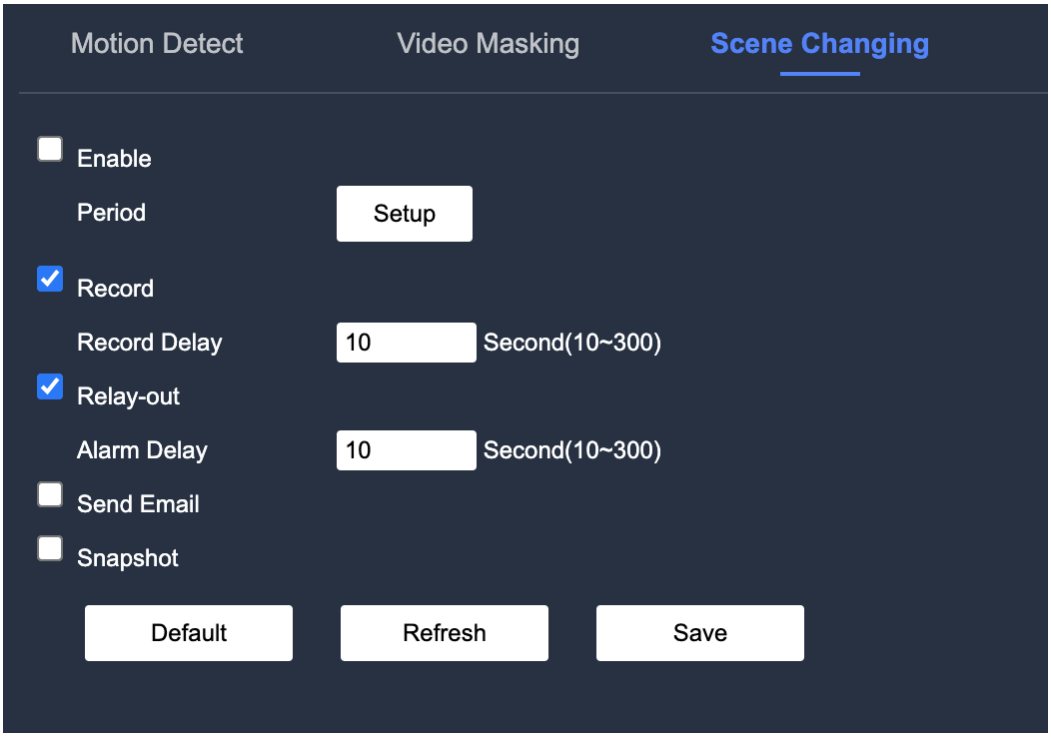
Steo 3: Click “Save” to complete the configuration of the Video Masking Parameters.

4.4.1.3 Scene Changing Settings

After enabling Scene Change detection, the system executes an alarm whenever the monitoring screen switches from the one scene(current) to another.

Procedure

Step 1: Select Settings – Event Management – Video Detection – Scene Changing, to show the Scene Changing configuration interface as shown in the figure below.



Step 2: Set up the parameters; see the table below.

Parameter	Description
Enable	Check Enable to enable“Scene Changing” features.
Period	After setting the time period for the alarm, the alarm event will only start within the specified time range.
Record	If “Record”is selected, the system will automatically record the alarm when an alarm occurs. When the alarm ends, the alarm recording extends for a period of time (according to the set time) then halted.
Record Delay	
Alarm Output	Check “Alarm Output” to enable the alarm linkage output; when an alarm occurs, the system links the corresponding alarm to the output device. When the alarm ends, the alarm recording extends for a period of time (according to the set time) then halted.
Alarm Delay	
Send Email	If “Send Email”is checked, the system will send an email to notify the user when an alarm occurs

Step 3: Click “Save” to complete the configuration of the Scene Changing parameters.

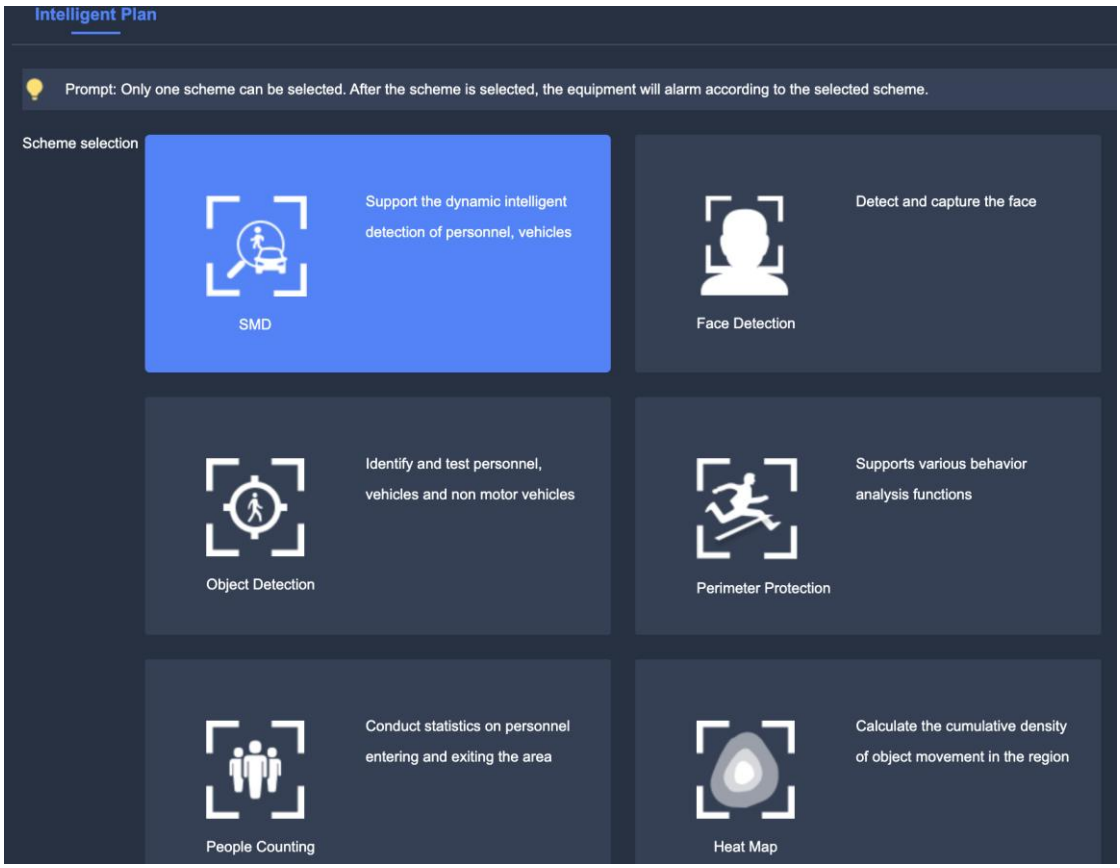
4.4.2 Intelligent Plan Settings

The Intelligent Plan acts as the master switch for smart analysis fucntions such as face detection,

perimeter prevention, people counting, heat map, etc.,and these functions only take effect after Intelligent Plan is enabled.

Procedures

Step 1: Select Settings – Event Management – Intelligent Plan, to display the Intelligent Plan interface as shown in the figure below.



Step 2: Select the preferred Intelligent Plan and click “Save” to finish the set up.

Instructions

The the smart function available on Intelligent Plans page are mutually exclusive, and only one of the functions can be selected.

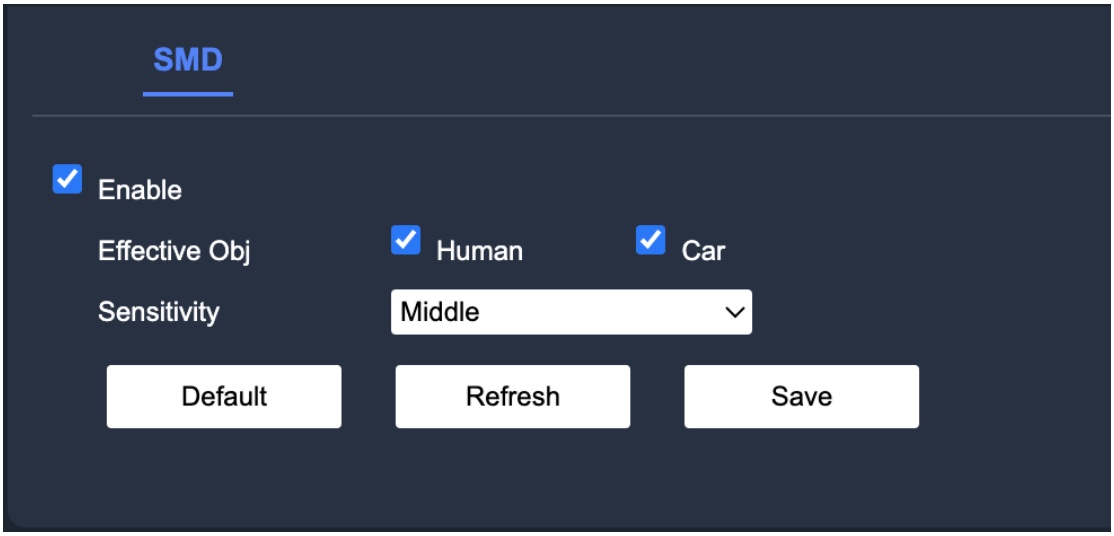
4.4.3 Smart Motion Detection Settings

Smart Motion Detection can detect targets (people, motorized vehicles and non-motorized vehicles) appearing on the screen. After setting up Smart Motion Detection,the system will execute an

alarm when people, non-motorized or motorized vehicles appear on the monitoring screen and the moving speed reaches the preset sensitivity, to avoid alarms triggered by changes in the natural environment and so on.

Procedure

Step 1: Select Settings – Event Management – Intelligent Plan, to display the Smart Motion Detection Inteface. The arming/disarming parameters and detection area have been set to motion detection and other configurations are show in the fillowing figure.



Step 2: Set the alarm targets and sensistivity

- Alarm Target: Selection of people and vehicles to target; when selecting the the type of car, the device can detect both motorized and non motorized vehicles simultaneously.
- Sensitivity: Supports High, Medium and Low sensitivity. The higher the sensitivity, the easier it is to trigger an alarm.

Step 3: Click “Save” to complete the configuration of the Smart Motion Detection parameters.

Instructions

1、The Smart Motion Detection function relies on the detection results of the Motion Detection function and follows all other parameters this function except sensitivity, including arming and disarming period, zone settings, linkage configuration, etc. When Motion Detection is not triggered, Smart Motion Detection is also not triggered.

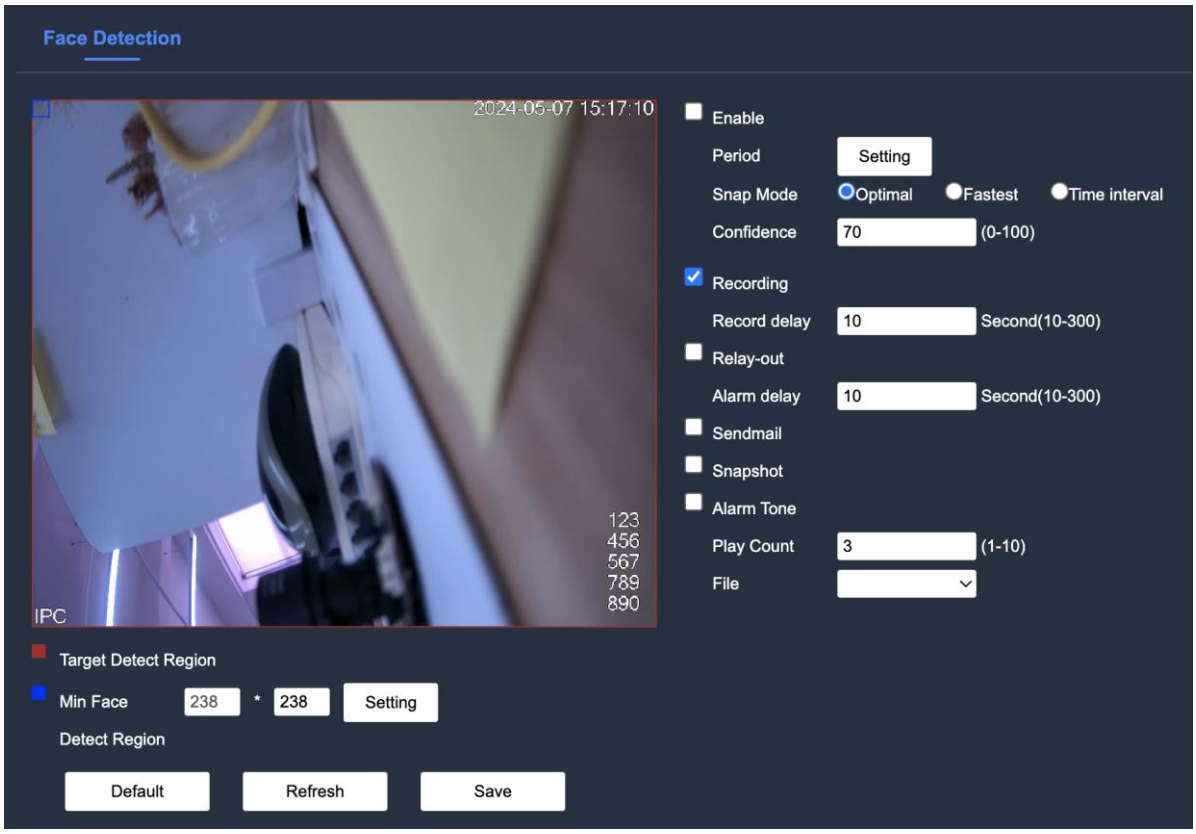
2、When Motion Detection is disabled, enabling Smart Motion Detection will automatically turn on the Motion Detection function; when both Motion Detection and Smart Motion Detection are enabled, disabling Motion Detection will also disable Smart Motion Detection.

4.4.4 Face Detection Settings

The system performs an alarm linkage action whenever a face is detected I the detection area.

Procedure

Step 1: Select Settings – Event Management – Face Detection, to display the Face Detection configuration interface as shown in the figure below.



Step 2: Set the parameters; refer to the following table

Parameter	Description
Enable	Check “Enable” to enable Face Detection features.
Target Detection	Using the right mouse button, draw the face detection area; the default detection

Region	area is the entire screen.
Minimum Face Detect Region	Using the right mouse button, draw the minimum face detection area on the preview screen or enter a value to draw. An alarm will be triggered when the size of the detected target is larger than the minimum detection boundaries.
Period	After setting the time period for the alarm, the alarm event will only start within the specified time range.
Snap Mode	The modes are Optimal, Fastest and Time-interval. • Optimal: Captures the clearest picture in the time it takes for the device to detect a face. • Fastest: The device detects a face and immediately takes a picture of it. • Time-interval: The device detects a face and takes the corresponding picture at a set time interval.
Confidence	This is the the confidence level at with the device detects a face. The higher the confidence level is set, the harder it is to detect; the value ranges from 0 to 100.
Record	If “Record”is selected, the system will automatically record the alarm when an alarm occurs. When the alarm ends, the alarm recording extends for a period of time (according to the set time) then halted.
Record Delay	
Alarm Output	Check “Alarm Output” to enable the alarm linkage output; when an alarm occurs, the system links the corresponding alarm to the output device. When the alarm ends, the alarm recording extends for a period of time (according to the set time) then halted.
Alarm Delay	
Send Email	If “Send Email”is checked, the system will send an email to notify the user when an alarm occurs.
Snapshot	Check “Snapshot”, and when an alarm occurs, the sytem will automatically capture the alarm.

Step 3: Click “Save” to complete the configuration of the Face Detection parameters.

4.4.5 Perimeter Defense Settings

This introduces the requirements for selecting scenarios and configuring rules for general perimenter defense. The basic requirements for selecting optimal scenarios are as follows:

- If the conditions allow, try to reduce the complexity of the monitoring and analysis environment; it is not recommended to use the smart analysis function in target-intensive scenarios with frequent changes in light.

- Try to avoid areas such as glass, reflective backgrounds and water; try to avoid tree branches, shadows and mosquito interference areas; try to avoid backlit scenes and avoid direct light.

Set up rules for Perimeter Defense include fence crossing, tripwire intrusion, area intrusion, items left behind, items moved, parking detection, people gathering, wandering detection, etc.

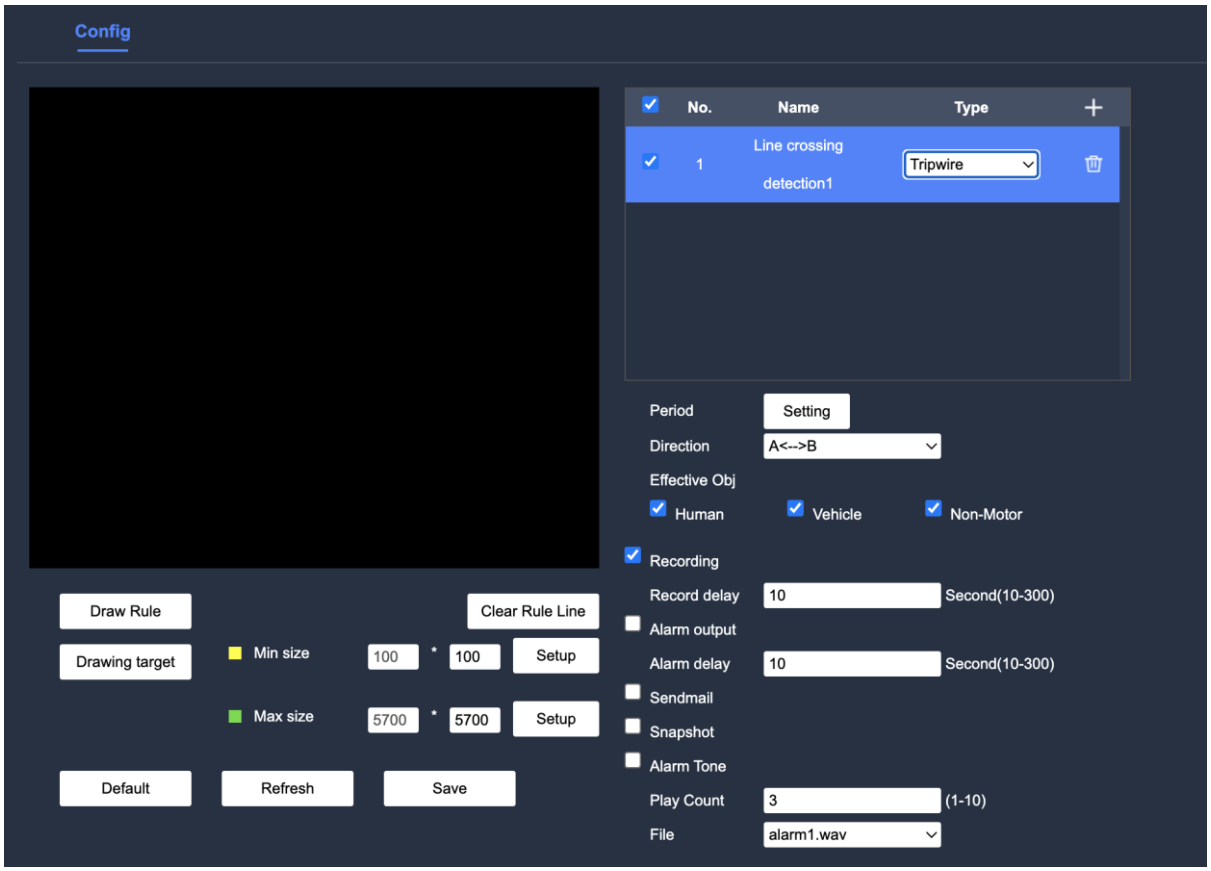
Background Information

The following table describes the roles and trial scenarios of each alarm type

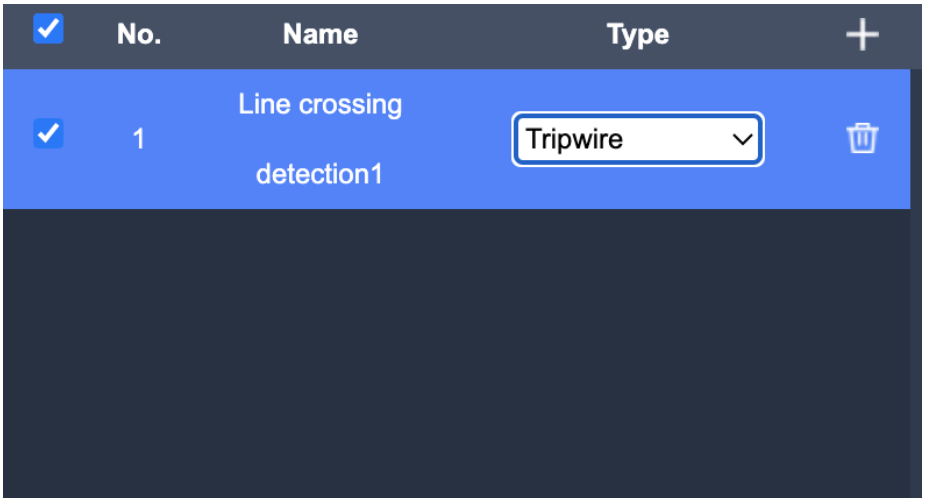
Alarm Type	Function	Trial Scenario
Tripwire	When a target crosses a tripwire in the set direction, the system executes an alarm.	Suitable for scenarios where targets are sparse and there is essentially no obstruction between targets.
Intrusion	When a target enters, leaves or appears in the detection area, the system executes an alarm.	
Object Abandoned	When targets remain in the detection area for more than the specified amount of time, the system executes an alarm.	Suitable for scenarios where targets are sparse, without obvious and frequent light changes, requiring the detection area to be as simple as possible in texture.
Object Ming	When the original target in the detection area is taken away for more than the set amount of time, the system executes an alarm	
Parking Detection	When the target is prohibited for more than the set period of time, an alarm is triggered.	Suitable for road monitoring scenarios.
Crowd Gathering	When a crowd gathers and stays or the crowd density is too large, the system executes an alarm.	Suitable for scenarios whereby targets are sparse, no obvious obstructions, and the camera is installed directly above the monitoring area as much as possible.
Loitering Detection	When a target lingers for longer than the set minimum alarm event, the system performs an alarm.	Suitable for locations such as campuses and halls.

Procedure

Step 1: Select Settings – Event Management – Intelligent Plan – Permimeter Defense - Rule Configuration, to display the Permiter Defense Rule Configuration interface as shown in the figure below; tripwire intrusion is used as an example.

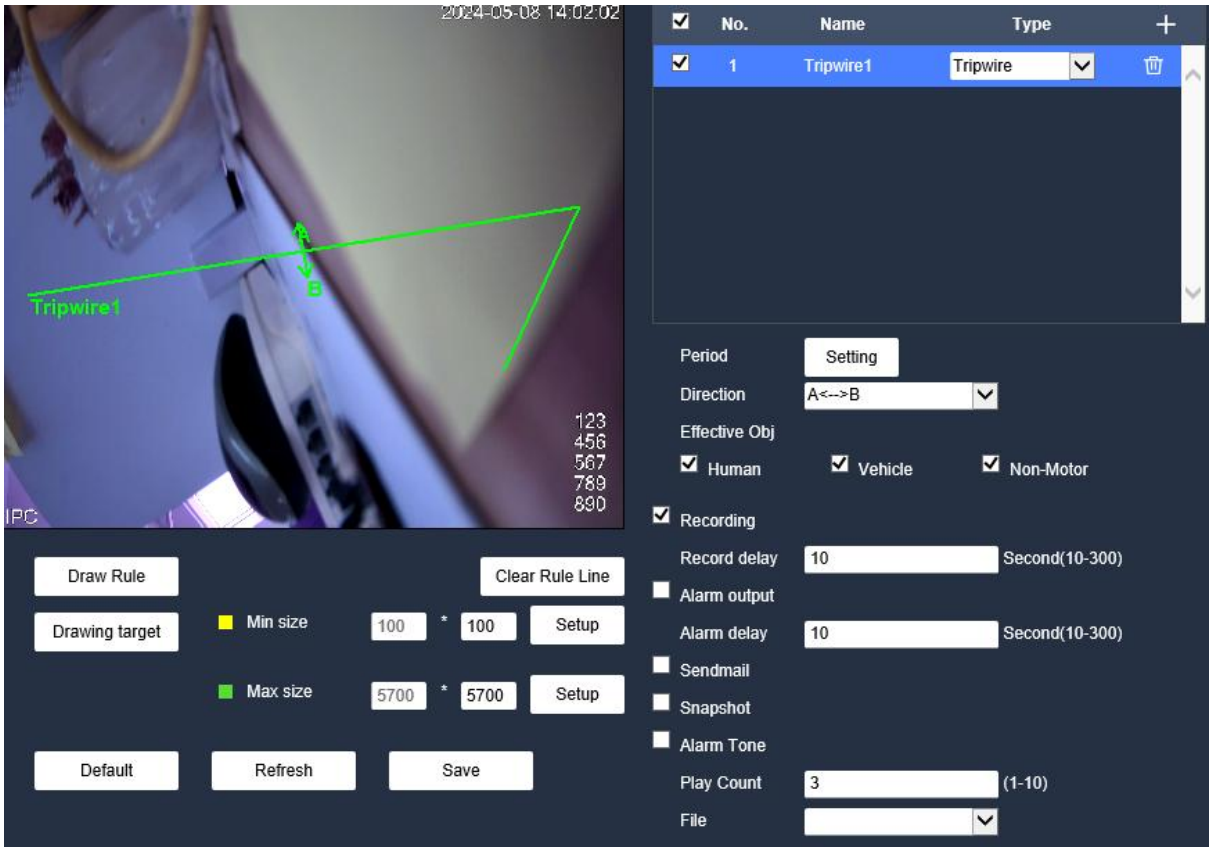


Step 2: Click the Name in the upper right corner of the page, double-click the name to modify the name of the rule, and select the type such as Tripwire intrusion as shown in the following figure.



Step 3: Rule Drawing

1、Click “Draw Rule” at the bottom of the video screen to draw the rule line for the Tripwire intrusion alarm on the preview screen using the right side of the mouse. Once the drawing is completed, the user can drag the corners of the detection area/detection line to adjust the range. Click the “Clear Rule Line” button to delete the rule line as shown in the figure below.



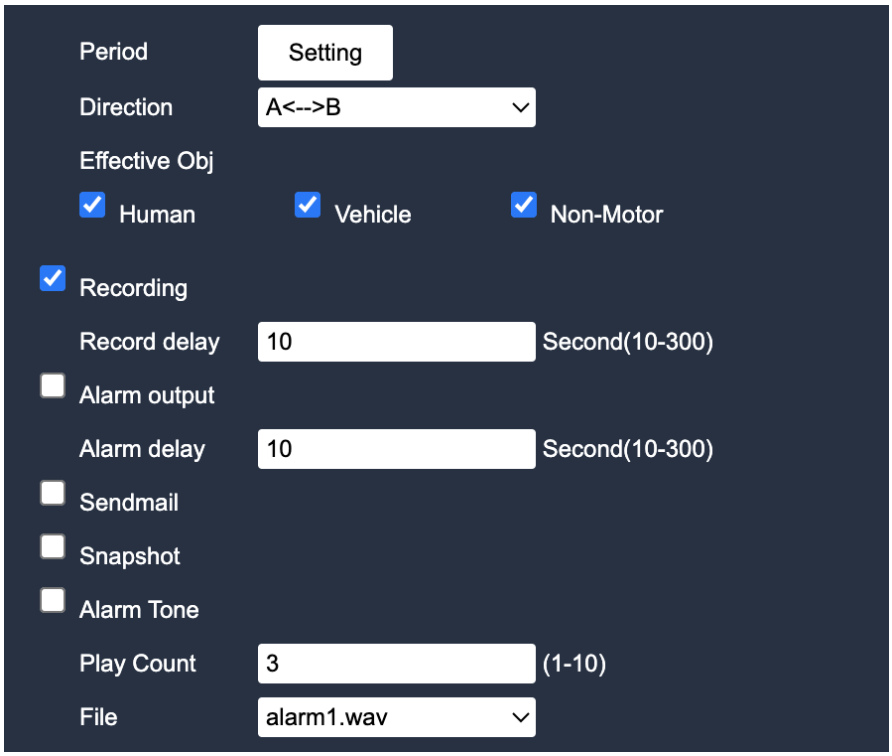
2、Drag the mouse or input the minimum/maximum values to draw the target area. The alarm will be triggered only when the size of the detected target fits between those boundaries; as shown in the figure below.

The Perimeter Defense functions are described in the following table

Rules	Description
Tripwire	Draw 1 detection line.
Intrusion	Draw 1 detection area. • When detecting objects left behind, if pedestrians/vehicles stay still for a long period of time, the alarm will also be triggered. If the objects left behind are smaller in size in comparison to the people or vehicles, either set the target size to filter out people and vehicles or extend the “Minimum Duration”value appropriately to avoid false alarms caused by people staying for a short period of time. • False alarms can be caused by low mounting heights, a single person occupying too large a portion of the frame or a heavily obscured target, constant jittering of the device, shifting leaves and shade, frequent opening and closing of park gates and dense traffic or dense gathering of people during detection
Object Abandoned	
Object Ming	
Parking Detection	
Crowd Gathering	
Loitering Detection	

Step 4: Set the rules and parameters of perimeter defense, and link the time period with the alarm.

The figure below shows the parameter configurations.



The following table describes the parameter settings

Parameters	**Description**
Period	After setting the time period for the alarm, the alarm event will only start within the specified time range.
Direction	Set the direction of thr rule's detection • When setting tripwire intrusion, the available directions are A->B, B->A and A<->B. • When setting up region intrusion detection, the available selctions are "Enter", "Exit" and "Entry and Exit".
Action	When setting up actions for Region Intrusion, the available selections are Emergence and Traversal areas
Effective Objectives	The effective targets for detection and alarm, which are the people, motor vehicles and non-motor vehicles
Recording	If "Record"is selected, the system will automatically record the alarm when an alarm occurs. When the alarm ends, the alarm recording extends for a period of time (according to the set time) then halted.
Record Delay	

Alarm Output	Check “Alarm Output” to enable the alarm linkage output; when the alarm occurs, the system links the corresponding alarm to the output device. When the alarm ends, the alarm recording extends for a period of time (according to the set time) then halted.
Alarm Delay	
Sending Mail	If “Send Email”is checked, the system will send an email to notify the user when an alarm occurs
Snapshot	Check “Snapshot”, and when an alarm occurs, the sytem will automatically capture the alarm.

Step 3: Click “Save” to complete the configuration of the perimeter prevention parameters.

4.4.6 Alarm

When the alarm input interface generates and alarm signal, the system executes the alarm action.

Procedure

Step 1: Select Settings – Event Management – Alarm Settings, to display the Alarm Settings to display the Alarm Settings configuration interface as shown in the figure below.

Step 2: Set the basic parameters; refer to the following table

Parameter	Description

Enable	Check “Enable” to enable the “Local Alarm” feature
Alarm Input	Select the alarm input port
Dejitter	Only one alarm event will be recorded during the dejittering time period.
Sensor Type	The options include the Normally Open type and Normally Closed type.
Period	After setting the time period for the alarm, the alarm event will only start within the specified time range.
Record	If “Record”is selected, the system will automatically record the alarm when an alarm occurs. When the alarm ends, the alarm recording extends for a period of time (according to the set time) then halted.
Record Delay	
Alarm Output	Check “Alarm Output” to enable the alarm linkage output; when the alarm occurs, the system links the corresponding alarm to the output device. When the alarm ends, the alarm recording extends for a period of time (according to the set time) then halted.
Alarm Delay	
Send Email	If “Send Email”is checked, the system will send an email to notify the user when an alarm occurs.
Snapshot	Check “Snapshot”, and when an alarm occurs, the sytem will automatically capture the alarm.

Step 3: Click “Save” to complete the configuration of the “Local Alarm” parameters.

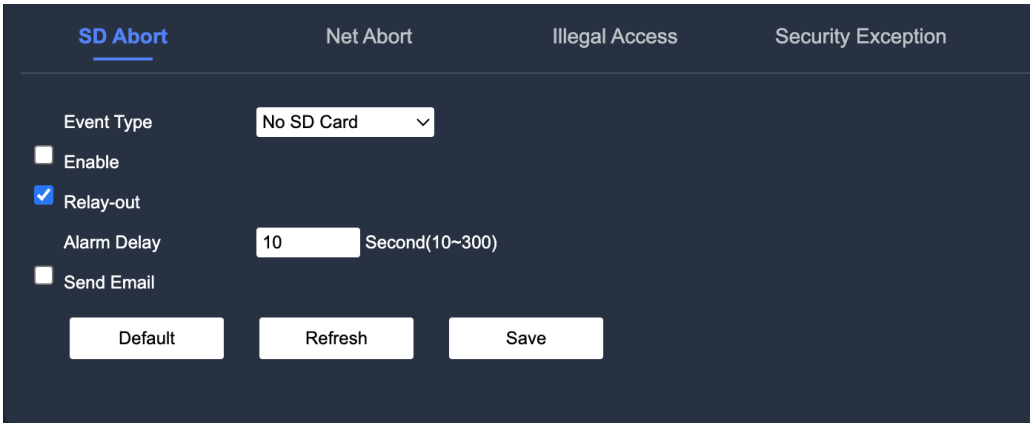
4.4.7 Abnormality

Anomaly handling includes the handling of SD card anomalies, network exceptions, unauthorized access and security exceptions.

4.4.7.1 SD Abort

When the SD card incurs an anomaly, the system will execute an alarm. SD card anomalies include no SD card, insufficient SD card storage, and SD card errors. Different devices support different functions, subjected to change based on the interface environment.

Step 1: Select Settings – Event Management – Anomaly Handling – SD Abort , to display the SD Abort interface as shown in the figure below.



Step 2: Set the basic parameters; refer to the table below

Parameter	Description
Event Type	The options include No SD Card, SD Card Insufficient Storage, and SD Card Error
Enable	Check “Enable” to enable the SD Card anomality handling feature.
Alarm Output	Check “Alarm Output” to enable the alarm linkage output; when the alarm occurs, the system links the corresponding alarm to the output device. When the alarm ends, the alarm recording extends for a period of time (according to the set time) then halted.
Alarm Delay	
Send Email	If “Send Email”is checked, the system will send an email to notify the user when an alarm occurs.

Step 3: Click “Save” to complete the configuration of the SD card anomaly handling parameters.

Instructions

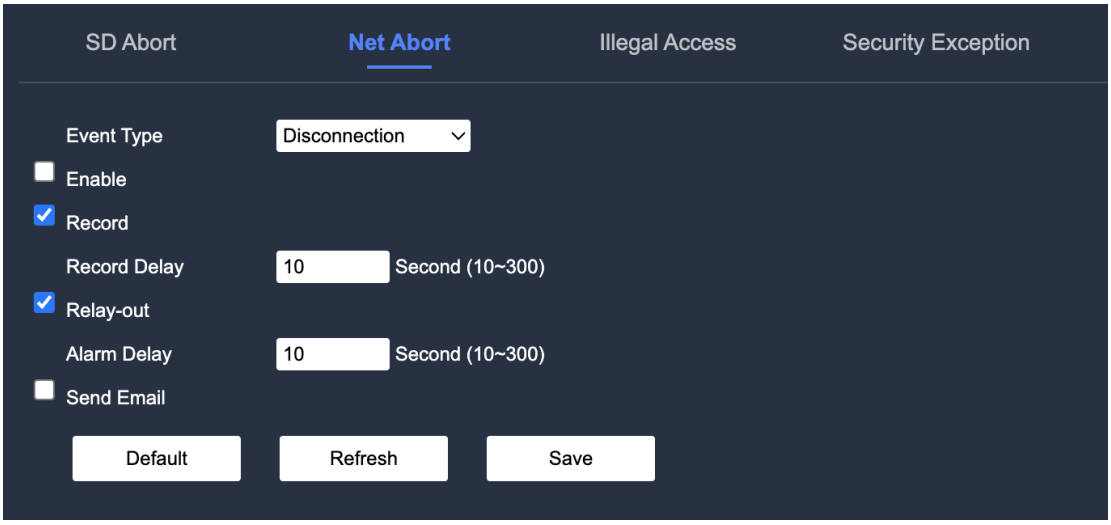
Only devices that support SD cards have anomaly handling functions such as “No SD Card”, “SD Card Insufficient Storage”and “SD Card Error”.

4.4.7.2 Network Abort

When the system incurs a network anomaly, the system performs an alarm linkage action. Network anomalies include network disconnection and IP conflicts.

Procedure

Step 1: Select Settings – Event Management – Anomaly Handling – Net Abort, to display the Net Abort configuration interface as shown in the figure below.



Step 2: Set the basic parameters: refer to the table below

Parameter	Description
Event Type	The options include Network Disconnection and IP conflicts
Enable	Check “Enable” to enable the “Net Abort” feature.
Record	If “Record”is selected, the system will automatically record the alarm when an alarm occurs. When the alarm ends, the alarm recording extends for a period of time (according to the set time) then halted.
Record Delay	
Alarm Output	Check “Alarm Output” to enable the alarm linkage output; when the alarm occurs, the system links the corresponding alarm to the output device. When the alarm ends, the alarm recording extends for a period of time (according to the set time) then halted.
Alarm Delay	
Send Email	If “Send Email”is checked, the system will send an email to notify the user when an alarm occurs.

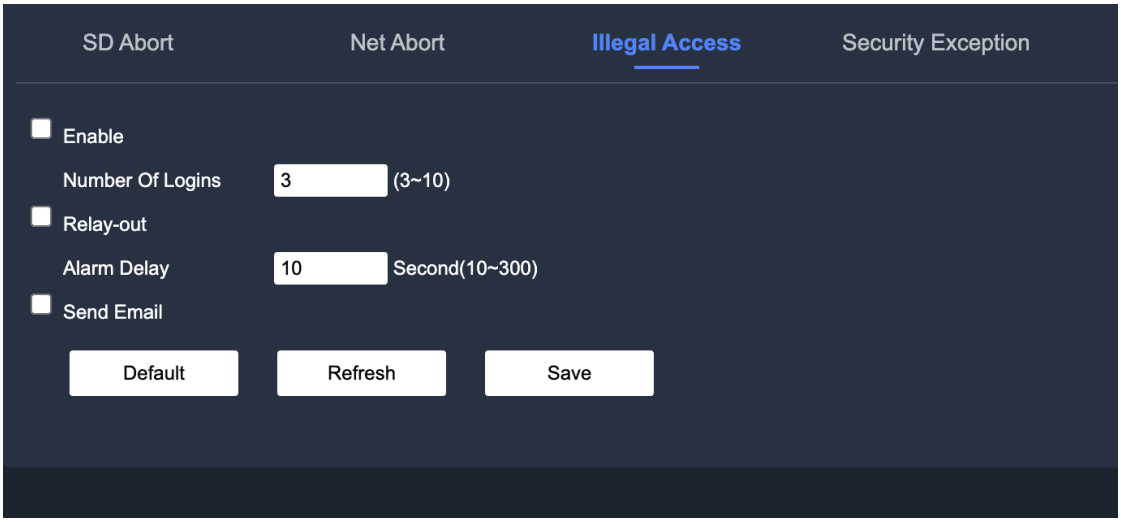
Step 3: Click “Save” to complete the configuration of the Network Anomaly handling parameters.

4.4.7.3 Illegal Access

When the number of incorrect login password entries exceeds the the limit, the system will perform an alarm linkage action.

Procedure

Step 1: Select Settings – Event Managemet – Anomaly Handling – Illegal Access, to display the Illegal Access configuration interface as shown below



Step 2: Set up the basic parameters; refer to the table below.

Parameters	Description
Enable	Check “Enable” to enable the “Illegal Access”feature
Number of Logins	Set the allowed maximum number of incrorrect login entries , and when the number of consecutive password entries exceeds this limit, the account will be locked.
Alarm Output	Check “Alarm Output” to enable the alarm linkage output; when the alarm occurs, the system links the corresponding alarm to the output device. When the alarm ends, the alarm recording extends for a period of time (according to the set time) then halted.
Alarm Delay	
Send Email	If “Send Email”is checked, the system will send an email to notify the user when an alarm occurs.

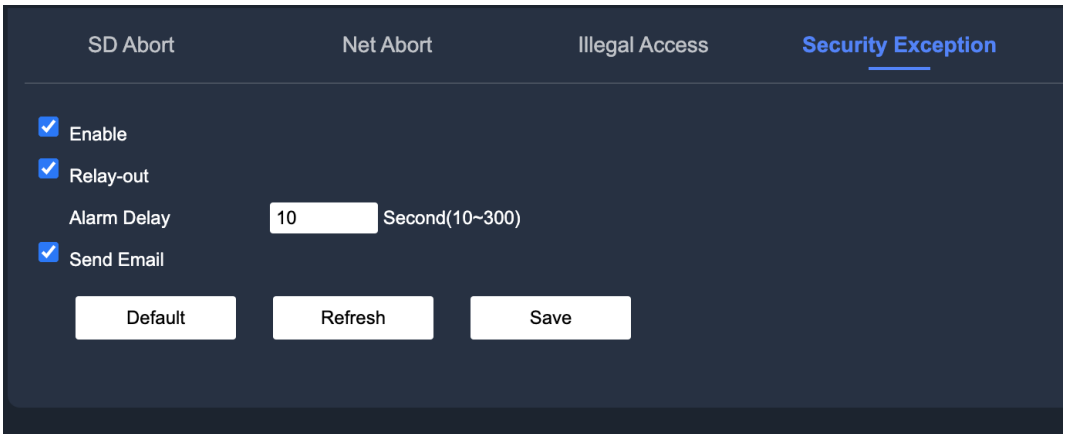
Step 3: Click “Save” to complete the configuration of the Illegal Access handling parameters.

4.4.7.4 Security Exception

When the number of incorrect login password entries exceeds the the limit, the system will perform an alarm linkage action.

Procedure

Step 1: Select Settings – Event – Anomaly – Security Exception, to display the Security Exception configuration interface.



Step 2: Set the basic parameters; refer to the table below

Parameter	Description
Enable	Check “Enable” to enable the “Security Exception” feature
Alarm Output	Check “Alarm Output” to enable the alarm linkage output; when the alarm occurs, the system links the corresponding alarm to the output device. When the alarm ends, the alarm recording extends for a period of time (according to the set time) then halted.
Alarm Delay	
Send Email	If “Send Email”is checked, the system will send an email to notify the user when an alarm occurs.

Step 3: Click “Save” to complete the configuration of the security exception handling parameters.

4.4.8 Setting Disarming

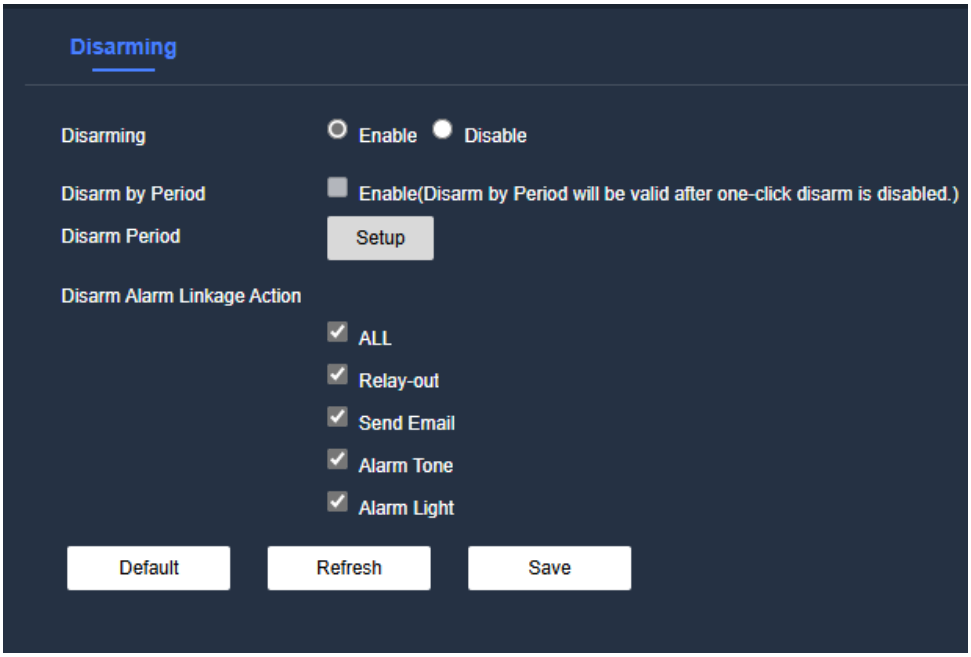
Support controlling disarm alarm linkage actions with one –click, After enabling Event Notification,the system only triggers the selected alarm linkage actions.

Procedure

Step 1: Select setup-Event-Disarming

Step 2: Enable disarming or Disarm by Period as need

- **Disarming**: The system stops triggering alarm linkage actions all the time
- **Disarm by Period**: The system stops triggering alarm linkage ctions in the selected period.



Step3: Enable or Disable **Event Notify**

Step4: select the Disarm alarm Linkage Action

Support Disarm alarm Linkage action include “Relay-out”、“ Send Email”、“Alarm Tone”、“Alarm Light”.

Selected Linkage actions, do not trigger the corresponding actions when an alarm occurs; while unselected Linkage actions, do trigger the corresponding actions during an alarm

Step5: Click **Save**

Instructions

The type of disarm alarm linkage action might vary on different device.Currently we support Relay-out, Send Email, Alarm Tone and Alarm Light.

4.4.9 Setting Auto Upload

Select the Upload mode, enable it, and then configure the parameters.the camera will upload reports of AI functions to a defined server periodically.

Procedure

Step 1: Select setup-Event-Auto Upload

Step 2: Enable the function.

Step3: Click **Add**, and the configure parameters of HTTP upload method. You can and 2 server information at most.

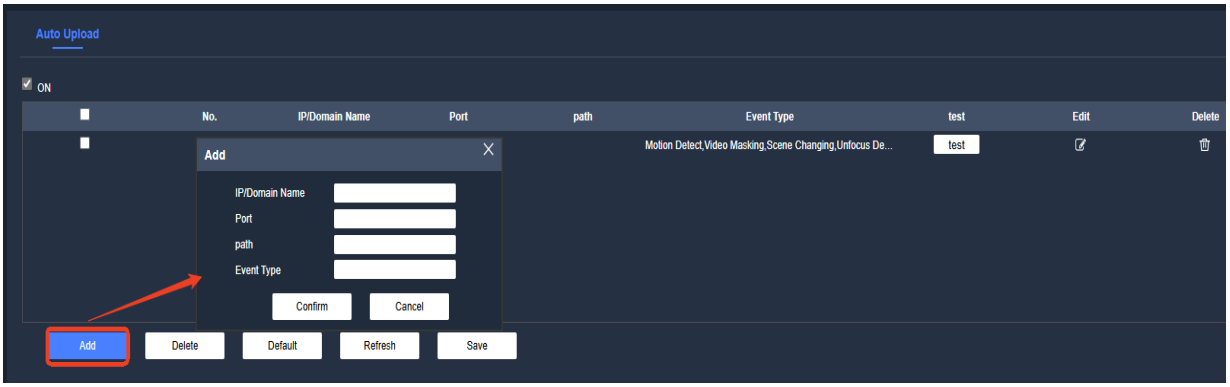


Image upload

Parameter	Description
IP/Domain name	The IP address and port number of the server which the report will be unloaded to
Port	
Path	The storage path of the server for the report
Event type	Select the event type form the drop-down list .You can select more than one types at the same time. **Instructions** The event types in the drop-down list are the same with that of picture playback.
Test	Test the network connection between the camera and the server

Description of HTTP mode psrameters

Step4: Click **Apply**

4.5 Storage Management

Storage management includes the management of resources (e.g video files) and storage space for the user's convenience and to improve the utilization of storage space.

4.5.1 Schedule

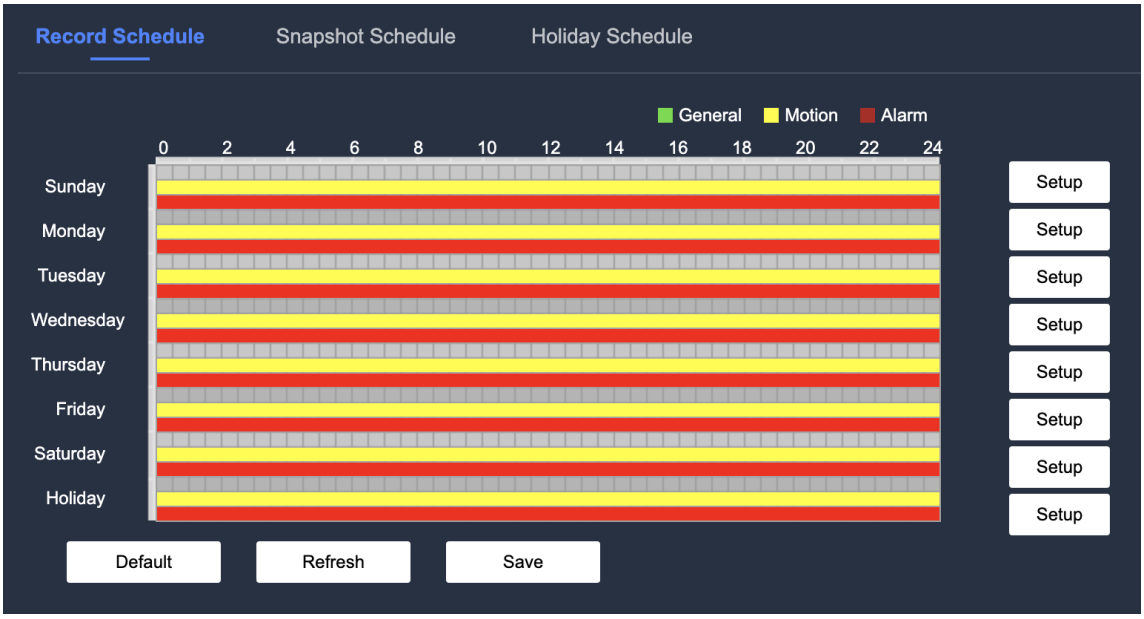
Schedule settings support setting recording schedukes, capture schedules and holiday schedules.

4.5.1.1 Record Schedule

After setting up the video channel normally, and setting up motion detection and alarm recording schedule, the video channel will be able to support alarm linkage recording

Procedure

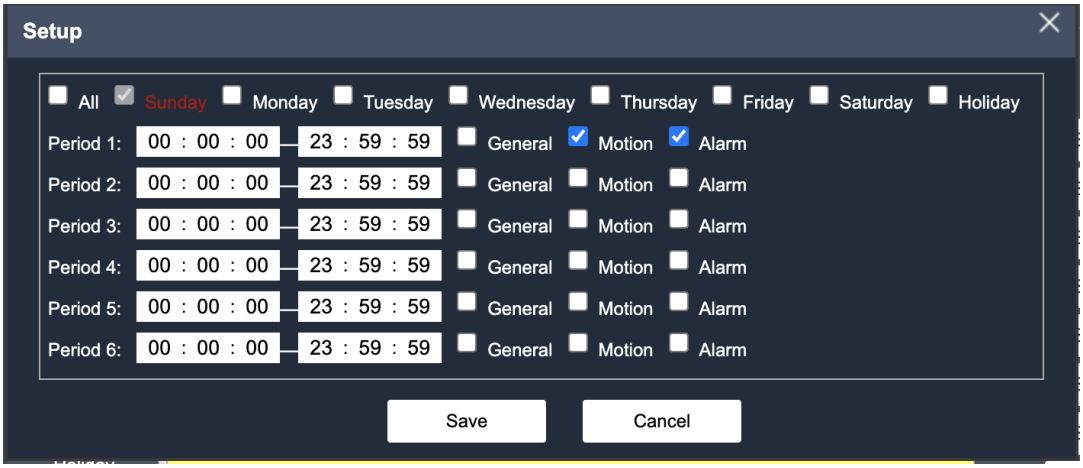
Step 1: Select Settings – Event Management – Storage Management –Schedule - Record Schedule, to display the Record Schedule interface as shown in the figure below.



Step 2: Set up the recording schedule

Green indicates a normal recording plan (i.e. timed recording), yellow indicates a dynamic recording plan (i.e. a recording plan triggered by a smart event), and red indicates an alarm recording plan (i.e. a recording triggered by an alarm).

Step 3: Click the “Setup”icon next to the preferred week and select the number of weeks (or “All”) the configuration should apply to in the pop-up “Settings” page. Select the recording type, such as “Normal”, then enter the start and end time of the recording session, and click “Save” to complete the recording plan setup. This is further illustrated in the figure below.

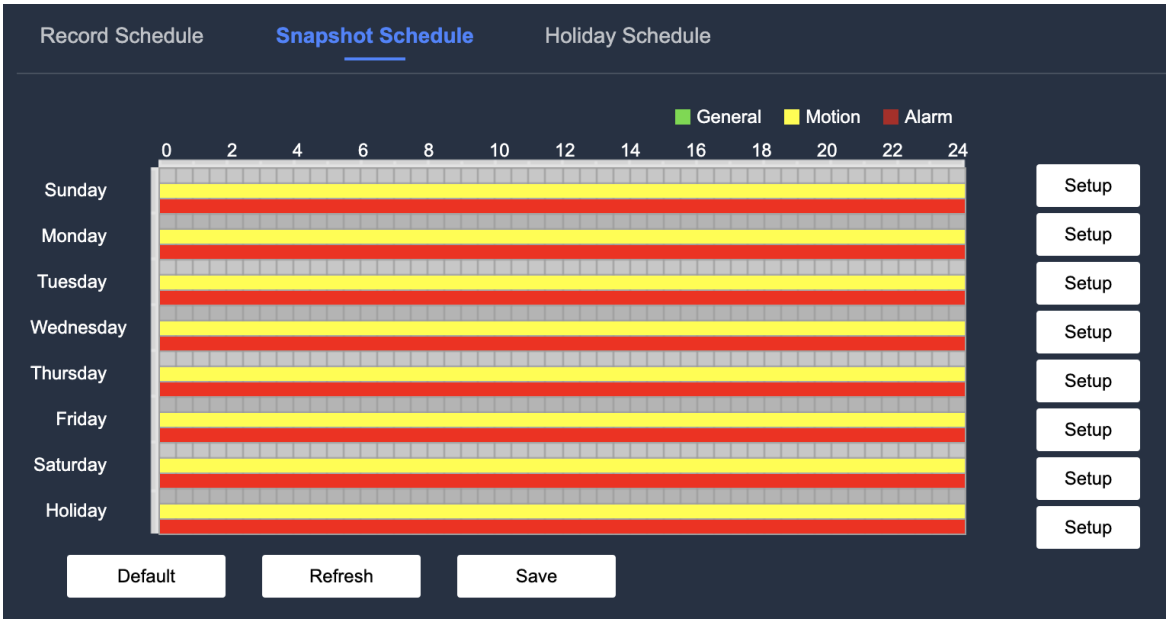


4.5.1.2 Snapshot Schedule

The system starts or stops capturing according to the set snapshpot schedule.

Procedure

Step 1: Select Settings – Event Management – Schedule – Snapshot Schedule, to display the Snapshot Schedule interface as shown in the figure below.

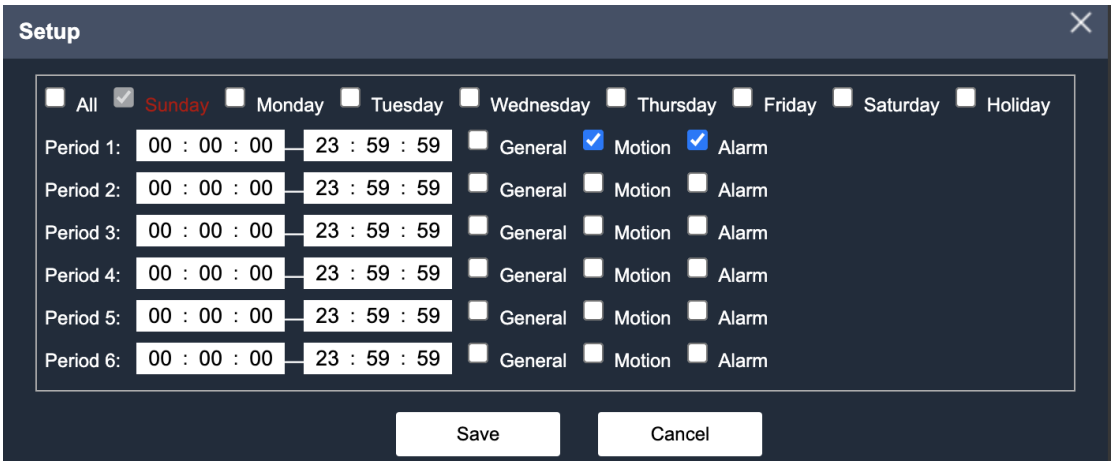


Step 2: Set up the snapshot schedule.

Green indicates a normal recording plan (i.e. timed recording), yellow indicates a dynamic recording plan (i.e. a recording plan triggered by a smart event), and red indicates an alarm recording plan (i.e. a recording triggered by an alarm).

Step 3: Click the “Setup”icon next to the preferred week and select the number of weeks (or

"All") the configuration should apply to in the pop-up "Settings" page. Select the recording type, such as "Normal", then enter the start and end time of the recording session, and click "Save" to complete the recording plan setup. This is further illustrated in the figure below.



4.5.2 Storage Settings

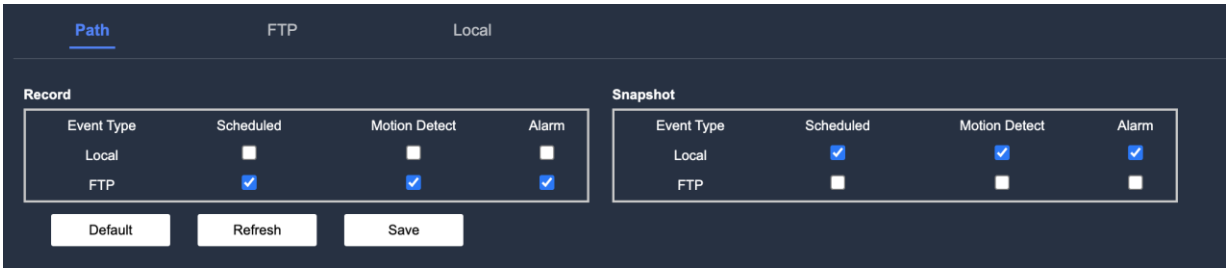
This section describes how to set up a storage point for a recording or capture of a device and how to operate on a storage point.

4.5.2.1 Path

The storage point sets the storage mode of the video and capture functions of the device. The user can choose the local SD card or FTP as storage, and store according to the type of the event recorded i.e., normal, dynamic detection and alarm event respectively. Check the box to store the the video or snapshot to its corresponding event type.

Procedure

Step 1: Select Settings – Event Management – Storage Management – Storage – Storage Point, to display the Storage Point configuration interface as shown in the figure below



Step 2: Select a storage method based on the capture and recording event type. The parameters to be set are described in the following table.

Parameters	Description
Event Type	Includes Timed, Dynamic Detection and Alarm
Local Storage	Store to an SD Card
FTP FTP	Store to an FTP server

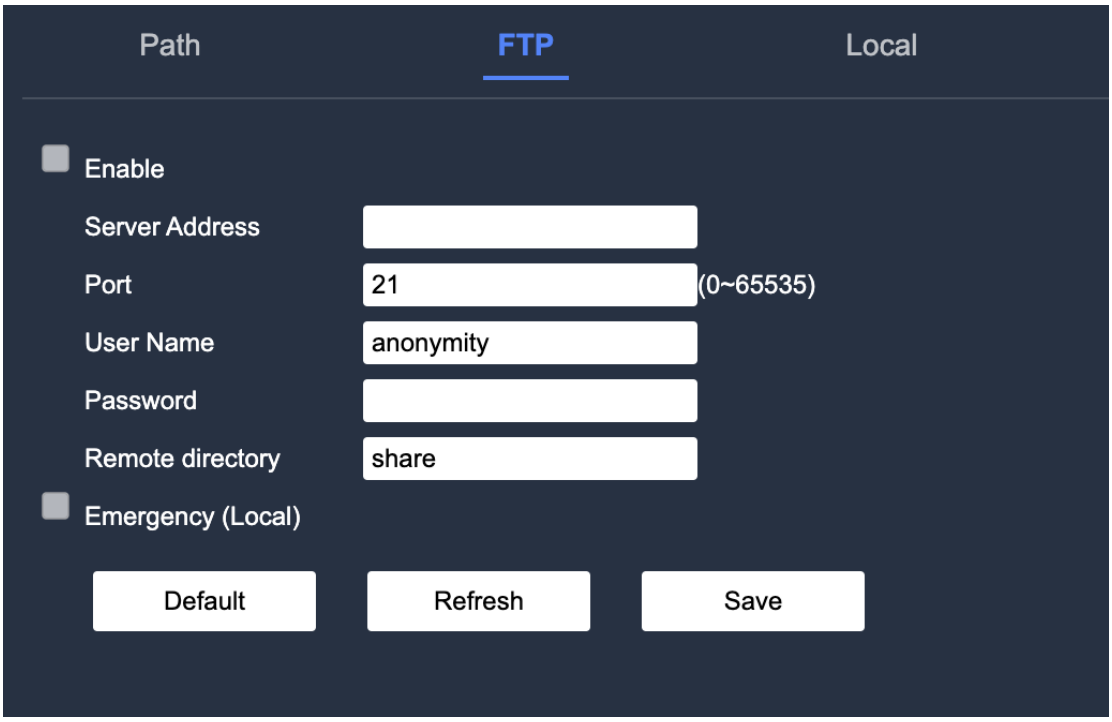
Step 3: Click “Save” to complete the configuration of the Storage Point Parameters.

4.5.2.2 FTP Storage Settings

The FTP function can be enabled only when the FTP storage mode is selected as the storage point. When the network is disconnected or malfunctioning, save all recordings or captures to the local SD card via “Emergency Save to Local”.

Procedure

Step 1: Select Settings – Event Management – Storage Management – Storage – FTP, to display the FTP configuration interface.



Step 2: Set up the basic FTP parameter as described in the table below

Parameter	Description
Enable	Check “Enable” to enable the FTP feature
Server Address	FTP server adress
Port	FTP Server port
User Name	FTP server log in account
Password	FTP server log in password
Remote Directory	The directory stored on the server; the default value is “Share”.
Emergency (Local)	Check “Emergenccy (Local)” to store the video or snpashot to a local SD card when the FTP server is malfunctioning.

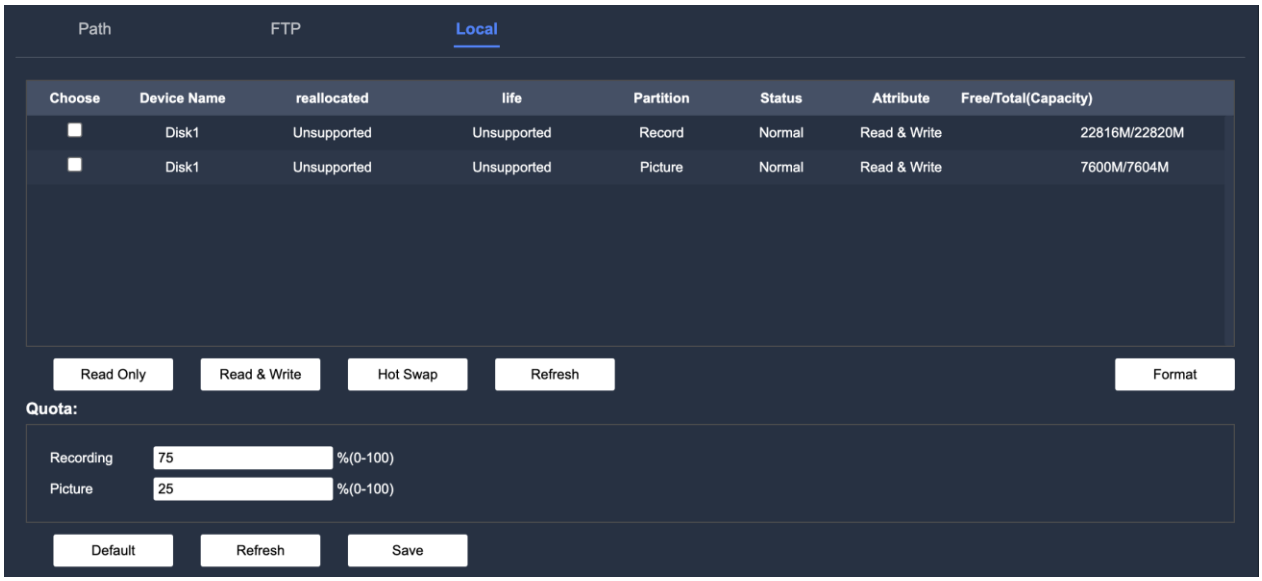
Step 3: Click “Save” to complete the configuration of the FTP parameters.

4.5.2.3 Local Storage Settings

Displays the information of the local SD card, sets the SD card to read-only, read-write or hot-swap and formats the SD card.

Procedure

Step 1: Select Settings – Event Management – Storage Management – Storage – Local Storage, to display the FTP configuration interface.



Step 2: The following table describes the local storage parameters

Parameter	Description
Choose	Select the Disk you want to set, and then you can set "Read Only "" Read & Write"“Hot Swap”""Format"
Set read-omly	SD card is set to read-only
Set read/write	SD card is set to read/write
Hot Swap	Hot swappable SD card
Format	Formats the SD card
Disk Quota	After inserting the SD card, the user can set a quota percentage. For video recording and pictures according to their needs with a threshold of (0-100%).

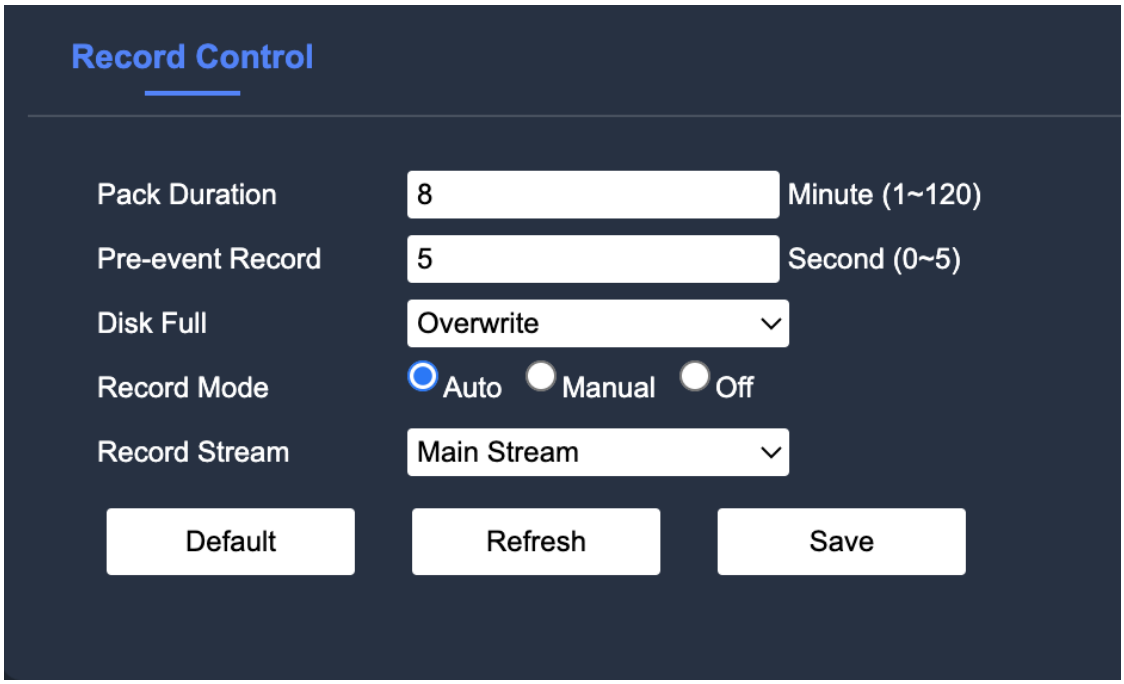
Step 3: click “Save” to complete the configuration of the local storage.

4.5.3 Record Control

Set the parameters such as recording length, pre-recording time, recording mode and recording stream.

Procedure

Step 1: Select Settings – Event Management – Storage Management – Recording Control, to display the Recording Control configuration interface.



Step 2: The following table describes the recording control parameters

Paramters	Description
Recording Length	Set the length of time to pack each video file. The default value is 8 min, with an available range of 1～120 minutes.
Pre-event Record	This is the length of time required to advance the video recording when an alarm occurs. If the preset time is set to 5 seconds, the system will store the first 5 seconds of the alarm in the recording file.
Disk Full	The user can choose to stop or overwrite • Stop: Stops recording when the working disk is full. • Overwrite: Cyclically overwrite the highest video file when the working disk is full.
Record Mode	The available modes are Manual, Automatic and Off • Manual: The system starts recording • Automatic: The system records the video within a set recording schedule • Off: The system does not record the video
Record Stream	Choose the recording stream : the main stream, substream 1 and substream 2

Step 3: Select “Save” to complete the configuration of the Record Control parameters.

4.5 System Administration

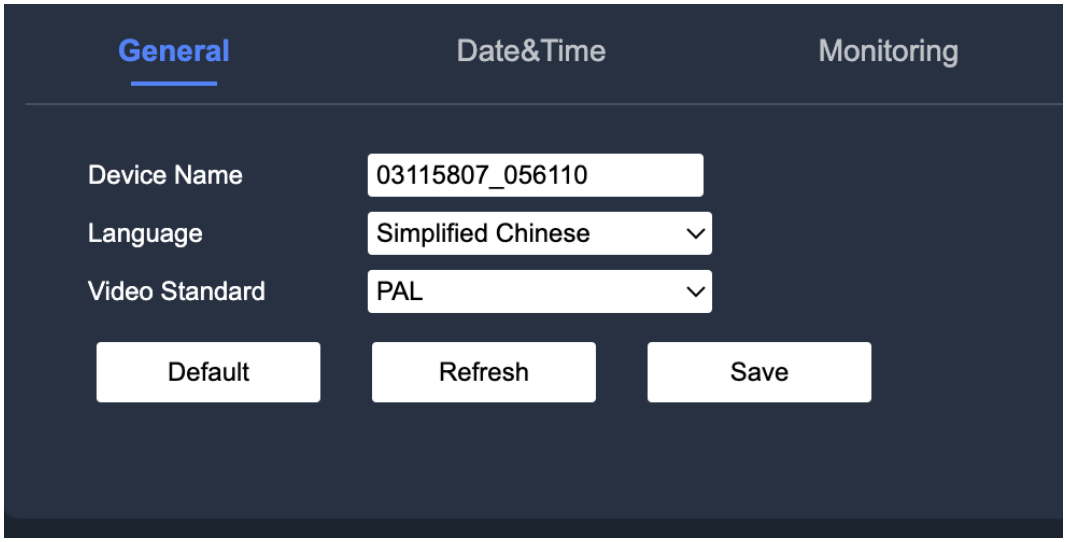
This section introduces the basic system settings such as date and time, user management, security management and configuration import and export.

4.5.1 General Setting

Sets up the basic system settings such as time and date, and general monitoring of the device.

Procedure

Step 1: Select Settings – Event Management – System Administration – General, to display the General Settings configuration interface as shown in the figure below.



Step 2: The following table describes the basic parameters

Parameter	Description
Devide Name	The device name
Language	Choose the preferred language as needed
Video Standard	Choose the preferred video format for the device

Step 3: Select “Save” to complete the configuration of the General Settings parameters

4.5.1.1 Date and Time Settings

Sets the date and time format, time zone, system time, enables daylight savings, and sets the NTP (Network Time Protocol) server.

Procedure

Step 1: Select Settings – Event Management – System Administration – General Settings - Date and Time, to display the Date and Time configuration interface as shown in the figure below.

Step 2: The following table describes the basic date and time parameters

Parameter	Description
Date Format	Select the preferred date format to be displayed
Time Format	Select the preferred time format to be displayed
Time Zone	Set the time zone accurately
Current Time	Click “Sync PC” to sync the PC time to your device time.
DST Enable	Enable Daylight-Saving Time when required at the device location. • Select “Enable” Daylight-Saving Time (DST) and set the start time and end time of Daylight-Saving Time by the day or week
DST Type	
Start Time	
End Time	
Synchronize with NTP	Sets whether to enable network synchronization and select “Enable” to enable this feature

NTP Server	Set the address of the time server
Port	Set the port number of the time server
Update Period	The period between the synchronization interval to and from and the device and time server

Step 3: Click “Save” to complete the Date and Time settings.

4.5.2 User Management

User management is used to manage the system’s user accounts, add users, delete users, or modify user information. You can manage users only when you have the user management permissions, including the ones aforementioned i.e. adding users/user groups, deleting users/user groups and modifying user information.

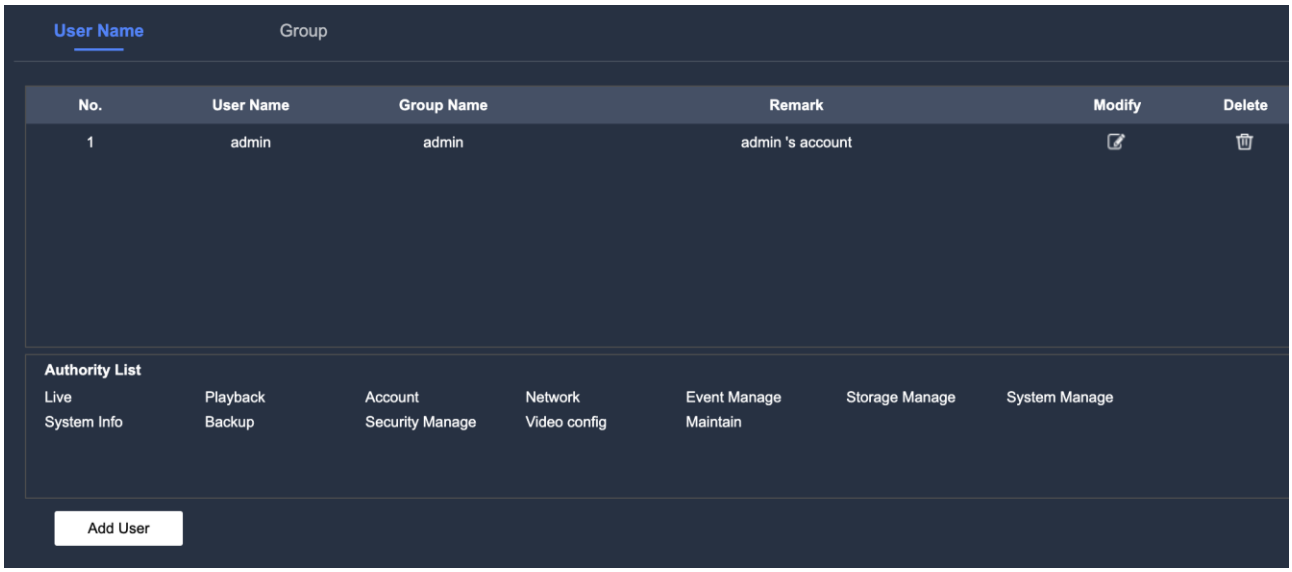
- One can add 18 users (excluding the “admin” account) and 6 user groups (excluding the “admin” and the“user”user group). User management adopts two levels of user groups and users, the group name and the user name cannot repeated. 1 user can only belong to 1 user group and the user’s privileges can only be selected as a subset ofnthe group’s privileges.
- A user actively logged in to the device can not modify his/her permissions.
- The default user in the system is “admin”, and the “admin” account has the highest priveleges in the system by default.

4.5.2.1 User

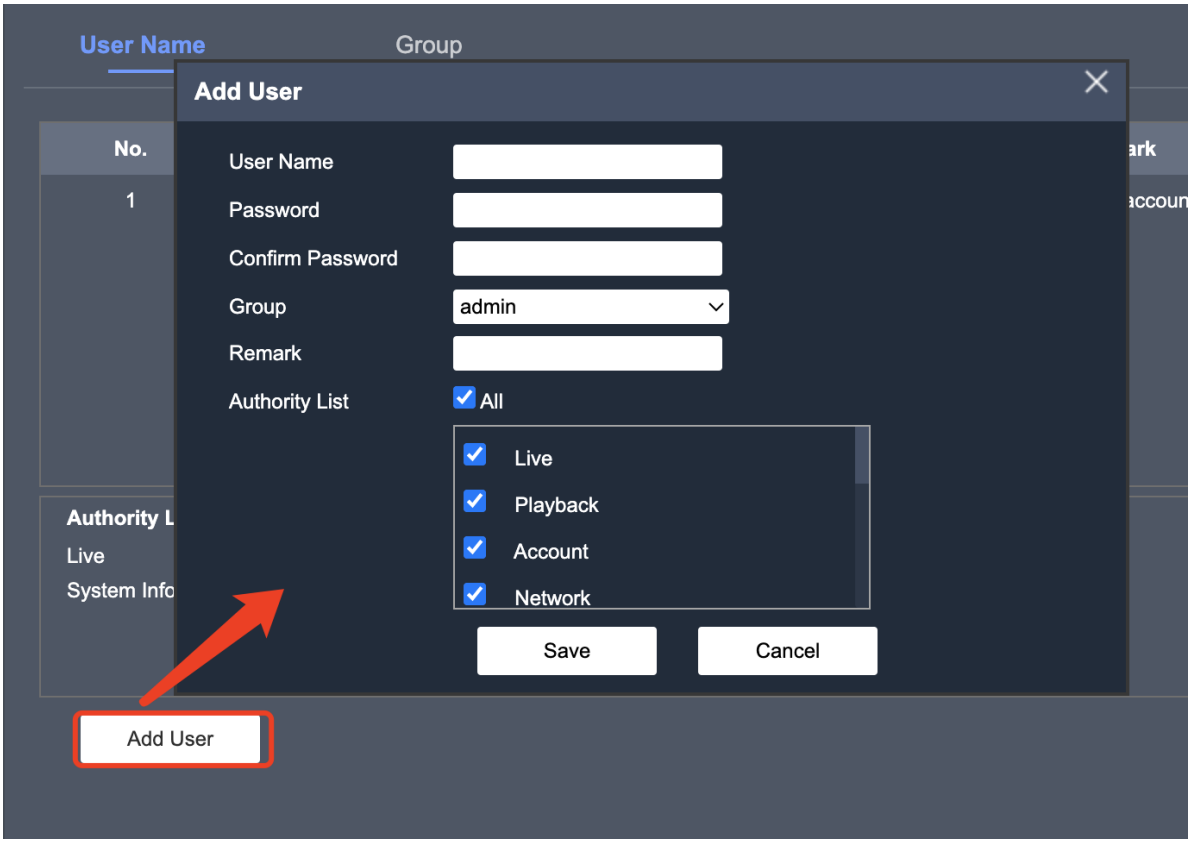
The default user of the system is the “admin” account. This account can add new users and assign different permissions to other account.

Procedure

Step 1: Select Settings – Event Management – System Administration – User Management - User, to display the User configuration interface as shown in the figure below.



Step 2: Click “Add User” to add user information, as shown in the following figure



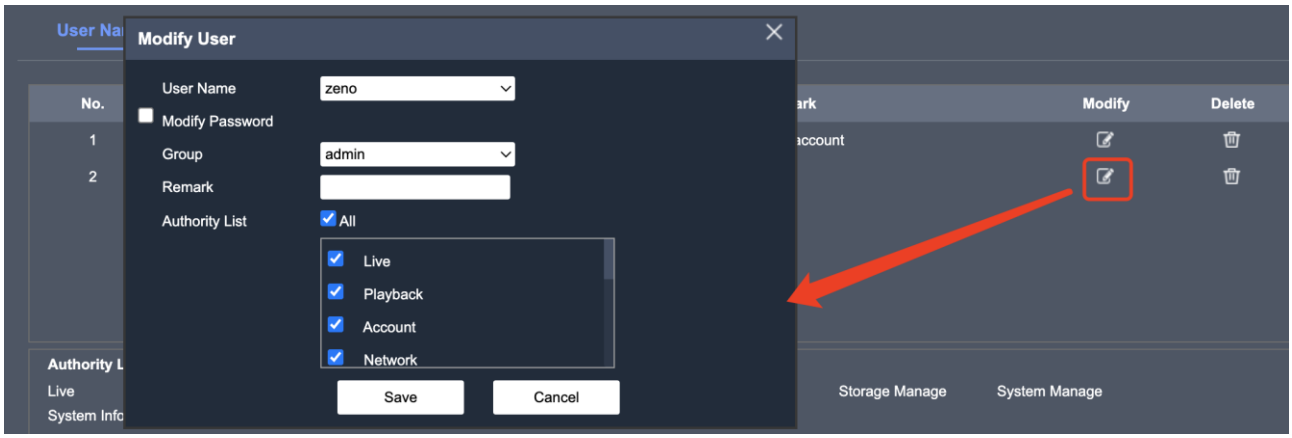
Step 3: The following table describes the basic parameters to add users

Paramter	Description
User	Enter the username; it must be unique and different from other existing usernames
Password	Enter a password and re-enter it to confirm it.

Confirm Password	
User Group	The group to which a user belongs; there should be different permissions for different user groups.
Remark	Description of the user
Authority List	Select the user's system permissions as needed.

Other Related Operations

- To modify the user's information, click to change the password of the added user, their corresponding user group, the remarks, the permissions, etc., as shown in the following figure.



Instructions

Only the "Admin" account can change the password.

- To delete a user, click to delete the user.

Instructions

The "Admin" account cannot be deleted

Step 3: Click"Save" to complete adding new users.

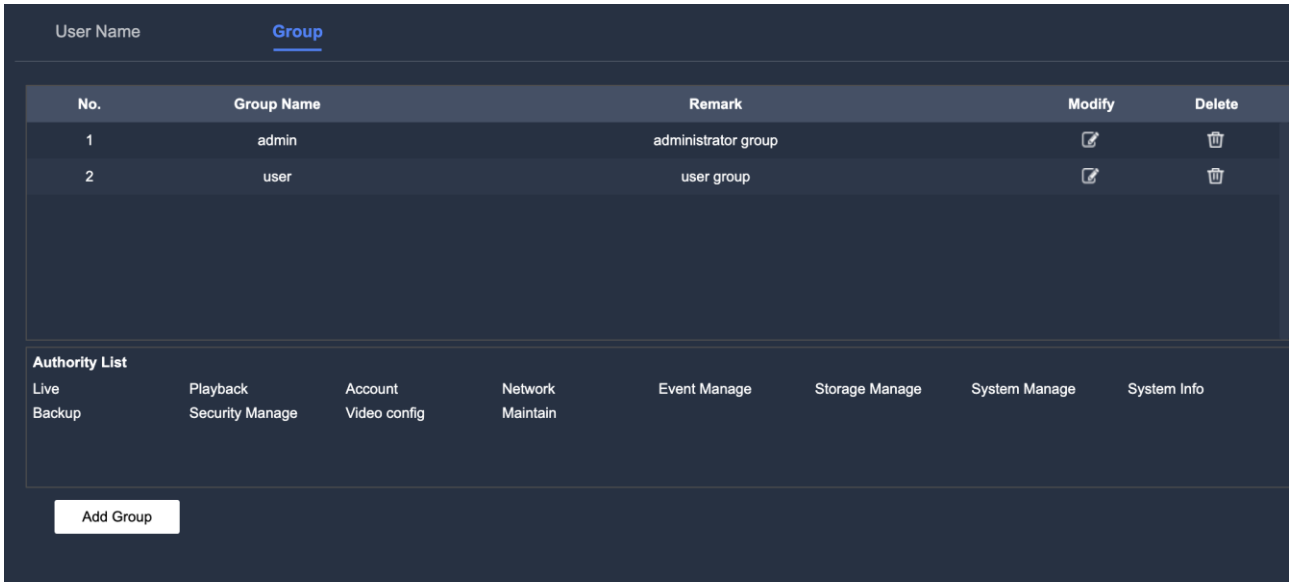
4.5.2.2 User Group

"admin" and "user"are the system's default user groups. One can add custom user groups, and after adding a user group, one can modify the permissions and remarks of the user book.

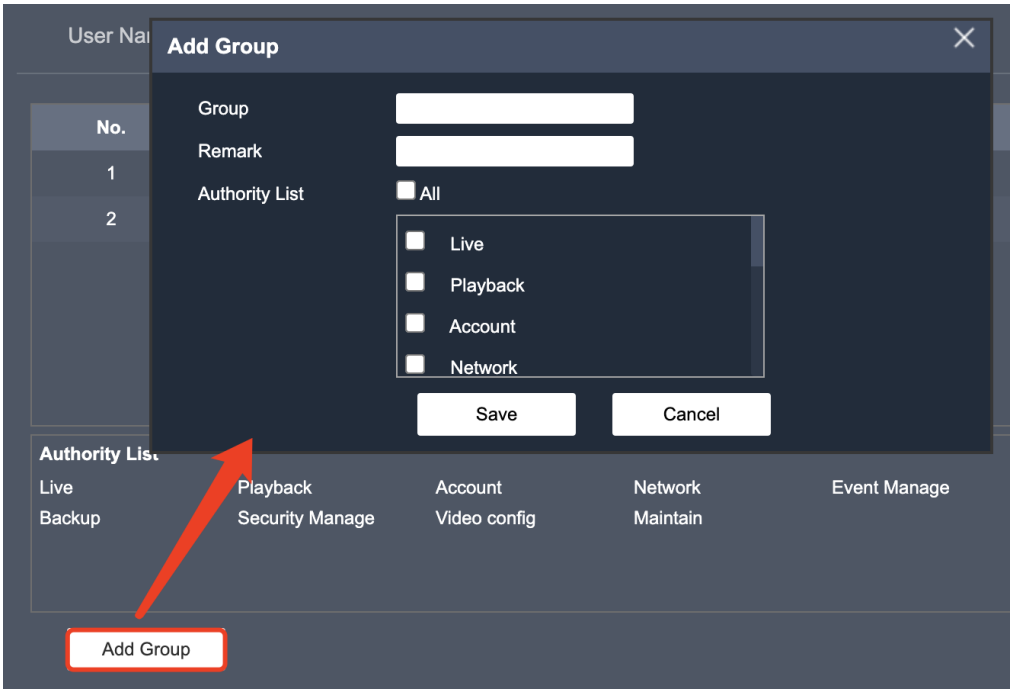
Procedure

Step 1: Select Settings – Event Management – System Administration – User Management –

User Group, to display the User configuration interface as shown in the figure below.



Step 2: Click “Add User Group” to add user group information, as shown in the folloing figure below.



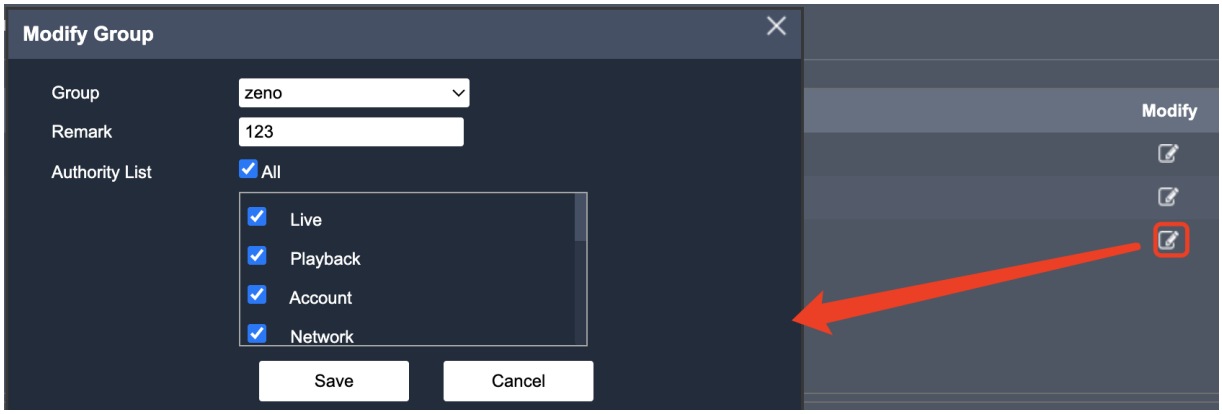
Step 3: The following table describes how to add user groups to the system

Parameter	Description
User Group	Enter the name of the user group; it must be unique and different from other existing user group names
Remark	Description of the user group

Authority List	Select the user group system permissions as needed

Other Related Operations

- To modify the user group information, click to modify the remarks and permissions of the added user as shown in the following figure.



- To delete a user group, click to delete a user group.

Instructions

The “Admin” and “user” user groups cannot be deleted

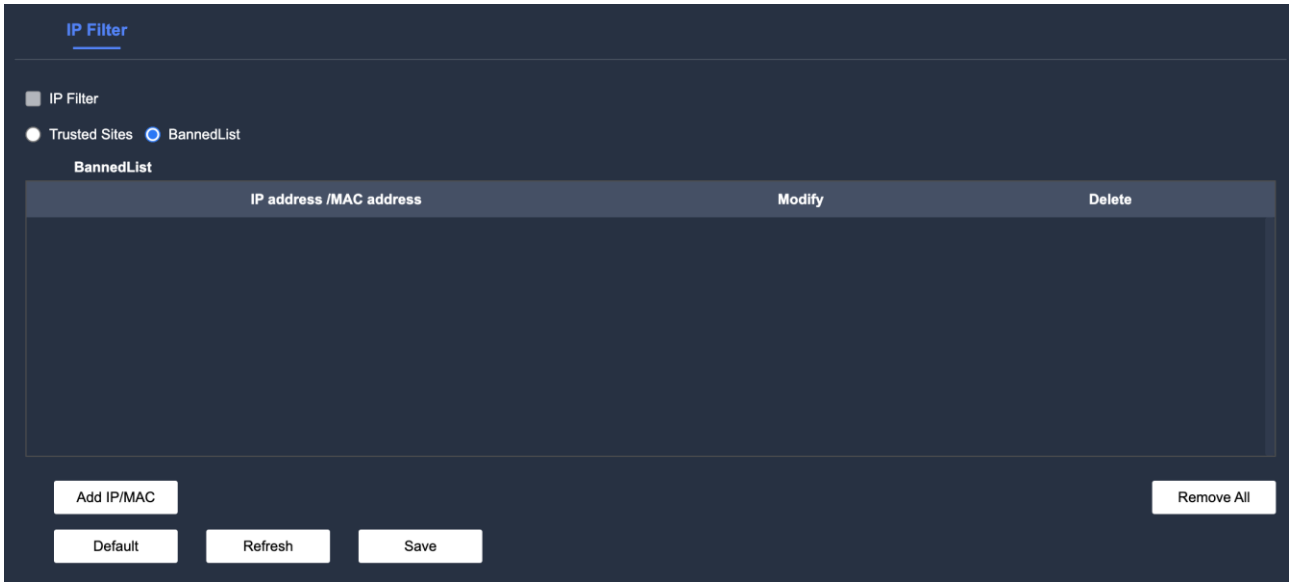
Step 3: Click “Save” to complete the adding of user groups

4.5.3 Safety Management

Sets IP permissions. It can also be set up to allow access to the device interoperability or to restict user access.

Procedure

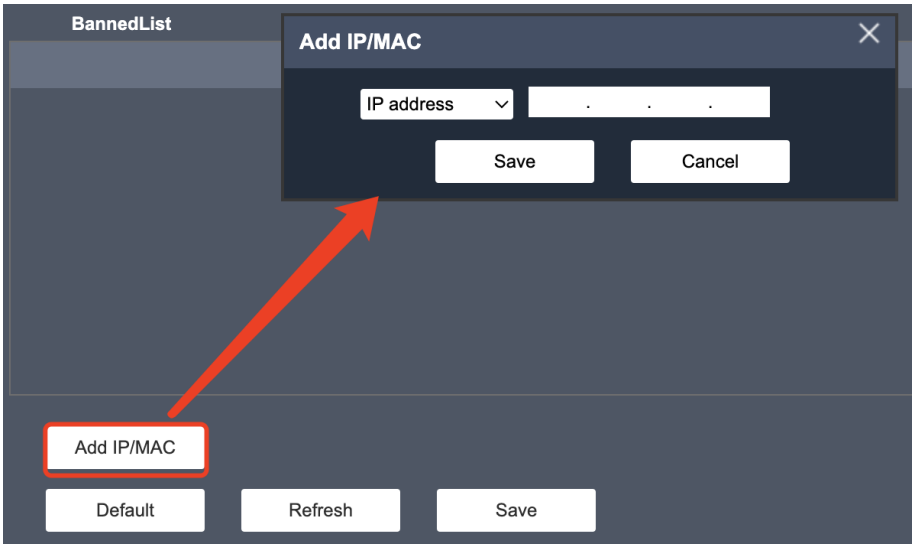
Step 1: Select Settings – Event Management – System Administration – Safety Management –IP Filter, to display the IP Filter configuration interface as shown in the figure below.



Step 2: Select the preferred IP permission mode

- Whitelist: Only the user IP/MAC addresses in the whitelist can access the device.
- Blacklist: The user IP/MAC addresses in the blacklist cannot access the device

Step 3: Click “Add IP/MAC”to add the host IP/MAC address into the whitelist or blacklist and click “Save” as shown in the following figure.



Other Related Operations

- To modify the host IP/MAC address into the blacklist or whitelist , click
- To delete the host IP/MAC address from the blacklist or whitelist , click

4.5.4 Factory Default Settings

Restores the device to its default settings

Select Settings – Event Management – System Administration – Default to display the Default configuration interface as shown in the figure below.

Simple Default: Configurations other than IP addresses, user management and other information will be restored.

Factory Default: Restore all the configurations of the device to their factory settings.

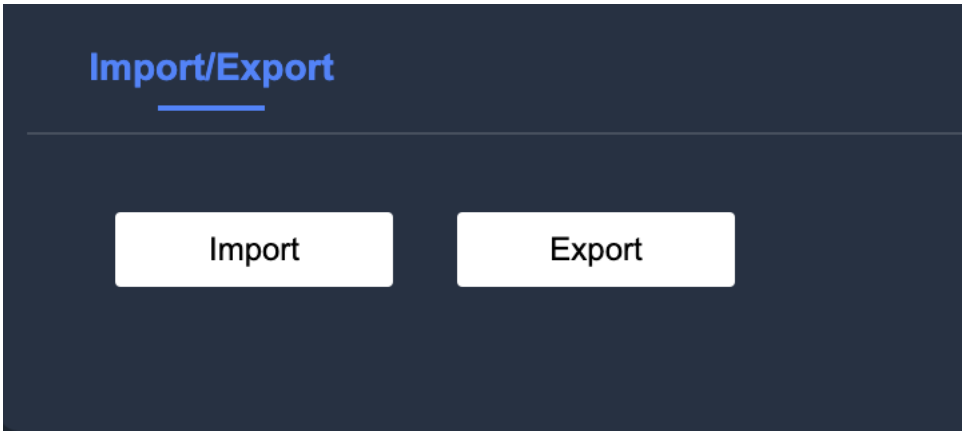
Caution

A simple default or factory default will erase information from the device, so use with caution.

4.5.5 Configuration Import and Export

Importing a configuration file allows you to quickly configure device information. Exporting a configuration file backs up the device configuration information.

Select Settings – Event Management – System Administration – Import/Export to display the Import/Export configuration interface as shown in the figure below.



Import: Import the locally backed up configuration file into the desired device.

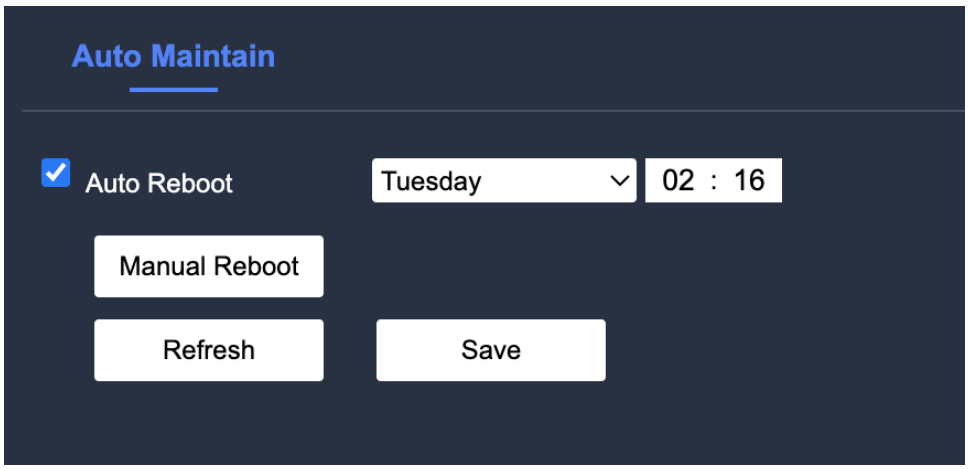
Export: The configuration file is saved in the download path of the browser by default.

4.5.6 Auto-Maintain

Users can set up automatic reboots when needed. The user can set the period and time; the default is set to every Teusday at 2:00 a.m. - automatic reboot. Users can also manually reboot the device.

Procedure

Step 1: Select Settings – Event Management – System Administration –Auto Maintain to display the Auto Maintain configuration interface as shown in the figure below.



Step 2: The following table describes the Auto-Maintain parameters

Parameter	Description
Auto Reboot	Select “Auto Reboot”to enable the automatic system restart function. Set the period and time of the automatic restart anf th device will automatically restart this time.
Refresh	Click “Refresh” to restart the device

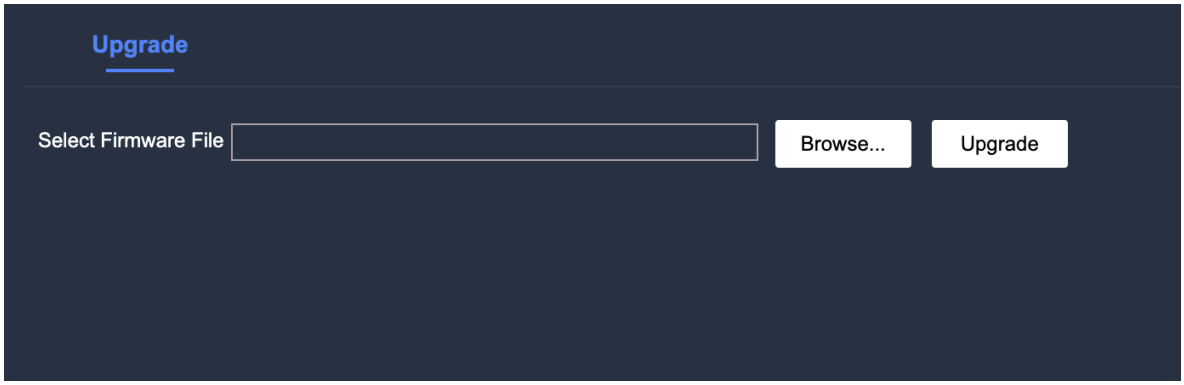
Step 3: Click “Save” to configure the parameters for automatic maintenance.

4.5.7 Upgrade

The device can be upgraded to improve the function and stability of the device,

Procedure

Step 1: Select Settings – Event Management – System Administration –Upgrade to display the Firmware Upgrade configuration interface as shown in the figure below.



Step 2: Click “Import” to import the local upgrade file which is a .bin type file. Click “Upgrade” to upgrade the device.

Instructions

1、Do not turn off the power during the upgrade process. The IP camera will automatically restart after the upgrade is completed

2、After the error file is upgraded, some functions of the device may be abnormal, and it is recommended to restart and restore the device to its previous version

4.6 Information

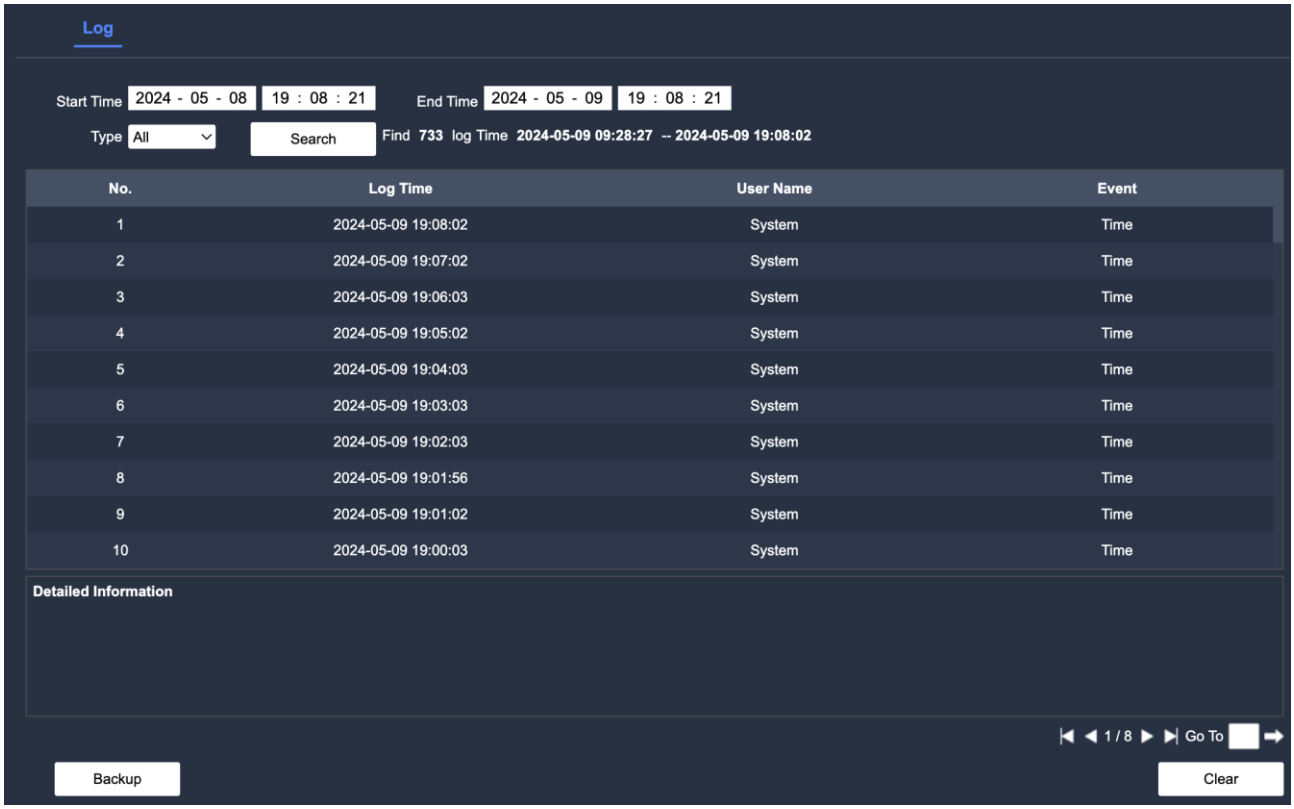
The user can view system logs, version information and the number of online users.

4.6.1 Logs

Views and backs up system log information

Procedure

Step 1: Select Settings – Event Management – System Administration –Log to display the System Logs configuration interface as shown in the figure below.



Step 2: The following table describes the System Log parameters

Parameters	Description
Start Time	Start time of log query (the earliest time that can be set is 2000–01–01)

End Time	End time of log query (the latest time is 2037-12-31)
Type	Log types include system operations, configuration operations, data operations, event operations, recording operations, user management and clearing logs
Backup	Back up the searched log information to the computer that is currently being used
Clear	Click “Clear” to clear all log information on the device.

4.6.2 Version

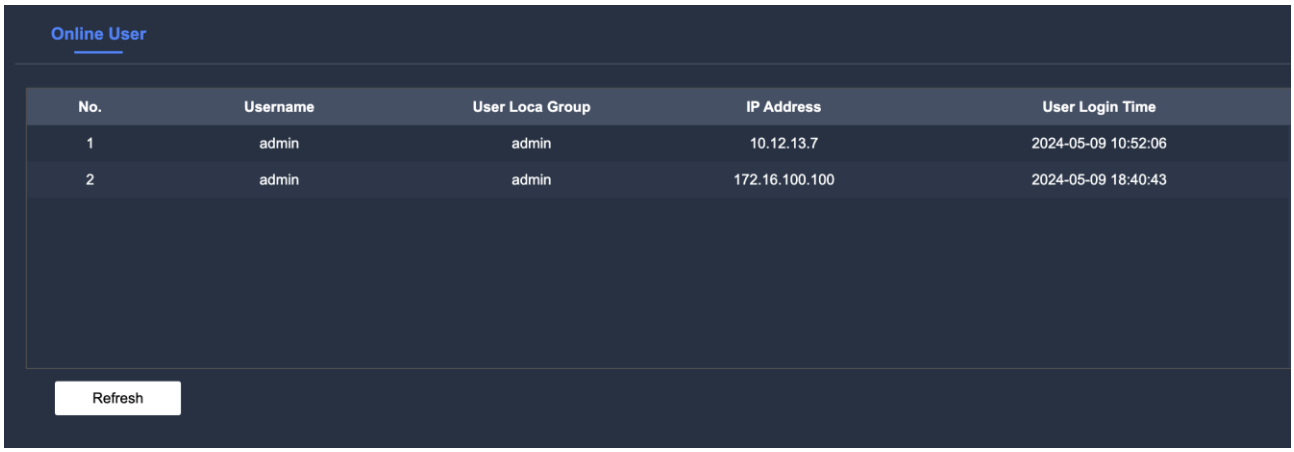
Users can view device information, system device type, software version, web version and other version information.

Select Settings – Event Management – System Administration –Version to display the Version Information interface as shown in the figure below.

4.6.3 Online User

Views the information of users currently logged in to the web.

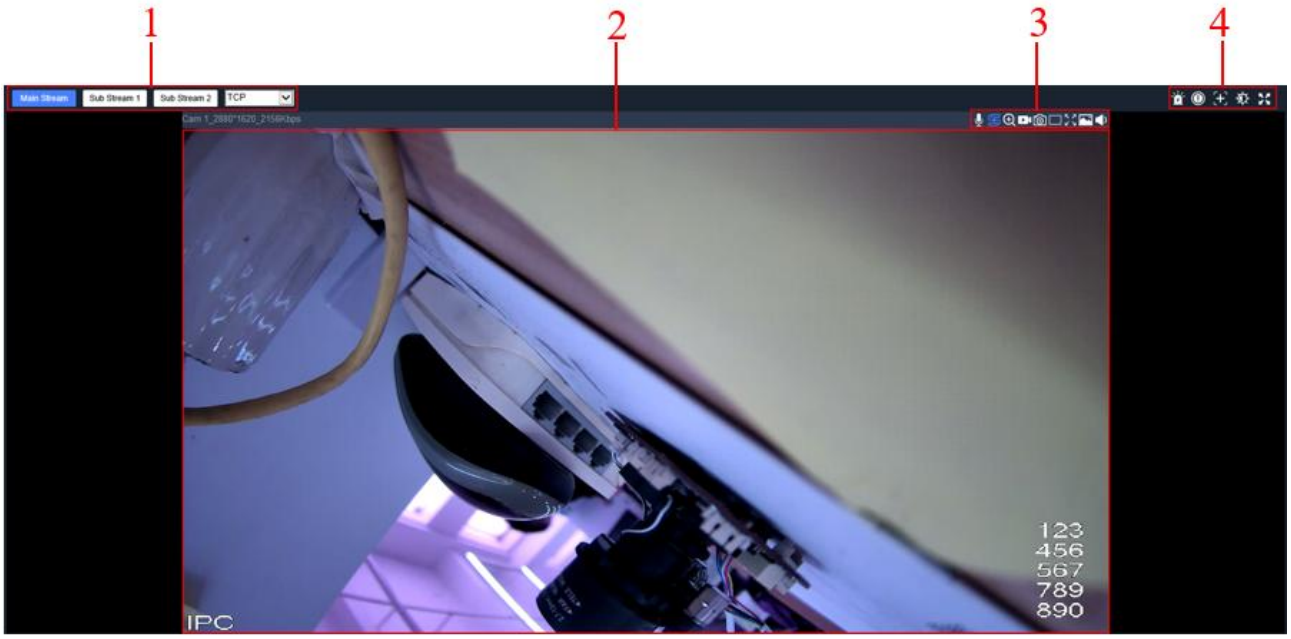
Select Settings – Event Management – System Administration –Online User to display the Online User interface as shown in the figure below.



5 Live

5.1 Preview Interface

The layout of the preview interface may vary for different device models. This section introduces the overall preview interface. On the web interface, click “Preview” to enter the video preview interface. Please refer to the figure below.



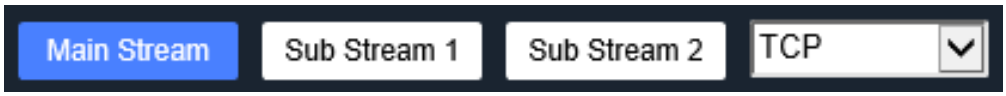
Preview Interface

The following table describes the layout of the preview page

Number	Feature	Description
1	Encoding Settings	Set the video stream type and streaming protocol type
2	Real-time Video	Displays a real-time preview of the device
3	Shortcut Control Bar	Displays the shortcut functions that are supported when viewing the live screen.
4	Picture Adjustment Bar	Displays the screen adjustment operations that are supported when viewing the live screen.

5.1.1 Encoding Parameter Settings

It is located on the left side of the preview page; select the channel video stream.



Coding Settings

Main Stream: This is a high-definition stream, with a bitstream value that is relatively large and relatively little image compression. As a result, the image clarity is high, however, the occupied bandwidth is relatively large, which is more suitable for storage and preview.

Sub-stream: Divide into sub-stream 1, an SD stream, and sub-stream, a smooth stream. The bitstream value is much smaller compared with the mainstream, the image is taught smoothly and occupies less bandwidth. This makes it suitable for previewing instead of the main stream when the network bandwidth is insufficient.

Streaming Protocol: Networ Transport Protocol. Supports TCP (Transmission Control Protocol), UDP (User Control Protocol) and multicast.

Instructions

Before selecting “Multicast” as the streaming protocol, the multicast parameters must be set.

5.1.2 Introduction to the Shortcut Function Bar

Shortcuts are availabe when viewing live video.

The following table describes the shortcut function

Icon	Feature	Description
	Talk	Turns voice intercom on or off
	Smart Info	Click this icon to enable or disable the pre-set smart rule information, which defaults to “enabled” every time you log on to the web interface.
	Local Range	Click on local zoom to zoom in on the selected area of the screen to view specific points that could be too small. The preview interface supports two types of zoom operations: • Method 1: Click on the icon, select the area to be in enlarged on the Preview screen, then right-click to restore to its original state. • Method 2: Click the icon and scroll the mouse wheel to zoom in and out of the video screen.
	Local Recordg	Records the preview video and saves it on the preferred storage location.
	Capture Picture	Makes a snapshot of the current preview screen and saves it on the preferred storage location.
	Fit Rate	Click this icon, and the video will be displayed to fit the window size. Click the icon again and the screen will be restored to the original scale.
	Full Screen	Click the icon to display the video in full screen. In full-screen mode, double-click the screen or press the【Esc】 key to exit full-screen mode.
	Triple Capture	Captures 3 images of the preview screen at a rate of 1 capture per second and saves in the set storage path.
	Audio Config	Click the icon to turn on/off the sound during preview.

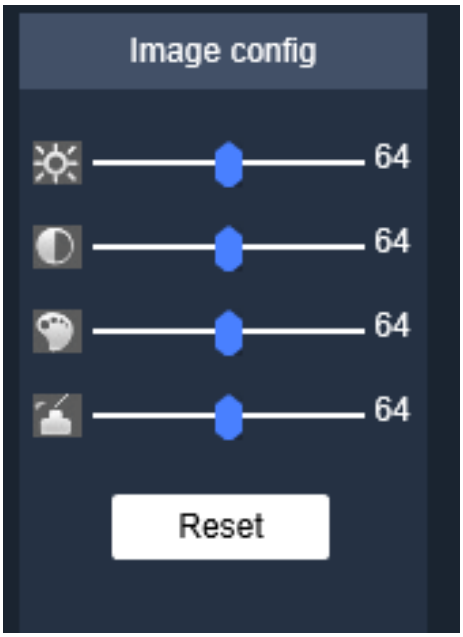
5.1.3 Introduction to the Screen Adjustment Bar

This section describes how to adjust the screen via the screen adjustment bar.

The following table describes the screen adjustment functions.

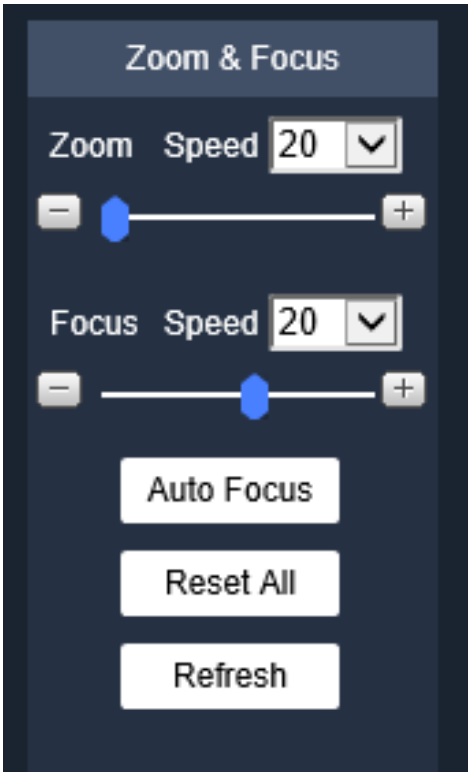
Icon	Features	Description
	Relay- Out	Displays the alarm output status. When the alarm output connector is connected to an alarm output device, click this icon to force the alarm signal to be output or turn off the alarm. When the alarm output status is red, the alarm output is turned on. When the alarm output status is black, the alarm output is off.
	Displays Alarm Subscription	Click this icon to view the alarm messages and related captures of real-time alarms in a waterfall stream.
	Zoom& Focus	Click this icon so the focus zoom interface appears on the right side of the preview interface. Left-click the mouse to adjust the focus zoom settings, and the device will automatically focus after adjustment. You can also click the auto-focus button to automatically focus on the video screen. **Instructions** For devices that supports motorized zoom only; fixed focus devices are not supported.
	Image Config	Click this icon and the “Image Adjustment” parameter will be displayed on the right side of the preview interface to adjust the brightness, contrast, chromaticity and saturation of the image. This adjustement does not modify the actual parameters of the device, and only takes effect in the opened WEB interface as shown in the figure below.  : Brightness: Adjusts the brightness of the image as a whole to be bright or dark.The image brightness of the entire screen is increased or decreased by an an equal amount when the adjustment is made.  : Contrast: Adjusts the contrast of the image when the overall brightness of the image is sufficient, but the contrast between the dark and bright areas of the image is low/high.  : Chroma: Adjusts the color depth. This threshold automatically generates a default value based on the sensor’s light-sensitive characteristics and generally does not need to be

		adjusted.  : Saturation: Adjusts the vividness of the colors in an image.Adjusting this characteristic, will not affect the overall brightness of the image.
	Full Screen	Click this icon to display the video in full screen . In full screen mode, double-click the screen or press the【Esc】to exit the full screen.



5.1.4 Introduction to Zoom Focus

Adjust the clarity and size of the video screen by zoom focus; the advice focuses automatically after adjusting the zoom parameters. According to the installed lens type, the correspoinding web interface will be displayed. After switching lenses, the device needs to be powered off and restarted after switching lenses. “Zoom Focus” is located on the upper right corner of the interface, and is used to adjust the parameters of the video screen as shown in the figure below.



The following table describes how to set the parameters of the zoom focus adjustment function

Feature	Description
Zoom	Adjusts the focal length of thens to minimize or enlarge parts of the image via the following steps: 1、Set the “Zoom Step”. This is the step size used to measure the size of the magnification amplitude of 1 click, the larger the step size the greater the zoom effect from a single click. 2、Click “+/-“ or drag the slider to adjust the zoom
Focus	Adjusts the optical back focus of the lense to improve the clarity of the video/picture and makes the image clearer 1、Set the “Focus Step”. This is the step size used to measure the size of the adjustment amplitude of 1 click, the larger the step size the greater the focus adjustment from a single click. 2、Click “+/-”or drag the slider to adjust the focus
Auto focus	Automatically adjusts the sharpness of the lens image
Reset All	If, even after repeating the zoom or focus functions multiple times, the image remains unclear, click “Reset All” to eliminate the cumulative adjustment errors from the lens.

Refresh	Tap “Refresh” to get the latest focus status of the device.

6 Playback

This section introduces the video playback feature of the device. Click “Playback” to enter the video playback interface; it supports query, playback and the.download of the video files which are stored in the SD card of the camera.

6.1 Playback Feature

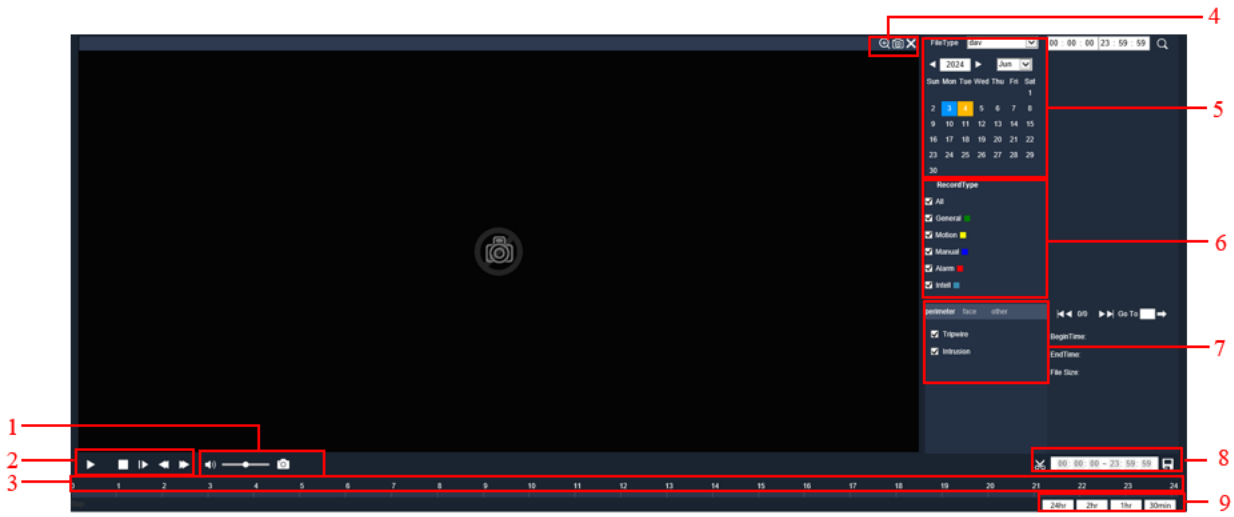
Stores queries and playbacks of the video files in the SD card, including video playback and image playback.

Preconditon

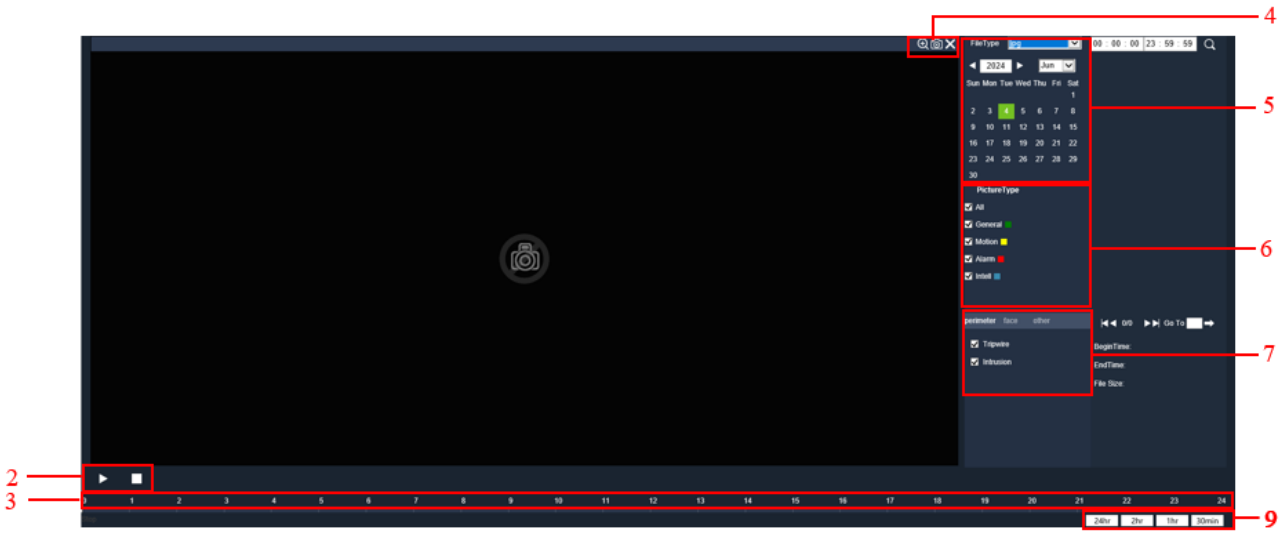
Before playing the playback recordings and images, make sure that the SD card is inserted into the devices and that the recording schedule, capture schedule and storage settings are set.

6.1.1 Introduction of the Playback Interface

Select “Playback” to display the “Playback” interface, which has slight variations for the video and image playback pages. The video playback is shown in the figure below.



The image playback is shown in the figure below.



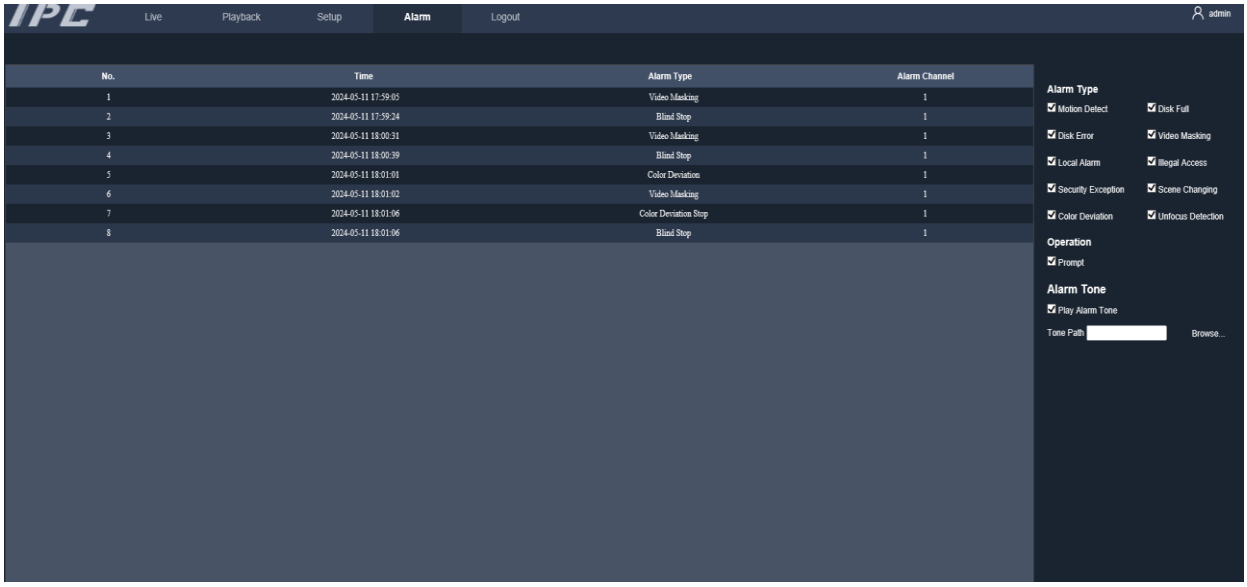
The following table describes the layout of the playback page

Number	Feature	Description
1	Sound/Snapshot	: Controls the volume during playback. : Takes a snap of the current image in the playback.
2	Playback Controls	Controls the playback of the video or image file : Pause or play the recording : Stops the recording : Skips to the next frame playback : Slows down the playback : Speeds up the playback
3	Progress Bar	Displays the type of recording and the time of period it was recorded. Click a point in the colored area to start the playback from that period of time Different types of videos are represented by different colors, thus please refer to the video type selection bar for the corresponding relationship.
4	Accessibility	: Click to zoom in on the selected area of the screen to view specific points that could be too small. The preview interface

		supports two types of zoom operations: Method 1: Click on the icon, select the area to be in enlarged on the Preview screen, then right-click to restore to its original state. Method 2: Click the icon and scroll the mouse wheel to zoom in and out of the video screen.  : Click this icon to capture an image and save it in a set storage path.  : Click the icon to close the video
5	Playback Files	This allows you to selectthe file type, data source, recording date and downloaded file.
6	Record/Capture Type	Select the type of recording or capture to view. Recording types include Normal, Dynamic, Alarm, Manual and Smart. Capture types include Normal, Dynamic, Alarm and Smart.
7	Smart Type	Smart Recording/capture type can be selected including the Perimeter, Face and others; types vary from model to model.
8	Video Clips	Takes a screenshot and saves it
9	Progress Bar Timeline	There are 4 types in total. The entire progress bar is 24 hours.

7 Alarm

The alarm module is mainly used by customers to subcribe to alarm events; when an alarm event that the user has subscribed to is triggered, the system records the alarm information on the left window bar. Different series of products vary in functions, therefore please refer to the actual product. The interface is showm in the following figure.



The following table describes the parameters on the Alarm page.

Category	Parameter	Parameter Description
Alarm Type	Motion Detection	When enabled, an alarm is generated if a moving target is detected on the video screen
	Disk Full	When enabled, an alarm is generated if the remaining space on SD card of the device is less than the set value.
	Disk Error	When enabled, an alarm is generated when the device SD card is faulty.
	Video Masking	When enabled, an alarm is generated when the video is blocked.
	Local Alarm	When enabled, an alarm is generated when there is an external alarm input.
	Illegal Access	When enabled, an alarm is generated if the log in password is continuously incorrect and the number of incorrect entries has exceeded the limit.

	Security Exception	When enabled, an alarm is generated if the number of connections exceeds the set limit.
	Scene Changing	When enabled, an alarm is generated if the monitoring scene changes.
	Color Deviation	When enabled, an alarm will be generated if the video image is biased.
	Unfocus Detection	When enabled, an alarm is generated if the video screen goes out of focus.
Operation	Prompt	When enabled, the system prompts and records alarm information based on the event. • When a subscribed alarm event is triggered and the system is not on the “Alarm”page, the Alarm information is automatically recorded on the “Alarm” tab  page. • When a subscribed alarm event is triggered and the system is displayed on the “Alerts” page, the alarm list on the right side of the alert page displays the corresponding alarm information.
Alarm Tone	Play Alarm Tone	When “Play Alarm Tone” is enabled, the system will play the selected sound finle to prompt that an alarm has been triggered if a subscribed alarm event is triggered.
	Tone Path	Customizes the alarm sound storage path.