

# Indoor Station & Villa Door Station

## User Manual

V2.16

# Contents

<b>About this Manual.....</b>	<b>1</b>
<b>1 Defaults.....</b>	<b>2</b>
<b>2 Home Screen.....</b>	<b>2</b>
<b>3 Lock Screen Manually.....</b>	<b>2</b>
<b>4 Do Not Disturb.....</b>	<b>3</b>
<b>5 Live View.....</b>	<b>3</b>
<b>6 Make Calls.....</b>	<b>6</b>
<b>7 Answer Calls.....</b>	<b>8</b>
<b>8 Message.....</b>	<b>10</b>
8.1 Snapshot.....	10
8.2 Video Recording.....	10
8.3 Visitor Message.....	11
<b>9 Settings.....</b>	<b>12</b>
9.1 Sounds.....	12
9.1.1 Call Settings.....	12
9.1.2 Volume Settings.....	14
9.2 General Settings.....	15
9.2.1 Display Settings.....	15
9.2.2 Time Settings.....	16
9.2.3 Password Settings.....	17
9.2.4 I/O Settings.....	18
9.2.5 Visitor Message Settings.....	19
9.3 Wi-Fi.....	20
9.4 Administration Configuration.....	22
9.4.1 Indoor Station.....	23
9.4.2 Devices.....	27
9.4.3 Main Indoor Station.....	34
9.4.4 Administrator Password.....	35
9.4.5 Device Maintenance.....	36
9.5 Device Info.....	37
<b>10 Web Operations.....</b>	<b>38</b>
10.1 Login.....	38
10.2 Live View.....	41
10.3 Person Library.....	43
10.4 Setup.....	46
10.4.1 Common.....	46
10.4.2 Network.....	57
10.4.3 Image.....	63

10.4.4 Intelligent.....	69
10.4.5 Events.....	73
10.4.6 Storage.....	75
10.4.7 Security.....	76
10.4.8 System.....	82

# About this Manual

---

This manual describes functions and operations of indoor station and villa door station.

## Copyright Statement

©2023-2024 Zhejiang Uniview Technologies Co., Ltd. All rights reserved.

No part of this manual may be copied, reproduced, translated or distributed in any form or by any means without prior consent in writing from Zhejiang Uniview Technologies Co., Ltd (hereinafter referred to as Uniview or us).

The product described in this manual may contain proprietary software owned by Uniview and its possible licensors. Unless permitted by Uniview and its licensors, no one is allowed to copy, distribute, modify, abstract, decompile, disassemble, decrypt, reverse engineer, rent, transfer, or sublicense the software in any form by any means.

## Disclaimer




Due to such reasons as product version upgrade or regulatory requirement of relevant regions, this manual will be periodically updated.

This manual is only for informational purpose, and all statements, information, and recommendations in this manual are presented without warranty.

The illustrations in this manual are for reference only and may vary depending on the version or model. The screenshots in this manual may have been customized to meet specific requirements and user preferences. As a result, some of the examples and functions featured may differ from those displayed on your monitor.

## Safety Symbols


The symbols in the following table may be found in this manual. Carefully follow the instructions indicated by the symbols to avoid hazardous situations and use the product properly.

Symbol	Description
 <b>NOTE!</b>	Indicates useful or supplemental information about the use of product.
 <b>CAUTION!</b>	Indicates a situation which, if not avoided, could result in damage, data loss or malfunction to product.
 <b>WARNING!</b>	Indicates a hazardous situation which, if not avoided, could result in bodily injury or death.

# 1 Defaults

The default parameters of the indoor station and villa door station (hereinafter referred to as "door station") are consistent.

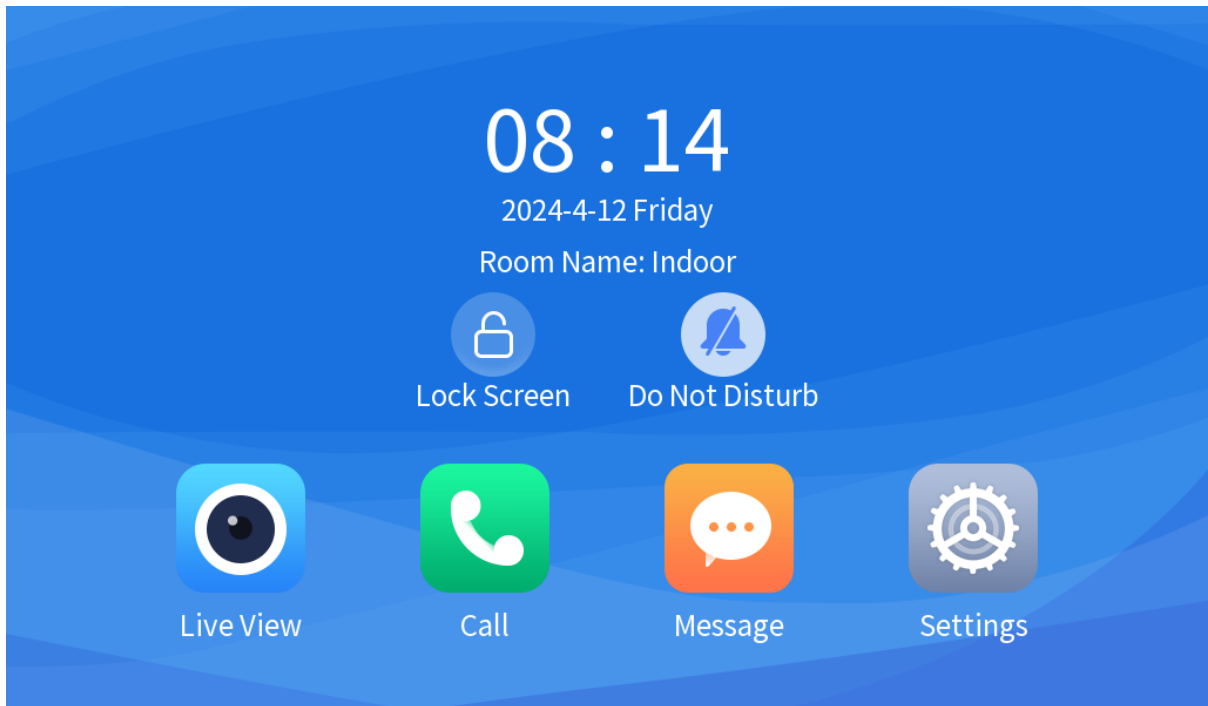
Username: admin	Password: 123456
Static IP address: 192.168.1.13	Subnet mask: 255.255.255.0

 **Note:** DHCP (Dynamic Host Configuration Protocol) is enabled by default on the device. If a DHCP server is deployed in the network, the device may be assigned an IP address, and you need to use the assigned IP address to log in.

# 2 Home Screen

When the indoor station starts up for the first time or after restoring all default settings, you need to follow the wizard to complete the basic settings including password, email, and network, and then the main screen (hereinafter referred to as "home screen") appears.


Figure 2-1: Home Screen




The home screen displays the current time (set on the [Web](#)), and supports [Lock Screen Manually](#), [Do Not Disturb](#), [Live View](#), [Make Calls](#), [Answer Calls](#), [Message](#), and [Settings](#).

# 3 Lock Screen Manually

You can lock the screen to save energy when not using it.

 **Note:** This function is available to the indoor station's screen.

Tap  to lock the screen; Tap any position to unlock the screen.

By default, the screen needs to be locked manually. To lock the screen automatically, enable [Auto-Lock Screen](#).


## 4 Do Not Disturb



---

When **Do Not Disturb** is on, the indoor station does not sound when a call comes in, but the call remains on the screen until it is answered or ended by the caller (the calls will be displayed by tapping the screen when the screen is locked.)

When [Visitor Message Settings](#) is enabled, the messages can be received normally. You can view the messages in [Visitor Message](#).

By default, this function is disabled.

 **Note:** This function is available to the indoor station's screen.

Tap  to enable **Do Not Disturb**. To disable this function, tap .

To automatically reject calls, enable **Auto Answer** on the [Call Settings](#) screen.

## 5 Live View

---

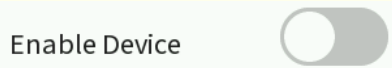
When the indoor station is connected to the intelligent recognition terminal, door station, and network camera, you can view live video on its screen.

After the extension is connected to the main indoor station, the extension screen can play the live video of intelligent recognition terminal, door station, and network camera connected to the main indoor station.


 **Note:**

- This function is available to the indoor station's screen.
- To connect the intelligent recognition terminal, door station, and network camera to the indoor station, please see [Related Devices](#), and ensure that **Enable Device** is on (port number is required for network camera connection).

**Figure 5-1: Enable Device**



- By default, the system will automatically return to the [Home Screen](#) if there is no operation and incoming calls within 60 seconds. You can change the time to automatically return to the home screen in [Indoor Station](#).

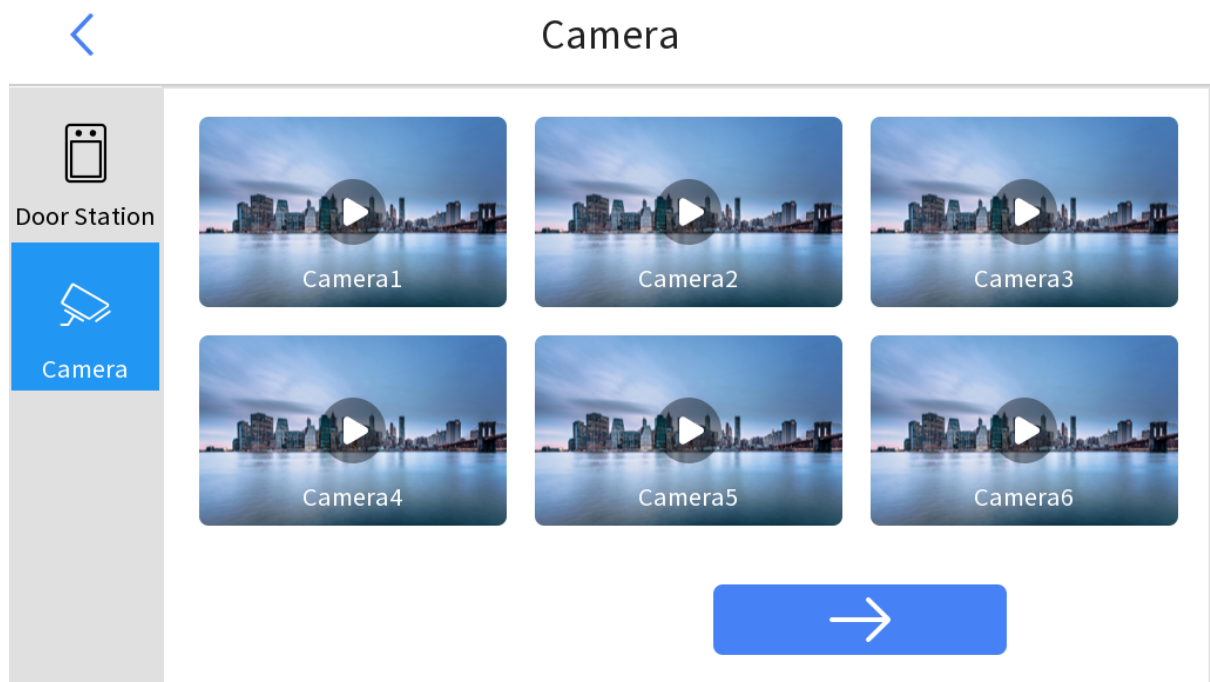
Tap . The live view screen appears.

- The live view list includes **Door Station** (intelligent recognition terminal/door station) and **Camera**. If the first device connected to the indoor station is an intelligent recognition terminal or door station, the **Door Station** tab will be displayed on the live view screen by default; If the first device connected to the indoor station is a camera, the **Camera** tab will be displayed by default.
- Up to 6 live videos can be displayed on one screen. You can switch to the next screen by tapping the arrow below.

Figure 5-2: Live View-Door Station



Figure 5-3: Live View-Camera



Tap any device to play its live video. The device name and remaining play time will be displayed at the top of the screen.


 **Note:** The default play time is the same as **Ringtone Duration(s)** in **Call Settings**. The screen will be automatically blacked out after the duration. To view the live video again, you need to tap the corresponding device.

Figure 5-4: Camera Live View



Figure 5-5: Intelligent Recognition Terminal Live View

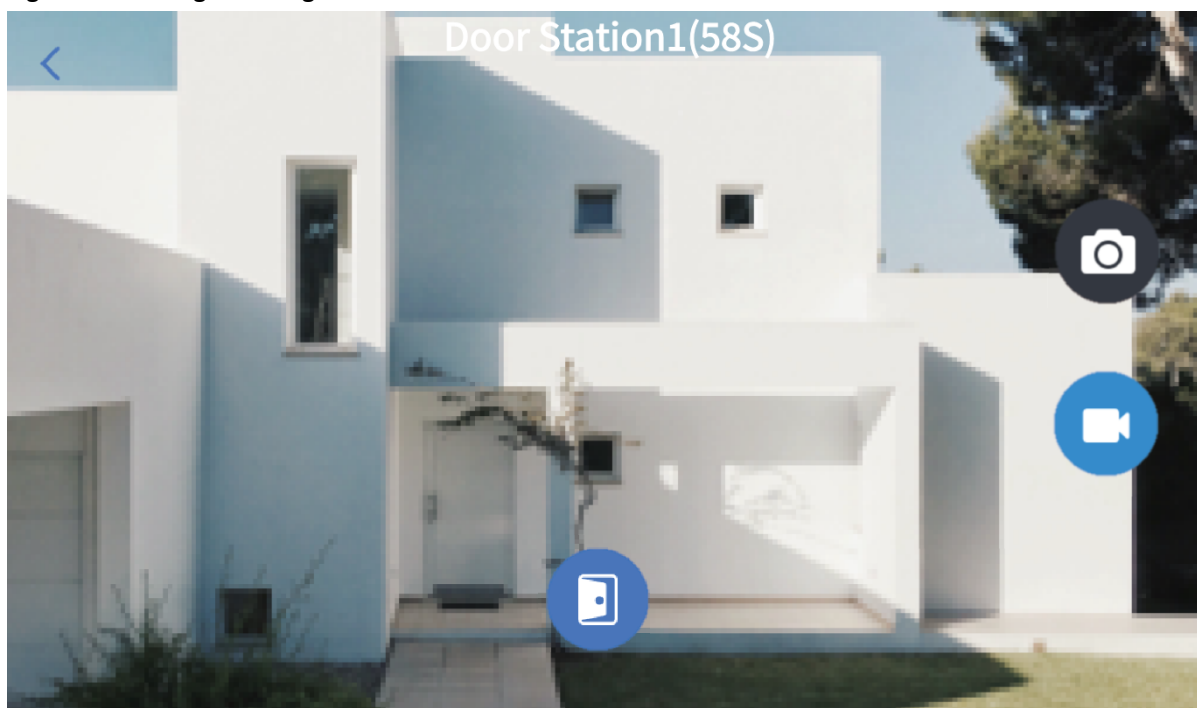
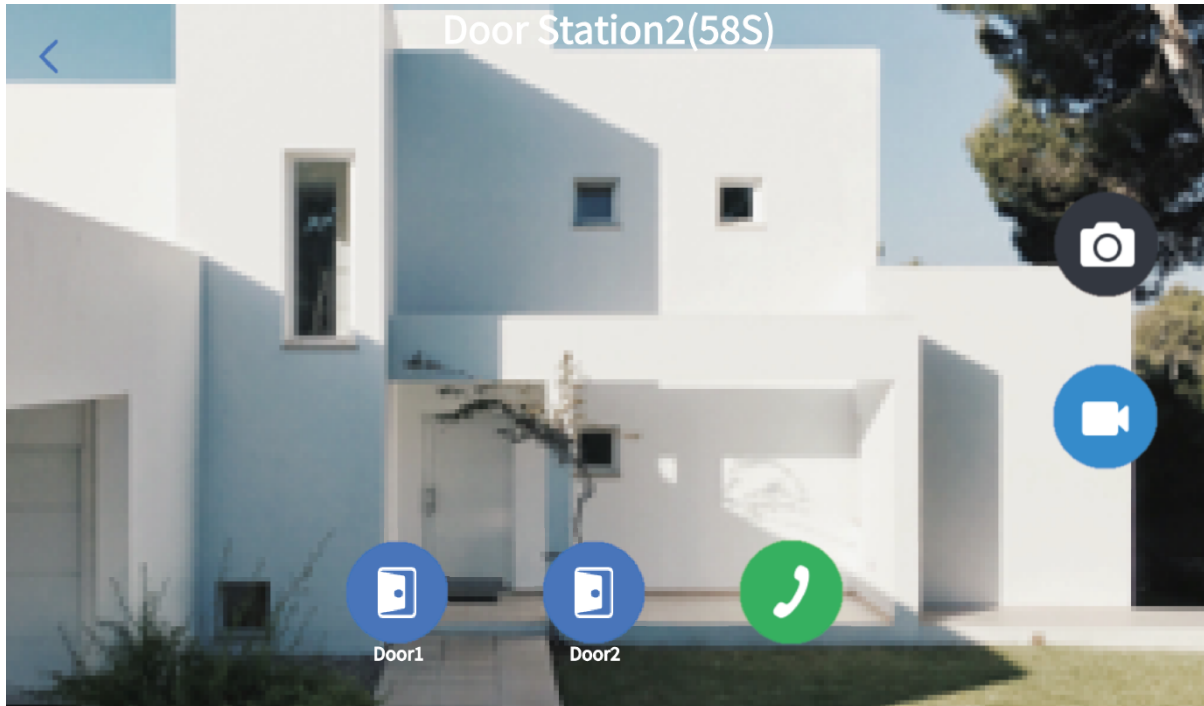










Figure 5-6: Door Station Live View



- : Tap to take a snapshot for the current image. You can view the snapshot records in [Message](#).
- : Tap to record live video. Tap  to stop recording. If the recording time reaches the upper limit or you exit the current screen, the recording will be ended. To play the recording, see [Video Recording](#).  
**Note:** To use the recording function, please install a formatted Micro SD card, and then the recording icon is blue, otherwise the icon is grayed out.
- : Tap to send a door opening signal to the intelligent recognition terminal or door station, so as to open the door remotely.
- : Tap to call the door station. Only available to the single-button door station.
- : Tap to return to the home screen.

## 6 Make Calls

You can call other extension users by entering the corresponding number on the indoor station's screen. You can also view the calling records.


 **Note:**

- This function is available to the indoor station's screen.
- Make sure the main indoor station has been related to the indoor extension (see [Device Discovery](#) for details).
- Extension user: Indoor stations at the same location (same room, unit, building, and district) are extensions. For details about location information, see [Device Location](#).

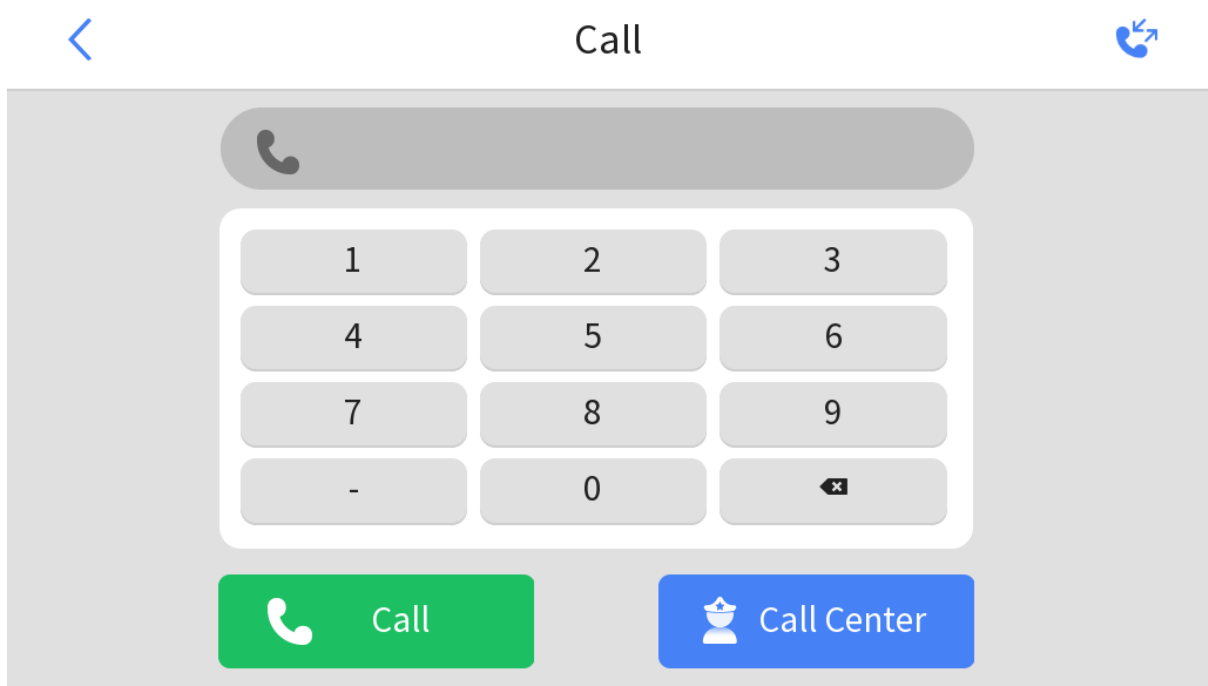
**Figure 6-1: Extension No.**

 Extension No.





- By default, the system will automatically return to the [Home Screen](#) if there is no operation and incoming calls within 60 seconds. You can change the time to automatically return to the home screen in [Indoor Station](#).



Tap . The **Call** screen appears.

**Figure 6-2: Call**

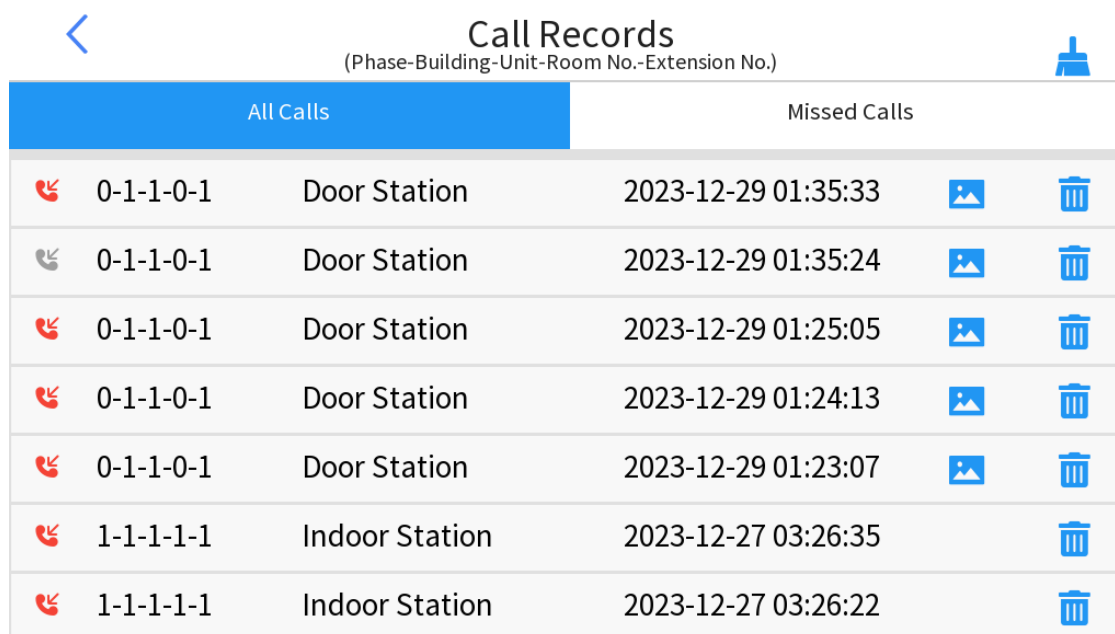





















- Main station calls extension:
  1. Input the extension number to be called.






For example, if the indoor station initiating the call is located at District 1, Building 1, Unit 1, Room 101, Extension Number 1, and the device to be called is located at District 1, Building 1, Unit 1, Room 101, and Extension Number 2, and then you need to input 2.
  2. Tap  to call the extension user.
- Extension calls main station: Input 0, and tap .
- Call center: If the indoor station is related to the central server (see [Configure Central Server](#) for details), you can tap  to call the central server.
- View call records: Up to latest 200 records can be displayed if the device has no memory card, including the **All Calls** and **Missed Calls** lists. Tap  in the upper-right corner to view the details.

If there are missed calls, a prompt will appear in the right corner of the Call and Call Records icons, for example  . The red number means the number of the missed calls, and it will disappear if you view the missed call records.

**Figure 6-3: Call Records**



All Calls		Missed Calls			
	0-1-1-0-1	Door Station	2023-12-29 01:35:33		
	0-1-1-0-1	Door Station	2023-12-29 01:35:24		
	0-1-1-0-1	Door Station	2023-12-29 01:25:05		
	0-1-1-0-1	Door Station	2023-12-29 01:24:13		
	0-1-1-0-1	Door Station	2023-12-29 01:23:07		
	1-1-1-1-1	Indoor Station	2023-12-27 03:26:35		
	1-1-1-1-1	Indoor Station	2023-12-27 03:26:22		

- : The call was accepted/declined.
- : The call was answered/hung up.
- Delete a record: Select a record you want to delete, tap , and then tap **Confirm** in the pop-up window.
- Delete all records: Tap  in the upper-right corner, and then tap **Confirm** in the pop-up window.
- View call snapshots: If you manually answer/hang up the call from the intelligent recognition terminal/door station, the indoor station will automatically capture the screen at the moment when the call is answered/hung up. Select a record, and tap  to view its call snapshot. Tap anywhere on the screen to close the snapshot.

## 7 Answer Calls

When the indoor station receives incoming calls from the connected intelligent recognition terminal, door station, or other extensions, you can operate as follows.


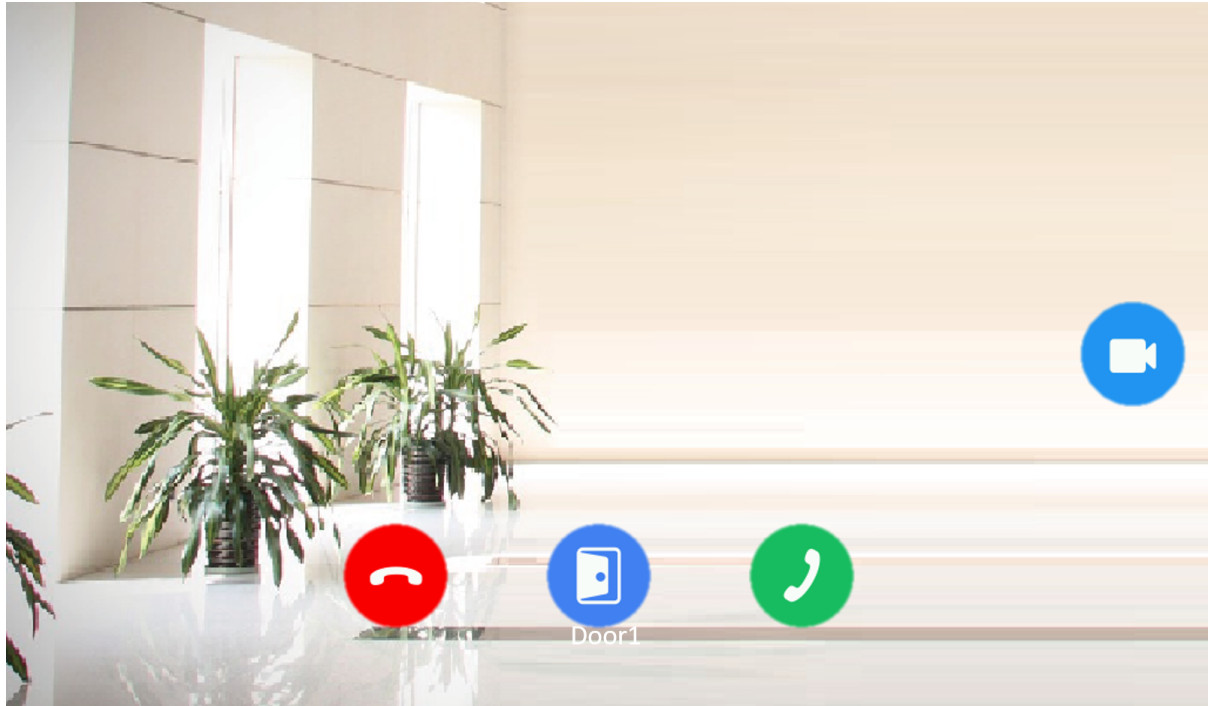







 **Note:** The indoor station can be used with the UNV-Link app after being connected to a Wi-Fi network (please relate the device to the app in [Device Maintenance](#) first). Then, you can view the live video, answer/reject calls, and remotely open the door on the app.

Figure 7-1: Answer




- View live video: When the indoor station receives a call from the connected intelligent recognition terminal or door station, the indoor station screen will play the live video of the call terminal. The live video will be ended if you reject the incoming call or hang up the call.

- : Tap to answer the call.
- : Tap to reject the incoming call or hang up the call.
- : Remotely open the door.
- : Tap to start recording. Tap  to stop recording. If the call is ended by caller or answer, or tap  to answer the call, the recording will be ended. To play the recording, see [Video Recording](#).


 **Note:** To use the recording function, please install a formatted Micro SD card.

- The response to an incoming call may vary, depending on the status of auto answer and visitor message.

Auto Answer	Visitor Message	Response
On	Off	The incoming call is hung up and the device that initiates calls plays the auto-answer voice.
On	On	The <b>Visitor Message</b> screen is displayed.
Off	On	<ul style="list-style-type: none"> <li>• Answer: The talk starts.</li> <li>• Reject: The incoming call is hung up.</li> <li>• No answer after timeout: The <b>Visitor Message</b> screen is displayed.</li> </ul>
Off	Off	<ul style="list-style-type: none"> <li>• Answer: The talk starts.</li> <li>• Reject/No answer after timeout: The incoming call is hung up.</li> </ul>

 **Note:** If the main indoor station has been related to an extension or the app, when the caller starts to leave a message, the extension or the app will automatically return to the home screen, while the main indoor station shows the incoming call and displays the prompt "**Leaving a message....**".


## 8 Message

 **Note:** By default, the system will automatically return to the [Home Screen](#) if there is no operation and incoming calls within 60 seconds. You can change the time to automatically return to the home screen in [Indoor Station](#).

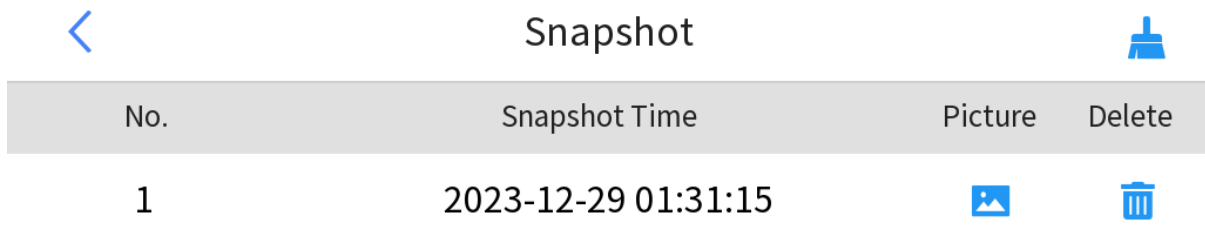
### 8.1 Snapshot

Store all snapshots from [Live View](#).

Up to 100 snapshots can be stored. When the storage space is full, the new image will automatically overwrite the oldest image.




Tap , tap **Snapshot**, and then the snapshot records are displayed in decreasing order of snapshot time.

**Figure 8-1: Snapshot**



The screenshot shows a mobile application interface for managing snapshots. At the top, there is a back arrow on the left, the title "Snapshot" in the center, and a blue trash can icon on the right. Below the title is a table with four columns: "No.", "Snapshot Time", "Picture", and "Delete". The table contains one row of data with the following values: "1", "2023-12-29 01:31:15", a picture icon, and a trash can icon.

No.	Snapshot Time	Picture	Delete
1	2023-12-29 01:31:15		

- View a snapshot: Select a snapshot, and tap  to view its call snapshot. Tap anywhere on the screen to close the snapshot.
- Delete a snapshot: Select a snapshot you want to delete, tap , and then tap **Confirm** in the pop-up window.
- Delete all snapshots: Tap  in the upper-right corner, and then tap **Confirm** in the pop-up window.

### 8.2 Video Recording

Store videos from [Live View](#) and [Answer Calls](#).

Up to 100 recordings can be stored for the device with a Micro SD card. When the storage space is full, the new video will automatically overwrite the oldest video.


Tap , tap **Video Recording**, and then the video recordings are displayed in decreasing order of recording time.

Figure 8-2: Video Recording

No.	Time	Play	Delete
1	2023-12-29 10:39:24		

- Play a recording: Select a recording, and tap to play the video.
- Delete a recording: Select a recording you want to delete, tap , and then tap **Confirm** in the pop-up window.
- Delete all recordings: Tap in the upper-right corner, and then tap **Confirm** in the pop-up window.

### 8.3 Visitor Message

If the indoor station does not answer the call until the calling duration is ended, a message recorded on the door station will be stored to it. If the number of messages reaches the upper limit, or the call is hung up by the indoor station or door station, the message will be ended. If the indoor station answers the call, this message will not be stored.

**Note:**







- Enable **Visitor Message** in [Visitor Message Settings](#) and configure the message duration as needed.
- Set the calling duration in [Call Settings](#).
- This function is only available to the main indoor station.




Visitor message storage limit: Up to 10 messages for the device without a Micro SD card; up to 100 messages for the device with a Micro SD card. When the storage space is full, the new message will automatically overwrite the oldest message.

If there are missed visitor messages, a prompt will appear in the upper-right corner of the Message icon, for example . The red number means the number of the missed visitor messages, and it will decrease accordingly after you play the missed messages.

Tap , tap **Visitor Message**, and then the visitor messages will be displayed in decreasing order of message time.


Figure 8-3: Visitor Message

No.	Time	Play	Delete
1	2023-12-29 01:36:20		
2	2023-12-29 01:35:46		
3	2023-12-29 01:25:18		

- Red time: This message is to be played; Black time: This message has been played.
- Play a message: Select a message, and tap  to play the message.
- Delete a message: Select a message you want to delete, tap , and then tap **Confirm** in the pop-up window.
- Delete all messages: Tap  in the upper-right corner, and then tap **Confirm** in the pop-up window.

## 9 Settings

The indoor station's screen supports [Sounds](#), [General Settings](#), [Wi-Fi](#), and [Administration Configuration](#).

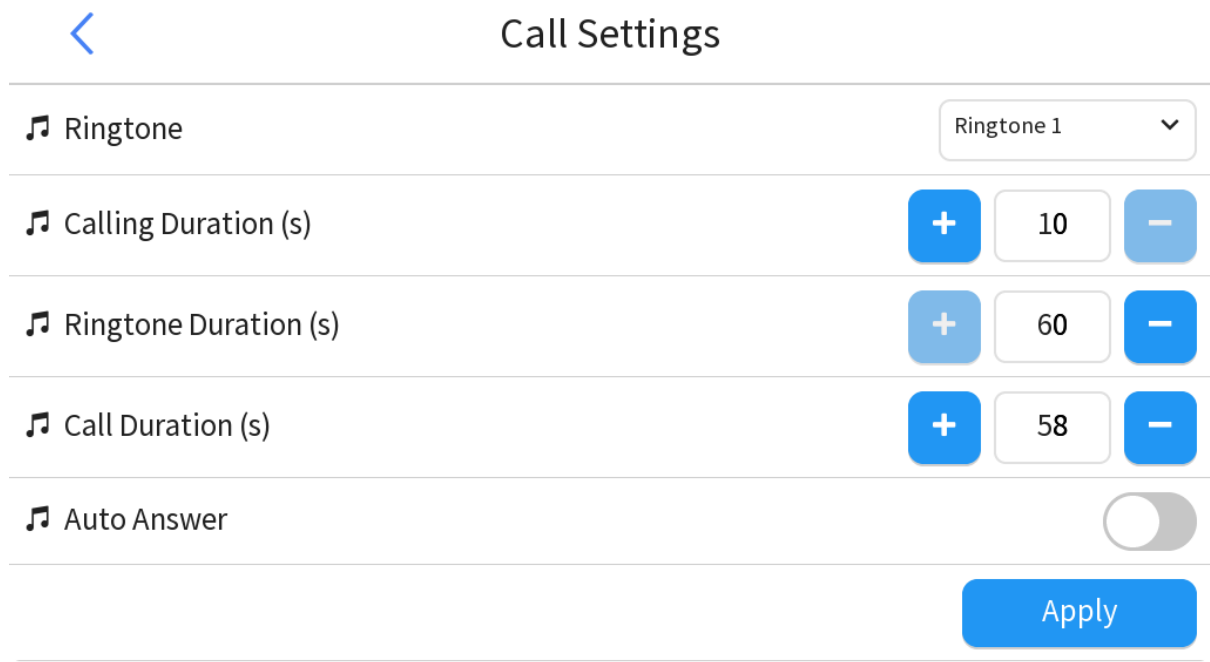
 **Note:** By default, the system will automatically return to the [Home Screen](#) if there is no operation and incoming calls within 60 seconds. You can change the time to automatically return to the home screen in [Indoor Station](#).

### 9.1 Sounds

#### 9.1.1 Call Settings

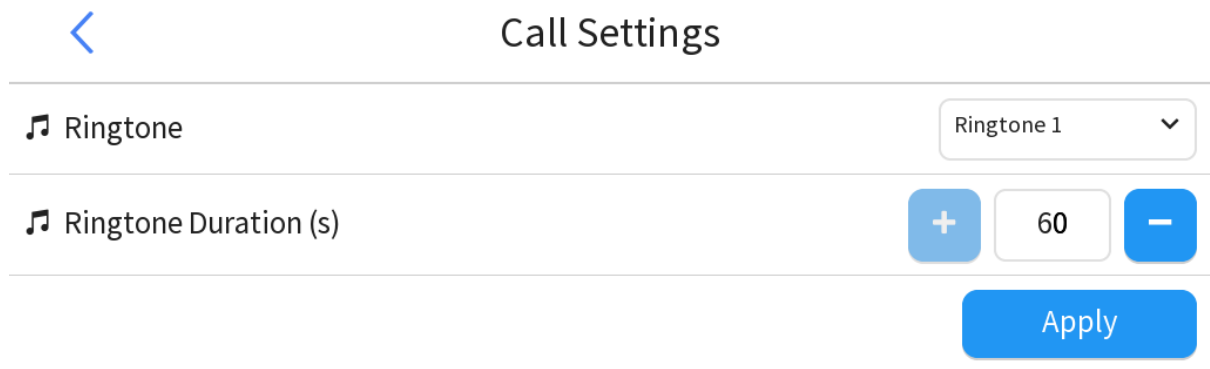
1. Go to  > **Sounds** > **Call Settings**.

Figure 9-1: Call Settings-Main Station



The screenshot shows the 'Call Settings' interface for a Main Station. At the top left is a blue back arrow, and at the top center is the title 'Call Settings'. Below this are five settings rows, each separated by a horizontal line. The first row is 'Ringtone' with a music note icon and a dropdown menu showing 'Ringtone 1'. The second row is 'Calling Duration (s)' with a music note icon, a blue '+' button, a white input field containing '10', and a blue '-' button. The third row is 'Ringtone Duration (s)' with a music note icon, a blue '+' button, a white input field containing '60', and a blue '-' button. The fourth row is 'Call Duration (s)' with a music note icon, a blue '+' button, a white input field containing '58', and a blue '-' button. The fifth row is 'Auto Answer' with a music note icon and a grey toggle switch that is currently turned off. At the bottom right of the settings area is a blue 'Apply' button.








Figure 9-2: Call Settings-Extension




The screenshot shows the 'Call Settings' interface for an Extension. At the top left is a blue back arrow, and at the top center is the title 'Call Settings'. Below this are two settings rows, each separated by a horizontal line. The first row is 'Ringtone' with a music note icon and a dropdown menu showing 'Ringtone 1'. The second row is 'Ringtone Duration (s)' with a music note icon, a blue '+' button, a white input field containing '60', and a blue '-' button. At the bottom right of the settings area is a blue 'Apply' button.

2. Set sound parameters as needed. Refer to the description below.



Parameter	Description
Ringtone	<p>The ringtone that sounds when the indoor station receives a call.</p> <p>Three ringtones are available by default, including Ringtone 1, Ringtone 2, and Ringtone 3.</p> <p>The custom ringtone is the same as the Ringtone 1 by default. You can also import a custom ringtone as follows:</p> <ol style="list-style-type: none"> <li>(1) Save the audio you want to use to a SD card. Audio requirements: MP3 file, 8K sample rate, 16bit, mono channel, less than 10 seconds, less than 25KB, named as <b>Custom</b>.</li> <li>(2) Power off the indoor station, and insert the SD card.</li> <li>(3) Start up the indoor station, enter the <b>Call Settings</b> screen, choose <b>Custom</b> from the <b>Ringtone</b> list, and then tap <b>Apply</b>.</li> </ol>
Calling Duration (s)	<p>The time period that the indoor station initiates a call until the call is answered.</p> <p>Range: [10-60], integer only. Default: 60. You can tap  /  to adjust the value.</p>
Ringtone Duration (s)	<p>Length of time that the ringtone sounds when the indoor station receives a call.</p> <p>Range: [10-60], integer only. Default: 60. You can tap  /  to adjust the value.</p>
Call Duration (s)	<p>The maximum time period that the indoor station answers a call until the call is ended. The call will end automatically when the call duration exceeds the set one.</p> <p>Range: [30-60], integer only. Default: 60. You can tap  /  to adjust the value.</p>
Auto Answer	<p>When enabled, the indoor station's screen that to be called has no response. The device's screen that initiates calls may vary with models. The description is shown below.</p> <ul style="list-style-type: none"> <li>• Extension/intelligent recognition terminal: A voice is played and a message is displayed on the screen to prompt no answer.</li> <li>• Door station: A voice is played "<b>The user you are calling is unavailable</b>".</li> </ul> <p>By default, this function is disabled. You can tap  to enable it.</p>

3. Tap . A success message means the settings are saved.

## 9.1.2 Volume Settings


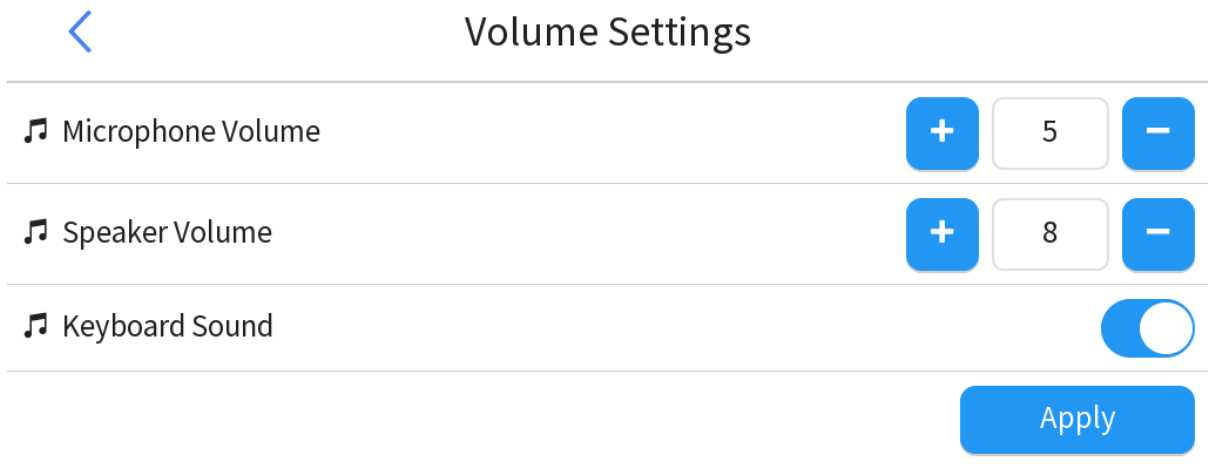






1. Go to  > **Sounds > Volume Settings**.

Figure 9-3: Volume Settings



2. Set sound parameters as needed. Refer to the description below.

Parameter	Description
Microphone Volume	Sound volume of the microphone during the call. Range: [0-10], integer only. Default: 5. You can tap  /  to adjust the value.
Speaker Volume	Sound volume of the speaker during the call. Range: [0-10], integer only. Default: 8. You can tap  /  to adjust the value.
Keyboard Sound	Sound to be played when you press on the indoor station's screen. By default, the keyboard sound is enabled. You can tap  to disable it.

3. Tap . A success message means the settings are saved.

## 9.2 General Settings

### 9.2.1 Display Settings

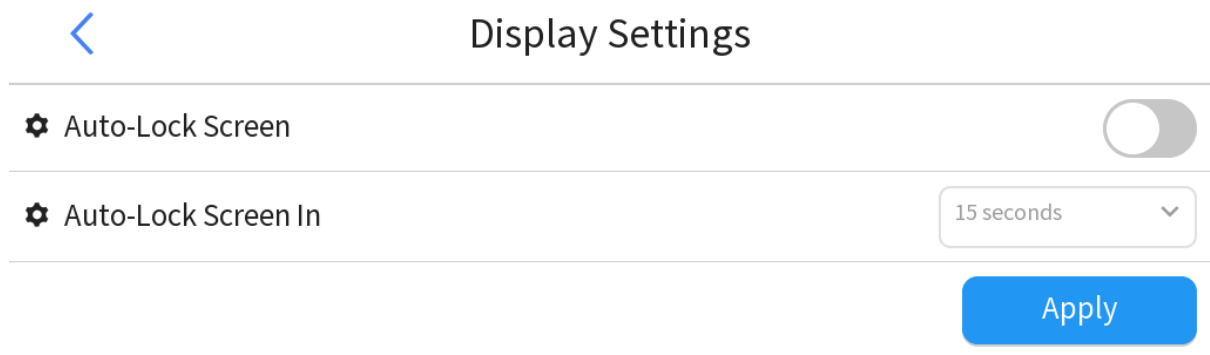
Set the auto-lock screen parameters.



When **Auto-Lock Screen** is enabled, the screen turns off automatically if there is no user operation and incoming call during the set time. Tap anywhere on the screen to unlock the screen.

User can turn off the screen manually anytime by tapping the **Lock Screen** button on the home screen. See [Lock Screen Manually](#) for details.

1. Go to  > **General Settings** > **Display Settings**.

Figure 9-4: Display Settings



2. Tap  to enable **Auto-Lock Screen**.
3. Set the auto-lock screen time. Default: 15 seconds. Options: 15s, 30s, 1min, 2min, 5min, 10min.
4. Tap . A success message means the settings are saved.

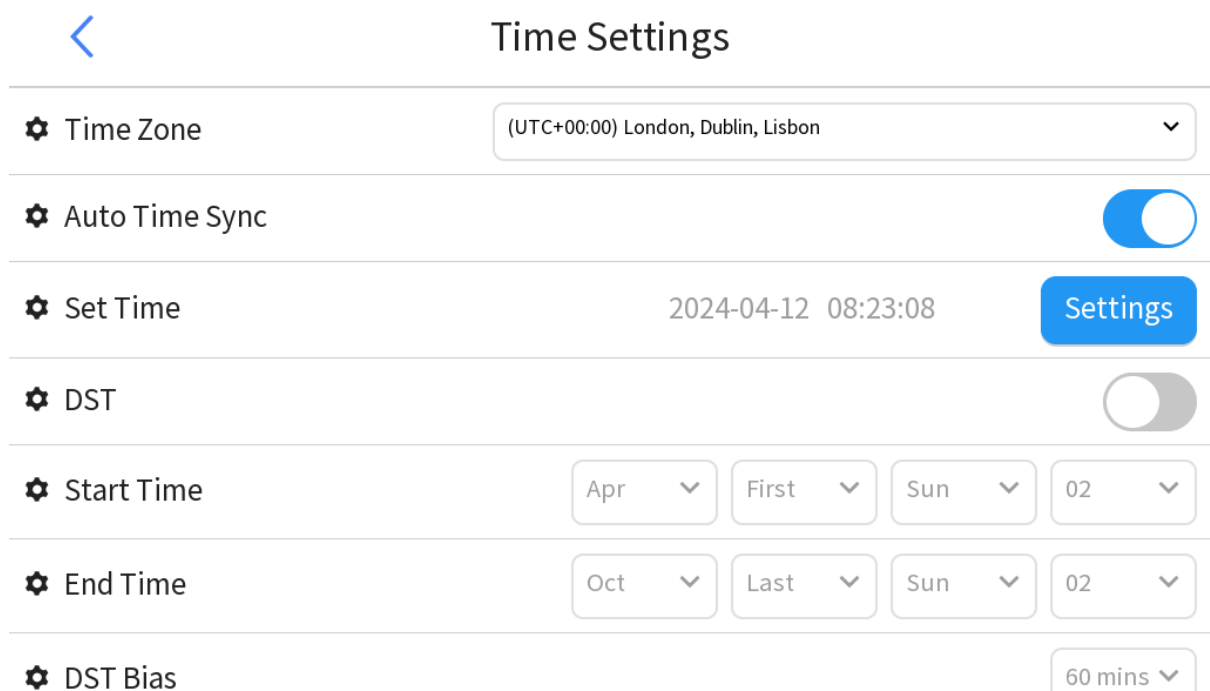
## 9.2.2 Time Settings


Set the system time of the indoor station.

For time configuration on the Web interface, see [Time](#).

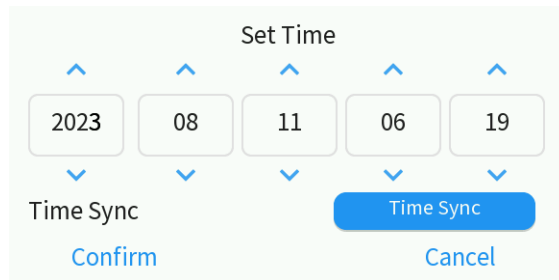
1. Go to  > **General Settings** > **Time Settings**.

Figure 9-5: Time Settings



2. Set the time zone. It takes effect immediately after setting.
3. Enable/disable **Auto Time Sync** as needed. It is enabled by default.
  - For the main indoor station that has no connected intelligent recognition terminal or door station:
    - When you add a device manually, the indoor station time will automatically sync with the connected device.
    - When you add devices in batches, the indoor station time will automatically sync with the first connected device.
  - For the extension: After the extension is connected to the main indoor station, the extension time will automatically sync with the main indoor station.
4. Tap . The **Set Time** screen appears.

**Figure 9-6: Set Time**




(1) The following two ways are available.

- Enter the specific time.
- Tap **Time Sync**. The indoor station time will automatically sync with the first connected device, or with the next connected device if the time synchronization fails. The extension time will automatically sync with the main indoor station.

 **Note:**

- After enabling the time synchronization, the specific time will be invalid.
- If the indoor station restarts or is connected to a new intelligent recognition terminal/door station, the time will be synced automatically.

(2) Tap **Confirm** to save the settings.

5. (Optional) Set the DST. It is disabled by default.
6. Tap  at the bottom of the screen. A success message means the settings are saved.

## 9.2.3 Password Settings

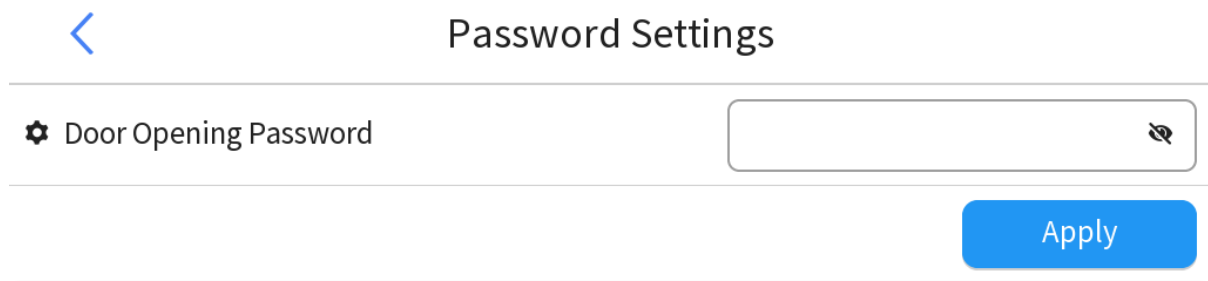
Set the door opening password. This password can be used to open all doors connected to the indoor station.


 **Note:**

- To use this function, enable the password verification function on the intelligent recognition terminal first.
- This function is only available to the main indoor station.

1. Go to  > **General Settings** > **Password Settings**.


Figure 9-7: Password Settings



2. Input the door opening password with 4 to 30 characters.
3. Tap . A success message means the settings are saved.

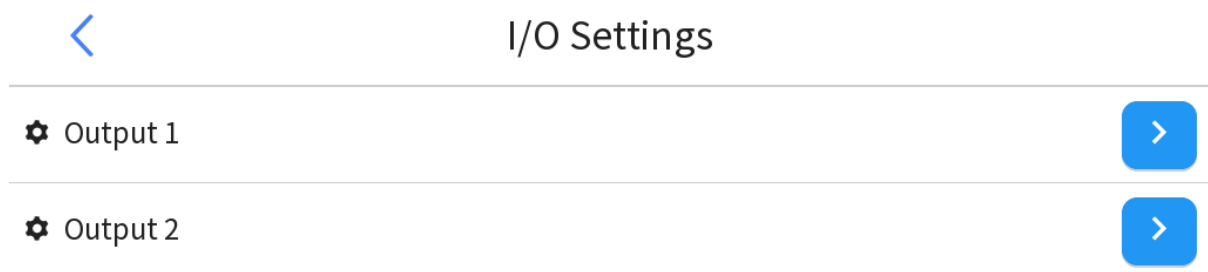
## 9.2.4 I/O Settings

When the indoor station receives a call from the door station, it will send output signals to the connected output devices (for example, alarm light).

 **Note:** To relate the door station to the indoor station, see [Related Devices](#) and [Device Discovery](#) for details.

1. Go to  > **General Settings** > **I/O Settings**.

Figure 9-8: I/O Settings



2. Tap **Output 1**, and then configure the related parameters.

Figure 9-9: I/O Settings-Output 1


Output 1

Enable

Delayed

Duration

Apply

- Enable: When enabled, the indoor station will send output signals to its connected output devices.
  - Delayed: The delayed time period after the door station initiates a call. The indoor station will send output signals after the delay ends but the call still continues or the call is in progress.
  - Duration: The time period that the indoor station continues sending output signals. If the call ends in the set duration, or the set duration reaches, the indoor station will no longer send output signals.
3. Tap . A success message means the settings are saved.
  4. (Optional) Tap **Output 2**, and then configure related parameters by referring to the steps above.

## 9.2.5 Visitor Message Settings

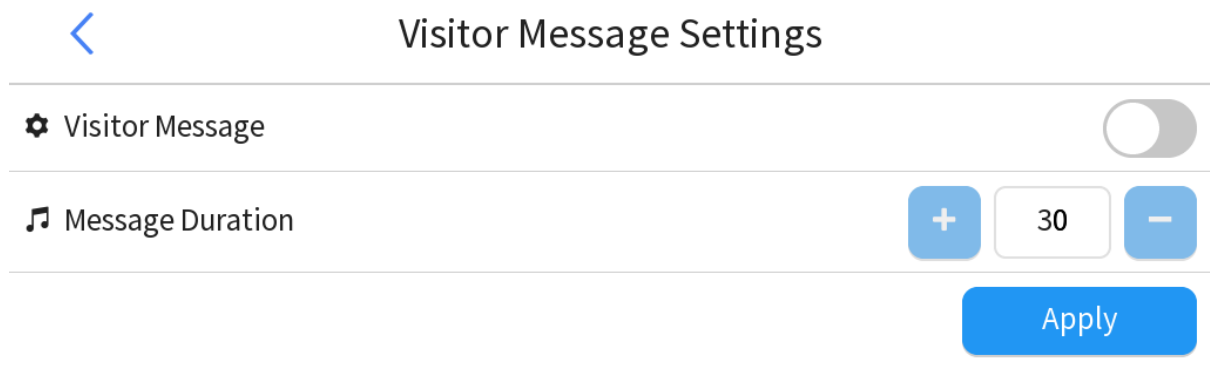
If the indoor station does not answer the call after the set call duration, the visitor can leave a message with the door station, and the message will be stored to the indoor station. You can view the message contents in [Visitor Message](#).

### Note:

- This function is only available to the main indoor station.
- You can set the calling duration in [Call Settings](#).


1. Go to  > **General Settings** > **Visitor Message Settings**.

Figure 9-10: Visitor Message Settings



2. Enable **Visitor Message**.
3. Set the message duration. If the message duration reaches the upper limit, or the call is hung up manually by the indoor station or door station, the message will be ended and stored to the indoor station. If the indoor station answers the call, this message will not be stored.

Range: [30-60], integer only. Default: 30.

4. Tap . A success message means the settings are saved.

## 9.3 Wi-Fi

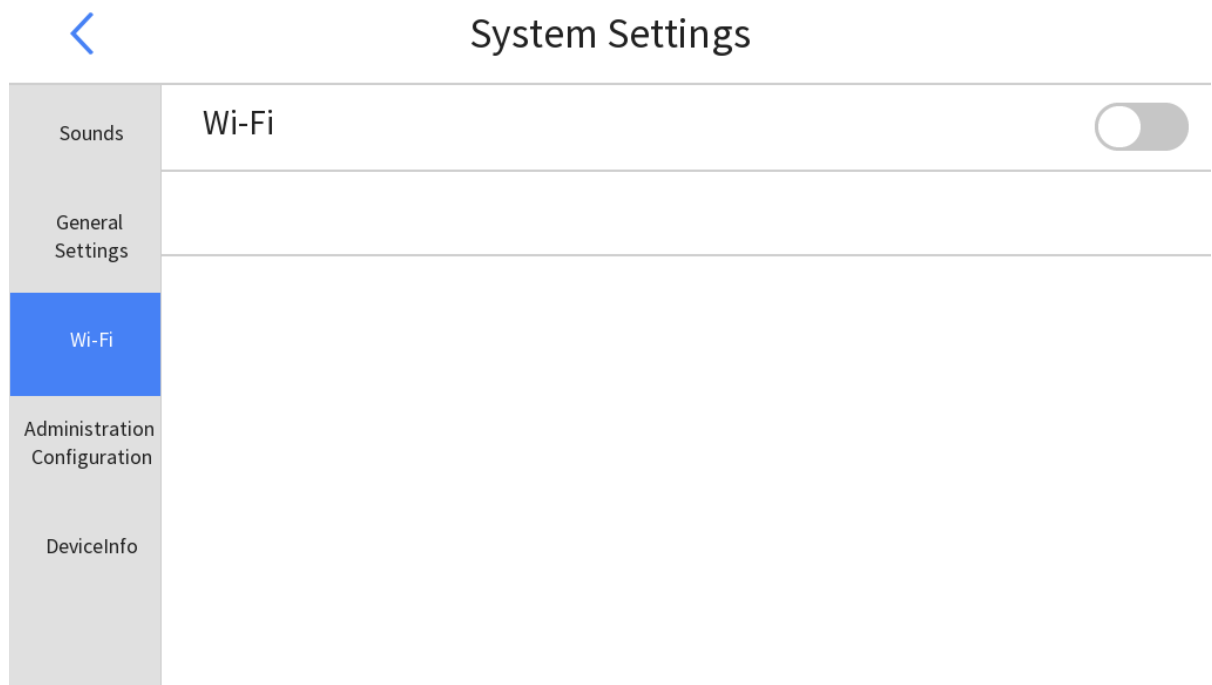
Configure Wi-Fi for the indoor station network connection, so the call, live view, device connection, and other operations can be used normally.

See [Wi-Fi](#) for details.

### Add Wi-Fi

1. Go to  > **Wi-Fi**.

Figure 9-11: Wi-Fi




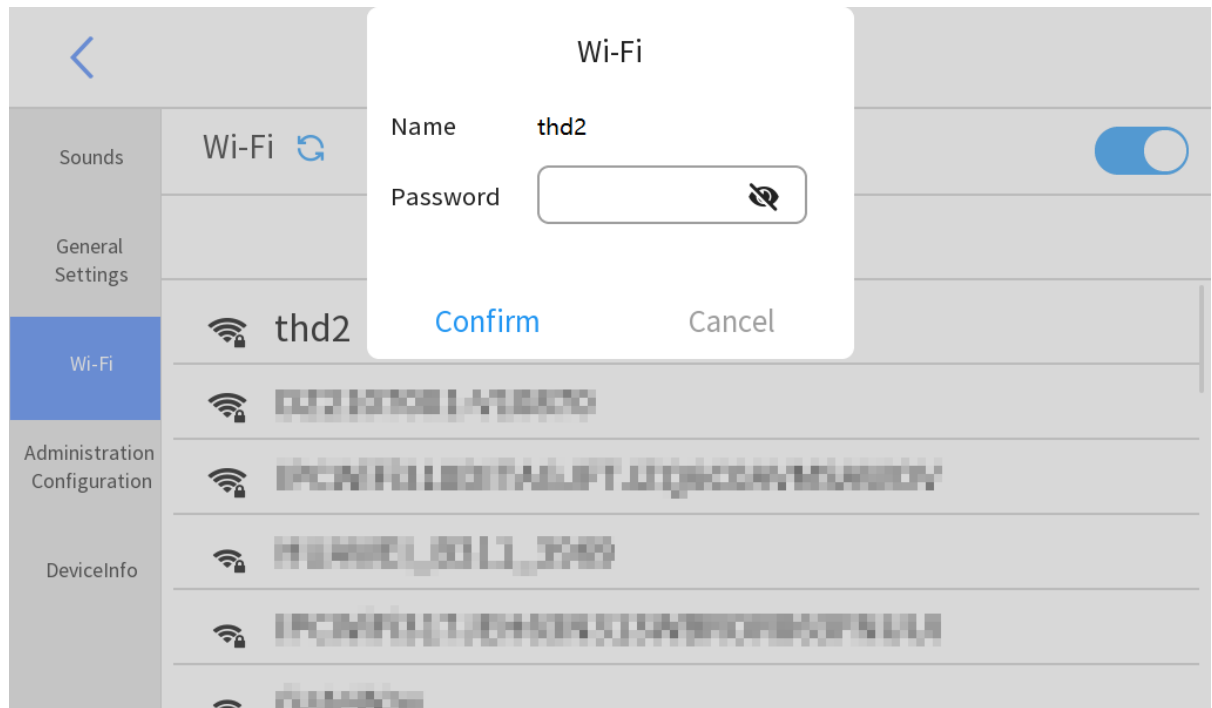
2. Tap  to enable Wi-Fi. The available Wi-Fi networks will be searched automatically and displayed in the list below from strong to weak signal.
3. Select the Wi-Fi to connect from the list below. Input the Wi-Fi password, and then tap **Confirm**.

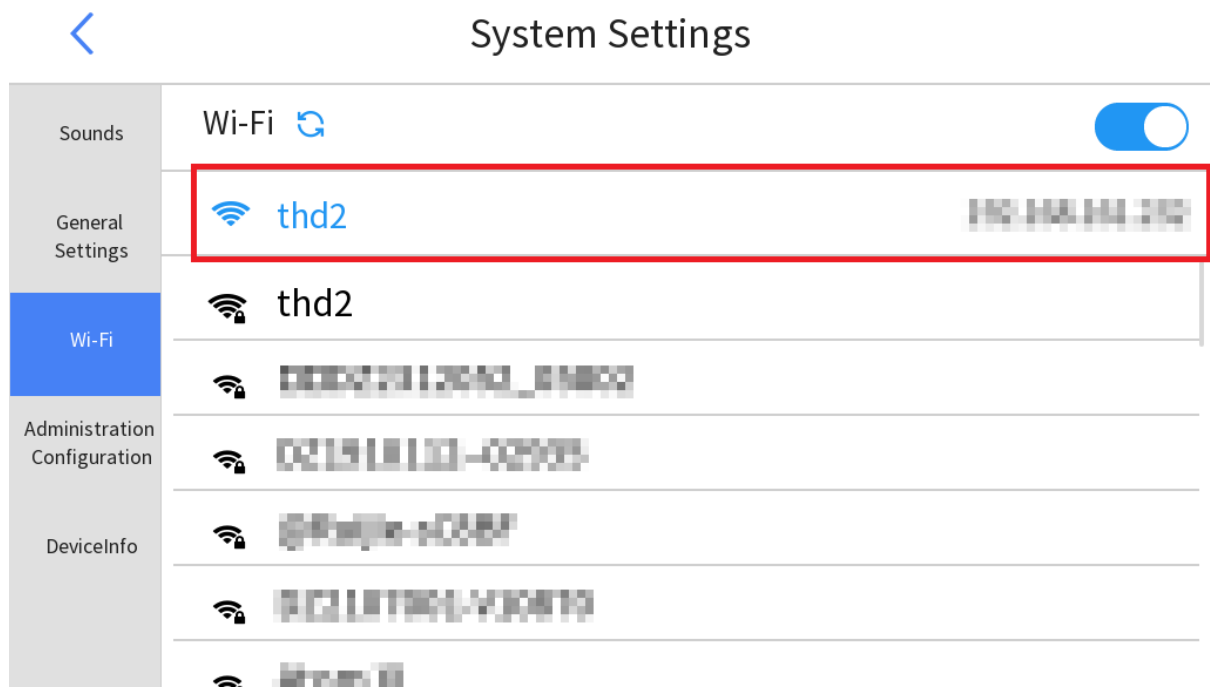
Figure 9-12: Connect Wi-Fi



After the Wi-Fi is connected, the Wi-Fi name and corresponding network information are displayed in the top list.



Figure 9-13: Wi-Fi Connection Succeeded



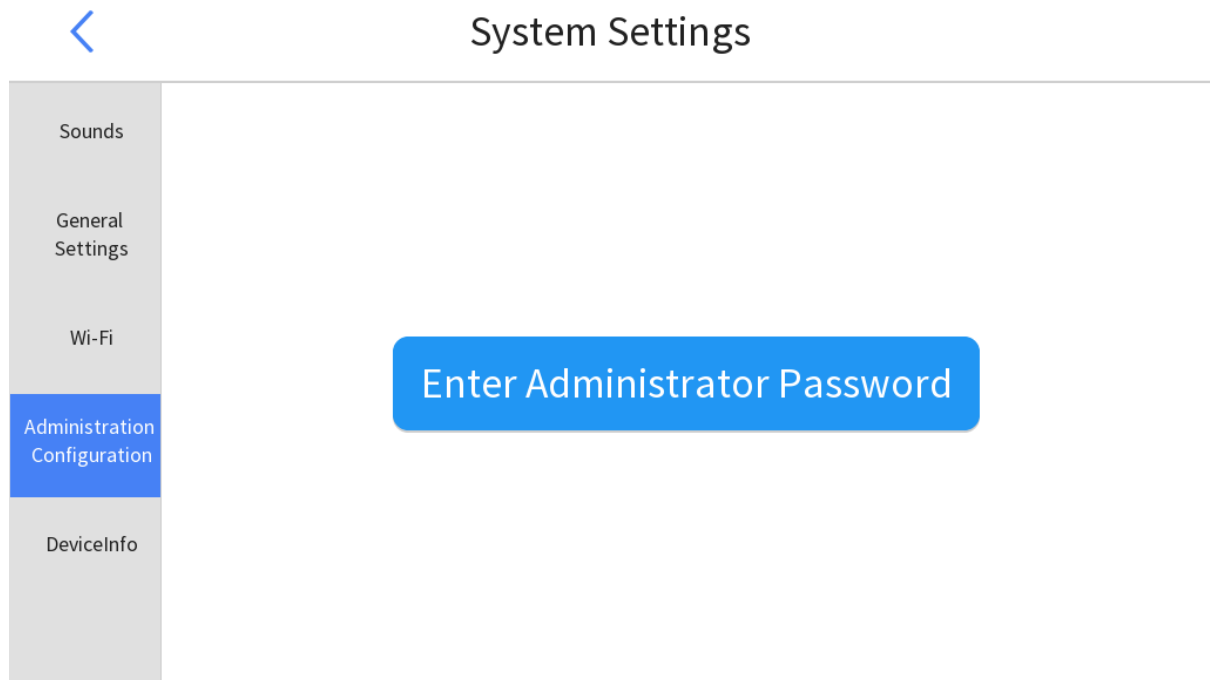
#### Disconnect Wi-Fi

Tap the Wi-Fi name that has been connected, and then a prompt appears. Tap **Confirm** to delete it.

## 9.4 Administration Configuration

1. Tap , and enter the **Administration Configuration** screen.

Figure 9-14: Administration Configuration



2. Tap **Enter Administrator Password**.

**Figure 9-15: Enter Password**


Please enter the administrator password.

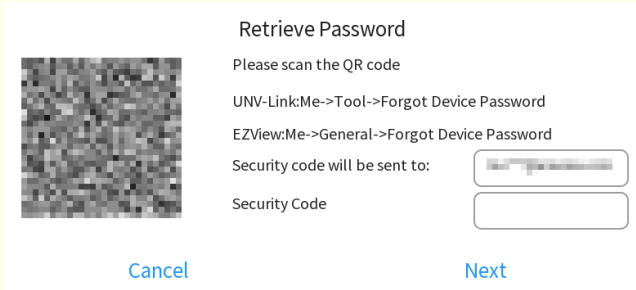
 [Forgot Password?](#)

Login

Cancel

3. Enter the administrator password. It is **123456** by default, which is consistent with the admin password to log in to the Web interface.

 **Note:** If you forgot your password, you can follow the on-screen instructions to obtain a security code. Enter the security code, and tap **Next** to reset your password.




The screen will display:

- Email not Set: No email address is bound to the device currently.
- Email address: The email address that is bound to the device.

4. Tap **Login**.

## 9.4.1 Indoor Station

Set the indoor station type, and its network and location parameters.

Tap , and go to **Administration Configuration > Indoor Station**.

**Figure 9-16: Indoor Station-Main Station**

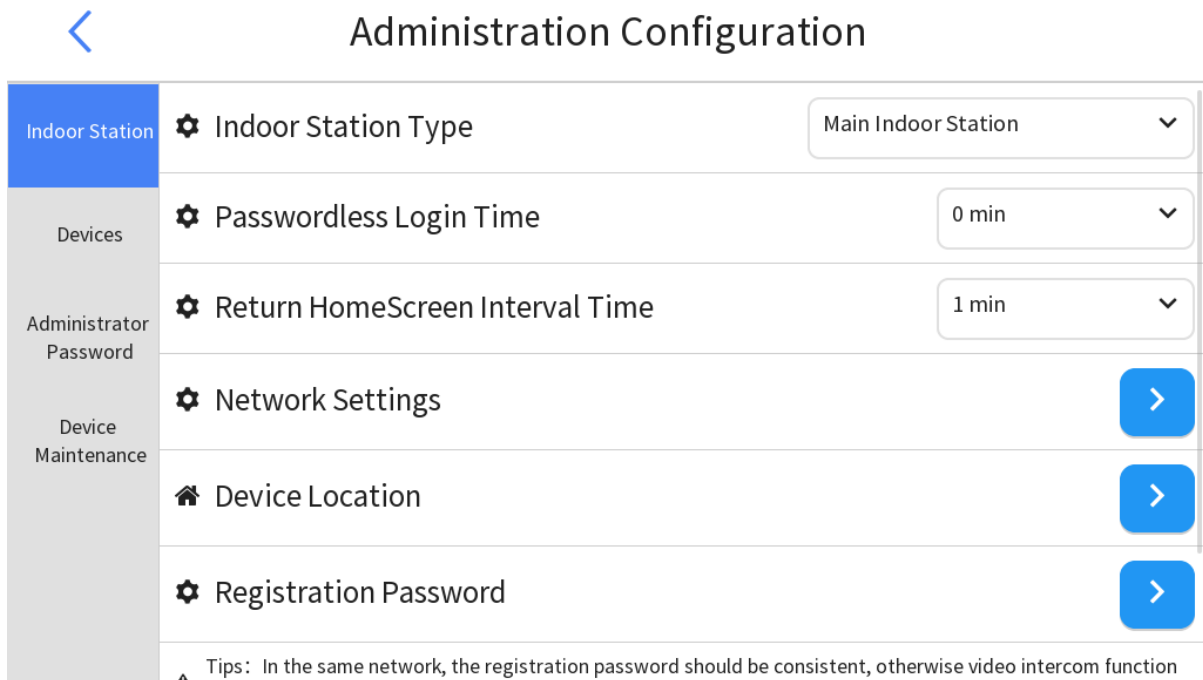
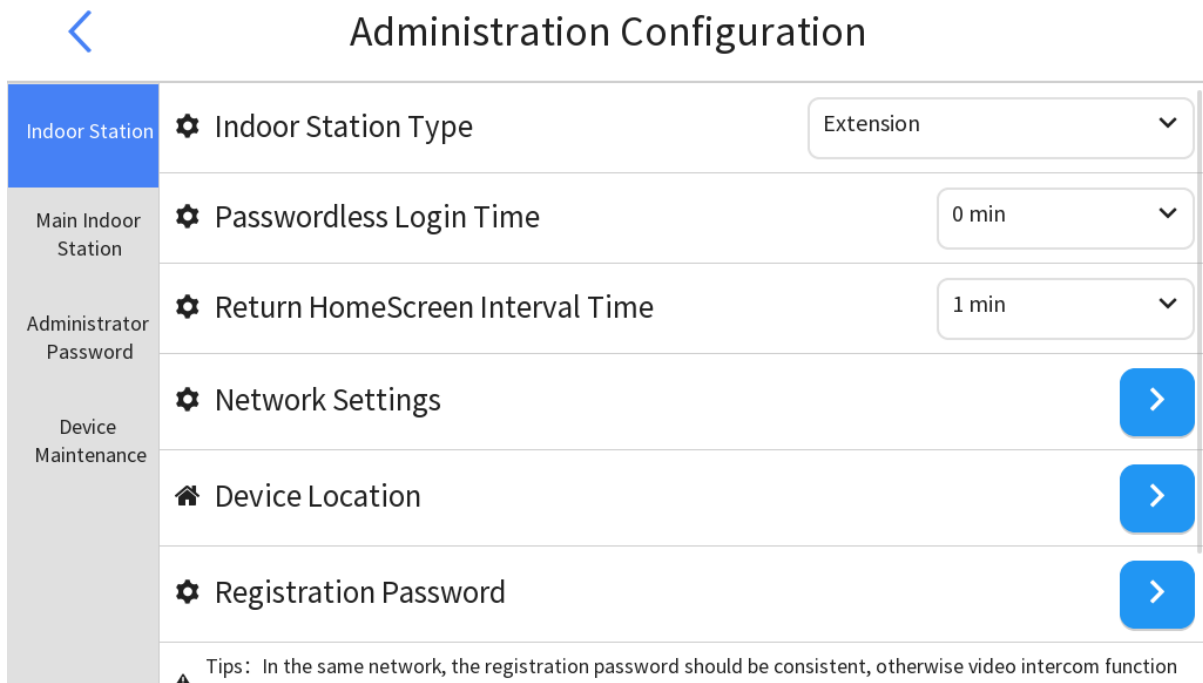


Figure 9-17: Indoor Station-Extension



- Indoor Station Type: It is Main Indoor Station by default. If it is set to **Extension**, the system will return to the home screen and restore some factory settings.
- Passwordless Login Time: The duration to log in to the [Administration Configuration](#) screen without the password. Default: 0 min.

 **Note:**

- If you change the parameter during the passwordless login time, the system will relock from the time that the change is completed.
  - If you restart the device during the passwordless login time, the system will relock from the time that the [Administration Configuration](#) screen is re-logged in after restart.
- Return HomeScreen Interval Time: The system will automatically return to the [Home Screen](#) if there is no operation or incoming calls within the set time. Default: 1 min.

### 9.4.1.1 Network Settings

For more network information, see [Wired Network](#).

1. Tap , go to **Administration Configuration > Indoor Station > Network Settings**.

Figure 9-18: Network Settings

Network Settings

Obtain Automatically(DHCP)


Static IP

IP Address

Subnet Mask

Default Gateway

Apply

2. Set network parameters. You can use DHCP to assign a dynamic IP address or set a static IP address.
  - Obtain Automatically (DHCP): If a DHCP (Dynamic Host Configuration Protocol) server is configured on the network, it will assign the indoor station an IP address automatically.
  - Static IP: Set a fixed IP address manually for long term use. Enable **Static IP**, and then set the IP address, subnet mask, and default gateway.
3. Tap . A success message means the settings are saved.

### 9.4.1.2 Device Location

1. Tap , go to **Administration Configuration > Indoor Station > Device Location**.

Figure 9-19: Device Location-Main Station

Device Location

Community Indoor

Phase 1

Building 1

Unit 1

Room No. 1

Extension No. 0


Figure 9-20: Device Location-Extension

The screenshot shows a mobile application interface for configuring a device's location. At the top left is a blue back arrow. The title 'Device Location' is centered at the top. Below the title is a horizontal line. Underneath, there is a label 'Extension No.' with a house icon to its left. To the right of the label is a text input field containing the number '1'. At the bottom right of the screen is a blue button with the text 'Apply' in white.

2. Set device location parameters, including community, phase, building, unit, room number, and extension number.

 **Note:**

- Main station: Phase, building, unit, and extension number range: [0-99]; Room range: [0-9999].
- Extension: Extension number range: [1-19].
- For the main indoor station, the extension number is 0 by default and cannot be modified. For the extension station, only the extension number can be set and must be unique. The extension location is consistent with the associated main indoor station except the extension number.

3. Tap  at the bottom of the screen. A success message means the settings are saved.

### 9.4.1.3 Registration Password

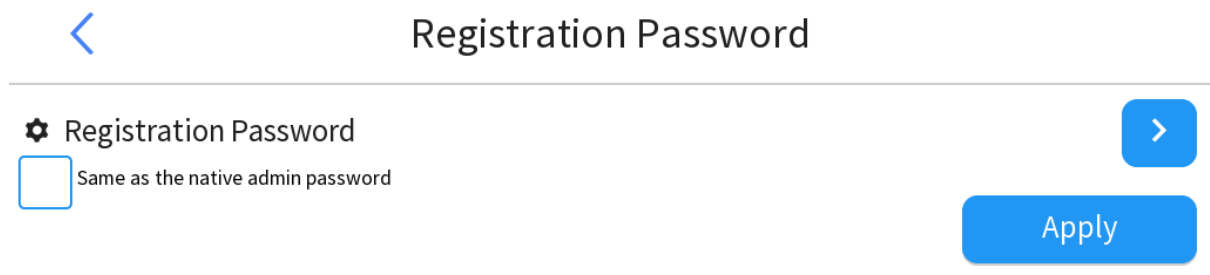
The registration password of the related device must be consistent with that of the indoor station in the same network segment, so the live view and video intercom functions can be used for networking security.

 **Note:**

- You can set the registration password of the related device in [Related Devices](#) or [Device Discovery](#).
- For the main indoor station, only the registration password of the single-button door station, and indoor station (including main station and extension) can be configured.
- For the indoor station extension, only the wizard page allows to set the registration password of the searched indoor station (including main station and extension).
- You can set the registration password on the Web interface. See [Set Registration Password](#) for details.

1. Tap , go to **Administration Configuration > Indoor Station > Registration Password**.

Figure 9-21: Registration Password



2. Set the registration password. Several methods are available:



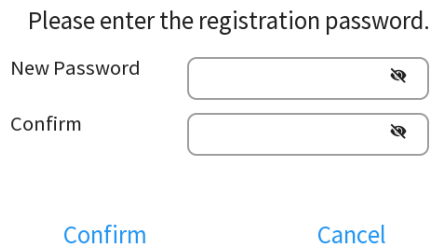

- Tap : The password is **12345678** by default.
- Tap **Registration Password**, set the registration password (9 to 32 characters including digits, letters, and special characters), and enter the password again to confirm, and tap **Confirm**. Tap , and the registration password is set successfully.


Figure 9-22: Enter Registration Password



- Select **Same as the native admin password**, tap , and then the registration password will be the same as the administrator password of the indoor station.

## 9.4.2 Devices

The devices screen includes related devices, indoor stations, and device discovery.

 **Note:** This function is only available to the main indoor station. For extension settings, see [Main Indoor Station](#).

### 9.4.2.1 Related Devices

Set an intelligent recognition terminal/door station/network camera so the indoor station can intercom with it, control it remotely, and open the door remotely.

Up to 20 door stations (intelligent recognition terminal/door station/network camera) can be bound to the indoor station.

The [Device Discovery](#) screen can automatically search for available door stations.


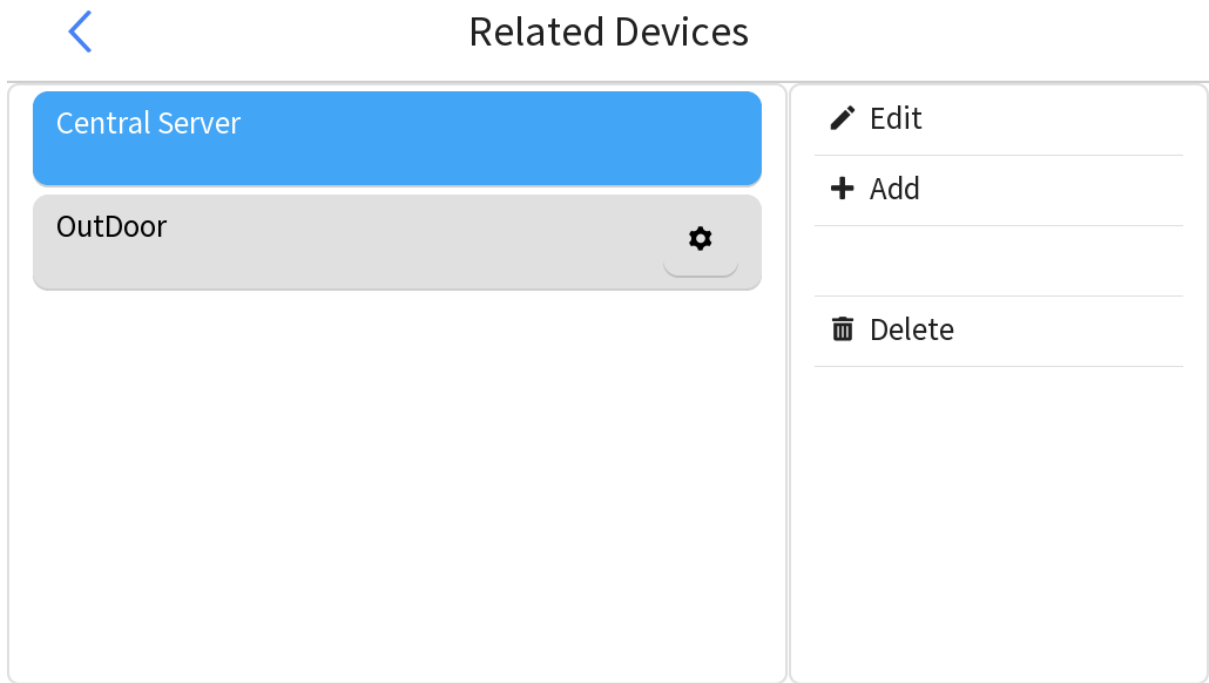
Tap , go to **Administration Configuration > Devices > Related Devices**.

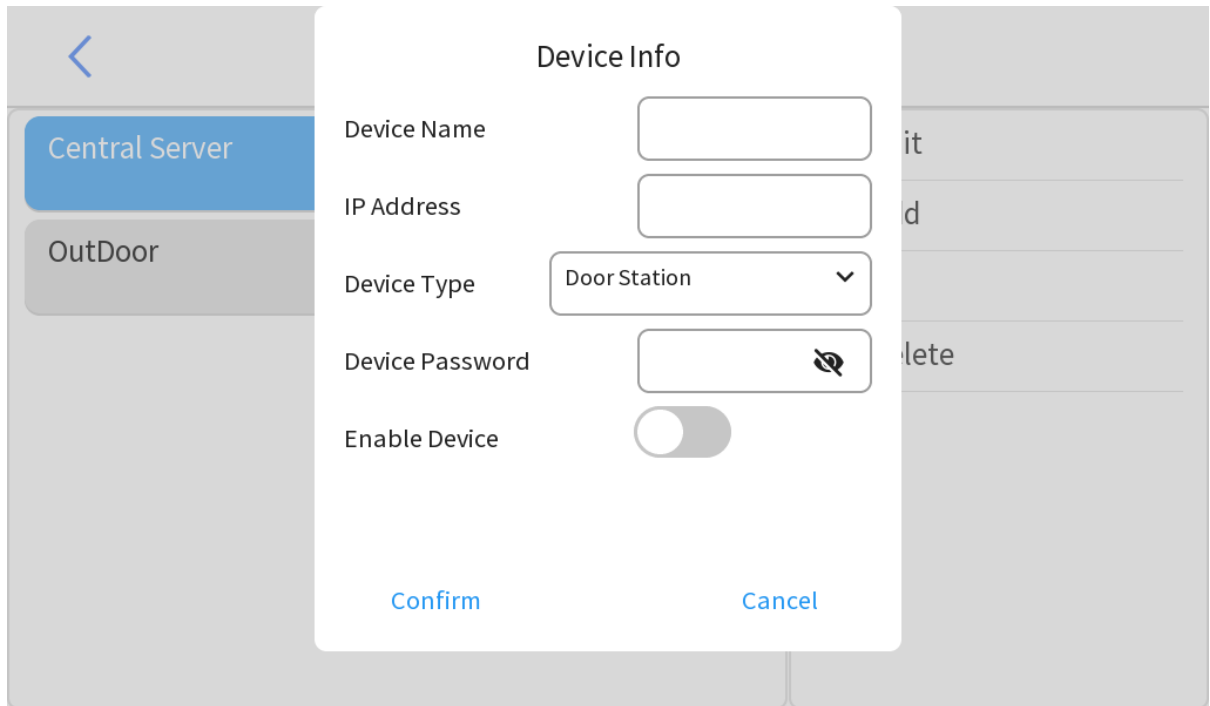
Figure 9-23: Related Devices




### Add

1. Tap **+ Add**. The **Device Info** screen appears.

Figure 9-24: Add




2. Input device information. Some parameters are described below.
  - IP Address: Required. The IP address of the intelligent recognition terminal/door station/network camera.

 **Note:**

  - The indoor station's IP must be on the same IP segment as the door station's IP to be bound.
  - To use a wireless network, the device to be bound should connect to a same Wi-Fi as the indoor station.


  - Device Type: Select **Door Station** for the intelligent recognition terminal and door station; select **Camera** for the network camera.

- Device Password: The administrator password of the related device.
- Enable Device: You need to enable the device in order to use the live view, call, and answer functions. By default, this function is disabled.
- Port (required only for **Device Type** as **Camera**): The port number of the network camera. Default: 80.

 **Note:** To view the live video, please enter the port number of the network camera.


3. Tap **Confirm** to save the settings.

### Edit

1. Tap the device name you want to edit.
2. Tap  **Edit** . The **Device Info** screen appears.
3. Edit the device information as needed.
4. Tap **Confirm** to save the settings.

### Delete

After the related devices are deleted, the corresponding live video cannot be played, but the deleted devices can still call the indoor station.

1. Tap the device name you want to delete.
2. Tap  **Delete** .
3. Tap **Confirm** to save the settings.

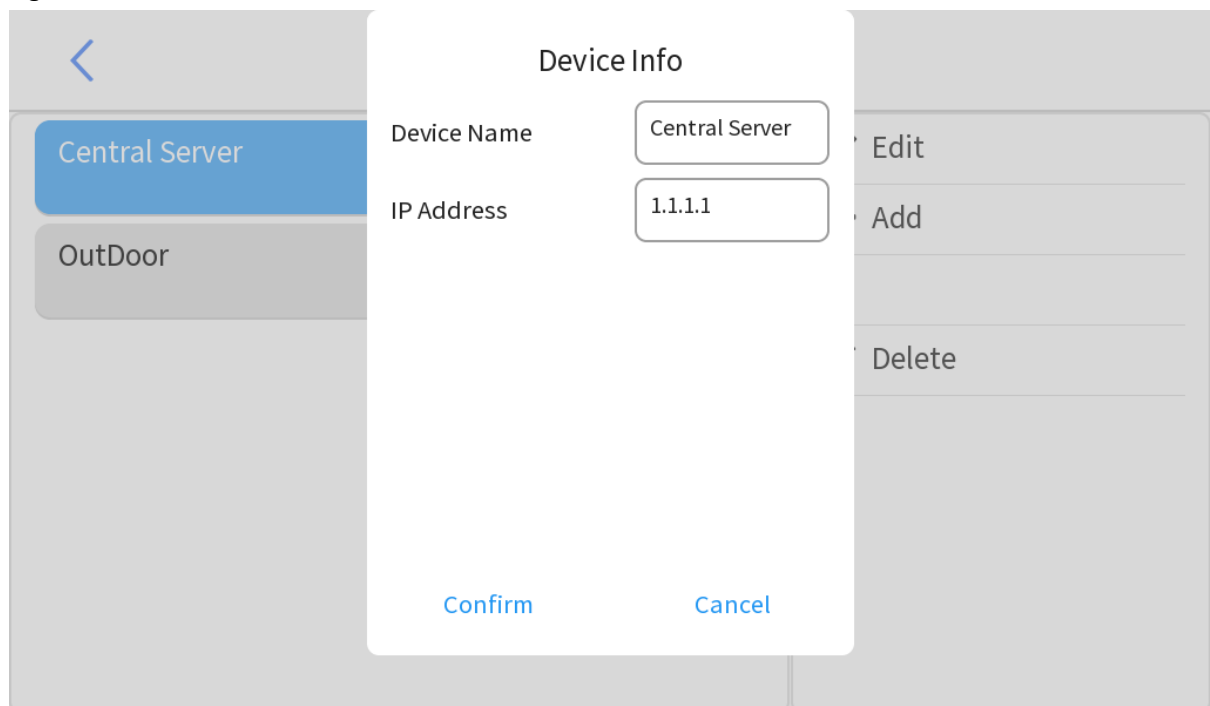
### Configure Central Server

The indoor station can be related to UMS, which can serve as a management center.

Only one central server is allowed, and it cannot be deleted.

1. Tap **Central Server**, tap **Edit**, and then the **Device Info** screen appears.

**Figure 9-25: Device Info**




2. The device name is **Central Server** by default, and cannot be changed. Please enter the IP address of UMS.
3. Tap **Confirm** to save the settings.

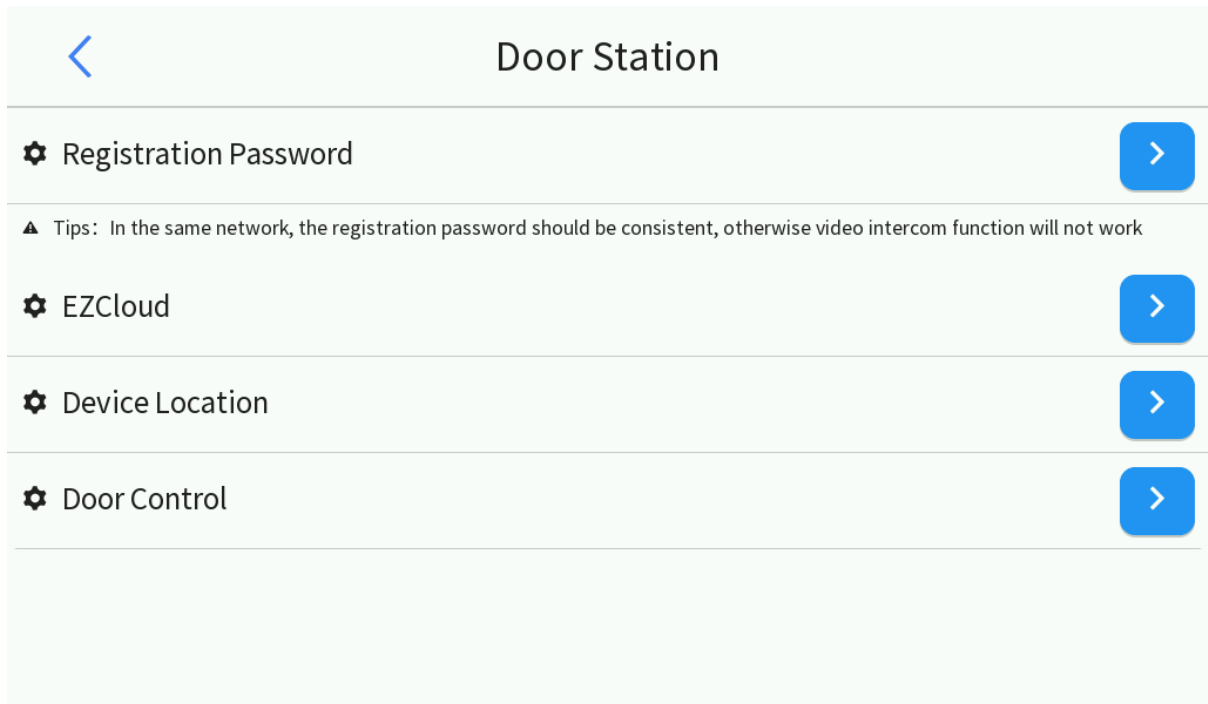


## Configure Related Devices

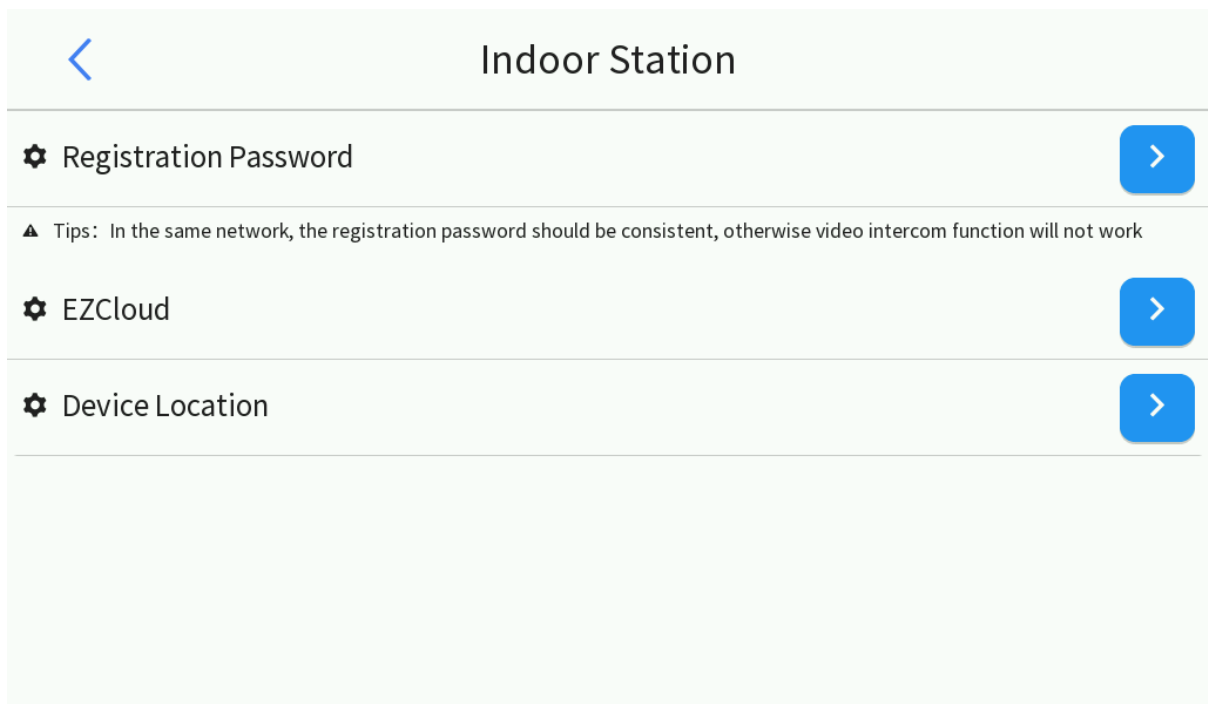
Configure the related device parameters, including registration password, device location, etc.

1. Tap  beside the device name, enter the administrator password, and then tap **Confirm**.
2. Configure the parameters including registration password, device location, etc.


**Figure 9-26: Related Device-Door Station**




**Figure 9-27: Related Device-Indoor Station**



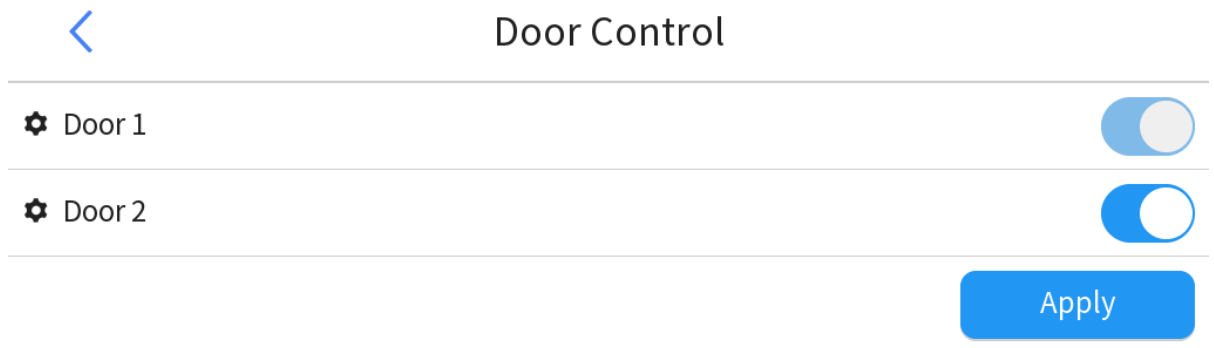
- **Registration Password:** To set the registration password or view the registration password of the device, see [Registration Password](#) for details.
- **EZCloud:** Tap **EZCloud**, and then the QR code appears. You can scan the QR code with the UNV-Link app and relate the device to it.

 **Note:** To view the QR code of the connected intelligent recognition terminal/door station, see [View Device QR Code](#).

- Device Location
  - To add the device to the indoor station, make sure the location information is the same except the extension number (see [Device Location](#) for indoor station location), and the extension number must be unique, otherwise the device will fail to add.
  - To add the device to the door station, set **Room No.** to 1 and make sure the extension number is unique.
- Door Control (only for door station): Enable/disable door control for the related devices. Only **Door 1** control is enabled by default. You can enable **Door 2** control as needed. The indoor station can open the door remotely when it receives a call from the door station.

 **Note:** See [I/O Settings](#) for indoor station configuration.

**Figure 9-28: Door Control**



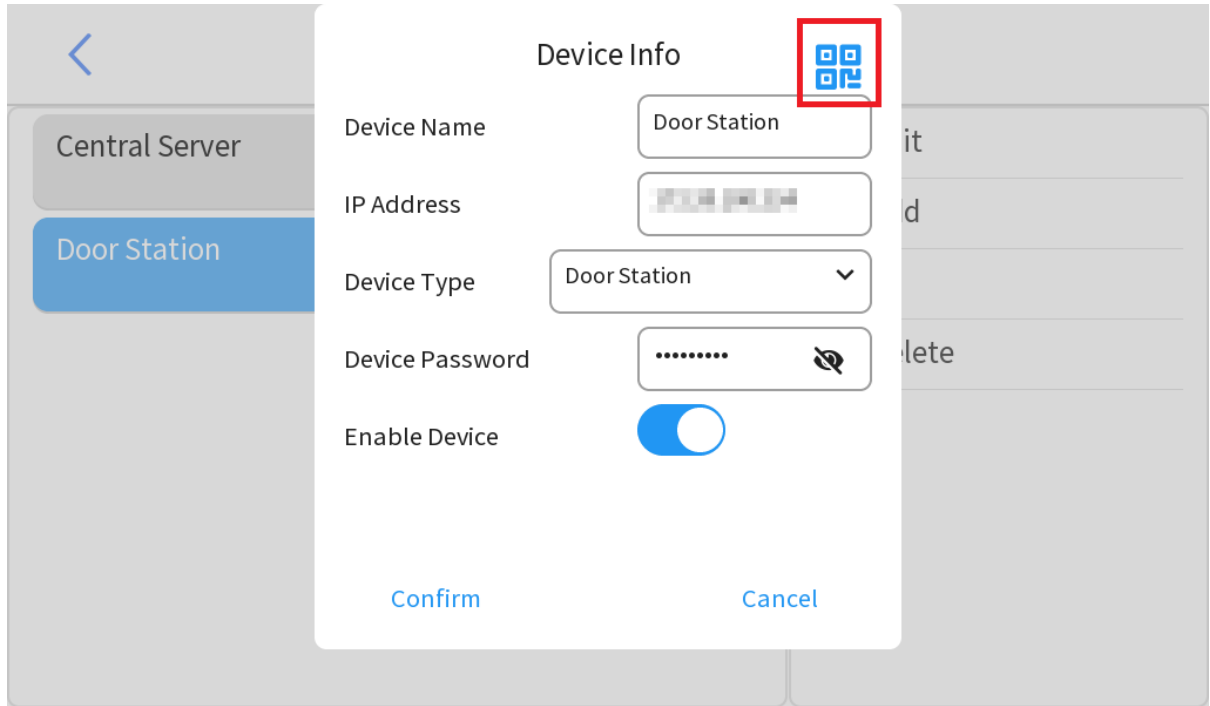
### View Device QR Code

 **Note:**

- This section describes how to view the QR code of a connected intelligent recognition terminal/door station.
- To view the QR code of this device, see [Device Maintenance](#).

1. Tap the device name that you want to view the QR code.
2. Tap **Edit**, then the device information appears. Tap the QR code icon right to the screen title, and then the code is displayed.

Figure 9-29: View QR Code



3. Scan the QR code with the UNV-Link app and relate the device to it.


### 9.4.2.2 Indoor Stations

Show all extensions bound to the main indoor station.

Tap , go to **Administration Configuration > Devices > Indoor Stations**.

Figure 9-30: Indoor Stations

Room Name	IP Address	Extension No.
Indoor	[blurred]	1

To configure the extension parameters including registration password, location information, etc., enter [Device Discovery](#), select a device you want to configure, and then tap .

### 9.4.2.3 Device Discovery


Add the main indoor station to the door station or indoor station extension for video intercom.

 **Note:**

- This function is available to the main indoor station.
- You can add door stations manually in [Related Devices](#).

Tap , go to **Administration Configuration > Devices > Device Discovery**.

The extension stations and door stations will be searched in the same or different network segment(s), and a prompt **Searching...** appears on the screen. You can not refresh the list or add new devices during the search.



Tap  can exit the current screen.

The discovered devices will be displayed in the list below. You can tap **Refresh** in the upper-right corner to search again.

**Figure 9-31: Device Discovery-Search Completed**



The screenshot shows a mobile application interface titled "Device Discovery". At the top left is a back arrow icon, and at the top right are icons for adding (+), removing (-), and refreshing (circular arrow). Below the title is a table with five columns: Product Type, SN Code, IP Address, Settings, and Status. The table contains one row of data with a circular icon on the left, a product type string, a SN code string, an IP address string, a gear icon in the Settings column, and a status string.

Product Type	SN Code	IP Address	Settings	Status
 CH-001-1-1-1-1-1-1	12345678901234567890	192.168.1.100		1/1/2018/10:00

#### Bind Device

1. Select the device you want to add.
2. Tap the IP address of the device(s) to be added, set the wired network information, and then enter the username and password. Make sure the IP address of the device is on the same IP segment as that of the indoor station (see [Network Settings](#) for details).





 **Note:** To use a wireless network, the device to be added should connect to the same Wi-Fi as the main indoor station.


Figure 9-32: Network Settings, Username, and Password


Network Settings

IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>
Default Gateway	<input type="text"/>
Username	<input type="text" value="admin"/>
Password	<input type="password" value="....."/> 


[Confirm](#)      [Cancel](#)

3. Configure the parameters of the device to be related. See [Configure Related Devices](#) for details.
4. Tap  to return to the **Device Discovery** screen. Select the configured device(s), tap , enter the administration password of the related device(s), then tap **Confirm**. You can view the added door stations in [Related Devices](#), and added extensions in [Indoor Stations](#).

 **Note:** If the indoor station restarts during the operation, the device will fail to be added and you need to add again.


After the device is related successfully, the status shows .

### Unbind Device

1. Select the device(s) you want to cancel the relation.
2. Tap  in the upper-right corner, and a pop-up window appears.
3. Tap **Confirm**.

## 9.4.3 Main Indoor Station

Set the main indoor station information on the extension, so as to add the extension to the main station for video intercom.

 **Note:** This function is only available to the extension station. For main indoor station settings, see [Devices](#).

1. Tap , and go to **Administration Configuration > Main Indoor Station**.

Figure 9-33: Main Indoor Station


Administration Configuration

Indoor Station Room Name

Main Indoor Station IP Address

Administrator Password Password

Device Maintenance

2. Enter the room name, IP address, and password of the main station to be bound.
3. Tap . A success message means the settings are saved.

## 9.4.4 Administrator Password

The administrator password is used to log in to the **Administration Configuration** screen and Web interface. To change the password on the Web interface, see [User](#) for details.

1. Tap , and go to **Administration Configuration > Administrator Password**.

Figure 9-34: Administrator Password


Administration Configuration

Indoor Station Old Password

Devices A strong password is required (9 to 32 characters including all three elements: digits, letters, and special characters).

Administrator Password New Password

Device Maintenance Confirm

2. Enter the old password, new password, and confirm the password as required.
3. Tap . A success message means the settings are saved.

## 9.4.5 Device Maintenance

Restart the indoor station and restore factory defaults.

For system maintenance on the Web interface, see [Maintenance](#).

Tap , and go to **Administration Configuration > Device Maintenance**.

Figure 9-35: Device Maintenance-Main Station

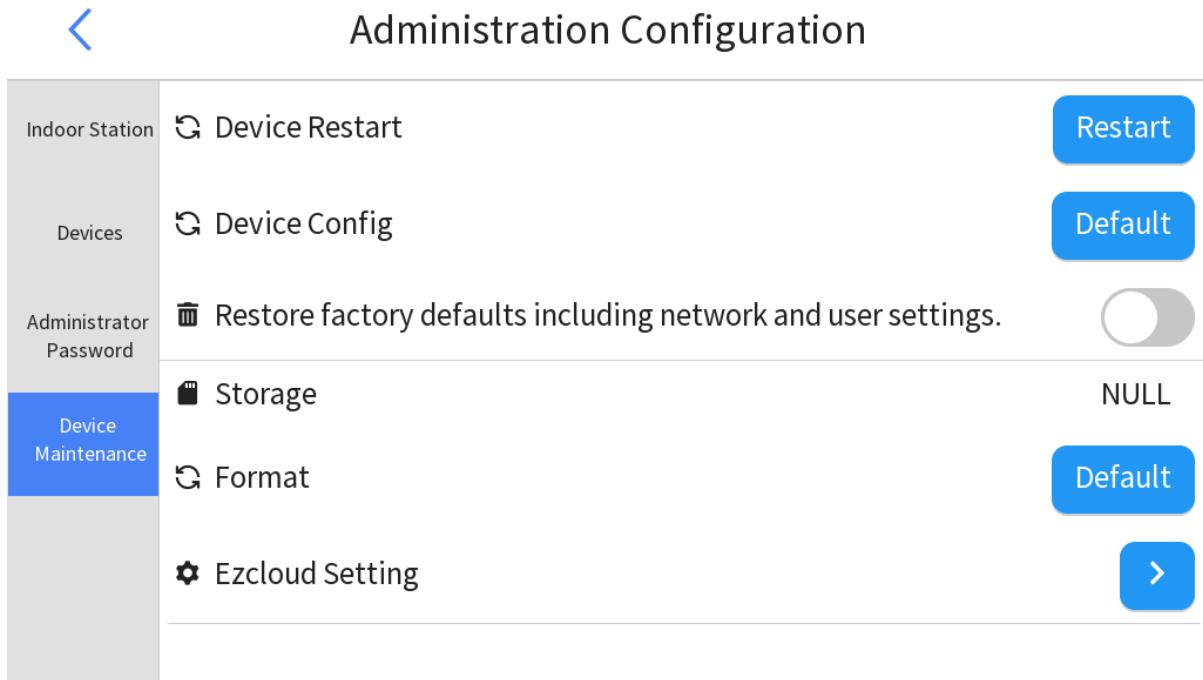
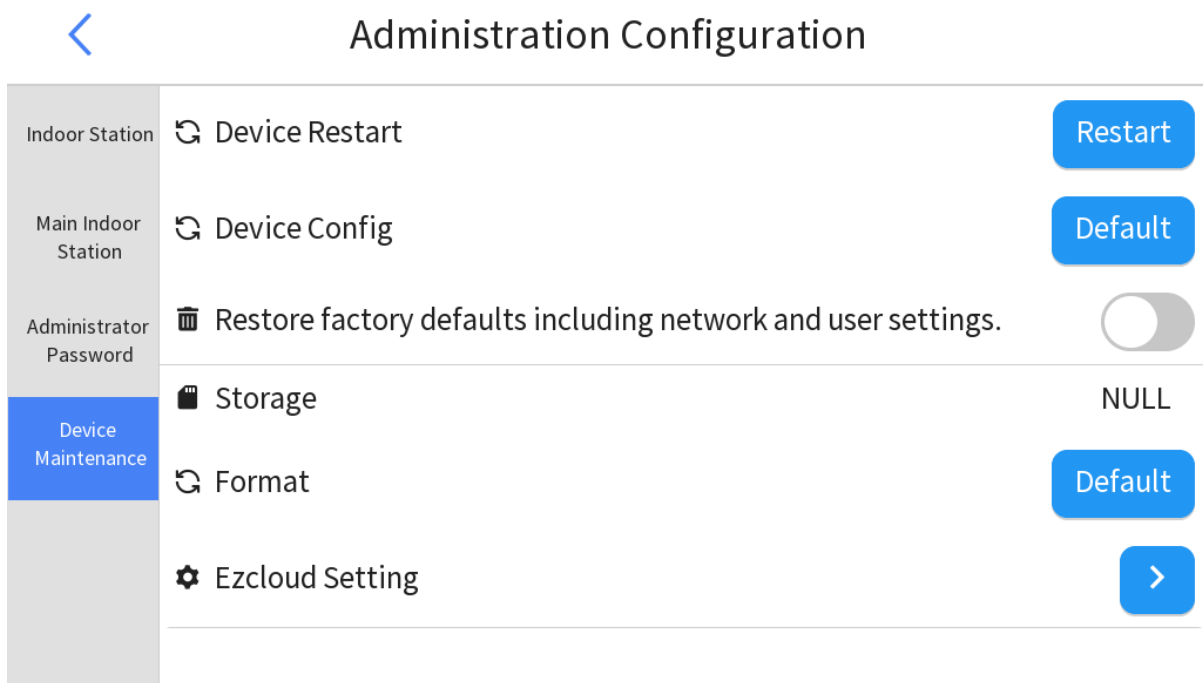





Figure 9-36: Device Maintenance-Extension



- Device Restart: Restart the indoor station. Tap , and then tap **Confirm** in the pop-up window to restart the indoor station.
- Device Config: All the parameters except network and user settings will be restored to default settings.

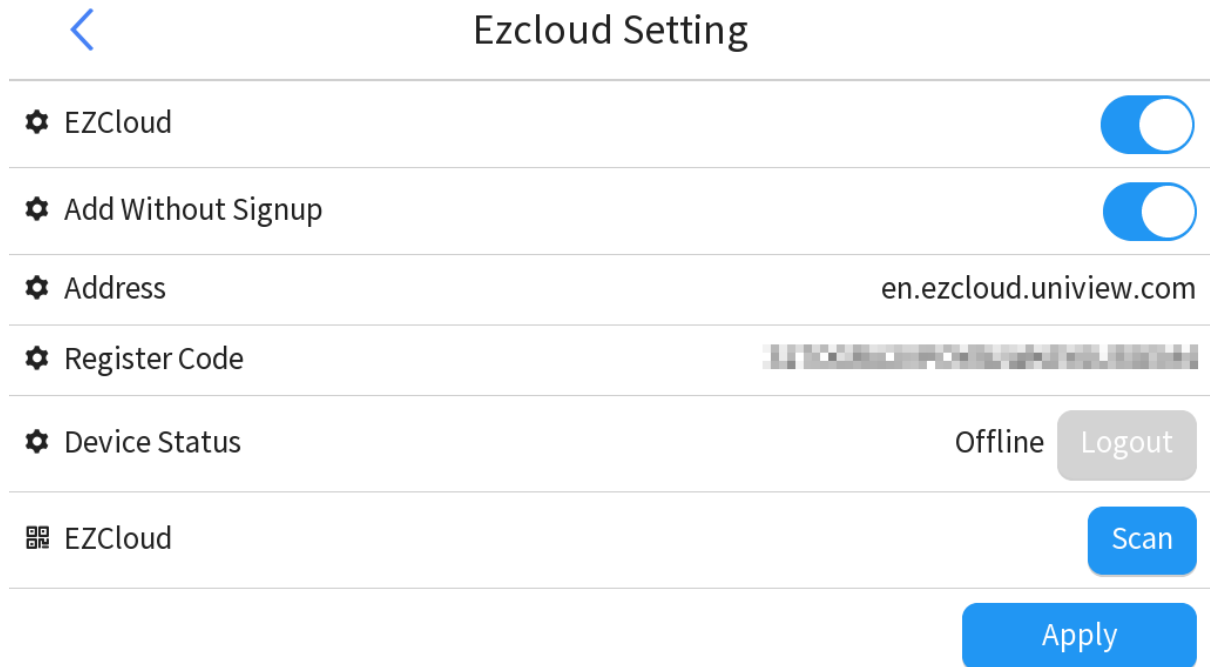
 **Note:** To restore all settings to factory defaults, enable **Restore factory defaults including network and user settings**.



- Storage: If a Micro SD card is inserted into the device, the screen will display the memory card capacity. To set storage parameters, please see [Storage](#).

 **Note:** Do not hot plug the Micro SD card, otherwise the device needs to restart according to on-screen prompts.


- Format: After a Micro SD card is inserted into the device, tap **Default** to format it.
- EZCloud Setting: Set EZCloud parameters and relate the device to EZCloud.

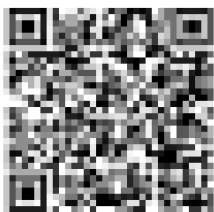
**Figure 9-37: EZCloud Setting**





1. Enable **EZCloud**.
2. (Optional) Enable **Add Without Signup**, and then you can log in to the app and relate the device to it without registering the account.
3. Tap . A success message means the settings are saved.
4. Tap , scan the QR code with the UNV-Link app, and follow the on-screen instructions to relate the device to the app.

**Figure 9-38: QR Code**

 Scan the QR code with the app



 **Note:** To view the QR code of the connected intelligent recognition terminal/door station, see [View Device QR Code](#).

If the device status is online, it indicates that the device is related successfully. To delete the device from cloud, tap .

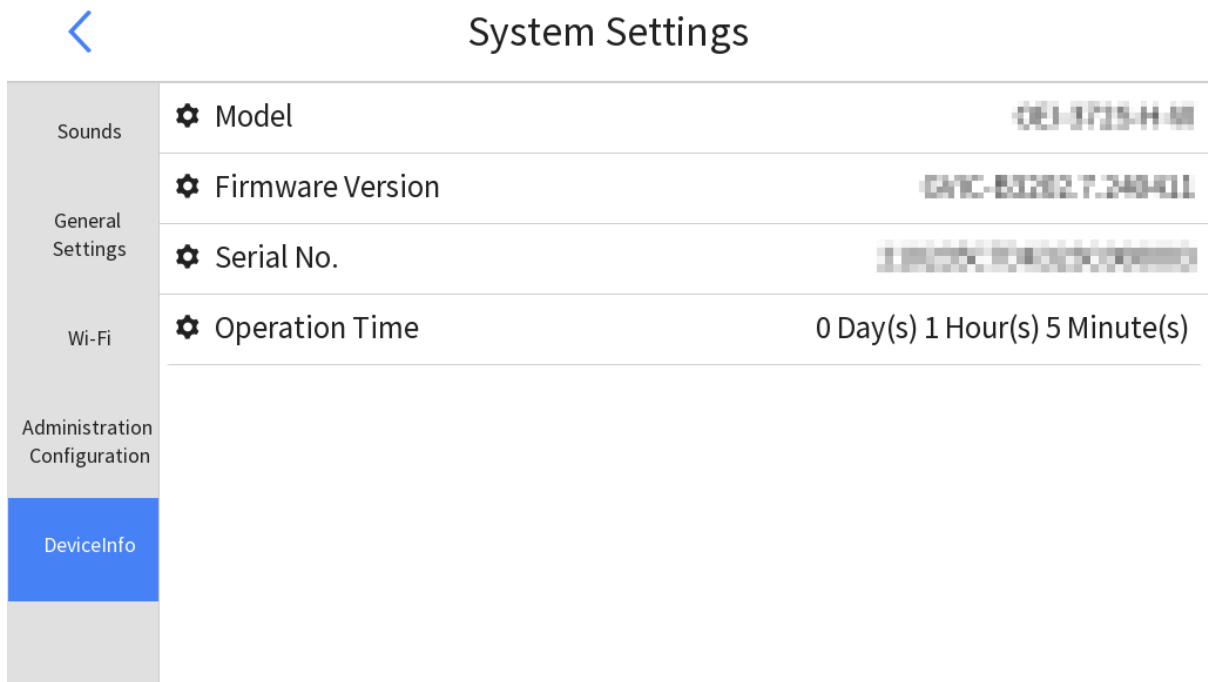
## 9.5 Device Info

Show the basic device information.




Go to  > DeviceInfo.

Figure 9-39: Device Info



## 10 Web Operations

This section mainly introduces how to use the indoor station and door station on the Web interface (hereinafter collectively referred to as "device").

 **Note:** This manual is suitable for various device models. The interface and function operations may vary with device models.

### 10.1 Login

#### Check Before Login

- The device runs normally.
- The client computer (hereinafter referred to as "client") is on the same network segment and the device is connected to the network.

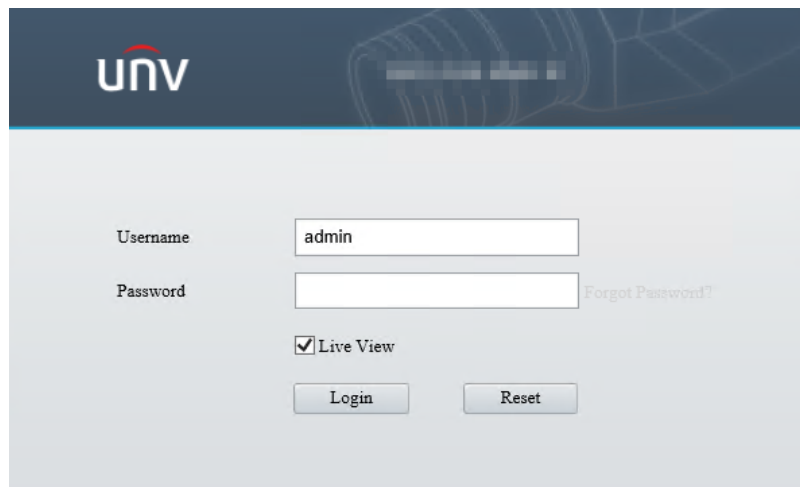
#### Log in to Web

1. Open a browser, enter the device's IP address (default: **192.168.1.13**) in the address bar, and press **Enter**.

**Figure 10-1: Indoor Station**




**Figure 10-2: Door Station**



2. At your first login, you need to follow the on-screen instructions to install the latest plug-in; otherwise, you cannot view the live video.

**Figure 10-3: Plug-in Installation Prompt**

 Please click here to [Download](#) and install the latest plug-in. Close your browser before installation.

3. Enter the username and password (**admin/123456** by default).
4. (Optional for door station) Select **Live View**, and then the live view will play automatically.
5. Click **Login**, and then the indoor station will enter the [Setup](#) interface, and the door station will enter the [Live View](#) interface.
6. After your first login to the Web interface, the **Privacy Policy** interface will appear. Please read the terms carefully and select **I have read and agree to the above policy** if no problem, and then click **OK**.
7. After the first login, the **Change Password** interface appears, in which you must set a strong password and enter your email address (it can receive a security code if you forgot the password, and can be changed in [User](#) later). Then, use the new password to log in again.

Indoor station / door station password: 9 to 32 characters, including digits, letters, and special characters.

**Figure 10-4: Indoor Station**

**Change Password**

Username

User Type

Old Password

Password

Weak Medium Strong

Confirm

Email

Used to reset password. You are recommended to fill in.

**Note:**Your password is weak. Please change your password and log in again (8 to 32 characters including at least two elements of the following three: digits, letters, and special characters).

OK

**Figure 10-5: Door Station**

**Change Password**

Username

User Type

Old Password

Password

Weak Medium Strong

Confirm

Email

Used to reset password. You are recommended to fill in.

**Select Permission**

Parameter...  Live View  Snapshot  Two-way A...  Event Subs...


Log  Maintenance  Upgrade

**Note:**Your password is weak. Please change your password and log in again (9 to 32 characters including all three elements: digits, letters, and special characters).

OK

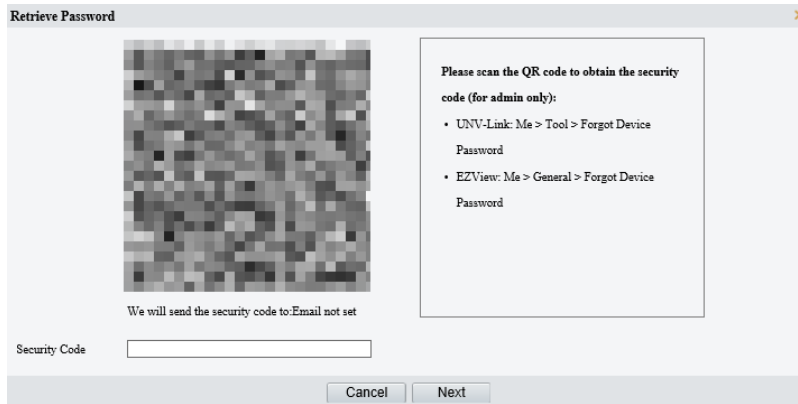
## Forgot Password

If you forgot your password, you can click **Forgot Password** and obtain a security code to reset the password.

 **Note:** To use this function, make sure an email address has been bound to the device, otherwise contact the local technical support to reset the password. The email can be set at the first login, or changed in [User](#).

1. Click **Forgot Password** on the login page, and then the **Retrieve Password** interface will appear.


**Figure 10-6: Retrieve Password**



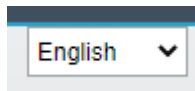
2. Obtain a security code according to the on-screen prompt.
3. Enter the security code, and click **Next** to retrieve the password. Please note this new password.

### Change Language

The default language is **English**. You can change the language to **Chinese Simplified** on the **Login** page, or on the **Maintenance** page after login.

 **Note:** This function is only available to the indoor station.

**Figure 10-7: Change Language**



## 10.2 Live View

Play live video and audio.

 **Note:**


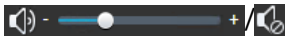






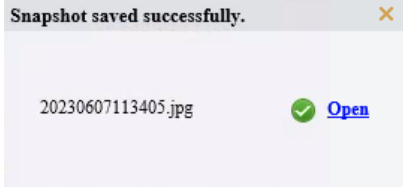

- This function is only available to the door station.
- To view the live video, complete the following operations:
  - Select **Live View** on the **Login** page.
  - Follow the on-screen instructions to install a plug-in and run it successfully.


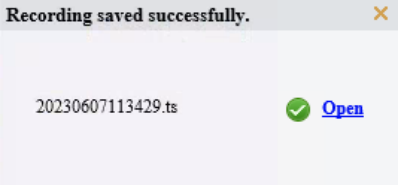





After login, the **Live View** page appears by default.

**Figure 10-8: Live View**




Double-click the live view window to play it in full screen, and double-click again or press **Esc** to exit full screen.

Parameter	Description
Proportional	<p>Set the image display ratio in the window.</p> <ul style="list-style-type: none"> <li>Scale: Displays 16:9 images.</li> <li>Stretch: Displays images according to the window size (stretch images to fit the window).</li> <li>Original: Displays images with original size.</li> </ul>
Main Stream/Sub Stream	Select a live video stream according to the device.
Image & General Parameters	<p>Set <b>General Parameters</b> on the right to improve the live video effect.</p> <p>To view detailed parameters information or set more image parameters, click <b>Image</b> in the upper-right corner to enter the <a href="#">Image</a> page.</p>
	Start/stop live view.
	<p>Turn off/on sound.</p> <p>Range: [0-100]. Default: 0. The greater the value, the higher the volume.</p> <p> <b>Note:</b> To set the output sound volume of the door station, please see <a href="#">Volume Control</a>.</p>
	<p>Adjust the microphone volume on the client during audio communication between the client and the device.</p> <p>Range: [0-100]. Default: 100. The greater the value, the higher the volume.</p>
	Show the current frame rate, network transmission rate, resolution, bit rate, and packet loss rate.
	<p>Enable/disable pixel calculation.</p> <p>When enabled, a default rectangular box of 400px in width and 200px in height will appear on the center of the live view page. Drag the four points of the box to adjust the detection area, and the pixel value appears in the upper-left corner.</p> 
	<p>Take a snapshot of the current live video.</p> <p>After a snapshot is complete, a pop-up window appears, including snapshot time and format. You can click <b>Open</b> to view the folder where the snapshot is saved.</p>  <p> <b>Note:</b> See <a href="#">Local Parameters</a> for the path of the saved snapshots.</p>

Parameter	Description
	<p>Start/stop local recording.</p> <p>After a recording is complete, a pop-up window appears, including recording name, and format. You can click <b>Open</b> to view the folder where the recording is saved.</p>  <p> <b>Note:</b> See <a href="#">Local Parameters</a> for the path of the saved recordings.</p>
	Start/stop two-way audio between the client and the door station.
	<p>Enable/disable digital zoom.</p> <p>When enabled, you can zoom in the live view with the following two ways, and right-click to restore to the original ratio.</p> <ul style="list-style-type: none"> <li>• Left click and hold on the live view window and drag your mouse to specify the area (rectangular area) to be magnified.</li> <li>• Slide the mouse wheel up to zoom in on the image.</li> </ul>
	<p>Enter full screen mode.</p> <p>To exit full screen mode, double-click in the live view window again or press <b>Esc</b>.</p>
	Show/hide general parameters in the right.

## 10.3 Person Library

Users in the person libraries can pass through the door with the set authentication mode in the set time.

 **Note:** This function is only available to the door station.

You can add, edit, delete, and search persons in a person library.

Enter the **Person Library** tab.

**Figure 10-9: Person Library**



The left list shows the person libraries, and the top of the list shows the total number of people in libraries.

### Add

- Add Person Library
  1. Click **Add** at the top of the left list.

**Figure 10-10: Add Person Library**


The screenshot shows a dialog box titled "Add Person Library". It contains the following fields and options:

- Person Library Type:** A dropdown menu with "Employee Library" selected.
- Person Library Name:** An empty text input field.
- Check Template:** A dropdown menu with "None" selected.
- Verify Success Linkage Configuration:** A section containing two checked checkboxes: "Open door" and "Voice Prompt".
- Verify Failure Linkage Configuration:** A section containing one checked checkbox: "Voice Prompt".
- Buttons:** "OK" and "Cancel" buttons at the bottom.


2. Choose a person library type.
    - **Employee Library:** Choose this option for long-term users, such as residents, and security personnel.
    - **Visitor Library:** Choose this option for temporary visitors.
  3. Enter a unique name for the library. 1 to 20 characters are allowed.
  4. Choose a check template. You need to configure it in [Check Template](#).
  5. Select the triggered actions after the authentication succeeds. **Open Door** and **Voice Prompt** are enabled by default.
  6. Select the triggered actions after the authentication fails. **Voice Prompt** is enabled by default.
  7. Click **OK** to save the settings.
- **Add Person Information:** You can add persons one by one or import in batches.
    - **Add One by One**
      1. Select the person library to which you want to add the person.
      2. Click **Add** on the right.

**Figure 10-11: Add Person Info**

3. Enter the person number (0 to 15 characters are allowed, including letters, digits, underscores, and hyphens), person name (1 to 63 characters), and comment (0 to 20 characters).
4. Set the card information.

 **Note:** Up to 4 cards can be set for each person.


- (1) Set the card type to **IC Card**.
- (2) Enter the card number. The card number can be typed manually or identified automatically by clicking **Collection**.

 **Note:** The collection function is available when a card reader is connected to the device.

5. Set a specific time period for the person. It is effective permanently by default. At the same time, the time template is grayed out and cannot be set.
  - (1) Select **default**.
  - (2) Set the effective and expiration time.
  - (3) Click **OK** to save the settings.

- Add in Batches: Click **Batch Import**, and import person information in batches based on the template.


## Edit

- Edit Person Library
  1. Select the person library you want to edit, and click **Edit**.
  2. You can edit parameters excluding the person library type.
  3. Click **OK** to save the settings.
- Edit Person
  1. Click  under the person you want to edit.
  2. Edit the person information as needed.





3. Click **OK** to save the settings.

## Delete

 **Note:** The default template cannot be deleted.

- Delete person library: Select the target person library on the left. Click **Delete**, and then click **OK** to delete it.

 **Note:** Deleting a person library will also delete its related all person information. Please handle with caution.

- Delete person information: Click the corresponding  under the person, or select multiple person information you want to delete and click **Delete**, and then click **OK** in the pop-up window.

## 10.4 Setup

### 10.4.1 Common

Configure commonly used functions including [Basic Info](#), [Local Parameters](#), [Wired Network](#), [Time](#), [Server](#), [OSD](#), and [User](#).





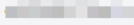



#### 10.4.1.1 Basic Info

##### 10.4.1.1.1 Basic Info





View the basic information and real-time operation status of the device, and quickly access certain common functions.

Go to **Setup > Common > Basic Info > Basic Info**.

**Figure 10-12: Indoor Station**

Basic Info		Common Configuration	
Model			Wired Network
IPv4 Network Info			Time
MAC Address			User
Firmware Version			
Hardware Version	A		
Boot Version	V1.0		
Serial No.			
Status			
System Time	2023/5/8 02:55:56		
Operation Time	0 Day(s) 0 Hour(s) 55 Minute(s)		
<input type="button" value="Refresh"/>			

**Figure 10-13: Door Station**

Basic Info		Common Configuration	
Model	h09824		Wired Network
IPv4 Network Info			Time
MAC Address			OSD
<b>Version Info</b>			User
Firmware Version			
Hardware Version	A		
Boot Version	V2.3		
Serial No.			
<b>Status</b>			
System Time	2023/6/7 03:30:36		
Operation Time	0 Day(s) 1 Hour(s) 29 Minute(s)		

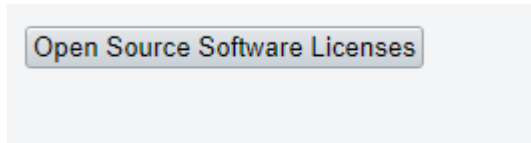
Common Configuration: Click the icon or text to quickly access the four common functions, including [Wired Network](#), [Time](#), [OSD](#), and [User](#).

### 10.4.1.1.2 About

View the open source software licenses.

1. Go to **Setup > Common > Basic Info > About**.


**Figure 10-14: About**



2. Click **Open Source Software Licenses** to view the details.

### 10.4.1.2 Local Parameters

Set local parameters for the device, including video, recording and snapshot.

 **Note:** This function is only available to the door station.

1. Go to **Setup > Common > Local Parameters**.

Figure 10-15: Local Parameters

**Video**

Display Mode Balanced ▼

Protocol TCP ▼

**Recording and Snapshot**

Recording Subsection By Time ▼

Subsection Time (min) 30

When Storage Full  Overwrite Recording  Stop Recording

Total Capacity(GB) 10

Local Recording TS ▼

Files Folder C:\Users\108722\WebPlugin\_IPC\IPCNE Browse... Open

Save

2. Set the parameters as needed.

Parameter		Description
Video	Display Mode	Set the video display mode according to the network status including <b>Min. Delay</b> , <b>Balanced</b> (default), and <b>Fluent</b> (from low delay to high delay). You may also customize the display mode as needed.
	Protocol	<p>Set the protocol used to transmit media streams.</p> <ul style="list-style-type: none"> <li>• UDP (default): Supports one-to-one, one-to-many, many-to-many, and many-to-one communication methods. Data can be sent without establishing a logical connection, but the data security and integrity cannot be guaranteed.</li> <li>• TCP: Supports one-to-one communication only. Data can only be sent after a logical connection has been established between the receiver and the sender, with higher security and reliability than UDP.</li> </ul>
Recording and Snapshot	Recording	<p>Mode to store the recording.</p> <ul style="list-style-type: none"> <li>• Subsection By Time (default): Save recording files of the set subsection time.</li> <li>• Subsection By Size: Save recording files of the set subsection size.</li> </ul>
	Subsection Time (min)/ Subsection Size (MB)	<ul style="list-style-type: none"> <li>• Subsection Time (min): Available when <b>Subsection By Time</b> is selected. Range: [1-60], default: 30.</li> <li>• Subsection Size (MB): Available when <b>Subsection By Size</b> is selected. Range: [10-1024], default: 100.</li> </ul>
	When Storage Full	<ul style="list-style-type: none"> <li>• Overwrite Recording (default): When the local recording capacity is full, the oldest recordings are overwritten automatically.</li> <li>• Stop Recording: When the local recording capacity is full, recording stops automatically.</li> </ul>
	Total Capacity (GB)	<p>Allocate storage capacity for local recording.</p> <p>Range: [1-1024], default: 10. The greater the value, the more the allocated recording storage capacity.</p>

Parameter		Description
	Local Recording	Set the file format for saving local recordings, including TS and MP4. The default format is TS.
	Files Folder	Set the location where snapshots and recordings are saved.

3. Click **Save**.

### 10.4.1.3 Wired Network

Configure network communication parameters for the device so it can communicate with other devices.

For network settings on the screen, see [Network Settings](#).

1. Go to **Setup > Common > Wired Network**.

**Figure 10-16: Wired Network**

2. Configure wired network parameters.

Parameter		Description
IPv4	Obtain IP Address	<ul style="list-style-type: none"> <li>Static: Configure a static public network IP address for the device manually. Set <b>Obtain IP Address</b> to <b>Static</b>, and enter the IP address, subnet mask, and default gateway.</li> <li>DHCP (default): If a DHCP (Dynamic Host Configuration Protocol) server is deployed in the network, the device can automatically obtain an IP address from the DHCP server.</li> <li>Configure PPPoE (Point to Point Protocol over Ethernet) to assign the device a dynamic IP address to establish network connection. Set <b>Obtain IP Address</b> to <b>PPPoE</b>, and enter the username and password provided by your ISP (Internet Service Provider).</li> </ul>
IPv6	Mode	<p>IPv6 has a lot more IP addresses than IPv4, and is faster and safer than IPv4 in terms of data transfer.</p> <p>The IPv6 mode includes <b>DHCP</b> and <b>Manual</b>. The default mode is <b>DHCP</b>.</p>


Parameter		Description
	MTU	<p>Maximum transmission unit, the maximum packet size supported by the device in bytes.</p> <p>IPv4 Range: [576-1500], integer only. Default: 1500.</p> <p>IPv6 Range: [1280-1500], integer only. Default: 1500.</p> <p>The greater the value, the higher the communication efficiency, the higher the transmission delay.</p>
Parameter	Operating Mode	<ul style="list-style-type: none"> <li>• Rate + Half Duplex: At the set rate, the port can only receive or send data at a given time, and there is a physical transmission distance limitation.</li> <li>• Rate + Full Duplex: At the set rate, the port can receive and send data at a given time, eliminating the physical transmission distance limitation of half duplex.</li> <li>• (Rate +) Auto-negotiation: The port automatically negotiates with the port of the peer end about the (speed and) operating mode, allowing both to run in the most efficient mode.</li> </ul>

3. Click **Save**.

## 10.4.1.4 Time

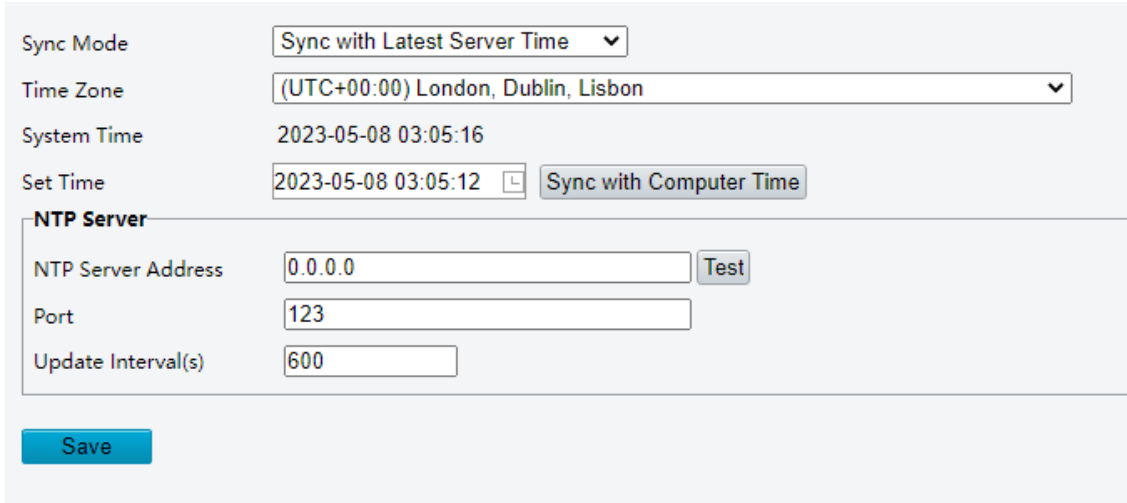
### 10.4.1.4.1 Time

Set the device time.

 **Note:** For time settings on the screen, see [Time](#).


1. Go to **Setup > Common > Time > Time**.

**Figure 10-17: Time**



2. You can set the device time manually or sync it with a server.

- Set manually: Click in the **Set Time** text box and set the time as needed.

 **Note:** When setting the system time manually, you need to set **Sync Mode** to **Sync with Latest Server Time**; otherwise, the device will still sync with other time sources after you set it manually.

- Sync time automatically:

(1) Select the sync mode.

Parameter	Description
Sync with System Configuration	The device uses the time provided by its built-in time module.

Parameter	Description
Sync with NTP Server	<p>NTP Server: A server used to sync time with the distributed server and client via NTP protocol.</p> <p>To sync the server time, you need to configure the NTP server address, port, and update interval.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p><b>NTP Server</b></p> <p>NTP Server Address <input type="text" value="0.0.0.0"/> <input type="button" value="Test"/></p> <p>Port <input type="text" value="123"/></p> <p>Update Interval(s) <input type="text" value="600"/></p> </div> <ul style="list-style-type: none"> <li>• NTP Server Address: Enter the NTP server address and click <b>Test</b> to check the network communication. A success message will appear if the NTP is verified successfully.</li> <li>• Port: Range: [1-65535], integer only, default: 123.</li> <li>• Update Interval (s): Range: [30-86400], integer only, default: 600.</li> </ul>
Sync with ONVIF Access Time	The device regularly syncs time with the management server connected via Onvif.
Sync with Latest Server Time	Default. The device regularly syncs time with all the connected servers.
Sync with Cloud Server	The device regularly syncs time with <a href="#">EZCloud</a> .

(2) Set the time zone as needed. The default time zone is (UTC+00:00) London, Dublin, Lisbon.


(3) Click **Sync with Computer Time**, and then the device time will be synced based on the set sync mode.

3. Click **Save**.

#### 10.4.1.4.2 DST

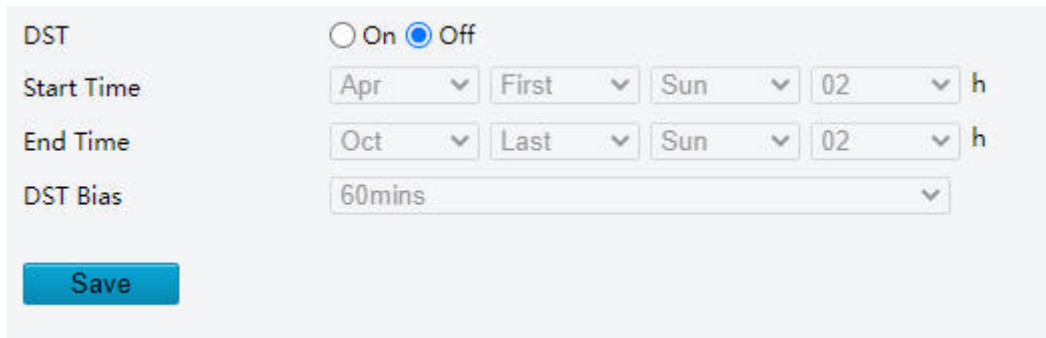
DST (Daylight Saving Time) is a local time system designed to make full use of daytime to save energy, which sets clocks forward by one hour in summer months.

By default, this function is disabled.

 **Note:** DST rules vary in different countries.

1. Go to **Setup > Common > Time > DST**.

**Figure 10-18: DST**



2. Enable **DST**.

3. Set the start time, end time, and DST bias.

4. Click **Save**.

#### 10.4.1.5 Server

You can add the device to EZCloud via the EZCloud website to remotely access the device and view the live video.

1. Go to **Setup > Common > Platform Access**.

**Figure 10-19: Platform Access**

2. Enable **EZCloud**.
3. (Optional) Enable **Add Without Signup**, and you can relate the device to EZCloud without registering the account.
4. Click **Save**. A success message means the settings are saved.
5. Scan the QR code with the UNV-Link app, and follow the on-screen instruction to relate the device to the app.

If the device status is online, it indicates that the device is related successfully. To delete the device from cloud, click **Logout**.

### 10.4.1.6 OSD

On Screen Display (OSD) are characters overlaid on **Live View**, including date, time, etc.

**Note:**

- This function is only available to the door station.
- Up to 8 OSDs are allowed.

1. Go to **Setup > Common > OSD**.

**Figure 10-20: OSD**

Enable	No.	Overlay OSD Content	X-Axis	Y-Axis
<input checked="" type="checkbox"/>	1	<Date & Time>	2	3
<input type="checkbox"/>	2		75	3
<input type="checkbox"/>	3		2	75
<input type="checkbox"/>	4		0	0
<input type="checkbox"/>	5		0	0
<input type="checkbox"/>	6		0	0
<input type="checkbox"/>	7		0	0
<input type="checkbox"/>	8		0	0

**Display Style**

Effect: Background

Font Size: Medium

Font Color: #ffffff

Min. Margin: None

Date Format: dd/MM/yyyy

Time Format: HH:mm:ss

dd=Day; dddd=Day of the week; M=Month; y=Year

h/H=12/24 Hour; tt=A.M. or P.M.; mm=Minute; ss=Second

2. To enable an OSD, select the check box in the **Enable** column, and then the OSD area will be displayed on the live video (OSD name format: area + OSD number, for example, area 1).
3. Set the OSD content you want to overlay.
  - Custom: 0 to 40 characters are allowed.

- Date & Time/Time/Date: Overlay the current date & time, time or date.
- Scroll OSD: The OSD text appears on the live video and scrolls from right to left.

Enter the text information you want to overlay. Up to 200 characters are allowed, and it will be only displayed in the area with the smallest number.

**Figure 10-21: ScrollOSD**

- Picture Overlay: Overlay the imported picture.

You can set the picture transparency as needed (an integer from 1 to 100 is allowed; the greater the value, the higher the transparency effect). Then, you can upload a picture with 24 or 32 bit depth, **.bmp** or **.png** format, and size of no more than 64K.

**Figure 10-22: Picture Overlay**

4. Specify the exact position of the OSD by entering the X and Y coordinates. Take the top left corner of the image as the origin coordinates (0, 0), the horizontal axis is the X-axis, and the vertical axis is the Y-axis.
5. Set the OSD display style as needed.
  - Effect: **Background** by default.
  - Font Size/Font Color: **Medium**, **#ffffff** by default.
  - Date Format/Time Format: **dd/MM/yyyy**, **HH:mm:ss** by default.
  - Min.Margin: The distance between the OSD area and the coordinate. Default: **None**.

### 10.4.1.7 User

Users are entities that manage and operate the device. A user type is a set of operation permissions. After a user type is assigned to a user, the user has all the permissions defined in the type.

The user types are described below.

- Admin: The default super administrator, which has all permissions for managing the device. Only 1 admin user is allowed. The admin cannot be added or deleted.
- Operator: It is created and configured by admin, with lower permission than admin.
- Common User: It is created and configured by admin, with lower permission than operator.

 **Note:** Only the door station involves **Operator** and **Common User**.

Go to **Setup > Common > User**.



**Figure 10-23: User**

No.	Username	User Type
1	admin	Admin
2	vic	Common User

### Add User

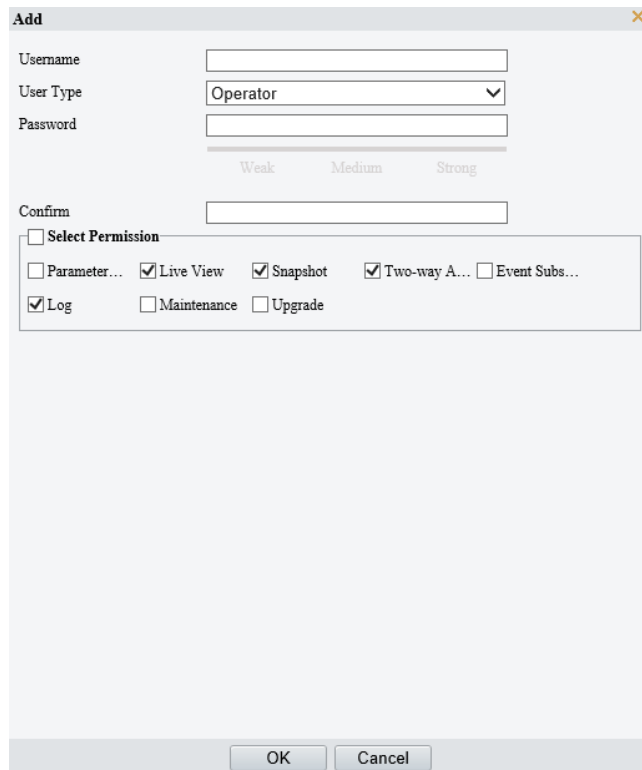


**Note:**

- Only the door station can add users.
- Up to 31 users are allowed, including operator and common user.

1. Click **Add**.

**Figure 10-24: Add Operator**



The 'Add Operator' dialog box contains the following fields and options:

- Username:** Text input field.
- User Type:** Dropdown menu with 'Operator' selected.
- Password:** Text input field with a strength indicator below it showing 'Weak', 'Medium', and 'Strong'.
- Confirm:** Text input field.
- Select Permission:** A group box containing several checkboxes:
  - Parameter...
  - Live View
  - Snapshot
  - Two-way A...
  - Event Subs...
  - Log
  - Maintenance
  - Upgrade

Buttons: OK, Cancel

**Figure 10-25: Add Common User**

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. It contains the following elements:

- Username:** A text input field.
- User Type:** A dropdown menu currently showing "Common User".
- Password:** A text input field with a strength indicator below it showing "Weak", "Medium", and "Strong" options.
- Confirm:** A text input field.
- Select Permission:** A checkbox that is currently unchecked.
- Live View:** A checkbox that is currently checked.
- Buttons:** "OK" and "Cancel" buttons at the bottom.

2. Enter the username. 1 to 32 characters are allowed, including letters(A-Z, a-z), digits(0-9), underscores(\_), hyphens(-), dots(.), and plus signs(+).
3. Choose a user type, including **Operator** or **Common User**.
4. Enter the password with 9 to 32 characters, including digits, letters and special characters.
5. Select permissions you want to assign to the new user.

 **Note:** You can select the **Select Permission** check box to select/deselect all permissions.

6. Click **Save**.

### Delete User

 **Note:**

- The admin and vic users cannot be deleted.
- Only the door station can delete users.

1. Select the user you want to delete, and click **Delete**.
2. Click **OK** to confirm the deletion.

### Edit User

Admin can change the device password and email. Common user and operator can change the device password and allocate the permission.

 **Note:**

- To edit a user, you need to enter the admin password.
- To change the email or permission, you need to reset the admin password, otherwise the configuration will not be saved successfully. After changing the password, the **Login** interface will appear, and you can log in with the new password.

1. Select the user you want to edit, and click **Edit**.
2. Enter the admin password, new password and then confirm it by entering again.
3. Change the email or permissions.
4. Click **OK**.

## Set Registration Password

The registration password of the related device must be consistent with that of the indoor station in the same network segment, so the live view and video intercom functions can be used for networking security.

The password of the vic user is the registration password. Default: 12345678.

You can set the registration password on the local interface. See [Registration Password](#) for details.

1. Select the vic user, and click **Edit**.

**Figure 10-26: Set Registration Password**

The screenshot shows a dialog box titled "Edit" with a close button (X) in the top right corner. It contains the following fields and options:


- Username:** A text input field containing "vic".
- User Type:** A dropdown menu showing "Common User".
- Admin Password:** An empty text input field.
- Password:** An empty text input field. Below it are three indicators: "Weak", "Medium", and "Strong".
- Confirm:** An empty text input field.
- Select Permission:** A section with a checkbox "Select Permission" (unchecked) and a sub-section containing a checked checkbox "Live View".
- Buttons:** "OK" and "Cancel" buttons at the bottom.

2. Enter the admin password and registration password (9 to 32 characters including digits, letters, and special characters), and enter the registration password again to confirm.
3. Click **OK**.

### 10.4.1.8 Personalization

When **Auto Answer** is enabled on the indoor station, the door station will play the custom audio when its call is rejected by the indoor station.

1. Go to **Setup > Common > Personalization**.
2. Click **Browse...**, and select a custom auto answer audio for the first use.

 **Note:** The audio must be a PCM file with the file size of no more than 108KB and file name of no more than 32 characters.

**Figure 10-27: Custom Auto Answer Audio**


The screenshot shows the "Custom Auto Answer Audio" interface. It includes the following elements:

- Alarm Audio File:** A text input field with "Browse..." and "Import" buttons to its right.
- Note:** "The audio file must be a PCM file with no more than 108KB."
- Table:** A table with three columns: "No.", "Audio", and "Operation".

No.	Audio	Operation
1	CollectSuccess.pcm	

3. Click **Import**, and then the custom audio will be displayed in the audio list.

Only one audio is allowed.

To cancel the custom audio, tap , and then the audio will restore to the default ("The user you are calling is unavailable.").

To change the audio, follow the steps above, and the new audio will automatically overwrite the previous one.

## 10.4.2 Network

### 10.4.2.1 Basic Config

Configure network parameters for the device to communication with other devices.

#### 10.4.2.1.1 Wired Network

See [Wired Network](#) for details.

#### 10.4.2.1.2 Wi-Fi

Configure Wi-Fi for the device to connect to the network, and then the call, live view, and other functions can be used normally.

For Wi-Fi configuration on the screen, see [Wi-Fi](#).

Go to **Setup > Network > Basic Config > Wi-Fi**.

**Figure 10-28: Wi-Fi**

Wi-Fi Mode: Off

Save

### Connect Wi-Fi

**Note:** After the Wi-Fi is connected, the network response will be sluggish. Please be patient.

1. Set **Wi-Fi Mode** to **Wi-Fi**. You can view the current Wi-Fi network status, the list of available Wi-Fi networks, and detailed Wi-Fi information.

**Figure 10-29: Wi-Fi**

Wi-Fi Mode: Wi-Fi

**Network Status**

Current Status	Disconnected
SSID	None
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
MAC Address	
Strength	...

**Wi-Fi Network**

Search

SSID	Channel	MAC Address	Authentication	Encryption	Strength	Strength(dBm)
[blurred]	6	[blurred]	WPA-PSK WPA2-PSK	CCMP	[signal]	-64
[blurred]	11	[blurred]	WPA-PSK WPA2-PSK	CCMP	[signal]	-64
[blurred]	11	[blurred]	WPA-PSK WPA2-PSK	CCMP-TKIP	[signal]	-69
[blurred]	1	[blurred]	WPA-PSK WPA2-PSK	CCMP	[signal]	-70
[blurred]	1	[blurred]	WPA-PSK WPA2-PSK	CCMP-TKIP	[signal]	-72
[blurred]	6	[blurred]	WPA-PSK WPA2-PSK	TKIP	[signal]	-76
[blurred]	12	[blurred]	WPA-PSK WPA2-PSK	CCMP-TKIP	[signal]	-76

**Wi-Fi**

SSID: [input field]

Authentication: [dropdown menu]

2. Click **Search** on the **Wi-Fi Network** tab to search for available Wi-Fi networks.
3. Select the Wi-Fi you want to connect from the list.

**Figure 10-30: Select Wi-Fi**

SSID	Channel	MAC Address	Authentication	Encryption	Strength	Strength(dBm)
thd2	11	[blurred]	WPA-PSK WPA2-PSK	CCMP	[signal icon]	-50
[blurred]	1	[blurred]	WPA-PSK WPA2-PSK	CCMP	[signal icon]	-54
[blurred]	6	[blurred]	WPA-PSK WPA2-PSK	CCMP	[signal icon]	-55
[blurred]	6	[blurred]	WPA-PSK WPA2-PSK	TKIP	[signal icon]	-56
[blurred]	6	[blurred]	WPA-PSK WPA2-PSK	TKIP	[signal icon]	-56
[blurred]	11	[blurred]	WPA-PSK WPA2-PSK	CCMP	[signal icon]	-56
[blurred]	2	[blurred]	WPA-PSK WPA2-PSK	CCMP	[signal icon]	-58

4. Enter the Wi-Fi password and confirm the password.

**Figure 10-31: Enter Password**

**Wi-Fi**

SSID:

Authentication:

Password:

Confirm:

Encryption:

Obtain IP Address:

MTU:

5. Click **Save**. Wait about 3 seconds, and then the **Network Status** tab displays the current network status of connected Wi-Fi.

**Figure 10-32: Connected Wi-Fi**

Network Status	
Current Status	Connected
SSID	thd2
IP Address	[blurred]
Subnet Mask	[blurred]
Default Gateway	[blurred]
MAC Address	[blurred]
Strength	[signal icon]

## Enable Wi-Fi Hotspot

The device can function as a Wi-Fi hotspot for other devices.

**Note:** This function is only available to the indoor station.

1. Set **Wi-Fi Mode** to **Wi-Fi Hotspot**.

**Figure 10-33: Enable Wi-Fi Hotspot**

Wi-Fi Mode

**Hotspot Settings**

SSID

Password

Confirm

Channel

Gateway Address

2. (Optional) Set the SSID, a name for the Wi-Fi hotspot. 1 to 32 characters are allowed, including uppercase and lowercase letters, digits, underscores, and hyphens.
3. Set a password for the Wi-Fi hotspot. 8 to 32 characters are allowed, including uppercase and lowercase letters, digits, and special characters.
4. Click **Save**.

### Disable Wi-Fi/Wi-Fi Hotspot

1. Set **Wi-Fi Mode** to **Off**.

**Figure 10-34: Off**

Wi-Fi Mode

2. Click **Save**.

#### 10.4.2.1.3 DNS

DNS (Domain Name System) is a globally distributed service that translates human readable domain names into numeric IP addresses, facilitating devices to access external servers or hosts through domain names.

1. Go to **Setup > Network > Basic Config > DNS**.

**Figure 10-35: DNS**


Preferred DNS Server

Alternate DNS Server

2. Enter the DNS server address.
3. Click **Save**.

#### 10.4.2.1.4 DDNS

DDNS (Dynamic Domain Name Server) can map the dynamic IP address of the device to a fixed domain name, which is designed to help other devices on the public network access the network with the fixed domain name. With DDNS, users can access the private network device for remote control with the public IP address.

 **Note:** This function is only available to the door station.

1. Go to **Setup > Network > Basic Config > DDNS**.

**Figure 10-36: DDNS**

DDNS Service  On  Off

DDNS Type

Server Address

Domain Name

Username

Password

Confirm

**Save**

2. Enable **DDNS Service**.
3. Set DDNS parameters.
  - DynDNS/No-IP: Enter the domain name, username, and password, and confirm the password.
    - Domain name: Domain name assigned by your DDNS service provider, for example, www.dyndns.com.
    - Username and password: The corresponding username/password for your DDNS account, for example, www.dyndns.com.
  - EZDDNS: Custom a domain name for your device. 4 to 63 characters are allowed, including letters, digits, underscores, and hyphens. Click **Test** to check if the domain name is available.
4. Click **Save**.

#### 10.4.2.1.5 Port

Set the port to access the device via network.

1. Go to **Setup > Network > Basic Config > Port**.

**Figure 10-37: Port**

HTTP Port

HTTPS Port

RTSP Port


**Note:** Modifying the RTSP port number will cause the device to restart.

**Save**

2. You can use the defaults or customize them in case of port conflicts.
  - 📌 **Note:** If the HTTP port number you entered has been used, a message "Port conflicts. Please try again." will appear. 23, 81, 82, 85, 3260, and 49152 have been assigned for other purposes and cannot be used. In addition to the above port numbers, the system can also dynamically detect other port numbers that are already in use.
    - HTTP/HTTPS Port: If you change the HTTP/HTTPS port number, then you need to add the new port number after the IP address when logging in. For example, if the HTTP port number is set to 88, you need to use http://192.168.1.13:88 to log in to the device.
    - RTSP Port: Real-Time Streaming Protocol port. You can enter an available port number.
3. Click **Save**.

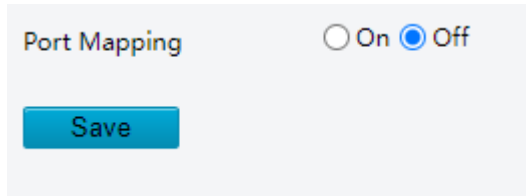
#### 10.4.2.1.6 Port Mapping

Configure port mapping so computers on the WAN can access the device on the LAN.

 **Note:** By default, this function is disabled.

1. Go to **Setup > Network > Basic Config > Port Mapping**.

**Figure 10-38: Port Mapping**

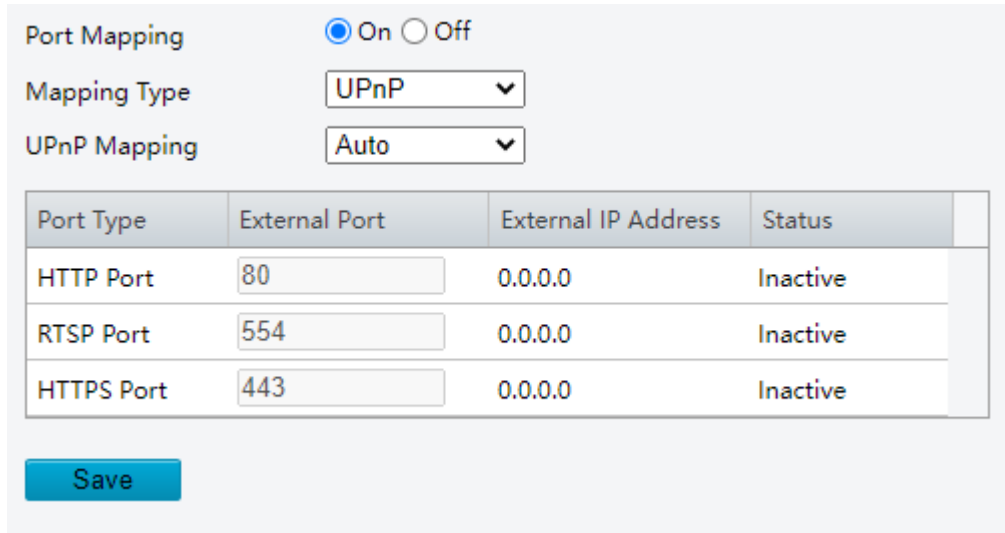


Port Mapping  On  Off

Save

2. Enable **Port Mapping**.

**Figure 10-39: Enable Port Mapping**



Port Mapping  On  Off

Mapping Type

UPnP Mapping


Port Type	External Port	External IP Address	Status
HTTP Port	<input type="text" value="80"/>	0.0.0.0	Inactive
RTSP Port	<input type="text" value="554"/>	0.0.0.0	Inactive
HTTPS Port	<input type="text" value="443"/>	0.0.0.0	Inactive

Save

3. Choose a mode from the UPnP list, including **Automatic** (default) and **Manual**.
  - Automatic: The external port numbers and IP address are assigned automatically.
  - Manual: The external port numbers need to be set manually.
4. Click **Save**.

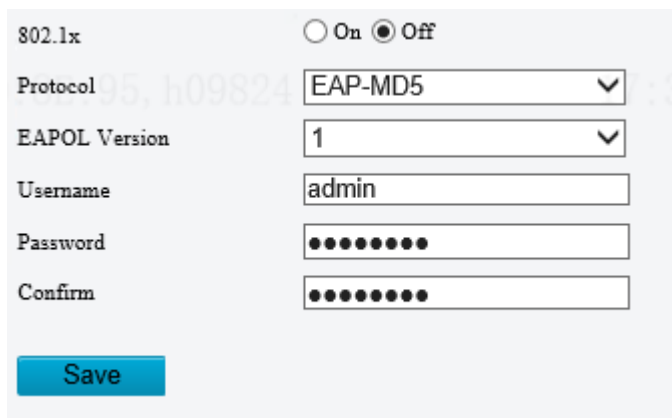
#### 10.4.2.1.7 802.1x

The 802.1x protocol is an access control protocol for a device to access the network. In situations with high security requirements, 802.1x authentication is necessary when the device is connected to the network. Only successfully authenticated devices are allowed to access the LAN, so as to ensure network security and realize normal communication.

 **Note:** This function is only available to the door station.

1. Go to **Setup > Network > Basic Config > 802.1x**

**Figure 10-40: 802.1x**



802.1x  On  Off

Protocol

EAPOL Version

Username

Password

Confirm

Save


2. Enable **802.1x**.



3. Select the EAPOL version (Extensible Authentication Protocol over LAN) as needed.
4. Enter the device username and password, and then confirm the password
5. Click **Save**.

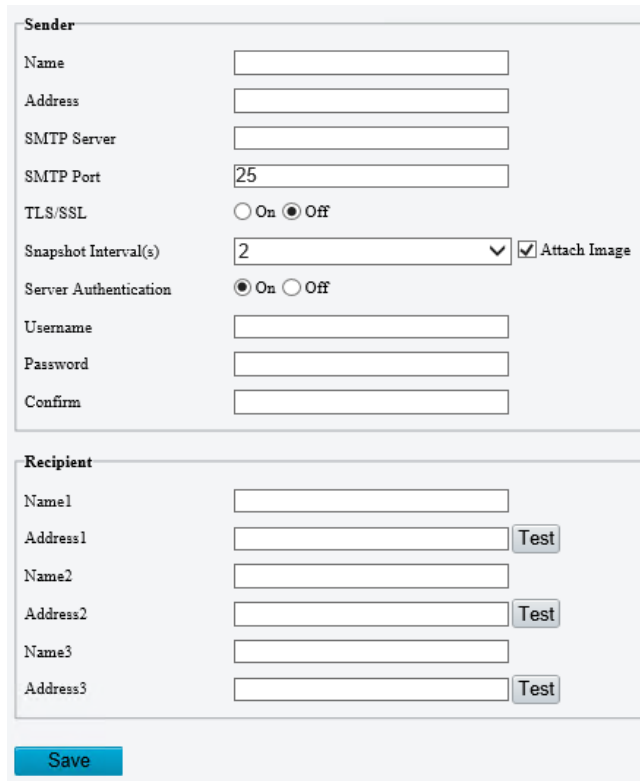
## 10.4.2.2 Service Config

### 10.4.2.2.1 E-mail


 **Note:** This function is only available to the door station.

1. Go to **Setup > Network > Service Config > E-mail**.

**Figure 10-41: E-mail**



2. Set the sender information.
  - Name/Address: The door station's name and address.
  - SMTP Server/SMTP Port: The IP address and port number of the sender's SMTP server. Taking Gmail and QQ mailbox as examples, the SMTP server address can be obtained from the help center. The default SMTP port number is 25.
  - TLS/SSL: Enable **TLS/SSL**, and then emails will be encrypted by TLS or SSL to secure data security and integrity.
  - Attach Image: When enabled, the device will automatically send an alarm e-mail with 3 attached snapshots taken at set intervals in the event of an alarm. It is enabled by default.
  - Snapshot Interval(s): Set the interval for taking snapshots to be attached to alarm e-mails. Default: 2s.
  - Server Authentication: Enable SMTP server authentication to secure e-mail transmission.
  - Username/Password: Enter the username and password of the SMTP server.

 **Note:** The email only shows the sender name. Username will not be displayed.

3. Set the recipient names and email addresses.
4. Click **Save**.

### 10.4.2.2.2 QoS

QoS (Quality of Service) can alleviate network delay and network congestion by providing high-priority communication services.

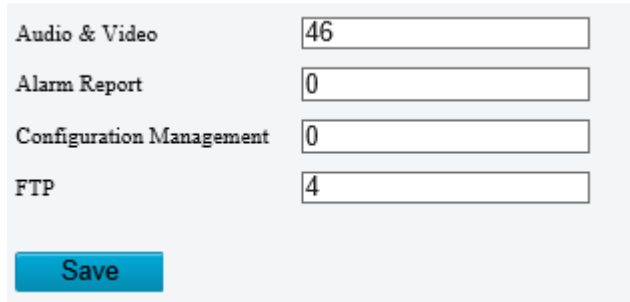
 **Note:**

- This function is only available to the door station.
- To use QoS, the same QoS rules must also be configured on the router or network switch.

At present, QoS allows you to assign different priority to audio and video, alarm report, configuration management, and FTP transmission.

1. Go to **Setup > Network > Service Config > QoS**.

**Figure 10-42: QoS**




Audio & Video	<input type="text" value="46"/>
Alarm Report	<input type="text" value="0"/>
Configuration Management	<input type="text" value="0"/>
FTP	<input type="text" value="4"/>

2. Set a priority level for each service. Range: [0-63]. The greater the value, the higher the priority.  
For example, when the audio & video is set to 60, and alarm report, configuration management and FTP are set to 0, the device first ensures smooth audio and video in the case of network congestion.
3. Click **Save**.

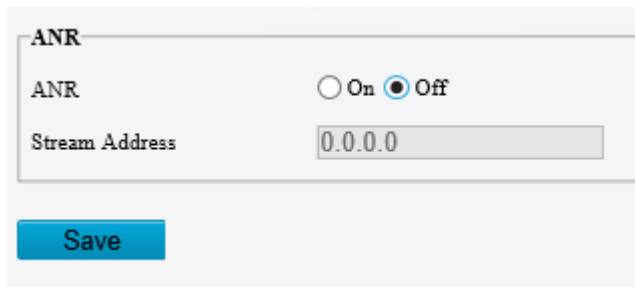
### 10.4.2.2.3 ANR(ONVIF)

If the network connection between the device and the peer (stream receiving address) is disconnected, the device can store videos according to the configured recording schedule; and after the network connection is restored, the device can retransfer the video stored during the interruption period to the stream receiving address on the request of the peer.

 **Note:** This function is only available to the door station.

1. Go to **Setup > Network > Service Config > ONVIF**.

**Figure 10-43: ONVIF**



ANR

ANR  On  Off

Stream Address

2. Enable **ANR**.
3. Set the stream address.
4. Click **Save**.

### 10.4.2.3 Server

See [Server](#) for details.

## 10.4.3 Image

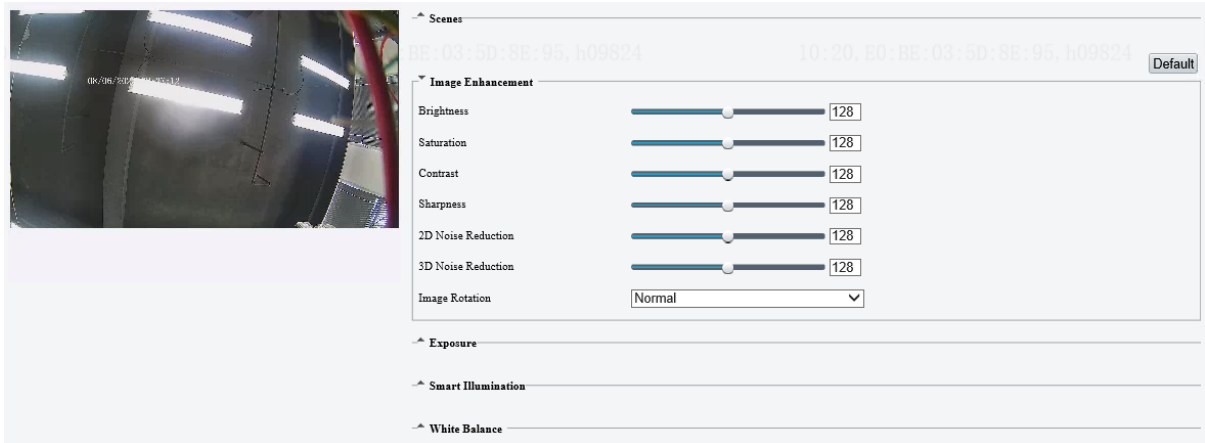
### 10.4.3.1 Image

#### 10.4.3.1.1 Image

Set image parameters include scenes, image enhancement, exposure, etc.

1. Go to **Setup > Image > Image**. Double-click the image on the left to play it in full screen, and double-click again or press **Esc** to exit full screen.

**Figure 10-44: Image**



2. Set the image scenes.

There are 4 preset scenes for the door station, and the image parameters of each scene are different. After a scene mode is selected, image parameters are automatically switched.

You can adjust the scene parameters as needed.

Up to 5 scenes are allowed (include custom scene).






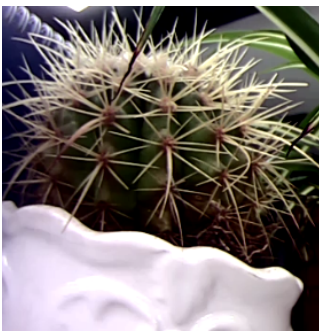


**Figure 10-45: Scene**











- (1) Select the scene you want to use.
  - (2) Select the scene mode.
    - Common: Recommended for outdoor scenes.
    - Indoor: Recommended for indoor scenes.
    - Test: Recommended for test scenes.
    - Custom: Set a scene as needed.
  - (3) Set the image scene name, which will be used in [Image Scene Switch](#).
3. Set the image enhancement, exposure, smart illumination, and white balance parameters in turn.


**Note:**

- Image enhancement parameters range: [0-225]. Default: 128.
- To restore default settings under all the tabs, click **Default** in the upper right corner.

Parameter	Description	
Image Enhancement	Brightness	<p data-bbox="762 146 1267 176">The overall lightness or darkness of the image.</p> <div style="display: flex; justify-content: space-around;">   </div> <div style="display: flex; justify-content: space-around; margin-top: 5px;"> <span data-bbox="735 545 900 575">Low brightness</span> <span data-bbox="1158 545 1329 575">High brightness</span> </div>
	Saturation	<p data-bbox="751 599 1275 629">The intensity or vividness of colors in the image.</p> <div style="display: flex; justify-content: space-around;">   </div> <div style="display: flex; justify-content: space-around; margin-top: 5px;"> <span data-bbox="735 998 900 1028">Low saturation</span> <span data-bbox="1158 998 1329 1028">High saturation</span> </div>
	Contrast	<p data-bbox="775 1052 1251 1108">The black-to-white ratio in the image, that is, the gradient of color from black to white.</p> <div style="display: flex; justify-content: space-around;">   </div> <div style="display: flex; justify-content: space-around; margin-top: 5px;"> <span data-bbox="743 1483 884 1513">Low contrast</span> <span data-bbox="1169 1483 1318 1513">High contrast</span> </div>
	Sharpness	<p data-bbox="815 1539 1211 1569">The definition of edges in the image.</p> <div style="display: flex; justify-content: space-around;">   </div> <div style="display: flex; justify-content: space-around; margin-top: 5px;"> <span data-bbox="735 1946 900 1977">Low sharpness</span> <span data-bbox="1158 1946 1329 1977">High sharpness</span> </div>

Parameter		Description
	2D Noise Reduction	Reduce noise by individually analyzing each frame, which may cause image blur.
	3D Noise Reduction	Reduce noise by analyzing the difference between successive frames, which may cause image smearing or ghosting.
Exposure	Exposure Mode	<p>Select the exposure mode from the drop-down list to achieve the desired exposure effect.</p> <ul style="list-style-type: none"> <li>• Automatic: The door station automatically adjusts the exposure parameters based on the environment.</li> <li>• Custom: User can set exposure parameters as needed.</li> <li>• Shutter Priority: The device adjusts shutter as priority to adjust the image quality.</li> <li>• Indoor 50Hz/60Hz: Reduce stripes by limiting shutter frequency.</li> <li>• Manual: Fine-tune image quality by setting shutter and gain manually.</li> </ul>
	Shutter(s)	<p>Shutter is used to control the light that comes into the door station's lens. A fast shutter speed is ideal for scenes in quick motion. A slow shutter speed is ideal for scenes that change slowly.</p> <p> <b>Note:</b></p> <ul style="list-style-type: none"> <li>• This parameter is configurable when <b>Exposure Mode</b> is set to <b>Manual</b>. The minimum and maximum time can be configurable when <b>Exposure Mode</b> is set to <b>Custom</b>.</li> <li>• If <b>Slow Shutter</b> is disabled, the reciprocal of the shutter speed must be greater than the frame rate.</li> </ul>
	Gain	<p>Control image signals so that the device can output standard video signals in different light conditions.</p> <p> <b>Note:</b> This parameter is configurable when <b>Exposure Mode</b> is set to <b>Manual</b> or <b>Custom</b>. The minimum and maximum gain value can be configurable when <b>Exposure Mode</b> is set to <b>Custom</b>.</p>
	Slow Shutter	When enabled, the device can improve image brightness in low light conditions.
	Slowest Shutter	Set the slowest shutter speed for exposure.
	Compensation	<p>Adjust the compensation value as required to achieve the desired image effect.</p> <p>The valid range is -100 to 100. The default is 0.</p> <p> <b>Note:</b> This parameter is configurable when <b>Exposure Mode</b> is not set to <b>Manual</b>.</p>

Parameter		Description
	Metering Control	<p>Set how the door station measures the intensity of light.</p> <ul style="list-style-type: none"> <li>Center-Weighted Average Metering: Measure light mainly in the central part of the image.</li> <li>Evaluative Metering: The device measures light mainly in the central part of the image.</li> <li>Face Metering: The device adjusts the image quality in poor lighting or backlighting conditions by controlling the brightness of captured faces in face scenes.</li> <li>Smart Metering: The device obtains an accurate exposure by weighting according to the exposure and importance of each area on the whole image.</li> </ul> <p> <b>Note:</b> This parameter is configurable when <b>Exposure Mode</b> is not set to <b>Manual</b>.</p>
	Day/Night Mode	<ul style="list-style-type: none"> <li>Automatic: The device automatically switches between day mode and night mode according to the ambient lighting condition to output optimum images.</li> <li>Day: The device outputs high-quality images in daylight conditions.</li> <li>Night: The device outputs high-quality images in low-light conditions.</li> <li>Input Boolean: The device switches between day mode and night mode according to the Boolean value input from a connected third-party. If alarm type is set to <b>N.O.</b>, the device is on the day mode; if the alarm type is set to <b>N.C.</b>, the device is on the night mode.</li> </ul>
	Day/Night Sensitivity	<p>Light threshold for switching between day mode and night mode. A higher sensitivity value means that the device is more sensitive to the change of light and is therefore more easily to switch between day mode and night mode.</p> <p> <b>Note:</b> This parameter is configurable when <b>Night Mode</b> is not set to <b>Manual</b>.</p>
	Day/Night Switching(s)	<p>Set the length of time before the camera switches between day mode and night mode after the switching conditions are met.</p> <p> <b>Note:</b> This parameter is configurable when <b>Day/Night Mode</b> is set to <b>Automatic</b>.</p>
	WDR	<p>Enable WDR to ensure clear images in high contrast conditions.</p> <p> <b>Note:</b> This parameter is configurable when <b>Exposure Mode</b> is not set to <b>Manual</b>.</p>
	WDR Level	<p>When WDR is enabled, you can adjust the WDR level to improve image quality.</p> <p>The valid range is 1 to 9. The default is 5.</p> <p> <b>Note:</b> In the case of low contrast, it is recommended to disable WDR or use level 1 to 6. Level 7 or higher is recommended if there is a high contrast between the bright and dark areas in the scene.</p>
	WDR Open/Close Sensitivity	<p>When <b>WDR</b> is set to <b>Automatic</b>, adjust the parameter to change the WDR switching sensitivity.</p> <p>The valid range is 1 to 9. The default is 5.</p>
Smart Illumination	IlluminationMode	<p>Infrared: The device uses infrared light illumination.</p>

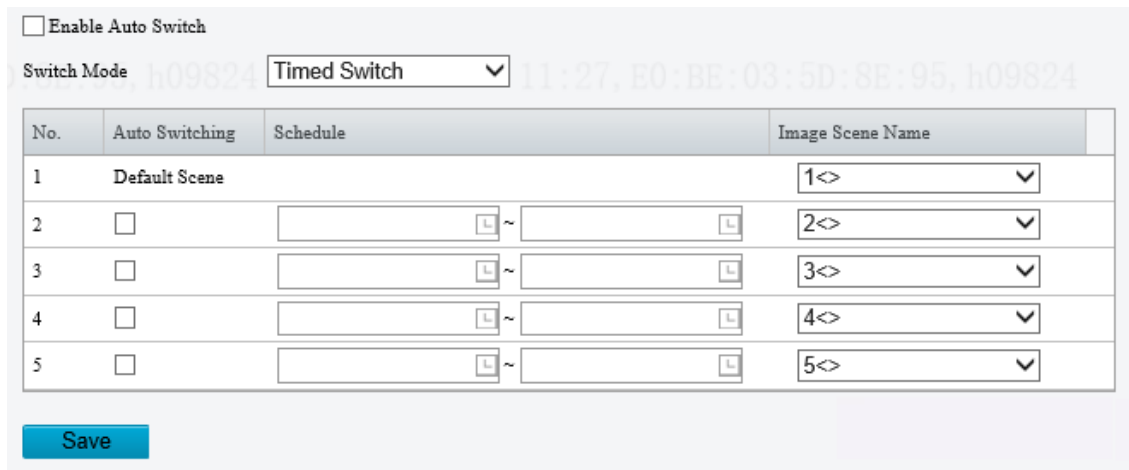
Parameter		Description
	Control Mode	(Available for 1-button door stations) Overexposure Restrain: The device automatically adjusts illumination brightness and exposure to avoid regional overexposure.  (Available for 2-button and 4-button door stations) Global Mode: The device automatically adjusts illumination and exposure to achieve the balanced image effect.
	Illumination Level	Default: 500. The greater the value, the higher the intensity.
White Balance	White Balance	<ul style="list-style-type: none"> <li>• Auto/Auto 2: Automatically adjust the red and blue gains according to the lighting conditions. If there are still color casts in <b>Auto</b> mode, try <b>Auto 2</b> mode.</li> <li>• Outdoor: Recommended for outdoor scenes where the color temperature varies widely.</li> <li>• Fine Tune: Allows user to manually adjust red and blue offsets.</li> <li>• Fine Tune (Base on night mode): Allows user to adjust red and blue offsets manually to adapt to poor lighting conditions.</li> <li>• Sodium Lamp: Automatically adjust the red and blue gains for optimal color reproduction in sodium light sources.</li> <li>• Locked: Keep the current color temperature.</li> </ul>
	Red/Blue Offset	Adjust the red offset or blue offset manually.   <b>Note:</b> This parameter is configurable when <b>White Balance</b> is set to <b>Fine Tune</b> .

### 10.4.3.1.2 Image Scene Switch

Add scenes configured in [Image](#) to the **Auto Switching** column. When the system is in the set time period, the device will automatically switch to corresponding image scene. Otherwise, it will keep the default scene.

1. Go to **Setup > Image > Image > Image Scene Switch**.

**Figure 10-46: Image Scene Switch**




Enable Auto Switch

Switch Mode: h09824 Timed Switch 11:27, E0:BE:03:5D:8E:95, h09824

No.	Auto Switching	Schedule	Image Scene Name
1	Default Scene		1<> ▼
2	<input type="checkbox"/>	<input type="text"/> ~ <input type="text"/>	2<> ▼
3	<input type="checkbox"/>	<input type="text"/> ~ <input type="text"/>	3<> ▼
4	<input type="checkbox"/>	<input type="text"/> ~ <input type="text"/>	4<> ▼
5	<input type="checkbox"/>	<input type="text"/> ~ <input type="text"/>	5<> ▼

2. Select **Enable Auto Switch**.
3. Select a time template. You need to configure it in [Time Template](#).
4. Set the time period.

 **Note:** Up to 5 time periods are allowed (include default scene). The time periods cannot overlap.

- (1) Select the time period.
- (2) Set the start and end time.
- (3) Choose a scene for each period. The scene name can be configured in [Image](#).


5. Click **Save**.

### 10.4.3.2 OSD

See [OSD](#) for details.

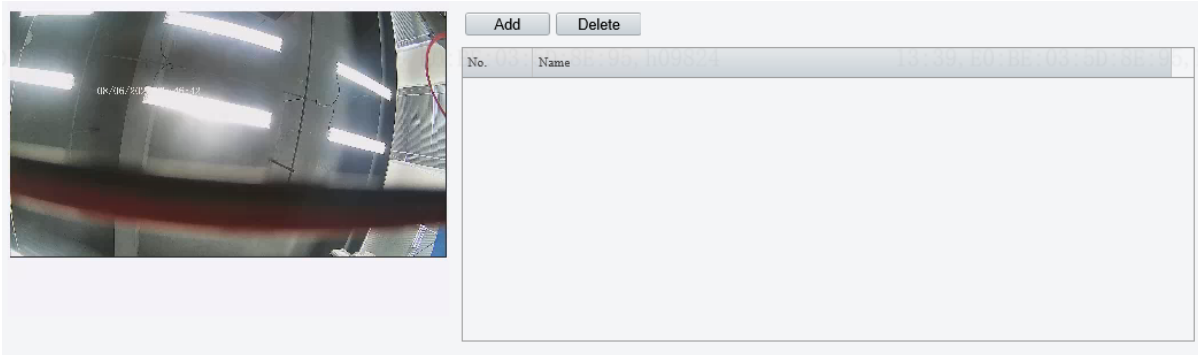
### 10.4.3.3 Privacy Mask

Privacy mask is used to cover certain areas on the image for privacy.

 **Note:** Up to 4 privacy areas are allowed, and their names are respectively Mask 1, Mask 2, Mask 3, and Mask 4.

Go to **Setup > Image > Privacy Mask**.

**Figure 10-47: Privacy Mask**



#### Add

1. Click **Add**, and then a rectangle mask appears on the left image.
2. Set the privacy area.
  - (1) Double-click the image on the left to play it in full screen.
  - (2) Select a privacy mask, and set the size of the mask as the following two ways.
    - Drag the rectangle to the desired position, point to a handle of the mask and drag to resize it.
    - Long press the left mouse button and drag it to draw a privacy mask.
  - (3) Double-click the image again or press **Esc** to exit full screen.
3. (Optional) To add multiple privacy areas, please follow the step 2 and step 3.

#### Delete

To delete a privacy mask, select the mask from the right list, and then click **Delete**.

## 10.4.4 Intelligent

### 10.4.4.1 Check Template

Set authentication modes for different time periods in a week for different scenarios.

You can add, edit, and delete check templates.

Go to **Setup > Intelligent > Check Template**.




**Figure 10-48: Check Template**

**Add**

1. Click **Add**, an empty template appears on the right.


**Figure 10-49: Empty Check Template**

2. Enter the template name with 1 to 20 characters, including uppercase and lowercase letters, digits, underscores, and hyphens.
  3. Set the time interval.
-  **Note:** Up to 8 periods are allowed, and periods cannot overlap.
4. Set authentication modes.
  5. (Optional) Repeat the above steps and complete the settings for other six days. To apply the current settings to other days, select the check box(es) for the days and then click **Copy**.
  6. Click **Save** to complete the settings.

**Edit**

1. Select the template to be edited on the left, and then edit the settings.
2. After completing the settings, click **Save**.

**Delete**

 **Note:** The default template cannot be deleted.

1. Select the template to be deleted on the left.
2. Click **Delete**, and then click **OK** to delete it.

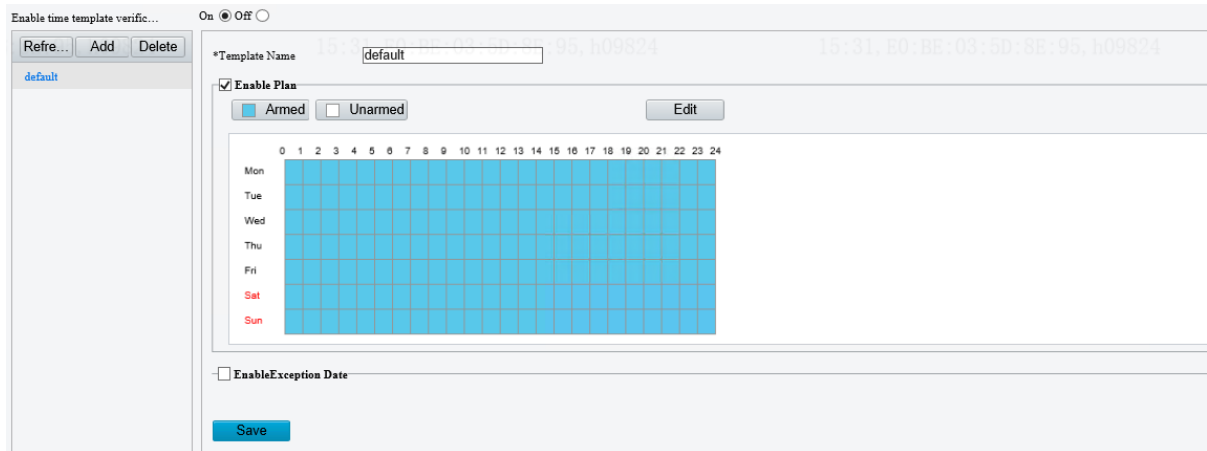
**10.4.4.2 Time Template**

Set time periods for an arming schedule in a week.

You can add, edit, and delete time templates.

Go to **Setup > Intelligent > Time Template**.

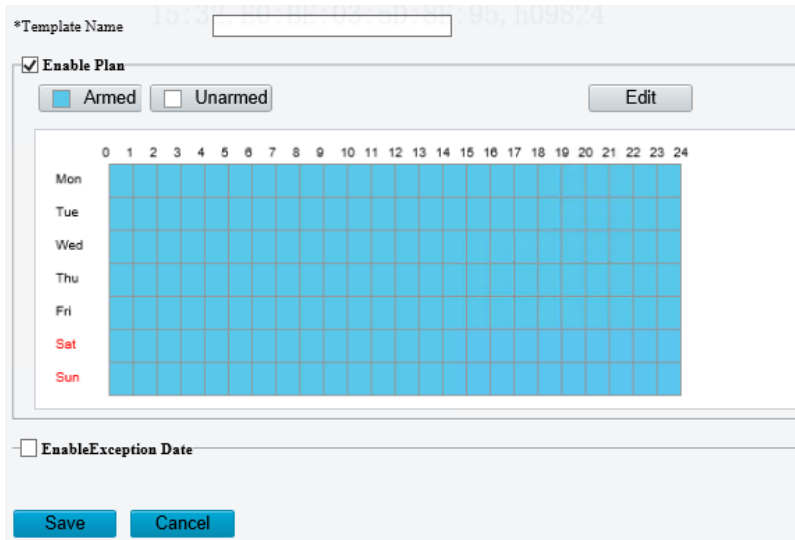
**Figure 10-50: Time Template**




## Add

1. Click **On** to enable time template verification.
2. Click **Add**, an empty template appears on the right.

**Figure 10-51: Empty Time Template**



3. Enter the template name with 1 to 20 characters, including uppercase and lowercase letters, digits, underscores, and hyphens.
4. Select **Enable Plan**.
5. Set the arming schedule. The following two ways are available.

 **Note:** The default arming schedule is 24/7.

- Use the blue and white grids (minimum editable unit: hour).  
Click  **Unarmed**, and select blue grids to delete time periods.  
Click  **Armed**, and select white grids to add time periods.
- Use the **Edit** button (minimum editable unit: second).  
(1) Click **Edit**. The **Edit** page appears.

**Figure 10-52: Edit**

No.	Start Time	End Time
1	00:00:00	23:59:59
2		
3		
4		
5		
6		
7		
8		

Copy To  Select All  
 Mon  Tue  Wed  Thu  Fri  Sat  Sun

OK Cancel Copy

- (2) Set the time periods for the current day. Up to 8 time periods are allowed and periods cannot overlap.
  - (3) (Optional) Repeat the above steps and complete the settings for other six days. To apply the current settings to other days, select the check box(es) for the days and then click **Copy**.
  - (4) After completing the settings, click **Save**.
6. (Optional) You can set the exception date to cancel the arming schedule.
    - (1) Select **Enable Exception Date**.
    - (2) Click **Add**.

**Figure 10-53: Add Exception Date**

Date

Time Interval 00:00:00 -- 23:59:59


OK Cancel

- (3) Set the exception date and time period.
  - (4) Click **OK**.
7. Click **Save**.

### Edit

1. Select the template to be edited on the left, and then edit the settings.
2. Click **Save**.

### Delete

 **Note:** The default template cannot be deleted.

1. Select the template to be deleted on the left.
2. Click **Delete**, and then click **OK** to delete it.

## 10.4.4.3 Advanced Settings

You can view door opening mode and call mode, and set the authentication records to be uploaded by the device.

1. Go to **Setup > Intelligent > Advanced Setting**.

**Figure 10-54: Advanced Settings**

Door Opening Mode  Authentication

Call Mode

Record Upload Settings

Reporting Type

2. Configure the authentication record type.
  - Upload All: The device reports all authentication records including success and failure records to the intelligent server.
  - Upload Success Record: The device only reports authentication success records to the intelligent server.
3. Click **Save**.

## 10.4.5 Events

The trigger actions supported may vary with device model.

### 10.4.5.1 Fire Alarm

A fire alarm occurs when the connected external device detects fire.

1. Go to **Setup > Events > Fire Alarm**.

**Figure 10-55: Fire Alarm**

Alarm Name

Alarm ID

Alarm Input  On  Off

Trigger Actions

Snapshot  Open door

Enable Plan

Armed  Unarmed

	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
Mon	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed
Tue	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed
Wed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed
Thu	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed
Fri	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed
Sat	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed
Sun	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed	Armed

2. Set the alarm name (default: 1, only 0 and 1 can be displayed), and alarm ID.
3. Enable **Alarm Input**, and then the device can receive fire alarms; otherwise, the device cannot receive fire alarms.
4. Select alarm-triggered actions as needed. When a fire alarm occurs, the station can take a snapshot and send door opening signal to the connected device.
5. Select **Enable Plan**. Only during the set arming periods can the alarm be reported and the alarm actions be triggered.
6. Set the arming schedule.

The default arming schedule is 24/7. To change the schedule, see [Time Template](#).

7. Click **Save**.

### 10.4.5.2 Tamper Alarm

If the device is disassembled, the tamper button will be triggered and the device will report a tamper alarm.

1. Go to **Setup > Events > Tamper Alarm**.

**Figure 10-56: Tamper Alarm**

Alarm Name: 1

Alarm ID:

Alarm Type: N.C.

Alarm Input:  On  Off

Trigger Actions

Snapshot

Enable Plan

Armed  Unarmed Edit

	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
Mon																									
Tue																									
Wed																									
Thu																									
Fri																									
Sat																									
Sun																									

Save

2. Set the alarm name (default: 1, only 0 and 1 can be displayed), and alarm ID.
3. Choose the alarm type to **N.O.** or **N.C.**. The default is **N.O.**.
4. Enable **Alarm Input**, and then the device can receive fire alarms; otherwise, the device cannot receive fire alarms.
5. Select the alarm-triggered action. When **Snapshot** is enabled, the station takes a snapshot when an alarm occurs.
6. Select **Enable Plan**. Only during the set arming periods can the alarm be reported.
7. Set the arming schedule.

The default arming schedule is 24/7. To change the schedule, see [Time Template](#).

8. Click **Save**.

### 10.4.5.3 Door Magnet Alarm

When a door magnet is connected to the device, it can receive door magnet alarms.

1. Go to **Setup > Events > Door Magnet Alarm**.

**Figure 10-57: Door Magnet Alarm**

Alarm Name: 1

Alarm ID:

Alarm Input:  On  Off

**Trigger Actions**

Snapshot

**Enable Plan**


Armed  Unarmed

	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
Mon																									
Tue																									
Wed																									
Thu																									
Fri																									
Sat																									
Sun																									

2. Set the alarm name (default: 1, only 0 and 1 can be displayed), and alarm ID.
3. Enable **Alarm Input**, and then the device can receive door magnet alarms; otherwise, the device cannot receive door magnet alarms.
4. Select the alarm-triggered action. When **Snapshot** is enabled, the station takes a snapshot when an alarm occurs.
5. Select **Enable Plan**. Only during the set arming periods can the alarm be reported.
6. Set the arming schedule.  
The default arming schedule is 24/7. To change the schedule, see [Time Template](#).
7. Click **Save**.

## 10.4.6 Storage

The door station has no memory card by default. After a memory card is inserted into the device, you can format the card, view the card status and capacity, and configure video storage parameters.

 **Note:** This function is only available to the indoor station.

1. Go to **Setup > Storage > Storage**.

**Figure 10-58: Storage**

- (Optional) To format the memory card, set **Storage Medium** to **Memory Card**, and click **Format**.
- Set the storage parameters.

Parameter	Description
Storage Policy	<ul style="list-style-type: none"> <li>Manual and Alarm Recording</li> <li>Alarm Recording Only</li> </ul>
When Storage Full	The storage policy when the storage is full. <ul style="list-style-type: none"> <li>Overwrite: When the storage is full, the new data overwrites the oldest data.</li> <li>Stop(default): When the storage is full, the device stops saving new data.</li> </ul>
Post-Record(s)	The duration of video to be recorded after an alarm. The device continues to record video after an alarm occurs.

- Click **Save**.

## 10.4.7 Security

### 10.4.7.1 User

See [User](#) for details.

### 10.4.7.2 Network Security

#### 10.4.7.2.1 HTTPS

HTTPS is a secure version of the HTTP protocol that uses SSL protocol to authenticate both a client and a server, and encrypt data during transmission to prevent data from being stolen or altered, enhancing data security.

- Go to **Setup > Security > Network Security > HTTPS**.

**Figure 10-59: HTTPS**

- Enable **HTTPS**.
- Click **Browse**, locate the SSL certificate, and click **Upload**.

 **Note:**

- An SSL certificate is issued by the Certificate Authority after verifying that the server is reliable and compliant with the SSL protocol. It is used to activate SSL protocol (an Internet protocol used for authentication and encryption), transmit encrypted data between client and server so that it cannot be leaked and tampered with, and confirm the reliability of the server.

An SSL certificate includes a public key (for encryption) and private key (for decryption).

- Put the RSA public key and private key in one pem file, and then import.

4. Click **Save**.

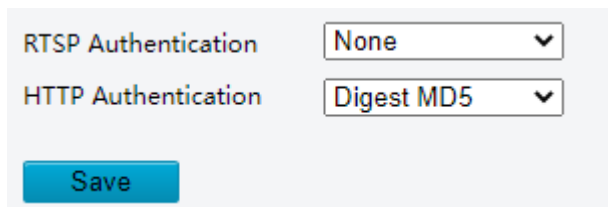
### 10.4.7.2.2 Authentication

Authentication refers to the procedure of identifying clients. Only after successful authentication can the data be transmitted based on the protocol, improving the security of data transmission.

- **RTSP Authentication:** Transmits audio and video data in real time through the RTSP protocol. It establishes a two-way connection between the server and the client, and controls either a single or several streams of continuous media such as audio and video for a long time.
- **HTTP authentication:** Transfers data as a file via the HTTP protocol. It establishes a one-way connection between the client and the server, and the connection will end after the server responds to the request from the client. The connection will be re-built to transfer data if there is a new request.

1. Go to **Setup > Security > Network Security > Authentication**.

**Figure 10-60: Authentication**



2. Choose an authentication mode.

Parameter	Description
RTSP Authentication	Choose an authentication mode from the drop-down list, including <b>None</b> , <b>Basic</b> , <b>Digest MD5</b> , and <b>Digest SHA256</b> . <ul style="list-style-type: none"><li>• <b>None:</b> Transmits data without authentication.</li><li>• <b>Basic:</b> Authentication information is transferred in plaintext without encryption, which imposes serious security risks.</li><li>• <b>Digest:</b> Authentication information is encrypted to provide higher security. Digest SHA256 provides higher security than Digest MD5.</li></ul>
HTTP Authentication	Choose an authentication mode from the drop-down list, including <b>None</b> , <b>Digest MD5</b> , and <b>Digest SHA256</b> .

3. Click **Save**.

### 10.4.7.2.3 ARP Protection

ARP attack mainly exists in local area network, which forges IP address and physical address (MAC address) to achieve ARP spoofing, causing communication failures among devices within the local area network. Configure ARP protection, and the device will verify the physical address (MAC address) of the access source, so as to avoid ARP spoofing attacks.

1. Go to **Setup > Security > Network Security > ARP Protection**.



**Figure 10-61: ARP Protection**

ARP Protection  On  Off

Gateway

Gateway MAC Address

**Save**

2. Enable **ARP Protection**.
3. Enter the gateway's physical address (legal MAC address).
4. Click **Save**.

#### 10.4.7.2.4 IP Address Filtering

Use IP address filtering to allow or forbid access from specified IP addresses.

1. Go to **Setup > Security > Network Security > IP Address Filtering**.

**Figure 10-62: IP Address Filtering**

IP Address Filtering  On  Off

Filtering Mode

No.	IP Address	+

**Save**

2. Enable **IP Address Filtering**.
3. Select the filtering mode from the drop-down list. If **Allowlist** is selected, only the added IP addresses are allowed to access the device. If **Deny Access** is selected, then only the added IP addresses cannot access the device.
4. Click **+**, and enter IP address(es).
  - Up to 32 IP addresses can be added. Duplicate addresses are not allowed.
  - The first byte of the IP must be 1 to 233, and the fourth byte cannot be 0. Invalid IP addresses such as 0.0.0.0, 127.0.0.1, 255.255.255.255, and 224.0.0.1 are not allowed.
5. Click **Save**.

#### 10.4.7.2.5 Access Policy

Configure access policy to protect the device from illegal use or illegal access.

The access policy includes MAC authentication, illegal login lock, and session timeout. The session timeout is disabled by default.

1. Go to **Setup > Security > Network Security > Access Policy**.

**Figure 10-63: Access Policy**

MAC Authentication  On  Off

**Illegal Login Lock**

Illegal Login Lock  On  Off

Illegal Login Limit

Lock Time (min)

**Session Timeout**

Session Timeout  On  Off

Timeout (min)

**Save**

2. Configure parameters of MAC authentication, illegal login lock and session timeout. The following shows the description.
  - **MAC Authentication:** When enabled, access is allowed only if the Mac address is authenticated successfully, which has higher security; When disabled, access is allowed for any Mac address, which poses security risks.
  - **Illegal Login Lock:** If the client IP address is not on the blacklist, the input username is correct, but the input password is wrong, it is an illegal login attempt. User can try to log in again after setting the lock time.
    - **Illegal Login Limit:** The maximum number of illegal login attempts allowed. Range: [2-10], integer only. Default: 5.
    - **Lock Time (min):** The account is locked when the lock time is reached. Range: [1-120], integer only. Default: 5.
  - **Session Timeout:** When enabled, if the client cannot obtain or save configurations within the set time, the user will automatically log out. To user the account, the user need to log in again. Range (min): [1-120], integer only. Default: 120.
3. Click **Save**.

#### 10.4.7.2.6 Certificate Management

A certificate is an electronic file that uniquely represents individuals and resources on the Internet and enables secure and confidential communications between the two entities. On the **Certificate Management** interface, you can set different servers, create CA certificates, view certificate properties, etc.

Go to **Setup > Security > Network Security > Certificate Management**.

**Figure 10-64: Certificate Management**

The screenshot shows a web interface for certificate management. It is divided into two main sections: "Certificate" and "CA Certificate".

**Certificate Section:** This section has a header with buttons: "Create Self-Signed Certificate", "Create Certificate", "Import Certificate", "Export Certificate", "Delete Certificate", and "Certificate Properties". Below the buttons is a table with the following data:

Certificate Name	Valid From	Valid To	Certificate Status	Function
default	2023-06-06 01:35:45	2024-06-06 01:35:45	Normal	HTTPS

**CA Certificate Section:** This section has a header with buttons: "Import Certificate", "Delete Certificate", and "Certificate Properties". Below the buttons is an empty table with the same column headers as the first section:

Certificate Name	Valid From	Valid To	Certificate Status	Function

### Add Certificate

- Self-signed certificate: It is a digital certificate issued by an untrusted certificate authority (CA), that is, created, issued, and signed by a company or software developer. It is suitable for application scenarios with low security requirements.

**Figure 10-65: Create Self-Signed Certificate**

The screenshot shows a dialog box titled "Create Self-Signed Certificate" with a close button (X) in the top right corner. The dialog contains the following fields:

- Certificate Name:
- Public Key:  (dropdown arrow)
- Country:  Example: CN
- Domain Name/IP:
- Valid Period(day):
- Province:
- City:
- Organization:
- Organizational Unit:
- Email:

At the bottom of the dialog are two buttons: "OK" and "Cancel".

- Certificate: It is used to apply the self-signed certificate or imported certificate to be a CA certificate, which is suitable for application scenarios with high security requirements.

Figure 10-66: Create Certificate

**Create Certificate** ✕

Country  Example:CN

Domain Name/IP


Province

City

Organization

Organizational Unit

Email

 **Note:** After the certificate request is created, export the certificate request file. After the certificate authority (CA) signs and issues a certificate in accordance with the request, import the certificate into the device.

- Import Certificate: A non-CA certificate can be imported.

Figure 10-67: Import Certificate

**Import Certificate** ✕

Import Format  ▾

Certificate Name

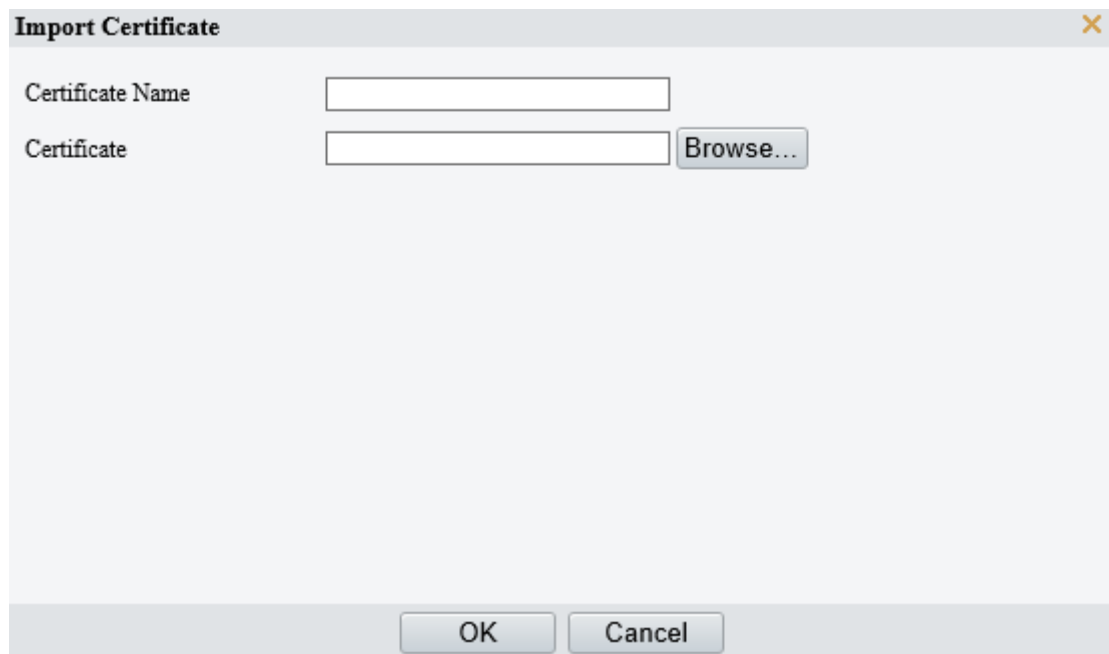
Certificate

Private Key

Private Key Password

- CA Certificate: CA, an authority to issue certificate, is the core of the public key infrastructure. It can sign and issue certificates, and manage certificates issued. A CA certificate is a self-signed certificate issued by an untrusted certificate authority (CA) and thus is more secure and reliable.

Figure 10-68: Import Certificate



The image shows a dialog box titled "Import Certificate". It has a title bar with a close button (X) in the top right corner. Inside the dialog, there are two input fields: "Certificate Name" and "Certificate". The "Certificate" field has a "Browse..." button to its right. At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

### Delete Certificate

A certificate that is in use cannot be deleted.

### Export Certificate

Click **Export Certificate** to save the certificate to your computer.

### Certificate Properties


Select a certificate to view its properties.

## 10.4.8 System

### 10.4.8.1 Time


See [Time](#) for details.

### 10.4.8.2 Ports & Devices

 **Note:** This function is only available to the door station.

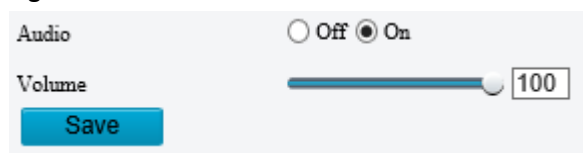
#### 10.4.8.2.1 Volume Control

Configure the volume of the door station.

 **Note:** You may also configure the volume on the screen. See [Live View](#) for details.

1. Go to **Setup > System > Ports & Devices > Volume Control**.

Figure 10-69: Volume Control



The image shows the "Volume Control" settings. It has a section for "Audio" with two radio buttons: "Off" and "On". The "On" radio button is selected. Below this is a "Volume" section with a slider and a text box containing the value "100". At the bottom, there is a blue "Save" button.

2. Select whether to turn audio off. If **Turn Audio Off** is disabled, you can adjust the volume.  
Range: [1-100], integer only. Default: 100.
3. Click **Save**.

### 10.4.8.2.2 Door Configuration

Configure the door that is physically connected to the door station.

1. Go to **Setup > System > Ports & Devices > Door Configuration**.

**Figure 10-70: Door Configuration**

The screenshot shows a configuration window for two doors, Door1 and Door2. The Door2 tab is selected. The configuration options are as follows:

Parameter	Value / Option
Enable	<input checked="" type="radio"/> On <input type="radio"/> Off
Name	Door1
Door Contact Type	<input type="radio"/> N.O. <input checked="" type="radio"/> N.C.
Open Duration	5 s
Unlock Interval	0 s
Door Opening Timeout	10 s
Auto Door Lock Upon Closing	<input type="radio"/> On <input checked="" type="radio"/> Off
Query door magnetic status when the door is closed	<input type="radio"/> On <input checked="" type="radio"/> Off
Door magnetic query time	<input checked="" type="radio"/> Before closing the door <input type="radio"/> After closing the door

A blue **Save** button is located at the bottom left of the configuration area.

2. Enable Door1.

3. Configure door parameters.

- Name: **Door 1** by default. It can be named as needed, and must be unique.
- Door Contact Type: Set it to **N.O.**, otherwise this function cannot be used.
- Unlock Interval (s): The time interval between two unlocks.

After the door lock is opened, it can only be opened again after the set time.

If it is set to **0**, the door lock opens every time it receives an opening signal.

Range: [0-300]s, integer only. Default: 0s.

- Door Opening Timeout (s): The door lock automatically locks when the closing time exceeds the set time and the door magnet detects that the door is closed in place.

Range: [1-300]s, integer only. Default: 10s.

 **Note:**

- To use this function, enable **Auto Door Lock Upon Closing** first.
- Set an appropriate value according to the actual situation, otherwise a short timeout may affect door opening.
- Auto Door Lock Upon Closing
  - On: The door lock automatically locks when the door closing time exceeds the set **Door Opening Timeout** and the door magnet detects that the door is closed in place.
  - Off: The door lock locks after the set pulse width.
- Query door magnetic status when the door is closed: Check if the door has door magnet.
- Door magnetic query time: For the door with door magnet, set **Door Magnetic Query Time** to **Before closing the door** or **After closing the door** based on the actual door lock type. If the door magnet is closed, it means that the door is locked.

 **Note:** To use this function, enable **Query door magnetic status when the door is closed** first.

4. To enable the second door, click the **Door2** tab, enable Door2, and configure other parameters as the above description.

5. Click **Save**.

### 10.4.8.2.3 I/O Input

Configure the door magnet and door button that are physically connected to the door station, and corresponding fire alarm.

1. Go to **Setup > System > Ports & Devices > I/O Input**.

**Figure 10-71: I/O Input**

	I/O1	I/O2	I/O3	I/O4
Enable	<input checked="" type="radio"/> On <input type="radio"/> Off			
Mode	<input type="radio"/> N.O. <input checked="" type="radio"/> N.C.			
Type	Door Magnet1			

Save

2. Enable **I/O1**.
3. Set the mode to **N.O.**, otherwise the door station cannot receive the input signal.
4. Select the I/O type. By default, the type of I/O1 and I/O2 is door magnet, while the type of I/O3 and I/O4 is door button.

**Note:** A door station can connect 2 door magnets or 2 door buttons at the same time. Only one fire alarm is supported. The type must be unique for each I/O input.

5. Click **Save**.

## 10.4.8.3 Maintenance

### 10.4.8.3.1 Maintenance

System maintenance includes software upgrade, system configuration, diagnosis information, system restart, and custom voice.

**Note:**

- The device will restart if you perform operations such as software upgrade, restart, restoring default configurations, and importing configurations.
- Restarting the device will interrupt the ongoing services. Please handle with caution.

For maintenance settings on the screen, see [Maintenance](#).

Go to **Setup > System > Maintenance**.

### Software Upgrade

Local upgrade and cloud upgrade are available.

**Note:**

- Make sure the upgrade file matches the device; otherwise, unexpected problems may occur.
- The version file is a .zip file that includes all the upgrade files.
- Power must be connected throughout the upgrade.

**Figure 10-72: Software Upgrade**

Software Upgrade


Local Upgrade     Upgrade Boot Program

Cloud Upgrade

**Note: The upgrade will take a while. Please do not disconnect power.**

- Local Upgrade

1. Click **Browse**, and then select the correct upgrade file.


 **Note:** If applicable, select **Upgrade Boot Program**, and the boot program will also be upgraded.

2. Click **Upgrade**. The device will restart automatically after the upgrade is completed, and then the **Login** interface is displayed.

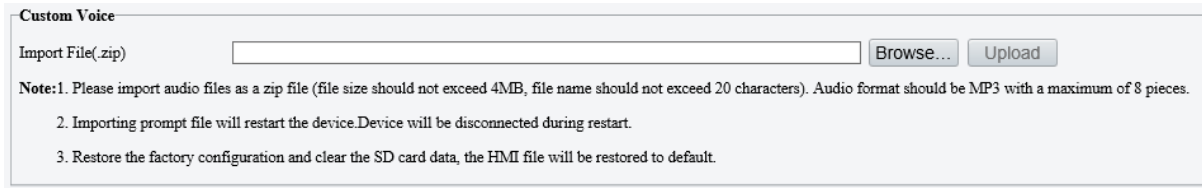
- Cloud upgrade: Click **Detect** to check for new versions. You can perform a cloud upgrade if a new version is available on the cloud server.

## Custom Voice

You can import custom voice files to replace the default ones.

 **Note:** Only available for the 1-button door station.

**Figure 10-73: Custom Voice**



Custom Voice

Import File(.zip)

**Note:** 1. Please import audio files as a zip file (file size should not exceed 4MB, file name should not exceed 20 characters). Audio format should be MP3 with a maximum of 8 pieces.  
2. Importing prompt file will restart the device. Device will be disconnected during restart.  
3. Restore the factory configuration and clear the SD card data, the HMI file will be restored to default.

The following shows the default voice file name and the corresponding voice content:

File Name	Voice Content
CollectFail.mp3	Collection failed.
CollectSuccess.mp3	Collection succeeded.
CounterpartyBusy.mp3	The user you are calling is busy.
ICFail.mp3	Card verification failed.
ICTips.mp3	Please swipe card.
OpenSucceed.mp3	Door opened successfully.
Refuse.mp3	The user you are calling is unavailable.
Success.mp3	Successful identification.
TimeFail.mp3	Not allowed time.
CallingFailed.mp3	Calling Failed.
MsgRecBegin.mp3	Please leave a message after the beep.

To replace the default voice files, follow the steps below:

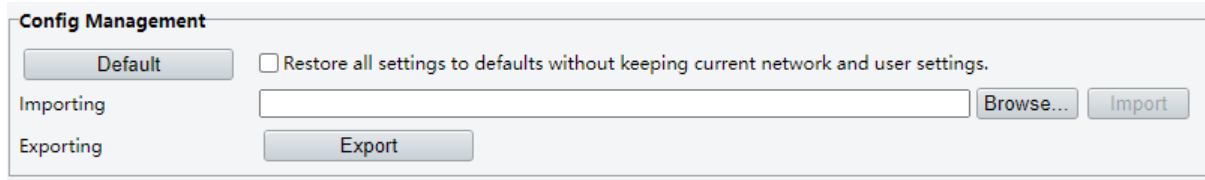
1. Change the name of the custom voice file to be the same as the name of the default voice file. Besides, the custom voice must be a MP3 file (8KHz, 16-bit, mono).
2. Compress all custom voice files into a .zip package with the file name no more than 20 characters and file size no more than 4MB.
3. Click **Browse**, and choose the package to import.
4. Click **Upload** to replace the default voice files. The device will restart after successful replacement.

## System Config

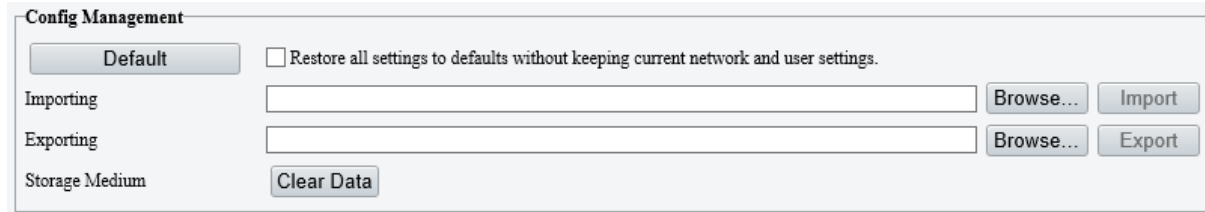
You can export the current configurations of the device and save them to the local device or an external storage device. You can also restore configurations by importing an exported configuration file.



**Figure 10-74: Indoor Station**




**Figure 10-75: Door Station**



- Default: Clicking **Default** will restore settings to defaults except the administrator login password, network settings, and system time, and then the device will automatically restart.

To restore all settings to factory defaults, select **Restore all settings to defaults without keeping current network and user settings**.

- Import configurations


 **Note:** Make sure the configuration file to import matches the device model; otherwise, unexpected results may occur.

1. Click **Browse** next to the **Import** button.
2. Select the configuration file you want to import, and then click **Import**.
3. Click **OK**. The device will restart after you import the configuration file.

- Export configurations

- Indoor Station Operation

1. Click **Export**. The **File Encryption** page appears.

 **Note:** The exported configuration file should be encrypted by default, and the password should be 1 to 16 common characters.

2. Enter the encryption password, and confirm the password. Click **OK**, and then the configuration file will be automatically saved to the browser's default folder.

- Door Station Operation

1. Click **Browse**, and choose the destination folder.
2. Click **Export**, enter the encryption password, confirm the password, and then click **OK**.

- Clear data: Click **Clear Data**, and then all data will be deleted.

 **Note:**

- This function is only available to the door station.
- Please handle with caution.

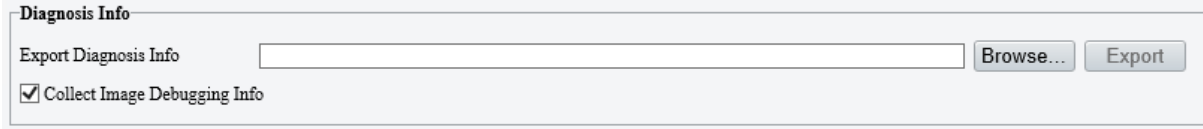
## Diagnosis Info

Diagnosis information includes logs and system configurations, and you can export them to the local device.

**Figure 10-76: Indoor Station**



**Figure 10-77: Door Station**



Diagnosis Info


Export Diagnosis Info

Collect Image Debugging Info

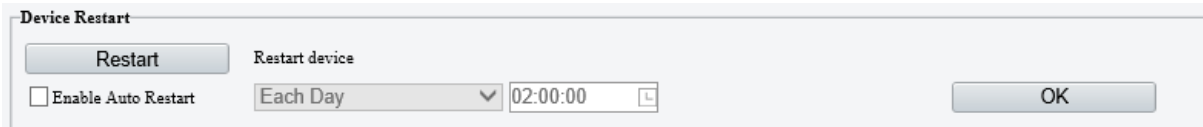
- Indoor Station Operation: Click **Export**, and then the records will be automatically saved to the browser's default folder in .tgz format.
- Door Station Operation
  1. Click **Browse**, and choose the destination folder.
  2. (Optional) By default, **Collect Image Debugging Info** is selected. You can clear the check box as needed.
  3. Click **Export**.

## Device Restart

You can choose to restart the device manually or automatically.

 **Note:** Restarting the device will interrupt the ongoing services.

**Figure 10-78: Device Restart**



Device Restart


Restart device

Enable Auto Restart

- Restart manually: Click **Restart**, and then confirm to restart the device.
- Restart automatically:
  1. Select **Enable Auto Restart** and set the restart time.
  2. Click **OK**, and then the device will automatically restart at the set time.

## Language

The default language is English. You can switch the language to **Chinese Simplified** here, or set it on the **Login** page.

 **Note:** This function is only available to the indoor station.

1. Select **Chinese Simplified** from the **Language** drop-down list.
2. Click **OK** to confirm the selection.

### 10.4.8.3.2 Network Diagnosis

Diagnose the NIC and network latency.

Go to **System > Maintenance > Network Diagnosis**.

Figure 10-79: Network Diagnosis


The screenshot shows two panels. The top panel, titled "Network Diagnosis", includes a "Select NIC" dropdown menu with "NIC1" selected, "IP Filter" and "Port Filter" sections each with radio buttons for "All", "Specify", and "Filter", and an unchecked "Custom Rules" checkbox. A "Start Capture" button is at the bottom. The bottom panel, titled "Network Delay and Packet Loss Test", has a "Test Address" input field, a "Packet Size (Bytes)" input field with "64" entered, and a "Test Result" section with a "Test" button.

## Network Diagnosis

Check network to ensure the data packets can be transmitted and received in security.

Figure 10-80: Network Diagnosis

This screenshot is identical to Figure 10-79, showing the "Network Diagnosis" and "Network Delay and Packet Loss Test" panels.

1. Select a NIC. NIC1 is the device's IP address.
2. Select an IP and port filter mode.
  - All: Capture packets of all the ports and IPs.
  - Specify: Capture packets of the specified port and IP.
  - Filter: Capture packets except that of the specified port and IP.
3. (Optional) Select **Custom Rules** and set the rules. Click  to view the rules information.
4. Click **Start Capture** to start capturing packets.


## Network Delay and Packet Loss Test

The system can send test packets to a test address for many times, and check if the operation is normal and network is smooth based on average delay and packet loss, which can help users to find the cause of network failures. The average delay refers to the average length of time from test packets are sent till responses are received. The packet loss rate refers to the ratio of lost packets to the sent packets.

Figure 10-81: Packet Loss Test

This screenshot is identical to Figure 10-79, showing the "Network Delay and Packet Loss Test" panel.

1. Enter the test address. It must be a valid IP address or domain name. If the address is invalid, a prompt will be displayed on the interface.
2. Enter the test packet size. It means the size of test packets to be sent. Unit: Bytes. Range: [64-65507], integer only. Default: 64. If the value exceeds the range, a prompt will be displayed on the interface.
3. Click **Test**. The results will appear after the test is complete.
  - The destination is unreachable: The test address cannot be pinged or reached.
  - The packet loss rate is not 0%: The test address cannot be pinged, but it can be reached with high network latency.
  - The packet loss rate is 0%: The test address is successfully pinged.

 **Note:** Due to high network latency, there is occasional randomness when pinging larger test packets. If the test address cannot be pinged, it is recommended to test with smaller packet.

### 10.4.8.3.3 About

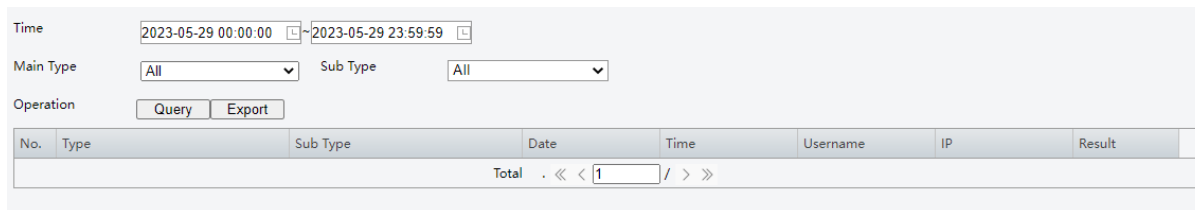
See [About](#) for details.

### 10.4.8.4 Log

Logs contain information about user operation, date, username, IP, and results. User can search and export logs by conditions.


1. Go to **Setup > System > Log**.

**Figure 10-82: Log**



The screenshot shows a web interface for viewing logs. At the top, there are two date pickers for 'Time', with the first set to '2023-05-29 00:00:00' and the second to '2023-05-29 23:59:59'. Below these are two dropdown menus for 'Main Type' and 'Sub Type', both currently set to 'All'. Underneath are two buttons: 'Query' and 'Export'. Below the filters is a table with the following columns: 'No.', 'Type', 'Sub Type', 'Date', 'Time', 'Username', 'IP', and 'Result'. At the bottom of the table area, there is a pagination bar showing 'Total' and a page number '1' between navigation arrows.

2. Set a time range, main type, and sub type.
3. Click **Search**. The latest logs are displayed in the list below.
4. Click **Export** to save search results as a .csv file to the default path of the browser.

 **Note:** Up to 100 logs can be displayed and exported. The logs are displayed in descending chronological order.