

Video Intercom Door Station

User Manual

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

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.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

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	Network Connection	1
1.1	Wired Network Connection	1
1.2	Wi-Fi Connection	4
1.3	WAN	5
2	Live View via Web.....	7
3	Configuration via Web.....	9
3.1	Face Detection Settings.....	9
3.2	People Management	11
3.3	Door Station Settings	12
3.4	Video Intercom Operation	13
3.4.1	Button Calling Settings	13
3.4.2	Call Resident	14
3.4.3	Call Platform	14
3.4.4	Call APP.....	14
3.4.5	SIP Number Settings	16
3.5	Unlock Door.....	16
3.5.1	Unlock by Swiping Card	16
3.5.2	Unlock via Web	16
3.5.3	Unlock via APP.....	16
3.6	Access Control System Settings	17
3.6.1	Local Settings.....	17
3.6.2	Door Lock Settings	18
3.6.3	Door Contact Settings	20
3.6.4	Wiegand Settings	21
3.6.5	Tampering Alarm Settings	21
3.6.6	RS485 Settings.....	22
3.6.7	Elevator Settings	22
3.7	System Settings	23
3.7.1	Basic Information.....	23
3.7.2	Date and Time	24
3.7.3	Local Config	24
3.7.4	Storage	25
3.8	Image Configuration	27
3.8.1	Display Configuration.....	27
3.8.2	Video / Audio Configuration.....	29
3.8.3	OSD Configuration	31
3.8.4	ROI.....	31
3.9	Alarm Configuration	32
3.9.1	Motion Detection	32

3.9.2 Video Exception	33
3.9.3 Exception Alarm	34
3.9.4 Alarm Server	35
3.9.5 Person Detection	36
3.10 Network Configuration	36
3.10.1 TCP/IP	36
3.10.2 Port	38
3.10.3 Server Configuration	38
3.10.4 Onvif	39
3.10.5 DDNS	39
3.10.6 SNMP	41
3.10.7 802.1x	43
3.10.8 RTSP	43
3.10.9 RTMP	44
3.10.10 UPnP	45
3.10.11 Email	45
3.10.12 FTP	46
3.10.13 HTTPS	46
3.10.14 HTTP POST	48
3.10.15 P2P	48
3.10.16 QoS	48
3.10.17 Wi-Fi Settings	49
3.10.18 SIP	50
3.11 Security Configuration	51
3.11.1 User Configuration	51
3.11.2 Online User	52
3.11.3 Block and Allow Lists	53
3.11.4 Security Management	53
3.12 Maintenance Configuration	54
3.12.1 Backup and Restore	54
3.12.2 Reboot	55
3.12.3 Upgrade	55
3.12.4 Operation Log	56
4 Search	57
4.1 Image Search	57
4.2 Video Search	59
4.2.1 Local Video Search	59
4.2.2 SD Card Video Search	60
5 Data Record Search	62
Appendix	63
Appendix 1 How to Call Indoor Station	63
Appendix 1-1 One Door Station Calls One Indoor Station	63
Appendix 1-2 One Door Station Calls Multiple Indoor Stations	64



Appendix 1-3 Multiple Door Stations Call One Indoor Station 65

Appendix 1-4 Multiple Door Stations Call Multiple Indoor Stations..... 67

Appendix 2 Troubleshooting..... 71

1 Network Connection

1.1 Wired Network Connection

Here we take device access via Web browser for example.

Web browser: IE (plug-in required)/ Firefox/Edge/ Google Chrome

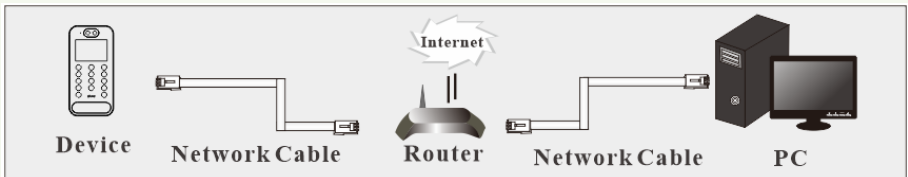
It is recommended to use the latest version of these web browsers.

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.

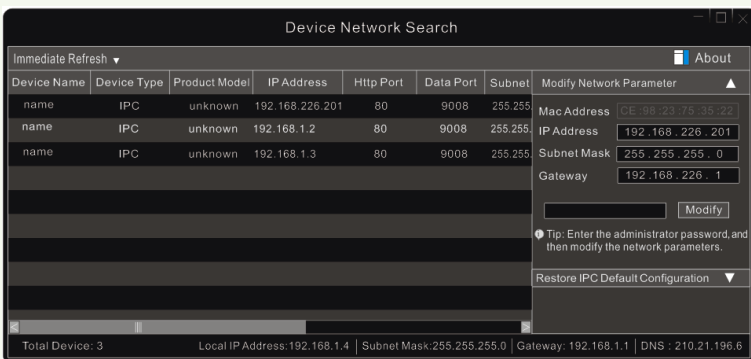
Connect IP-Cam via LAN or WAN. Here only take IE browser for example. The details are as follows:

● Access through IP-Tool

Network connection:

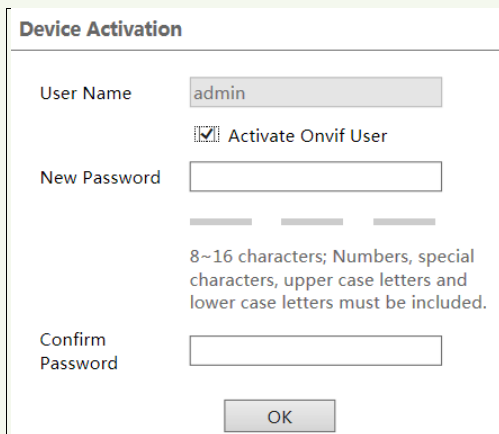


- ① Make sure the PC and device are connected to the same local network and the IP-Tool is installed in the PC.
- ② Double click the IP-Tool icon on the desktop to run this software as shown below:



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

- ③ Double 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 image shows a 'Device Activation' dialog box. It contains the following elements:

- User Name:** A text field with 'admin' entered.
- Activate Onvif User:** A checkbox that is checked, with the label 'Activate Onvif User'.
- New Password:** A text field that is empty.
- Password Requirements:** A note stating '8~16 characters; Numbers, special characters, upper case letters and lower case letters must be included.'
- Confirm Password:** A text field that is empty.
- OK Button:** A button at the bottom right.

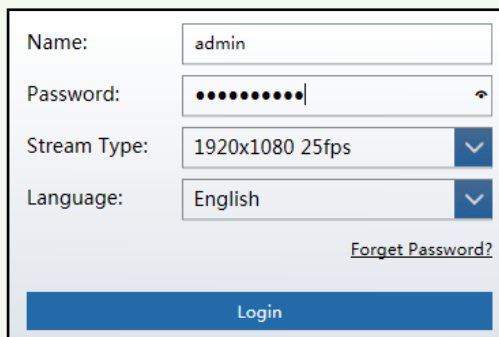
The default username is “admin”. Please self-define the password of admin according to the tip.

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** 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.

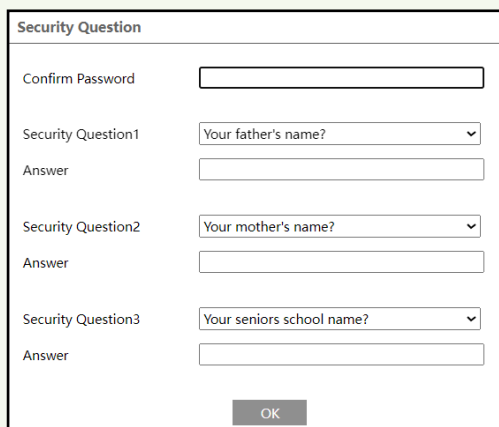


The login form contains the following fields and elements:

- Name:** A text input field containing the text "admin".
- Password:** A password input field with masked characters (dots) and a toggle icon on the right.
- Stream Type:** A dropdown menu currently showing "1920x1080 25fps".
- Language:** A dropdown menu currently showing "English".
- Forget Password?** A text link located below the language dropdown.
- Login:** A large blue button at the bottom of the form.

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.



The Security Question form contains the following fields and elements:

- Confirm Password:** A text input field.
- Security Question1:** A dropdown menu with the option "Your father's name?".
- Answer:** A text input field corresponding to Security Question1.
- Security Question2:** A dropdown menu with the option "Your mother's name?".
- Answer:** A text input field corresponding to Security Question2.
- Security Question3:** A dropdown menu with the option "Your seniors school name?".
- Answer:** A text input field corresponding to Security Question3.
- OK:** A button at the bottom right of the form.

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.

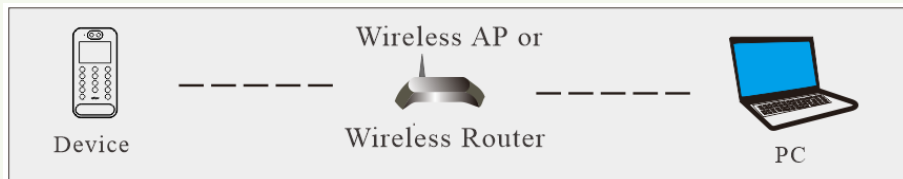
You can set the account security question during the activation, or you can go to **Config → Security → User**, click **Safety Question**, select the security questions and input your answers.

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.

1.2 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.

☒ Enable

Wi-Fi Networks

Search

Index	SSID	Working Mode	Security Mode	Channel	Signal	Mbps	Connection
1	uest	Manage	WPA2-personal	12	54	150	Unconnected
2	menjin	Manage	WPA2-personal	12	54	150	Unconnected
3	test-mac	Manage	not-encrypted	12	54	11	Unconnected
4	DevTest	Manage	not-encrypted	12	54	11	Unconnected
5	.T	Manage	WPA2-personal	12	52	150	Unconnected

1 / 1
20
View 1 - 14 of 14

Wi-Fi

SSID

Test

Security Mode

WPA-personal

Key 1

Encryption Type

AES

After that, select “Obtain an IP address automatically” or manually enter the IP address by clicking “Use the following IP address”.

LAN	
☐ Obtain an IP address automatically ☒ Use the following IP address	
IP Address	192.168.1.201
Subnet Mask	255.255.255.0
Gateway	192.168.1.1
Preferred DNS Server	192.168.1.1
Alternate DNS Server	8.8.8.8

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.

④ Pull the network cable out of the camera.

⑤ Run the IP-Tool and find the camera through IP address or MAC address. Then double click it listed in the IP-Tool or enter the IP address of the camera in the address bar of the web browser to access the camera.

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

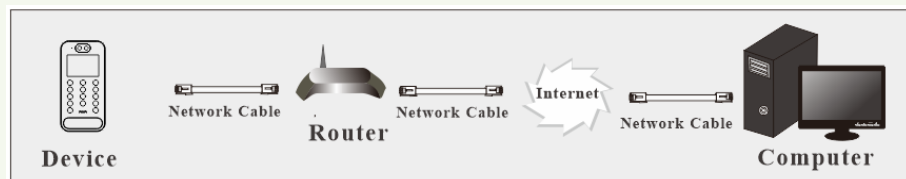
1.3 WAN

➤ Access via P2P

Connect and activate the device according to the above-mentioned steps (See 1.1). 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:

① 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.

HTTP Port	80
HTTPS Port	443
Data Port	9008
RTSP Port	554

Port Setup

- ② Go to **Config** → **Network** → **TCP/IP** menu to modify the IP address.

IPv4	IPv6	PPPoE Config	IP Change Notification Config
☐ Obtain an IP address automatically			
☒ Use the following IP address			
IP Address	192.168.226.201	Test	
Subnet Mask	255.255.255.0		
Gateway	192.168.226.1		
Preferred DNS Server	210.21.196.6		
Alternate DNS Server	8.8.8.8		

IP Setup

- ③ Go to the router's management interface through IE browser to forward the IP address and port of the camera in the "Virtual Server".

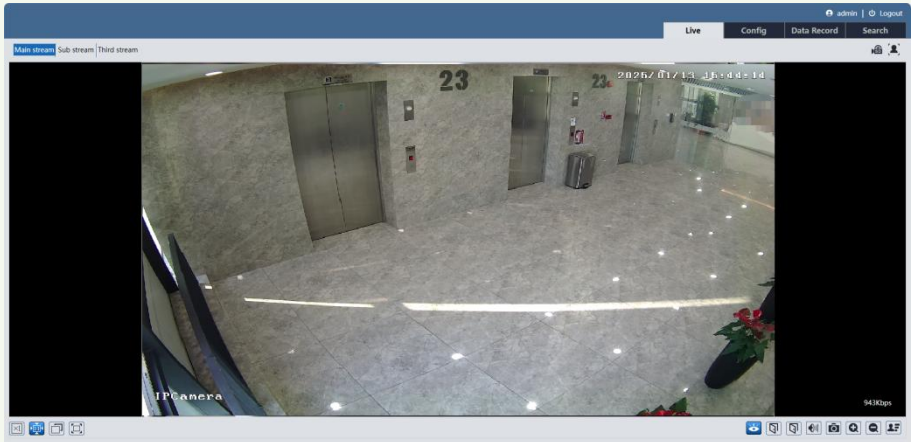
Port Range					
Application	Start	End	Protocol	IP Address	Enable
1	9007	to 9008	Both	192.168.1.201	☒
2	80	to 81	Both	192.168.1.201	☒
3	10000	to 10001	Both	192.168.1.166	☐
4	21000	to 21001	Both	192.168.1.166	☐

Router Setup

- ④ 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).

2 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.

3 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.

3.1 Face Detection Settings

1. Go to *Config* → *Face* → *Face Detection*.

Detection Config	Area	Advanced	Schedule
State Working			
☒ Enable			
Alarm Holding Time 20 Seconds ▼			
☐ Trigger SD Card Snapshot			
☐ Trigger SD Card Recording			
☐ Trigger Email			
☐ Trigger FTP			
Save			

1. Enable the face detection function.
2. 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.

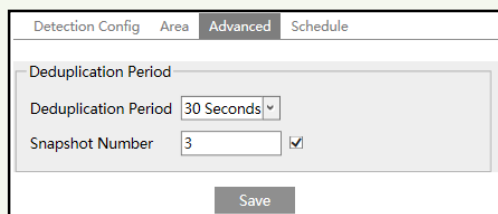
Trigger FTP: If “Trigger FTP” is checked, the captured pictures will be sent to the FTP server address. Please refer to the FTP configuration section for more details.

3. 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. Advanced settings. Choose the snapshot interval and number as needed to avoid capturing multiple similar pictures in a very short period of time.



Deduplication Period: If 30 seconds is selected, the camera will capture the same target once every 30 seconds during its continuous tracking period.

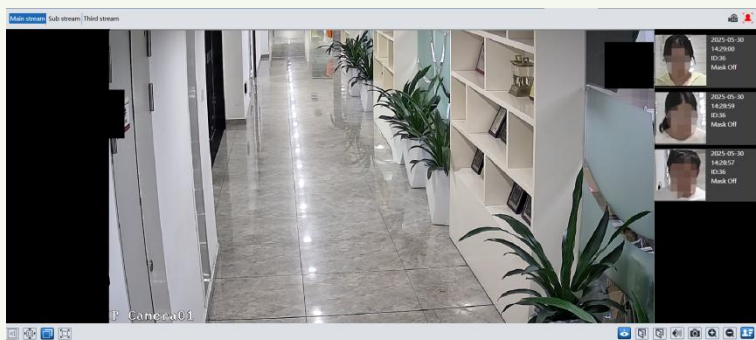
Snapshot Number: If the snapshot number is enabled and set (eg. 3), the camera will capture the same target once every 30 seconds and it will capture this target 3 times at most during its continuous tracking period. If the snapshot number is disabled, the camera will capture the same target once every 30 seconds until the target disappears in the detected area.

5. Set the schedule of the face detection. The setup steps of the schedule are the same as schedule recording setup (See [Schedule Recording](#)).

Face Capture View

After enabling face detection function, return to the live view interface. Click  to go to

the following interface. When there are faces detected, the face pictures will be listed on the right. In addition, you can also view the capture time, ID information, whether to wear a mask, etc.



3.2 People Management

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

Add User

ID NO.

List Type

Allow list

Name

Gender

☒ Male
☐ Female

Age

Floor

Room No.

Tel

Card NO.

Add

Always Valid

☒

Unlocking Mode

Only Swiping Card

Door Lock

☒ Door Lock1
☒ Door Lock2

Remark

Entry

There are two ways to add people information.

① Adding one by one

Click  to pop up an adding user box. Then fill out the relevant information of the person you want to add and click “Entry” to add.

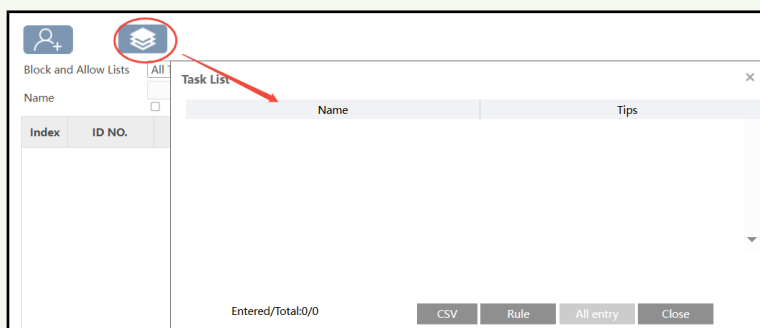
List Type: allow list, block list, and administrator.

Unlocking mode: only swiping card

Note: If “Swiping card” is included, the card No. should be entered by swiping card on the device when adding a person. Each person can add a maximum of 5 cards.

② Adding people information at a time

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



Task List	
Name	Tips
Entered/Total:0/0	

Click “CSV” to select the directory and then click “All entry” to upload.

Click “Modify” to change the person’s information and click “Delete” to delete this person’s information.

Click “Export” to export all personal information.

3.3 Door Station Settings

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

Config

Device Type: Main Door Station
Sector: 0
Building No.: 0
Unit No.: 0
Floor No.: 0
Number: 0
Community No.: 0
☒ Device Binding Authentication
Save

Config

Device Type: Sub Door Station
Main Door Station IP: 0.0.0.0
User Name: ☐ Anonymous
Password:
Binding State:
Sector: 0
Building No.: 0
Unit No.: 0
Floor No.: 0
Number: 1
Community No.: 0
Save

Device Type: main door station or sub door station.

Note:1. The number of the main door station is 0; the number of the sub door station is from 1 to 99. The same number is not allowed to enter for different sub door stations.

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

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

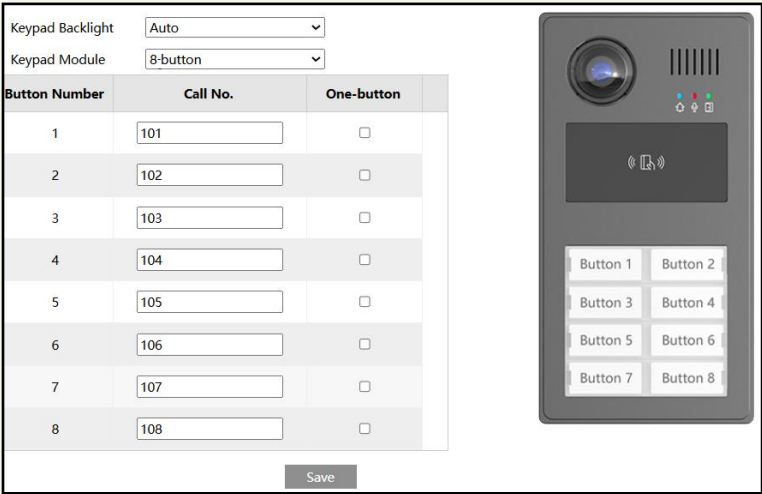
If the device type is set to “Main door station” and “Device Binding Authentication” is enabled, you need to enter the password of “admin” when adding the main door station to the indoor station.

If the device type is set to “Sub door station” and “Device Binding Authentication” is enabled in the main door station you want to connect, you need to disable “Anonymous” and enter the username and password of the main door station (Note that the password should be the password of the default admin user).

3.4 Video Intercom Operation

3.4.1 Button Calling Settings

Click **Config** → **Intercom** → **Button Calling**. In this interface, you can set the keypad backlight, keypad module, calling shortcut key and call no.



Button Number	Call No.	One-button
1	101	☐
2	102	☐
3	103	☐
4	104	☐
5	105	☐
6	106	☐
7	107	☐
8	108	☐

Save

Keypad Backlight: Choose “Auto”, “Manual” or “Close”. If “Manual” is selected, the light will be on behind the nametag buttons immediately. If “Auto” is selected, the light will be on behind the nametag buttons only when pressing a button.

One-button: Set the calling shortcut key. After a button is checked, it will be set as a shortcut key and the call no. cannot be set. You can directly call the APP/platform/resident by pressing this button.

Keypad Module: 1-button/2-button/4-button/8-button can be selectable. Please select it as needed. Here we take 8-button module as an example.

Number 1 corresponds to Button 1 (shown in the device picture on the right)

Number 2 corresponds to Button2 (shown in the device picture on the right)

.....

Set the room number (call no.) for different buttons. After that, you can press a button to call the corresponding resident.

3.4.2 Call Resident

- Go to **Config → Intercom → Button Calling**. Check a one-button calling shortcut (For example: Button1).
- Go to **Config → Intercom**. Check “Press button to call indoor station” and then enter the room number. Finally, click “Save”.

The screenshot shows a configuration window titled 'Config'. Under the 'Intercom' tab, the 'Button Calling' section is expanded. It contains three checked checkboxes: 'Press button to call platform', 'Press button to call APP', and 'Press button to call indoor station'. To the right of the third checkbox is an empty text input field. At the bottom right of the window is a 'Save' button.

- Press the shortcut button to call the resident.

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

3.4.3 Call Platform

- Go to **Config → Intercom → Button Calling**. Check a one-button calling shortcut (For example: Button1).
- Go to **Config → Intercom**. Check “Press button to call platform” and then click “Save”.
- Press the shortcut button to call the platform.

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

3.4.4 Call APP

- **Press one button to call the administrator account of the APP**
- Go to **Config → Intercom → Button Calling**. Check a one-button calling shortcut (For example: Button1).
- Go to **Config → Intercom**. Check “Press button to call APP” and then click “Save”.
- Press the shortcut button to call the platform.

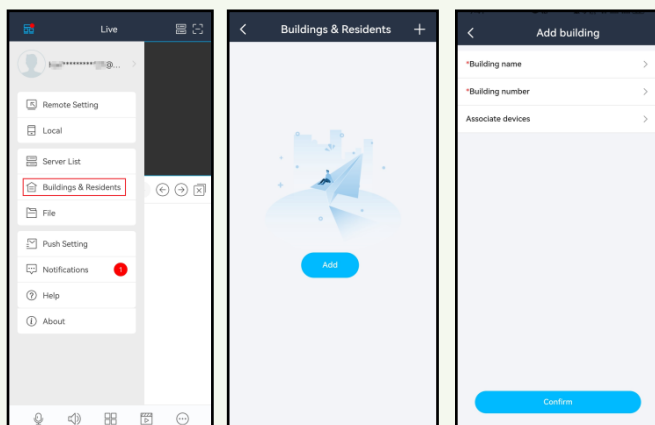
Note: Please add the door station to the mobile APP before calling.

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

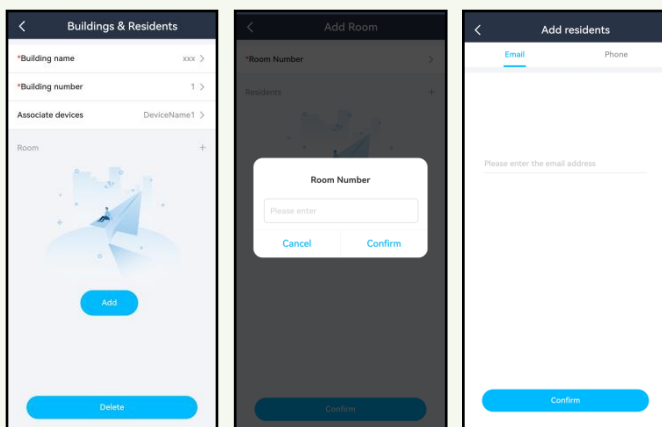
➤ Press the pre-defined room number to call the resident account of the APP

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 live interface of the APP, tap  and select “Buildings & Residents”.
3. 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.

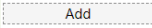


5. Press the corresponding button on the door station to call the resident. (See [Button Calling Settings](#) for room number setup)
6. In the APP, the resident can receive or reject the call as needed.

3.4.5 SIP Number Settings

Link the room No. and SIP numbers.

Go to **Config → Intercom → SIP Number Settings**. Click “Add” to show the following window.

Enter the room number and SIP number as needed. If there are multiple SIP numbers, click  to add more SIP numbers. After linking the room numbers and SIP numbers and setting the SIP protocol (See [SIP](#) for more details), you can call the SIP terminal through the corresponding room number.

3.5 Unlock Door

3.5.1 Unlock by Swiping Card

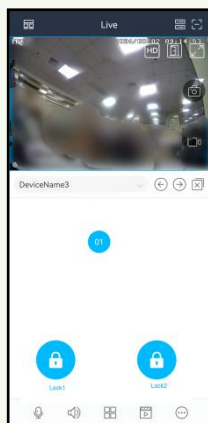
When the unlocking mode is set to “Only Swiping Card”, the door will be opened by swipe a card.

3.5.2 Unlock via Web

In the live view interface of the Web client, select the door lock1/2 icon and click  to unlock the door.

3.5.3 Unlock via APP

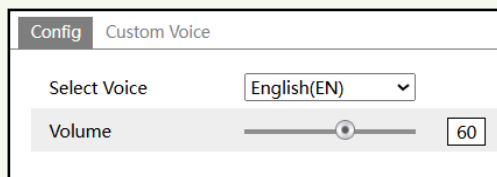
In the live view interface of the APP, tap the image and then  will shown on the image as shown below. Tap  to open the door as needed.



3.6 Access Control System Settings

3.6.1 Local Settings

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



Select Voice: Select the language of the voice prompt or the custom voice prompt.

Volume: Set the volume of the voice prompt.

● Customizing Voice

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

Select the voice you want to replace and then click “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.

3.6.2 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.

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

Door Lock ID: Select “Door Lock1” or “Door Lock2” as needed.

Lock Name: Set the lock name as needed.

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”.

Exit Button Type: Choose “NO” or “NC” as needed.

Power-off State: Set the power-off state of the door. Choose “NO” or “NC” 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.

☒ Enable

Door Lock1 ▼

Lock Condition NO ▼

○ Erase ● Add

Week Schedule

Sun. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 Manual Input

Mon. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 Manual Input

Tue. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 Manual Input

Wed. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 Manual Input

Thu. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 Manual Input

Fri. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 Manual Input

Sat. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 Manual Input

Holiday Schedule

Date 08-29 Add Delete

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 Manual Input

00:00-24:00

Save

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.

3.6.3 Door Contact Settings

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

Config	
Door Contact Input ID	Door Contact1
☒ Enable	
Door Contact Input Type	NO
Unlocking Delay Time	10 Seconds
Alarm Delay Time	0 (s)
☐ Trigger Audio Alarm	
☐ Trigger SD Card Snapshot	
☐ Trigger SD Card Recording	
☐ Trigger Email	
☐ Trigger FTP	
Save	

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.

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.

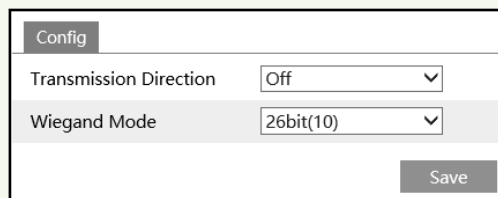
Trigger FTP: If “Trigger FTP” is checked, the captured pictures will be sent to the FTP

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.

3.6.4 Wiegand Settings

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



Config	
Transmission Direction	Off
Wiegand Mode	26bit(10)
Save	

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”.

When “Wiegand Output” is selected, you can enable or disable “Transparent Transmission of Card No”. If enabled, the card number can be output immediately after swiping a card through the Wiegand output without any other verification actions. If disabled, the card number can be output after all unlocking conditions you set are satisfied (for example: the unlocking mode is set to “Only swiping card”). The card number can be output until the correct card is swiped).

Wiegand Mode: 26bit(8), 26bit(10), 34bit, 37bit, 42bit, 46bit, 58bit or 66bit can be selectable.

3.6.5 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.

Config	
☒	Enable
Alarm Holding Time	20 Seconds ▼
☐	Trigger Audio Alarm
☐	Trigger SD Card Snapshot
☐	Trigger SD Card Recording
☐	Trigger Email
☐	Trigger FTP
Save	

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.

3.6.6 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.

If “Access Control System” is selected, you can enable or disable “Transparent transmission of Card No”. If enabled, the card number can be output immediately after swiping a card through the RS485 protocol without any other verification actions. If disabled, the card number can be output after all unlocking conditions you set are satisfied (for example: the unlocking mode is set to “Only swiping card”. The card number can be output until the correct card is swiped).

For other parameters of RS 485, it is recommended to use the default settings.

3.6.7 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**. 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.

Elevator control parameter

☒ Enable

Elevator controller name

WebRelay

Floor

QueryAddDelete

Index	Floor	Add the elevator control parameters	Password	Operate
		Floor IP Address Port Number State Duration of State Password SaveCancel		

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.

3.7 System Settings

3.7.1 Basic Information

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

Device Name

IPC

Product Model

Brand

Software Version

5.1.2.0(63547)

Software Build Date

2025-05-22

Onvif Version

24.12

MAC

aa:00:aa:ae:8

Device ID

80V12EFL

Binding state

Unbound

Refresh

Security Code

Required when adding to APP device list

About this machine

View

Privacy Statement

View



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.

3.7.2 Date and Time

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

Zone Date and Time

Zone GMT (Dublin, Lisbon, London, Reykjavik)

☐ DST

☒ Auto DST

☐ Manual DST

Start Time January First Sunday 00 Hour

End Time February First Monday 00 Hour

Time Offset 120 Minutes

Save

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.

Zone Date and Time

Time Mode:

☒ Synchronize with NTP server

NTP server: time.windows.com Update period: 1440 Minutes

☐ Synchronize with computer time

Date 2021-09-01 Time 17:37:36

☐ Set manually

2021-09-01 09:37:32

Time Format 24-Hour

Save

3.7.3 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.

Picture Path	C:\Program Files\EntranceGuardClient	Browse
Record Path	C:\Program Files\EntranceGuardClient	Browse
Video Audio Settings	☐ Open ☒ Close	
Show Bitrate	☐ Open ☒ Close	
Local Smart Snapshot Storage	☐ Open ☒ Close	
Save		

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.

3.7.4 Storage

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

Management		Record	Snapshot
Total picture capacity	379 MB		
Picture remaining space	379 MB		
Total recording capacity	3329 MB		
Record remaining space	2816 MB		
State	Normal		
Snapshot Quota	10	%	
Video Quota	90	%	
Changes in the quota ratio need to be formatted before they become effective.			
Eject Format			

● 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.

Record Parameters

Record Stream: Main stream ▼

Pre Record Time: No Pre Record ▼ (H264,H265,MJPEG)

Cycle Write: Yes ▼

Timing

☐ Enable Schedule Record

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. Check “Enable Schedule Record” and set the schedule.

☐ Erase
 ☒ Add

Week Schedule

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Sun.	00:00-24:00																								
	Manual Input																								
Mon.	00:00-24:00																								
	Manual Input																								
Tue.	00:00-24:00																								
	Manual Input																								
Wed.	00:00-24:00																								
	Manual Input																								
Thu.	00:00-24:00																								
	Manual Input																								
Fri.	00:00-24:00																								
	Manual Input																								
Sat.	00:00-24:00																								
	Manual Input																								

Holiday Schedule

Date

09-01

+

-

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	00:00-24:00																								
	Manual Input																								

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.

Management Record Snapshot	
Snapshot Parameters	
Image Format	JPEG
Resolution	704x576
Image Quality	Low
Event Trigger	
Snapshot Interval	1 Second
Snapshot Quantity	5
Timing	
☒	Enable Timing Snapshot
Snapshot Interval	5 Second

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.

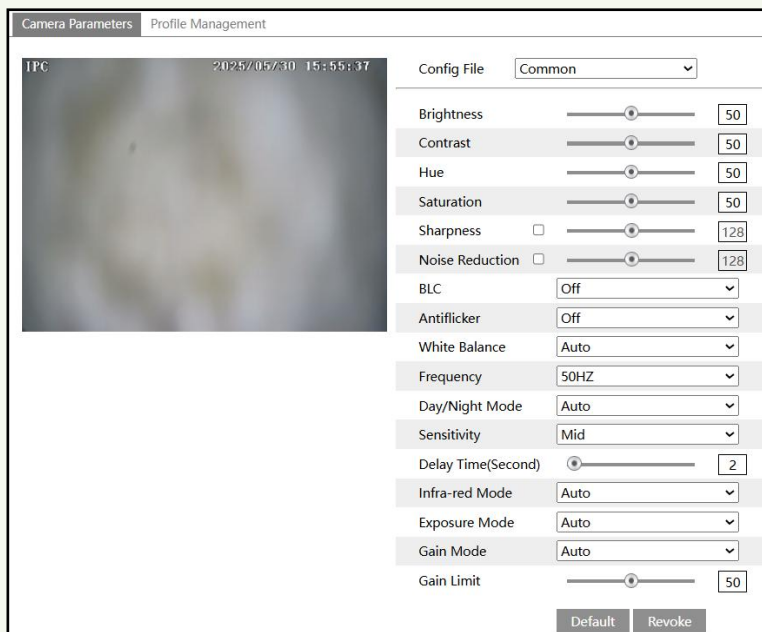
Snapshot Quantity: The number you set here is the maximum quantity of snapshots. The actual quantity of snapshots may be less than this number. Supposing the occurrence time of an alarm event is less than the time of capturing pictures, the actual quantity of snapshots is less than the set quantity of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

3.8 Image Configuration

3.8.1 Display Configuration

Go to **Image** → **Display Settings** 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.

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.

Day/Night Mode: Choose “Auto”, “Day”, “Night” or “Timing”.

If “Timing” is selected, you need to set daytime and night time. For example: if “Daytime” is set to “7:00”, the camera will switch to Day mode at 7:00 o’clock; if “Night time” is set to “17:00”, the camera will switch from Day mode to Night mode at 17:00 o’clock.

Infra-red Mode: Choose “Auto”, “ON” or “OFF”.

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.

Schedule Settings of Image Parameters:

Click the “Profile Management” tab as shown below.

Camera Parameters Profile Management

Schedule Full Time

Config File Common

Save

Set full time schedule for common or auto mode.

3.8.2 Video / Audio Configuration

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

Index	Stream	Resolution	Frame	Bitrate Type	Bitrate(Kbps)	Video	I Frame	Video	Profile
1	Main stream	1920x1080	25	CBR	3072	Highest	100	H264	High Profile
2	Sub stream	704x576	25	CBR	768	Highest	100	H264	High Profile
3	Third stream	352x288	25	CBR	128	Higher	100	H264	High Profile

Send Snapshot Sub stream Size: (704x576)

☐ Video encode slice split

☐ Watermark (Only support H264, H265) Watermark content:

Save

Three 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.

The screenshot shows a configuration window with two tabs: 'Video' and 'Audio'. The 'Audio' tab is active. Inside the tab, there is a section for audio settings. At the top, there is a checkbox labeled 'Enable' which is checked. Below it, there are two dropdown menus: 'Audio Encoding' set to 'G711A' and 'Audio Type' set to 'MIC'. Below these is a slider for 'MIC In Volume' with a value of 75. At the bottom right of the configuration area is a 'Save' button.

Check “Enable” to enable audio.

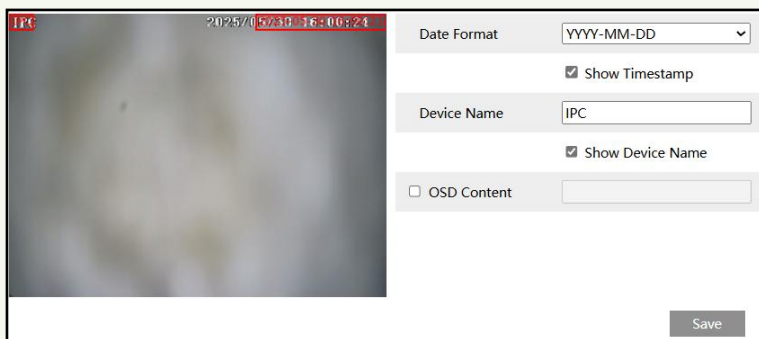
Audio Encoding: G711A and G711U are selectable.

Audio Type: (built-in) MIC.

MIC In Volume: Set the volume of the built-in microphone.

3.8.3 OSD Configuration

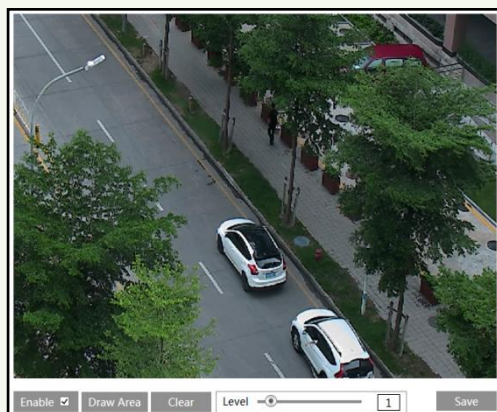
Go to **Image**→**OSD** as shown below.



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.

3.8.4 ROI

Go to **Image**→**ROI Config** as shown below. An area in the image can be set as a region of interest. This area will have a higher bitrate than the rest of the image, resulting in better image quality for the identified area.



1. Check “Enable” and then click the “Draw Area” button.
2. Drag the mouse to set the ROI area.
3. Set the level.
4. Click the “Save” button to save the settings.

3.9 Alarm Configuration

3.9.1 Motion Detection

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

The screenshot shows the 'Motion Detection' configuration window. The 'Detection Config' tab is active. It contains the following settings:

- ☒ Enable
- Alarm Holding Time: 20 Seconds (dropdown menu)
- ☐ Trigger Audio Alarm
- ☐ Trigger SD Card Snapshot
- ☐ Trigger SD Card Recording
- ☐ Trigger Email
- ☐ Trigger FTP
- Save button

1. Check “Enable” check box to activate motion based alarms. If unchecked, the camera will not send out any signals to trigger motion-based recording to the NVR or CMS, even if there is motion in the video.

Alarm Holding Time: it refers to the time that the alarm extends for after an alarm ends. For instance, if the alarm holding time is set to 20 seconds, once the camera detects a motion, it will go to alarm and would not detect any other motion in 20 seconds. If there is another motion detected during this period, it will be considered as continuous movement; otherwise it will be considered as a single motion.

Trigger Audio Alarm: If selected, you will hear the warning sound on detecting a motion based alarm.

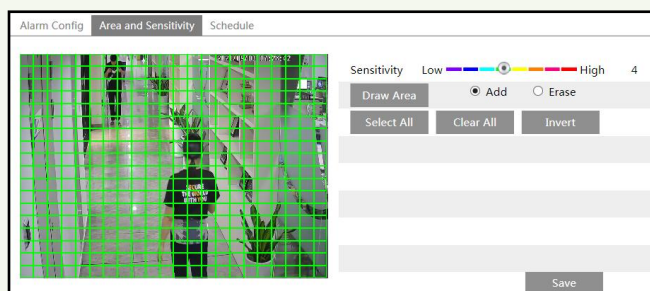
Trigger SD Card Snapshot: If selected, the system will capture images on motion detection and save the images on an SD card.

Trigger SD Card Recording: If selected, the video will be recorded on an SD card on motion detection.

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

Trigger FTP: If “Trigger FTP” and “Attach Picture” are checked, the captured pictures will be sent to the FTP server address. Please refer to [FTP configuration](#) for more details.

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



Move the “Sensitivity” scroll bar to set the sensitivity. A higher sensitivity value means that motion will be triggered more easily.

Select “Add” and click “Draw”. Drag the mouse to draw the motion detection area; Select “Erase” and drag the mouse to clear motion detection area.

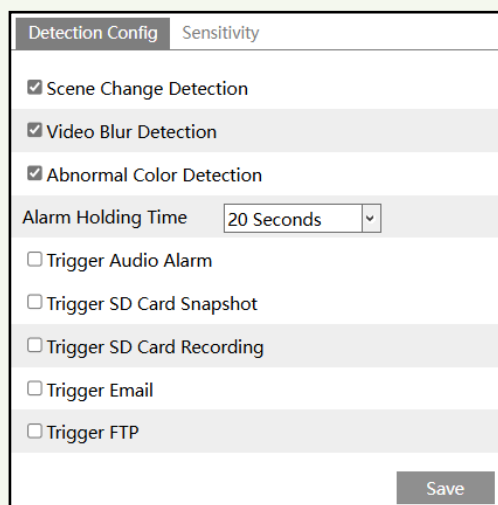
After that, click “Save” to save the settings.

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

3.9.2 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** as shown below.



1. 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.

3. 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.

4. 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.

3.9.3 Exception Alarm

● SD Card Full

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

SD Card Full	SD Card Error
☒ Enable	
Alarm Holding Time	20 Seconds ▼
☐ Trigger Email	
☐ Trigger FTP	
Save	

2. Click “Enable”.
3. Set the alarm holding time and alarm trigger options. Trigger Email and FTP.

● 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.

SD Card Full	SD Card Error
☒ Enable	
Alarm Holding Time	20 Seconds ▼
☐ Trigger Email	
☐ Trigger FTP	
Save	

2. Click “Enable”.
3. Set the alarm holding time and alarm trigger options. Trigger Email and FTP.

3.9.4 Alarm Server

Go to **Alarm** → **Alarm Server** as shown below.

Set the server address, port, heartbeat and heartbeat interval. When an alarm occurs, the camera will transfer the alarm event to the alarm server. If an alarm server is not needed, there is no need to configure this section.

Server Address	0.0.0.0
Port	8010
Heartbeat	Disable ▼
Heartbeat interval	30 Second
OK	

3.9.5 Person Detection

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

Detection Config	Schedule
☒ Enable	
Alarm Holding Time	20 Seconds ▼
☐ Trigger SD Card Snapshot	
☐ Trigger SD Card Recording	
☐ Trigger Email	
☐ Trigger FTP	
Save	

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

3.10 Network Configuration

3.10.1 TCP/IP

Go to **Config → Network → TCP/IP** 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.

3.10.2 Port

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

HTTP Port	80
HTTPS Port	443
Data Port	9008
RTSP Port	554
Persistent connection Port	8080 ☒ Enable
WebSocket Port	7681

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.

3.10.3 Server Configuration

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

☒ Enable	
Server Port	2009
Server Address	
Device ID	1

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.

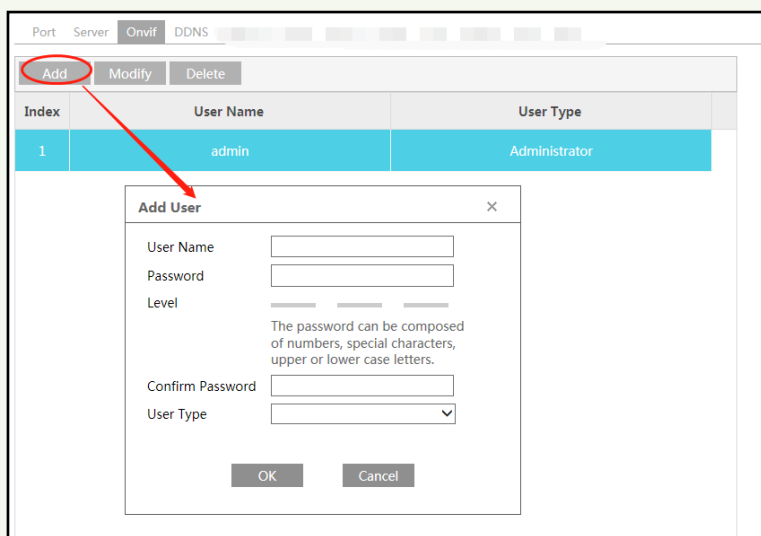
3. Enter the above-mentioned server address, server port and device ID in the corresponding boxes. Click the “Save” button to save the settings.

3.10.4 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 simultaneously. 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.

3.10.5 DDNS

If the camera is set up with a DHCP connection, DDNS should be set for the internet.

1. Go to **Config** → **Network** → **DDNS**.

☒ Enable
Server Type www.dyndns.com
User Name
Password
Domain
Save

2. Apply for a domain name. Take www.dvr dyndns.com for example.

Enter www.dvr dyndns.com in the IE address bar to visit its website. Then Click the "Registration" button.

NEW USER REGISTRATION	
USER NAME	XXXX
PASSWORD	•••••
PASSWORD CONFIRM	•••••
FIRST NAME	XXX
LAST NAME	XXX
SECURITY QUESTION.	My first phone number.
ANSWER	XXXXXXXX
CONFIRM YOU'RE HUMAN	718408 New Captcha Enter the text you see above
Submit Reset	

Create domain name.

<i>You must create a domain name to continue.</i>	
Domain name must start with (a-z, 0-9). Cannot end or start, but may contain a hyphen and is not case-sensitive.	
	dvr dyndns.com Request Domain

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

Click a name to edit your domain settings.

NAME	STATUS	DOMAIN
654321ABC		654321abc.dvrdyns.com

Last Update: *Not yet updated* IP Address: 210.21.229.138

Create additional domain names

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

3.10.6 SNMP

To get camera status, parameters and alarm information and remotely manage the camera, the SNMP function can be used. Before using SNMP, please install an SNMP management tool and set the parameters of the SNMP, such as SNMP port, trap address.

1. Go to **Config** → **Network** → **SNMP**.

SNMP v1/v2	
☐ Enable SNMPv1	
☐ Enable SNMPv2	
Read SNMP Community	public
Write SNMP Community	private
Trap Address	192.168.226.201
Trap Port	162
Trap community	public
SNMP v3	
☐ Enable SNMPv3	
Read User Name	public
Security Level	auth, priv
Authentication Algorithm	☒ MD5 ☐ SHA
Authentication Password	*****
Private-key Algorithm	☒ DES ☐ AES
Private-key Algorithm	*****
Write User Name	private
Security Level	auth, priv
Authentication Algorithm	☒ MD5 ☐ SHA
Authentication Password	*****
Private-key Algorithm	☒ DES ☐ AES
Private-key Algorithm	*****
Other Settings	
SNMP Port	161
Save	

2. Check the corresponding version checkbox (Enable SNMPv1, Enable SNMPv2, Enable SNMPv3) according to the version of the SNMP software that will be used.
3. Set the values for “Read SNMP Community”, “Write SNMP Community”, “Trap Address”, “Trap Port” and so on. Please make sure the settings are the same as that of the SNMP software.

Note: Please use the version in accordance with the security level you need. The higher the

version is, the higher the level of the security is.

3.10.7 802.1x

If it is enabled, the camera's data can be protected. When the camera is connected to the network protected by the IEEE802.1x, user authentication is needed.

☒ Enable	
Protocol Type	EAP_MD5
EAPOL Version	1
User Name	test
Password	•••••
Confirm Password	•••••

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.

3.10.8 RTSP

Go to **Config** → **Network** → **RTSP**.

☒ Enable			
Port	554		
Address	rtsp://IP or domain name:port/profile1		
	rtsp://IP or domain name:port/profile2		
	rtsp://IP or domain name:port/profile3		
Multicast address			
Main stream	239.0.0.0	50554	☐ Automatic start
Sub stream	239.0.0.1	51554	☐ Automatic start
Third stream	239.0.0.2	52554	☐ Automatic start
Audio	239.0.0.3	53554	☐ Automatic start
☐ Allow anonymous login (No username or password required)			
Save			

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 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 player to play the video.

Note:1. This camera supports local preview through players (for example: VLC). 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.

3.10.9 RTMP

You can access the third-party (like YouTube) to realize video live view through RTMP protocol.

Go to **Config** → **Network** → **RTMP**.

☒ Enable (Only supports H264)

Stream Type: ☒ Main stream ☐ Sub stream ☐ Third stream

Reconnect After Timeout: Second

Server Address:

Connection Status:

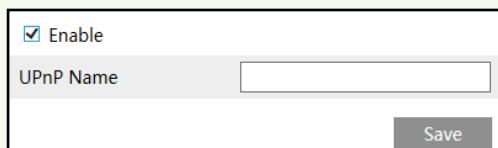
Check “Enable”, select stream type, set the reconnection time after timeout and server address as needed.

Server address: Enter the server address allocated by the third party server.

After that, click “Save” to save the settings. Then click “Refresh” to view the connection status.

3.10.10 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.

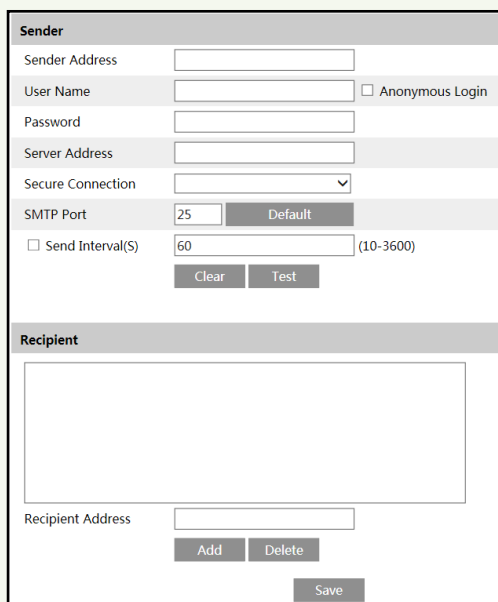


The UPnP configuration interface includes a checkbox labeled "Enable" which is checked. Below it is a text input field for "UPnP Name". At the bottom right is a "Save" button.

3.10.11 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**.



The Email configuration interface is divided into two main sections: "Sender" and "Recipient".

Sender Section:

- Sender Address: Text input field.
- User Name: Text input field, with an "Anonymous Login" checkbox.
- Password: Text input field.
- Server Address: Text input field.
- Secure Connection: Pull-down menu.
- SMTP Port: Text input field (25) with a "Default" button.
- Send Interval(S): Text input field (60) with a range of (10-3600) and a "Send Interval(S)" checkbox.
- Buttons: "Clear" and "Test".

Recipient Section:

- Recipient Address: Text input field.
- Buttons: "Add", "Delete", and "Save".

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.

3.10.12 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.

3.10.13 HTTPS

HTTPS provides authentication of the web site and protects user privacy.

Go to **Config** → **Network** → **HTTPS** as shown below.

☐ Enable

Certificate installed	C=CN, ST=GD, L=SZ, O=IPC, OU=embedded	Delete
Attribute	Issued to: C=CN, ST=GD, L=SZ, O=IPC, OU=embeddedsoftware, H=localhost, Issuer: C=CN, ST=GD, L=SZ, O=IPC, OU=embeddedsoftware, H=localhost, Validity date: 2020-03-14 08:12:45 ~ 2033-11-21 08:12:45	

Save

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.

☐ Enable

Installation type

☒ Have signed certificate, install directly

☐ Create a private certificate

☐ Create a certificate request

Install certificate

Browse Install

Save

* 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.

☐ Enable

Installation type

☐ Have signed certificate, install directly

☒ Create a private certificate

☐ Create a certificate request

Create a private certificate

Create

Save

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.

3.10.14 HTTP POST

Go to **Config** → **Network** → **HTTP POST**.

Check “Enable”, select protocol type and then set the server address (IP address/domain name), server port and heartbeat interval.

Server address: the IP address/domain name of the third-party platform.

Server port: the server port of the third-party platform.

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

3.10.15 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.

3.10.16 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	13
Alarm DSCP	35
Manager DSCP	53

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.

3.10.17 Wi-Fi Settings

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

☒ Enable

Wi-Fi Networks
Search

Index	SSID	Working Mode	Security Mode	Channel	Signal	Mbps	Connection
1	FDCA	Manage	WPA2-personal	11	49	150	Unconnected
2	-EBYXSR	Manage	WPA2-personal	1	48	150	Unconnected
3	KFC	Manage	WPA2-personal	1	48	150	Unconnected
4	leader	Manage	WPA2-personal	8	48	150	Unconnected
5	HY	Manage	WPA2-personal	6	44	150	Unconnected

1 / 1
20
View 1 - 15 of 15

Wi-Fi

SSID Test

Security Mode WPA-personal

Key 1

Encryption Type AES

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”.

LAN	
☒	Obtain an IP address automatically
☐	Use the following IP address
IP Address	192.168.1.201
Subnet Mask	255.255.255.0
Gateway	192.168.1.1
Preferred DNS Server	192.168.1.1
Alternate DNS Server	8.8.8.8

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.

3.10.18 SIP

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

☒ Enable VOIP Gateway	
Register User Name	
Registration Password	
Server Address	
Server Port	0
Expiry Time	0 Minutes
Register Status	Register Failed
Number	
Display User Name	
Save	

Enable “VOIP Gateway” and set the relevant parameters.

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

3.11 Security Configuration

3.11.1 User Configuration

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

Add Modify Delete Security Question		
Index	User Name	User Type
1	admin	Administrator

Add user:

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

Add User

User Name

Password

Level

The password can be composed of numbers, special characters, upper or lower case letters.

Confirm Password

User Type

Advanced User

☐ Select All

☐ Remote storage settings

☐ Remote image settings

☐ Remote alarm server configuration

☐ Remote intelligent event configuration

☐ Remote network advanced configuration

☐ Remote security management

☐ Remote configuration backup and recovery

OK

Cancel

2. Enter user name in the “User Name” textbox.
3. 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** 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.

- The “Edit user” dialog box pops up by clicking the “Modify” button.

Edit User

User Name: admin

Old Password:

New Password:

Level:

The password can be composed of numbers, special characters, upper or lower case letters.

Confirm Password:

User Type: Administrator

- ☒ Select All
- ☒ Remote storage settings
- ☒ Remote image settings
- ☒ Remote alarm server configuration
- ☒ Remote intelligent event configuration
- ☒ Remote network advanced configuration
- ☒ Remote security management
- ☒ Remote configuration backup and recovery

OK Cancel

- Enter the old password of the user in the “Old Password” text box.
- Enter the new password in the “New password” and “Confirm Password” text box.
- Select the user permissions for advanced or normal user.
- Click the “OK” button to save the settings.

Delete user:

- Select the user to be deleted in the user configuration list box.
- 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 to reset the password after you forget the password.

3.11.2 Online User

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

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

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

3.11.3 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.

3.11.4 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

Security Service	Password Security	Authentication
Password Level	Weak ▼	
Expiration Time	Never ▼	
		Save

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.

Security Service	Password Security	Authentication
HTTP Authentication	Basic ▼	
		Save

3.12 Maintenance Configuration

3.12.1 Backup and Restore

Go to Config→Maintenance→Backup and Restore.

The screenshot displays a web-based configuration interface with three main sections:

- Import Setting:** Contains a text input field labeled "Path" followed by a "Browse" button. Below this is a button labeled "Import Setting".
- Export Settings:** Contains a single button labeled "Export Settings".
- Default Settings:** Features a "Keep" label next to a container with three unchecked checkboxes: "Network Config", "Security Configuration", and "Image Configuration". Below these checkboxes is a button labeled "Load Default".

● Import & Export Settings

Configuration settings of the camera can be exported from 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.

3.12.2 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.

3.12.3 Upgrade

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

 Do not allow downgrading from the current version to the lower version.
Do not disconnect power during the upgrade.

Local upgrade

Path

 **System 1: Normal** | System 2: Normal

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:

1. You cannot downgrade to a lower version.
2. Do not refresh/close the browser or disconnect the camera from the network during the upgrade, or it will cause system failure. After the device is successfully upgraded, there are ten minutes of observation. During this observation period, do not upgrade the device again.

Note: To decrease the upgrade risk, this series of cameras adopts two systems. After one system is successfully upgraded, the other system will be synchronized. If one system fails caused by power failure or other reasons during the upgrade, the other system will not be affected and the camera still can work normally. You can also upgrade your camera through the normal system.

3.12.4 Operation Log

To query and export log:

1. Go to **Config** → **Maintenance** → **Operation Log**.

Main Type	All logs	Sub Type	All logs			
Start Time	2024-08-14 00:00:00	End Time	2024-08-14 23:59:59	Search	Export	
Index	Time	Main Type	Sub Type	User Name	Login IP	Hostname
1	2024-08-14 06:55:41	Operation	System config modify			
2	2024-08-14 06:55:31	Operation	System config modify			
3	2024-08-14 06:26:35	Operation	Log in	admin	10.15.1.155	
4	2024-08-14 04:42:28	Operation	Log out	admin	10.15.1.155	
5	2024-08-14 03:41:33	Operation	Video config modify	admin	10.15.1.155	
6	2024-08-14 03:41:28	Operation	Video config modify	admin	10.15.1.155	

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.

4.1 Image Search

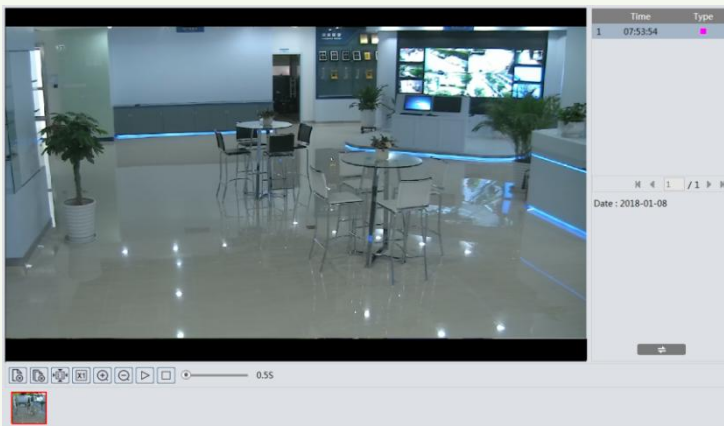
Click **Search** to go to the interface as shown below. Images that are saved on the SD card can be found here.

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



● Local Image Search

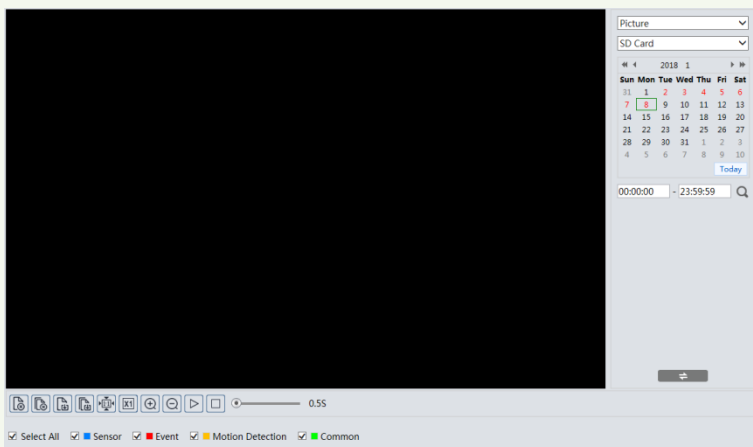
1. Choose “Picture”—“Local”.
2. Set time: Select date and choose the start and end time.
3. Click  to search the images.
4. Double click a file name in the list to view the captured photos as shown above.



Click  to return to the previous interface.

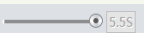
● SD Card Image Search

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.

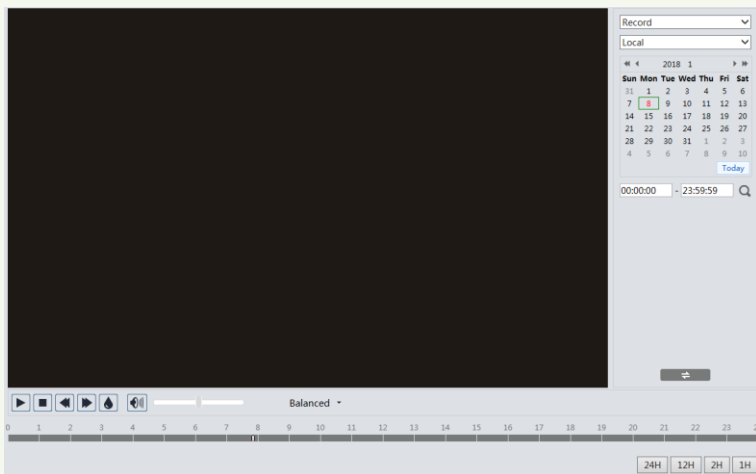
Icon	Description	Icon	Description
	Close: Select an image and click this button to close the image.		Close all: Click this button to close all images.
	Save: Click this button to select the path for saving the image on the PC.		Save all: Click this button to select the path for saving all pictures on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

4.2 Video Search

4.2.1 Local Video Search

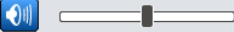
Click Search to go to the interface as shown below. Videos were recorded locally to the PC can be played in this interface.

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.

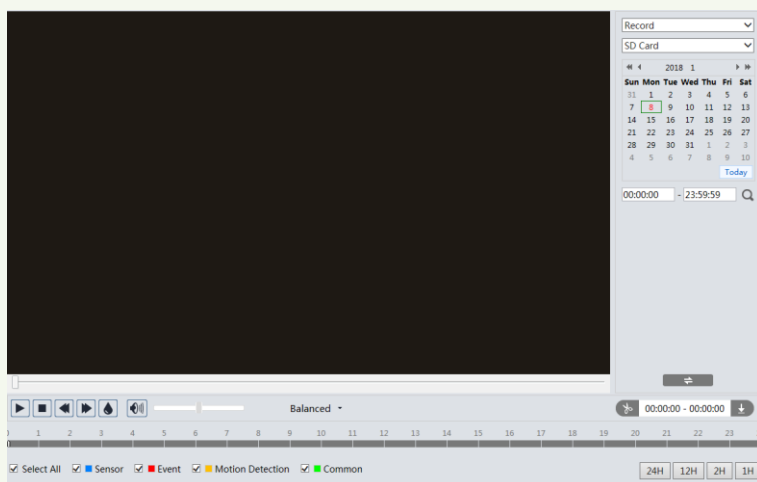


Icon	Description	Icon	Description
	Play button. After pausing the video, click this button to continue playing.		Pause button
	Stop button		Speed down
	Speed up		Watermark display
	Enable / disable audio; drag the slider to adjust the volume after enabling audio.		

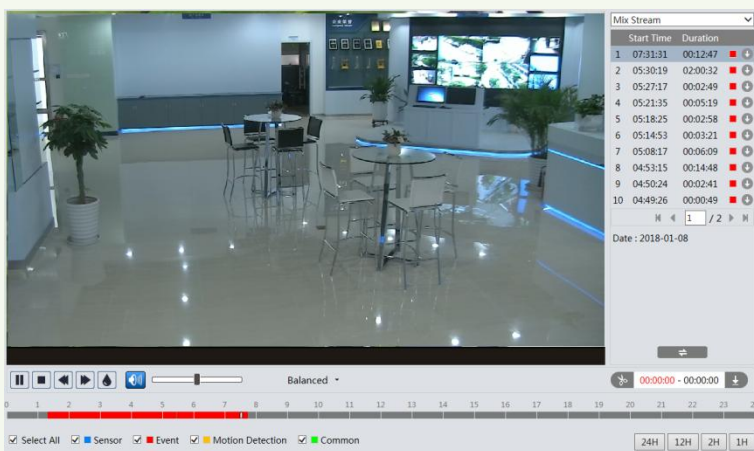
4.2.2 SD Card Video Search

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: ⏮ and ⏭ cannot be displayed 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.

Index	Process	Record	Start Time	End Time	Path	Operate
1	100%	Cut	2018-01-16 01:1...	2018-01-16 01:1...	Favorites	Open
Set up D:\Favorites Clear List Close						

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.

5 Data Record Search

● Event Log Search

Click **Data Record**.

You can search the logs related to the access control events by filtering main/sub type. The main type includes “All logs”, “Unlocking event”, “Authentication Type”, “Lock Status” and “Alarm event”. Each main type has many sub types. Please search logs as needed. In addition, you can also search logs by operation result, time and account.

Access Event Log										
Main Type All logs	Index	ID NO.	Card NO.	Room No.	IP	Account	Channel	Event Type	Time	Operation Result
Sub Type All logs	1	--	--	--	--	--	1	Lock Close	2025-05-29 16:20:40	--
Operation Result All	2	--	--	--	--	--	1	Lock Open	2025-05-29 16:20:37	--
Start Time 2025-05-26 00:00:00	3	--	--	--	10.15.1.155	admin	1	Remote Unlocking	2025-05-29 16:20:37	--
End Time 2025-05-30 23:59:59										
Account Search										
Export										

Account: refers to the accounts that are used to open the door remotely, like APP account, web login account, etc.

For the searched logs, you can view its detailed information on the right table. If a snapshot is captured, click “Snapshot” to view the captured picture.

Appendix 1 How to Call Indoor Station

Appendix 1-1 One Door Station Calls One Indoor Station

Application: Install one door station and bind one indoor station. Press the corresponding button to call indoor station

The setting steps are as follows:

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

Config	
Device Type	Main Door Station ▼
Sector	0
Building No.	0
Unit No.	0
Floor No.	0
Number	0
Community No.	0
☒ Device Binding Authentication	

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.

Device Information	
Indoor Station Type	Indoor Station
Room No.	101
Binding State	Failure
Device Binding Authentication	☒

Device Management	
Main Door Station	10.100.50.6
IP Camera	
ONVIF Camera	
RTSP Settings	
IPC	Main 10.100.50.6

Note: If “Device Binding Authentication” is enabled in the main door station, you need to enter the password of the main door station’s admin when binding the main door station to the indoor 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: Install one door station and bind multiple indoor stations with the same room number set. Press the corresponding button 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”.

Config	
Device Type	Main Door Station
Sector	0
Building No.	0
Unit No.	0
Floor No.	0
Number	0
Community No.	0
☒ Device Binding Authentication	

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.

Device Information	
Indoor Station Type	Indoor Station
Room No.	101
Binding State	Failure
Device Binding Authentication	☒

Device Management	
Main Door Station	10.100.50.6
IP Camera	
ONVIF Camera	
RTSP Settings	>
IPC	Main 10.100.50.6

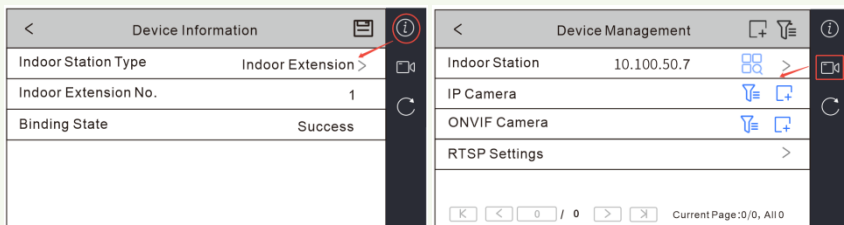
Note: If “Device Binding Authentication” is enabled in the main door station, you need to enter the password of the main door station’s admin when binding the main door station to the indoor station.

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.



Note: If “Device Binding Authentication” is enabled in the indoor station, you need to enter the password of the indoor station’s admin when binding the indoor station to the indoor extension.

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

Application B: Install one door station and bind multiple indoor stations with the different room number set. Press different buttons 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 buttons to call different indoor stations. (See Button Calling Settings for details)

Appendix 1-3 Multiple Door Stations Call One Indoor Station

Application: Install multiple door stations and bind one indoor station. Press the corresponding buttons 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”.

Config	
Device Type	Main Door Station ▼
Sector	0
Building No.	0
Unit No.	0
Floor No.	0
Number	0
Community No.	0
☒ Device Binding Authentication	

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”.

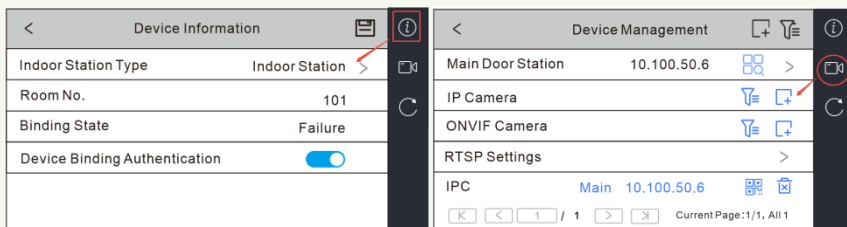
Config	
Device Type	Sub Door Station ▼
Main Door Station IP	10.100.50.6
User Name	☐ Anonymous
Password	
Binding State	
Sector	0
Building No.	0
Unit No.	0
Floor No.	0
Number	1
Community No.	0

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.

User Name and Password: If “Device Binding Authentication” of the main door station is enabled, you need to enter the user name and password of the main door station.

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.



Note: If “Device Binding Authentication” is enabled in the main door station, you need to enter the password of the main door station’s admin when binding the main door station to the indoor 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:

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”.

Config

Device Type	Main Door Station
Sector	0
Building No.	0
Unit No.	0
Floor No.	0
Number	0
Community No.	0
☒ Device Binding Authentication	

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”.

Config	
Device Type	Sub Door Station
Main Door Station IP	10.100.50.6
User Name	☐ Anonymous
Password	
Binding State	
Sector	0
Building No.	0
Unit No.	0
Floor No.	0
Number	1
Community No.	0

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.

User Name and Password: If “Device Binding Authentication” of the main door station is enabled, you need to enter the user name and password of the main door station.

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.

Device Information		Device Management	
Indoor Station Type	Indoor Station	Main Door Station	10.100.50.6
Room No.	101	IP Camera	
Binding State	Failure	ONVIF Camera	
Device Binding Authentication	☒	RTSP Settings	
		IPC	Main 10.100.50.6

Note: If “Device Binding Authentication” is enabled in the main door station, you need to enter the password of the main door station’s admin when binding the main door station to the indoor station.

5. 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.

6. Press different buttons 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”.

Config	
Device Type	Main Door Station ▼
Sector	0
Building No.	0
Unit No.	0
Floor No.	0
Number	0
Community No.	0
☒ Device Binding Authentication	

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”.

Config	
Device Type	Sub Door Station ▼
Main Door Station IP	10.100.50.6
User Name	☐ Anonymous
Password	
Binding State	
Sector	0
Building No.	0
Unit No.	0
Floor No.	0
Number	1
Community No.	0

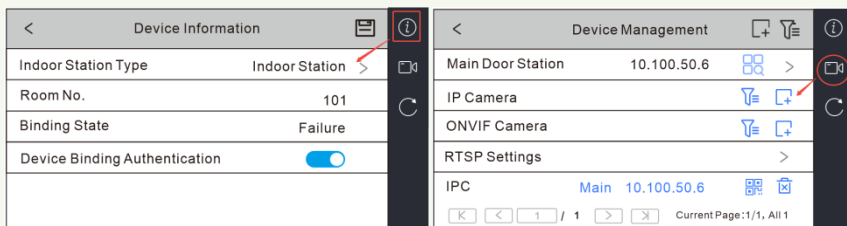
Enter the actual IP address of the main door station and door station no.

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.

User Name and Password: If “Device Binding Authentication” of the main door station is enabled, you need to enter the user name and password of the main door station.

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.

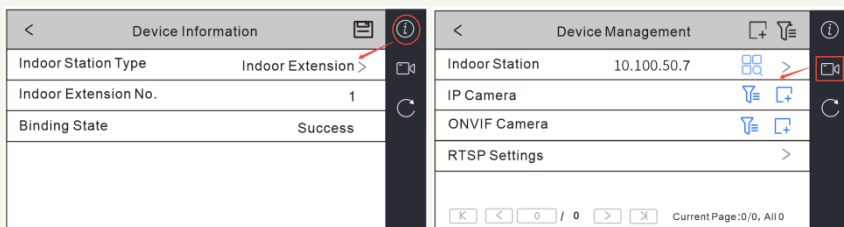


Note: If “Device Binding Authentication” is enabled in the main door station, you need to enter the password of the main door station’s admin when binding the main door station to the indoor station.

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.



Note: If “Device Binding Authentication” is enabled in the indoor station, you need to enter the password of the indoor station’s admin when binding the indoor station to the indoor extension.

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.

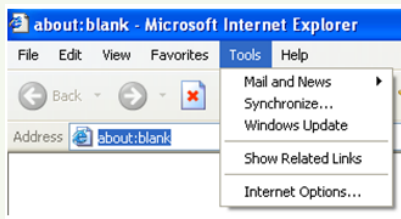
IP tool cannot search devices.

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.

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

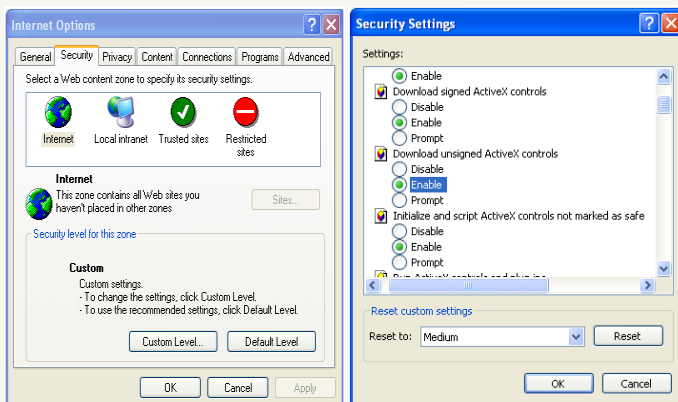


② Select Security-----Custom Level....

③ Enable all the options under “ActiveX controls and plug-ins”.

④ Click OK to finish setup.

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



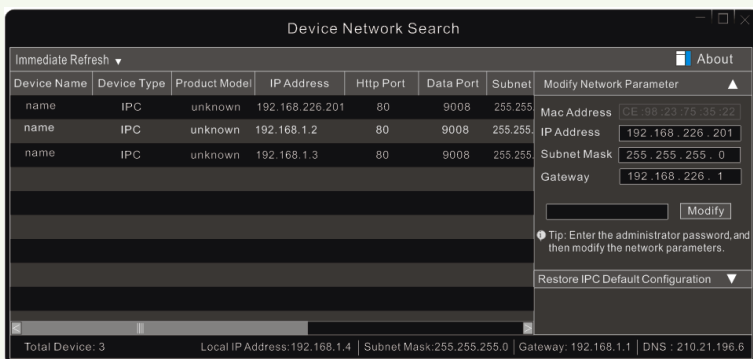
No sound can be heard.

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 ▼ next to “Restore IPC Default Configuration” to expand the menu, then enter the MAC address and click “OK”. After that, manually reboot your camera within 30s. Then the camera will successfully restore to the factory default setting

Device Name	Device Type	Product Model	IP Address	Http Port	Data Port	Subnet
name	IPC	unknown	192.168.226.201	80	9008	255.255.255.0
name	IPC	unknown	192.168.1.2	80	9008	255.255.255.0
name	IPC	unknown	192.168.1.3	80	9008	255.255.255.0

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 an 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.