Video Doorbell
User Manual

O2DB1

Please read this manual carefully before operating the unit and keep it for further reference

Important Safeguards and Warnings

1. Electrical safety

All installation and operation here should conform to local electrical safety codes.
Use a certified/listed 12VDC Class2 power supply only.
Please note: Do not connect two power-supplying sources to the device at the same time; it may result in device damage! The product must be grounded to reduce the risk of electric shock.
Improper handling and/or installation could run the risk of fire or electrical shock.

2. Environment

Do not expose the unit to heavy stress, violent vibration, or long-term exposure to water and humidity during transportation, storage, and/or installation.
Do not install near sources of heat.
Only install the product in environments inside the specification operating temperature and humidity range.
Do not install the camera near power lines, radar equipment, or other electromagnetic radiation.
Do not block any ventilation openings if any.
Use all the weatherproofing hardware requirements to minimize weather intrusion.

3. Operation and Daily Maintenance

Please shut down the device and then unplug the power cable before you begin any maintenance work.
Do not touch the CMOS sensor optic component. You can use a blower to clean the dust on the lens surface.
Always use a dry soft cloth to clean the device. If there is too much dust, use a cloth dampened with a small quantity of neutral detergent. Finally, use a dry cloth to clean the device.
Please use a professional optical cleaning method to clean the enclosure. Improper enclosure cleaning (such as using cloth) may result in poor IR functionality and/or IR reflection.
The grounding holes of the product are recommended to be grounded to further enhance the reliability of the camera.
The dome cover is an optical device, please do not touch or wipe the cover surface directly during installation and use, please refer to the following methods if dirt is found.
Stained with dirt:
Use an oil-free soft brush or hair dryer to remove it gently.
Stained with grease or fingerprint.
Use oil-free cotton cloth or paper soaked with alcohol or detergent to wipe from the lens center outward. Change the cloth and wipe it several times if it is not clean enough.

Warning

This camera should be installed by qualified personnel only.
All the examination and repair work should be done by qualified personnel.
Any unauthorized changes or modifications could void the warranty.

Statement

This guide is for reference only.
Product, manuals, and specifications may be modified without prior notice. Speco Technologies reserves the right to modify these without notice and without incurring any obligation.
Speco Technologies is not liable for any loss caused by improper operation.

Regulatory Information

FCC conditions:

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

FCC compliance:

This equipment has been tested and found to comply with the limits for a digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Note:

Before installation, check the package and make sure that all components are included.
Contact your rep or Speco customer service department immediately if something is broken or missing in the package.

Accessory name	Amount
Network Camera Unit	1
Junction box	1
Quick Start Guide	1
Installation Accessories Bag	1
CD	1

Table of Contents

1 Introduction

Welcome

Thank you for purchasing this network camera!
Please read this manual carefully before operating the unit and retain it for further reference.
Should you require any technical assistance, please get in touch with Speco Technologies Technical Support at 1-800-645-5516.

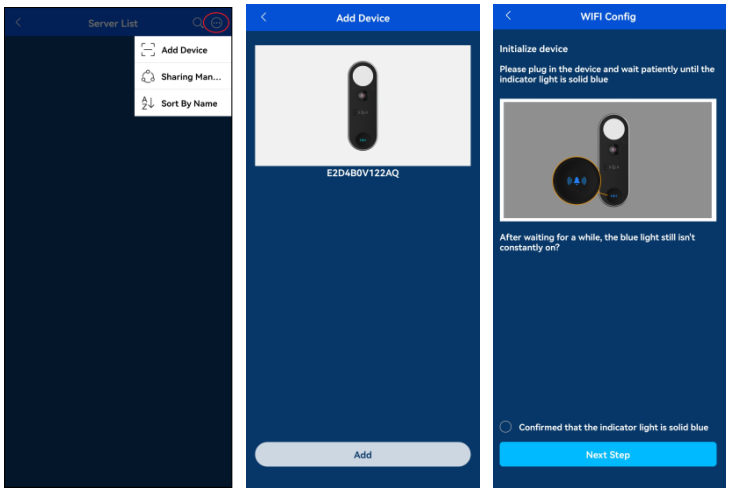
Main Features

- Visual intercom function: two-way remote communication between the doorbell and mobile APP
- 2.4G Wi-Fi
- Access control function
- Wide field of view achieving doorway security monitoring

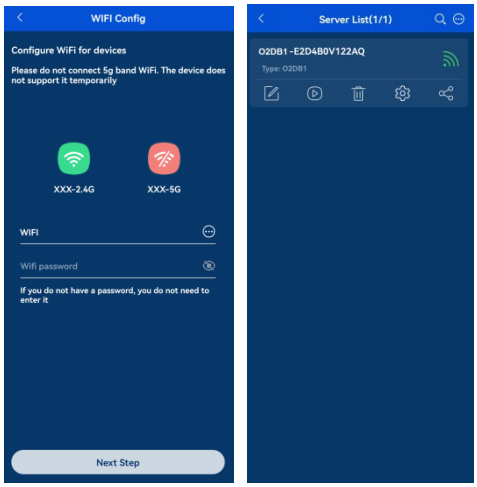
2 Network Connection & Login

2.1 APP Connection

1. Enable Wi-Fi network of your phone. Then scan the QR Code of the Speco Blue APP in the QSG (Quick Start Guide). Then install the mobile APP in your phone.
2. Run the mobile APP and then log in your account of the APP (if you don't register, please register and log in first). Then enter the server list interface of the APP.
3. Power on your video doorbell. Then tap "Add Device" in the server list interface of the APP. Scan the QR Code attached on the back of the video doorbell or the QR Code of the video doorbell in the QSG. After that, go to the Wi-Fi configuration interface by tapping "Add". When the indicator of the doorbell is blue, check "Confirmed that…" and tap "Next Step".



4. Enter the key (or password) of the Wi-Fi network. Tap "Next Step". Then join the Wi-Fi network by tapping "Join" .
After that, the doorbell will be automatically added to the server list.



Note: 1. When configuring the Wi-Fi network via the APP, (a). **DO NOT** connect the network cable to the Ethernet connector of the device; (b). your mobile phone must be connected to the Wi-Fi network; (c). the doorbell must be within the mobile phone signal covering area. **DO NOT** move your phone too far away with the doorbell.

2. After the Wi-Fi of the doorbell is successfully connected, you can use Wi-Fi or mobile web in your mobile phone as needed. However, if you want to remotely view the doorbell video via mobile web, please make sure the wireless router/AP connected the doorbell has been connected to the Ethernet.

2.2 Wired Network Connection

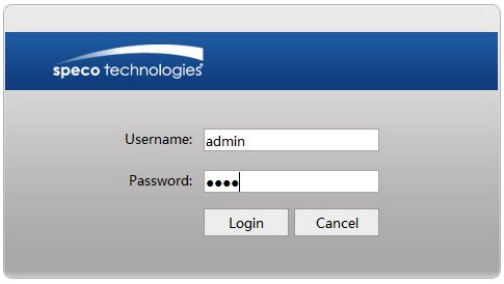
Here we take device access via Web browser for example.
Web browser: IE (plug-in required)/ Firefox/Edge/Safari/Google Chrome
It is recommended to use the latest version of these web browsers.
The menu display and operation of the camera may be slightly different by using the browser with plug-in or without plug-in. Installing a plug-in will display more functions of the camera.
Connect IP-Cam via LAN or WAN. Here only take IE browser for example. The details are as follows:

- Access through IP Scanner

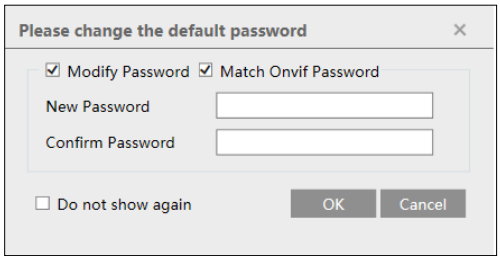
Network connection:

① Make sure the PC and IP-Cam are connected on the same local network. The camera is set to DHCP by default and will be assigned an IP address by the DHCP server. Make sure that the local network has a DHCP server. Routers typically have a DHCP server built in.
② Install Speco Blue Scanner and run it after installation. Speco Blue Scanner is the tool for discovering the IP cameras on the local network. It can be downloaded from www.specotech.com.

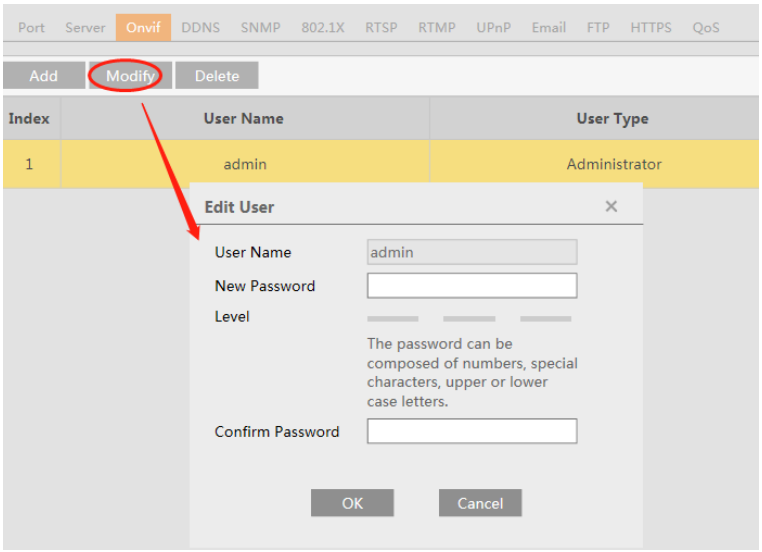
③ In the device list, the IP address, model number, and MAC address of each device will be listed. Select the applicable device and double-click to open up the web viewer. You can also manually enter the IP address in the address bar of the web browser.



The login interface is shown above. The default username is **admin** and the password is **1234**. After logging in, follow directions to install applicable plug-ins for viewing video if prompted.



If this is the first time for you to log in, the password prompt may only change the admin password. By default, the ONVIF password will match the admin password that you set. Should you wish to change the ONVIF password to a different password than your admin password, go to the ONVIF section to change the password. (Config→Network→Ports/Connections→Onvif)



After that, you can add your device to the APP. The steps are as follows:

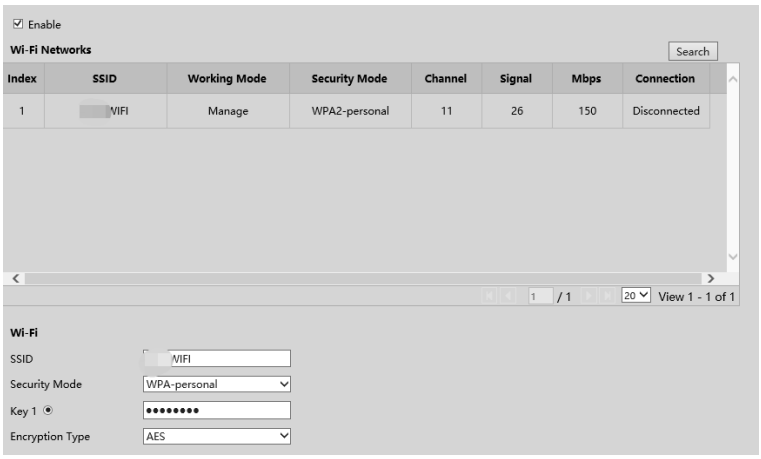
1) Scan the QR Code of the APP in the QSG (Quick Start Guide) or open your phone's APP store. Then install the mobile APP (Speco Blue) on your phone.
2) Run the mobile APP and then log in to your account of the APP (if you don't register, please register and log in first). Then enter the server list interface of the APP.
3) Tap "Add Device" in the server list interface of the APP. Scan the QR Code (log in via web and then go to Config→ Basic Information interface) to directly add the device to the server list of the APP.

- Wi-Fi Connection

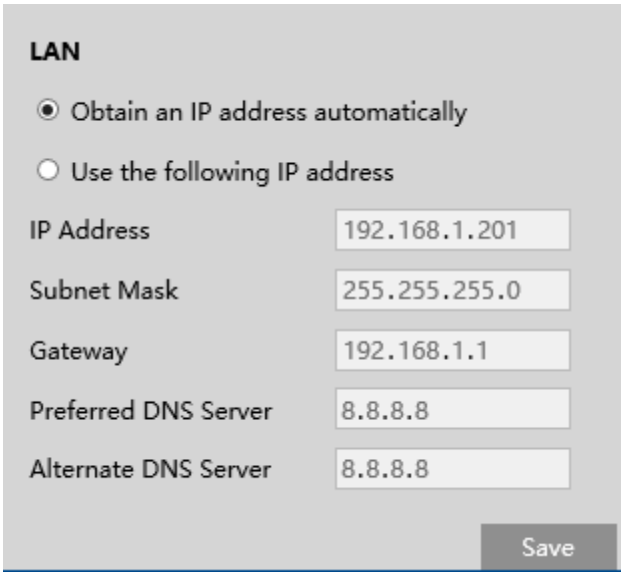
① Use the network cable to connect the device and wireless router or AP.

② Connect to the above wireless network with your PC. Then run the IP Scanner on your PC, select the applicable device, and double-click to open the web viewer. This will bring you to the login interface of the camera. Enter the default username and password to log in.

③ Click Config→Network→Ports/Connections→WIFI to go to the following interface. Enable WIFI, select the desired router, enter the key, and select encryption type.



After that, select "Obtain an IP address automatically" or manually enter the IP address by clicking "Use the following IP address". Then click "Save" to save the settings.

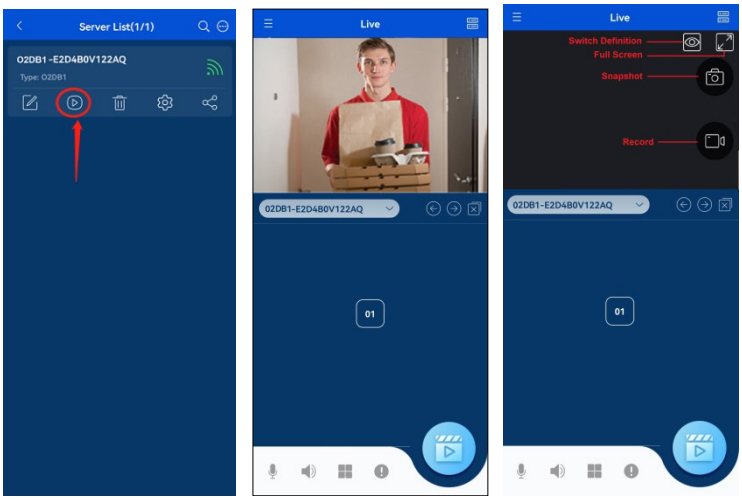


④ Pull the network cable out of the camera.
⑤ Run the IP-Tool and find the camera through IP address or MAC address. Then double click it listed in the IP-Tool or enter the IP address of the camera in the address bar of the web browser to access the camera.
After that, you can also use the downloaded APP to scan the QR code of the device to directly add it to the server list of the APP.

3 Configuration via APP

3.1 Live View via APP

After the device is added to the APP, tap  in the server list interface to view the video.

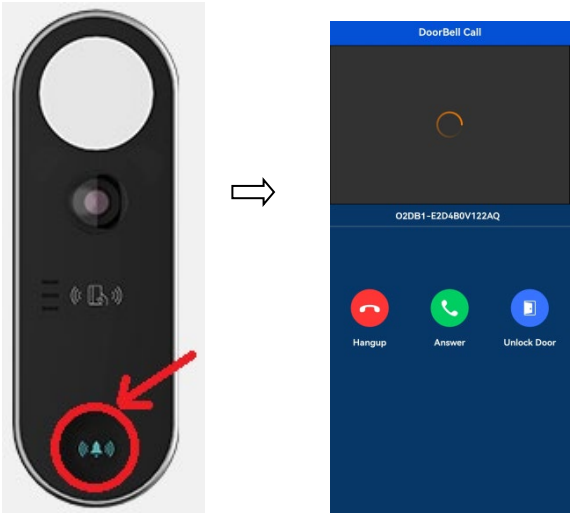


Tap the video and then multiple icons will be displayed. You can do the above-mentioned operations as needed (like taking a snapshot, recording, and switching definition).

Note: You can add the device to the APP by directly scanning the QR Code of the device, or connect the device to the Ethernet via the wired/wireless network connection first and then scan the QR Code of the device to add it via the APP.

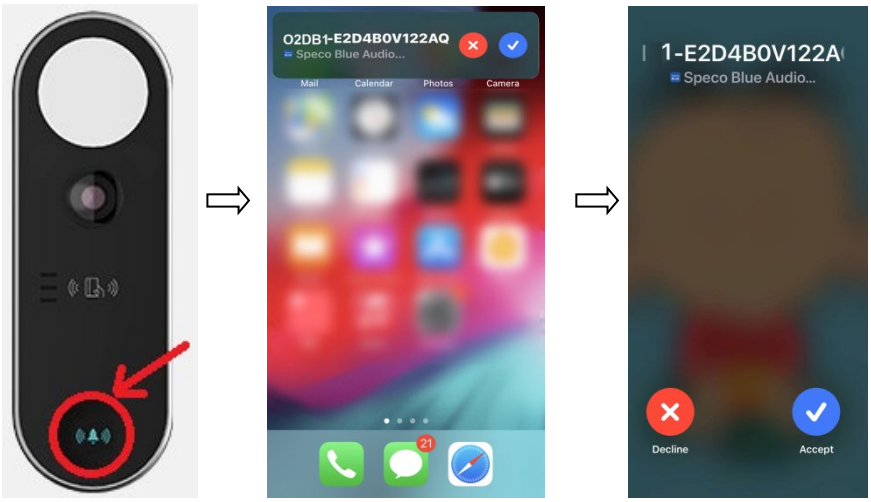
3.2 Receive/Reject a Call or Open the Door via APP

You can receive or reject a call when the APP window is opened or closed.
1. When the APP is opened,



Press the Call button on the doorbell, and then a calling interface will be shown in the APP. Now, you can answer or hang up the call or choose to remotely open the door as needed.

2. When the APP is closed,

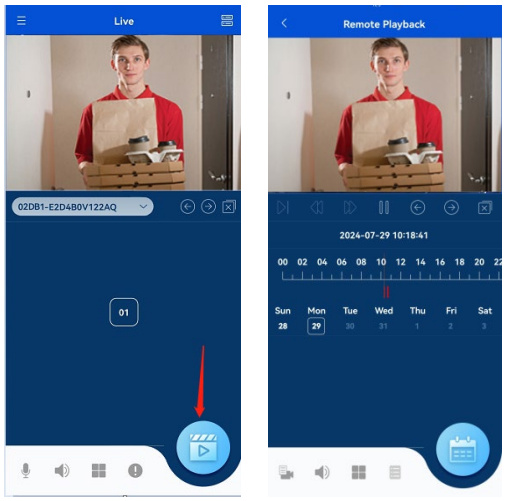


Press the Call button on the doorbell, then a message will appear on the top of the home page. Tap this message within 60s to enter the calling interface.

Note: You must enable the notification function of the APP on your phone first, or no message will be received.

3.3 Remote Playback via APP

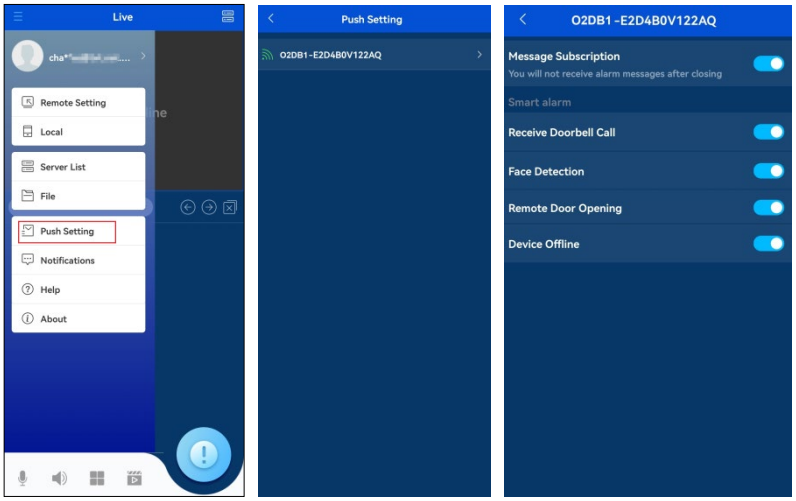
You can remotely play back the recorded files stored on the SD card via the APP. In the live view interface of the APP, select the video doorbell channel and then tap to remotely play back the video. You can select the playback time on the timescale.



In the remote playback interface, tap to select the detailed date and time as needed.

3.4 Disable Push Notifications via APP

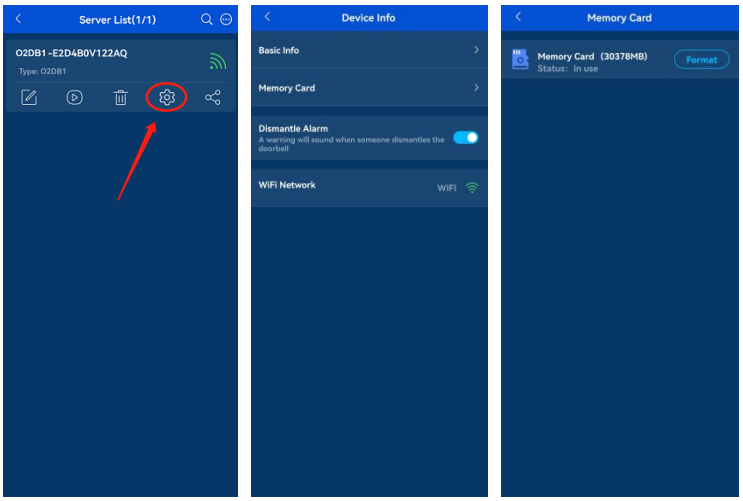
If you don’t want to receive the doorbell information, you can disable the relevant push notifications via APP.



Tap ***Main Menu→Push Setting***. Select the doorbell channel name to enter. Disabling "Message Subscription" will turn off all intelligent alarm notifications of the device. You can also disable one more item listed on the interface as needed.

3.5 Device Settings via APP

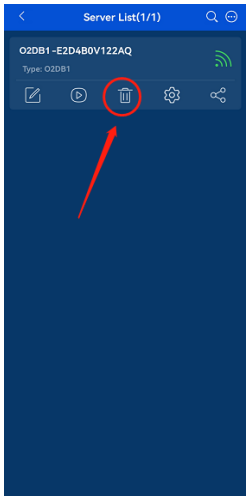
In the server list interface, tap  under the doorbell name. This will take you to the device information interface as shown below.



On the device information page, you can view basic information, SD card information, and Wi-Fi information about the device. There is also an option to enable or disable the "Dismantle Alarm" (Tampering alarm).
Note: If your SD card has been used in other devices before it is inserted in this device, you need to format it first.

3.6 Unbind the Doorbell from the APP

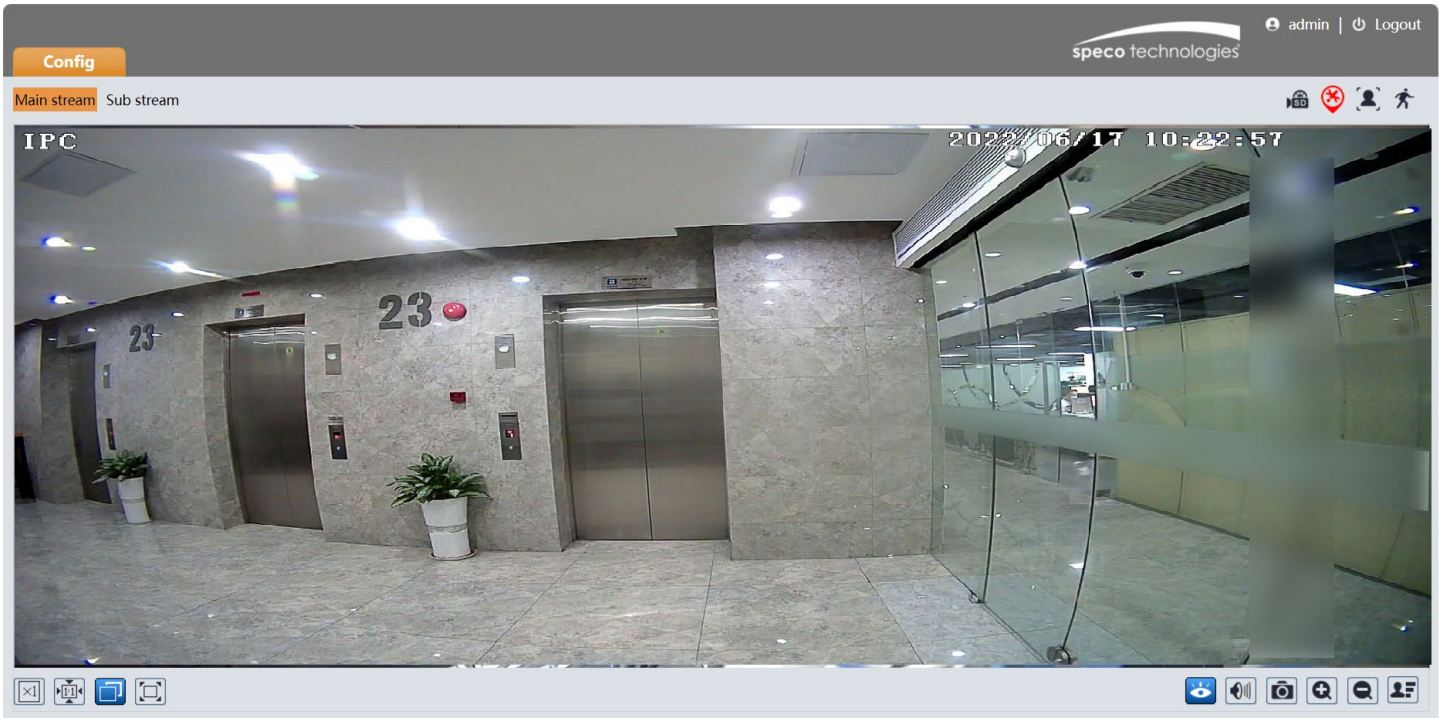
In the server list interface of the APP, tap  under the video doorbell name to unbind it.



Note that the device also can be unbound from the APP via Web (Config→System→Basic Information).

4 Live View via Web

The window below will be shown after logging in.



The following table describes the icons on the live view interface

Icon	Description	Icon	Description
	Original size of resolution		Zoom out (for motorized models)
	Fit (correct scale)		SD card recording indicator
	Auto (fill the window)		Abnormal color indicator
	Full screen (show video only)		Abnormal clarity indicator
	Start/stop live view		Scene change indicator
	Start/stop two-way audio		Tampering alarm indicator
	Enable/disable audio		Alarm input indicator
	Snapshot		Face detection indicator
	Start/stop local recording		Face Detection
	Zoom in (for motorized models)		

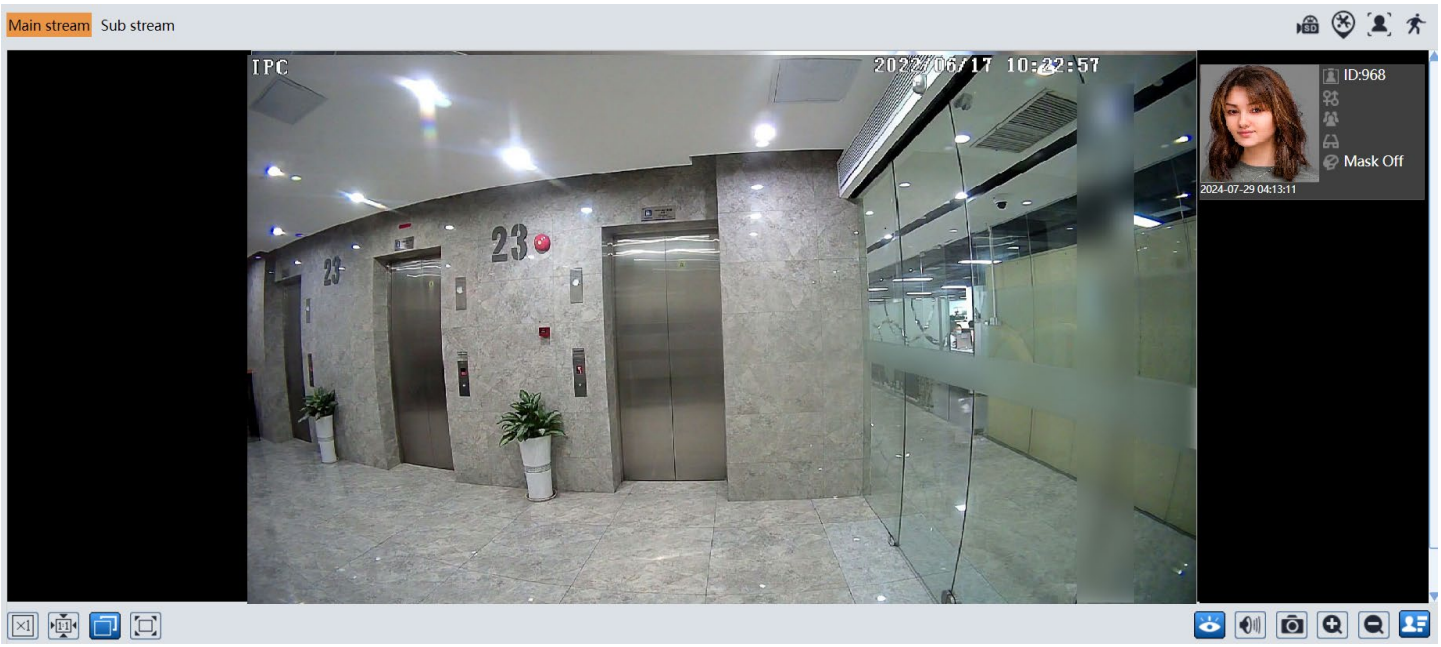
*Plug-in free live view: Two-way audio and local recording are not supported.

- All indicator icons above will flash in the live view interface only when the corresponding events are enabled.
- In full-screen mode, to exit, double-click on the mouse or press the ESC key on the keyboard.

Face Capture View

① Go to Config→Event→Face Detection interface. Check “Enable”.

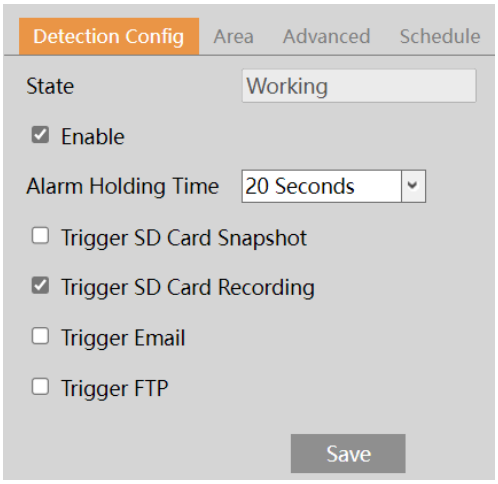
② Return to the live view interface. Click  to go to the following interface. When faces are detected, the images will appear on the right



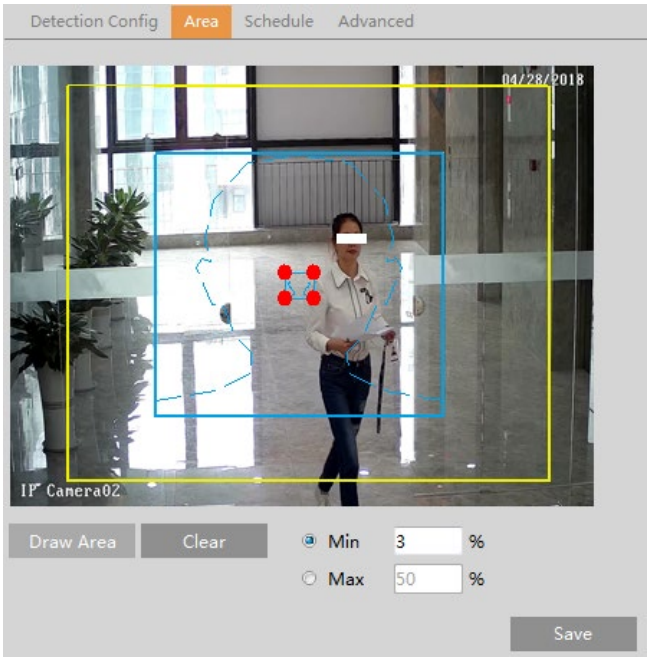
Press the “Setup” button to go to the configuration interface.
Note: Wherever applicable, click the “Save” button to save the settings.

5.1 Face Detection

The face detection feature identifies faces in the surveillance scene and triggers alarms when a face is detected.
The setting steps are as follows:
1. Go to Event→Face Detection as shown below.



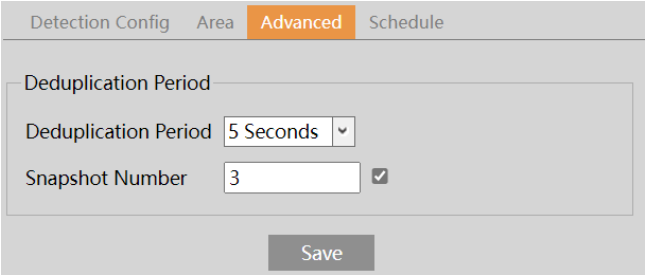
2. Enable the face detection function.
3. Set alarm holding time and alarm trigger options. The alarm trigger setup steps are the same as motion detection setup. Please refer to the motion detection section for details.
4. Set alarm detection area.



Use this to draw the approximate size of the face that you want the camera to capture. This is useful when multiple faces in the

background or foreground do not need to be captured. To enable, click “Draw Area” and drag the border lines of the rectangle to modify its size. Move the rectangle to change its position. Click “Stop Draw” to stop drawing the area. Click “Clear” to clear the area. Then set the detectable face size by defining the maximum value and the minimum value (The default size range of a single face image occupies from 3% to 50% of the entire image).

5. Advanced configuration. Choose the snapshot interval and number as needed to avoid capturing multiple similar pictures in a very short time.



Snapshot Interval: If 5 seconds is selected, the camera will capture the same target once every 5 seconds during its continuous tracking period.

Snapshot Number: If the snapshot number is enabled and set (eg. 3), the camera will capture the same target once every 5 seconds and it will capture this target 3 times at most during its continuous tracking period. If the snapshot number is disabled, the camera will capture the same target once every 5 seconds until the target disappears in the detected area.

6. Set the schedule of the face detection. The setup steps of the schedule are the same as the schedule recording setup (See Schedule Recording).

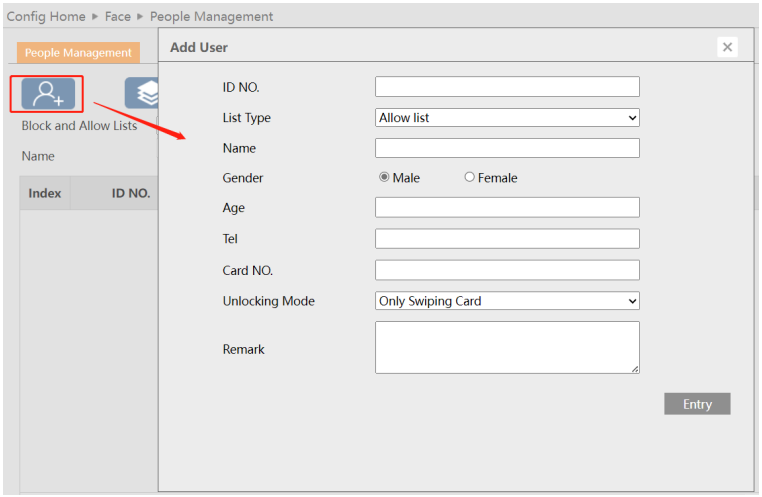
5.2 People Management

Please log in to the video doorbell via Web client and then Click the “Config”→“People Management” tab.

There are two ways to add personnel information.

① Adding personal information one by one

Click  to display an adding user box. After that, fill out the relevant information and click “Entry” to add.



List type: it includes allow list, visitor, and block list.

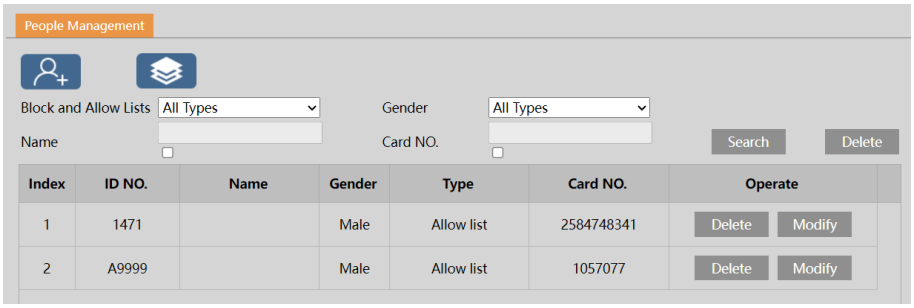
Note: Please swipe the card on the device when adding the user information and then the ID number will be automatically filled in.

② Adding the information of many people at a time

Click  and then add the information of many people once according to the prompted rules.

Click “Browse” to select the directory and then click “Start” to upload.

After the personal information is added, you can search them by name, gender, ID number and so on.

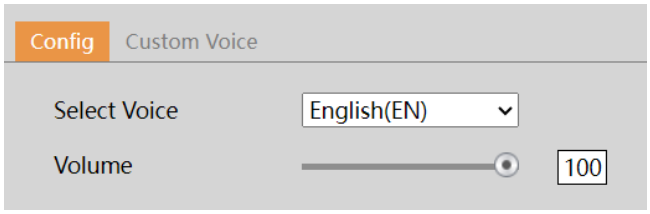


Click “Modify” to change people's information and click “Delete” to delete the personal information.

Note: Face pictures are not supported in the face database.

5.3 Access Control System Settings

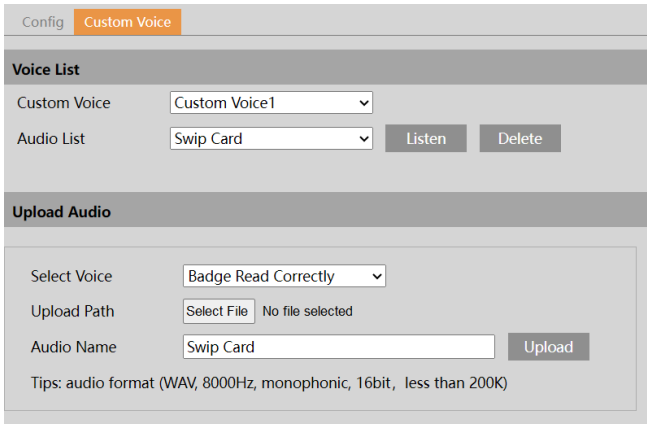
Click Config→Access Control→Access Control System Settings to go to the following interface.



Select Voice: Select the language of the voice prompt.
Volume: Set the volume of the voice prompt.

- **Customizing Voice**

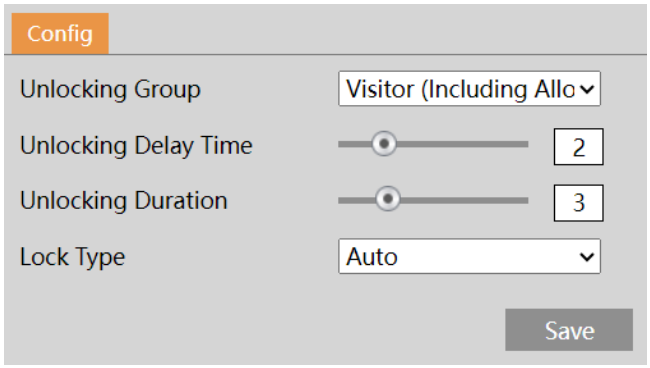
If you are dissatisfied with the default voice prompt, you can customize your own voice prompt. In the above interface, click “Custom Voice” tab to go to the following interface.



Select the voice you want to replace and then click “Select File” to select the desired audio file. After that, click “Upload” to upload the audio file. Rename the audio as needed.
After your own voice prompt is uploaded, you can select it from the audio list and click “Listen” to listen to your voice prompt.

5.4 Door Lock Settings

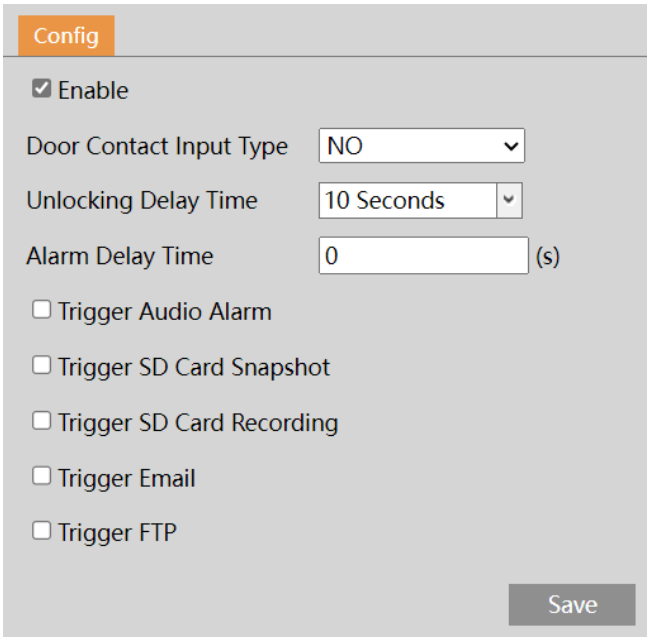
Click Config→Access Control→Door Lock to go to the following interface. After the access control device is connected to the device, you can set unlocking mode in this interface.



Unlocking Group: Allow list, visitor (including allow list), stranger (including visitor and allow list).
Unlocking Delay Time: Set the door unlocking delay time. The time range is from 0 to 10 seconds. For example, the unlocking mode is "Swiping Card" and the delay time is set to "2" seconds; the door will be opened 2 seconds later after successfully reading card.
Unlocking Duration: If the door has been unlocked for a period that exceeds the unlocking duration, the door will be automatically locked. The time range is from 0 to 10 seconds. For example, the duration is set to "3" seconds; the unlocking door will be automatically locked 3 seconds later.
Lock Type: Choose "Auto", "NO" or "NC" as needed. If "Auto" is selected, the system will open the door according to the pre-defined unlocking condition. "NO" means "normally open"; "NC" means "normally closed".

5.5 Door Contact Settings

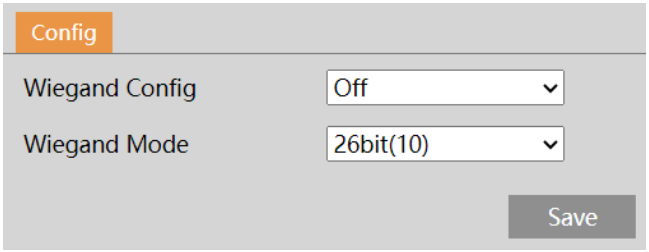
Click Config→Access Control→Door Contact Setting to go to the following interface.



Door Contact Input Type: NO or NC
Unlocking Delay Time: the allowable unlocking time. For example, if it is set to 10 seconds, alarms will be triggered when the door is not closed after 10 seconds.
Alarm Delay Time: set the alarm delay time when faults of the door contact are detected. For example, if it is set to 3s when detecting the failure of the door contact, alarms will be triggered 3s later. (The value ranges from 0~999. If "0" is selected, it means that alarms will be triggered immediately.)
Please select the alarm trigger options as needed.
Trigger Audio Alarm: if enabled, you will hear the warning sound when the door contact alarm is triggered.
The setup steps of other alarm trigger options are similar to the motion detection settings. Please refer to the motion detection settings section for details.

5.6 Wiegand Settings

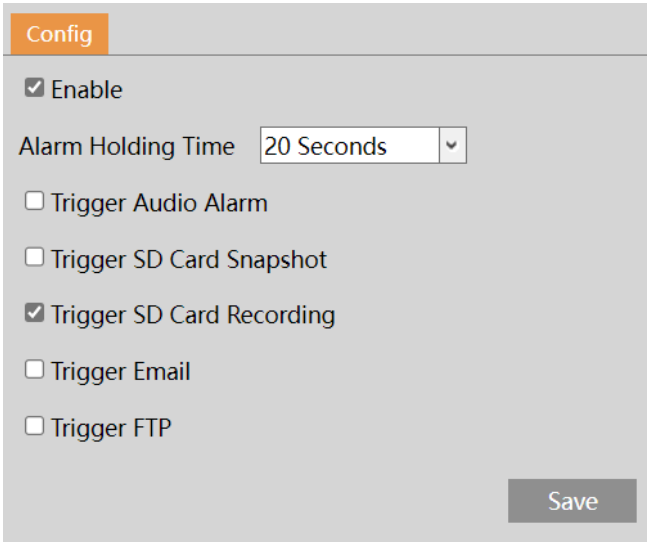
Click Config→Access Control→Wiegand Config to go to the following interface.



Wiegand Config: Wiegand Input, Wiegand Output or Off can be selected. If the card reader is connected to the Wiegand interface, please select "Wiegand Input". If the access controller is connected to the Wiegand interface, please select "Wiegand Output".
Wiegand Mode: 26bit (8), 26bit(10), 34bit, 37bit, 42bit, 46bit, 58bit or 66bit can be selectable.

5.7 Tampering Alarm Settings

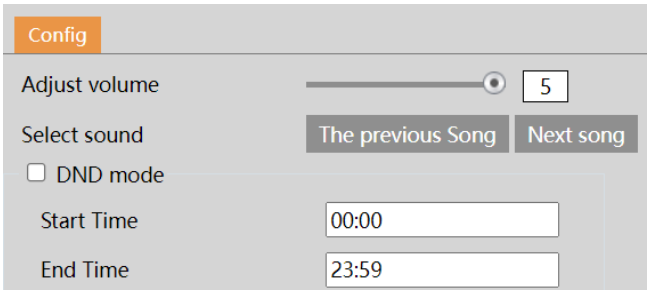
In order to avoid the removal or damage by the external force, the tampering alarm can be set for the terminal. Click Config→Access Control→Tampering Alarm Setting to go to the following interface.



Enable "Tampering Alarm" and then set the alarm holding time and alarm trigger options.
Trigger Audio Alarm: if enabled, you will hear the warning sound when the doorbell is removed or damaged by an external force.
The setup steps of other alarm trigger options are like the motion detection settings. Please refer to the motion detection settings section for details.

5.8 Chime Configuration

If your doorbell is paired with a Chime, you can set the relevant parameters of the Chime.
Go *to* Config→Ring Device Configuration interface.

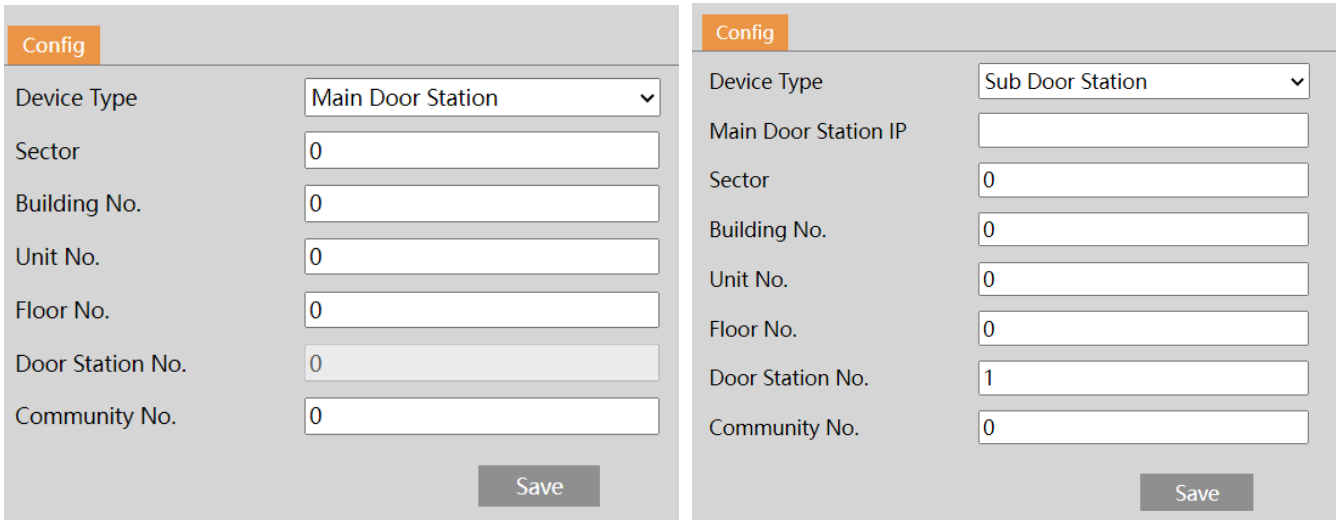


Volume: Select the volume of the chime.
Select sound: Select the ringtone of the chime.
DND mode: Do Not Disturb mode. If enabled, the chime will not ring during the set time.

5.9 Intercom Configuration

5.9.1 Door Station Settings

Go to Config→Intercom interface as shown below. Configure door station information, such as sector no., building no., floor no, etc.

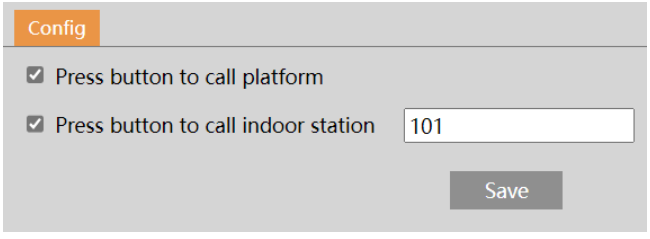


Device Type: main door station or sub door station.

Note: 1. The number of the main door station is 0; the number of the sub door station is from 1 to 99. The same number is not allowed to enter for different sub-door stations.
2. Each unit should install 1 main door station. A maximum of 9 sub-door stations can be linked to the main door station.
3. The sector no., building no., unit no., and community no. of the door station must be the same as the main door station.

5.9.2 Call Platform

Press the Call button to call the platform. Please enable this function before using this button. Go to Config→Intercom→One-button Calling interface. Check “Press button to call platform” and then save.



Note: Please add the door station to the platform before calling.

5.9.3 Call Resident

Press the Call button to directly call the resident. Please set the room number in advance before using this button. Go to Config→Intercom→One-button Calling interface. Check “Press button to call indoor station” and then enter the room number. Finally, click “Save”.

Note: Please add the door station to the indoor station before calling. Please see Appendix 1 for details.

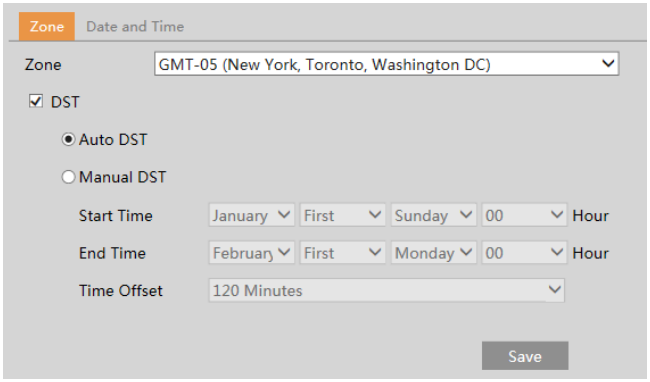
5.10 System Configuration

5.10.1 System Information

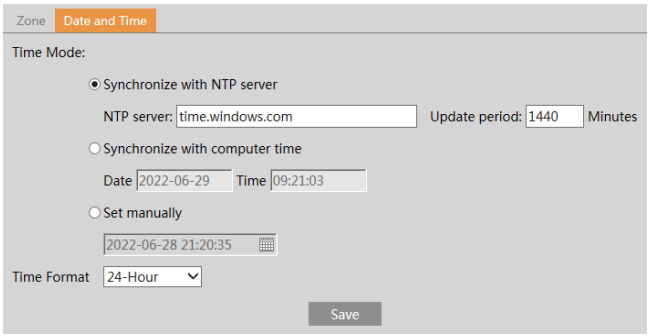
In the “System Information” interface, the system information of the device is listed, such as device name, product model, MAC, software version, etc.

5.10.2 Date and Time

To set the time and date, go to System→Date and Time. Please refer to the following interface.

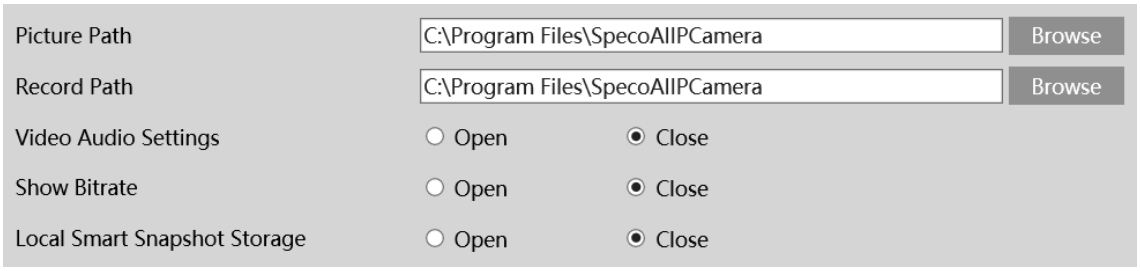


Select the applicable time zone and enable/disable DST as needed.
Click the “Date and Time” tab to set the time, date, and time format.



5.10.3 Local Recording

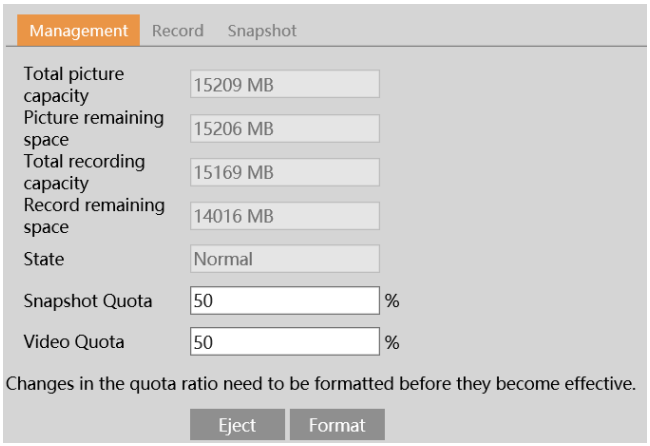
Go to System→Local Recording to set up the storage path of captured pictures and recorded videos on the local PC. There is also an option to enable or disable audio in the recorded files.



Additionally, the snapshots triggered by smart events can be selected to save to the local PC.
Note: when you access your camera by the web browser without the plug-in, only Show Bitrate can be set in the above interface.

5.10.4 Storage

Go to System→Storage to go to the interface as shown below.

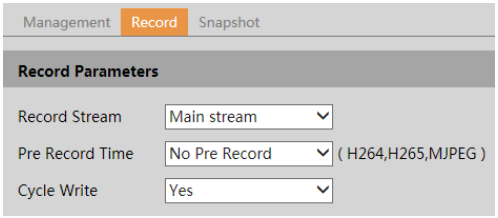


- **SD Card Management**

When the card is used for the first time, click the "Format" button to format the SD card. **All data on the card will be cleared by clicking this button.**
Click the "Eject" button to stop writing data to the SD card. Then the SD card can be ejected safely.
Snapshot Quota: Set the capacity proportion of captured pictures on the SD card.
Video Quota: Set the capacity proportion of record files on the SD card.

- **Schedule Recording Settings**

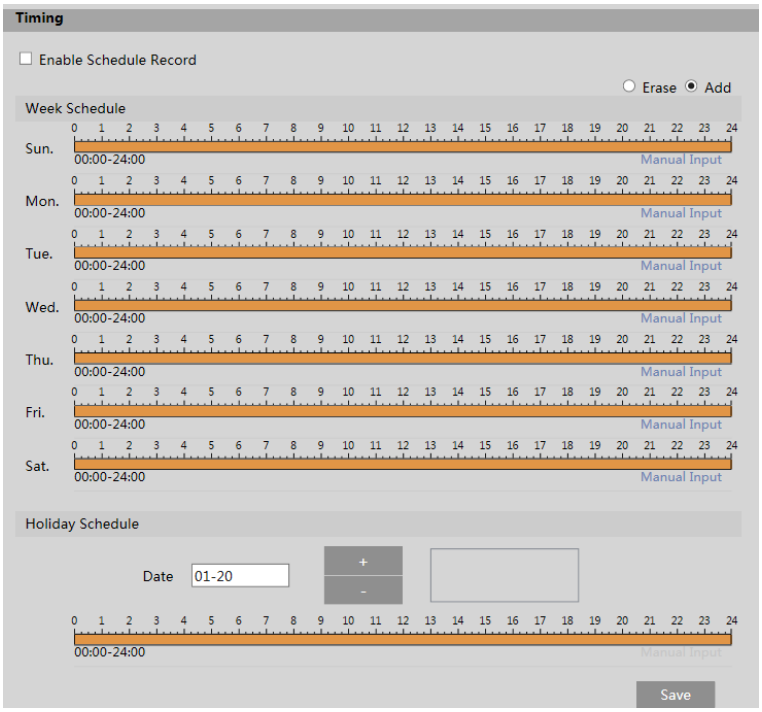
1. Go to Storage→Record to go to the interface as shown below.



2. Set record stream, pre-record time, and cycle writing.

Pre-Record Time: Set the time to record before the actual recording begins.

3. Set schedule recording. Check "Enable Schedule Record" and set the schedule.



Weekly Schedule

Set the alarm time from Monday to Sunday for a single week. Each day is divided in one-hour increments. Green means scheduled. Blank means unscheduled.

"Add": Add the schedule for a special day. Drag the mouse to set the time on the timeline.

"Erase": Delete the schedule. Drag the mouse to erase the time on the timeline.

Manual Input: Click it for a specific day to enter specific start and end times. This adds more granularities (minutes).

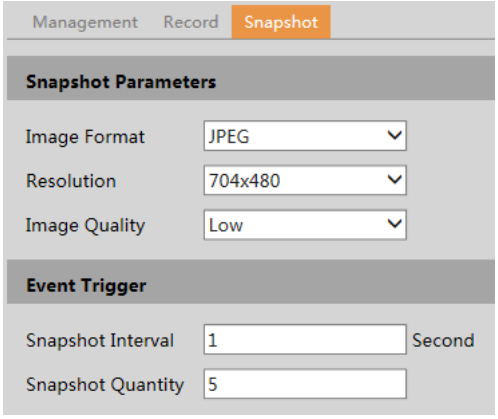
Day schedule

Set the alarm time for a special day, such as a holiday.

Note: Holiday schedule takes priority over weekly schedule.

- **Snapshot Settings**

Go to System→Storage→Snapshot to go to the interface as shown below.



Set the format, resolution, and quality of the image saved on the SD card and the snapshot interval and quantity and the timing snapshot here.

Snapshot Quantity: The number you set here is the maximum quantity of snapshots. The actual quantity of snapshots may be less than this number. Supposing the occurrence time of an alarm event is less than the time of capturing pictures, the actual quantity of snapshots is less than the set quantity of snapshots.

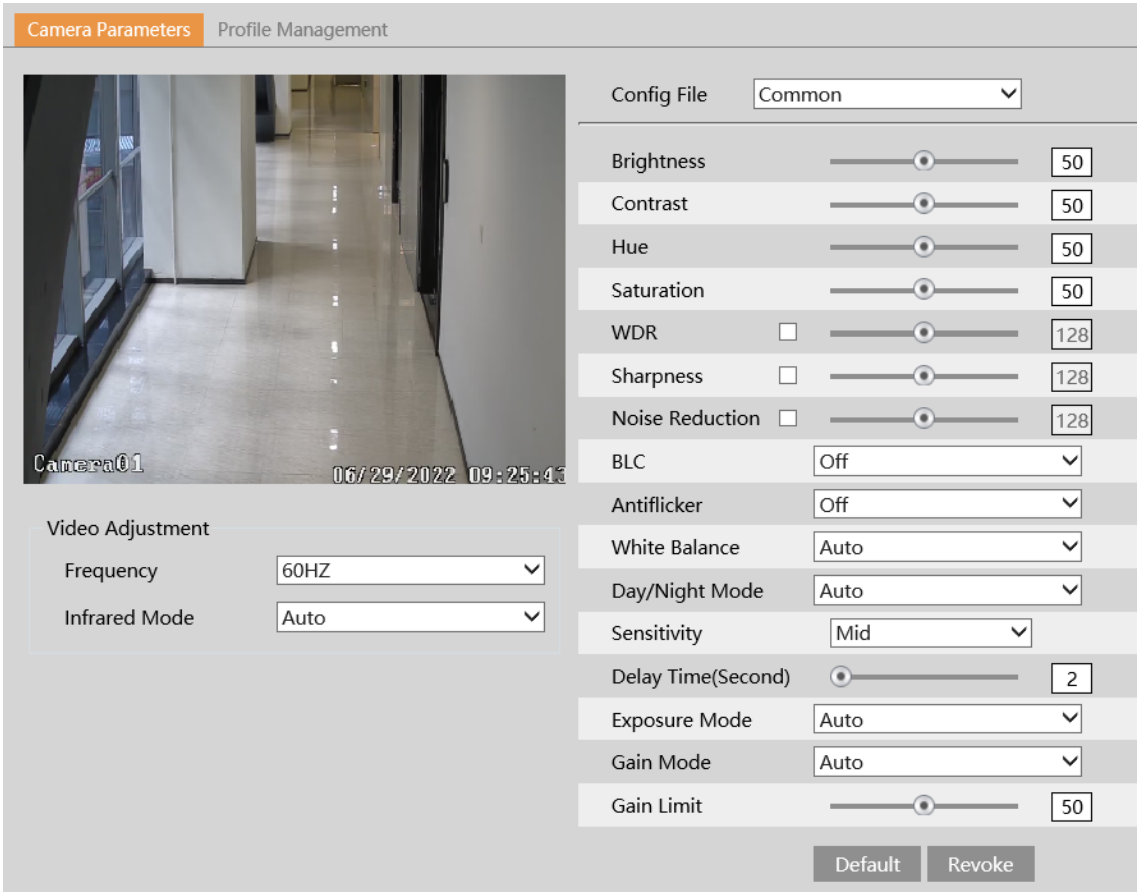
Timing Snapshot: Enable timing snapshot first and then set the snapshot interval and schedule. The setup steps of schedule are the

same as the schedule recording (See Schedule Recording).

5.11 Video Configuration

5.11.1 Image Configuration

In the Image Settings interface as shown below, various settings can be adjusted, such as brightness, contrast, hue, and saturation and so on. The common mode and day and night mode can be set up separately. The image effect can be quickly viewed by switching the configuration file.



Brightness: Set the brightness level of the camera's image.
Contrast: Set the color difference between the brightest and darkest parts.
Hue: Set the total color degree of the image.
Saturation: Set the degree of color purity. The purer the color, the brighter the image is.
WDR: WDR can adjust the camera to provide a better image when there are both very bright and very dark areas simultaneously in the field of view by lowering the brightness of the bright area and increasing the brightness of the dark area.
Recording will be stopped for a few seconds while the mode is changing from non-WDR to WDR mode.
Sharpness: Set the resolution level of the image plane and the sharpness level of the image edge.
Noise Reduction: Decrease the noise and make the image more thorough. Increasing the value will make the noise reduction effect better but it will reduce the image resolution.
Backlight Compensation (BLC):

- Off: disables the backlight compensation function. It is the default mode.
- HLC: lowers the brightness of the entire image by suppressing the brightness of the image's bright area and reducing the size of the halo area.
- BLC: If enabled, the auto exposure will activate according to the scene so that the object of the image in the darkest area will be seen clearly.

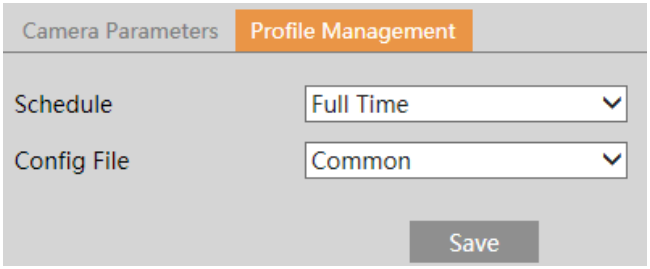
Antiflicker:

- Off: disables the anti-flicker function. This is used mostly in outdoor installations.

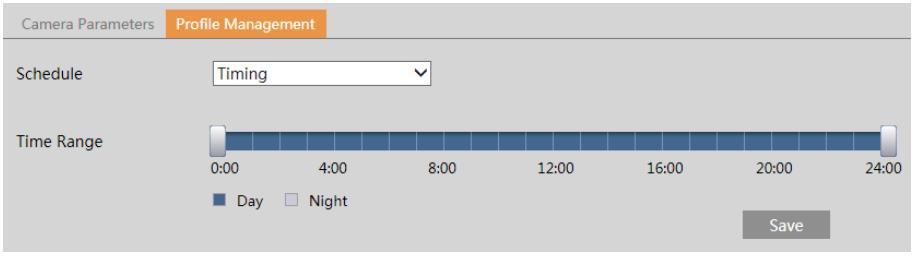
- 50Hz: reduces flicker in 50Hz lighting conditions.
- 60Hz: reduces flicker in 60Hz lighting conditions.

White Balance: Adjust the color temperature according to the environment automatically.
Day/Night Mode: Choose “Auto”, “Day”, “Night” or “Timing”.
Exposure Mode: Choose “Auto” or “Manual”. If the manual is chosen, the digital shutter speed can be adjusted.
Gain Mode: Choose “Auto” or “Manual”. If “Auto” is selected, the gain value will be automatically adjusted according to the actual situation. If “Manual” is selected, the gain value shall be set manually. The higher the value is, the brighter the image is.
Frequency: 50Hz and 60Hz can be optional.
Infrared Mode: Choose “Auto”, “ON” or “OFF”.

Schedule Settings of Image Parameters:
Click the “Profile Management” tab as shown below.



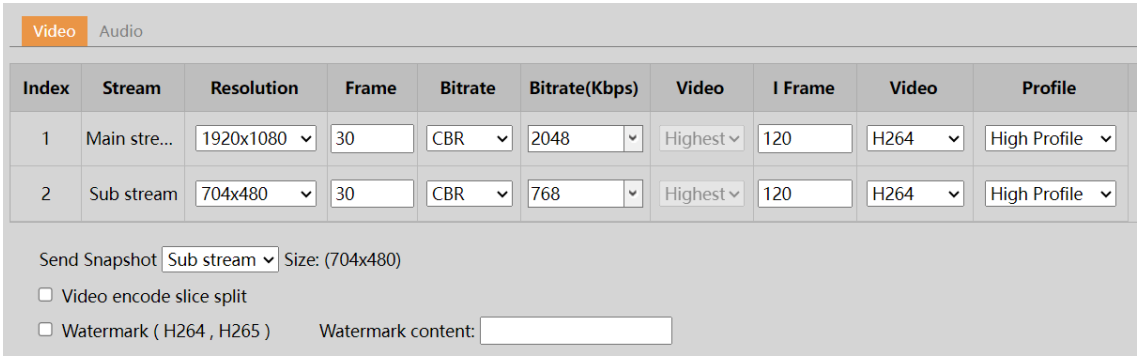
Set full schedule for common, day or night mode and specified time schedule for day and night. Choose “Timing” in the drop-down box of the schedule as shown below.



Drag “” icons to set the time of day and night. Blue means daytime and blank means night time. If the current mode of camera parameters is set to “Timing”, the image configuration mode will automatically switch between day and night according to the schedule.

5.11.2 Video / Audio Configuration

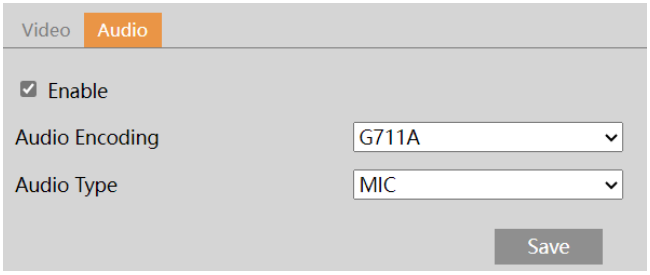
Go to Image→Video / Audio interface as shown below. In this interface, set the resolution, frame rate, bitrate type, video quality and so on subject to the actual network condition.



Two video streams can be adjustable.

Resolution: The size of the image.
Frame rate: The higher the frame rate, the video is smoother.
Bitrate type: CBR and VBR are optional. Bitrate is related to image quality. CBR means that no matter how much change is seen in the video scene, the compression bitrate will be kept constant. VBR means that the compression bitrate will be adjusted according to scene changes. For example, for scenes that do not have much movement, the bitrate will be kept at a lower value. This can help optimize the network bandwidth usage.
Bitrate: it can be adjusted when the mode is set to CBR. The higher the bitrate, the better the image quality will be.
Video Quality: It can be adjusted when the mode is set to VBR. The higher the image quality, the more bitrate will be required.
I Frame interval: It determines how many frames are allowed between a "group of pictures". When a new scene begins in a video, until that scene ends, the entire group of frames (or pictures) can be considered as a group of pictures. If there is not much movement in the scene, setting the value higher than the frame rate is fine, potentially resulting in less bandwidth usage. However, if the value is set too high, and there is a high frequency of movement in the video, there is a risk of frame skipping.
Video Compression: MJPEG, H264+, H264, H265 or H265+can be optional. MJPEG is not available for the mainstream. If H.265/H.265+/ H.265S is chosen, make sure the client system can decode H.265/H.265+. Compared to H.265, H.265+ saves more storage space with the same maximum bitrate in most scenes. Compared to H.264, H.265 reduces the transmission bitrate under the same resolution, frame rate, and image quality.
Profile: For H.264. Baseline, main, and high profiles are selectable.
Send Snapshot: Set the snapshot stream.
Videos encode slice split: If this function is enabled, a smooth image can be obtained even though using a low-performance PC.
Watermark: When playing back the local recorded video in the search interface, the watermark can be displayed. To enable it, check the watermark box and enter the watermark text.

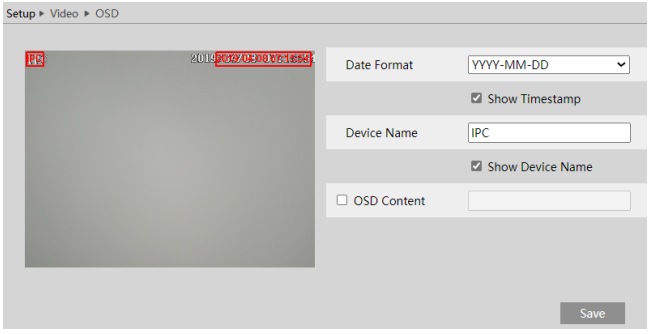
Click the "Audio" tab to go to the interface as shown below.



Audio Encoding: G711A and G711U are selectable.
Audio Type: MIC

5.11.3 OSD Configuration

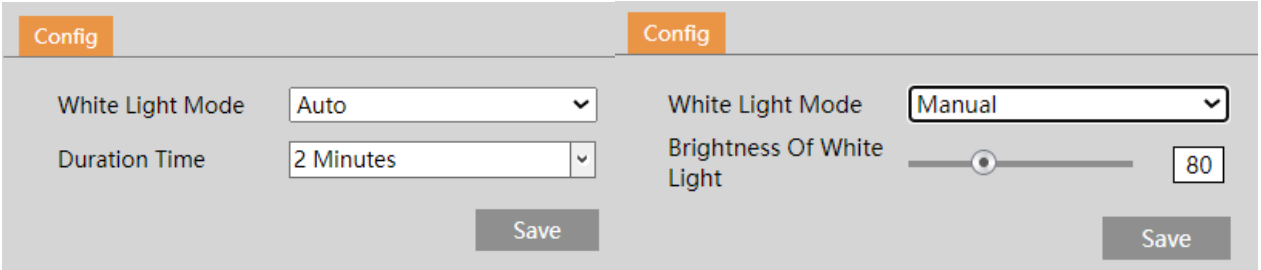
Go to the Video→OSD interface as shown below.



Set time stamp, device name, and OSD content here. After enabling the corresponding display and entering the content, drag them to change their position. Then click the "Save" button to save the settings.

5.11.4 White Light Control

Click Config→Image→White Light Control to go to the following interface.

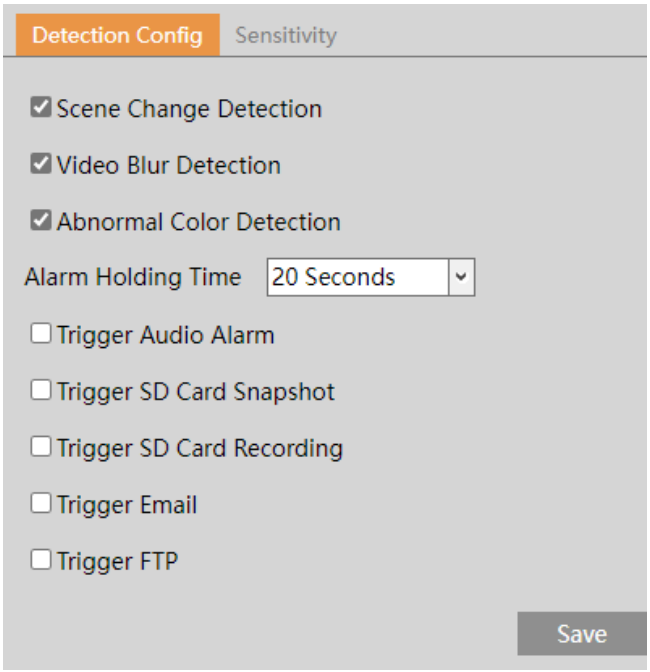


White Light Mode: "OFF", "Manual" or "Auto" is optional. In low illumination conditions, this mode can be enabled.
Auto: The white light will be automatically enabled when collecting a face in low illumination conditions. If the auto mode is selected, the duration time should be set to save energy. For example, the white light is on and the duration time is set to "2 minutes"; if no face appears in the detection area after 2 minutes, the white light will be turned off automatically.
Manual: Select this mode and click "Save". The white light will be turned on. In this mode, you can also set the brightness of white light as needed.

5.12 Alarm Setup

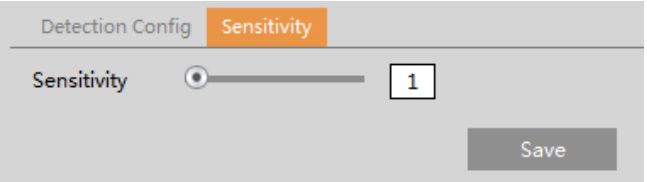
5.12.1 Video Exception

This function can detect changes in the surveillance environment affected by external factors.
Go to Event→Video Exception interface as shown below.



1. Enable the applicable detection that is desired.
Scene Change Detection: Alarms will be triggered if the scene of the video has changed.
Video Blur Detection: Alarms will be triggered if the video becomes blurry.
Abnormal Color Detection: Alarms will be triggered if the image is abnormal caused by color deviation.
2. Set the alarm holding time and alarm trigger options.
Trigger Audio Alarm: If selected, you will hear the warning sound when the video exception happens.
Trigger SD Card Snapshot: If selected, the system will capture images on video exception detection and save the images on an SD card.
Trigger SD Card Recording: If selected, the video will be recorded on an SD card on video exception detection.

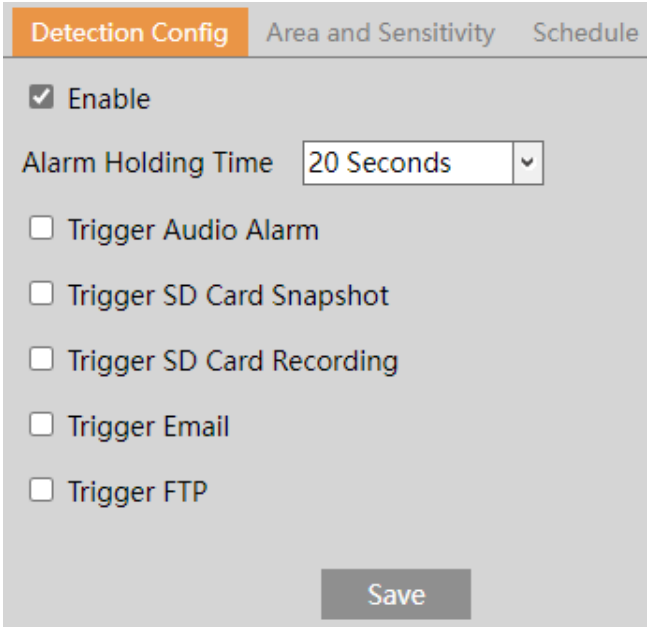
Trigger Email: If "Trigger Email" and "Attach Picture" are checked (email address must be set first in the Email configuration interface), the captured pictures and triggered event will be sent into those addresses.
Trigger FTP: If "Trigger FTP" is checked, the captured pictures will be sent into FTP server address. Please refer to FTP configuration chapter for more details.
3. Click "Save" button to save the settings.
4. Set the sensitivity of the exception detection. Click "Sensitivity" tab to go to the interface as shown below.



Drag the slider to set the sensitivity value or directly enter the sensitivity value in the textbox. Click "Save" button to save the settings.
The sensitivity value of Scene Change Detection: The higher the value is, the more sensitive the system responds to the amplitude of the scene change.
The sensitivity value of Video Blur Detection: The higher the value is, the more sensitive the system responds to the blurriness of the image.
The sensitivity value of Abnormal Color Detection: The higher the value is, the more sensitive the system responds to the color shift of the image.
Note: Try not to enable exception detection when light changes greatly in the scene.

5.12.2 Motion Detection

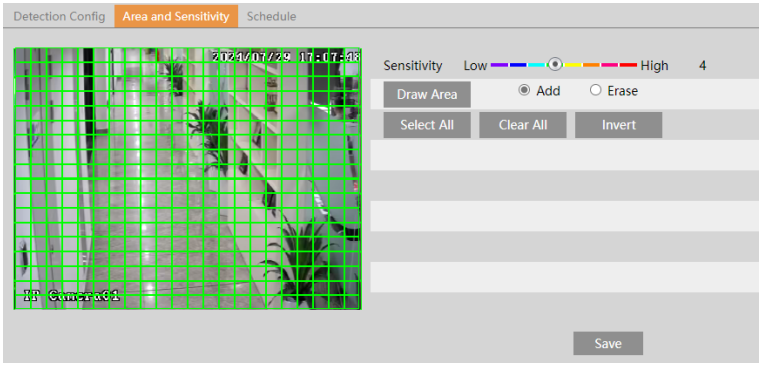
Go to Alarm→Motion Detection to set the motion detection alarm.



1. Check "Enable" check box to activate motion-based alarms. If unchecked, the camera will not send out any signals to trigger motion-based recording to the NVR or CMS, even if there is motion in the video.
Alarm Holding Time: it refers to the time that the alarm extends for after an alarm ends. For instance, if the alarm holding time is set to 20 seconds, once the camera detects a motion, it will go to alarm and would not detect any other motion in 20 seconds. If there is another motion detected during this period, it will be considered as continuous movement; otherwise, it will be considered as a single motion.
Trigger Audio Alarm: If selected, the camera will play the pre-defined warning voice on detecting a motion-based alarm.
Trigger SD Card Snapshot: If selected, the system will capture images on motion detection and save the images on an SD card.
Trigger SD Card Recording: If selected, video will be recorded on an SD card on motion detection.

Trigger Email: If “Trigger Email” and “Attach Picture” are checked (email address must be set first in the Email configuration interface), the captured pictures and triggered event will be sent to those addresses.
Trigger FTP: If “Trigger FTP” and “Attach Picture” are checked, the captured pictures will be sent to the FTP server address. Please refer to the FTP configuration section for more details.

2. Set motion detection area and sensitivity. Click the “Area and Sensitivity” tab to go to the interface as shown below.

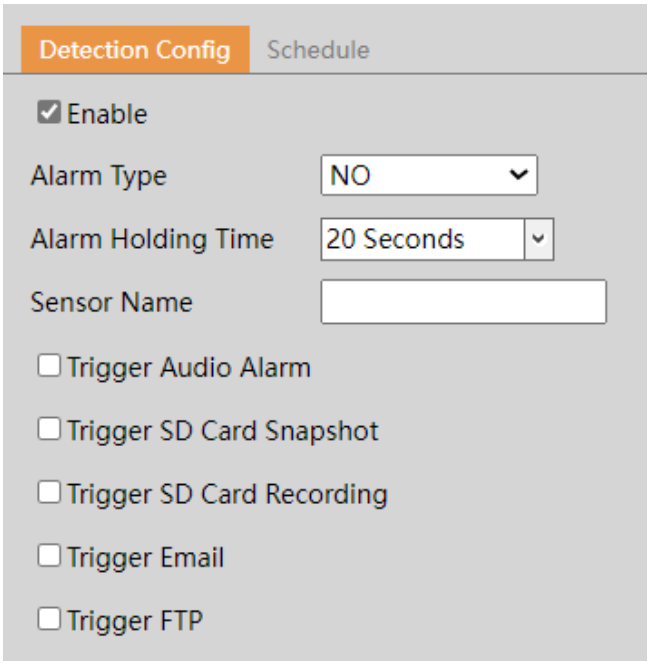


Move the “Sensitivity” scroll bar to set the sensitivity. A higher sensitivity value means that motion will be triggered more easily. Select “Add” and click “Draw”. Drag the mouse to draw the motion detection area; Select “Erase” and drag the mouse to clear the motion detection area.
After that, click “Save” to save the settings. “Clear All” can be used to clear out the entire motion zone.

3. Set the schedule for motion detection. The schedule setup steps of the motion detection are the same as the schedule recording setup (See Schedule Recording).

5.12.3 Alarm In (Sensor Input)

This function is only available for some models. To set sensor alarm (alarm in):
Go to Alarm→Alarm In interface as shown below.

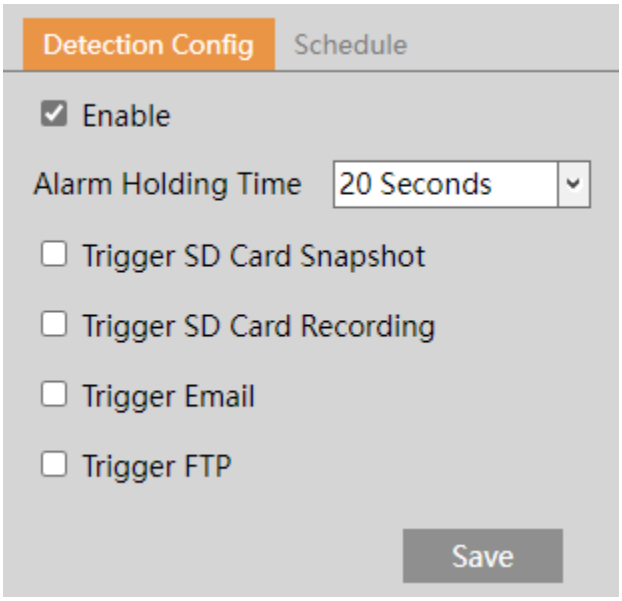


1. Click “Enable” and set the alarm type, alarm holding time and sensor name.
2. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to motion detection section for details.
3. Click “Save” button to save the settings.

4. Set the schedule of the sensor alarm. The setup steps of the schedule are the same as the schedule recording setup. (See Schedule Recording).

5.12.4 Person Detection

Alarms will be triggered when the camera detects a person. Go to Config→Alarm→ Person Detection.

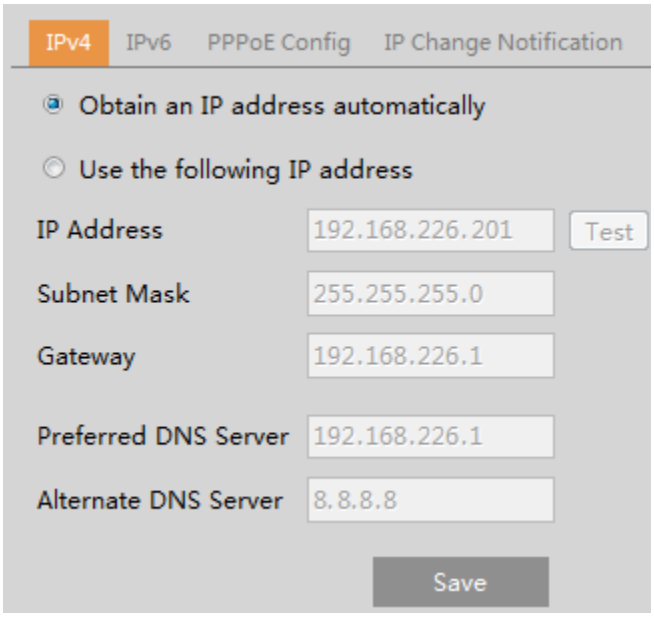


1. Enable person detection and then set the alarm holding time.
2. Set alarm trigger options. The setup steps are the same as the alarm trigger settings of motion detection.
3. Set the schedule of person detection. The setup steps of schedule are the same as the schedule recording (See Schedule Recording).

5.13 Network Configuration

5.13.1 TCP/IP

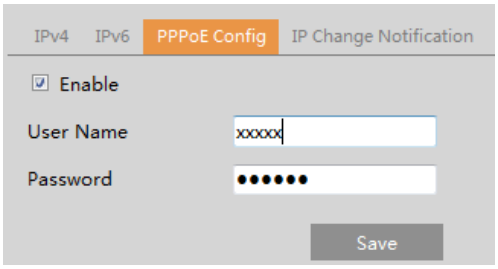
Go to Network→TCP/IP interface as shown below. There are two ways for network connection.



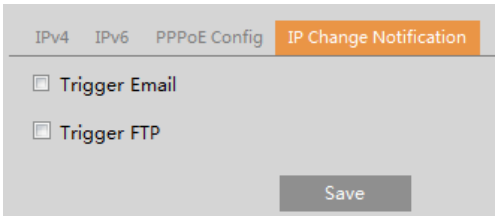
Use IP address (take IPv4 for example)-obtain a local IP address automatically through DHCP. A typical router has a DHCP server

built in, and therefore can assign an IP address to the camera.

Use PPPoE-Click the "PPPoE Config" tab to go to the interface as shown below. Enable PPPoE and then enter the username and password from your ISP.



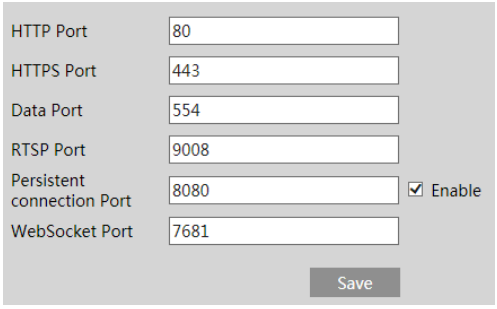
Method of network connection can be used. If PPPoE is used to connect to the internet, the camera will get a dynamic WAN IP address. This IP address will change frequently. To be notified, the IP change notification function can be used.
Click "IP Change Notification Config" to go to the interface as shown below.



Trigger Email: when the IP address of the device is changed, the new IP address will be sent to the email address that has been set up.
Trigger FTP: when the IP address of the device is changed, the new IP address will be sent to the FTP server that has been set up.

5.13.2 Port

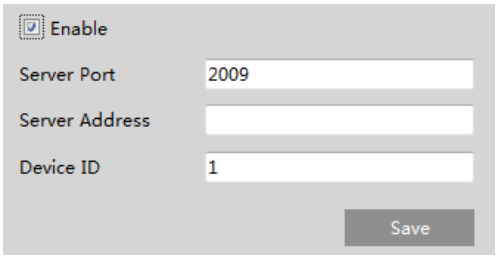
Go to Network→Ports/Connections as shown below. HTTP port, Data port, and RTSP port can be set.



HTTP Port: The default HTTP port is 80. It can be changed to any port which is not occupied.
HTTPS Port: The default HTTPs port is 443. It can be changed to any port which is not occupied.
Data Port: The default data port is 9008. Please change it as necessary.
RTSP Port: The default port is 554. Please change it as necessary.
Persistent Connection Port: The port is used for a persistent connection of the third-party platform to push smart data, like face pictures.
WebSocket Port: Communication protocol port for plug-in free preview.

5.13.3 Server Configuration

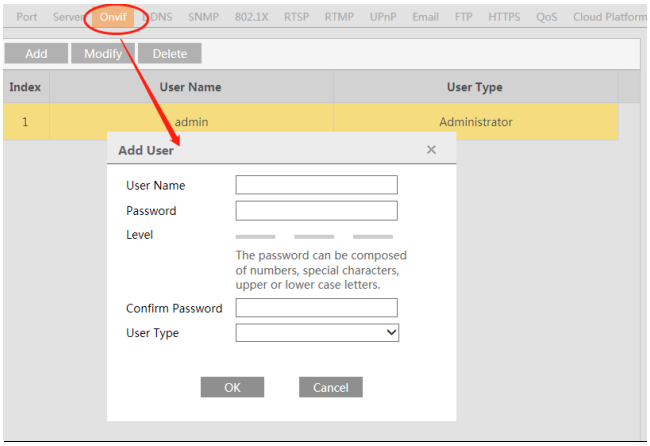
This function is mainly used for connecting network video management systems.



1. Check “Enable”.
2. Check the IP address and port of the transfer media server in the VMS. Then enable the auto report in the VMS when adding a new device. Next, enter the remaining information of the device in the VMS. After that, the system will automatically allot a device ID. Please check it in the VMS.
3. Enter the above-mentioned server address, server port and device ID in the corresponding boxes. Click the “Save” button to save the settings.

5.13.4 Onvif

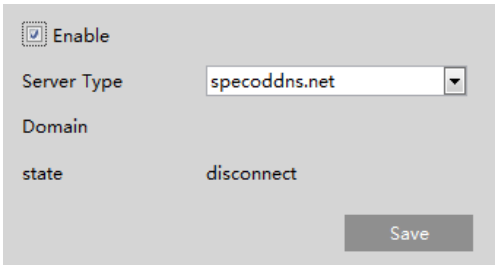
The camera can be searched and connected to the third-party platform via ONVIF/RTSP protocol.



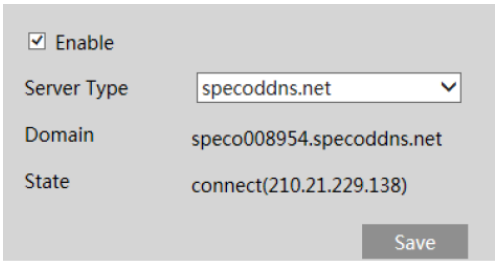
Note: when adding the device to the third-party platform with ONVIF/RTSP protocol, please enter the username and password created in the above interface.

5.13.5 DDNS

If the camera is set up with a DHCP connection, DDNS should be set for accessing the camera from the internet.
1. Go to Network→Ports/Connections→ DDNS.

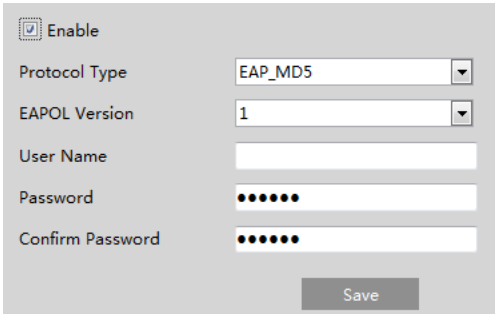


2. Enable, save and use DDNS to log in.



5.13.6 802.1x

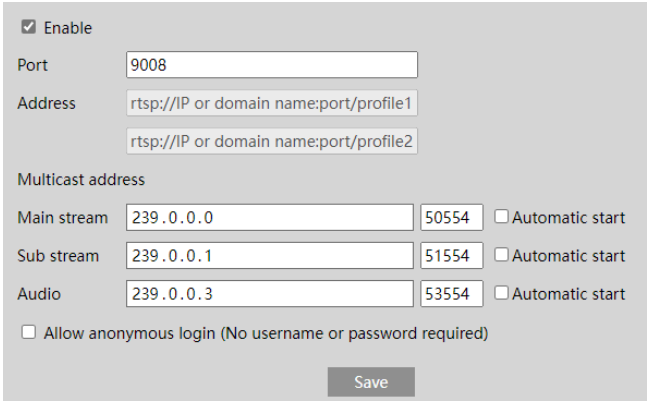
If it is enabled, the camera's data can be protected. When the camera is connected to the network protected by the IEE802.1x, user authentication is needed.



To use this function, the camera shall be connected to a switch supporting the 802.1x protocol. The switch can be reckoned as an authentication system to identify the device in a local network. If the camera connected to the network interface of the switch has passed the authentication of the switch, it can be accessed via the local network.
Protocol type and EAPOL version: Please use the default settings.
Username and password: The username and password must be the same as the user name and password applied for and registered in the authentication server.

5.13.7 RTSP

Go to Network→Ports/Connections→RTSP.



Select "Enable" to enable the RTSP function.
Port: Access port of the streaming media. The default number is 554.
RTSP Address: The RTSP address (unicast) format that can be used to play the stream in a media player.

Multicast Address
Mainstream: The address format is
"rtsp://IP address: rtsp port/profile1?transportmode=mcast".
Substream: The address format is

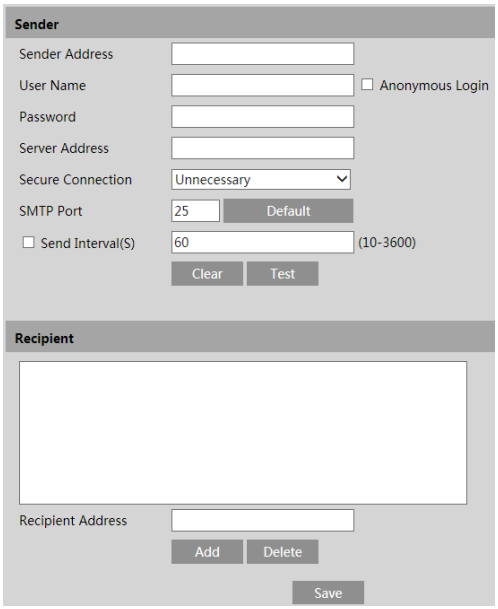
"rtsp://IP address: rtsp port/profile2?transportmode=mcast".
Audio: Having entered the main/sub stream in a media player (like VLC), the video and audio will play automatically.
If "Allow anonymous login…" is checked, there is no need to enter the username and password to view the video.
If "auto start" is enabled, the multicast received data should be added to a VLC player to play the video.

5.13.8 UPNP

If this function is enabled, the camera can be quickly accessed through the LAN.
Go to Network→Ports/Connections→UPnP. Enable UPNP and then enter UPnP name.

5.13.9 Email

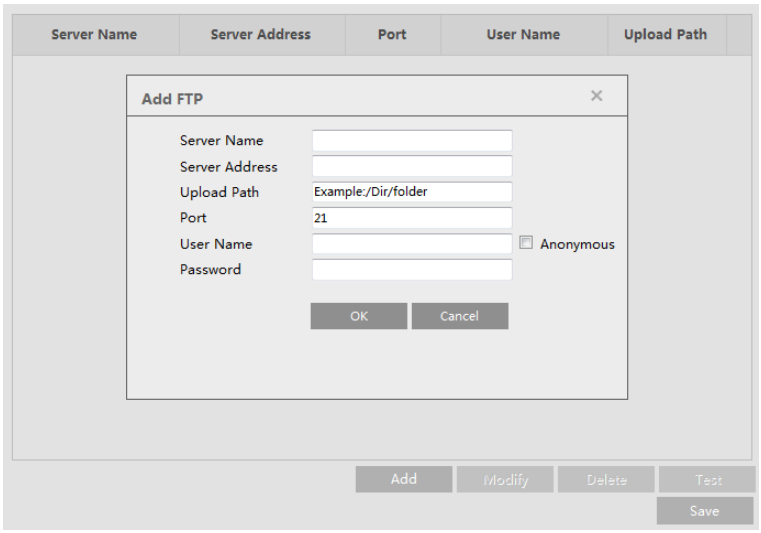
If you need to trigger an Email when an alarm happens or IP address is changed, please set the Email here first.
Go to Network→Ports/Connections→Email.



Sender Address: sender's e-mail address.
User name and password: sender's user name and password (you don't have to enter the username and password if "Anonymous Login" is enabled).
Server Address: The SMTP IP address or host name.
Select the secure connection type at the "Secure Connection" pull-down list according to what's required.
SMTP Port: The SMTP port.
Send Interval(S): The time interval of sending an email. For example, if it is set to 60 seconds and multiple motion detection alarms are triggered within 60 seconds, they will be considered as only one alarm event and only one email will be sent. If one motion alarm event is triggered and then another motion detection alarm event is triggered after 60 seconds, two emails will be sent. When different alarms are triggered at the same time, multiple emails will be sent separately.
Click the "Test" button to test the connection of the account.
Recipient Address: receiver's e-mail address.

5.13.10 FTP

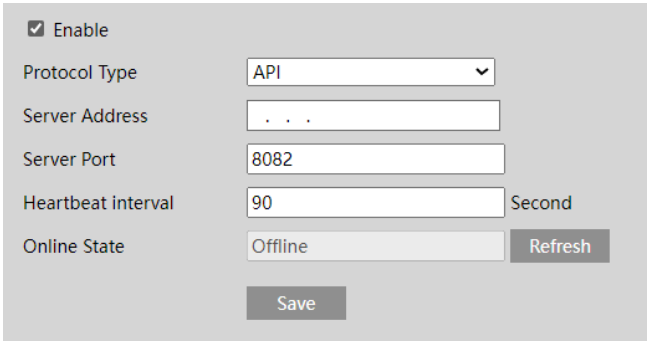
After an FTP server is set up, captured pictures from events will be uploaded to the FTP server.
Go to Network→Ports/Connections→FTP.



Server Name: The name of the FTP server.
Server Address: The IP address or domain name of the FTP.
Upload Path: The directory where files will be uploaded to.
Port: The port of the FTP server.
Use Name and Password: The username and password that are used to login to the FTP server.

5.13.11 HTTP POST

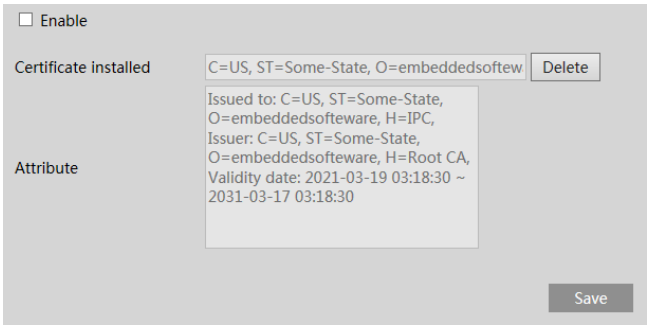
Go to Network→Ports/Connections→HTTP POST interface.
Check "Enable", select protocol type, and then set the server address (IP address/domain name), server port, and heartbeat interval.



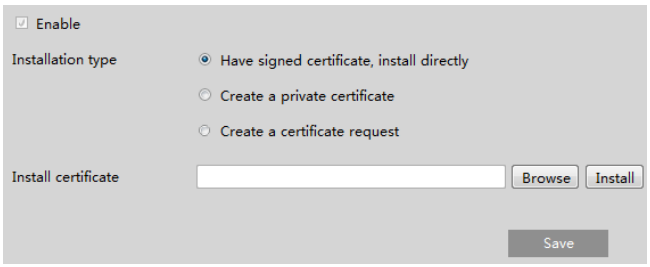
Server address: the IP address/domain name of the third-party platform.
Server port: the server port of the third-party platform.
After the above parameters are set, click "Save" to save the settings. Then the camera will automatically connect to the third-party platform. The online state can be viewed in the above interface. After the camera is successfully connected, it will send the alarm information (HTTP format) to the third-party platform once the smart alarm is triggered. The alarm information includes target tracing coordinates, target features, the captured original/target image (like the captured face picture), and so on.

5.13.12 HTTPS

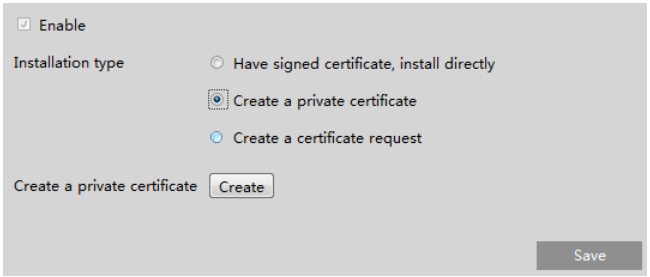
HTTPs provide authentication of the website and protect user privacy.
Go to Network→Ports/Connections→HTTPS as shown below.



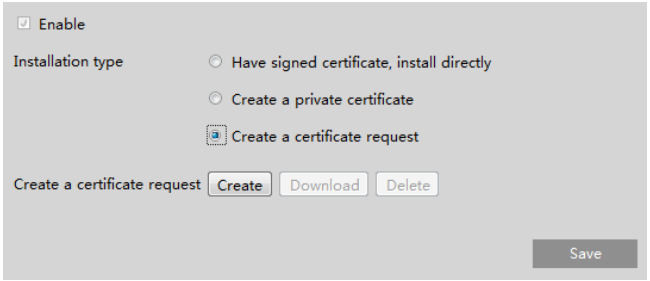
There is a certificate installed by default as shown above. Enable this function and save it. Then the camera can be accessed by entering https://IP: https port via the web browser (eg. https://192.168.226.201:443).
A private certificate can be created if users don't want to use the default one. Click "Delete" to cancel the default certificate. Then the following interface will be displayed.



* If there is a signed certificate, click "Browse" to select it and then click "Install" to install it.
* Click "Create a private certificate" to enter the following creation interface.



Click the "Create" button to create a private certificate. Enter the country (only two letters available), domain (camera's IP address/domain), validity date, password, province/state, region and so on. Then click "OK" to save the settings.
* Click "Create a certificate request" to enter the following interface.

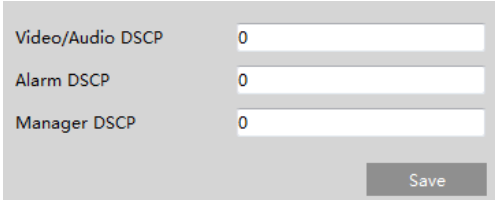


Click "Create" to create the certificate request. Then download the certificate request and submit it to the trusted certificate authority for signature. After receiving the signed certificate, import the certificate to the device.

5.13.13 QoS

QoS (Quality of Service) function is used to provide different quality of services for different network applications. With the deficient

bandwidth, the router or switch will sort the data streams and transfer them according to their priority to solve the network delay and network congestion by using this function.
Go to Network→QoS.

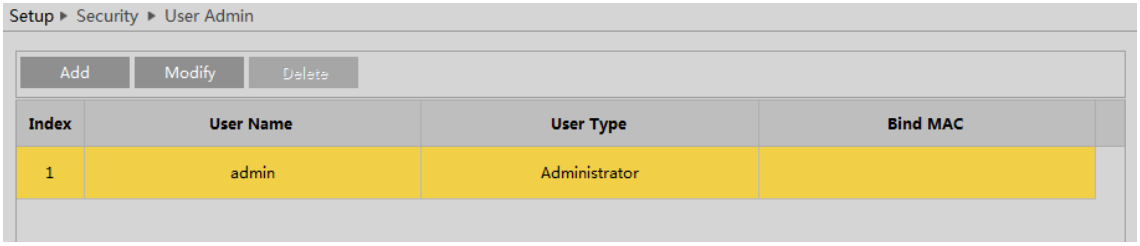


Video/Audio DSCP: The range is from 0 to 63.
Alarm DSCP: The range is from 0 to 63.
Manager DSCP: The range is from 0 to 63.
Generally speaking, the larger the number is, the higher the priority is.

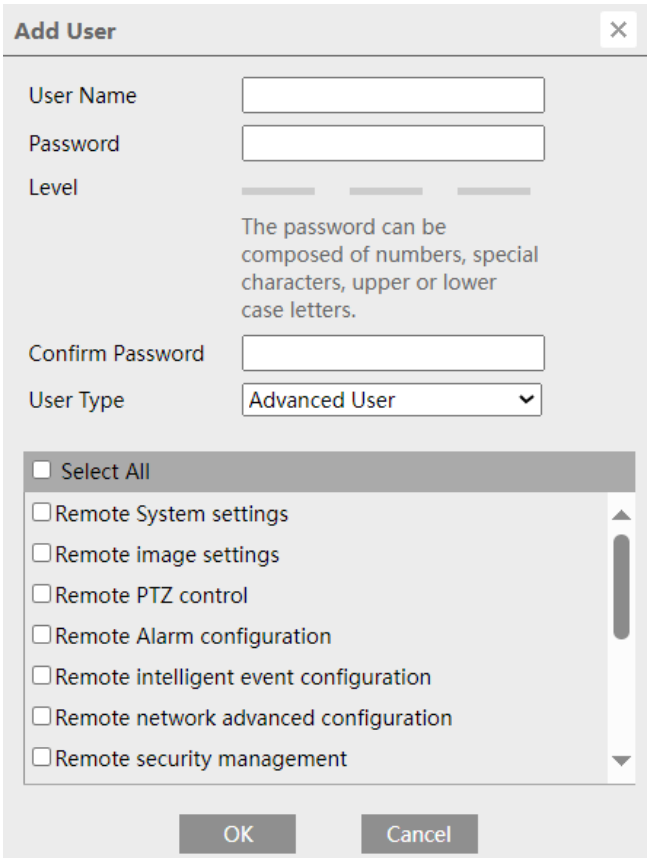
5.14 Security Configuration

5.14.1 User Admin

Go to Security→User Admin interface as shown below.

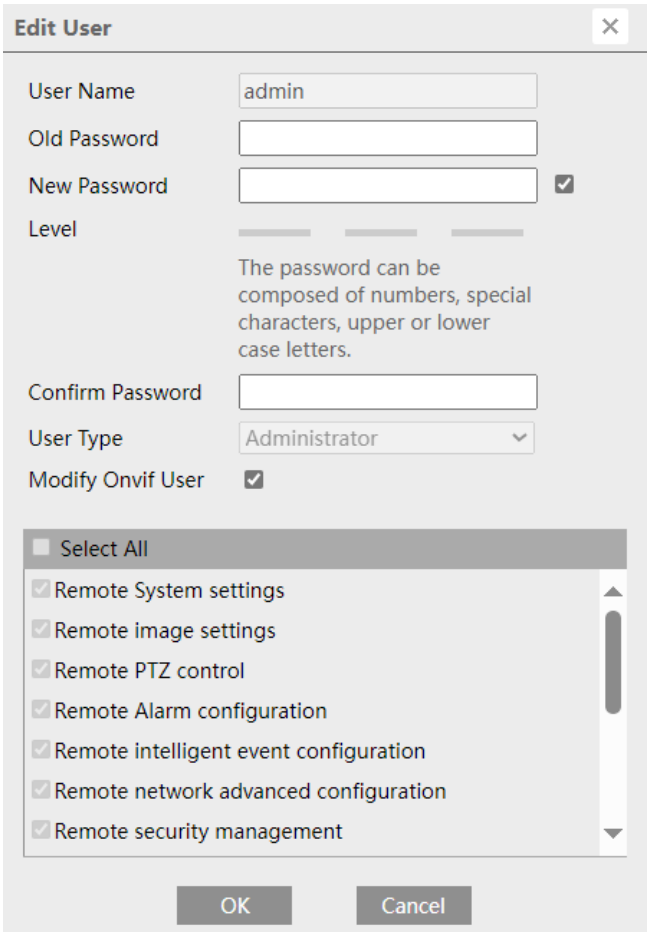


Add user:
1. Click “Add” to pop up the following textbox.



2. Enter user name in “User Name” textbox.
3. Enter letters or numbers in “Password” and “Confirm Password” textbox. Please set the password according to the requirement of the password security level (Go to Setup→Security→Security Management→Password Security interface to set the security level).
4. Choose the user type and select the permission.
6. Click the “OK” button and then the newly added user will be displayed in the user list.

Modify user:
1. Select a user to modify password and MAC address if necessary in the user configuration list box.
2. The “Edit user” dialog box pops up by clicking the “Modify” button.



3. Enter the old password of the user in the “Old Password” text box.
4. Enter the new password in the “New password” and “Confirm Password” text box.
5. Modify the permission as necessary.
6. Click the “OK” button to save the settings.

Note: To change the access level of a user, the user must be deleted and added again with the new access level.

Delete user:

1. Select the user to be deleted in the user configuration list box.
2. Click the “Delete” button to delete the user.

Note: The default administrator account cannot be deleted.

5.14.2 Online User

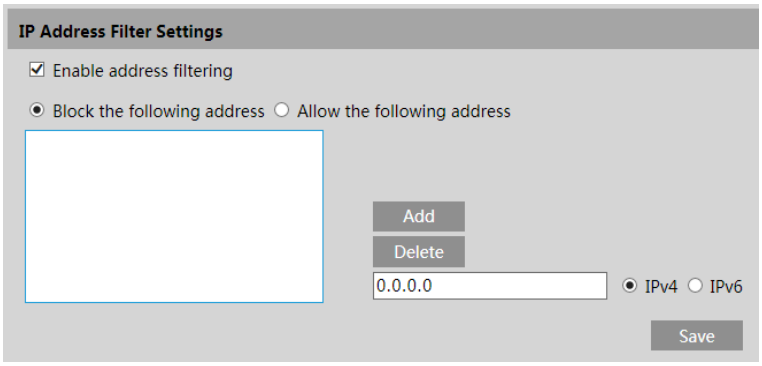
Go to Security→Online User to view the user who is viewing the live video.

Index	Client Address	Port	User Name	User Type	
1	192.168.17.232	55760	admin	Administrator	Kick Out

An administrator user can kick out all the other users (including other administrators).

5.14.3 Block and Allow Lists

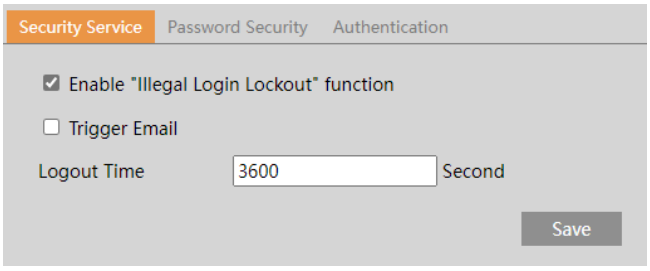
Go to Security→Block and Allow Lists as shown below.



The setup steps are as follows:
Check the “Enable address filtering” check box.
Select “Block/Allow the following address”, IPv4/IPv6 and then enter IP address in the address box and click the “Add” button.

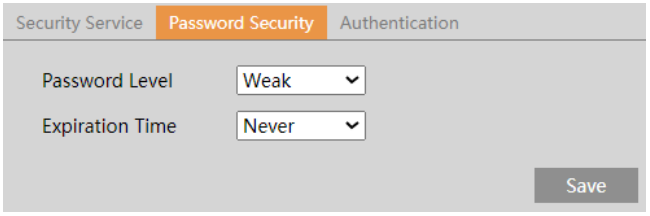
5.14.4 Security Management

Go to Security→Security Management as shown below.



In order to prevent against malicious password unlocking, “Illegal Login Lockout” function can be enabled here. If this function is enabled, login failure after trying five times will make the login interface locked. The camera can be logged in again after a half hour or after the camera reboots.
Trigger Email: if enabled, e-mail will be sent when logging in/out or illegal login lock occurs.
Logout time: Set the logout time as needed. For example: 3600s, you will be automatically logged out after 3600s and then you need to enter the username and password again to log in.

- **Password Security**

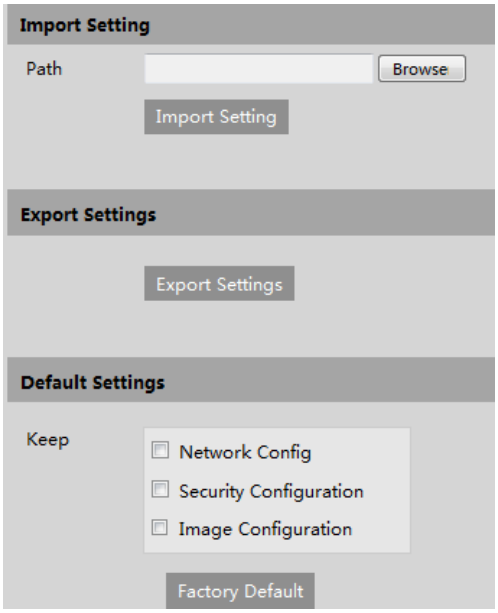


Please set the password level and expiration time as needed.
Password Level: Weak, Medium or Strong.
Weak level: Numbers, special characters, upper or lower case letters can be used. You can choose one of them or any combination of them when setting the password.
Medium Level: 8~16 characters, including at least two of the following categories: numbers, special characters, upper case letters, lower case letters.
Strong Level: 8~16 characters. Numbers, special characters, upper case letters and lower case letters must be included.
For your account security, it is recommended to set a strong password and change your password regularly.
HTTP Authentication: Basic or Token is selectable.

5.15 Maintenance Configuration

5.15.1 Backup and Restore

Go to Maintenance→Backup & Restore.



- **Import & Export Settings**

Configuration settings of the camera can be exported form a camera into another camera.
1. Click “Browse” to select the save path for import or export information on the PC.
2. Click the “Import Setting” or “Export Setting” button.

- **Default Settings**

Click the “Load Default” button to restore all system settings to the default factory settings except those you want to keep.

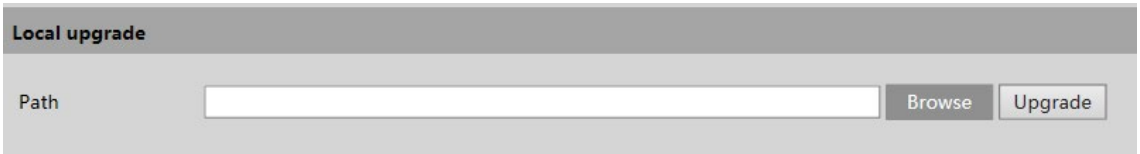
5.15.2 Reboot

Go to Maintenance→Reboot.
Click the “Reboot” button to reboot the device.

Timed Reboot Setting:
If necessary, the camera can be set up to reboot on a time interval. Enable “Time Settings”, set the date and time and then click the “Save” button to save the settings.

5.15.3 Upgrade

Go to Maintenance→Upgrade. In this interface, the camera firmware can be updated.



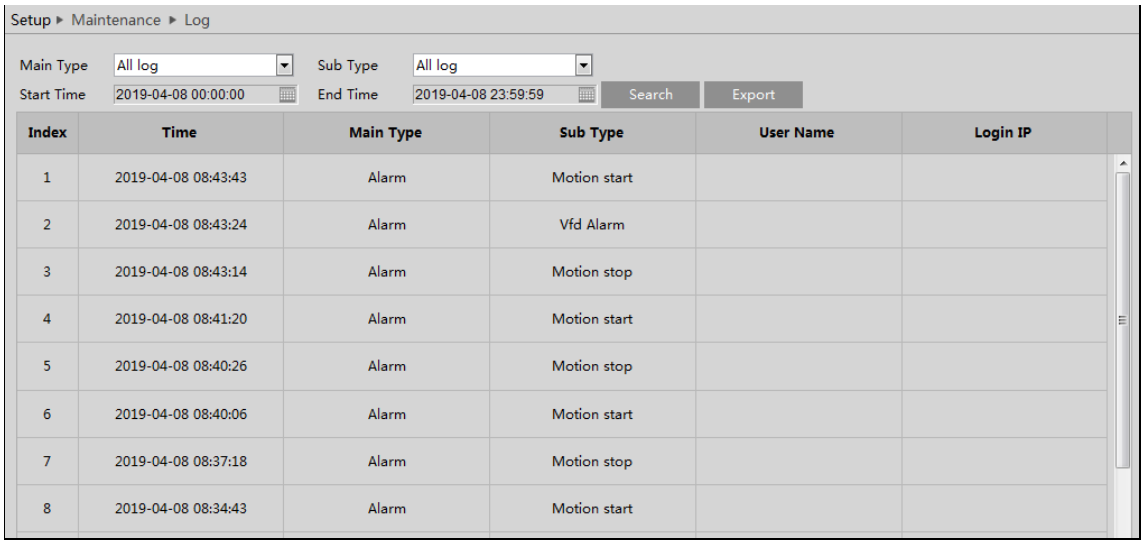
1. Click the “Browse” button to select the save path of the upgrade file
2. Click the “Upgrade” button to start upgrading the firmware.
3. The device will restart automatically

Caution! Do not close the browser or disconnect the camera from the network during the upgrade.

5.15.4 Operation Log

To query and export log:

1. Go to Maintenance→Operation Log.

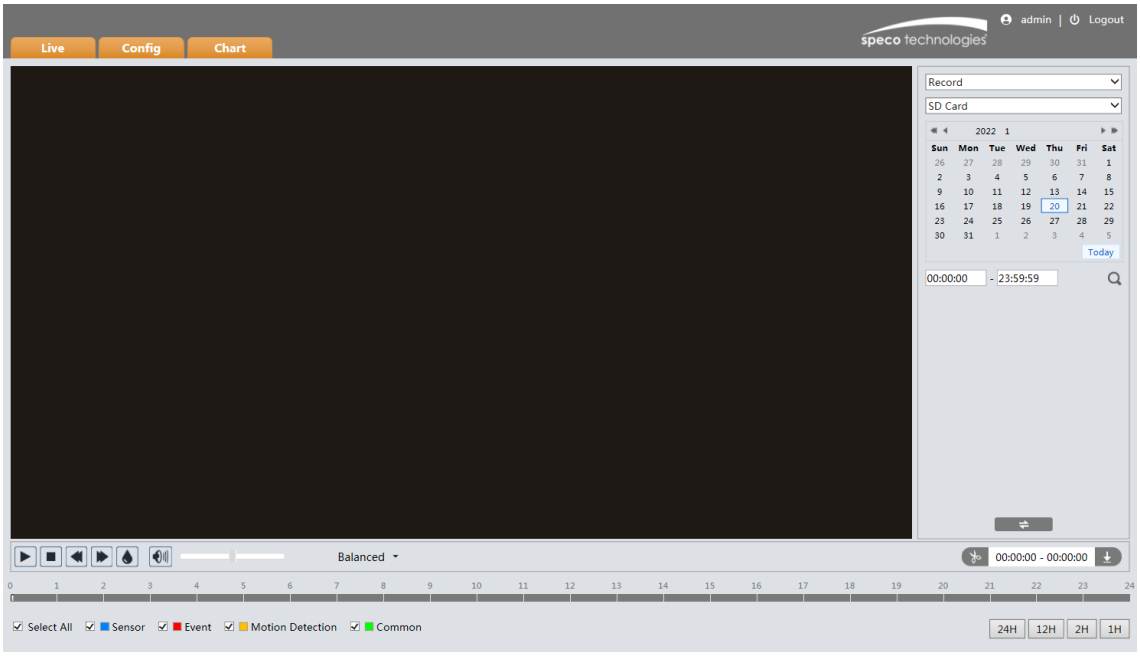


2. Select the main type, sub type, start and end time.
3. Click “Search” to view the operation log.
4. Click “Export” to export the operation log.

6 Search

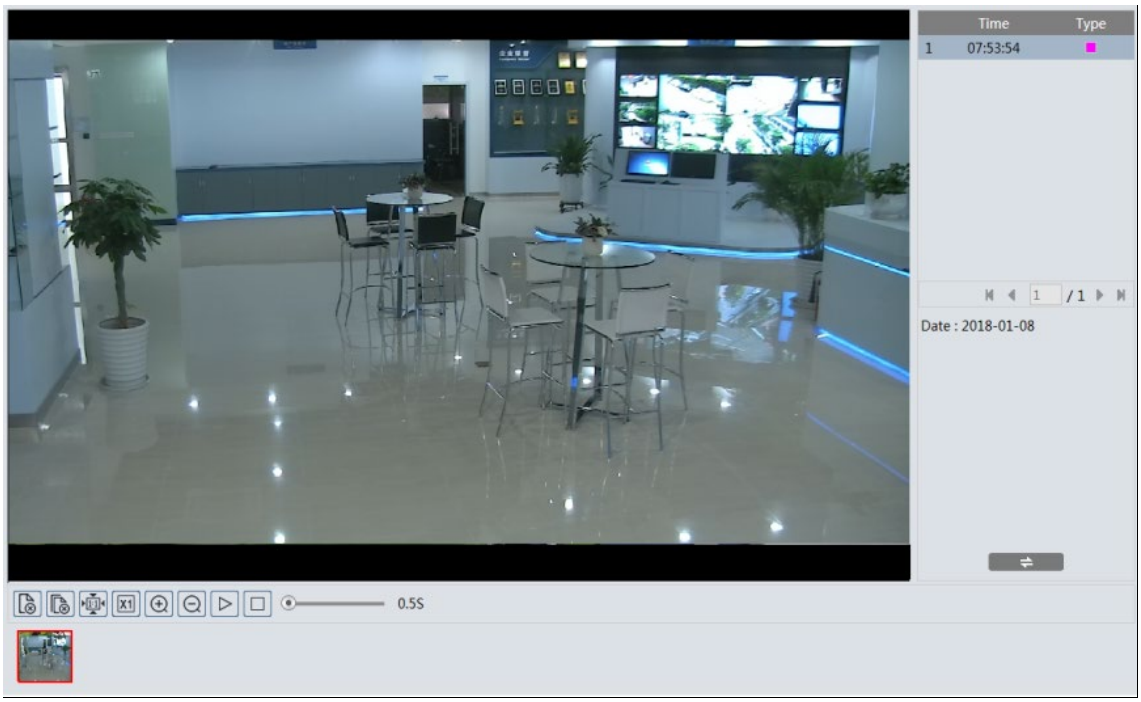
6.1 Image Search

In the Setup interface, click Search to go to the interface as shown below. Images that are saved on the PC or SD card can be found here.



- **Local Image Search**

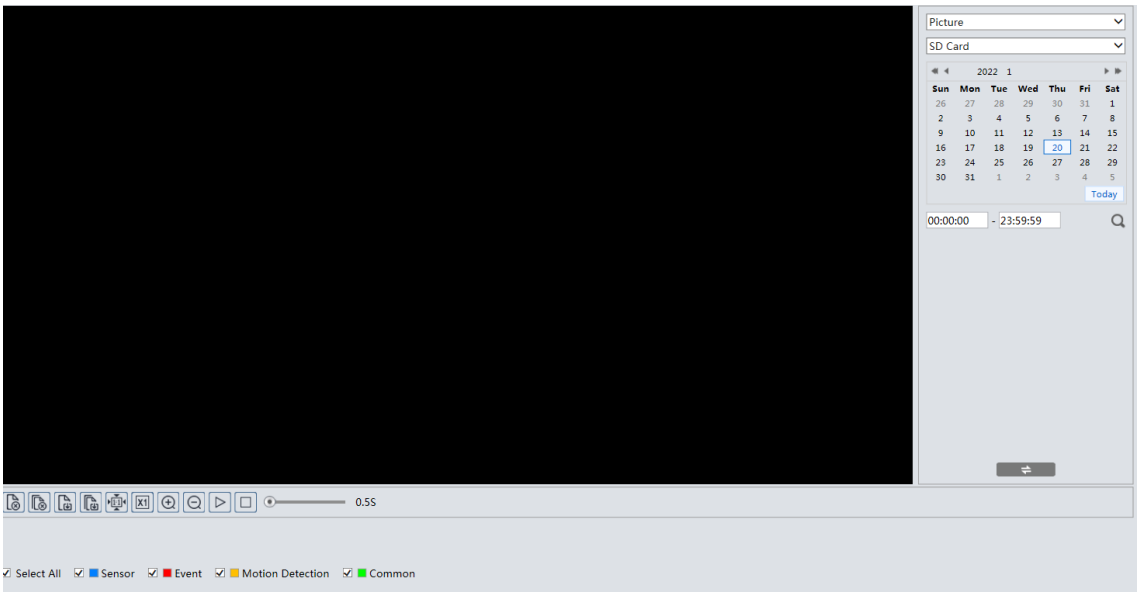
1. Choose “Picture”—“Local”.
2. Set time: Select date and choose the start and end time.
3. Click to search the images.
4. Double click a filename in the list to view the captured photos as shown above.



Click ⇌ to return to the previous interface.

- **SD Card Image Search**

1. Choose “Picture”—“SD Card”.



2. Set time: Select date and choose the start and end time.
3. Choose the alarm events at the bottom of the interface.
4. Click to search the images.
5. Double click a file name in the list to view the captured photos.

Click ⇌ to return to the previous interface.

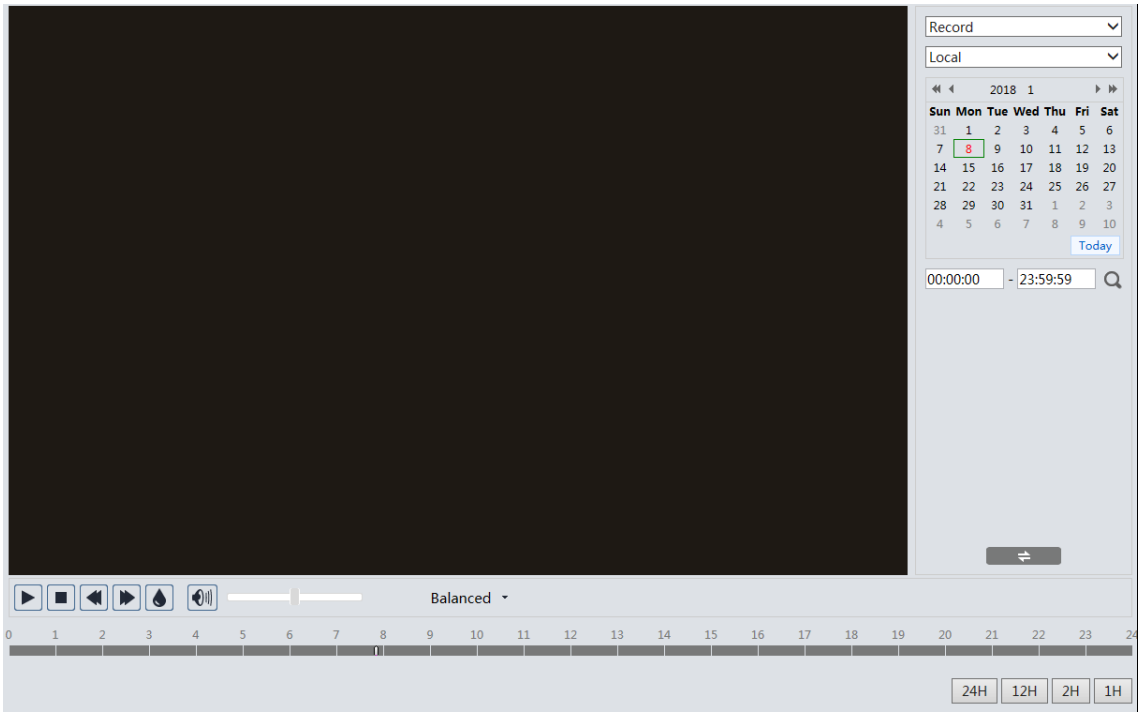
The descriptions of the buttons are shown as follows.

Icon	Description	Icon	Description
	Close: Select an image and click this button to close the image.		Close all: Click this button to close all images.
	Save: Click this button to select the path for saving the image on the PC.		Save all: Click this button to select the path for saving all pictures on the PC.
	Fit size: Click to fit the image on the screen.		Actual size: Click this button to display the actual size of the image.
	Zoom in: Click this button to digitally zoom in.		Zoom out: Click this button to digitally zoom out.
	Slide show play: Click this button to start the slide show mode.		Stop: Click this button to stop the slide show.
5.5S	Play speed: Play speed of the slide show.		

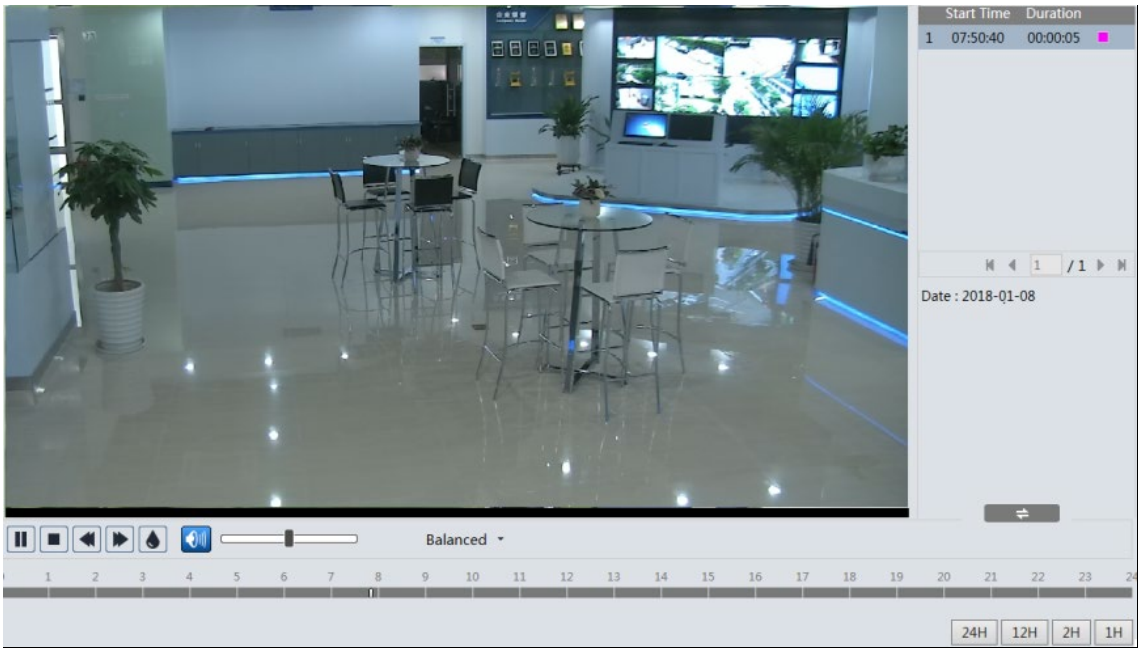
6.2 Video Search

6.2.1 Local Video Search

Click Search to go to the interface as shown below. Videos were recorded locally to the PC can be played in this interface.



1. Choose “Record”—“Local”.
2. Set search time: Select the date and choose the start and end time.
3. Click to search the images.
4. Double click on a file name in the list to start playback.

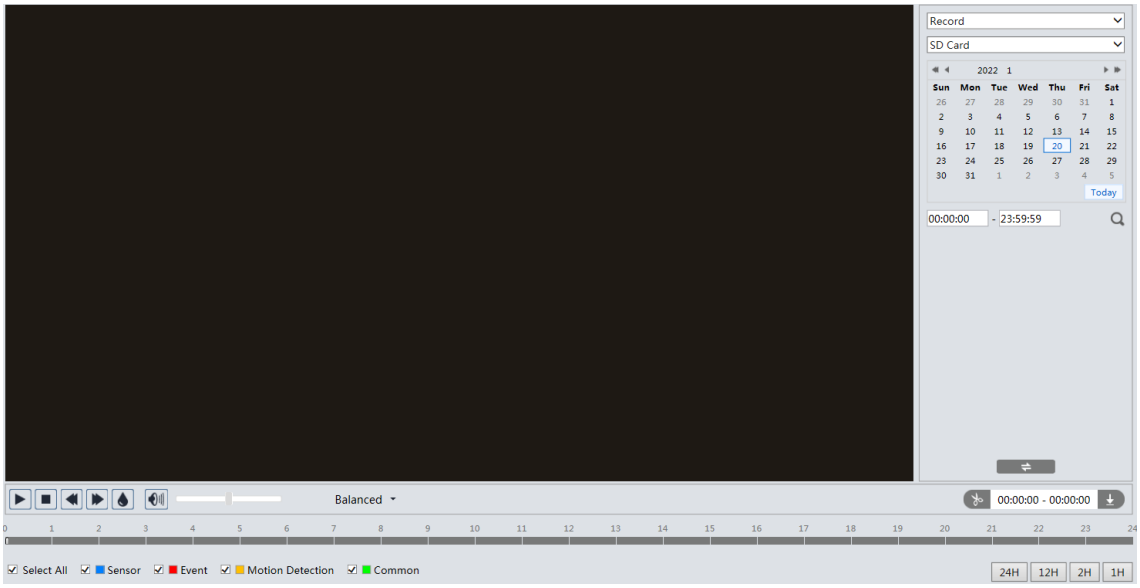


Icon	Description	Icon	Description
	Play button. After pausing the video, click this button to continue playing.		Pause button
	Stop button		Speed down
	Speed up		Watermark display
	Enable / disable audio; drag the slider to adjust the volume after enabling audio.		

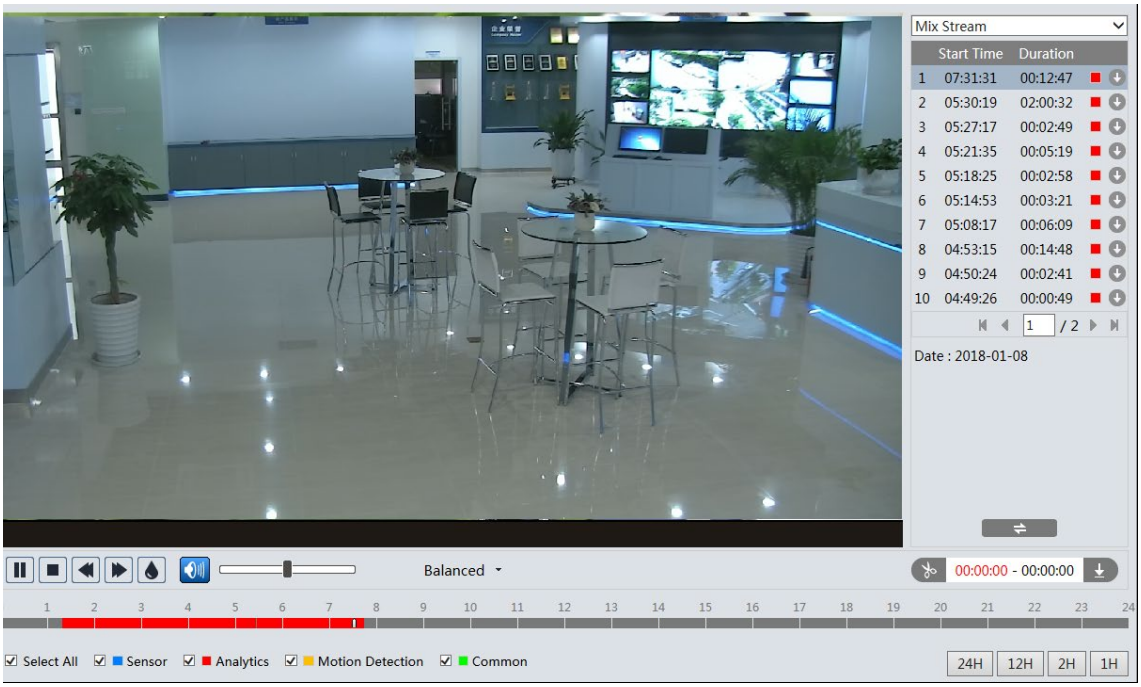
6.2.2 SD Card Video Search

Click Search to go to the interface as shown below. Videos that were recorded on the SD card can be played in this interface.

1. Choose “Record”—“SD Card”.
2. Set search time: Select the date and choose the start and end time.
3. Click to search the images.



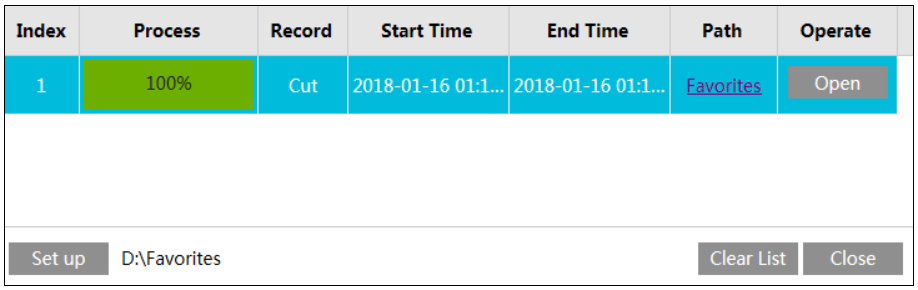
4. Select the alarm events at the bottom of the interface.
5. Select mix stream (video and audio stream) or video stream as needed.
6. Double click on a file name in the list to start playback.



The time table can be shown in 24H/12H/2H/1H format by clicking the corresponding buttons.

Video clip and downloading

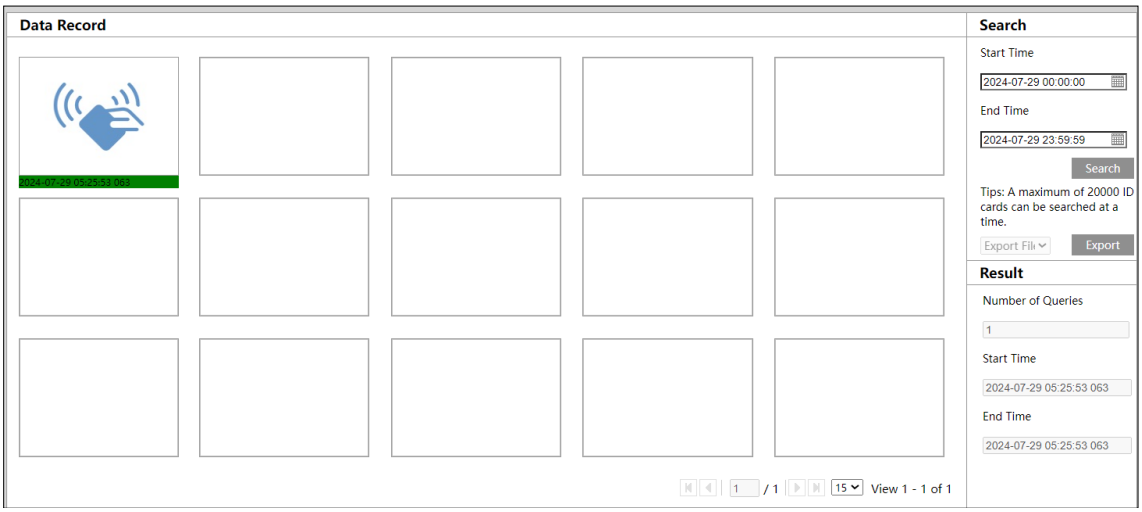
1. Search the video files according to the above mentioned steps.
2. Select the start time by clicking on the time table.
3. Click to set the start time and then this button turns blue ( ).
4. Select the end time by clicking on the time table. Then click to set the end time.
5. Click to download the video file in the PC.



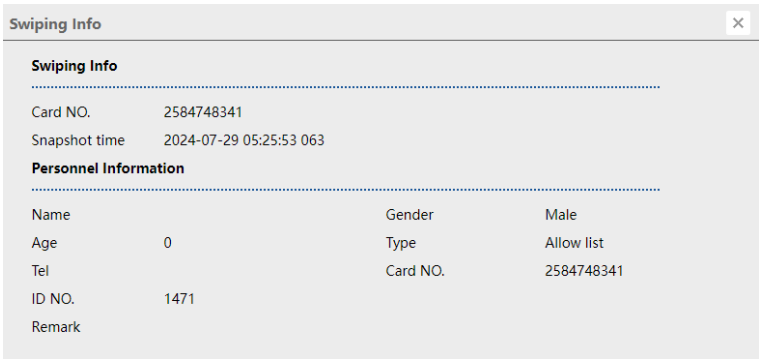
Click “Set up” to set the storage directory of the video files.
Click “Open” to play the video.
Click “Clear List” to clear the downloading list.
Click “Close” to close the downloading window.

6.3 Match Result Search

Click “Data Record” tab to go to the recognition result search interface.
Set the start time and end time and click “Search” to view the card swiping result.



Green time tag means there is a comparison result. Click the picture with green time tag and then the comparison information can be viewed as shown below.



Click “Export” to export the swiping information.

Appendix

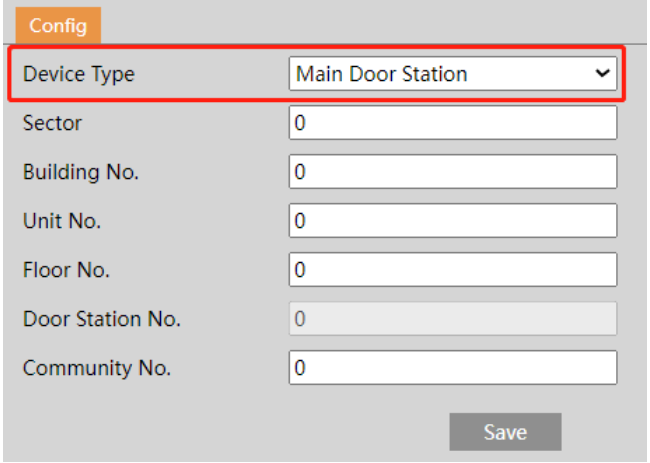
Appendix 1 How to Call Indoor Station

Appendix 1-1 One Door Station Calls One Indoor Station

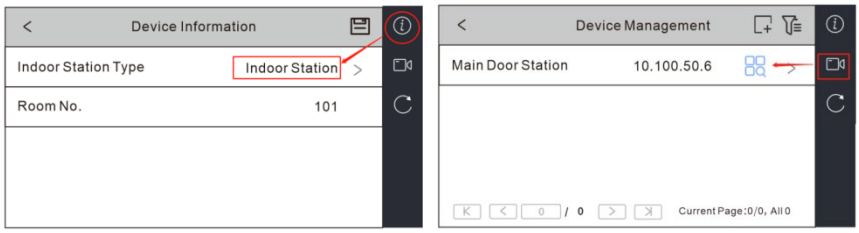
Application: Install one doorbell (hereinafter referred to as door station) and bind one indoor station. Press the Call button to call indoor station

The setting steps are as follows:

1. Connect your door station and indoor station to the same local network and then set their network parameters to the same network segment.
2. Log in the web client of the door station. Click ***Config→Intercom→Number Configuration*** to go to the following interface. Set the device type to "Main Door Station".



3. Tap ***Settings→More Settings→Configuration*** in the indoor station. Then enter the password of Admin to enter the following interface. Set the indoor station type (it should be set to "Indoor station"), room number, IP address of the main door station.



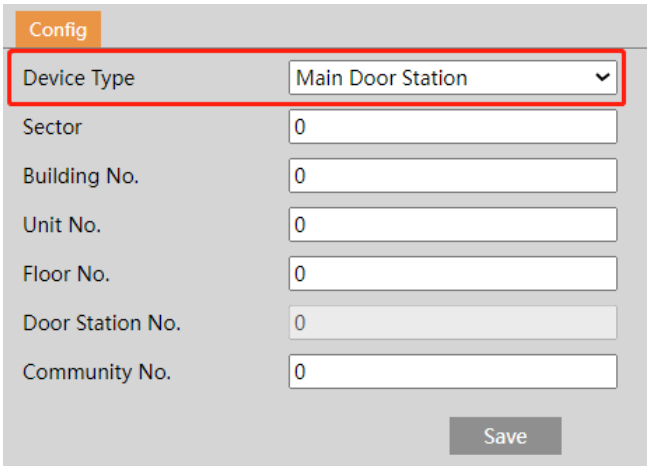
4. Call indoor station through your door station (See Call Resident for details).

Appendix 1-2 One Door Station Calls Multiple Indoor Stations

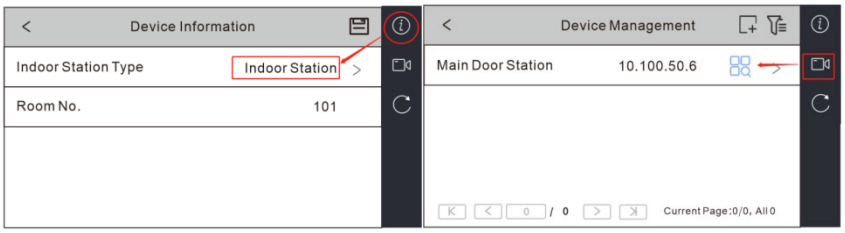
Application: Install one door station and bind multiple indoor stations with the same room number set. Press the Call button to call indoor station. All indoor stations will respond at the same time. The resident can answer any one of them and open the door.

The setting steps are as follows:

1. Connect your door station and indoor station to the same local network and then set their network parameters to the same network segment.
2. Log in the web client of the door station. Click ***Config→Intercom→Number Configuration*** to go to the following interface. Set the device type to "Main Door Station".



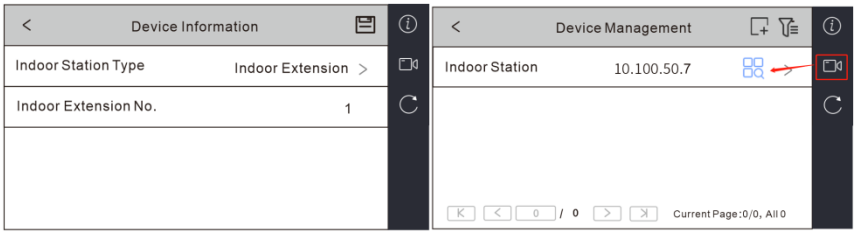
3. Tap ***Settings→More Settings→Configuration*** in the indoor station. Then enter the password of Admin to enter the following interface. Set the indoor station type (it should be set to "Indoor station"), room number (like 101), IP address of the main door station.



4. Set indoor extensions.

Tap ***Settings→More Settings→Configuration*** in the indoor station. Then enter the password of Admin to enter the following interface. Set the indoor station type (it should be set to "Indoor Extension"), number (ranging from 1 to 5), IP address of the indoor station.

Note： For one indoor station, up to 5 indoor extensions can be configured. The indoor station number is 0 by default.



5. Call indoor station through your door station (See Call Resident for details). All indoor stations (including indoor station and extensions) will respond at the same time.

Appendix 1-3 Multiple Door Stations Call One Indoor Station

Application: Install multiple door stations and bind one indoor station. Press the Call button to call indoor station

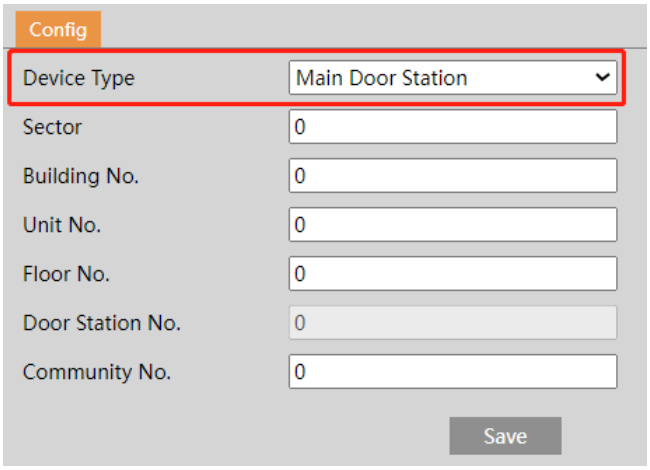
Note: Up to 9 sub door stations can be set for a main door station.

The setting steps are as follows:

1. Connect your door stations and indoor station to the same local network and then set their network parameters to the same network segment.

2. Main door station settings

Log in the web client of the door station. Click ***Config→Intercom→Number Configuration*** to go to the following interface. Set the device type to "Main Door Station".

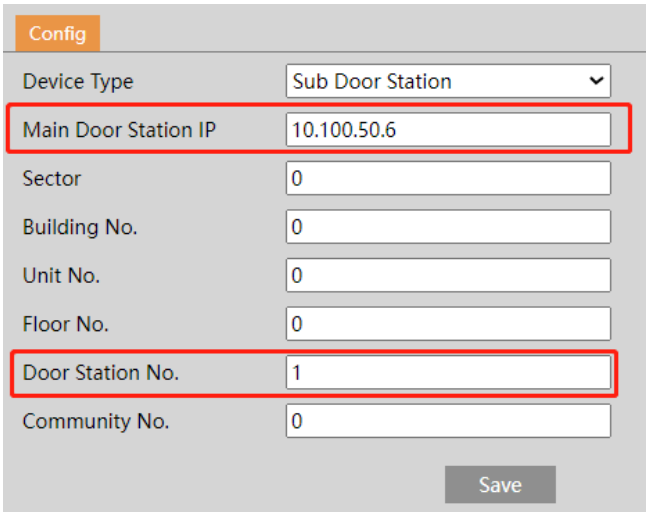


3. Sub door station settings

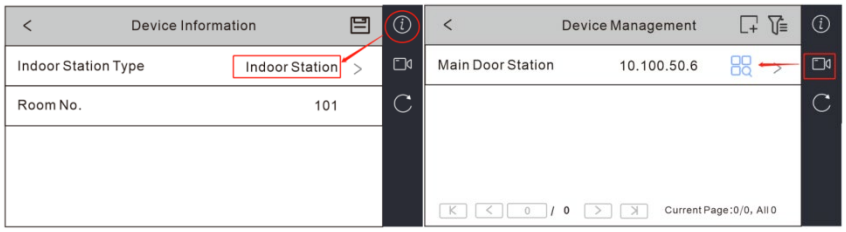
Log in the web client of the door station. Click ***Config→Intercom→Number Configuration*** to go to the following interface. Set the device type to "Sub Door Station".

Enter the actual IP address of the main door station and door station no.

Door Station No.: enter the sub door station number (ranging from 1 to 99; 0 is main station number by default). Different sub door stations should have different door station number.



4. Tap ***Settings→More Settings→Configuration*** in the indoor station. Then enter the password of Admin to enter the following interface. Set the indoor station type (it should be set to "Indoor station"), room number, IP address of the main door station.



5. Call indoor station through your main or sub door station (See Call Resident for details).

Appendix 1-4 Multiple Door Stations Call Multiple Indoor Stations

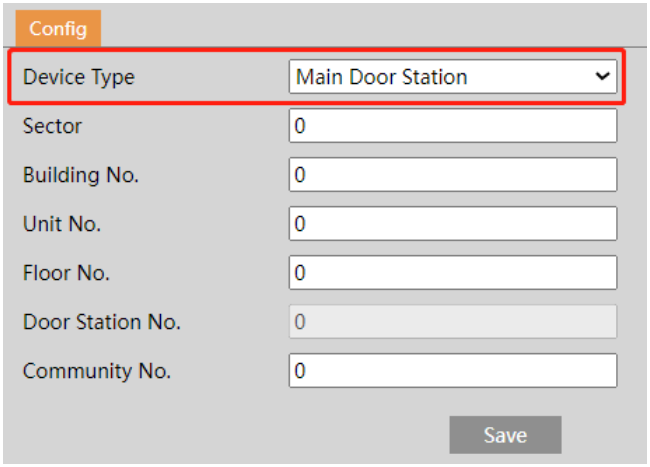
Application: Install multiple door stations (one is main door station, others are sub door stations) and multiple indoor stations (one is indoor station, others are indoor extensions). When main door station or sub door stations call indoor stations installed in different rooms, all indoor stations will respond at the same time. The resident can answer any one of the indoor stations and open the door.

The setting steps are as follows:

1. Connect your door stations and indoor stations to the same local network and then set their network parameters to the same network segment.

2. Main door station settings

Log in the web client of the door station. Click ***Config→Intercom→Number Configuration*** to go to the following interface. Set the device type to "Main Door Station".

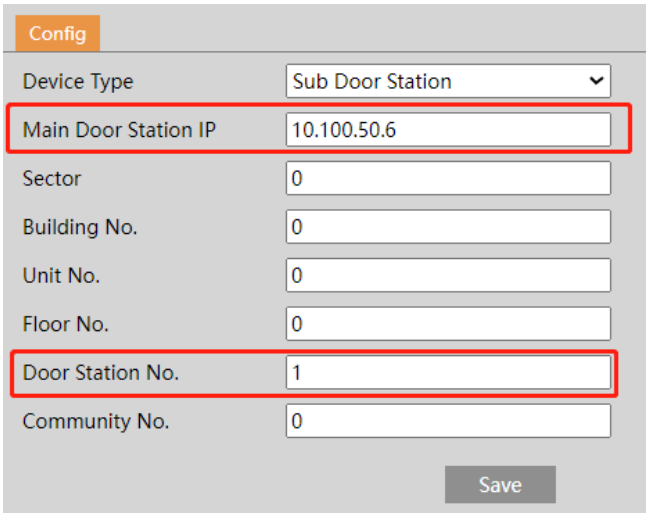


3. Sub door station settings

Log in the web client of the door station. Click ***Config→Intercom→Number Configuration*** to go to the following interface. Set the device type to "Sub Door Station".

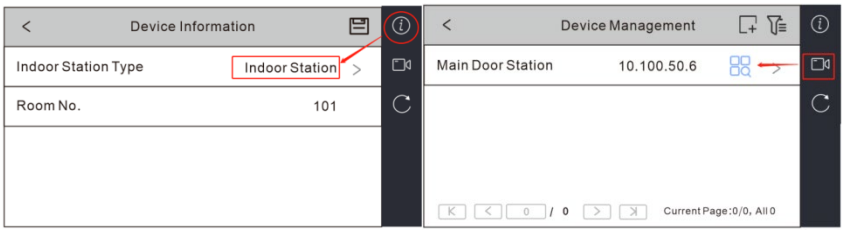
Enter the actual IP address of the main door station and door station no.

Door Station No.: enter the sub door station number (ranging from 1 to 99; 0 is main station number by default). Different sub door stations should have different door station number.



4. Indoor station settings

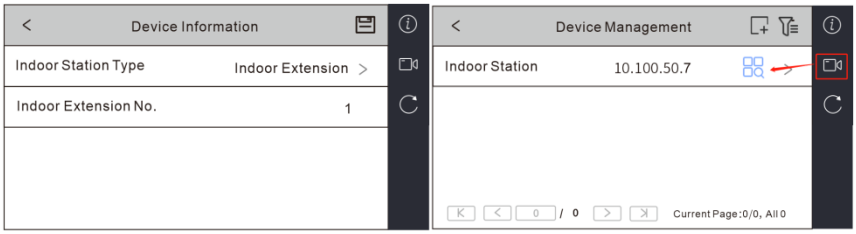
Tap ***Settings→More Settings→Configuration*** in the indoor station. Then enter the password of Admin to enter the following interface. Set the indoor station type (it should be set to "Indoor station"), room number, IP address of the main door station.



5. Indoor extension settings

Tap ***Settings→More Settings→Configuration*** in the indoor station. Then enter the password of Admin to enter the following interface. Set the indoor station type (it should be set to “Indoor Extension”), number (ranging from 1 to 5), IP address of the indoor station.

Note： For one indoor station, up to 5 indoor extensions can be configured. The indoor station number is 0 by default.



6. Call indoor stations through your main door station or sub door stations (See Call Resident for calling details). All indoor stations (including indoor station and extensions) will respond at the same time.

Appendix 2 Troubleshooting

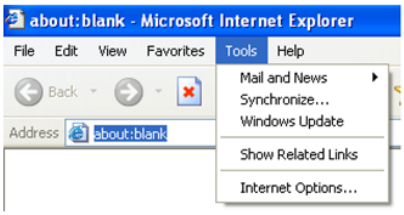
IP Scanner does not show any device.

Make sure that the PC that’s running Blue Scanner is on the same local network as the devices.

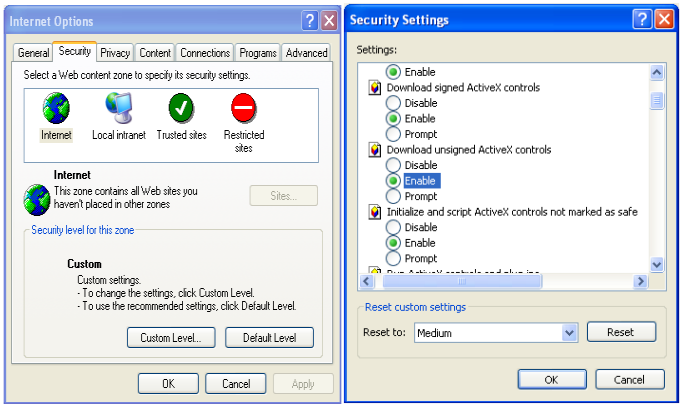
Internet Explorer cannot download ActiveX control.

IE browser may be set up to block ActiveX. Follow the steps below.

1. Open IE browser and then click Tools→Internet Options.



2.Select Security→Custom Level.
3. Enable all the options under “ActiveX controls and plug-ins”.
4. Click OK to finish setup.



No sound can be heard.
1. Audio input device is not connected. Please connect and try again.
2. Audio function is not enabled at the corresponding channel. Please enable this function.

Models: O2DB1

Federal Communications Commission (FCC) Statements

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

FCC Responsible Party:

Speco Technologies
200 New Highway
Amityville, NY11701
www.specotech.com