Video Intercom Door Station

GCN4000

User Manual

Please read these instructions carefully before operating the unit and keep for further reference.

genie

The following symbols or words may be found in this manual.

Symbols/Words	Description
⚠ **Warning**	Indicates a medium or low potential hazardous situation which , if not avoided, will or could result in slight or moderate injury
⚠ **Caution**	Indicates a potential risk which, if not avoided, will or could result in device damage, data loss, lower performance or unexpected results
☞ **Note**	Provides additional information to emphasize or supplement important points of the text.

About the Manual

- This manual is suitable for many models. All examples, screenshots, figures, charts, and illustrations used in the manual are for reference purpose, and actual products may be different with this Manual.
- Please read this user manual carefully to ensure that you can use the device correctly and safely.
- Within the maximum scope permitted by the law, the products described in this Manual (including hardware, software, firmware, etc.) are provided “AS IS”. The information in this document (including URL and other Internet site reference data) is subject to change without notice. This Manual may contain technical incorrect places or printing errors. This information will be periodically updated, and these changes will be added into the latest version of this Manual without prior notice.
- In this manual, the trademarks, product names, service names and company names that are not owned by our company are the properties of their respective owners.

Use of the Product

- This product should not be used for illegal purposes.
- The company does not allow anyone to use the Company's products to infringe the privacy, personal information, and portrait rights of others. The user shall not use this product for any illegal use or any prohibited use under these terms, conditions, and declarations. When using this product, the user shall not damage, disable, overload or obstruct any of the hardware of this product in any way, or interfere with the use of this product by any other users. Also, the user should not attempt to use the product or the software, by hacking, stealing the password, or any other means.

Electrical Safety

- This product is intended to be supplied by a Listed Power Unit, marked with 'Limited Power Source', 'LPS' on unit, output rated minimum 12V/2 A or POE 48V/ 350mA, no more than 2000m altitude of operation and Tma=60 Deg.C.
- As for the modes with PoE function, the function of the ITE being investigated to IEC 60950-1 standard is considered not likely to require connection to an Ethernet network with outside plant routing, including campus environment and the ITE is to be connected only to PoE networks without routing to the outside plant.
- Improper handling and/or installation could run the risk of fire or electrical shock.
- The product must be grounded to reduce the risk of electric shock.
- ⚠ Warning: Wear anti-static gloves or discharge static electricity before removing the bubble or cover of the camera.

Environment

- Heavy stress, violent vibration or exposure to water is not allowed during transportation, storage and installation.
- Avoid aiming the camera directly towards extremely bright objects, such as, sun, as this may damage the image sensor.
- Keep away from heat sources such as radiators, heat registers, stove, etc.
- Do not expose the product to the direct airflow from an air conditioner.
- Do not block any ventilation openings and ensure proper ventilation around the camera.
- Do not place the device in a damp, dusty extremely hot or cold environment, or the locations with strong electromagnetic radiation or unstable lighting.
- Make sure that no reflective surface is too close to the camera lens. The IR light from the camera may reflect back into the lens, resulting in image blur.

Operation and Daily Maintenance

- There are no user-serviceable parts inside. Please contact the nearest service center if the product does not work properly.
- Please shut down the device and then unplug the power cable before you begin any maintenance work.
- ⚠ Warning: All the examination and repair work should be done by qualified personnel.
- 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 cleaning (such as using cloth) may result in poor IR functionality and/or IR reflection.
- Always use a dry soft cloth to clean the device. If there is too much dust, use a cloth cleaning (such as using cloth) may result in poor IR/illumination LEDs functionality and/or IR/illumination LEDs reflection.
- The dome cover is an optical device, please don't touch or wipe the cover surface directly during installation and use. For dust, use an oil-free soft brush or hair dryer to remove it gently; for grease or finger print, use oil-free cotton cloth or paper soaked with detergent to wipe from the lens center outward. Change the cloth and wipe several

times if it is not clean enough.

Privacy Protection

- When installing cameras in public areas, a warning notice shall be given in a reasonable and effective manner and clarify the monitoring range.
- As the device user or data controller, you might collect the personal data of others, such as face, car plate number, etc. As a result, you shall implement reasonable and necessary measures to protect the legitimate rights and interests of other people, avoiding data leakage, improper use, including but not limited to, setting up access control, providing clear and visible notice to inform people of the existence of the surveillance area, providing required contact information and so on.

Disclaimer

- With regard to the product with internet access, the use of product shall be wholly at your own risks. Our company shall be irresponsible for abnormal operation, privacy leakage or other damages resulting from cyber attack, hacker attack, virus inspection, or other internet security risks; however, Our company will provide timely technical support if necessary.
- Surveillance laws vary from country to country. Check all laws in your local region before using this product for surveillance purposes. We shall not take the responsibility for any consequences resulting from illegal operations.

Cybersecurity Recommendations

- Use a strong password. At least 8 characters or a combination of characters, numbers, and upper and lower case letters should be used in your password.
- Regularly change the passwords of your devices to ensure that only authorized users can access the system (recommended time is 90 days).
- It is recommended to change the service default ports (like HTTP-80, HTTPS-443, etc.) to reduce the risk of outsiders being able to access.
- It is recommended to set the firewall of your router. But note that some important ports cannot be closed (like HTTP port, HTTPS port, Data Port).
- It is not recommended to expose the device to the public network. When it is necessary to be exposed to the public network, please set the external hardware firewall and the corresponding firewall policy.
- It is not recommended to use the v1 and v2 functions of SNMP.
- In order to enhance the security of WEB client access, please create a TLS certificate to enable HTTPS.
- Use black and white list to filter the IP address. This will prevent everyone, except those specified IP addresses from accessing the system.
- If you add multiple users, please limit functions of guest accounts.

- If you enable UPnP, it will automatically try to forward ports in your router or modem. It is really very convenient for users, but this will increase the risk of data leakage when the system automatically forwards ports. Disabling UPnP is recommended when the function is not used in real applications.
- Check the log. If you want to know whether your device has been accessed by unauthorized users or not, you can check the log. The system log will show you which IP addresses were used to log in your system and what was accessed.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

1. FCC compliance

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

2. FCC conditions:

- This device complies with part 15 of the FCC Rules. Operation of this product is subject the following two conditions:
- This device may not cause harmful interface.
- This device must accept any interference received, including interference that may cause undesired operation.

RoHS

The products have been designed and manufactured in accordance with Directive EU RoHS Directive 2011/65/EU and its amendment Directive EU 2015/863 on the restriction of the use of certain hazardous substances in electrical and electronic equipment.

2012/19/EU (WEEE directive): The Directive on waste electrical and electronic equipment (WEEE Directive). To improve the environmental management of WEEE, the improvement of collection, treatment and recycling of electronics at the end of their life is essential. Therefore, the product marked with this symbol must be disposed of in a responsible manner.

Directive 94/62/EC: The Directive aims at the management of packaging and packaging waste and environmental protection. The packaging and packaging waste of the product in this manual refers to must be disposed of at designated collection points for proper recycling and environmental protection.

REACH(EC1907/2006): REACH concerns the Registration, Evaluation, Authorization and Restriction of Chemicals, which aims to ensure a high level of protection of human health and the environment through better and earlier identification of the intrinsic properties of chemical substances. The product in this manual refers to conforms to the rules and regulations of REACH. For more information of REACH, please refer to DG GROWTH or ECHA websites.

Table of Contents

1 Introduction 1
1.1 Main Features 1
1.2 Description of Buttons 1

2 Network Connection 3
2.1 Wired Network Connection 3
2.2 Wi-Fi Connection 6
2.3 WAN 7

3 Live View via Web 9

4 Configuration via Web 11
4.1 Face Recognition Settings 11
4.1.1 Face Comparison Settings 11
4.1.2 Face Database Management 13
4.1.3 Face Match View 15
4.2 Door Station Settings 16
4.3 Video Intercom Operation 17
4.3.1 Call Resident 17
4.3.2 Call Platform 17
4.3.3 Call APP 18
4.3.4 Configuring Contacts 19
4.4 Unlock Door 20
4.4.1 Unlock by Super PIN Code 20
4.4.2 Unlock by Successful Face Comparison 20
4.4.3 Unlock by Swiping Card 20
4.4.4 Unlock by Combination Mode 20
4.4.5 Unlock via Web 21
4.4.6 Unlock via APP 22
4.5 Access Control System Settings 22
4.5.1 Local Settings 22
4.5.2 Door Lock Settings 23
4.5.3 Door Contact Settings 25
4.5.4 Wiegand Settings 26
4.5.5 Tampering Alarm Settings 26
4.5.6 Card Reader Settings 27
4.5.7 RS485 Settings 28
4.5.8 Elevator Settings 28
4.6 System Settings 28
4.6.1 Basic Information 28
4.6.2 Date and Time 29

4.6.3 Local Config 30
4.6.4 Storage 30
4.7 Image Configuration 33
4.7.1 Display Configuration 33
4.7.2 Video / Audio Configuration 35
4.7.3 OSD Configuration 36
4.8 Alarm Configuration 37
4.8.1 Video Exception 37
4.8.2 Exception Alarm 39
4.8.3 Alarm In 40
4.8.4 Alarm Out 42
4.9 Network Configuration 43
4.9.1 TCP/IP 43
4.9.2 Port 44
4.9.3 Server Configuration 45
4.9.4 Onvif 45
4.9.5 DDNS 46
4.9.6 802.1x 47
4.9.7 RTSP 48
4.9.8 UPnP 49
4.9.9 Email 49
4.9.10 FTP 50
4.9.11 HTTPS 51
4.9.12 P2P 52
4.9.13 QoS 52
4.9.14 Wi-Fi Settings 53
4.9.15 SIP 54
4.10 Security Configuration 55
4.10.1 User Configuration 55
4.10.2 Online User 56
4.10.3 Block and Allow Lists 57
4.10.4 Security Management 57
4.11 Maintenance Configuration 58
4.11.1 Backup and Restore 58
4.11.2 Reboot 59
4.11.3 Upgrade 59
4.11.4 Operation Log 59

5 Search 61

5.1 Image Search 61
5.2 Video Search 63
5.2.1 Local Video Search 63
5.2.2 SD Card Video Search 64

6 Face Recognition Result Search 66

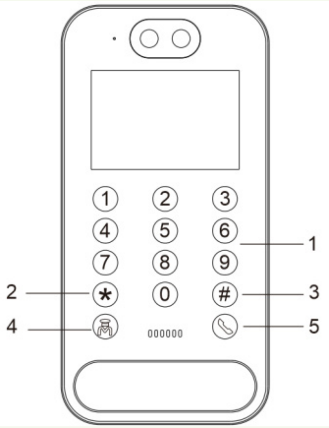
Appendix
67 Appendix 1 How to Call Indoor Station 67
Appendix 1-1 One Door Station Calls One Indoor Station 67
Appendix 1-2 One Door Station Calls Multiple Indoor Stations 68
Appendix 1-3 Multiple Door Stations Call One Indoor Station 69
Appendix 1-4 Multiple Door Stations Call Multiple Indoor Stations 71
Appendix 2 Troubleshooting 75

1 Introduction

1.1 Main Features

- Max. resolution: 2MP (1920×1080)
- H.265+/H.265/H.264+/H.264/MJPEG coding
- Face recognition distance: 0.3m-2m
- Support face detection technology distinguishing real faces from non-real face spoof attacks
- Support 3D DNR, HWDR, BLC, HLC, Defog, etc.
- Support multiple door opening modes (by swiping card, by password, by face recognition, etc.)
- Support door opening by indoor station or by mobile APP
- Support copy-prevention for IC card; support IC card encryption
- Support anti-tampering alarm; support triggering alarms when the door is not secured or the door is broken by others
- Support calling indoor station/APP
- Support card reader access via RS485 interface
- Support 2.4G Wi-Fi; Support P2P function
- Support remote surveillance via mobile APP, web browser or tablet PC
- Intelligent analytics: video exception detection, face detection, face capture, face comparison

1.2 Description of Buttons



No.	Description
1	Keypad
2	Press it to delete the input number or return to the live view interface
3	#
4	Press it to call the control center/indoor station/APP
5	Call button

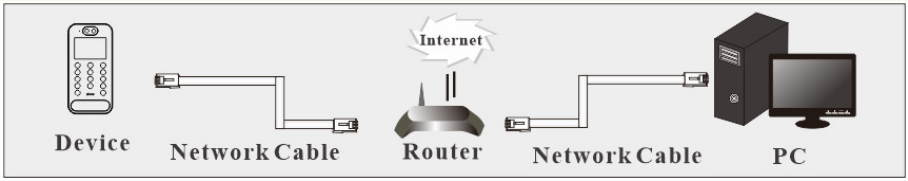
2 Network Connection

2.1 Wired Network Connection

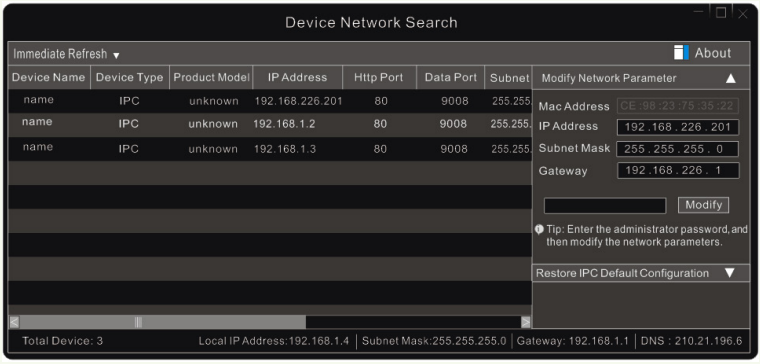
Here we take device access via Web browser for example.
Web browser: IE (plug-in required)/ Firefox/Edge/ Google Chrome
It is recommended to use the latest version of these web browsers.
The menu display and operation of the camera may be slightly different by using the browser with plug-in or without plug-in. Installing the 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-Tool**
Network connection:

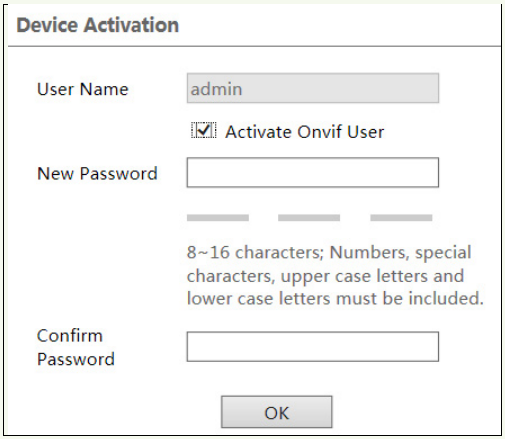


Make sure the PC and device are connected to the same local network and the IP-Tool is installed in the PC.
② Double click the IP-Tool icon on the desktop to run this software as shown below:



If there are many devices, please find your device via its MAC address.

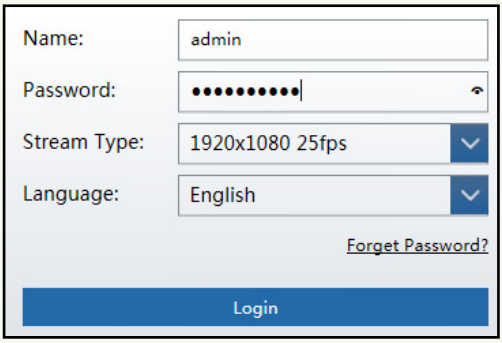
③Double click the IP address and then the system will pop up the IE browser to connect IP-CAM. After you read the privacy statement, check and click “Already Read”. Then activate the device.



The default username is “admin”. Please self-define the password according to the tip.

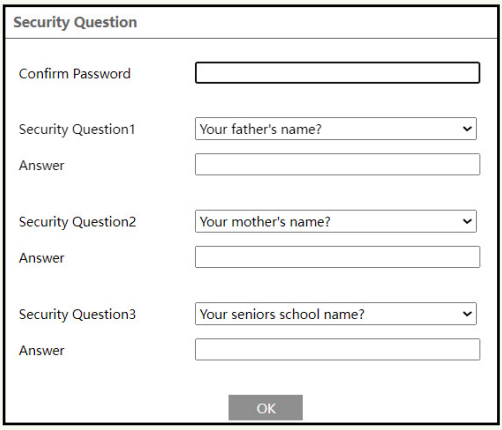
Note: It is highly recommended to use the strong password for your account security. If you want to change your password level, you can go to **Config→Security Management →Password Security** interface to change the level and then modify the admin password (Go to **Config→User**).

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→Onvif**)
When you connect the camera through the ONVIF protocol in the third-party platform, you can use the username and the password set to connect.
After that, follow directions to download, install and run the Active X control if prompted. Re-connect your camera via IE browser and then a login box will appear.



Please enter the user name (admin) and password. Then select the stream type and language as needed.

The security questions must be set after you click “Login” button. It is very important for you to reset your password. Please remember these answers.



If you forget the admin password, you can reset the password by clicking **Forget Password** on the login page. Then you can reset the password by the security questions and answers you set.

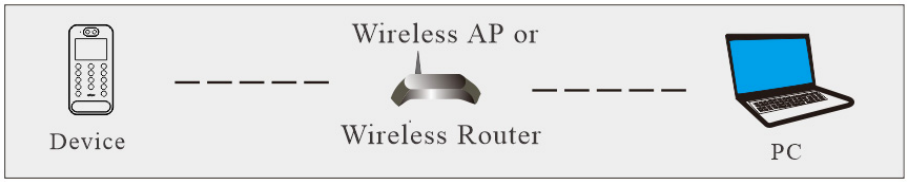
You can set the account security question during the activation, or you can go to ***Config→ Security→ User***, click ***Safety Question***, select the security questions and input your answers.

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

1) Open your phone’s APP store and search “Superlive Plus”. Then install the mobile APP (Superlive Plus) on 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) Tap “Add Device” in the server list interface of the APP. Scan the QR Code (log in via web and then go to ***Config→System →Basic Information***) and then enter the security code (DO NOT use the username and password, or the device cannot be added successfully) to add the device to the server list of the APP.

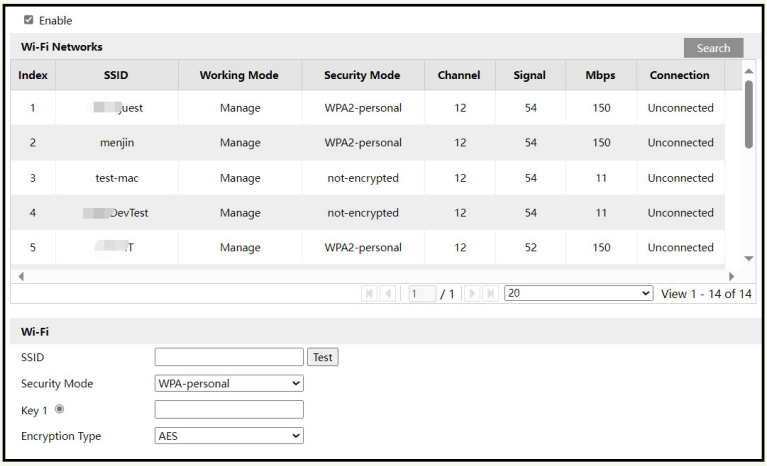
2.2 Wi-Fi Connection



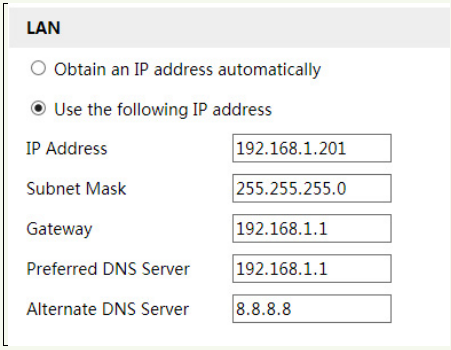
① Use the network cable to connect the device and wireless router or AP.

② Connect to the above wireless network with your PC. Then run the IP-Tool on your PC and then find the device via its MAC address. Then double click it. This will bring you to the login interface of the camera. Enter the default username and password to log in.

③ Click ***Config→Network→WIFI*** to go to the following interface. Enable WI-FI, 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”.



Note: It is recommended to set the network parameters manually, because the IP address may be changed by obtaining an IP address automatically.
Then click "Test" to check whether the wireless network is connected. After successful connection, click "Save" to save the settings.

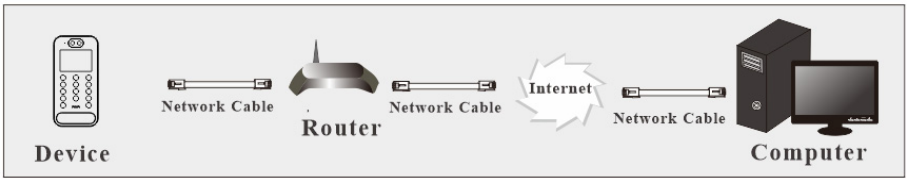
- Pull the network cable out of the camera.
- Run the IP-Tool and find the camera through IP address or MAC address. Then double click it listed in the IP-Tool or enter the IP address of the camera in the address bar of the web browser to access the camera.

After that, you can also use the downloaded APP to scan the QR code of the device and then enter the security code to add it to the server list of the APP.

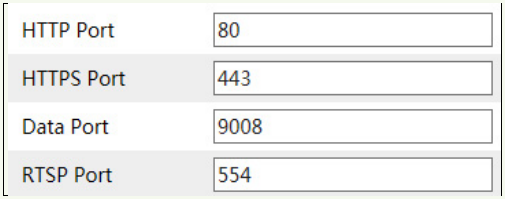
2.3 WAN

➢**Access via P2P**
Connect and activate the device according to the above-mentioned steps (See 2.1). Enable P2P (click **Config→Network→P2P**) and then enter www.autonat.com to visit IE client remotely. (This function is only available for IE browser)
Note: Different regions may have different login addresses. Please contact your dealer for details.

- **Access through the router or virtual server**

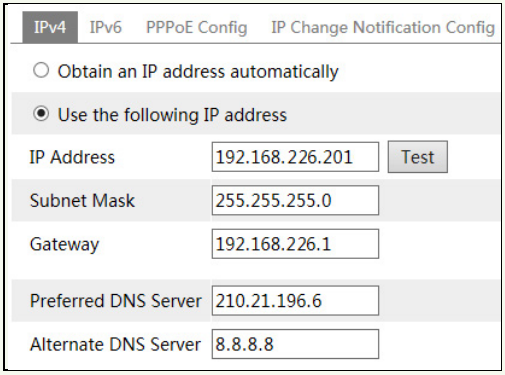


To remotely access the device via Web, the setting steps are as follows:
Make sure the camera is well connected via LAN and then log in the camera via LAN and go to ***Config→Network→Port*** menu to set the port number.



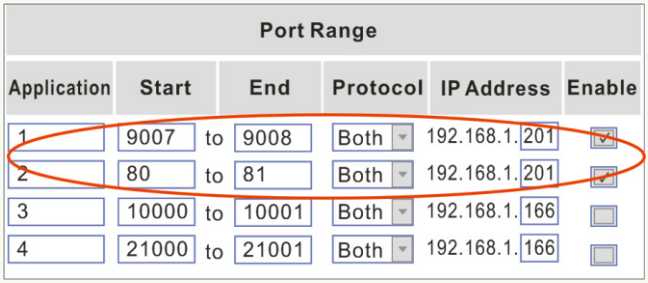
Port Setup

- Go to ***Config →Network→TCP/IP*** menu to modify the IP address.



IP Setup

- Go to the router's management interface through IE browser to forward the IP address and port of the camera in the "Virtual Server".

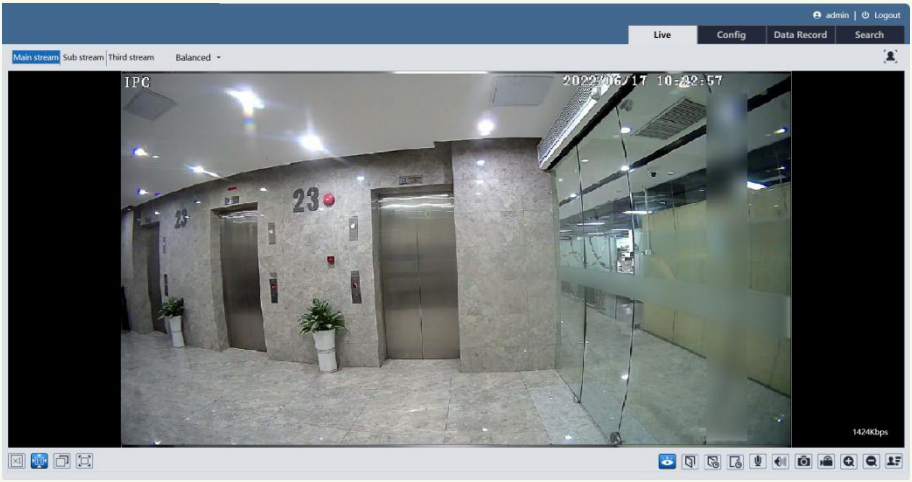


Router Setup

- Open the IE browser and enter its WAN IP and http port to access. (for example, if the http port is changed to 81, please enter "192.198.1.201:81" in the address bar of web browser to access).

3 Live View via Web

After logging in, the following window will be shown.



The following table is the instructions of the icons on the live view interface.

Icon	Description	Icon	Description
	Original size		Zoom in
	Fit correct scale		Zoom out
	Auto (fill the window)		Face detection
	Full screen		Color abnormal indicator
	Start/stop live view		Abnormal clarity indicator
	Open the door		Scene change indicator
	Normally open		Tampering alarm indicator
	Normally close		Alarm input indicator
	Start/stop two-way audio		Face detection indicator
	Enable/disable audio		SD card recording indicator
	Snapshot		Door contact alarm indicator
	Start/stop local recording		

* Those smart alarm indicators will flash only when the camera supports those functions and the corresponding events are enabled.
* Plug-in free live view: the local recording is not supported and the preview mode switch (real-time/balanced/fluent mode) is not available too.
* To set the stream profile, select Main stream, Sub stream, and Third stream. Go to ***Configure*** →***Video/Audio*** to set the resolution for each stream as needed.

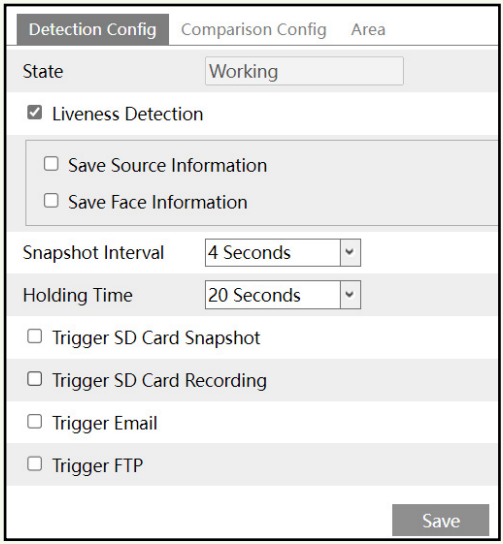
4 Configuration via Web

In the Webcam client, choose “Config” to go to the configuration interface.
Note: Wherever applicable, click the “Save” button to save the settings.

4.1 Face Recognition Settings

4.1.1 Face Comparison Settings

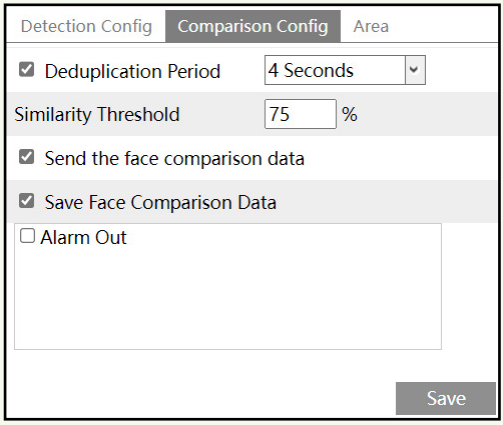
1. Go to ***Config→Face →Face Match Config*** interface.



Enable liveness detection. If enabled, the system can distinguish real faces from non-real face spoof attacks.
Enable “Save Source Information” or “Save Face Information”. Save Source Information: if checked, the whole picture will be saved to the SD card when detecting a face. Save Face Information: if checked, the captured face picture will be saved to the SD card when detecting a face. **Note**: To save images to the local PC, please enable the local smart snapshot storage first (***Config→System →Local Config***). To save images to the SD card, please install an SD card first.
Snapshot Interval: If 4 seconds is selected, the camera will capture the same target once every 4 seconds during its continuous tracking period.

Set alarm holding time and alarm trigger options. **Holding Time**: The alarm holding time of face detection **Trigger SD Card Snapshot:** If selected, the system will capture images when detecting a face and save the images on an SD card. **Trigger SD Card Recording:** If selected, the video will be recorded on an SD card when detecting a face. **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" is checked, the captured pictures will be sent to the FTP server address. Please refer to the FTP configuration section for more details.

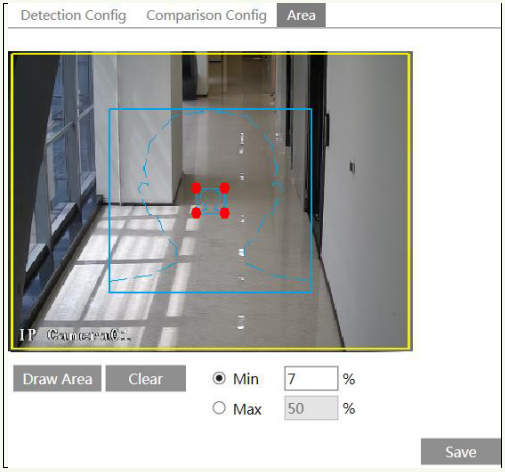
5. Set face comparison options.



Deduplication Period: In the set period, delete the repeated comparison results.
Similarity threshold: When the similarity of the captured face picture and the face picture added into the face database exceeds the similarity threshold, alarms will be triggered.
Send the face comparison data: if disabled, the face comparison result will not be displayed in the live interface of the web client.
Save face comparison data: if enabled, the comparison data will be saved and you can search the face recognition result from the data record interface. Note that an SD card must be inserted. If disabled, the face comparison data will not be searched in the data record interface.

Alarm out: Please select the alarm out triggered by face comparison as needed.

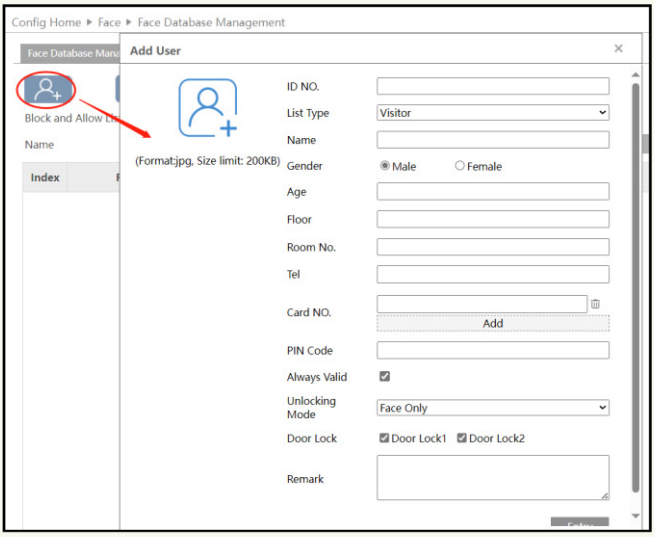
6. Set alarm detection area.



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).

4.1.2 Face Database Management

Click the “Face Database Management” tab. This will enter the following interface.



There are four ways to add face pictures.

Adding face pictures one by one

Click to select face pictures and add the user to PC. Please select the picture according to the specified format and size limit. After that, fill out the relevant information of the face picture and click “Entry” to add.

List Type: Visitor, allow list, block list, and administrator.

Unlocking mode: please select face only, only swiping card or other combination unlocking mode.

Note: If “Swiping card” is included, the card No. should be entered by swiping card on the device when adding a person. If “Only Swiping Card” is selected, there is no need to add a face picture. Each person can add a maximum of 5 cards.

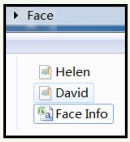
Adding multiple face pictures at a time

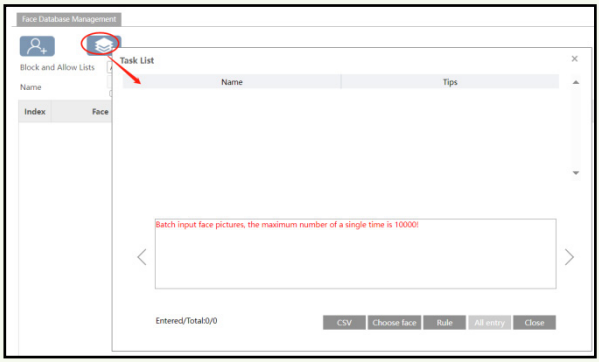
Click and then add multiple face pictures once according to the rules.

Here is the example of the people information file (.csv).

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	(01)Name	(02)Gende	(03)Birthd	(04)PIN C	(05)Unlocl	(06)List ty	(07)Card NO.(A max	(08)Tel	(09)Remar	(10)ID NC	(11)D	(12)Start Time	(13)End Time	(14)Floor	(15)Room	(16)Picture Name	
2	user	1	2018/1/1	123456	1	1	10001#10002#10003	18888888888	Remark	1111	1#2	2021/1/1 0:00	2022/1/1 0:00	1	1	user.jpg	
3																	

It is recommended to put the people information file and images into the same directory as shown on the below left.



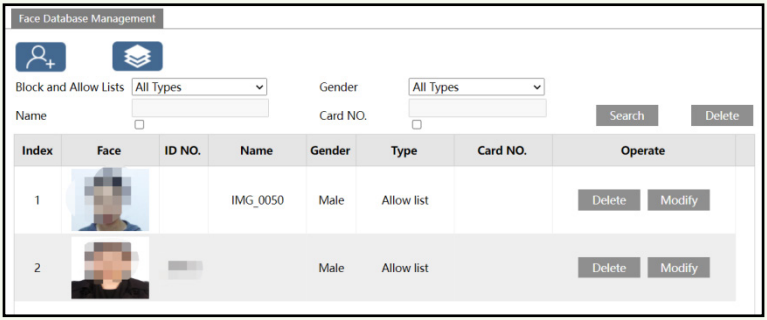


Click “CSV” to select the directory and then click “Choose face” to select the faces you want to import. Then click “All entry” to upload.

Note: If people enter by only swiping card, only people information file need to import. There is no need to add face pictures.

- Add face pictures by using face album management tool
- Add the captured picture in the live mode (See **Add captured face pictures to the face database**).

After adding face pictures, you can search them by name, gender, ID number and so on.



Click “Modify” to change people’s information and click “Delete” to delete this face picture.

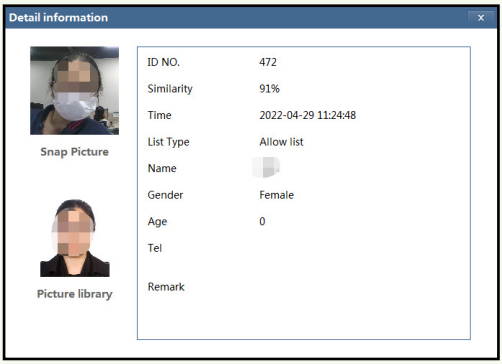
4.1.3 Face Match View

After all face comparison settings are set successfully, enter the live view interface. Click to view the captured face pictures and face comparison information.

Area ①: captured face pictures; area ②: face comparison area

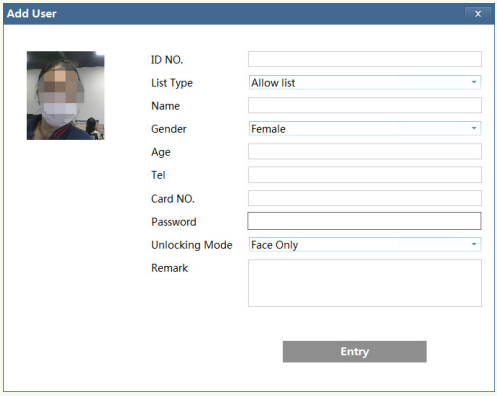
●View the comparison details

In area ②, click the compared face picture to bring the following window. In this interface, you can view the detailed comparison information.



●Add captured face pictures to the face database

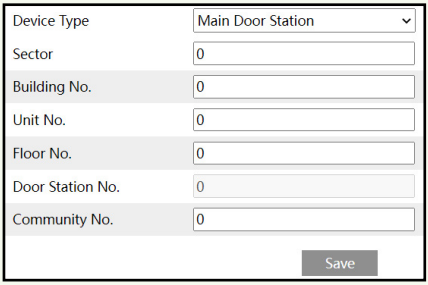
Click a captured picture in area ①. This will bring a face picture adding box.

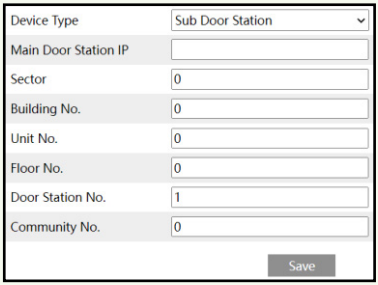


Fill out the relevant information and click “Entry” to add this face picture.

4.2 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.

Each unit should install 1 main door station. A maximum of 9 sub door stations can be linked to the main door station.

The sector no., building no., unit no., and community no. of sub door station must be the same as the main door station.

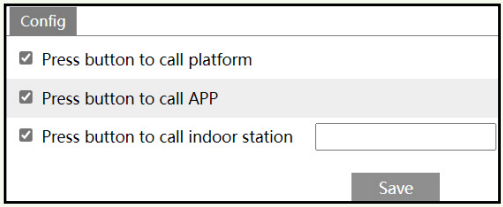
4.3 Video Intercom Operation

4.3.1 Call Resident

- Press any digit button on the main or sub door station to enter the calling page.

Enter the room No. and press to call resident.

- Press button to call indoor station directly. Go to ***Config → Intercom*** 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.

4.3.2 Call Platform

Press on the main or sub door station to call the platform. Please enable this function

before using this button. Go to ***Config→Intercom*** interface. Check “Press button to call platform” and then save.

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

4.3.3 Call APP

➢Press one button to call the administrator account of the APP

Press the button on main or sub door station to call the APP. Please enable this function before using this button. Go to ***Config→Intercom*** interface. Check “Press button to call APP ” and then save.

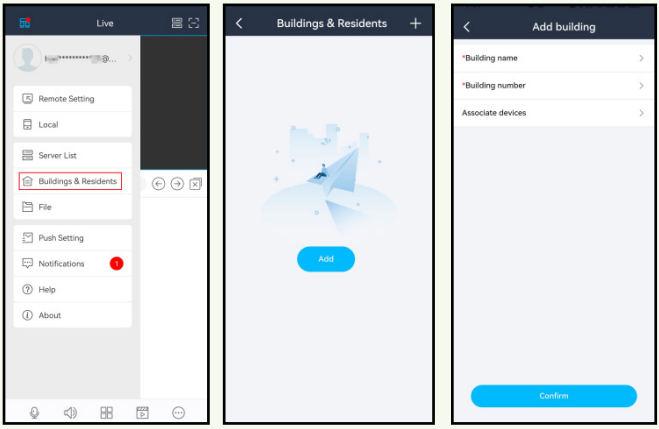
Note: Please add the door station to the mobile APP before calling.

In addition, these three calling mentioned above can be checked simultaneously. After pressing the APP/platform/indoor station will respond at the same time. If one of them clicks “Answer ”, others will be hung up automatically.

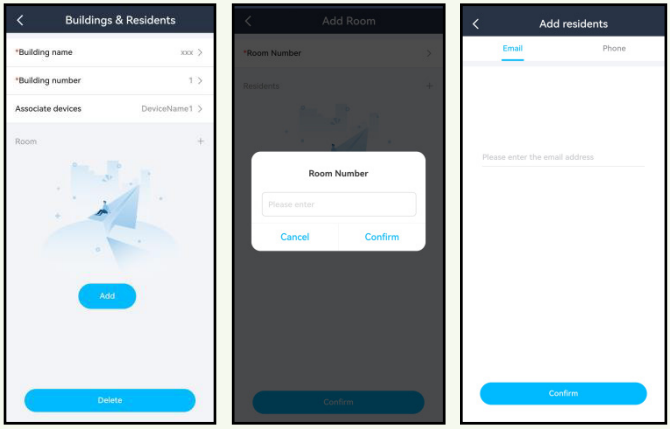
➢Press the pre-defined room number to call the resident account of the APP

A visitor can call the APP of the resident by pressing the corresponding room number on the door station. Before calling, the administrator needs to set the building number, room number and the resident’s account in the APP. The setting steps are as follows:

1. Log in the APP account of the administrator and scan the QR code of the device. Then add the device by entering the security code. Go to ***Config→System→Basic Information*** to get the QR Code and security code.
2. In the “Buildings & Residents” tap “Add” to add the building name, building number and link your door station.



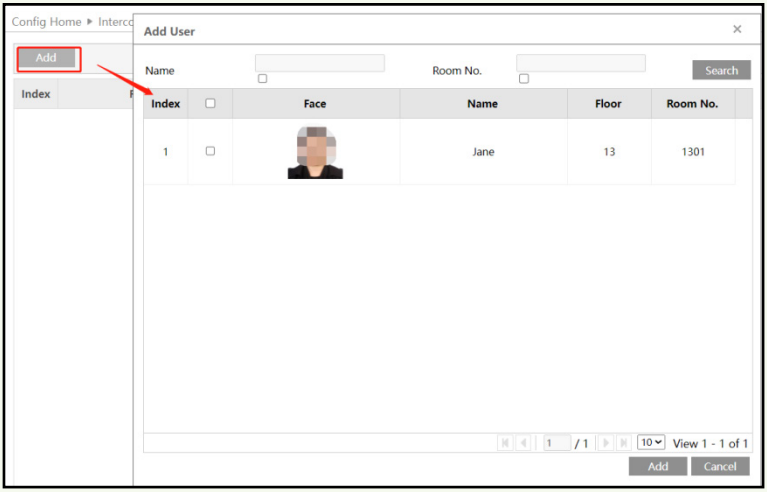
4. Add the room number and bind the resident's account.



5. Press the set room number and on the door station to call the resident.
6. In the APP, the resident can receive or reject the call as needed.

4.3.4 Configuring Contacts

Before you adding a person to the contacts, you need set the floor and room number when adding a person to the face database. Go to ***Config→Intercom→Contacts***. You can view the person information you have added to the face database.



Select the person you want to add into the contacts and click "Add". After the person is added to the contacts, visitors can find the person's room number in the door station by hitting the

"*" button.

4.4 Unlock Door

4.4.1 Unlock by Super PIN Code

Press any digit button on the main or sub door station to enter the calling page. Enter Super PIN Code# to directly open the door. You can go to ***Config→Access Control→Door Lock →PIN Code Setting*** to set and save the super PIN code.

4.4.2 Unlock by Successful Face Comparison

When the unlocking mode is set to "Only Face", the door will be opened by successful face comparison. Please set the compared list type when adding persons as needed (See Door Lock Settings for details).

4.4.3 Unlock by Swiping Card

When the unlocking mode is set to "Only Swiping Card", the door will be opened by swipe a card.

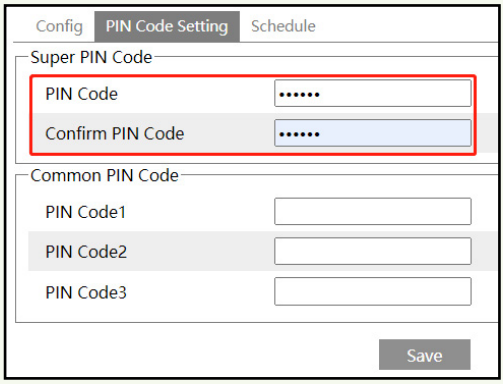
4.4.4 Unlock by Combination Mode

●Face Comparison + PIN Code

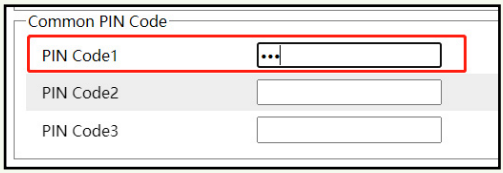
When the unlocking mode is set to "Face Comparison and PIN Code" (To set the unlocking mode, see Face Database Management for details), you need to enter PIN code# after successful face comparison.

Password: You can enter one of the following three types of passwords.

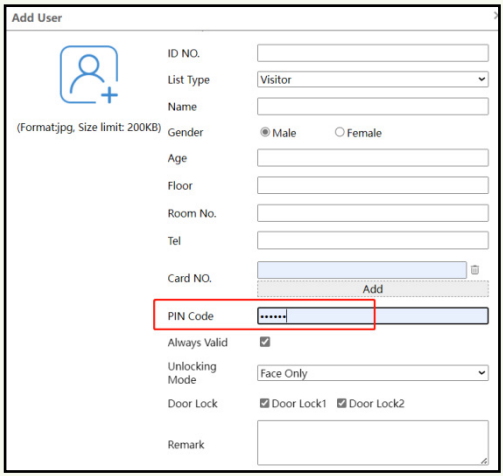
① Super PIN Code (***Config→Access Control→Door Lock→PIN Code Setting***)



② Common PIN Code, any one of them



③ The PIN code you entered when adding a person



When adding a person, you can set the validity period for the PIN code. Uncheck “Always Valid” to set the start and end time as needed.

●Face Comparison + Swiping Card

When the unlocking mode is set to “Face Comparison and Swiping Card” (To set the unlocking mode, see Face Database Management for details), you need to swipe a card after successful face comparison.

●Comparison or Swiping Card

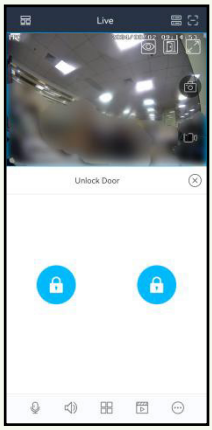
When the unlocking mode is set to “Face Comparison or Swiping Card” (To set the unlocking mode, see Face Database Management for details), you can enter by swiping a card or scanning your face.

4.4.5 Unlock via Web

In the live view interface of the Web client, click to unlock the door.

4.4.6 Unlock via APP

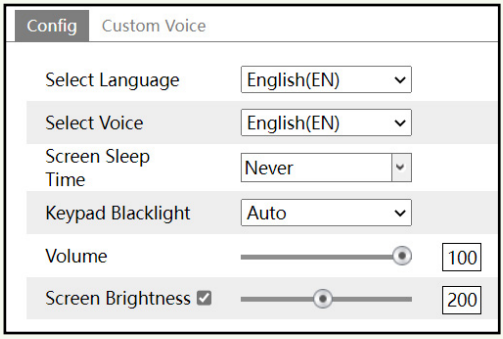
With the live view interface as shown below, tap the image and then to open the door as needed.



4.5 Access Control System Settings

4.5.1 Local Settings

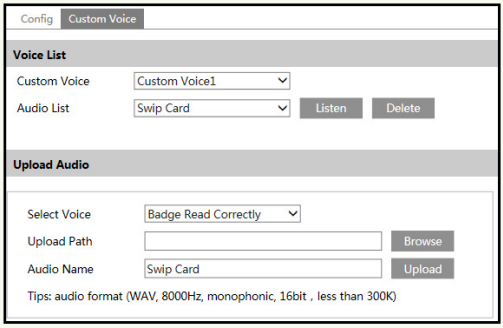
Click ***Config→Access Control→Access Control System Config*** to go to the following interface.



Select Language: Select the screen display language on the panel/tablet.
Select Voice: Select the language of the voice prompt or the custom voice prompt.
Screen Sleep Time: Set how long the screen display will turn off after no person appears. Please set it as needed. In a sleep state, once a person is detected by the panel, it will be aroused immediately.
Keypad Backlight: Select “Auto”, “Manual” or “Off” as needed.

Volume: Set the volume of the voice prompt.
Screen Brightness: Set the brightness of the screen of the terminal (panel/tablet). The adjustable range is from 150 to 255.

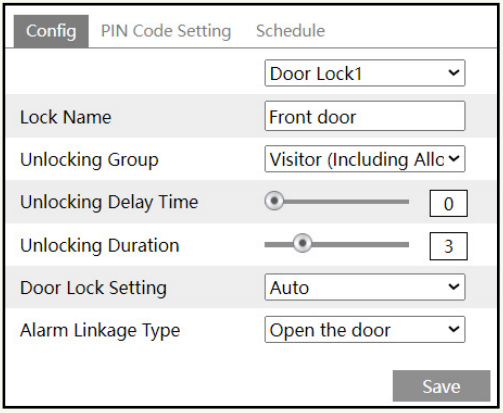
●**Customizing Voice**
If you are dissatisfied with the default voice prompt, you can customize your own voice prompt. In the above interface, click "Custom Voice" tab to go to the following interface.



Select the voice you want to replace and then click "Browse" 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.

4.5.2 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.



Lock Name: Set the lock name as needed.

Unlocking Group: Allow list, visitor (including allow list), stranger (including visitor and allow list).

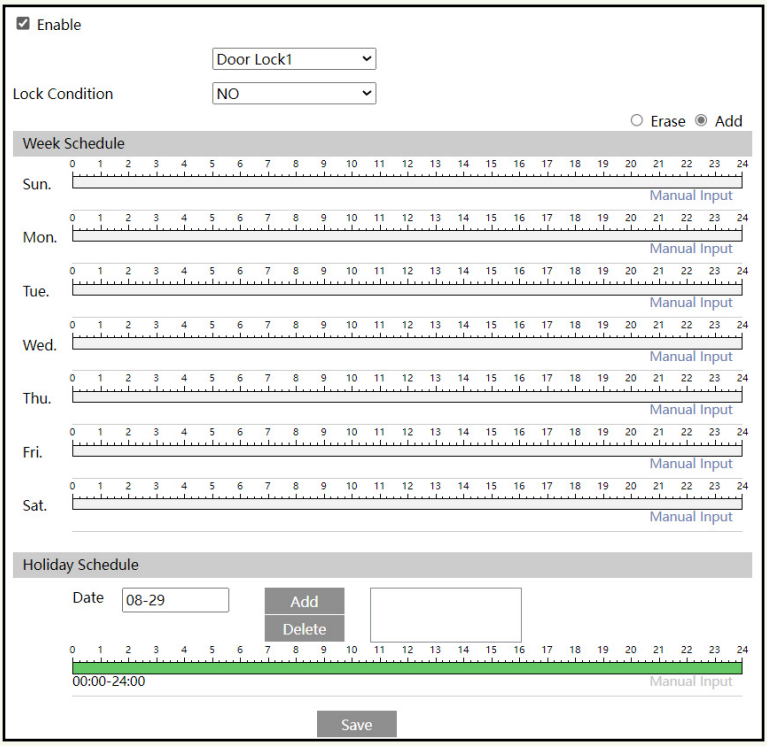
Unlocking Delay Time: Set the door unlocking delay time. The time range is from 0 to 10 seconds. For example, the unlocking mode is “Swiping Card” and the delay time is set to “2” seconds; the door will be opened 2 seconds later after successfully reading card.

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.

Door Lock Setting: 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”.

Alarm Linkage Type: Open or close the door when an alarm is triggered. Please select it as needed.

Schedule Settings: The door can be normally opened or closed within the schedule time. Select “NO” or “NC” and then set the schedule. Enable the schedule first.



Weekly Schedule

Set the schedule time from Monday to Sunday for a single week. Each day is divided into

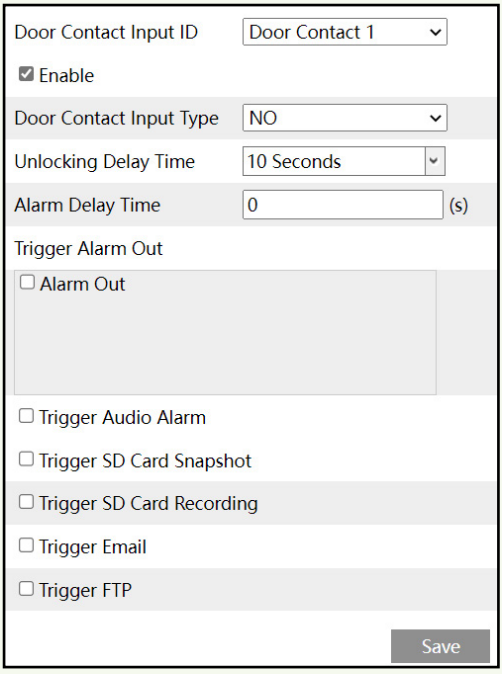
one-hour increments. Green means scheduled. Blank means unscheduled. “Add”: Add the schedule for a special day. Drag the mouse to set the time on the timeline. “Erase”: Delete the schedule. Drag the mouse to erase the time on the timeline.
Manual Input: Click it for a specific day to enter specific start and end times. This adds more granularities (minutes).

Day Schedule

Set the schedule time for a special day, such as a holiday.
Note: Holiday schedule takes priority over weekly schedule.

4.5.3 Door Contact Settings

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

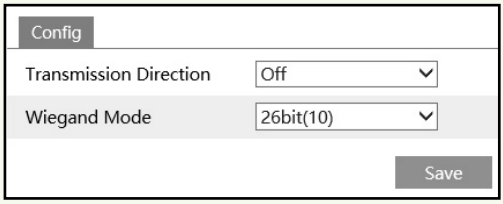


Door Contact Input ID: Choose door contact 1 or 2.
Door Contact Input Type: NO or NC
Unlocking Delay Time: the allowable unlocking time. For example, if it is set to 10 seconds, alarms will be triggered when the door is not closed after 10 seconds.
Alarm Delay Time: set the alarm delay time when faults 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.
Alarm Out: If selected, this would trigger an external relay output that is connected to the camera when faults of the door contact are detected.
Trigger Audio Alarm: if enabled, you will hear the warning sound when the door contact alarm is triggered.
Trigger SD Card Snapshot: If selected, the system will capture images when detecting a face and save the images on an SD card.
Trigger SD Card Recording: If selected, the video will be recorded on an SD card when detecting a face.
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" is checked, the captured pictures will be sent to the FTP server address. Please refer to the FTP configuration section for more details.
The setup steps of other alarm trigger options are similar to the face detection settings. Please refer to the face detection settings section for details.

4.5.4 Wiegand Settings

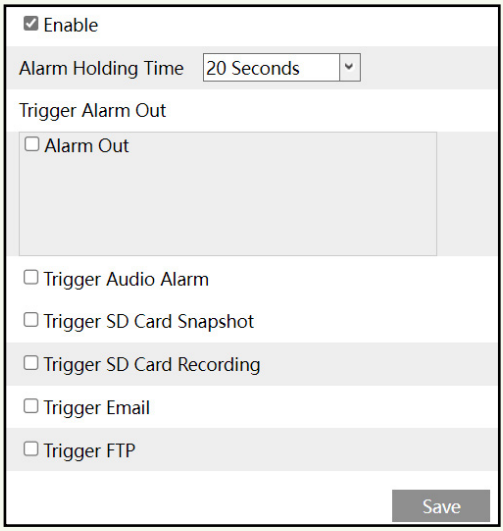
Click ***Config→Access Control→Wiegand Config*** to go to the following interface.



Transmission Direction: 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.

4.5.5 Tampering Alarm Settings

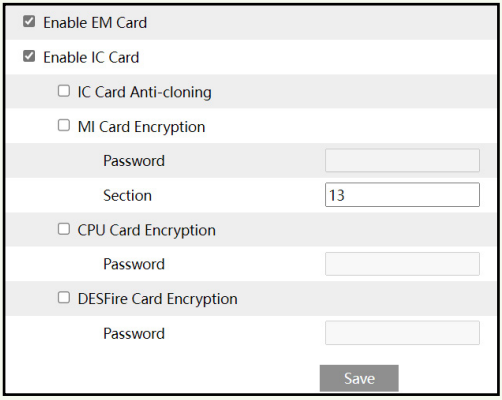
In order to avoid the removal or damage by the external force, the tampering alarm can be set for the terminal. Click ***Config→Access Control→Tampering Alarm Setting*** to go to the following interface.



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 the external force.
The setup steps of other alarm trigger options are similar to the face detection settings. Please refer to the face detection settings section for details.

4.5.6 Card Reader Settings

In the card reader interface, you can choose the card type as needed, including EM card and IC card.



If “IC Card” is enabled, you can enable IC card anti-cloning, MI card encryption, CPU card encryption or DESFire Card encryption as needed.

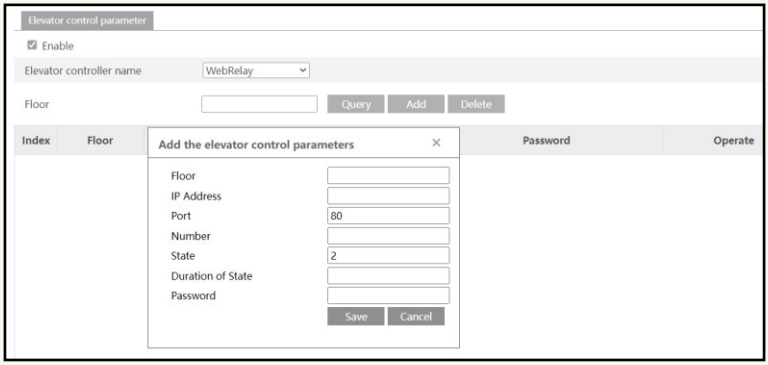
Note: You need to use a professional card enroller to encrypt the cards. If you want to use card encryption function, please purchase a card enroller and set in advance.

4.5.7 RS485 Settings

Click ***Config→Access Control→RS485*** to go to the RS485 interface.
You can connect a RS485 card reader or access control system through the RS485 interface of your door station as needed. Please set the external device type according to the external device you connect. For other parameters of RS 485, it is recommended to use the default settings.

4.5.8 Elevator Settings

Currently, the device only supports Web Relay elevator controller. The setting steps are as follows:
1. Set the room number and floor information of the resident you add in the face database.
2. Go to ***Config→Access Control→Elevator Config*** interface. Enable the elevator control function. Then click "Add" to add the floor number and other parameters. After saving the settings, a command string of the floor will be generated automatically.

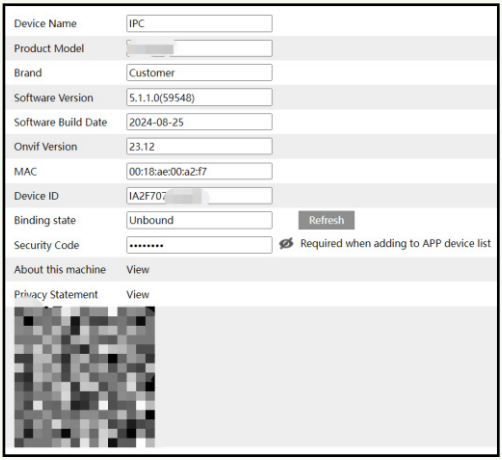


3. When a visitor arrives, the resident hits the unlock button on the indoor station, and also sends a command string to the web relay, which in turn gives the visitor access to the floor the resident lives on.

4.6 System Settings

4.6.1 Basic Information

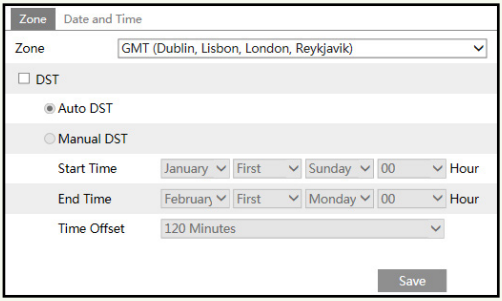
In the "Basic Information" interface, the system information of the device is listed.



In the above interface, you can view the product model, brand, software version, software build date, onvif version, MAC adress, device ID, QR Code security code and so on. You can scan the QR code and enter the security code to add the device to the surveillance APP. In addition, you can unbind the device from the account of the APP by clicking the "Unbind" button. Click to view the security code which is used to add the device to the APP.

4.6.2 Date and Time

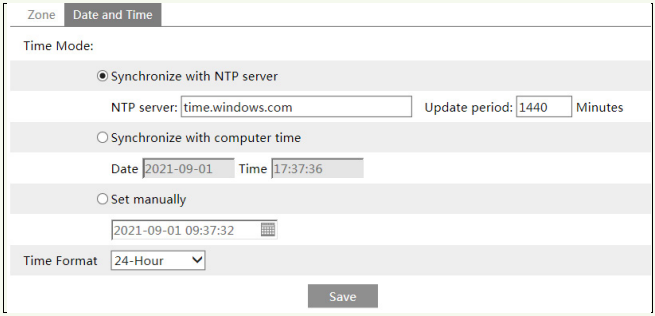
Go to ***Config→System →Date and Time***. Please refer to the following interface.



Select the time zone and DST as required.

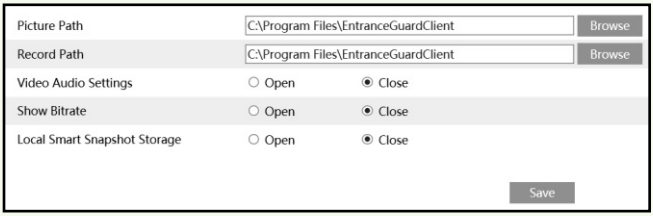
Note: The time zone of the camera and the computer must be the same. It is recommended to modify the time zone of the camera according to the time zone of the computer. If the time zone of the computer is modified, the current web client needs to be closed. Then re-open it and log in again.

Click the "Date and Time" tab to set the time mode and time format.



4.6.3 Local Config

Go to ***Config→System →Local Config*** 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 the bitrate display in the recorded files.

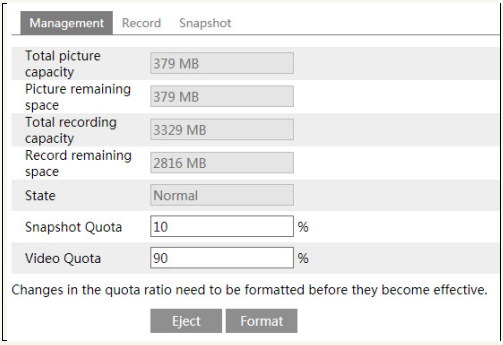


Additionally, “Local smart snapshot storage” can be enabled or disabled here. If enabled, the captured pictures triggered by smart events will be saved to the local PC.

Note: when you access your camera by the web browser without the plug-in, only Show Bitrate can be set in the above interface.

4.6.4 Storage

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



●SD Card Management

Click the "Format" button to format the SD card. All data will be cleared by clicking this button.

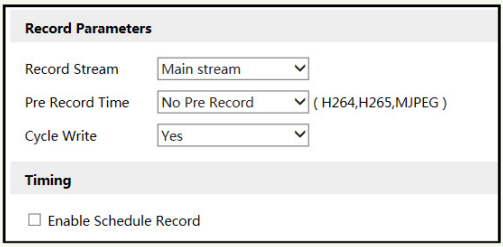
Click the "Eject" button to stop writing data to the SD card. Then the SD card can be ejected safely.

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.

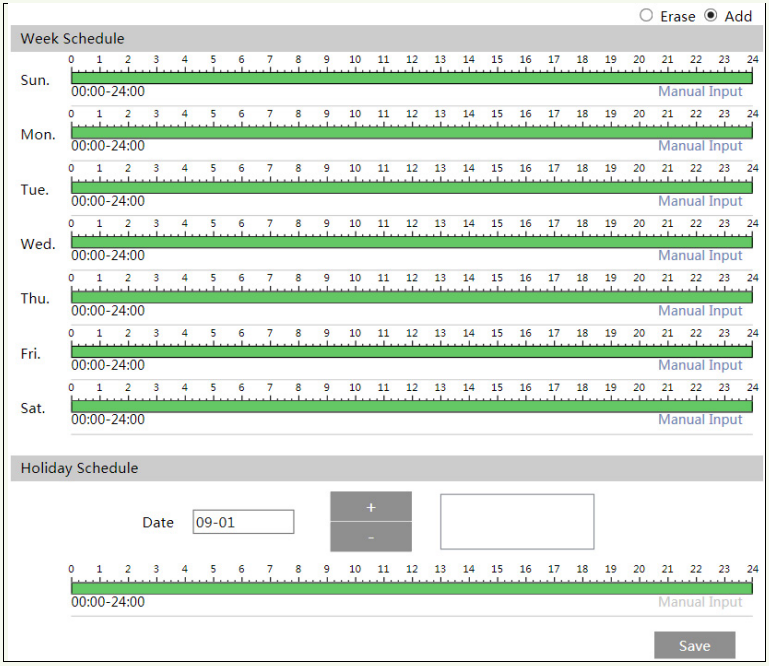
●Schedule Recording Settings

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



2. Set record stream, pre-record time, cycle writing. **Pre-Record Time**: Set the time to record before the actual recording begins.

3. Set schedule recording. **C**heck "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 into 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).

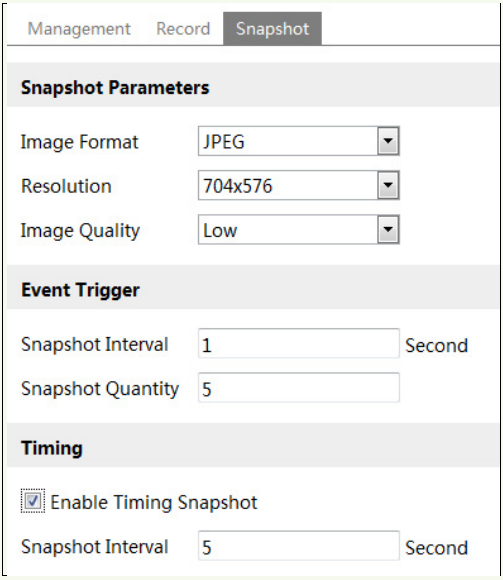
Day Schedule

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

Note: Holiday schedule takes priority over weekly schedule.

●Snapshot Settings

Go to ***Config→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.

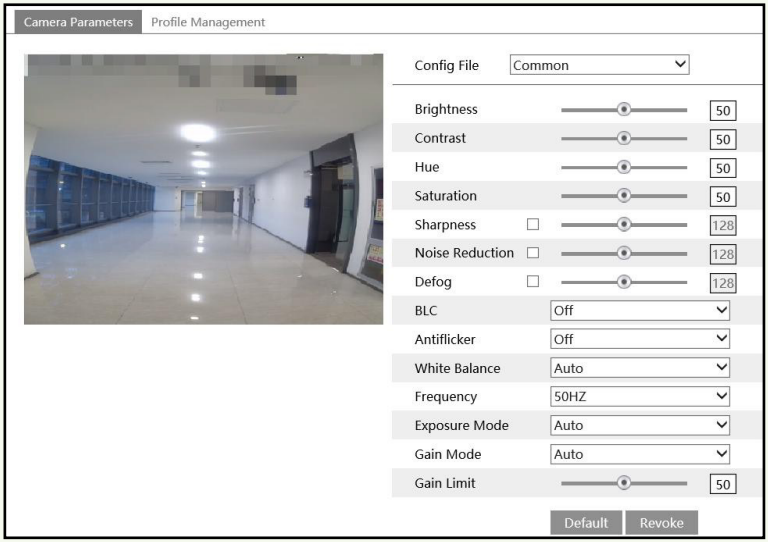
Snapshot Quantity: The number you set here is the maximum quantity of snapshots. The actual quantity of snapshots may be less than this number. Supposing the occurrence time of an alarm event is less than the time of capturing pictures, the actual quantity of snapshots is less than the set quantity of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

Timing Snapshot: Enable timing snapshot first and then set the snapshot interval and schedule. The setup steps of the schedule are the same as the schedule recording (See Schedule Recording).

4.7 Image Configuration

4.7.1 Display Configuration

Go to ***Image→Display*** interface as shown below. The image's brightness, contrast, hue and saturation and so on for common, day and night mode can be set up separately. The image effect can be quickly seen 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.
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.
Defog: Activating this function and setting an appropriate value as needed in foggy, dusty, smoggy, or rainy environment to get clear images.
Backlight Compensation (BLC):

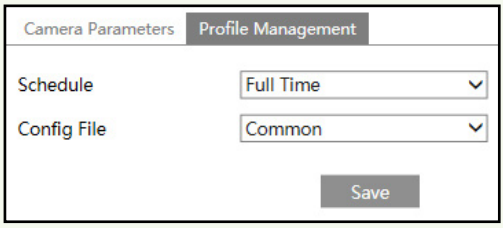
- Off: disables the backlight compensation function. It is the default mode.
- HWDR: WDR can adjust the camera to provide a better image when there are both very bright and very dark areas simultaneously in the field of view by lowering the brightness of the bright area and increasing the brightness of the dark area. Recording will be stopped for a few seconds while the mode is changing from non-WDR to WDR mode.
- 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.

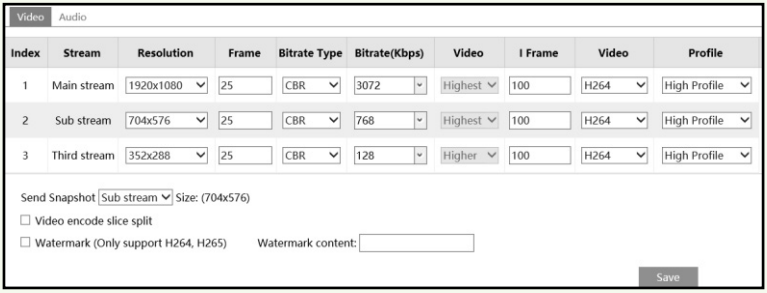
Frequency: 50Hz and 60Hz can be optional.
Exposure Mode: Choose “Auto” or “Manual”. If “Manual” is chosen, the digital shutter speed can be adjusted.
Gain Mode: Choose “Auto” or “Manual”. If “Auto” is selected, the gain value will be automatically adjusted (within the set gain limit value) according 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.
Note: For some items, if selected/enabled, the camera will reboot automatically. After that, clicking “Default” button will not take effect.
Schedule Settings of Image Parameters:
Click the “Profile Management” tab as shown below.



Set full time schedule for common or auto mode.

4.7.2 Video / Audio Configuration

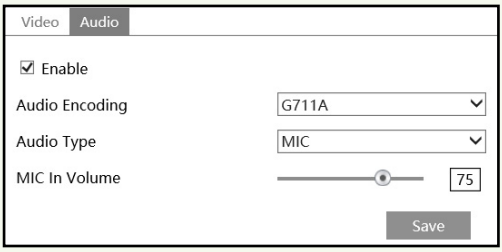
Go to ***Image→Video/Audio*** interface as shown below. In this interface, set the resolution, frame rate, bitrate type, video quality and so on subject to the actual network condition.



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, H265+ can be optional. MJPEG is not available for main stream. If H.265/H.265+ is chosen, make sure the client system is able to decode H.265/H.265+.
Profile: For H.264. Baseline, main and high profiles are selectable.
Send Snapshot: Select the snapshot stream.
Video encode slice split: If this function is enabled, a smooth image can be obtained even though using the 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.



Check "Enable" to enable audio.
Audio Encoding: G711A and G711U are selectable.
Audio Type: (built-in) MIC.
MIC In Volume: Set the volume of the built-in microphone.

4.7.3 OSD Configuration

Go to ***Image →OSD*** interface as shown below.

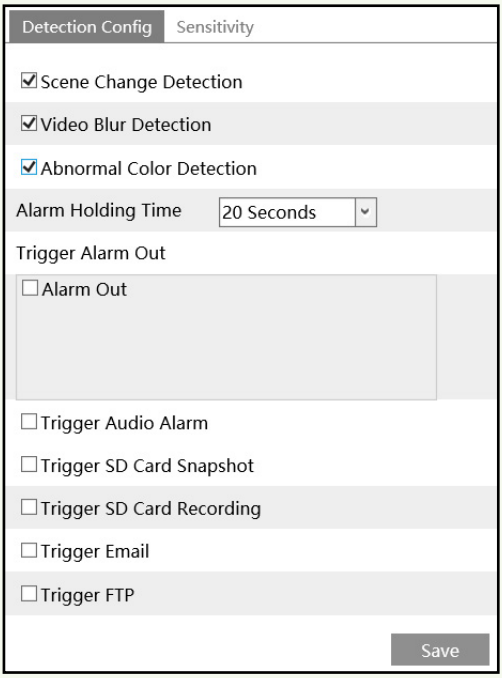
Set time stamp, device name, OSD content and picture overlap here. After enabling the corresponding display and entering the content, drag them to change their position. Then click the “Save” button to save the settings.

Picture Overlap Settings:
Check “OSD Content1”, choose “Picture Overlay” and click “Browse” to select the overlapping picture. Then click “Upload” to upload the overlapping picture. The pixel of the image shall not exceed 200*200, or it cannot be uploaded.

4.8 Alarm Configuration

4.8.1 Video Exception

This function can detect changes in the surveillance environment affected by external factors.
To set exception detection:
Go to ***Config→Alarm →Video Exception*** interface as shown below.



Enable the applicable detection that's desired. **Scene Change Detection**: Alarms will be triggered if the scene of the monitor 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.

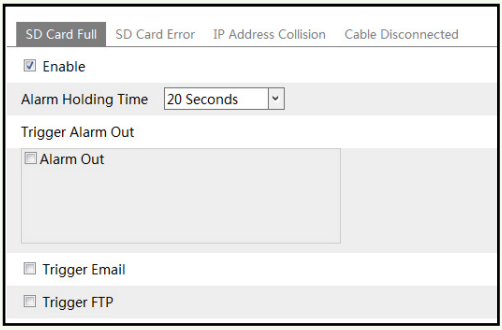
Set alarm trigger options. **Trigger Audio Alarm:** If selected, you will hear the warning sound when the video exception happens. **Trigger SD Card Snapshot:** If selected, the system will capture images on video exception detection and save the images on an SD card. **Trigger SD Card Recording:** If 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 to those addresses. **Trigger FTP**: If "Trigger FTP" is checked, the captured pictures will be sent to the FTP server address. Please refer to the FTP configuration section for more details.

Set the sensitivity of the exception detection. Drag the slider to set the sensitivity value or directly enter the sensitivity value in the textbox.

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.
5. Click the "Save" button to save the settings.

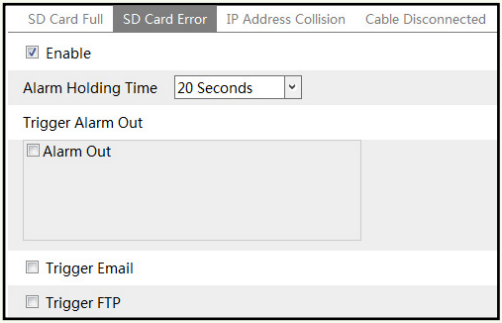
4.8.2 Exception Alarm

●SD Card Full
1. Go to ***Config→Alarm →Exception Alarm →SD Card Full***.



2. Click "Enable".
3. Set the alarm holding time and alarm trigger options.

●SD Card Error
When there are some errors in writing to the SD card, the corresponding alarms will be triggered.
1. Go to ***Config→Alarm →Exception Alarm →SD Card Error*** as shown below.

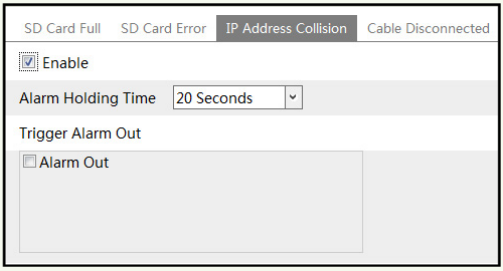


2. Click "Enable".

3. Set the alarm holding time and alarm trigger options. Trigger alarm out, Email, and FTP.

●IP Address Conflict

1. Go to ***Config →Alarm →Exception Alarm →IP Address Collision*** as shown below.

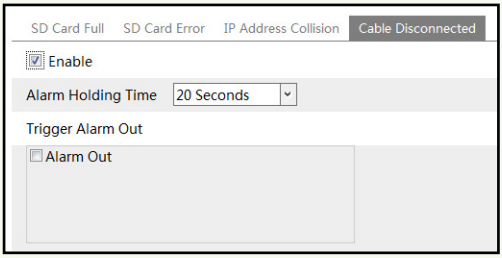


2. Click "Enable" and set the alarm holding time.

Trigger alarm out. When the IP address of the camera conflicts with the IP address of other devices, the system will trigger the alarm out.

●Cable Disconnection

1. Go to ***Config→Alarm →Exception Alarm →Cable Disconnected*** as shown below.

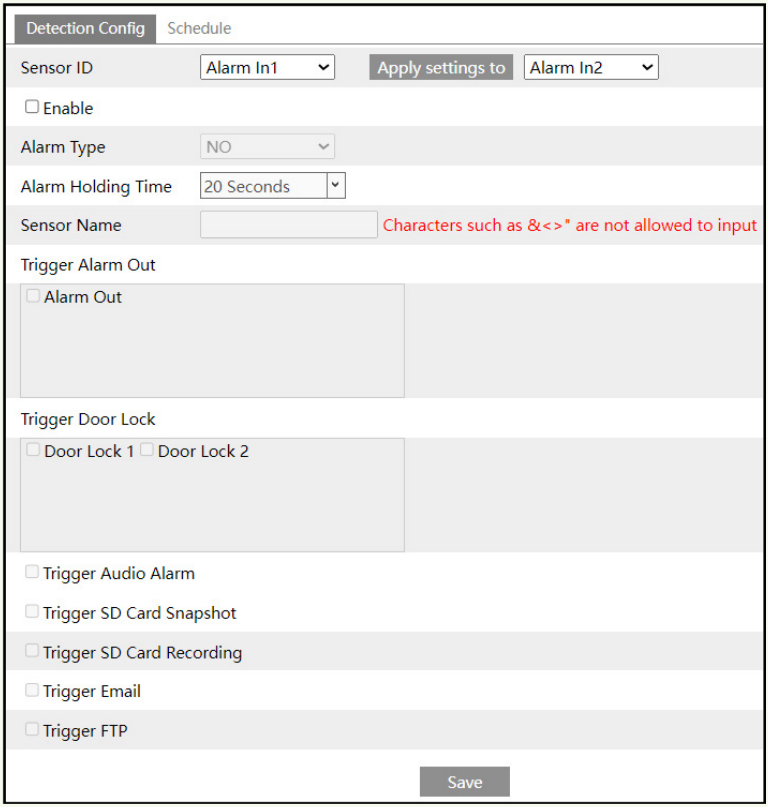


2. Click "Enable" and set the alarm holding time.
3. Trigger alarm out. When the camera is disconnected, the system will trigger the alarm out.

4.8.3 Alarm In

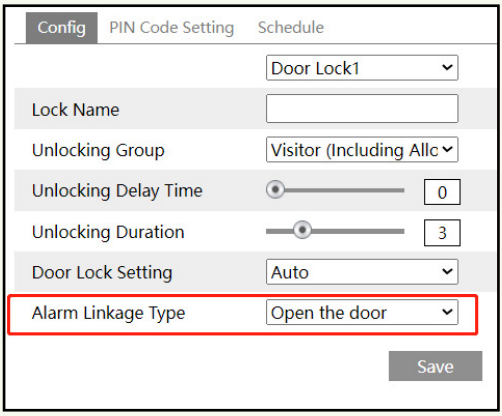
To set sensor alarm (alarm in):

Go to ***Config→Alarm →Alarm In*** interface as shown below.



1. Select the sensor ID.
2. Click “Enable” and set the alarm type, alarm holding time and sensor name.
3. Set alarm trigger options.

Trigger Door Lock: you can check “Door Lock1” or “Door Lock2”. When a sensor alarm occurs, the door1/2 will be opened or closed according to the alarm linkage type of door lock setting. Please set the alarm linkage type by clicking ***Config→Access Control→Door Lock*** as shown below.



The setup steps of other alarm trigger options are the same as the alarm trigger setup of the door contact settings.

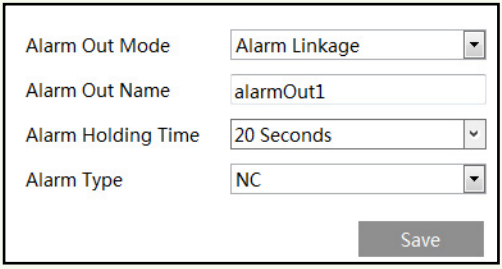
Set the schedule of the sensor alarm. The setup steps of the schedule are the same as the schedule recording (See Schedule Recording).

4. Click the "Save" button to save the settings.

Click "Apply settings to" to quickly apply the settings to the other alarm input.

4.8.4 Alarm Out

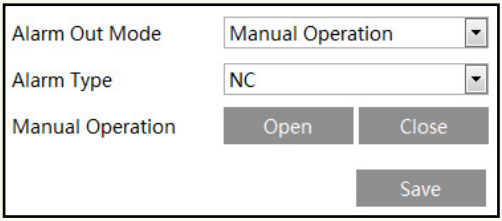
This function is only available for some models. Go to ***Config→Alarm →Alarm Out***.



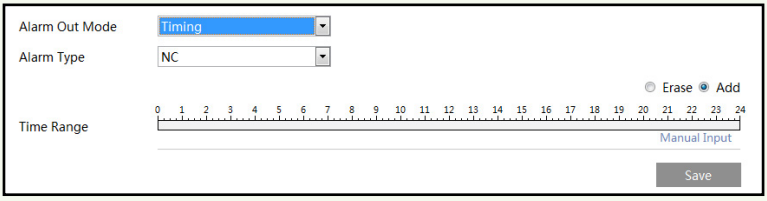
Alarm Out Mode: Alarm linkage, manual operation and timing are optional.

Alarm Linkage: Having selected this mode, select alarm out name, alarm holding time at the "Alarm Holding Time" pull down list box and alarm type.

Manual Operation: Having selected this mode, select the alarm type and click "Open" to trigger the alarm out immediately; click "Close" to stop alarm.



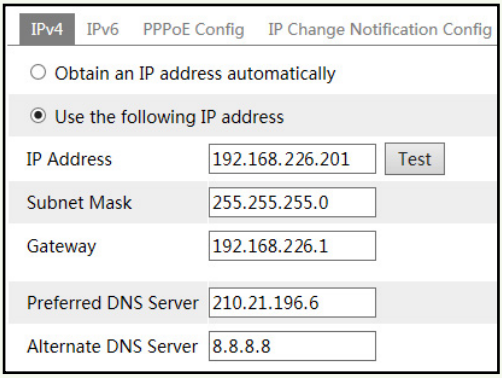
Timing: Select the alarm type. Then click "Add" and drag the mouse on the timeline to set the schedule of alarm out; click "Erase" and drag the mouse on the timeline to erase the set time schedule. After this schedule is saved, the alarm out will be triggered in the specified time.



4.9 Network Configuration

4.9.1 TCP/IP

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

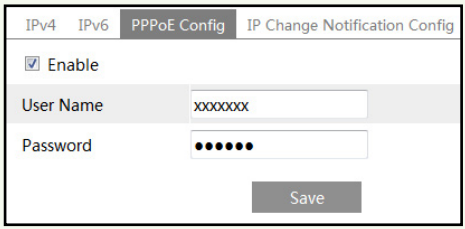


Use IP address (take IPv4 for example)-There are two options for IP setup: obtain an IP address automatically by DHCP and use the following IP address. Please choose one of the options as needed.

Note: It is recommended to set the network parameters manually, because the IP address may

be changed by obtaining an IP address automatically.

Test: Test the effectiveness of the IP address by clicking this button.
Use PPPoE-Click the "PPPoE Config" tab to go to the interface as shown below. Enable PPPoE and then enter the user name and password from your ISP.

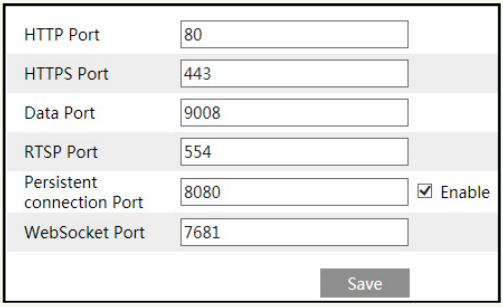


Either of the two network connection methods can be used. If PPPoE is used to connect internet, the camera will get a dynamic WAN IP address. This IP address will change frequently. To be notified, the IP change notification function can be used. Click "IP Change Notification Config" to go to the interface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

4.9.2 Port

Go to ***Config→Network→Port*** interface as shown below. HTTP port, Data port and RTSP port can be set.

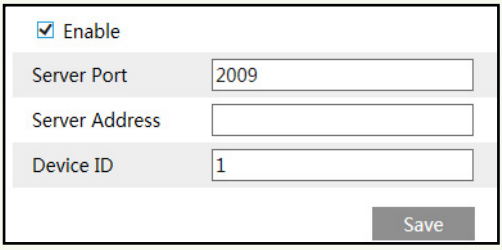


HTTP Port: The default HTTP port is 80. It can be changed to any port which is not occupied.

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.

4.9.3 Server Configuration

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

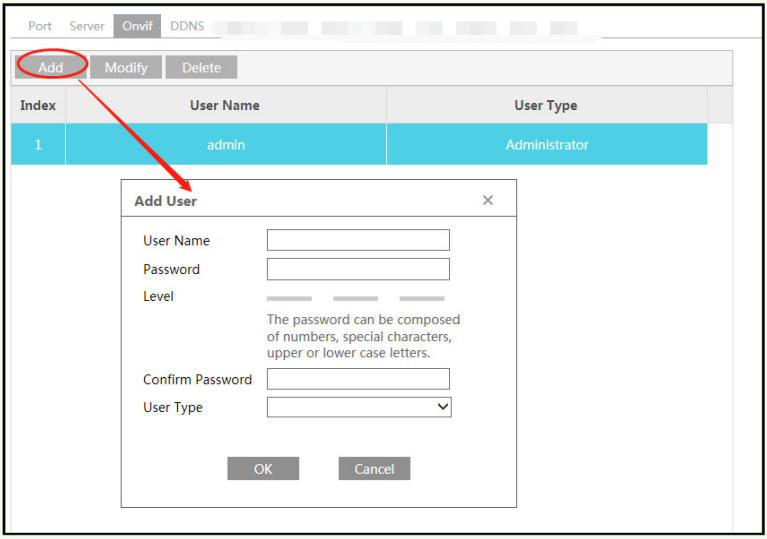


1. Check “Enable”.
2. Check the IP address and port of the transfer media server in the NVMS. Then enable the auto report in the NVMS when adding a new device. Next, enter the remaining information of the device in the NVMS. After that, the system will automatically allot a device ID. Please check it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

4.9.4 Onvif

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

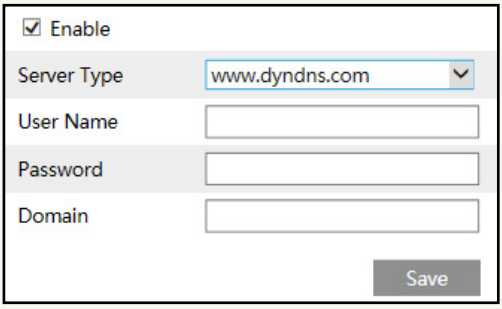
protocol.
If “Activate Onvif User” is enabled in the device activation interface, the ONVIF user can be activated simultanously. When you connect the camera through the ONVIF protocol in the third-party platform, you can use this onvif user to connect.
You can also add new users in the Onvif interface.



Note: when adding the device to the third-party platform with ONVIF/RTSP protocol, please use the onvif user in the above interface.

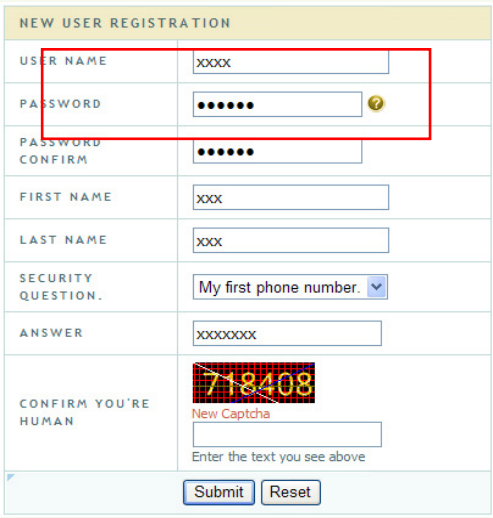
4.9.5 DDNS

If the camera is set up with a DHCP connection, DDNS should be set for the internet.
1. Go to ***Config→Network→DDNS***.



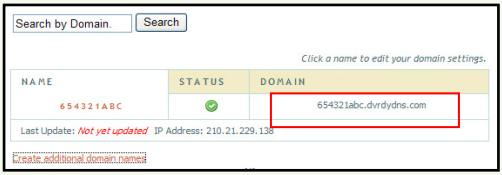
1Apply for a domain name. Take www.dvrdyndns.com for example. Enter www.dvrdydns.com in the IE address bar to visit its website. Then Click the

"Registration" button.



Create domain name.

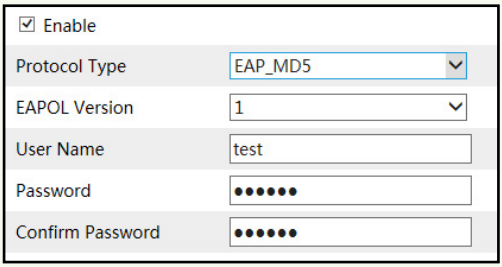
After the domain name is successfully applied for, the domain name will be listed as below.



3. Enter the username, password, domain you apply for in the DDNS configuration interface.
4. Click the "Save" button to save the settings.

4.9.6 802.1x

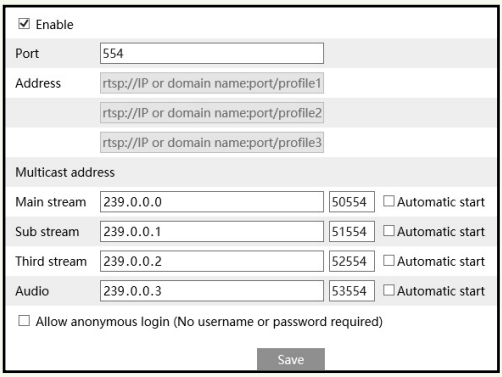
If it is enabled, the camera's data can be protected. When the camera is connected to the network protected by the IEE802.1x, user authentication is needed.



To use this function, the camera shall be connected to a switch supporting 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.
User name and password: The user name and password must be the same with the user name and password applied for and registered in the authentication server.

4.9.7 RTSP

Go to ***Config→Network→RTSP***.



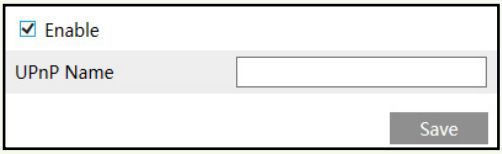
Select “Enable” to enable the RTSP function.
Port: Access port of the streaming media. The default number is 554.
RTSP Address: The RTSP address (unicast) format that can be used to play the stream in a media player.

Multicast Address
Main stream: The address format is
“rtsp://IP address: rtsp port/profile1?transportmode=mcast”.
Sub stream: The address format is
“rtsp://IP address: rtsp port/profile2?transportmode=mcast”.

Third stream: The address format is
"rtsp://IP address: rtsp port/profile3?transportmode=mcast".
Audio: Having entered the main/sub stream in a VLC player, 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 into a VLC player to play the video.
Note:1. This camera supports local preview through a VLC player. Enter the RTSP address (unicast or multicast, eg. rtsp://192.168.226.201:554/profile1?transportmode=mcast) in a VLC player to realize the simultaneous preview with the web client.
2. The IP address mentioned above cannot be the address of IPv6.
3. Avoid the use of the same multicast address in the same local network.
4. When playing the video through the multicast streams in a VLC player, please pay attention to the mode of the VLC player. If it is set to TCP mode, the video cannot be played.
5. If the coding format of the video of the main stream is MJPEG, the video may be disordered at some resolutions.

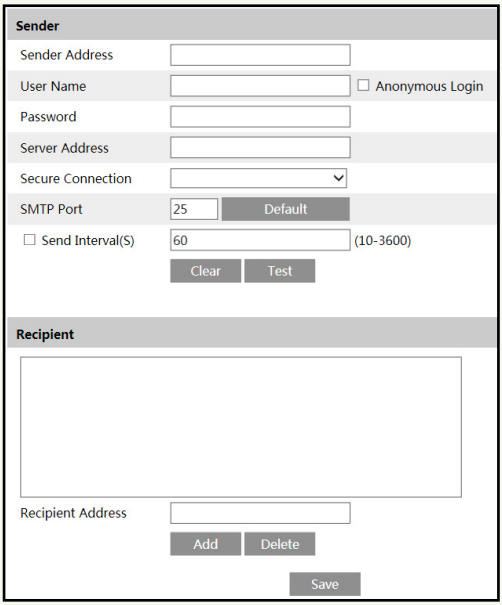
4.9.8 UPnP

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



4.9.9 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 ***Config→Network →Email***.

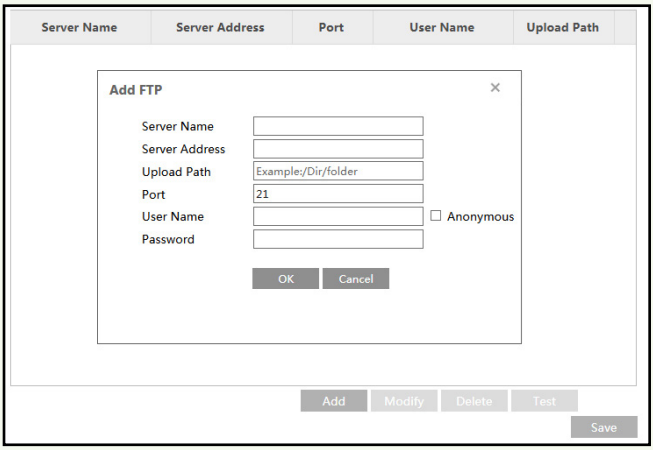


Sender Address: sender's e-mail address.
User name and password: sender's user name and password. If "Anonymous login" is selected, an anonymous Email will be sent when an alarm is triggered.
Server Address: The SMTP IP address or host name.
Select the secure connection type at the "Secure Connection" 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 alarms triggered by the same event within 60 seconds, they will be considered as only one alarm event and only one email will be sent. If one alarm event is triggered and then another 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.

4.9.10 FTP

After an FTP server is set up, captured pictures from events will be uploaded to the FTP server.

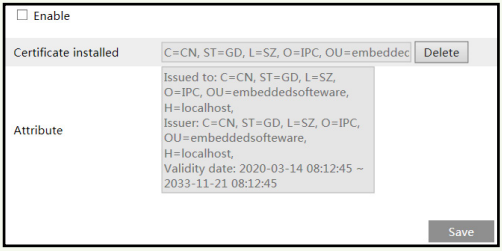
Go to ***Config→Network →FTP***.



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.
User Name and Password: The username and password that are used to login to the FTP server.

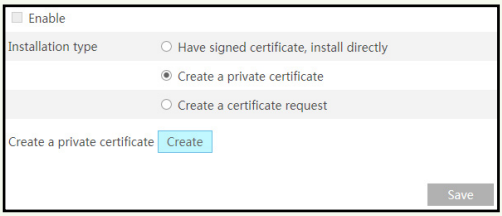
4.9.11 HTTPS

HTTPS provides authentication of the web site and protects user privacy.
Go to ***Config →Network→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.

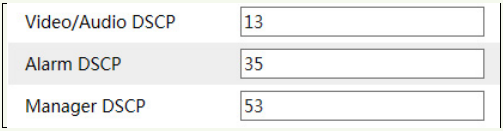
4.9.12 P2P

If this function is enabled, the network camera can be quickly accessed by scanning the QR code in mobile surveillance APP. This function is enabled by default.

4.9.13 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

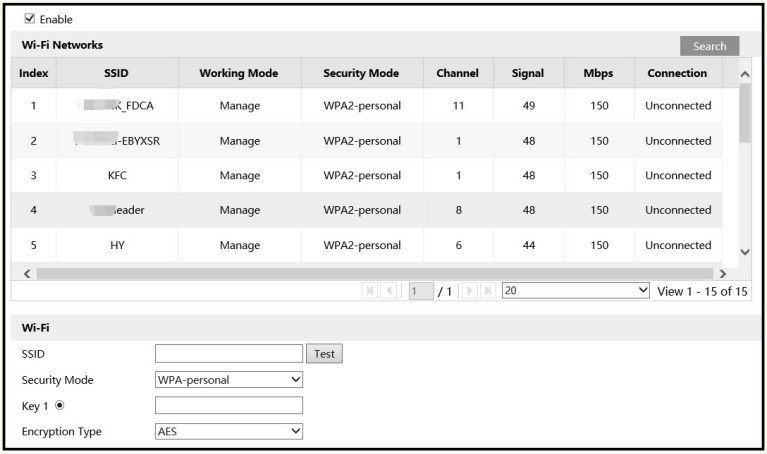
streams and transfer them according to their priority to solve the network delay and network congestion by using this function.
Go to ***Config→Network→QoS***.



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.

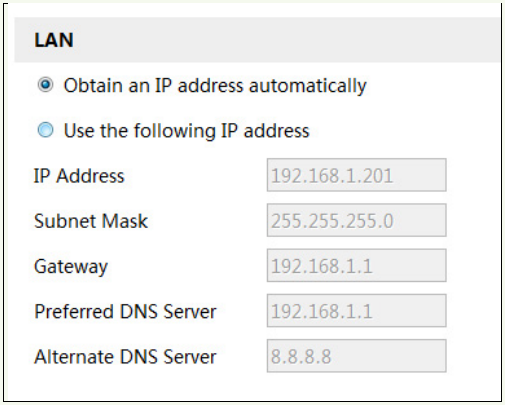
4.9.14 Wi-Fi Settings

Go to ***Config→Network→WIFI*** interface as shown below.



1. Checkmark “Enable” to enable Wi-Fi. Click “Search” to refresh the online wireless devices.
2. Choose a wireless device on the list. The SSID and security mode of the wireless device will be shown automatically. Please don’t change it manually.
3. Enter the key to connect the wireless device. This key should be set on the wireless device in advance for wireless network connection.

After the above-mentioned wireless network is configured, you can choose “Obtain an IP address automatically” or “Use the following IP address”.



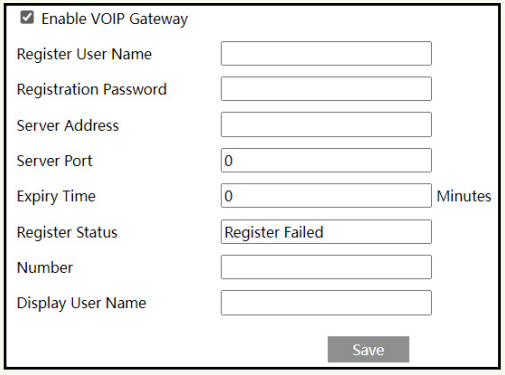
If you choose “Obtain an IP address automatically”, you shall get the IP address from the router. Or you can choose “Use the following IP address” to set the network parameters manually. Then you can use this IP address to log in mobile surveillance APP/ web client/NVMS/NVR/...

Note: It is recommended to set the network parameters manually, because the IP address may be changed by obtaining an IP address automatically.

4. Click “Test” to check whether the wireless network is connected. After successful connection, click “Save” to save the settings.

4.9.15 SIP

After enabling the SIP protocol, other SIP terminals can be called. Go to ***Config→Network→ SIP*** interface as shown below.



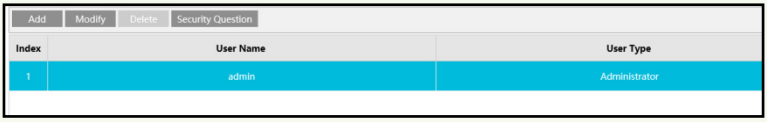
Enable “VOIP Gateway” and set the relevant parameters.

Note: The door station and other SIP terminals should be in the same IP segment.

4.10 Security Configuration

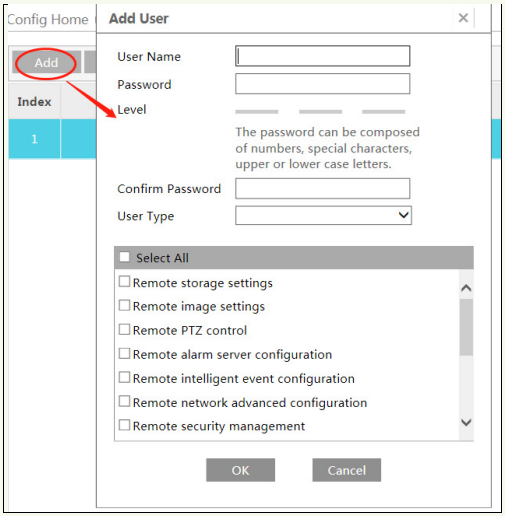
4.10.1 User Configuration

Go to ***Config→Security→User*** interface as shown below.



Add user:

1. Click the "Add" button to pop up the following textbox.



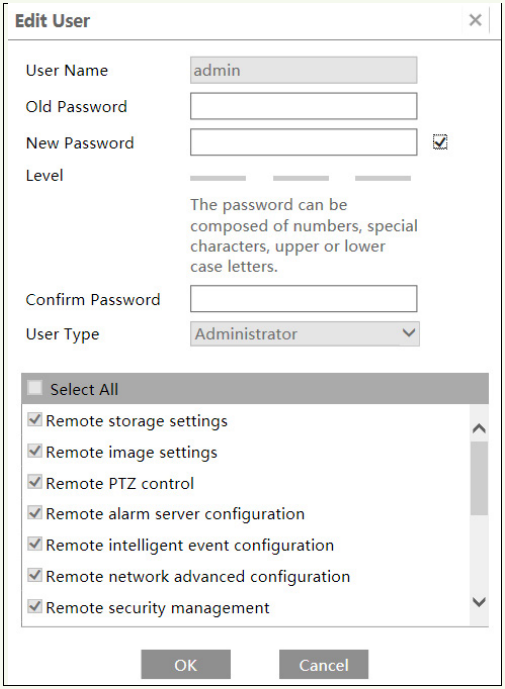
2. Enter user name in the "User Name" textbox.

Enter the password in the "Password" and "Confirm Password" textbox. Please set the password according to the requirement of the password security level (Go to ***Config→Security→Security Management →Password Security*** interface to set the security level).

4. Choose the user type and select the desired user permissions.
5. 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 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. Select the user permissions for advanced or normal user.
6. Click the “OK” button to save the settings.

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.

Safety Question Settings: set the questions and answers for admin so as to reset the password after you forget the password.

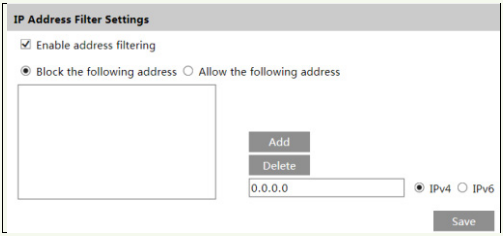
4.10.2 Online User

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

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

4.10.3 Block and Allow Lists

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



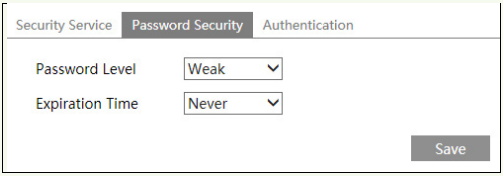
The setup steps are as follows:
Check the “Enable address filtering” check box.
Select “Block/Allow the following address”, IPv4/IPv6 and then enter IP address in the address box and click the “Add” button.

4.10.4 Security Management

Go to ***Config→Security→Security Management*** as shown below.

In order to prevent against malicious password unlocking, “locking once illegal login” 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.

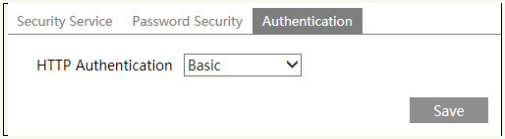
●Password Security



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 and 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.

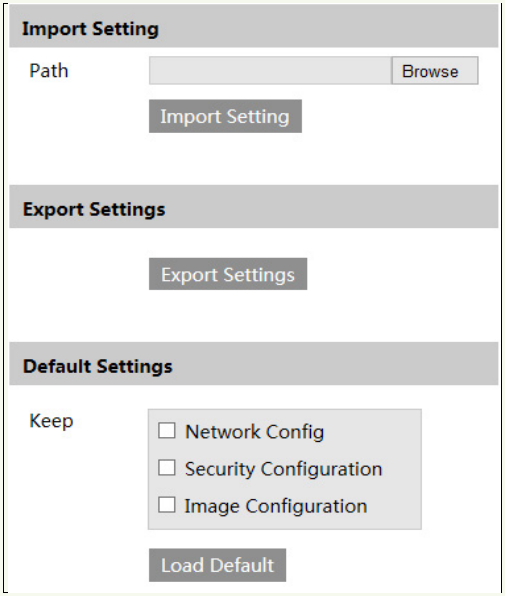
HTTP Authentication: Basic or Token is selectable.



4.11 Maintenance Configuration

4.11.1 Backup and Restore

Go to Config→Maintenance→Backup and 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.

Note: The login password needs to be entered after clicking the “Import Setting” button.

●**Default Settings**

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

4.11.2 Reboot

Go to Config→Maintenance→Reboot.

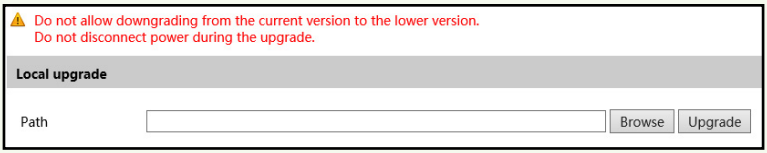
Click the “Reboot” button and then enter the password to reboot the device.

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, click the “Save” button and then enter the password to save the settings.

4.11.3 Upgrade

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



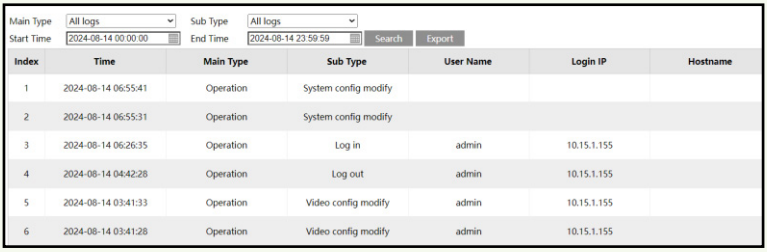
1. Click the “Browse” button to select the save path of the upgrade file
2. Click the “Upgrade” button to start upgrading the firmware.
3. Enter the correct password and then the device will restart automatically

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

4.11.4 Operation Log

To query and export log:

1. Go to ***Config→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.

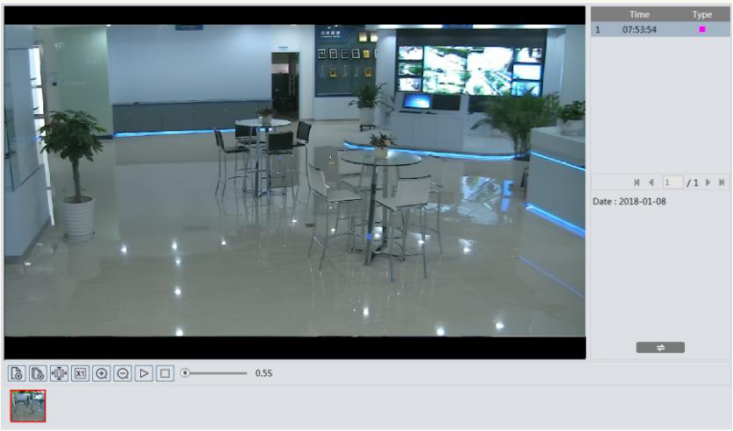
5.1 Image Search

Click **Search** to go to the interface as shown below. Images that are saved on the SD card can be found here.

Note: When using the plug-in free browser, the local images cannot be searched.

●Local Image Search

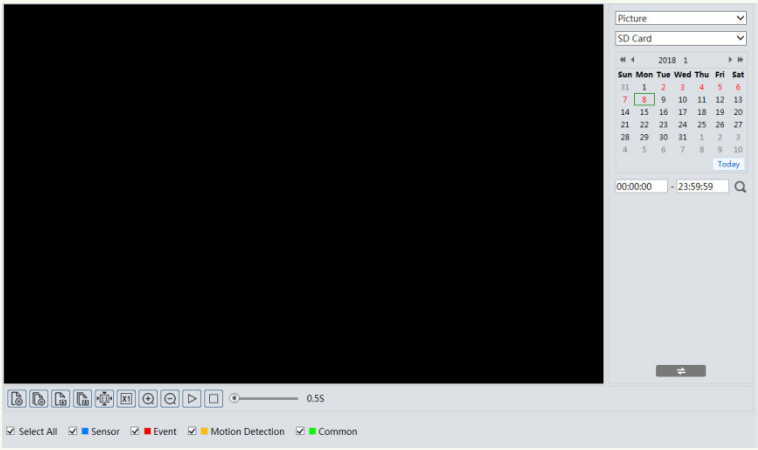
1. Choose “Picture”—“Local”.
2. Set time: Select date and choose the start and end time.
3. Click to search the images.
4. Double click a file name in the list to view the captured photos as shown above.



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.

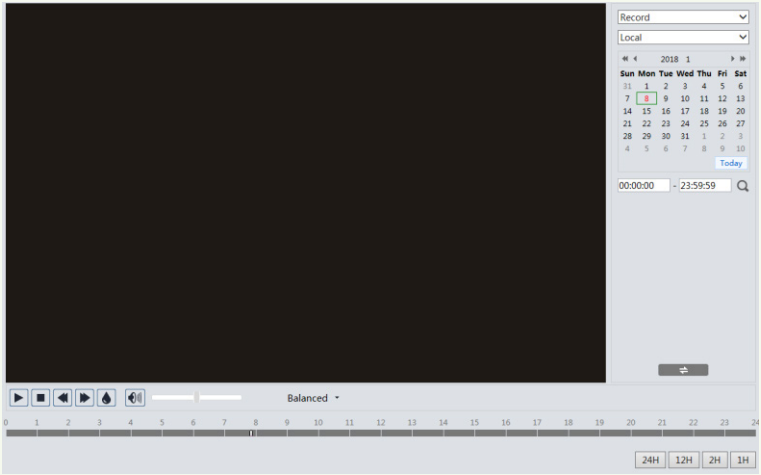
Icon	Description	Icon	Description
	Close: Select an image and click this button to close the image. Save: Click this button to select the path for saving the image on the PC.		Close all: Click this button to close all images. Save all: Click this button to select the path for saving all pictures on the PC. Actual size: Click this button to display the actual size of the image. Zoom out: Click this button to digitally zoom out.
	Fit size: Click to fit the image on the screen.		
	Zoom in: Click this button to digitally zoom in.		
	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.		

5.2 Video Search

5.2.1 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.

Note: When using the plug-in free browser, the local videos cannot be searched.



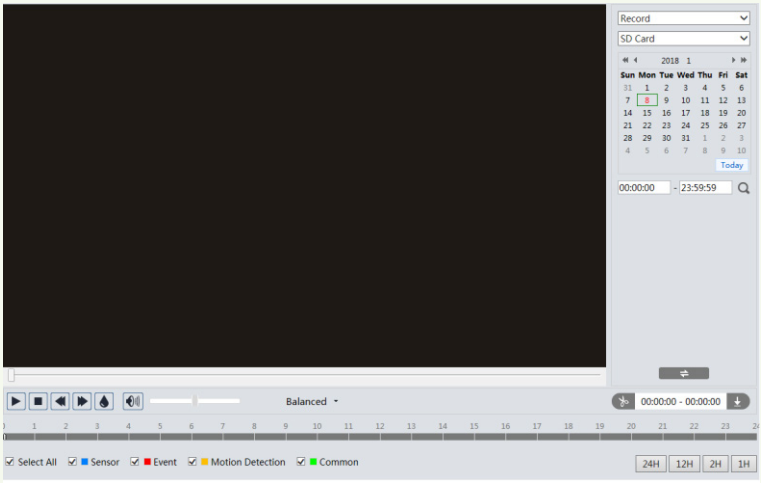
1. Choose “Record”—“Local”.
2. Set search time: Select the date and choose the start and end time.
3. Click to search the images.
4. Double click on a file name in the list to start playback.

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.		

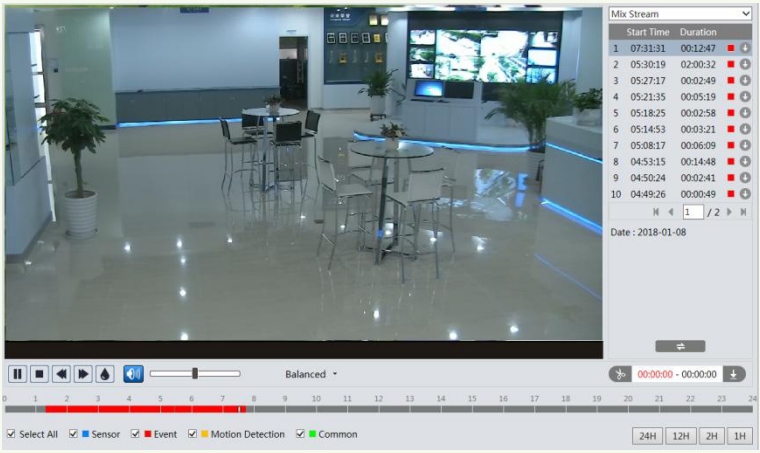
5.2.2 SD Card Video Search

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.

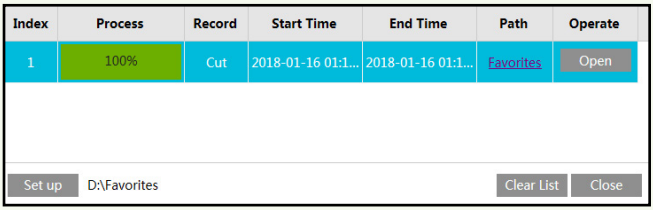


Note: Cannot display in the above interface via the plug-in free browser. Additionally, for plug-in free playback, playback mode switch (balanced/real-time/fluent mode) and downloading functions are not supported too.

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.

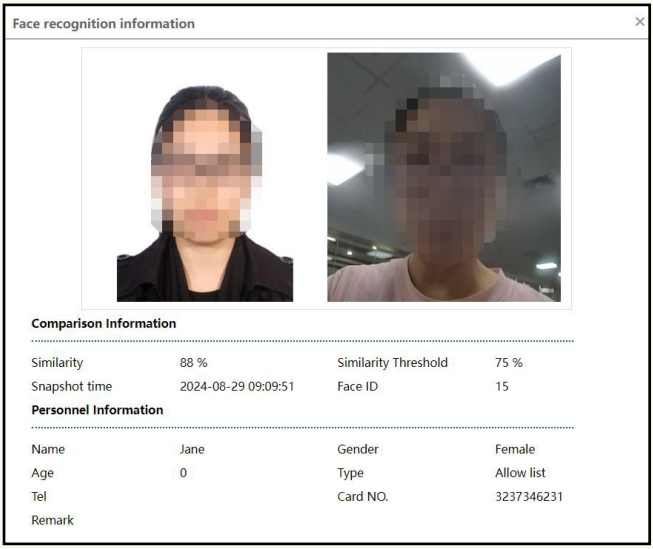


Click “Set up” to set the storage directory of the video files.
Click “Open” to play the video.
Click “Clear List” to clear the downloading list.
Click “Close” to close the downloading window.

6 Face Recognition Result Search

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

Red time tag means no comparison result. Click the picture with red time tag to add the person. Green time tag means there is a comparison result. Click the picture with green time tag and then the face comparison information can be viewed as shown below.



.

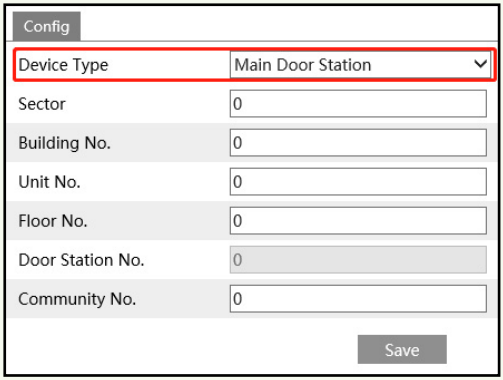
Appendix 1 How to Call Indoor Station

Appendix 1-1 One Door Station Calls One Indoor Station

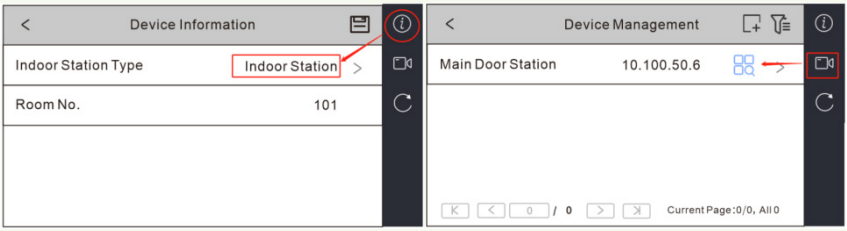
Application: One door station and bind one indoor station. Press the preset room number and call button or press to call indoor station

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.



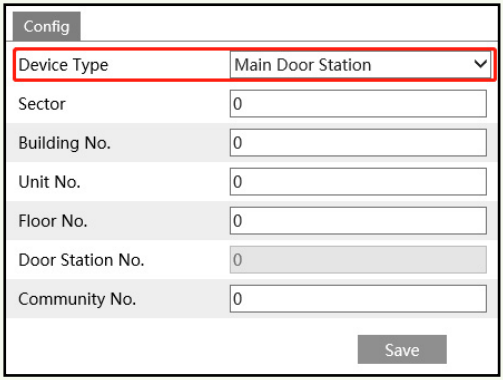
4. Call indoor station through your door station (See Call Resident for details).

Appendix 1-2 One Door Station Calls Multiple Indoor Stations

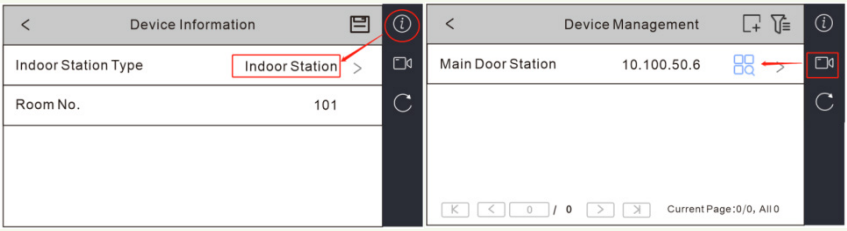
Application: A door station and bind multiple indoor stations with the same room number set. Press the room number and call button on the door station to call indoor stations. All indoor stations will respond at the same time. The resident can answer any one of them and open the door.

The setting steps are as follows:

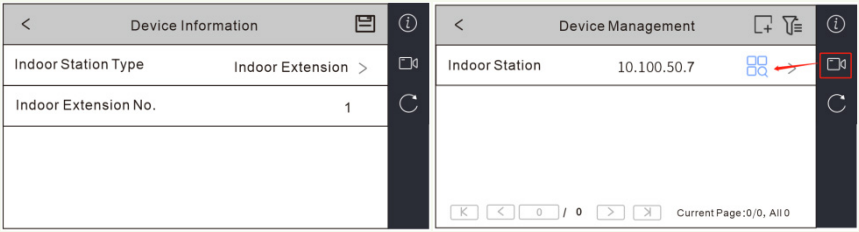
1. Connect your door station and indoor station to the same local network and then set their network parameters to the same network segment.
2. Log in the web client of the door station. Click ***Config→Intercom→Number Configuration*** to go to the following interface. Set the device type to "Main Door 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"), indoor extension No. (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.



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.

Application B: Install one door station and bind multiple indoor stations with the different room number set. Press different room numbers to call different indoor stations.

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. For other indoor stations, set the indoor station type to "Indoor Station", enter different room numbers and set the same IP address of the main door station.
5. Press different room numbers to call different indoor stations.

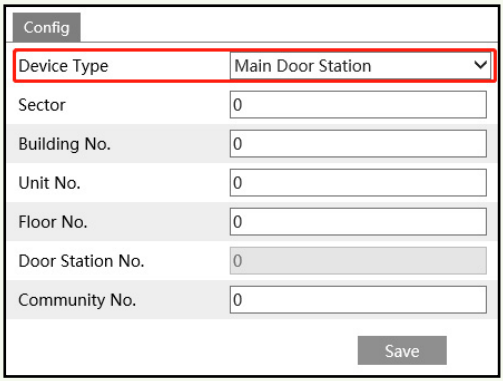
Appendix 1-3 Multiple Door Stations Call One Indoor Station

Application Multiple door stations and bind one indoor station. Press the preset room number and call button or press on different door stations to call indoor station.

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

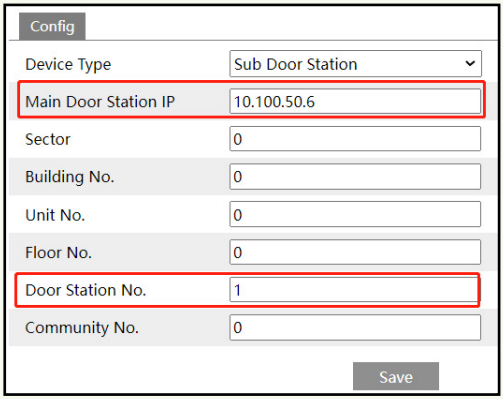
The setting steps are as follows:

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".

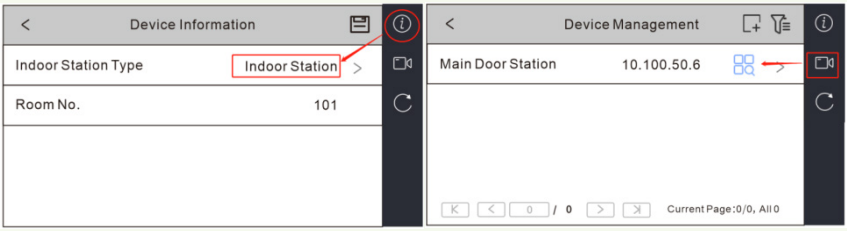


3. Sub door station settings

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 A: Install multiple door stations (one is main door station, others are sub door stations) and multiple indoor stations (all indoor stations are set as "Indoor Station"). Main door station and sub door stations can call different indoor stations installed in different rooms respectively.

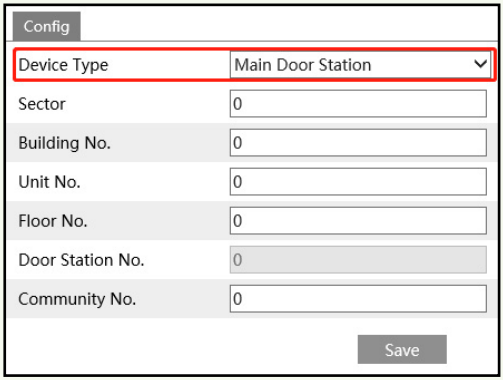
Note: Up to 9 sub door stations can be set for a main door station.

The setting steps are as follows:

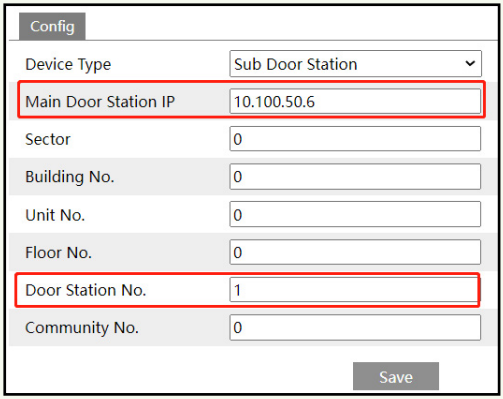
Connect your door stations and indoor stations to the same local network and then set their network parameters to the same network segment.

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".

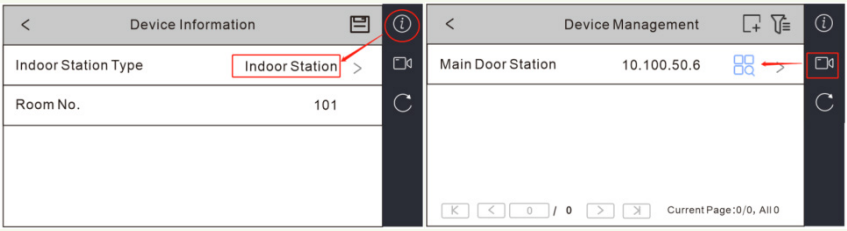


Sub door station settings Log in the web client of the door station. Click ***Config→Intercom→ Number Configuration*** to go to the following interface. Set the device type to "Sub Door Station". Enter the actual IP address of the main door station and door station no. Door Station No.: enter the sub 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.



6. Other indoor station settings Set other indoor station as "Indoor Station" and repeat the operation of step4. Different room number should be set for different indoor stations, but the same IP address of the main door station should be set.

7. Press different room numbers on different door stations (main or sub door stations) to call the corresponding indoor stations.

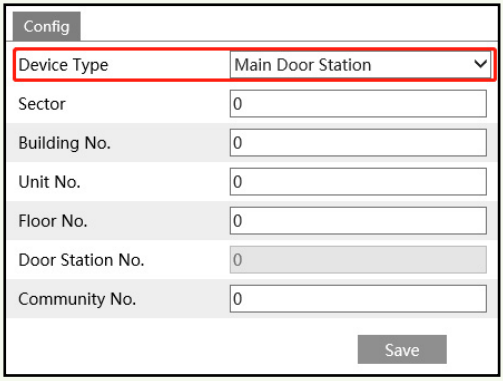
Application B: Install multiple door stations (one is main door station, others are sub door stations) and multiple indoor stations (one is indoor station, others are indoor extensions). When main door station or sub door stations call indoor stations installed in different rooms, all indoor stations 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.

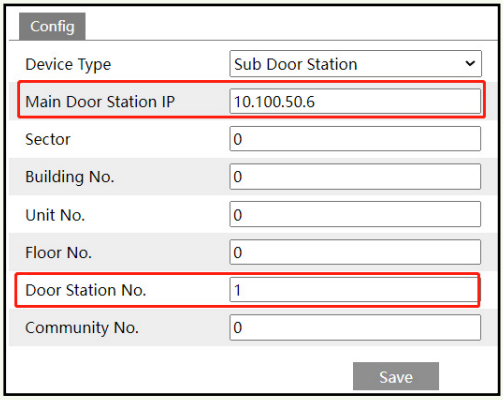
2. Main door station settings

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”.

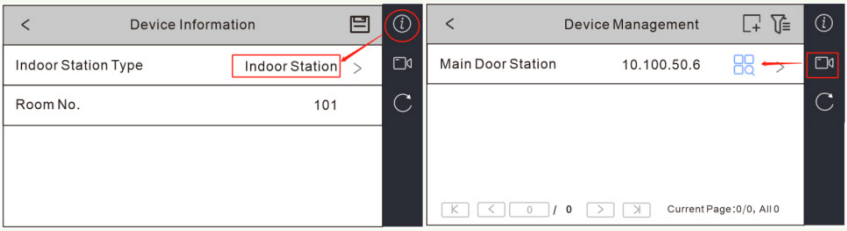


3. Sub door station settings

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.



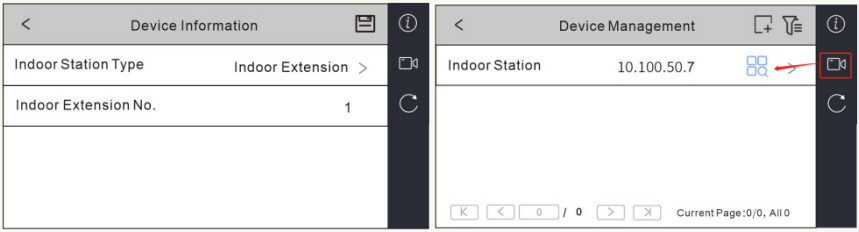
4. Indoor station settings Tap ***Settings→More Settings→Configuration*** in the indoor station. Then enter the password of Admin to enter the following interface. Set the indoor station type (it should be set to “Indoor station”), room number, IP address of the main door station.



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"), indoor extension No. (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

How to find the password?

A: The password for **admin** can be reset through "Edit Safety Question" function.

Click "Forget Password" in the login window and then enter the corresponding answer of the selected question in the popup window. After you correctly answer all questions, you can reset the password for **admin**. If you forget the answer of the question, this way will be invalid, please contact your dealer for help.

B: The passwords of other users can be reset by **admin**.

Fail to connect devices through IE browser.

A: Network is not well connected. Check the connection and make sure it is connected well.

B: IP address is not available. Reset the IP address.

C: Web port number has been changed: contact administrator to get the correct port number.

D: Exclude the above reasons. Restore to default setting by IP-Tool.

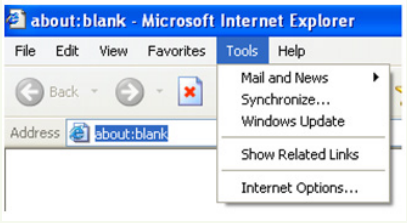
IP tool cannot search devices.

It may be caused by the anti-virus software in your computer. Please exit it and try to search device again.

IE cannot download ActiveX control.

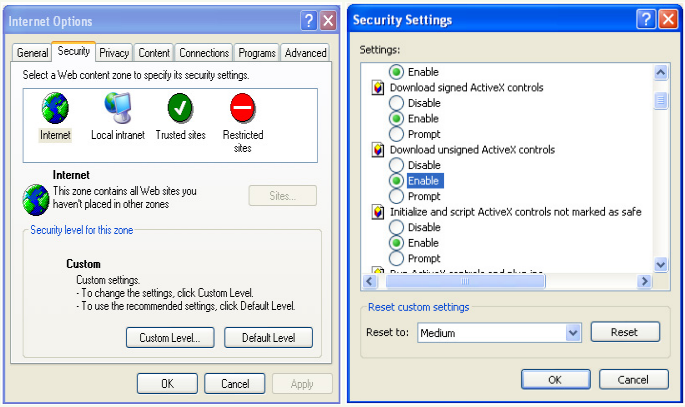
A. IE browser may be set up to block ActiveX. Follow the steps below.

Open IE browser and then click Tools—Internet Options.



- Select Security—Custom Level....
  - Enable all the options under "ActiveX controls and plug-ins".
    - Click OK to finish setup.

  B Other plug-ins or anti-virus blocks ActiveX. Please uninstall or close them.



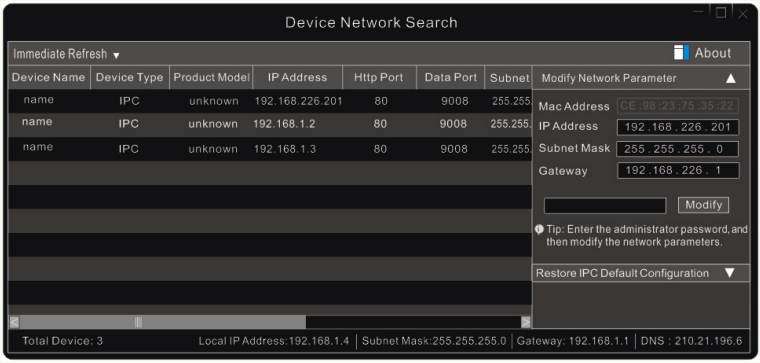
No sound can be heard.

A · Audio input device is not connected. Please connect and try again.

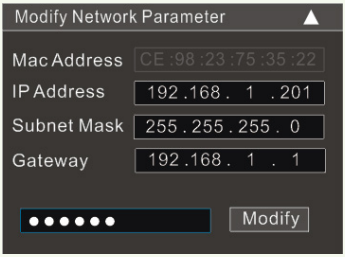
B: Audio function is not enabled at the corresponding channel. Please enable this function.

How to modify IP address through IP-Tool?

A: After you install the IP-Tool, run it as shown below.



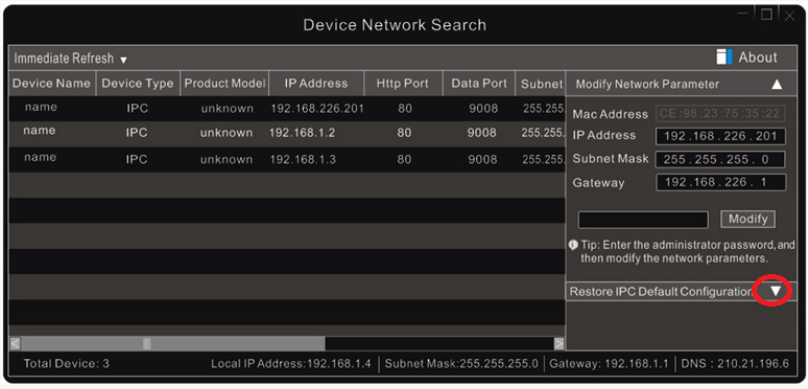
The default IP address of this camera is DHCP. Click the information of the camera listed in the above table to show the network information on the right hand. Modify the IP address and gateway of the camera and make sure its network address is in the same local network segment as the computer's. Please modify the IP address of your device according to the practical situation.



For example, the IP address of your computer is 192.168.1.4. So the IP address of the camera shall be changed to 192.168.1.X. After modification, please enter the password of “admin” which is set in the device activation interface in advance and then click the “Modify” button to change the network parameters.

How to restore to factory default setting through IP-Tool?

A · Drag the slider at the bottom of the device list to the right and then the MAC address of the searched devices will be viewed. Find the MAC address of the IPC you want to restore to the factory default setting, click Restore IPC Default Configuration next to “ ”. After that, manually add the name, then enter the MAC address and click “OK” to restore to the factory default setting



Door station failed to call indoor station.

1. Please check whether the network segment of the indoor station is the same as that of the door station.

2. Confirm whether the door station is main door station or sub door station

1) if it is a main door station,

a. check whether the room number of the indoor station is set

b. check whether the IP address of the main door station is set in the indoor station.

2) if it is a sub door station

a. check whether there is a main door station. If not, please set it as a main door station.

b. check whether the IP address of the main door station is added in the sub door station

c. check whether the main door station can be successfully called or not. If not, please refer to 1) to check.

3. Confirm the indoor station configuration

1) if it is a indoor station

a. check whether the IP address of the main door station added in the indoor station is right. If the IP address of the main door station is gotten by DHCP, please check whether the IP address is changed. It is recommended to set the IP address manually.

b. check whether the calling room number is the same as the room number set in the indoor station

2) if it is an indoor extension

a. check whether the IP address of the main indoor station set in the indoor extension is right or not. If the IP address of the main indoor station is gotten by DHCP, please check whether the IP address is changed. It is recommended to set the IP address manually.

If the gateway conflict occurs, what should I do?

1 Please check whether the wired network and wireless network are connected to the same router. If they are connected to the same router, disconnect one of them.

2 If not, please check whether the gateway addresses of the wired network and wireless network are the same one. If yes, please modify one of them.