# Video Intercom Indoor Station

GCN7000B, GCN7000W

User Manual

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

genie

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

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

## About the Manual

- This manual is suitable for many models. All examples, screenshots, figures, charts, and illustrations used in the manual are for reference purpose, and actual products may be different with this Manual.
- Please read this user manual carefully to ensure that you can use the device correctly and safely.
- Within the maximum scope permitted by the law, the products described in this Manual (including hardware, software, firmware, etc.) are provided “AS IS”. The information in this document (including URL and other Internet site reference data) is subject to change without notice. This Manual may contain technical incorrect places or printing errors. This information will be periodically updated, and these changes will be added into the latest version of this Manual without prior notice.

## 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.
- 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 place the device in a damp, dusty extremely hot or cold environment, or the locations with strong electromagnetic radiation or unstable lighting.

### 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.
- Always use a dry soft cloth to clean the device.

# 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

- It is recommended to set the firewall of your router. But note that some important ports cannot be closed (like HTTP 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.

# Regulatory Information

## FCC Information

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

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

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

**2. FCC conditions:**

- This device complies with part 15 of the FCC Rules. Operation of this product is

subject the following two conditions:

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

## RoHS

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

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

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

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

# Table of Contents


**1 Wizard Settings** ..... **1**

**2 Settings** ..... **5**

2.1 Network Settings ..... 5

2.1.1 Local Network Settings ..... 5

2.1.2 WIFI Settings ..... 5

2.2 Device Management ..... 6

2.3 Indoor Station Settings ..... 8

2.4 Call and Volume Settings ..... 10

2.4.1 Ringtone and Volume Settings ..... 10

2.4.2 Do Not Disturb ..... 10

2.4.3 Auto Snapshot/Record when Calling in ..... 11

2.4.4 Leave Messages ..... 11

2.4.5 Answer or Hang Up a Call ..... 11

2.5 Password Settings ..... 12

2.6 Zone Settings ..... 13

2.7 Scene Settings ..... 14

2.8 Device Information ..... 15

2.9 Zone and Time Settings ..... 15

2.10 Local Configuration ..... 15

2.11 Device Reboot ..... 16

2.12 Factory Default Settings ..... 16

2.13 Clean the Screen ..... 16

2.14 Upgrade ..... 16

**3 Live View** ..... **17**

**4 View Records** ..... **19**

4.1 View Alarm Records ..... 19

4.2 View Snapshots ..... 19

4.3 View Recorded Videos ..... 20

**5 Call Logs** ..... **22**

5.1 Make a Call ..... 22

5.2 Call Logs ..... 22

**6 Configuration via Web** ..... **24**

6.1 Web LAN Access ..... 24

6.2 Web WAN Access ..... 24

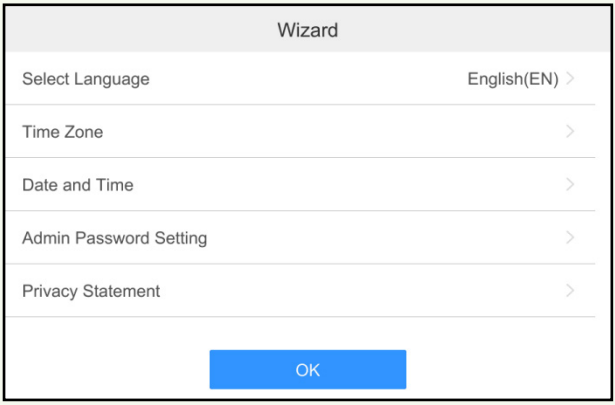
6.3 Web Remote Control.....25
6.4 Remote Preview.....25
6.5 Remote Playback .....28
6.6 Remote Search and Backup .....29
6.7 Remote Configuration .....29
6.7.1 View Record Status.....29
6.7.2 SD Card Management .....30
6.7.3 Network Settings .....30
6.7.4 Basic Settings .....33
6.7.5 Factory Default Settings .....33
6.7.6 Upgrade .....33
6.7.7 Backup and Restore .....33
6.7.8 Reboot.....34
6.7.9 Auto Maintenance.....34
6.7.10 View Log .....34
6.7.11 View System Information .....34
6.7.12 Account and Security .....34

**Appendix**
**..... 37**
**Appendix 1 How to Call Indoor Station..... 37**
Appendix 1-1 One Door Station Calls One Indoor Station.....37
Appendix 1-2 One Door Station Calls Multiple Indoor Stations .....38
Appendix 1-3 Multiple Door Stations Call One Indoor Station.....39
Appendix 1-4 Multiple Door Stations Call Multiple Indoor Stations ...41

**Appendix 2–Troubleshooting..... 45**

# 1 Wizard Settings

Pease make sure all the connections are done properly before you power on the unit. When powered on, the device will boot. After that, a WIZARD window will appear. You can quickly configure the device by wizard setup to make the device work normally.



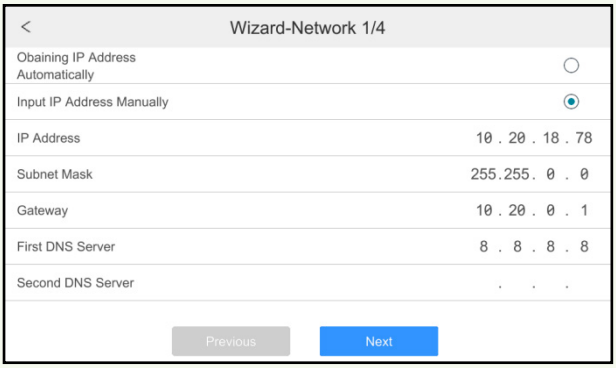

① Choose the language as needed if it is the first time for you to use the wizard.
② Select the time zone according to your location. Enable DST as needed.

- Date and Time Configuration. The date and time of the system need to be set up if you use the wizard for the first time. You can enable “Auto Date and Time” or manually set the date and time. Then select date format and time format as needed.

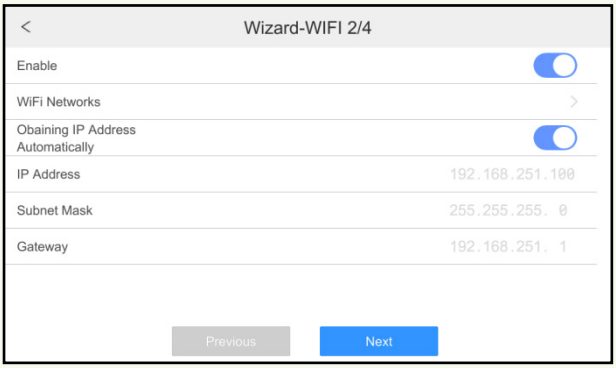
- Create a password for **Admin.**
- Read and agree the privacy statement. Then tap “OK” to enter the network configuration

page.

- Set the local network. The IP address is DHCP by default. It is recommended to input IP address manually to avoid IP address change. Please set the network parameters as needed.

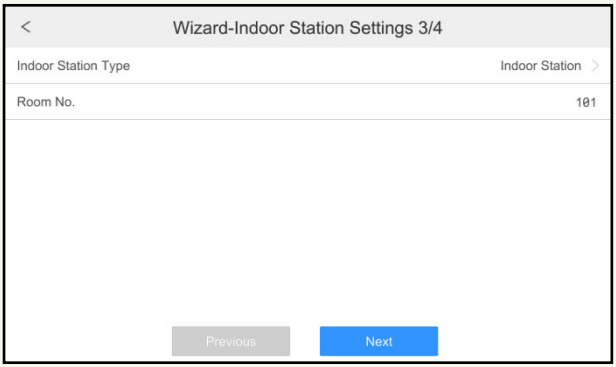



- Wi-Fi settings. Enable Wi-Fi as needed. If you don't want to configure Wi-FI, you can directly go to the next page by tapping "Next".



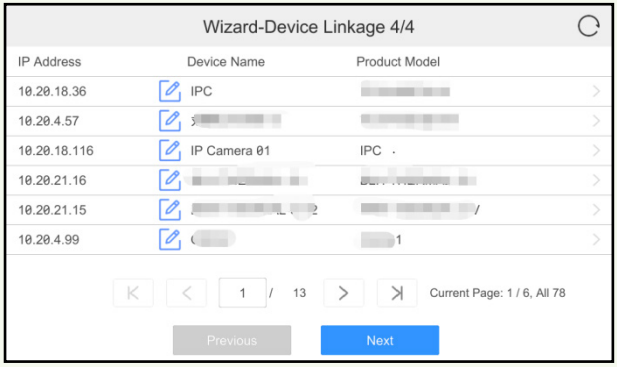

Enable Wi-Fi and then tap "WiFi Networks" to view the wireless device list. Tap the desired WiFi device and then enter the password to connect it. After that, you can view its connection status.

- Indoor station settings. Please select "Indoor Station" or "Indoor Extension" as needed. Please refer to Indoor Station Settings section for details.



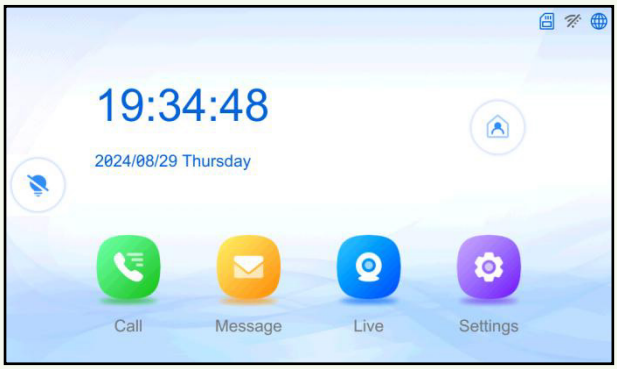

- Link the main door station.

Tap to automatically search the device in the same local network segment. Tap the searched IP address to add. Or tap to enter the IP address of the main door station.



**Add IP camera:** tap , select the IP camera you want to add, enter the password and tap "OK".

Tap to view the SN code and security code of the device. You can add the device quickly by scanning the QR code. Note that only some cameras support QR code display. After the wizard setup is finished, tap "Complete" to enter the home page.




In the home page, tap to turn off the screen immediately. Tap the screen to wake up it.

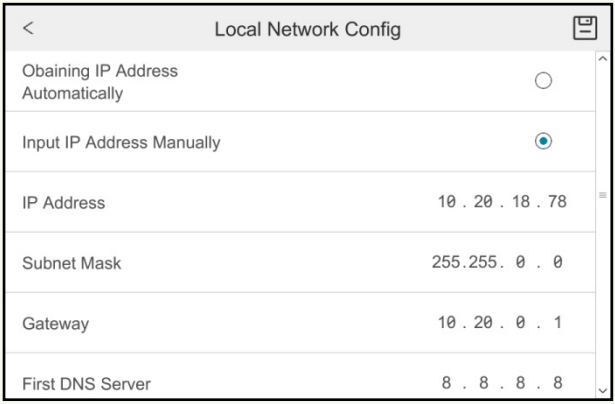
# 2 Settings

## 2.1 Network Settings

**Note**: a. when the wired network and wireless network are enabled simultaneously, the gateway addresses of them must be different, or the network error occurs.
the wired network and wireless network cannot be connected to the same router, or the network error occurs.

### 2.1.1 Local Network Settings

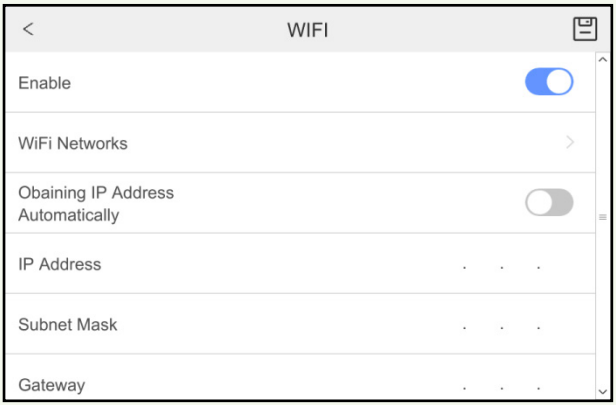
Tap the *Settings* → *Network Config* ( ) → *Local Network Config* to set the network parameters (such as IP address, subnet mask, gateway, etc.) as shown below.



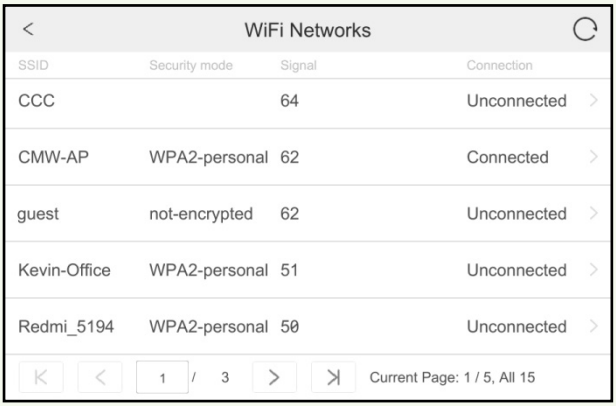

**Note**: It is recommended to input IP address manually to avoid IP address change. If the IP address is changed, the indoor station will not be called successfully.

### 2.1.2 WIFI Settings

Enable WIFI to search the wireless device. Click WIFI to enter the wireless device. *Settings* → *Network Config (* ) → *WIFI.*




Tap “WiFi Networks” to view the wireless device list. Tap the desired WiFi device and then enter the password to connect it. After that, you can view its connection status as shown below.

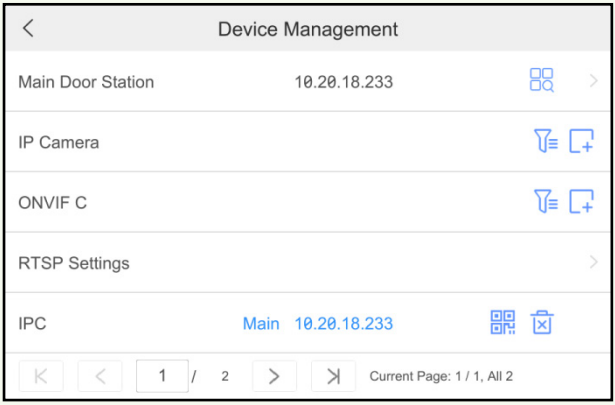



3. Manually enter the IP address, subnet mask and gateway as needed.

**Note**: It is not recommended to obtain the IP address automatically. Because the IP address may be changed by using this way. If the IP address is changed, the indoor station will not be called successfully.

## 2.2 Device Management

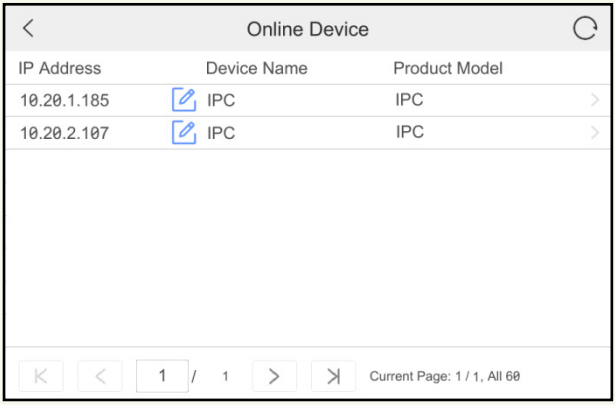
*Tap Settings (entering the password of Admin) → Device Management* on the screen to enter the device management interface.




Tap to ch the main door station in the same local network. Tap the searched IP address to add.

Tap to add a device. Enter the device name, IP address, data port, username and password to add a device.

Tap to search the online devices in the same local network. Select a device and then enter the login password to add.

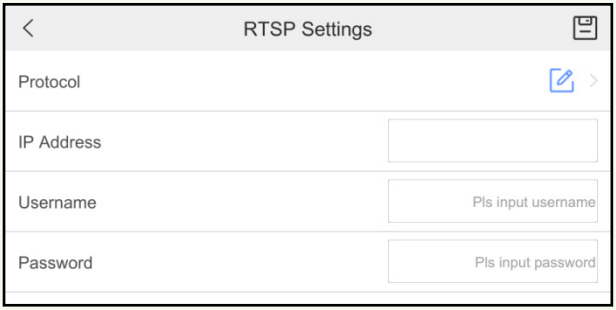



And enter the username and password to add it, you can also modify the IP address by tapping .

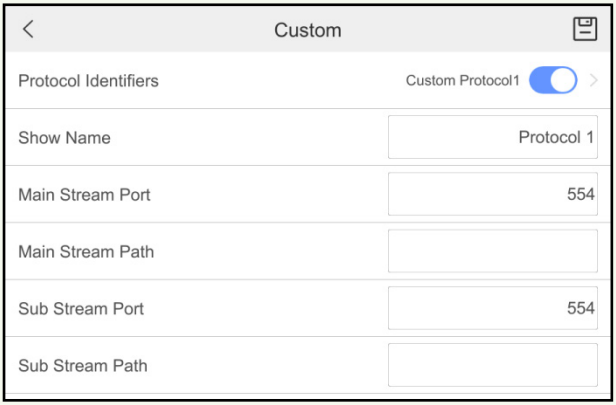
To modify the device information, tap to edit the added device, if its IP address or port is changed, you need to delete it and then add them again.

In addition, you can add cameras through ONVIF and RTSP protocols.

Adding cameras through RTSP protocol:




Protocol: Tap to enter the protocol customization interface.




A maximum of 16 RTSP protocols can be added to the indoor station. Tap  to select the custom protocol to edit. The default main/sub stream port is 554. ase enter the main/sub stream port and path as needed.

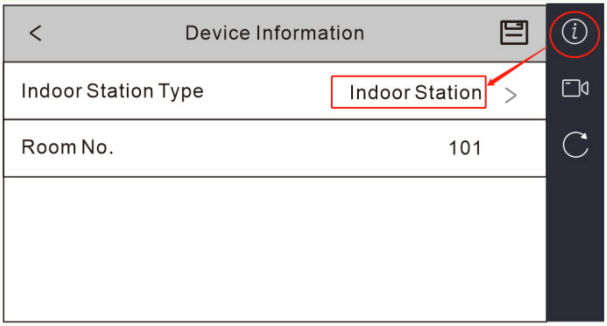
## 2.3 Indoor Station Settings

Tap ***Settings→More Settings ( )→*** ***figuration(entering the password of Admin)*** on the screen to enter the device information interface. In this interface, you can set the indoor station type and room number.

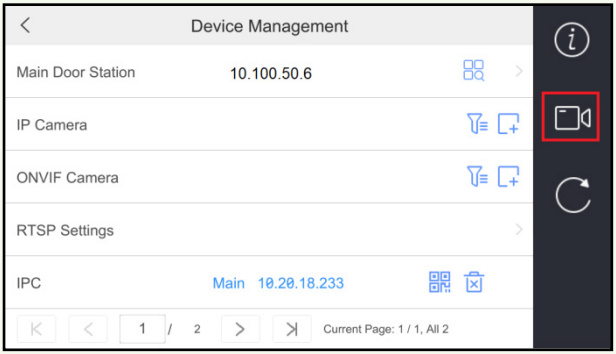
The indoor station type includes “Indoor Station” and “Indoor Extension”.

- Set as “Indoor Station”

Select the indoor station type as “Indoor Station” and then set the room number as needed.



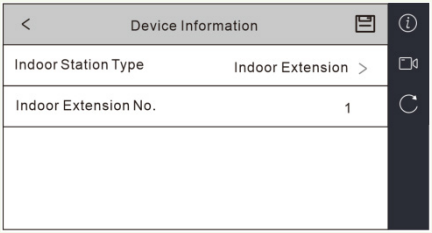

Bind a main door station:

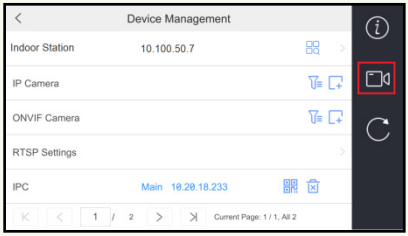



Tap to automatically search the device in the same local network segment. Tap the searched IP address to enter the IP address of the main door station you want to connect.

- Set as “Indoor Extension”
  1. Select the indoor station type as “Indoor Extension” as shown below.
  2. Set the indoor extension no. The indoor extension no. should be a numeric from 1 to 5.
  3. Set the IP address of the indoor station.

**Note**: Up to 5 indoor extensions can be set for 1 indoor station. The indoor station no. is 0 by default.

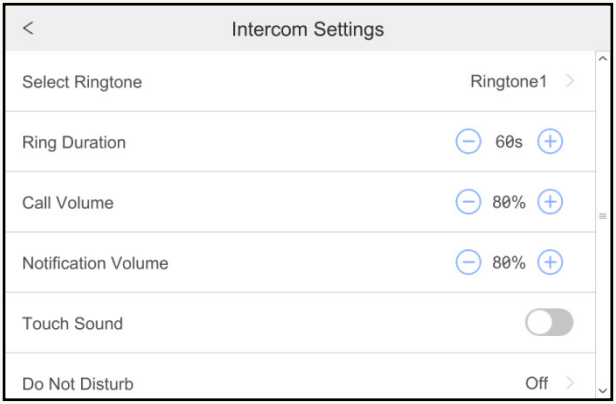



See Appendix 1 How to Call Indoor Station for details.

## 2.4 Call and Volume Settings

Tap ***Settings*** on the screen to enter the intercom settings interface as shown below.




### 2.4.1 Ringtone and Volume Settings

You can set ringtone, ring duration, call volume, notification volume and touch sound in the above interface.

**Note:** There are 4 ringtones by default. Ring duration ranges from 10s to 60s.

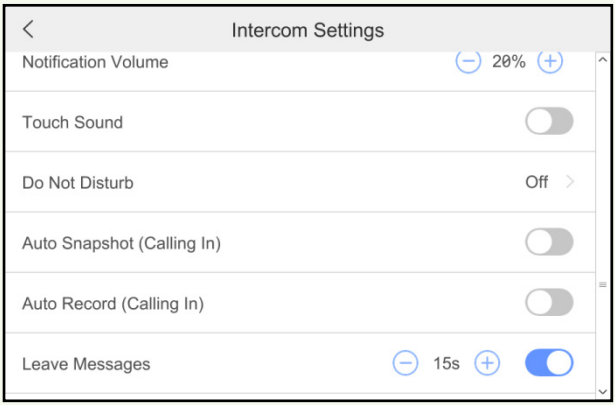
### 2.4.2 Do Not Disturb

After the “Do Not Disturb” function is set, the indoor station will not ring when it is called. You can choose “Off”, “All day” or “Timing”.

If “Off” is selected, the “Do Not Disturb” function will not be enabled.

If “All Day” is selected, the device will not be disturbed all day.

If “Timing” is select, you can set the start time and end time. Within the configured time duration, the device will not be disturbed.



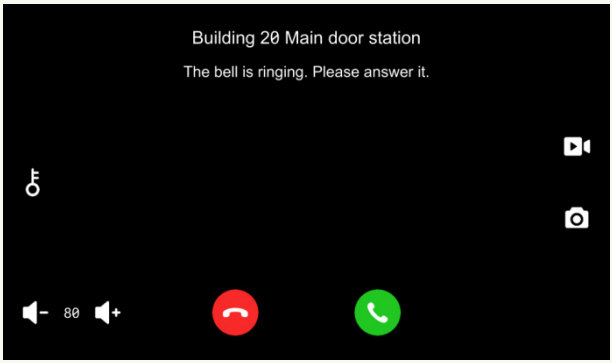

### 2.4.3 Auto Snapshot/Record when Calling in

**Auto Snapshot (Calling In)**: if enabled, it will automatically take a snapshot when someone presses the call button on the door station.
**Auto Record (Calling In)**: if enabled, it will automatically start record when someone presses the call button on the door station. The record will not stop until the call ends or automatically hang up.
**Note**: Before enabling the above-mentioned two functions, please insert a micro SD memory card first.

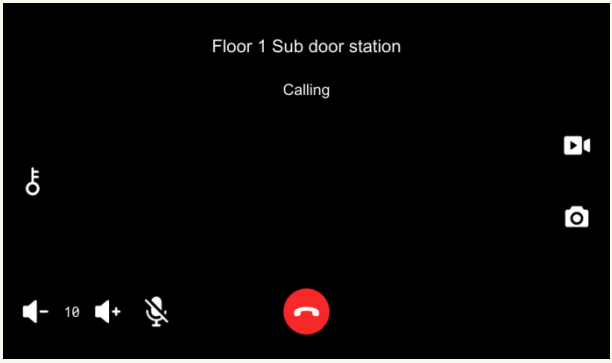
### 2.4.4 Leave Messages

In the intercom settings page, slide down the bar on the right and then enable “Leave Messages” and set the duration (the duration of the message setup).
When a visitor calls the resident through a door station, the visitor will hear “Please leave a message” from the door station if no one answers after the indoor station stops ringing. Then the visitor can leave a message within the set duration. After that, the resident can tap “Message” in the home page of the indoor station to enter the alarm record interface. Tap to listen to the message.

### 2.4.5 Answer or Hang Up a Call




When someone makes a call via the door station, you can answer or hang up through the button shown on the screen. Meanwhile, you can adjust the call volume and enable mute as needed on the screen.




## 2.5 Password Settings

You can modify the configuration password, unlocking password and arming/disarming password.

**Configuration Password:**

Tap the ***Settings*** → ***More Settings*** ( ) → ***Password Settings*** → ***Configuration*** on the right of the screen to view the password settings menu.

You can modify this password as needed.

**Arming/Disarming Password:**

When you want to switch scenes in the home page, you need to enter this password. Tap on the screen to set a password.

***Settings*** → ***More Settings*** ( ) → ***Password Settings*** → ***Arm/Disarm***

**Unlocking Password:**

Tap *Settings → More Settings (* *) → Password Settings → Unlock*

Tap *Settings → More Settings (* *) → Password Settings → Unlock* open the door. Only the main indoor station supports unlocking password setup.

**Scene Password:**

Tap *Settings → More Settings (*  *) → Scene Password* .
If enabled, there is no need to enter a password during scene mode switching.

## 2.6 Zone Settings

You can configure zone and set the corresponding alarm mode in the zone settings interface. When an exception occurs, the indoor station will receive the corresponding alarm message. The zone type includes active infrared, passive infrared, gas detector, smoke detector, door contact, doorbell and panic button.
There are three types of alarm mode: Instant Alarm, 24h Alarm, and Delay Alarm.

- If the zone type is set to be 24h Alarm, the indoor station will receive alarm message when an exception is detected no matter it is in arming mode or disarming mode.
- If the zone type is set to be Instant Alarm, only in arming mode, the indoor station will receive alarm message when an exception is detected.
- When the zone type is set to be Delay Alarm, you can set the exiting delay duration. Only in arming mode, the indoor station will receive alarm message when an exception is detected.

The setting steps are as follows:

1. Tap *Settings → Zone Settings (* *)* on the screen to go to the following interface.

2. Tap a zone (for instance: Zone 1) to display a zone edition window.

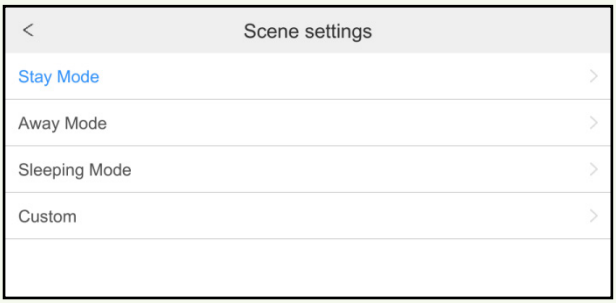
3. Set the zone type and alarm mode.
4. Select NO/NC as needed.
5. Set “Exiting Delay Duration”.
6. Tap “OK” to save the settings.

**Note**: Gas detector, smoke detector or doorbell zone only can be set to be 24h Alarm, among which alarm message of doorbell zone will not be reported.

## 2.7 Scene Settings

You can enable/disable zones for different scenes (including Stay Mode, Away Mode, Sleeping Mode and Custom).

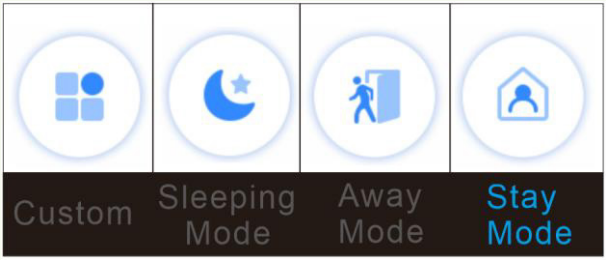
1. Tap ***Settings*** → ***Scene Settings (*** ) on the screen to go to the following interface.




2. Tap Stay mode, Away Mode, Sleeping Mode and Custom to enter the page.
3. Enable zones as needed.

To switch scene

In the home page, tap sarming password to view the following interface. If you don t set the arming/disarming password in advance, you will enter the arming/disarming password setting interface after tapping for the first time.




Select a mode as needed.

Note: After you set the scene password, there is no need to enter a password for scene switching.

You can tap ***Settings → More Settings ( )→ Scene Password*** to set.

## 2.8 Device Information

Tap ***Settings → More Settings ( )→ Device Information*** to view device information, including product model, software version and so on.

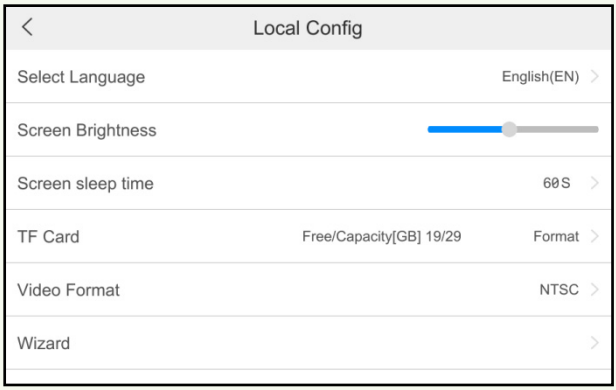
## 2.9 Zone and Time Settings

You can set and save the time zone by tapping ***Settings → More Settings ( )→ Time Zone.***

You can set and save the date and time by tapping ***Settings → More Settings ( )→ Date and Time.***

## 2.10 Local Configuration

Tap ***Settings → More Settings ( )→ Local Config*** to set language, screen brightness, screen sleep time and format TF card in this page.




**Select Language**: Select the screen display language.
**Screen Brightness**: Set the brightness of the screen.
**Screen Sleep Time**: Set how long the screen display will turn off after no operation. Please set it as needed.
**TF Card**: Tap to format the TF card you insert.
**Video Format**: Choose PAL or NTSC as needed.
**Wizard**: Tap to enter the wizard setup interface.

## 2.11 Device Reboot

Tap *Settings* → *More Settings* ( ) → *Reboot* . A window will pop up. Tap "OK" and the device will reboot.

## 2.12 Factory Default Settings

Tap *Settings* → *More Settings* ( ) → *Configuration(entering the password of Admin)* → *Device Maintenance(* ) on the screen to enter the following interface.

You can enable "Keep network configuration" or "Keep security configuration" to start to restore the device to factory default settings. If you want to restore all system settings to the default factory settings, you can directly tap in the above page.

## 2.13 Clean the Screen

More Settings ( ) → *Clean the Screen* . If necessary, you can enable "Clean the Screen" by tapping *Settings* → (moving down the slide bar) and then use clean cloth to wipe it gently, avoiding water or alcohol. One minute later, clean mode will automatically end. You can also hold and press the unlocking button on the screen to exit clean mode.

## 2.14 Upgrade

The setting steps are as follows:

1. Copy .pkg upgrade file to the home directory of your micro SD card (FAT32 format). Then insert the micro SD card to the micro SD card slot of the indoor station.
2. Tap *Settings* → *More Settings* ( ) → *Configuration(entering the password of Admin)* → *Device Maintenance(* ) → *Firmware Upgrade.*
3. The device will be upgraded automatically after reboot. The upgrade progress will show on the screen.

# 3 Live View

In the home page, tap “Live” to enter the live view page as shown below.

You can select 4 screen display mode or single screen display mode as needed.
Button Description:

: Tap to enter full screen mode of the single channel.

: and enter the configuration password to enter the device list interface. You can view the IP address of the added device. Additionally, you can add, delete and modify devices in this page. See Device Management for details.

: Manual record; before starting recording, please insert a micro SD card first.

: Snapshot; before taking a snapshot, please insert a micro SD card first.

le/disable two-way audio (the preview channel must support two-way audio, or this button will be hidden).

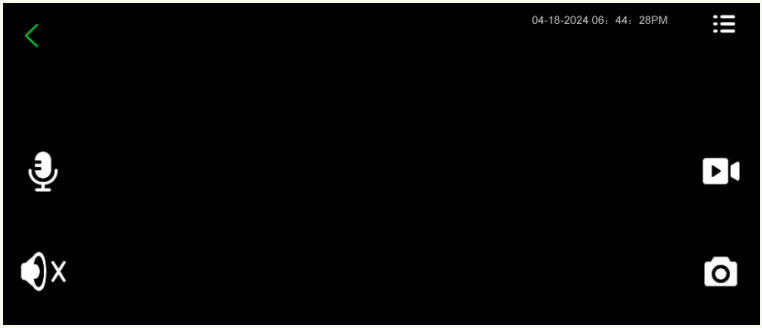
: Enable/disable audio.

/ : Unlock (the preview channel must support this function, or they will be hidden)

When more than 4 IPCs are added, you can tap to switch the preview. A maximum of 16CH can be viewed.

Tap in top right corner to enter the camera list page. In this page, you can view the pictures and IP addresses of the added cameras/door stations. Tap a camera/door station to

view its video as shown below.



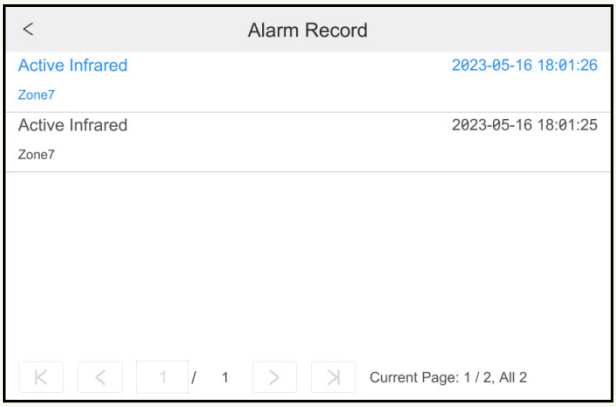

Tap to return to the previous page.

# 4 View Records

Alarm messages, snapshots and recorded videos are saved on the SD card can be found here.

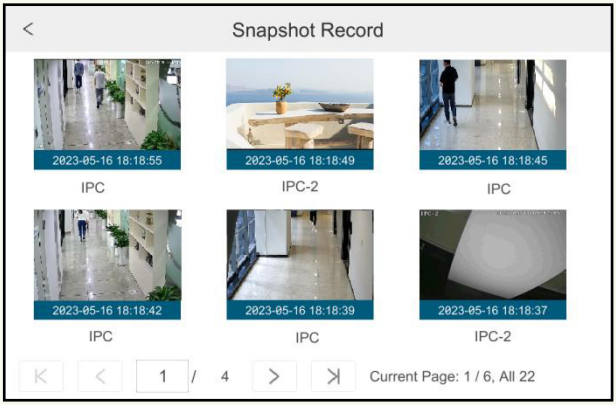
## 4.1 View Alarm Records

In the home page, tap "***Message***" to go to the alarm record page as shown below.




## 4.2 View Snapshots

To go to the *Message* → *Snapshot Record*, you view the captured pictures here.



Tap a picture to zoom in this picture. Tap to delete it.

## 4.3 View Recorded Videos

Tap to view the recorded file list.

Tap a recorded video file and then a play button will show in the middle of the picture. Tap the play button to play the recorded video.

Record Playback
X 1

# 5 Call Logs

In the home page, tap "*Call*" to enter the following page.

## 5.1 Make a Call

- **An indoor station calls another indoor station** : Enter the room number and tap

  **Note**: These two indoor stations must be connected to the same door station.

- **An indoor extension calls another indoor extension:** Enter "

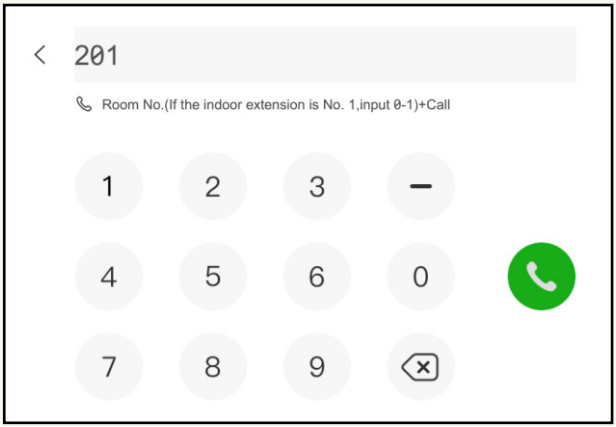
  " and tap

  **Note**: The indoor extensions must be connected to the same indoor station.

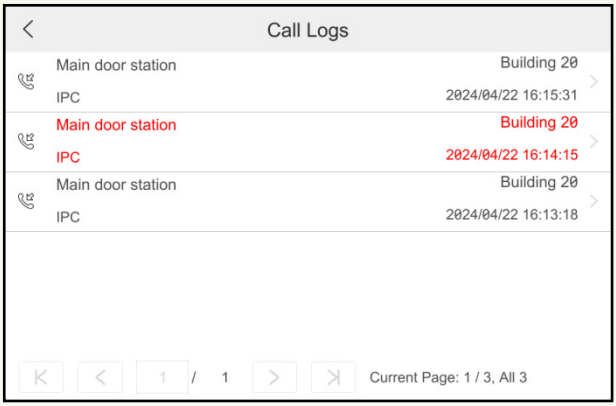
- **An indoor extension calls its indoor station:** Enter the room number and tap

- **An indoor station calls an indoor extension:** Enter "0-the indoor extension number"

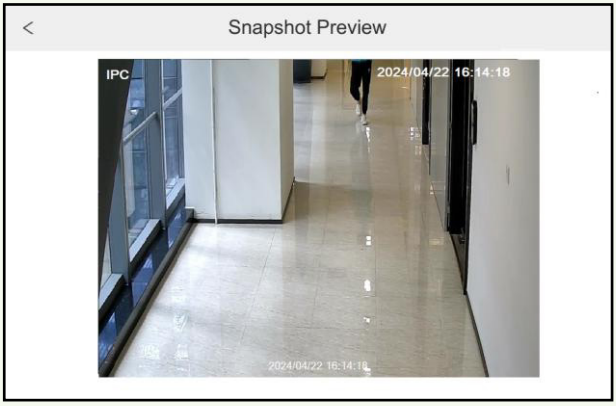
  **Note:** The indoor extension must be connected to the indoor station.




## 5.2 Call Logs




In this page, you can view the call logs of the indoor station.
Red logs are missed call logs.
Tap the call log between the indoor stations to call another indoor station. If “Auto Snapshot (Calling In)” is enabled and a micro SD card is inserted, the corresponding snapshots will be attached in the call logs. Tap one item above to view the snapshot.

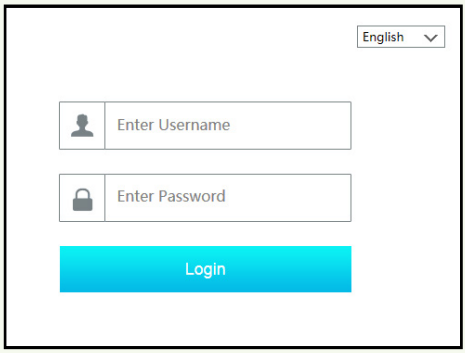


# 6 Configuration via Web

## 6.1 Web LAN Access

① Tap ***Settings*** → ***Network Config (*** )→ ***Lock Network Config*** on the screen to go to the "TCP/IP" interface. Set the IP address, subnet mask, gateway, preferred DNS and alternate DNS of the device.

② Open a web browser on your computer, enter the IP address of the device in the address bar and then press enter to go to the login interface as shown below. You can change the display language on the top right corner of the login interface. Enter the username and password of the device in the interface and then click "Login" to go to the live view interface.




If the device is not activated when you log in via Web, you can connect the device through IP-Tool. Double click the device information in the IP-Tool to open a browser. Then a wizard will appear. Please activate the device first.

***Notes: 1. Please make sure that the IP address of the device and the computer are both in the same local network segment. For example, supposing that the IP address of the computer is 192.168.1.41, the IP address of the device shall be set to 192.168.1.XXX.***

***2. If the HTTP port of the device is not 80, but another number, you need to enter the IP address plus port number in the address bar when accessing the device over a network. For example, the HTTP port is 81. You should enter http://192.168.1.42:81 in the address bar.***

## 6.2 Web WAN Access

**➢Router Access**

① Set the IP address, subnet mask, gateway, preferred DNS and alternate DNS of the device.

② Click ***Settings*** → ***Network*** → ***TCP/IP*** to go to the "TCP/IP" interface.

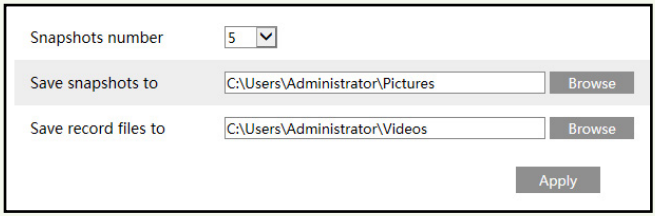
② Set the HTTP port (it is suggested to modify the HTTP port because the default HTTP port 80 might be taken up). Then forward the LAN IP address, HTTP port and server port of the device to the router. Port mapping settings may be different in different routers, so please refer to the user manual of the router for details.

③ Get the WAN IP address of the device from the router. Open a web browser on your computer, enter the WAN IP address plus HTTP port like http://116.30.18.215:100 in the address bar and then press enter to go to the login interface. Enter the username and password of the device in the interface and then click “Login” to go to the live view interface.

## 6.3 Web Remote Control

The device supports web client access with or without plug-in. The plug-in browser offers much improved features and performance.
The supported web browsers include IE11(plug-in required)/Firefox/Google chrome/Edge The buttons and icons on the top right corner of the remote interface are introduced as follows.

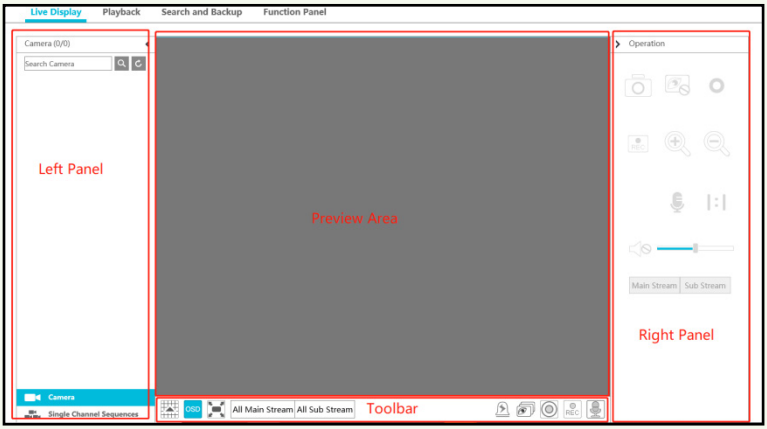
***admin***: the current login username.
***Logout***: click to log out and return to the login interface.
***Modify Password***: click to change the password of the currently active user. Enter the current password and then set a new password in the popup window. Click “OK” to save the new password.
***Local Settings***: click to change the local settings. Set the snapshot number and click “Browse” to set the snapshot path and record path as shown below. Click “Apply” to save the settings.




Below as an introduction is a web browser with the applicable plug-in installed.

## 6.4 Remote Preview

Click “Live Display” in the remote interface to go to the preview interface.
The preview interface consists of the four areas marked in the following picture.




## ➢Start Preview

Select a window in the preview area and then click one online camera on the left panel to preview the camera in the window. You can click in the tool bar to preview all the cameras.

## ➢Left Panel Introduction

Click to show panel. You can view all the added cameras and click group on the left panel.

## ●View Camera

Click Camera/ Camera (3/4) on the left panel stands for the number of online cameras; the right number is for the number of all the added cameras. Enter the camera name in the search box and then click to search for the camera. Click to refresh the camera list.

## ●View Group

Click Single Channel Sequences/ Single Channel Sequences on the left panel displays all the groups and the bottom displays all the cameras in the group. In the channel group interface, you can add, modify or delete the channel group.

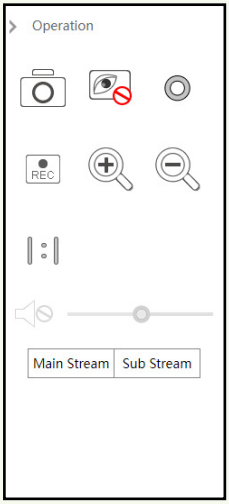
Add a channel group: Click "Add" to display an adding interface. Enter the group name, set the dwell time, select cameras and click "Add". After successfully adding a group, double-click the channel name to play in sequences. Click to stop playing.

## ➢Tool Bar Introduction

| Button | Meaning |
|---|---|
| | Screen mode button. |
| | Click to show full screen. Right click on the full screen to exit full screen. |
| | Click “All Main Stream” or “All Sub Stream” to set the stream of all the cameras. |
| | Manual alarm button. Click to open a window and then trigger and clear the alarm-out in the window manually. |
| | Click to preview all cameras. |
| | Click to close all the preview cameras. |
| | Click to start recording for all cameras to computer. Click to stop recording. |
| | Click to start recording for all cameras to the device. Click to stop recording. |
| | Click to enable talk through the device. |

**➢Right Panel Introduction**

Click on the right panel to show the panel and click to hide the panel.




Click one camera window in the preview area and then click to set the camera’s live preview stream and record stream to main stream in manual record mode; click to set the camera’s live preview stream and record stream to sub stream.

Operation panel introduction:

| Button | Meaning |
|---|---|
| | Click to take snapshots |
| | Click to start recording to computer |
| REC | Click to start recording to the device. |
| | Click to zoom in the image of the camera and then drag the mouse on the camera image to view the hidden area. |
| | Click to zoom out the image of the camera. |
| | Click to start two-way talk. |
| 3D | The 3D zoom in function is designed for P.T.Z. Click the button and then drag the image to zoom in or zoom out the image; click the image on different areas to view the image of the dome omni-directionally. |
| | Click to close the preview camera. |
| | Click to display original size |
| | Click to enable audio and then drag the slider bar to adjust the volume. You can listen to the camera audio by enabling audio. |

## 6.5 Remote Playback

Click “Playback” in the remote interface to go to the playback interface.

① Check the record event types and cameras on the left panel. Set the record date on the calendar beside the time scale.

② Click or directly to search the record date and then click

Place your mouse on the time scale and the following buttons will display. Click 1/2/ / to zoom in/out the time scale.

**Introduction of playback control buttons:**

| Button | Meaning |
|---|---|
| | Screen mode button. |
| | Click to show full screen. Right click on the full screen to exit full screen. |
| | Stop button. |
| | Rewind button. Click to play video backwards. |
| | Play button. Click to play video forwards. |
| | Pause button. |

| Button | Meaning |
|---|---|
| | Deceleration button. Click to decrease the playing speed. |
| | Acceleration button. Click to increase the playing speed. |
| | Previous frame button. It works only when the forward playing is paused in single screen mode. |
| | Next frame button. It works only when the forward playing is paused in single screen mode. |
| | Click to step backward 30s and click to step forward 30s. |
| | Backup start time button. Click the time scale and then click to set the backup start time. |
| | Backup end time button. Click the time scale and then click to set the backup end time. |
| | Backup button. |
| | Backup tasks button. Click to view the backup status. |
| | Event list button. Click to view the event record of manual/schedule/sensor/motion. |

## 6.6 Remote Search and Backup

Click “Search and Backup” in the remote interface to go to the backup interface. You can back up the record by event or by time.

**➢By Event**

Check the record type (manual record) on the left side of the interface and then click to search the record (the searched record data will be displayed in the list); check the record data in the list and

then click “Backup” to backup the record.

**➢By Time**

Click the start time and end time on the left side of the interface; check the cameras and then click on the right side to backup the record.

**View Backup Status**: Click “Backup Status” to view the backup status. Click “Pause” to pause; click “Resume” to continue the backup; click “Delete” to delete the task.

## 6.7 Remote Configuration

Click “Function Panel” in the remote interface and then configure the camera, record, event, SD card, network, intercom, call, account and authority, and system of the device remotely. The settings of camera, event, intercom and call are similar to the relevant settings of the device. See the configurations of the device for details.

### 6.7.1 View Record Status

Click ***Function Panel→Record.*** You can view each channel’s record status, resolution, bitrate,

etc.

### 6.7.2 SD Card Management

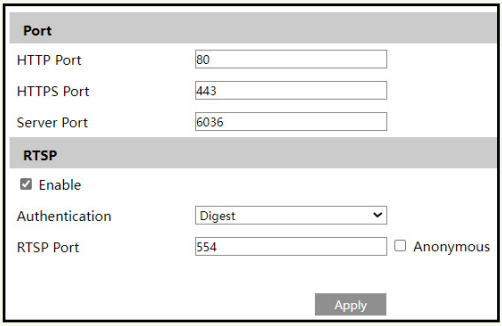
Click ***Function Panel→SD Card.*** You can format the SD card in this interface.

### 6.7.3 Network Settings

Click ***Function Panel→Network→TCP/IP.*** You can set the IP address, submask, gateway, preferred/Alternate DNS, default route and primary card as needed.

- Port Settings

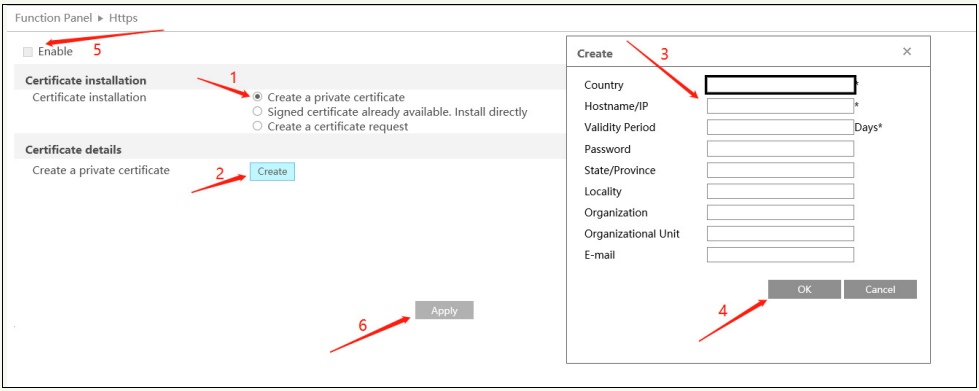
Click ***Function Panel→Network→Port*** to go to the interface as shown below.




Enter the HTTP port, HTTPS port, server port of the device, and then click “Apply” to save the settings. You can also enable and set RTSP port (please check “Anonymous” as required).
***HTTP Port***: the default HTTP port of the device is 80. The port number can be changed to another number such as 81. The port is mainly used for web client access. If you want to access the device through a web browser, you should enter the IP address plus HTTP port in the address bar of the web browser like http://192.168.11.61:81.
Note: The HTTP port and server port of the device should be mapped to the router before you access the device via WAN.

***HTTPS Port***: the default HTTPs port of the device is 443.
HTTPS provides authentication of the web site and protects user privacy. You can enter IP address plus HTTPS port in the address bar of the web browser. Then enter username and password to log in. Click Functional Panel→Network→HTTPS to go to the following interface. There are three ways to enable HTTPS service.

**A. Create a private certificate.**




① Select “Create a private certificate”.

② Click “Create”.

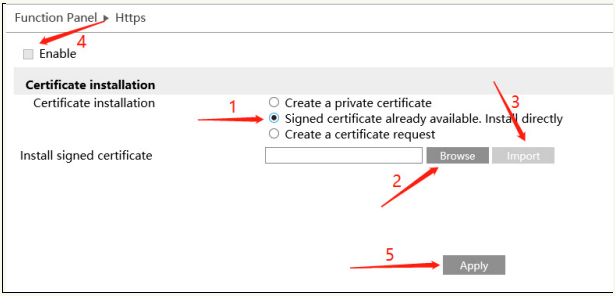
③ Fill out the corresponding information in the above creation box. Enter the country (only two letters available), domain (the device’s IP address/domain), validity date, password, province/state, region and so on.

④ Click “OK”.

⑤ Check “Enable” checkbox.

⑥ Click “Apply” to save the setting.

**B. Install a signed certificate**




① Check “Signed certificate already....”.

② Click “Browse” to select the certificate you want to import.

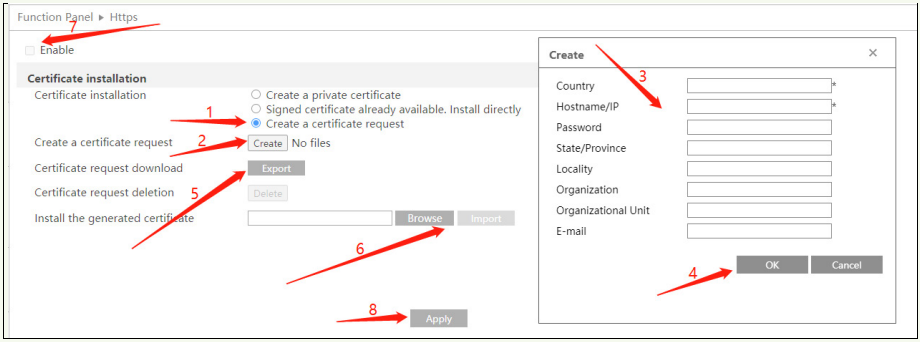
③ Click “Import”.

④ Check “Enable”.

⑤ Click “Apply” to save the settings.

Please note that the certificate uploaded here shall be a certificate with private key. To attach the private key to the certificate, please open the certificate and the private key files with an editor (like Notepad++) and then copy the private key to the certificate.

### C. Create a certificate request




① Check “Create a certificate request”.

② Click “Create”.

③ Fill out the corresponding information in the above creation box. Enter the country (only two letters available), domain (the device’s IP address/domain), validity date, password, province/state, region and so on.

④ Click “OK”. Then a certificate request file (CSR) will be created.

⑤ Click “Export” to export the certificate request file. Then send this file to the trusted third-party CA to apply a signed certificate.

⑥ Click “Browse” and select the signed certificate issued by the CA and then import this certificate.

⑦ Click “Enable”.

⑧ Click “Apply” to save the settings.

After that, the device can be accessed by entering https://IP: https port via the web browser (eg. https://192.168.1.201:443).

***Server Port***: the default server port of the device is 6036. The server port number can be changed as needed. The port is mainly used in network video management system. ***RTSP Port***: RTSP real-time stream protocol can be used to control the transfer of real-time data. . Through a media player which supports the RTSP real-time stream protocol (Such as VLC player), you can view live images synchronously. The default RTSP port is 554 and it can be changed as needed. (The address format: rtsp://IP address:554/chID=1&streamType=main or rtsp://IP address:554/chID=1&streamType=sub; main indicators main stream; sub indicators sub stream; chID indicators channel ID). ***Examples***: Enable RTSP and “Anonymous”. Then open the VLC player and enter the address (for example: rtsp://192.168.1.88:554/chID=1&streamType=main) in the network address bar of the VLC player. Then you can view the video of channel 1. Authentication: Choose “Digest” or “Basic” as needed.

WiFi Setttings: The WiFi setup via web is similar to the WiFi setup of the device.

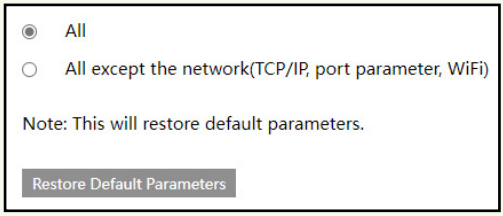
●ONVIF Settings
After ONVIF is enabled, it can be searched and connected to a third-party platform via ONVIF protocol.
Click ***Function Panel→Network→ONVIF*** to enter the following interface.
**Note**: when adding the device to a third-party platform with ONVIF protocol, please check "Enable ONVIF" first and then enter the username and password created in the above interface.

### 6.7.4 Basic Settings

Click ***Function Panel→System→General Settings*** to set the device name and video format as needed.
Click ***Function Panel→System→Date and Time*** to set the system time, date format, time format, time zone, DST, etc.

### 6.7.5 Factory Default Settings

Click ***Function Panel→System→Factory Default*** to go to the following interface. Please choose the item as needed.




### 6.7.6 Upgrade

Before upgrade, please get the upgrade file from your dealer.
The upgrade steps are as follows:
Click ***Function Panel→System→Upgrade*** to go to "Upgrade" interface. Click "Browse" and go to the path where the upgrade software exists. Select the upgrade software and then click "Upgrade". The system may automatically restart during upgrading. Please wait for a while and do not power off the device during upgrading.

### 6.7.7 Backup and Restore

You can back up the configuration file of the device by exporting the file to other storage devices; you can recover the configuration to other devices which are of the same model with the device by importing the configuration file to other devices for time saving. Click ***Function Panel→System→Config Backup and Restore***.

**●Backup**

Click “Browse” and then go to the path where you want to store the configuration backup file and then click “Export”; finally click “OK” in the popup window.

●**Recover**

Click “Browse” and then find the configuration backup file and then click “Import”; finally click “OK” in the popup window.

### 6.7.8 Reboot

Click ***Function Panel→System→Reboot***. In this interface, click “Reboot” and enter the username and password to restart the device.

### 6.7.9 Auto Maintenance

You can set the automatic restart time for the device to maintain it regularly. Click ***Function Panel→System →Auto Maintenance*** to go to the interface. Check “Enable”, set the interval days and schedule time and then click “Apply” to save the settings. The device will restart automatically at the schedule time every interval days.

### 6.7.10 View Log

Click ***Function Panel→System→View Log*** to go to the log view interface. Select the log main type, click . The searched log will be displayed in the list. Set the display and the time and then click “Search”

### 6.7.11 View System Information

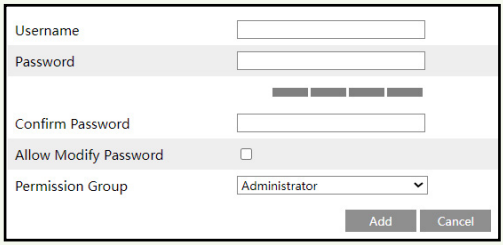
Click ***Function Panel→System→Information*** and then click the corresponding menu to view the “Basic”, “Camera Status”, “Network Status” and “SD Card Status” information of the system.

### 6.7.12 Account and Security

Click ***Function Panel→Account and Authority*** to enter the web account management interface. There are three default permission groups (“Administrator”, “Advanced” and “Common”) available when adding accounts. You can manually add new permission group (see Add Permission Group for details).
Only ***admin*** and the users that have the “Account and Authority” permission can manage the system’s accounts.

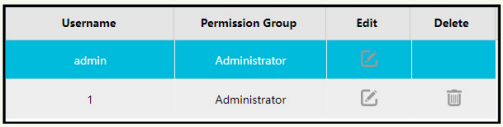
●Add User

Click ***Function Panel→Account and Authority→Add User*** to enter the search box in the account and authority popup. The window is shown below.

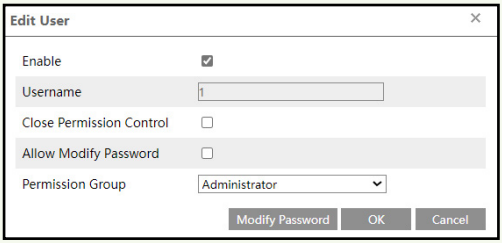



Set the username, password and group. In addition, there is an option to allow modify password. Click “Add” to add the user.

●Edit User

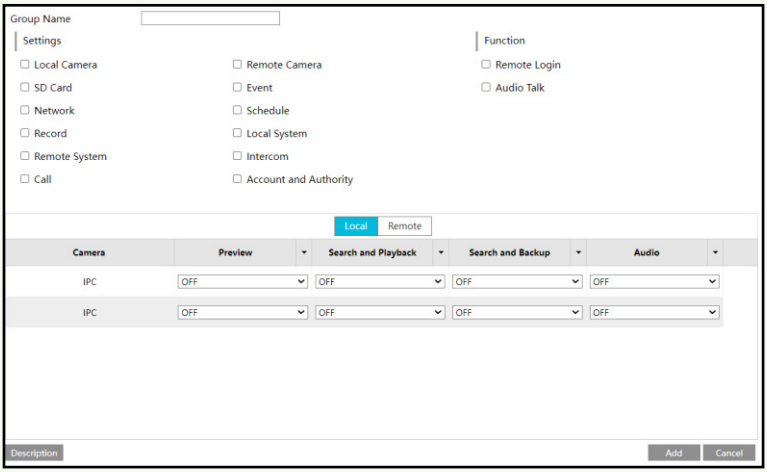



Click to edit user (the user list to edit the user information. Click cannot be deleted). For the default admin user, you can modify its password by clicking on the top right corner of the interface. For other users, you can click to modify their password. For the default admin user, its permission control is closed and permission group cannot be changed by default. You can enable or disable other users (if disabled, the user will be invalid), open or close their permission control (if closed, the user will get all the permissions which has) and set their permission groups. Click “OK” to save the settings.




●Permission Group Management

Click *Permission Group* → *Set the group authority* → *Edit Permission Group*. Click to add permission group. Set the group authority, check the permissions as required and then set the “Local” and “Remote” permissions. Click “Add” to save the settings.




Go to "Edit Permission" interface and then click of the Group "Edit Permission Group" are similar to that of the Add Permission Group. Click to delete the permission groups (group. Click "Administrator", "Advanced" and "Common") cannot be deleted.

- Block and Allow Lists

Click ***Function Panel→Account and Authority→Block and Allow List*** to go to the following interface.

Check "Enable" and then choose "Enable Allow List (white list)" or "Enable Block List (black list)" (the PC client of which the IP address is in the white list can access the device remotely while the PC client in the black list cannot).

Add IP/IP segment/MAC. Click "Add IP" or "Add IP segment/MAC" and then check "Enable" in the popup window (only if you check it can be added to the IP/IP segment/MAC you add "Enable" to edit IP/IP segment/MAC, click "OK". In the above interface, click to delete it. Click "Apply" to save the settings.

- Password Security

Click ***Function Panel→Account and Authority→Security→Password Security*** to go to the following interface. In this interface, you can set the level of the password.

- View Online User

Click ***Function Panel→Account and Authority→User Status*** to view the online user information (you can view the user name, login type, IP address and login time; click to pop up a window showing the preview occupied channel number and playback occupied channel number).

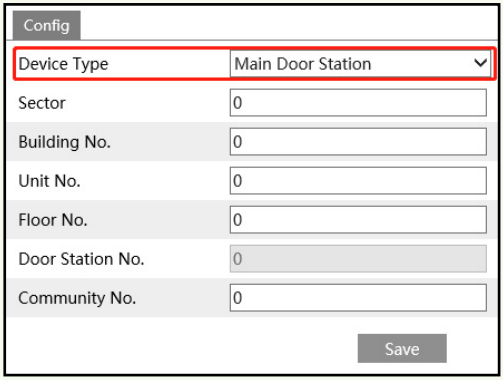
## Appendix 1 How to Call Indoor Station

### Appendix 1-1 One Door Station Calls One Indoor Station

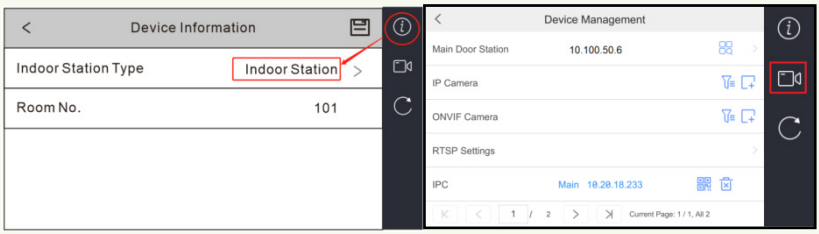
**Application:** One door station and bind one indoor station. Press the preset room number and call button or press to call indoor station

The setting steps are as follows:

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




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



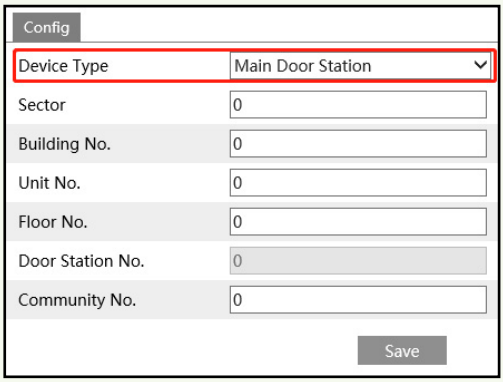

4. Call indoor station through your door station (See Call Resident for details).

**Appendix 1-2 One Door Station Calls Multiple Indoor Stations**

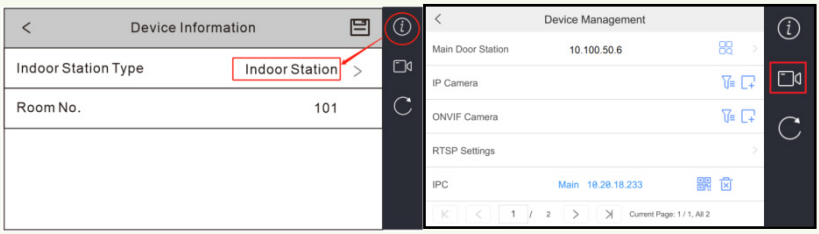
**Application:** A door station and bind multiple indoor stations with the same room number set. Press the room number and call button on villa to call indoor stations. All indoor stations will respond at the same time. The resident can answer any one of them and open the door.

The setting steps are as follows:

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



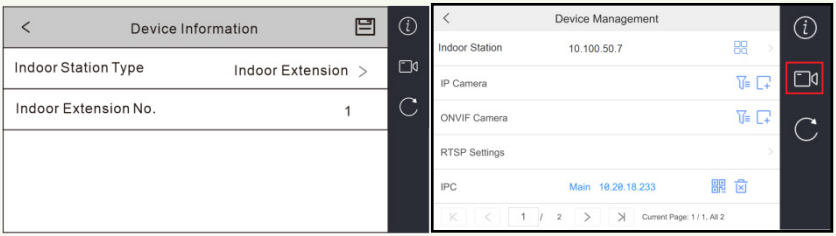

3. Tap ***Settings→More Settings→Configuration*** in the indoor station. Then enter the password of Admin to enter the following interface. Set the indoor station type (it should be set to "Indoor station"), room number (like 101), IP address of the main door station.




4. Set indoor extensions.

Tap ***Settings→More Settings→Configuration*** in the indoor station. Then enter the password of Admin to enter the following interface. Set the indoor station type (it should be set to "Indoor Extension"), indoor extension No. (ranging from 1 to 5), IP address of the indoor station.

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




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

**Application B:** Install one door station and bind multiple indoor stations with the different room number set. Press different room numbers to call different indoor stations. The setting steps are as follows:

1. Connect your door station and indoor station to the same local network and then set their network parameters to the same network segment.
2. Log in the web client of the door station. Click ***Config→Intercom→Number Configuration*** to go to the following interface. Set the device type to "Main Door Station".
3. Tap ***Settings→More Settings→Configuration*** in the indoor station. Then enter the password of Admin to enter the following interface. Set the indoor station type (it should be set to "Indoor station"), room number (like 101), IP address of the main door station.
4. For other indoor stations, set the indoor station type to "Indoor Station", enter different room numbers and set the same IP address of the main door station.
5. Press different room numbers to call different indoor stations.

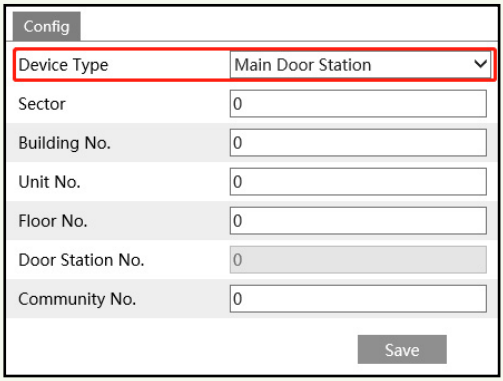
**Appendix 1-3 Multiple Door Stations Call One Indoor Station**

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

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

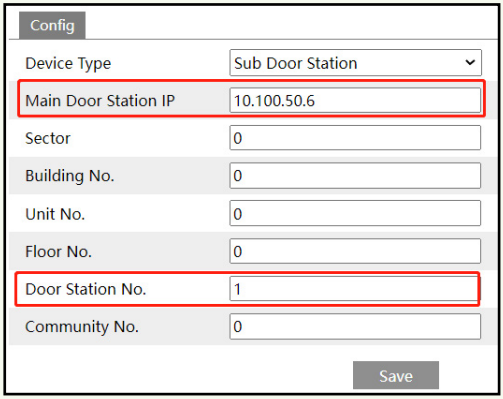
The setting steps are as follows:

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

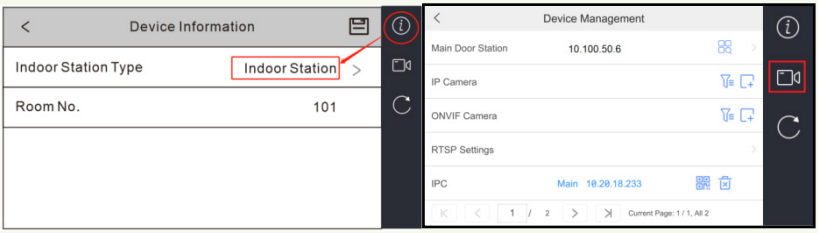



3. Sub door station settings

Log in the web client of the door station. Click ***Config→Intercom→Number Configuration*** to go to the following interface. Set the device type to "Sub Door Station". Enter the actual IP address of the main door station and door station no. Door Station No.: enter the sub door station number (ranging from 1 to 99; 0 is main station number by default). Different sub door stations should have different door station number.




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

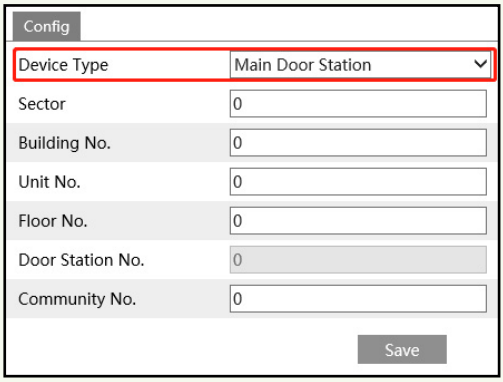


5. Call indoor station through your main or sub door station (See Call Resident for details).

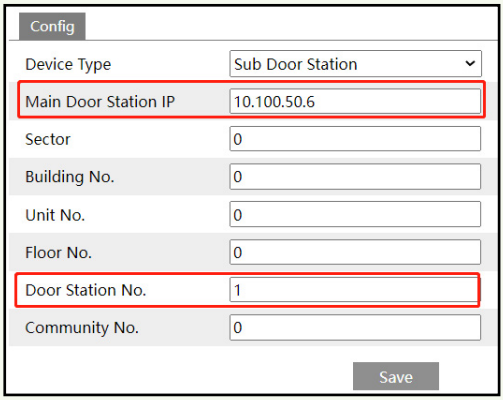
**Appendix 1-4 Multiple Door Stations Call Multiple Indoor Stations**

**Application A**: Install multiple door stations (one is main door station, others are sub door stations) and multiple indoor stations (all indoor stations are set as “Indoor Station”). Main door station and sub door stations can call different indoor stations installed in different rooms respectively.
**Note**: Up to 9 sub door stations can be set for a main door station.

The setting steps are as follows:
**C**onnect 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”.

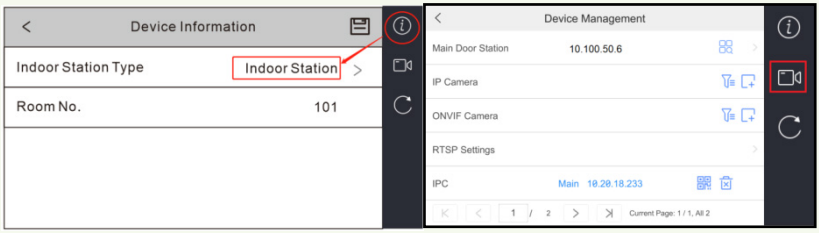



**S**ub door station settings Log in the web client of the door station. Click ***Config→Intercom→ Number Configuration*** to go to the following interface. Set the device type to “Sub Door Station”. Enter the actual IP address of the main door station and door station no. Door Station No.: enter the sub door station number (ranging from 1 to 99; 0 is main station number by default). Different sub door stations should have different door station number.




4. Indoor station settings

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




5. 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.

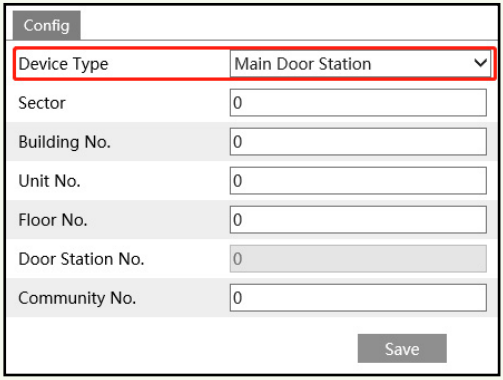
Press different room numbers on different door stations (main or sub door stations) to call the corresponding indoor stations.

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

The setting steps are as follows:

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

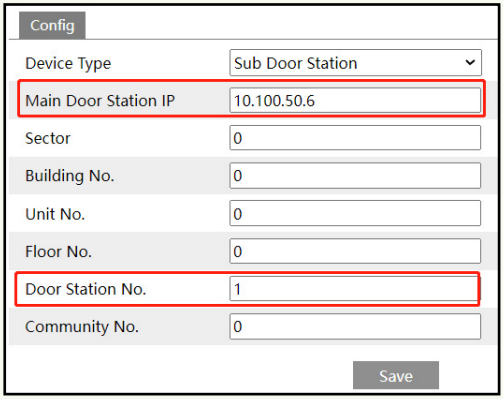
Main door station settings Log in the web client of the door station. Click ***Config→Intercom→Number Configuration*** to go to the following interface. Set the device type to "Main Door Station".



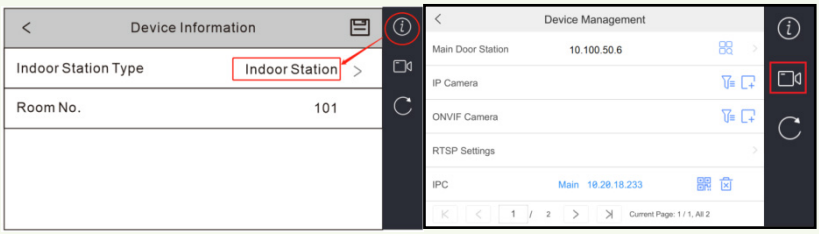

3. Sub door station settings

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

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



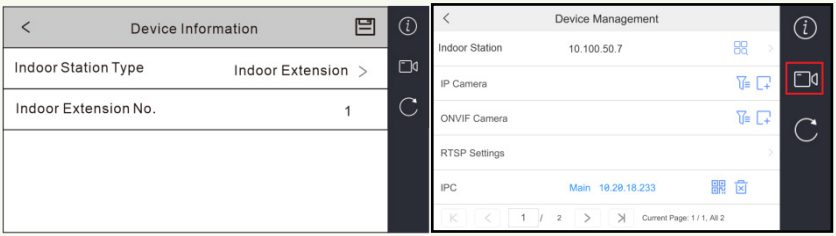

4. Indoor station settings Tap ***Settings→More Settings→Configuration*** in the indoor station. Then enter the password of Admin to enter the following interface. Set the indoor station type (it should be set to “Indoor station”), room number, IP address of the main door station.




5. Indoor extension settings

Tap ***Settings→More Settings→Configuration*** in the indoor station. Then enter the password of Admin to enter the following interface. Set the indoor station type (it should be set to "Indoor Extension"), indoor extension No. (ranging from 1 to 5), IP address of the indoor station.

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




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

## Appendix 2—Troubleshooting

1. If I forget the password, what should I do?
Hold and press the Reset button to restore to the factory default settings. Then reset the password.

2. 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.

3. No sound can be heard in the live view interface.
A: Audio input device of the IPC or access control device is not connected. Please connect and try again.
B: Audio function is not enabled at the corresponding channel. Please enable this function.

4. Door station failed to call indoor station.
- Please check whether the network segment of the indoor station is the same as that of the door station.
- 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.

- Confirm the indoor station configuration

1) if it is a indoor station

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

2) if it is an indoor extension

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

5. 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.