

Indoor Station & Door Station

User Manual

V1.10

Contents

About this Manual	1
1 Defaults	2
2 Home Screen	2
3 Lock Screen Manually	2
4 Do Not Disturb	2
5 Live View	3
6 Make Calls	4
7 Answer Calls	5
8 Message	5
9 Settings	6
9.1 Sounds.....	7
9.1.1 Call Settings.....	7
9.1.2 Volume Settings.....	8
9.2 General Settings.....	9
9.2.1 Display Settings.....	9
9.2.2 Time Settings.....	9
9.2.3 Password Settings.....	10
9.3 Wi-Fi.....	11
9.4 Administration Configuration.....	12
9.4.1 Indoor Station.....	13
9.4.2 Device Mgmt.....	15
9.4.3 Main Station.....	19
9.4.4 Administrator Password.....	20
9.4.5 Device Maintenance.....	21
10 Web Operations	21
10.1 Login.....	21
10.2 Live View.....	24
10.3 Person Library.....	26
10.4 Setup.....	29
10.4.1 Common.....	29
10.4.2 Network.....	37
10.4.3 Image.....	44
10.4.4 Intelligent.....	50
10.4.5 Events.....	53
10.4.6 Storage.....	53
10.4.7 Security.....	54
10.4.8 System.....	59

About this Manual

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

Copyright Statement

©2023 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
 NOTE!	Indicates useful or supplemental information about the use of product.
 CAUTION!	Indicates a situation which, if not avoided, could result in damage, data loss or malfunction to product.
 WARNING!	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 door station are consistent.

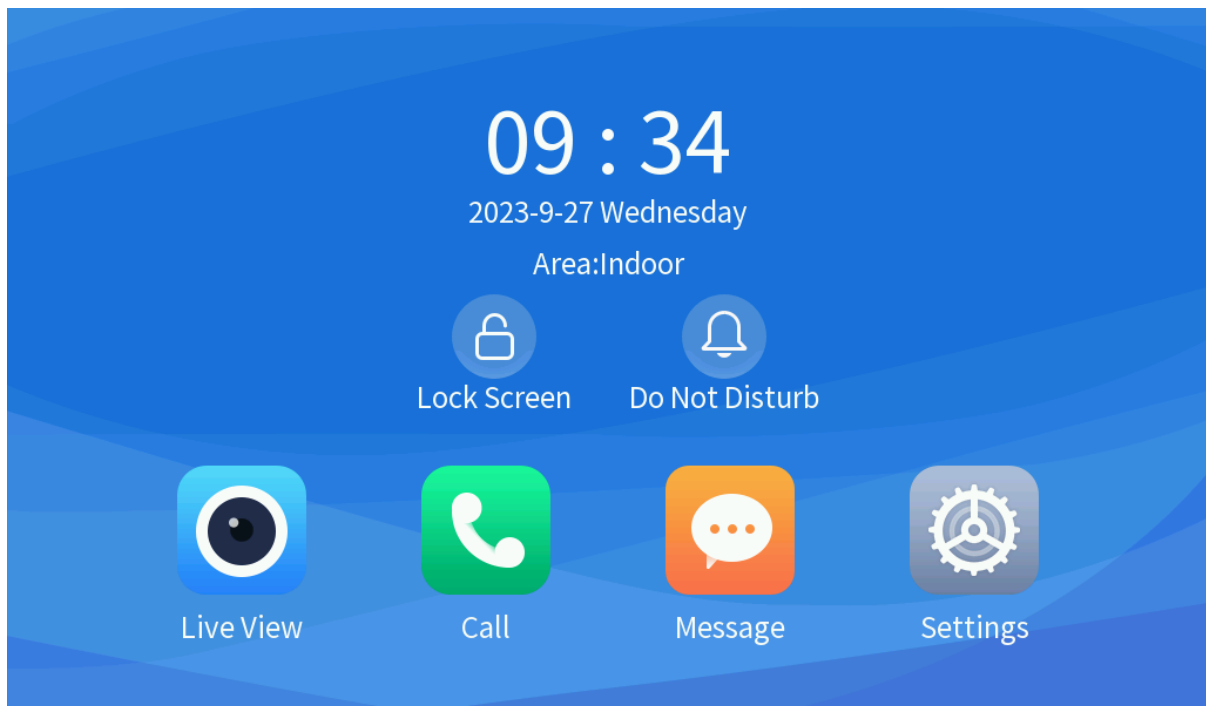
Username: admin	Password: 123456
Static IP address: 192.168.1.13	Subnet mask: 255.255.255.0

 **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, 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 [Automatic screen rest](#).

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. 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 [Sounds](#) screen.

5 Live View

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


 **Note:**

- This function is available to the indoor station's screen.
- To connect the face recognition terminal, door station, and network camera to the indoor station, please see [Door Station and IPC Management](#), and ensure that **Live View** is on.

Figure 5-1: Live View



- The system will automatically return to the [Home Screen](#) if there is no operation within 60 seconds.

Tap . The live view screen appears.

- The face recognition terminals/door stations connected to the indoor station are displayed in the right list. To view the connected network cameras, enter the **Camera** tab.
- Tap the device name, and the left window will play its live video.
- The device name and the remaining play time are displayed at the top of the screen.


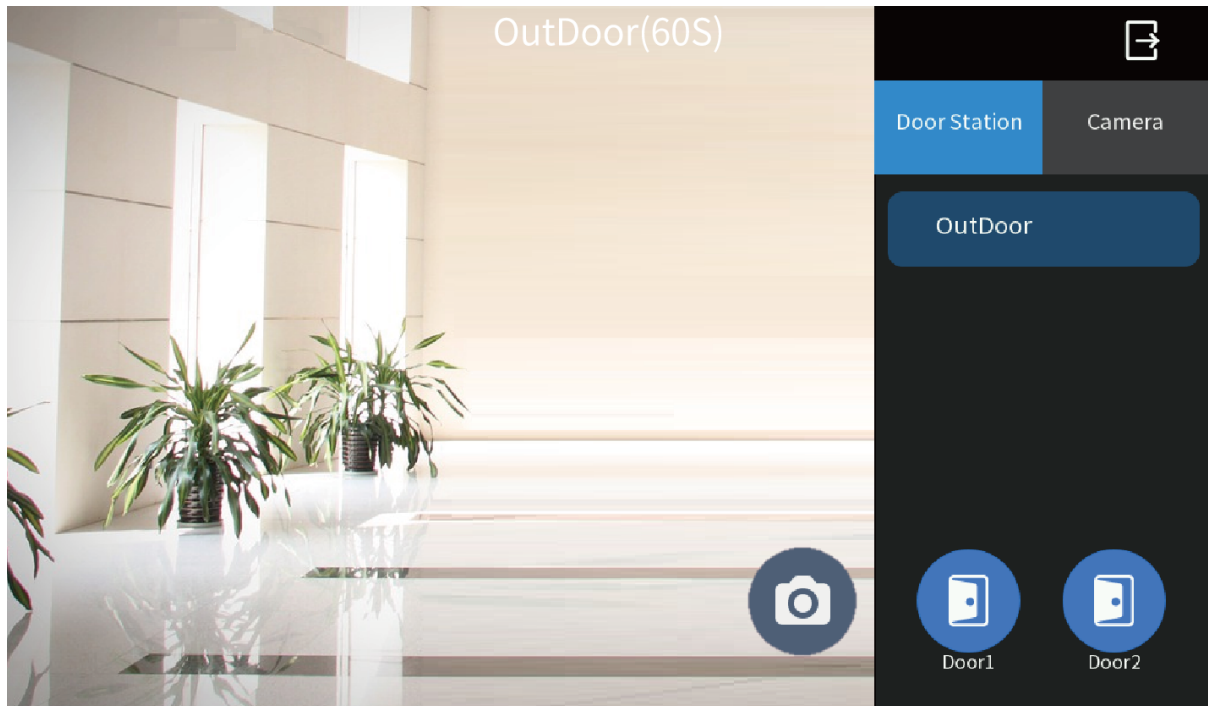



 **Note:** The default play time is the same as **Ringtone Duration(s)** in [Call Settings](#). The screen will be automatically blacked out after the duration. To view the live video again, you need to tap the corresponding device.

Figure 5-2: Live View



- : Tap to take a snapshot for the current image. You can view the snapshot records in [Message](#).
- : Tap to send a door opening signal to the face recognition terminal or door station, so as to open the door remotely.

- : Tap to return to the home screen.

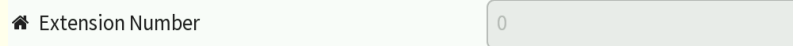
6 Make Calls

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 bound to the indoor extension (see [Door Station Auto Search](#) 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 Number Example



- The system will automatically return to the [Home Screen](#) if there is no operation within 60 seconds.


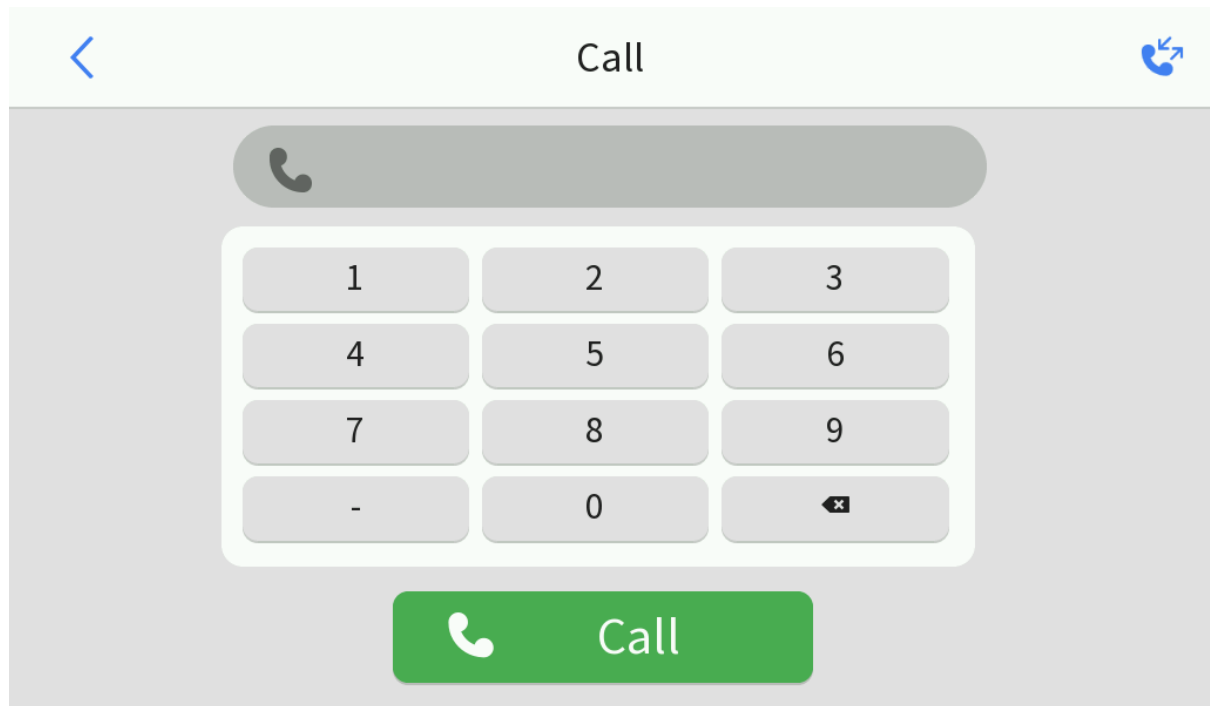
Tap . The **Call** screen appears.

Figure 6-2: Call





- Call other extension users.
 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.
- View call records: Up to latest 200 records can be displayed if the device has no memory card, including the **All Call Records** and **Missed Call** lists. Tap  in the upper-right corner to view the details.

Figure 6-3: Call Records

The screenshot shows a mobile application interface titled 'Call Record' with a subtitle '(District-Building-Unit-Room-Extension Number)'. Below the title is a navigation bar with two tabs: 'All Call Records' (highlighted in blue) and 'Missed Call'. The main content area displays a list of call records. Each record consists of a call status icon, a phone number '0-1-1-0-0', the location 'OutDoorStation', a timestamp, and a snapshot icon. The first record shows an accepted call at '2023-08-18 15:49:26'. The second record shows a declined call at '2023-08-18 15:48:49'. Below the list is a grey rectangular area, likely a placeholder for more records.

All Call Records		Missed Call		
	0-1-1-0-0	OutDoorStation	2023-08-18 15:49:26	
	0-1-1-0-0	OutDoorStation	2023-08-18 15:48:49	

- : The call was accepted/declined.
- : The call was answered/hung up.
- Delete a record: Long press the record you want to delete, and then tap **Delete**.
- Delete all records: Long press any record, tap **Clean**, and then tap **Confirm**.
- View call snapshots: If you manually answer/hang up the call from face recognition terminal/door station, the indoor station will automatically capture the screen at the moment when the call is answered/hung up. Long press the call record you want to view, and tap **Snapshot**.

7 Answer Calls

Tap to answer calls from the face recognition terminal, door station, or other extension devices; tap to hang up calls; tap to open the door remotely,

8 Message

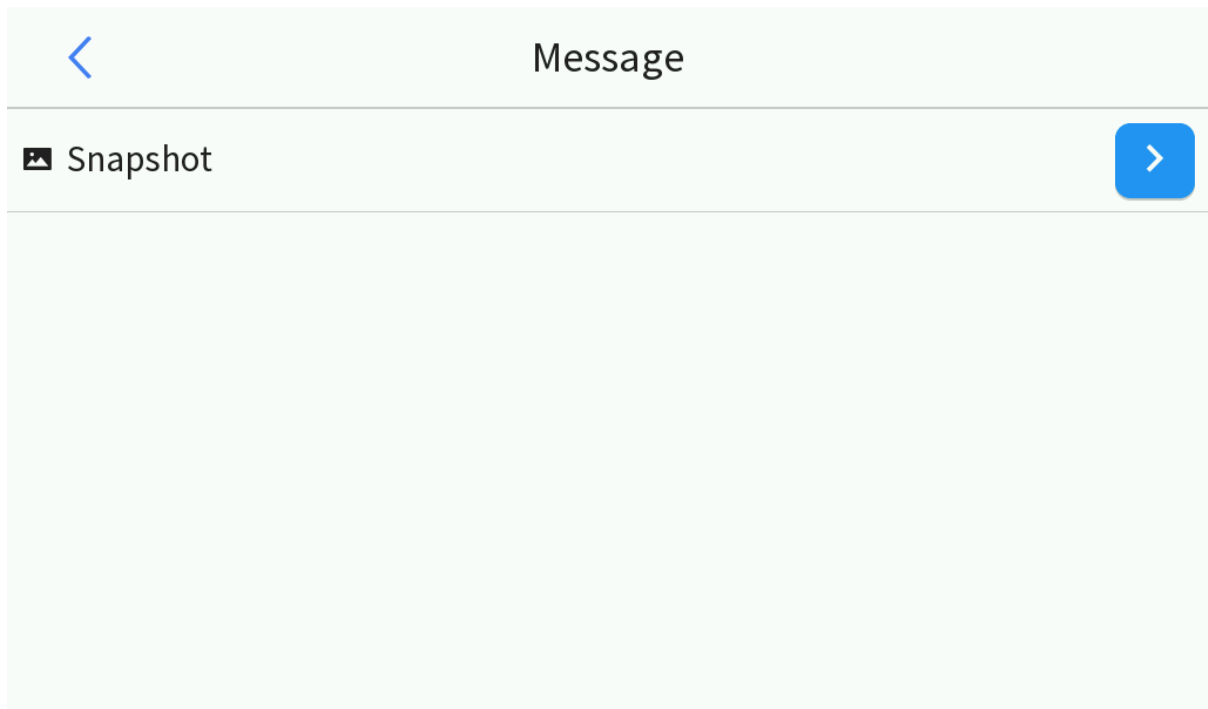
Store all snapshots from [Live View](#).

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

Note: The system will automatically return to the [Home Screen](#) if there is no operation within 60 seconds.





Tap . The **Message** screen appears.


Figure 8-1: Message



Tap . The **Snapshot** screen appears.


Figure 8-2: Snapshot

No.	Snapshot Time	Picture
0	2023-08-18 15:47:46	
1	2023-08-18 15:47:37	
2	2023-08-18 15:47:23	
3	2023-08-18 15:47:13	

The snapshot records are displayed in decreasing order of snapshot time. Tap  to view the details.

9 Settings

The indoor station's screen supports [Sounds](#), [Display Settings](#), [Time Settings](#), [Password Settings](#), [Message](#), and [Administration Configuration](#).

 **Note:** The system will automatically return to the [Home Screen](#) if there is no operation within 60 seconds.

9.1 Sounds

9.1.1 Call Settings



1. Go to  > **Sounds**, and tap  beside **Call Settings**.

Figure 9-1: Call Settings-Main Station

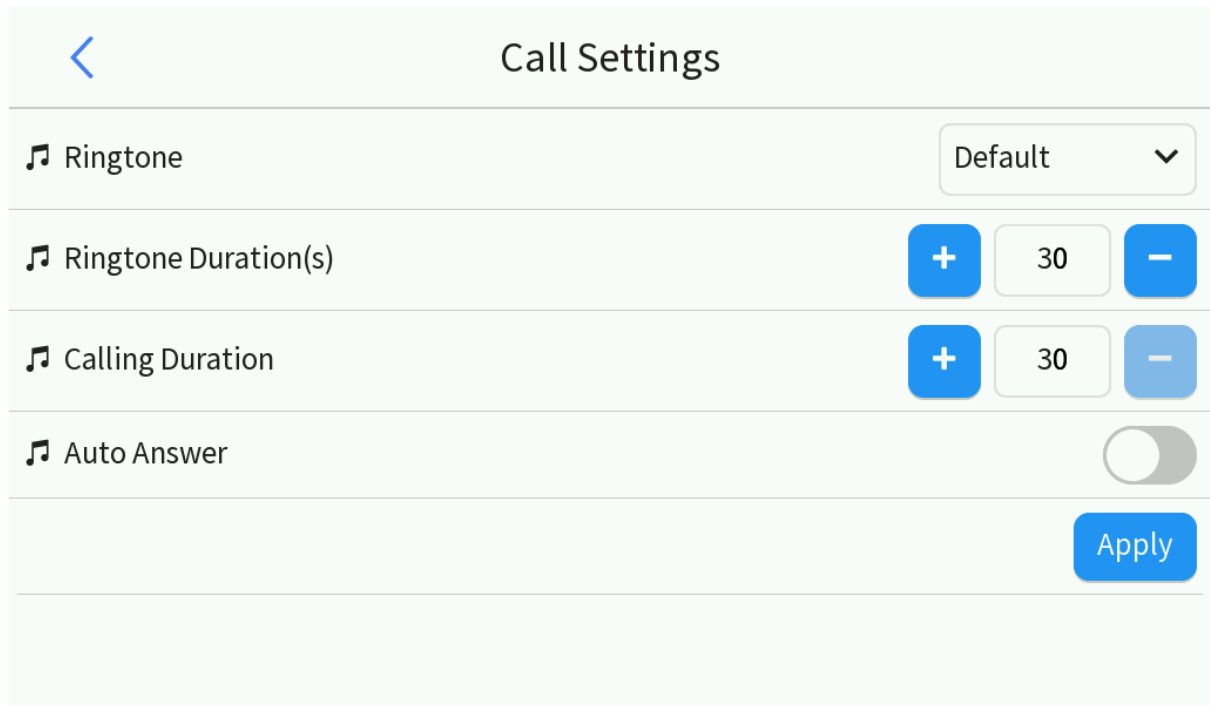
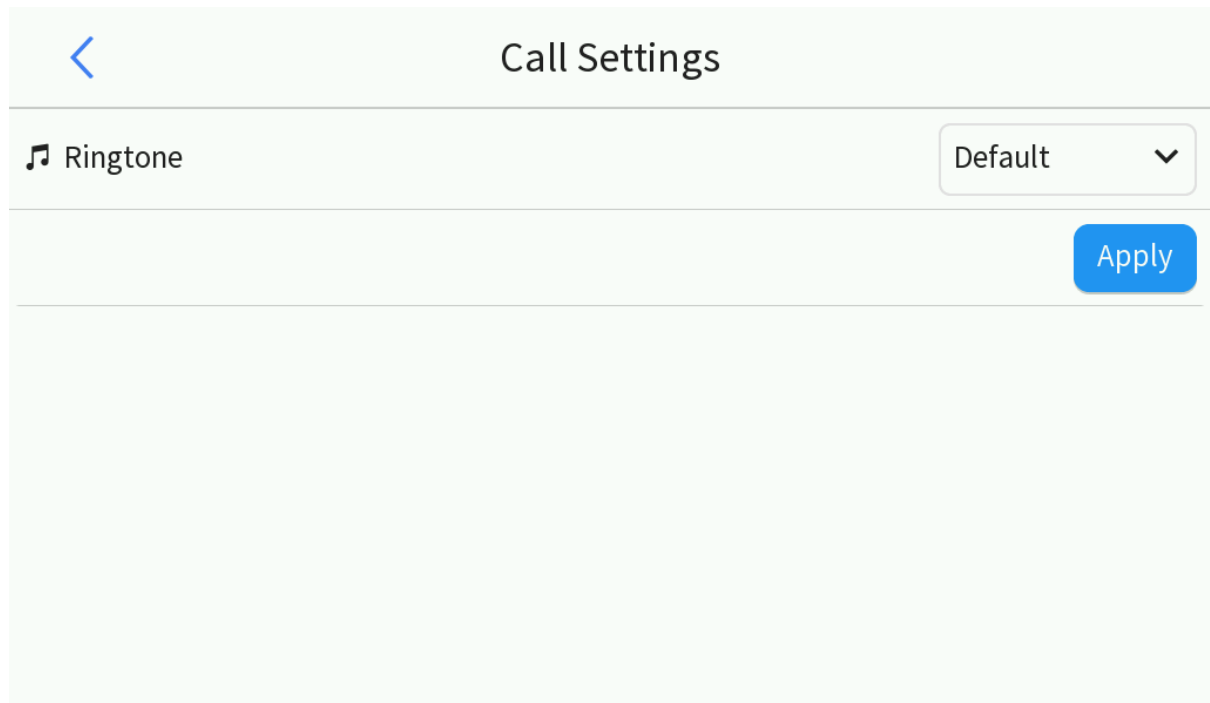








Figure 9-2: Call Settings-Extension



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

Parameter	Description
Ringtone Duration(s)	Length of time that the ringtone sounds when the indoor station receives a call. Range: [1-99], integer only. Default: 30. You can tap  /  to adjust the value.

Parameter	Description
Calling Duration	The time period that the indoor station initiates a call until the call is answered. Range: [30-60], integer only. Default: 30. You can tap  /  to adjust the value.
Auto Answer	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 are shown below. <ul style="list-style-type: none"> • Extension/face recognition terminal: A voice is played and a message is displayed on the screen to prompt no answer. • Door station: A voice is played "The user you are calling is unavailable". By default, this function is disabled. You can tap  to enable it.

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

9.1.2 Volume Settings



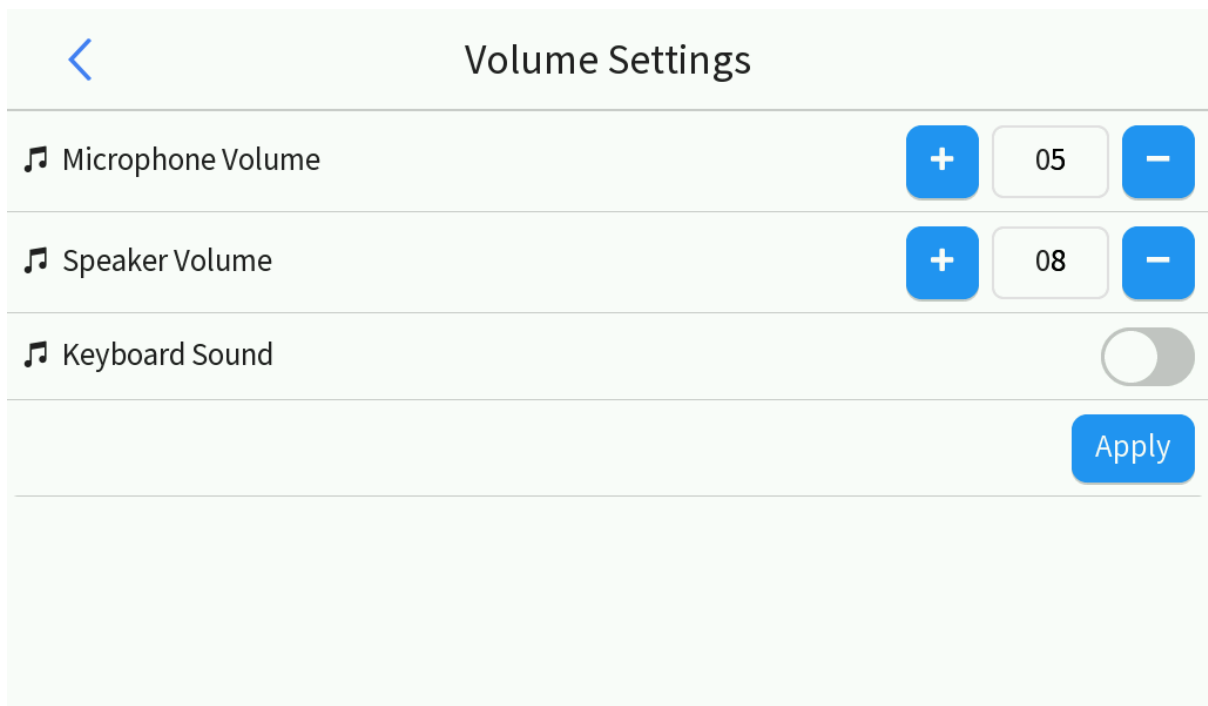






1. Go to  > **Sounds**, and tap  beside **Volume Settings**.

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: 05. You can tap  /  to adjust the value.
Speaker Volume	Sound volume of the speaker during the call. Range: [0-10], integer only. Default: 08. 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 screen rest parameters.

When **Automatic screen rest** 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.



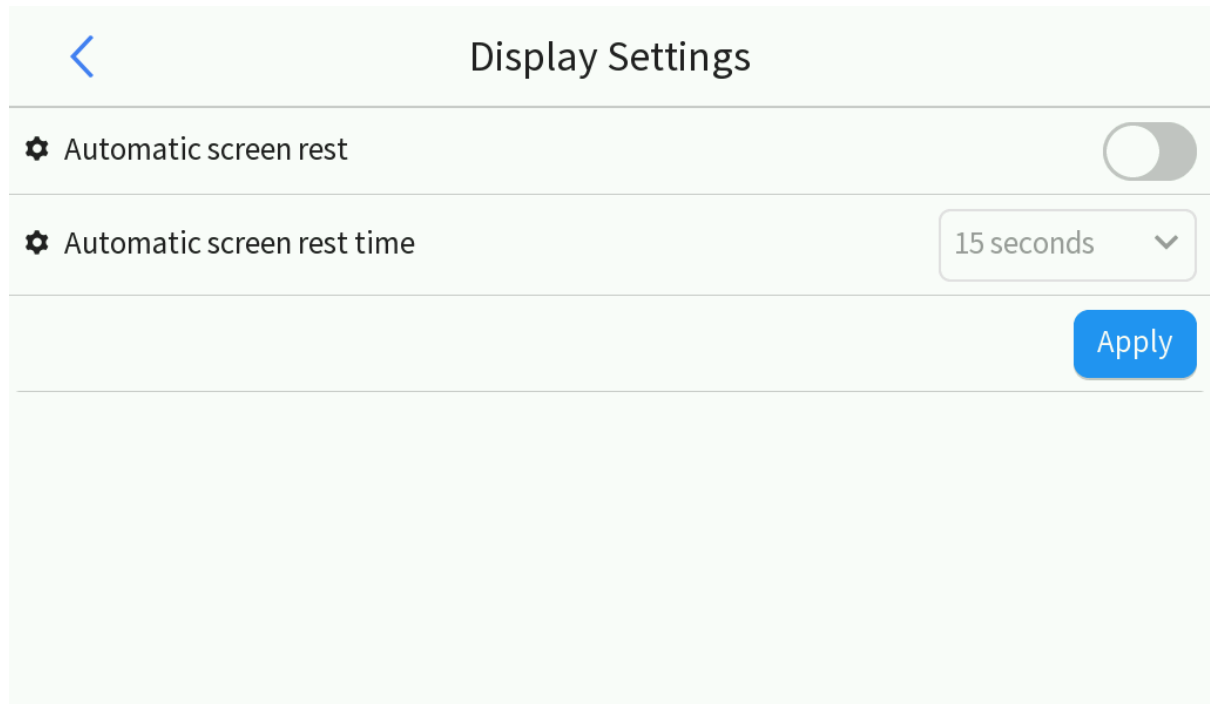


1. Go to  > **General Settings**, and tap  beside **Display Settings**.

Figure 9-4: Display Settings



2. Tap  to enable **Automatic screen rest**.
3. Set automatic screen rest parameters. 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](#).



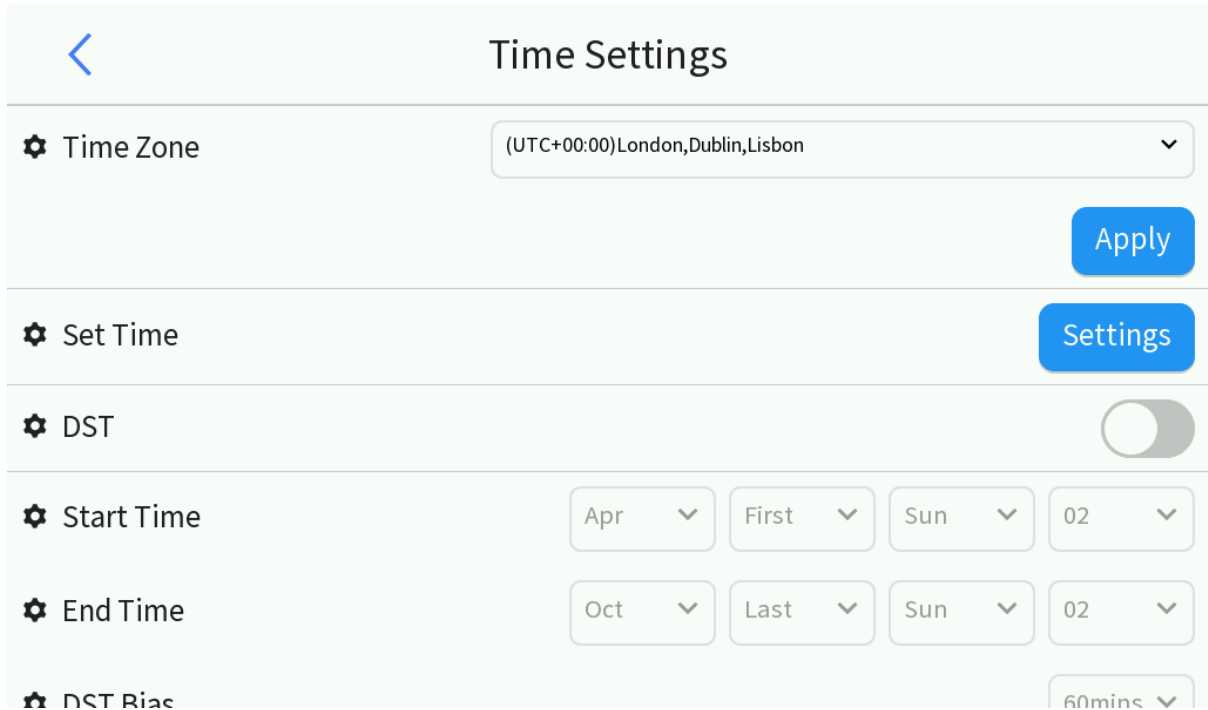
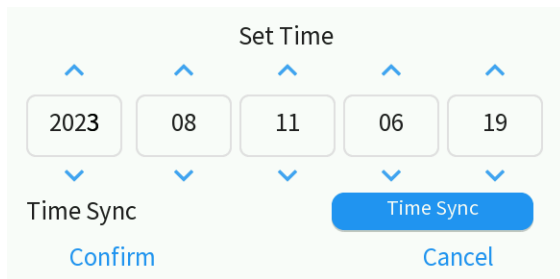
1. Go to  > **General Settings**, and tap  beside **Time Settings**.

Figure 9-5: Time Settings



2. Set the time zone. Default: (UTC+00:00)London,Dublin,Lisbon.
3. Tap **Apply**. A success message means the settings are saved.
4. Tap **Settings**. 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 time of the least added face recognition terminal/door station will be automatically synced to the 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 face recognition terminal/door station, the time will be synced automatically.

- (2) Click **Confirm** to save the settings.

5. (Optional) Set the DST. It is disabled by default.
6. Tap **Apply** 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 face recognition terminal first.



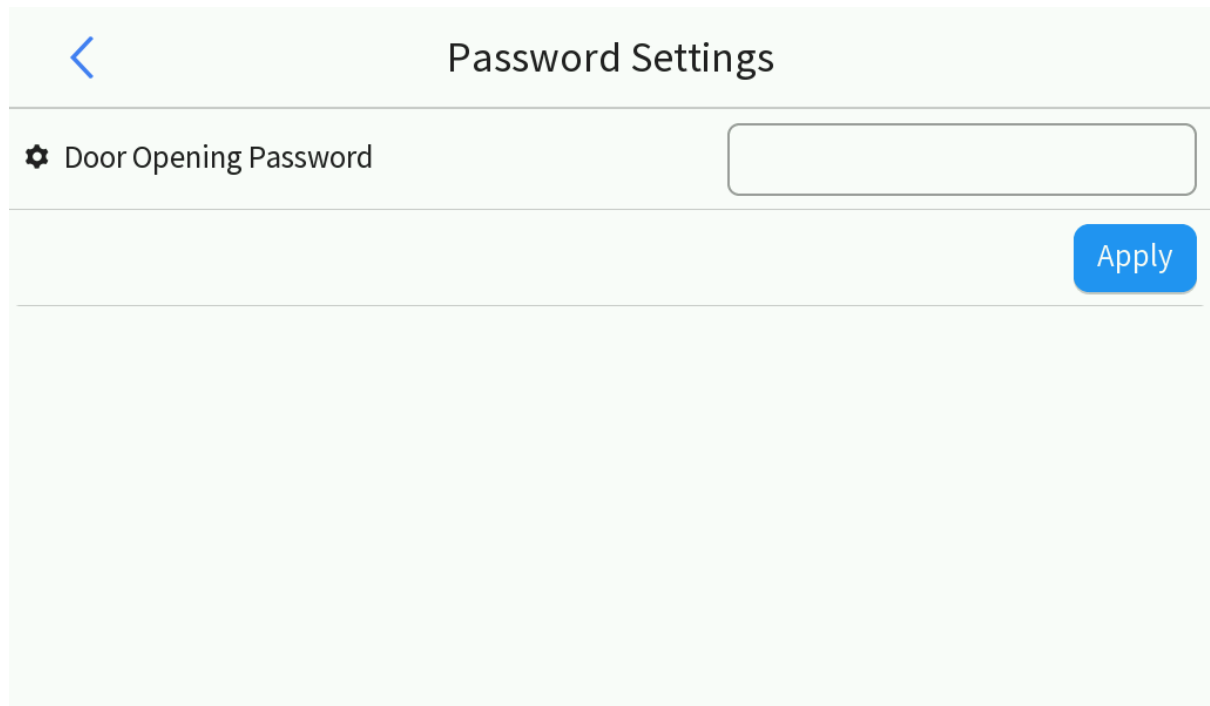

1. Go to  > **General Settings**, and tap  beside **Password Settings**.

Figure 9-7: Password Settings



2. Input the door opening password with 1 to 30 characters.
3. Tap . A success message means the settings are saved.

9.3 Wi-Fi

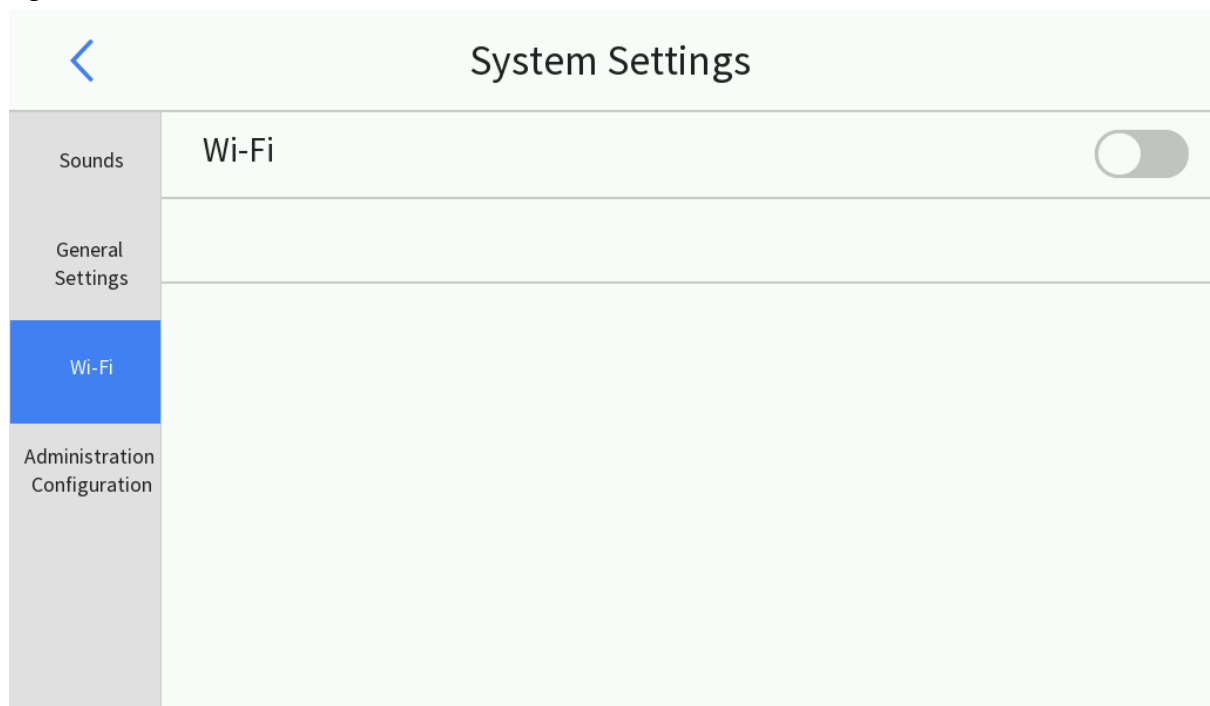
Configure Wi-Fi for the indoor station for network connection, so the call, live view, device connection, and other operations can be used normally.

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

Add Wi-Fi

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

Figure 9-8: Wi-Fi




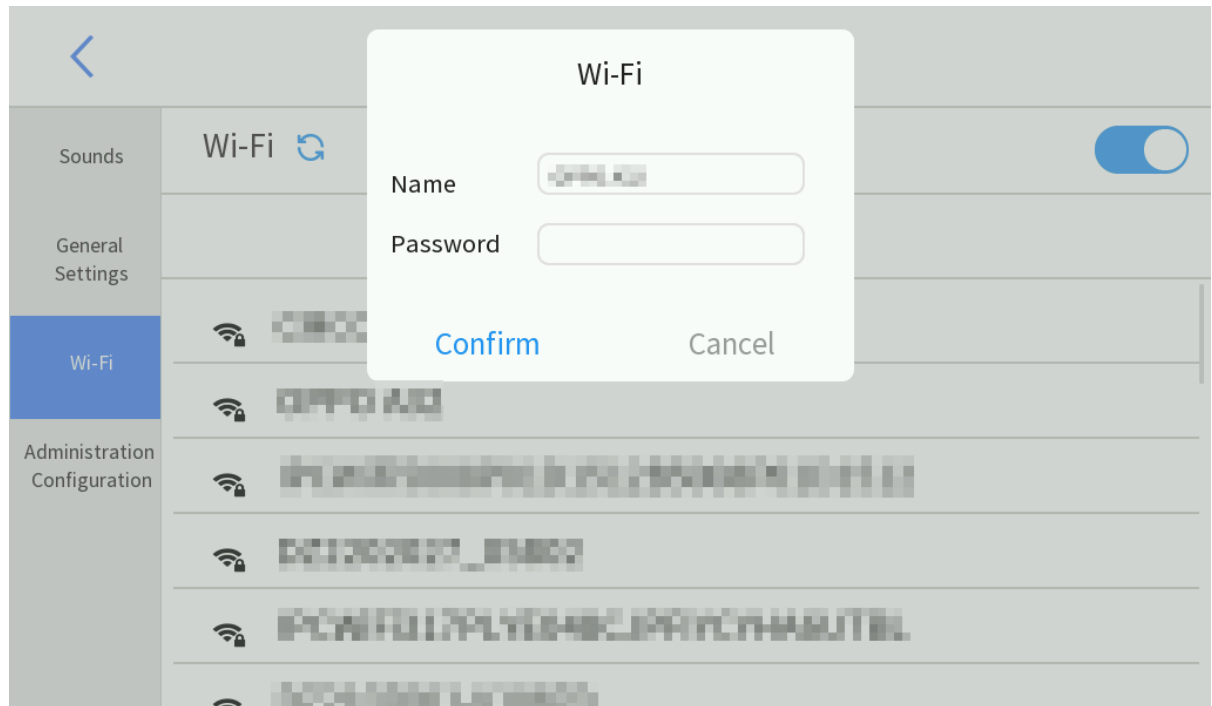
2. Tap  to enable Wi-Fi. The available Wi-Fi will be searched automatically and displayed in the list below from strong to weak signal.
3. Select the Wi-Fi to connect from the list below. Input the Wi-Fi password, and then tap **Confirm**.

Figure 9-9: Connect Wi-Fi



After the Wi-Fi is connected, a message will appear on the right.

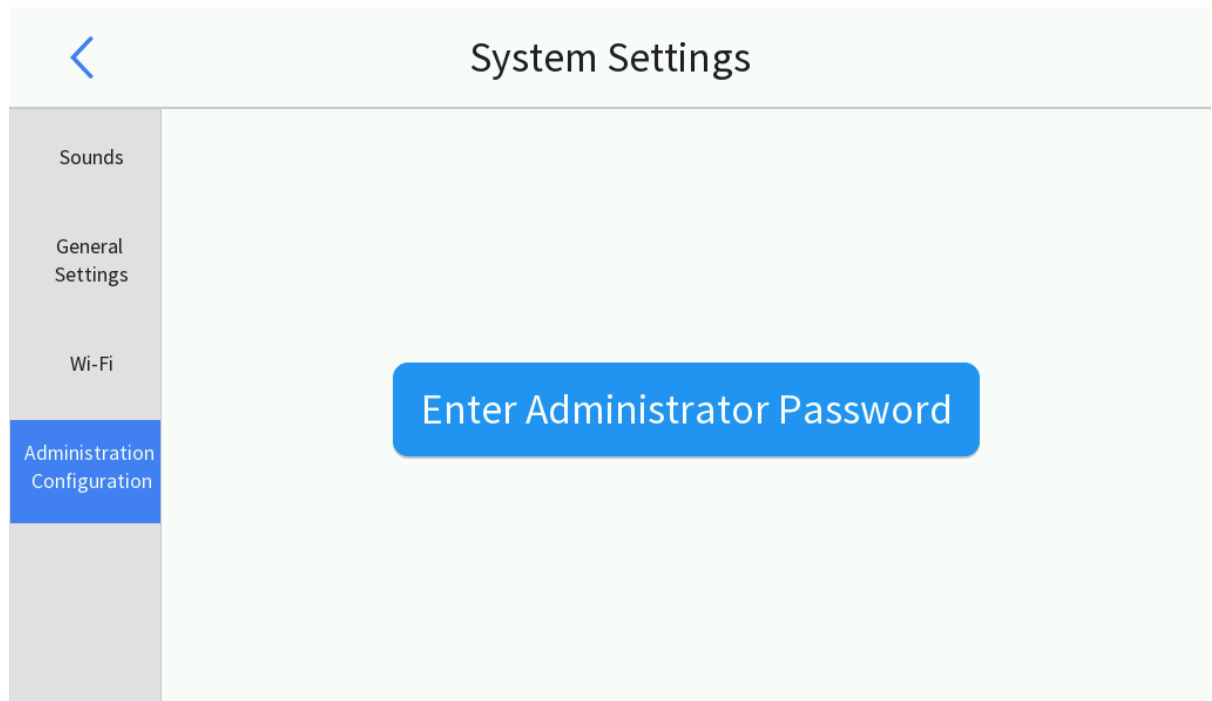
Disconnect Wi-Fi

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 9-10: Administration Configuration



2. Tap **Enter Administrator Password**.

Figure 9-11: Enter Password


Please enter the password.

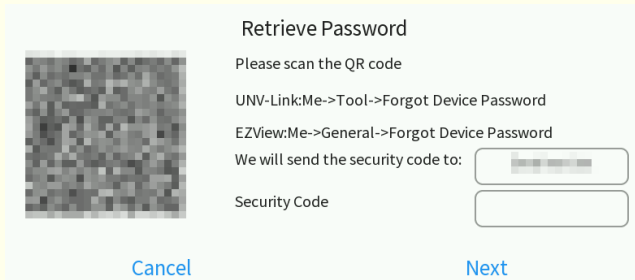
 [Forgot?](#)

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.

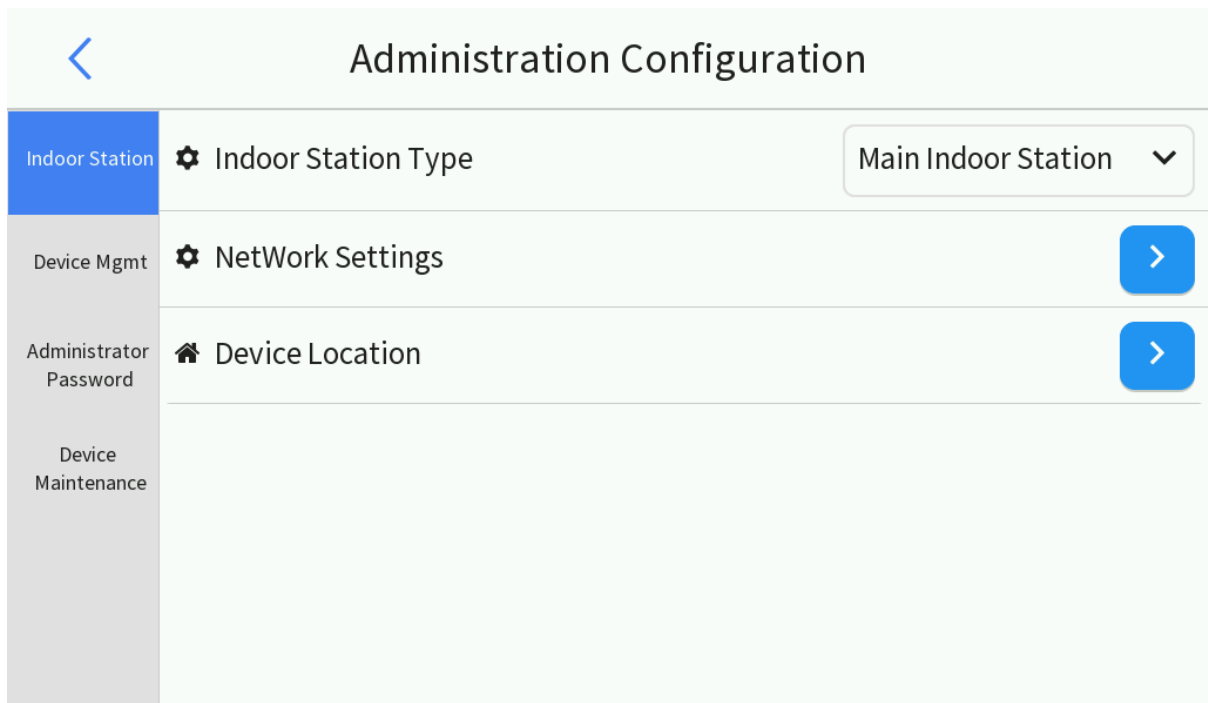
4. Tap **Login**.

9.4.1 Indoor Station

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

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

Figure 9-12: Indoor Station



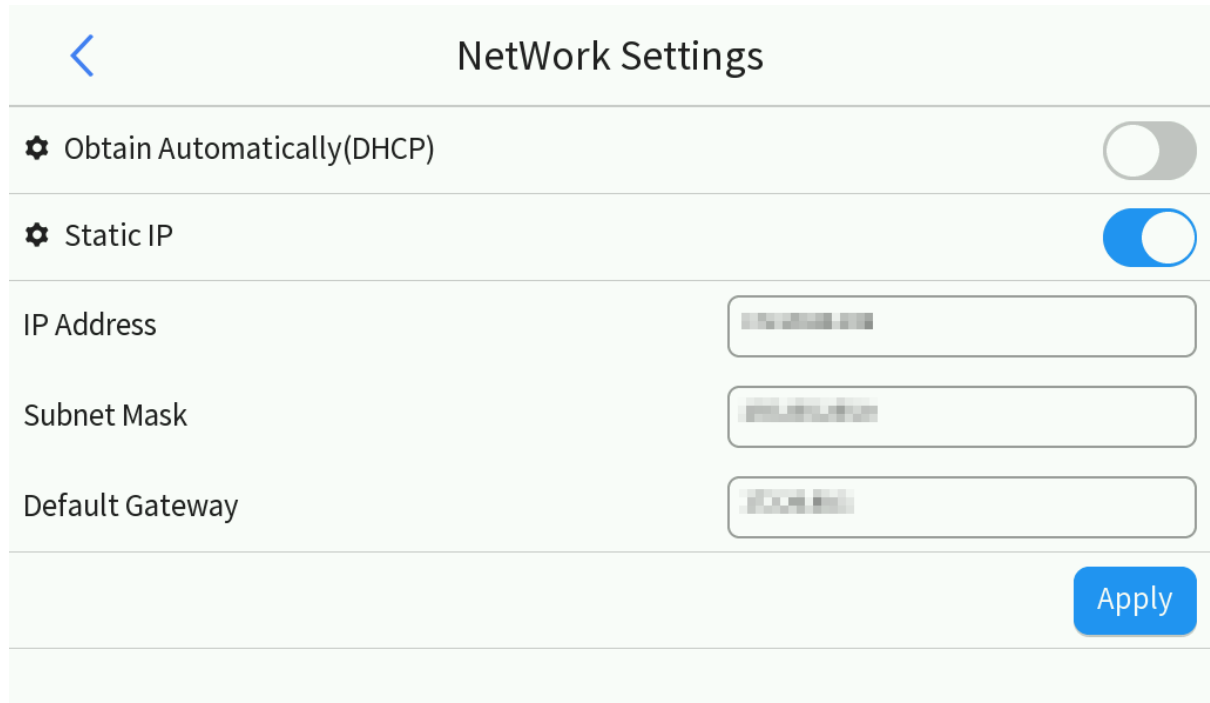
2. Set the indoor station type. It is **Main Indoor Station** by default. If it is set to **Extension**, the system will return to the home screen and restore factory default settings.




9.4.1.1 Network Settings


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

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

Figure 9-13: Network Settings



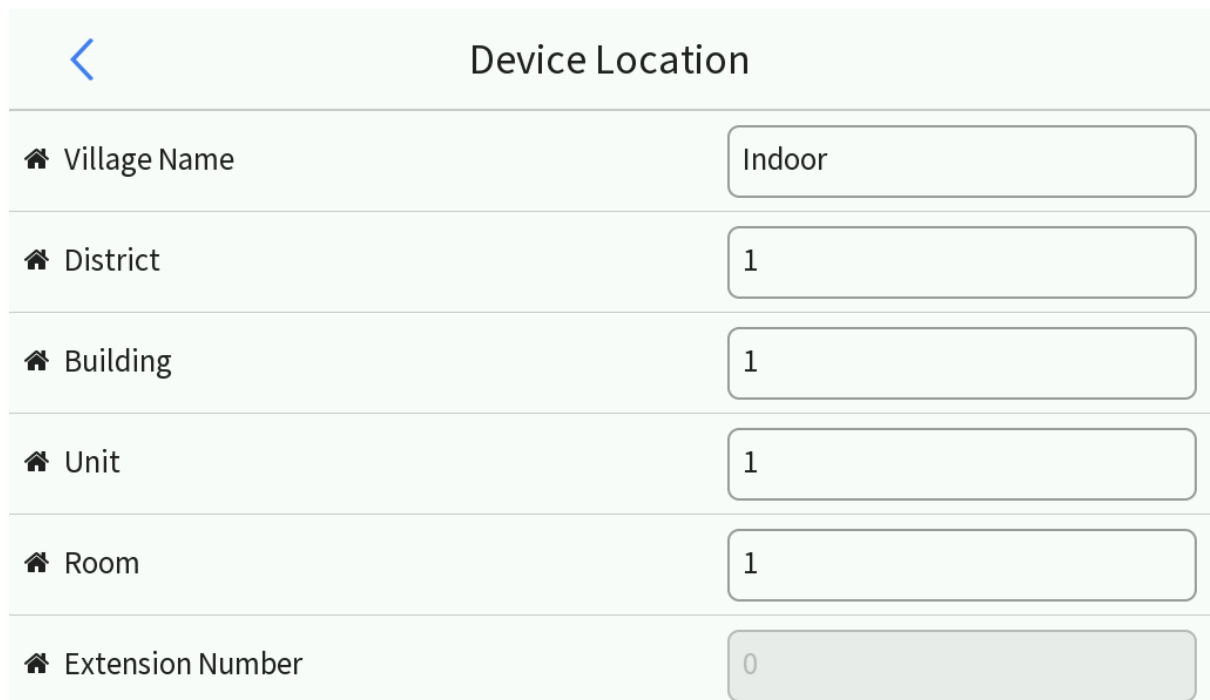
 NetWork Settings	
 Obtain Automatically(DHCP)	<input type="checkbox"/>
 Static IP	<input checked="" type="checkbox"/>
IP Address	<input type="text" value="192.168.1.100"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.1.1"/>
<input type="button" value="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**, and tap  beside **Device Location**.

Figure 9-14: Device Location-Main Station










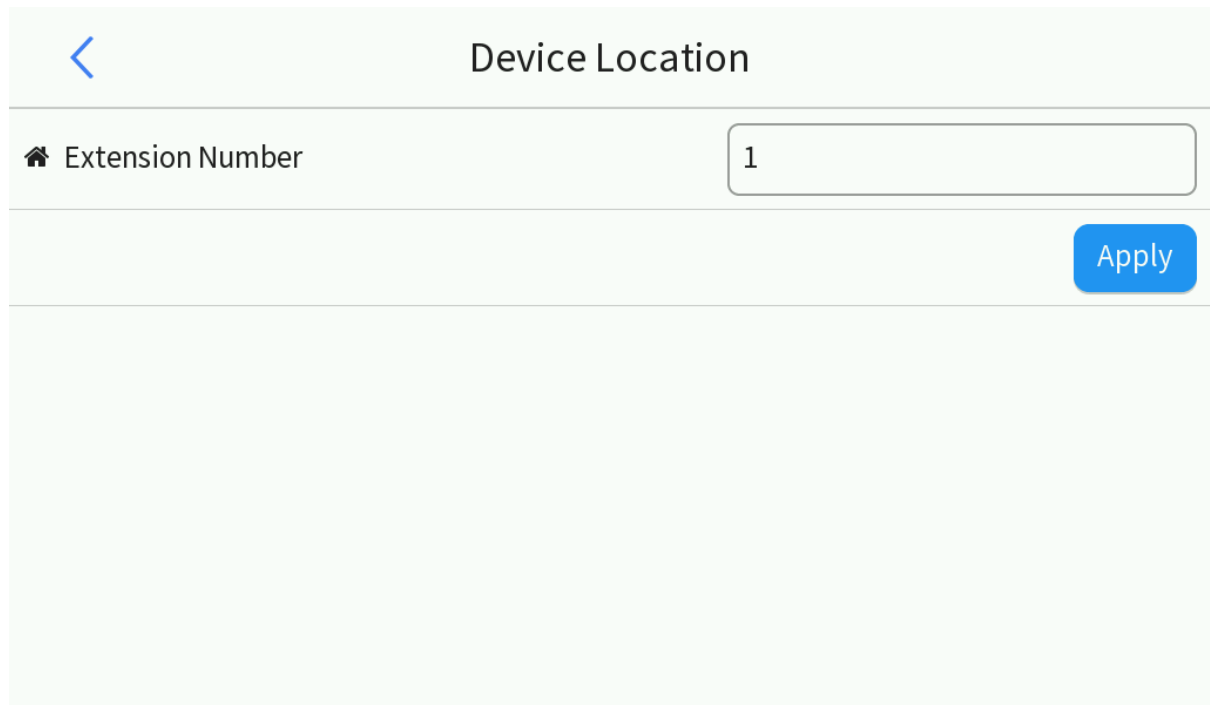
 Device Location	
 Village Name	<input type="text" value="Indoor"/>
 District	<input type="text" value="1"/>
 Building	<input type="text" value="1"/>
 Unit	<input type="text" value="1"/>
 Room	<input type="text" value="1"/>
 Extension Number	<input type="text" value="0"/>


Figure 9-15: Device Location-Extension



2. Set location parameters of the indoor station, including village name, extension number, district, building, unit, and room.


 **Note:**

- Extension number, district, building, and unit range: [0-99]; Room range: [0-9999].
- 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.

9.4.2 Device Mgmt

The device mgmt screen includes door station list, indoor station list, and door station auto search.

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

9.4.2.1 Door Station and IPC Management

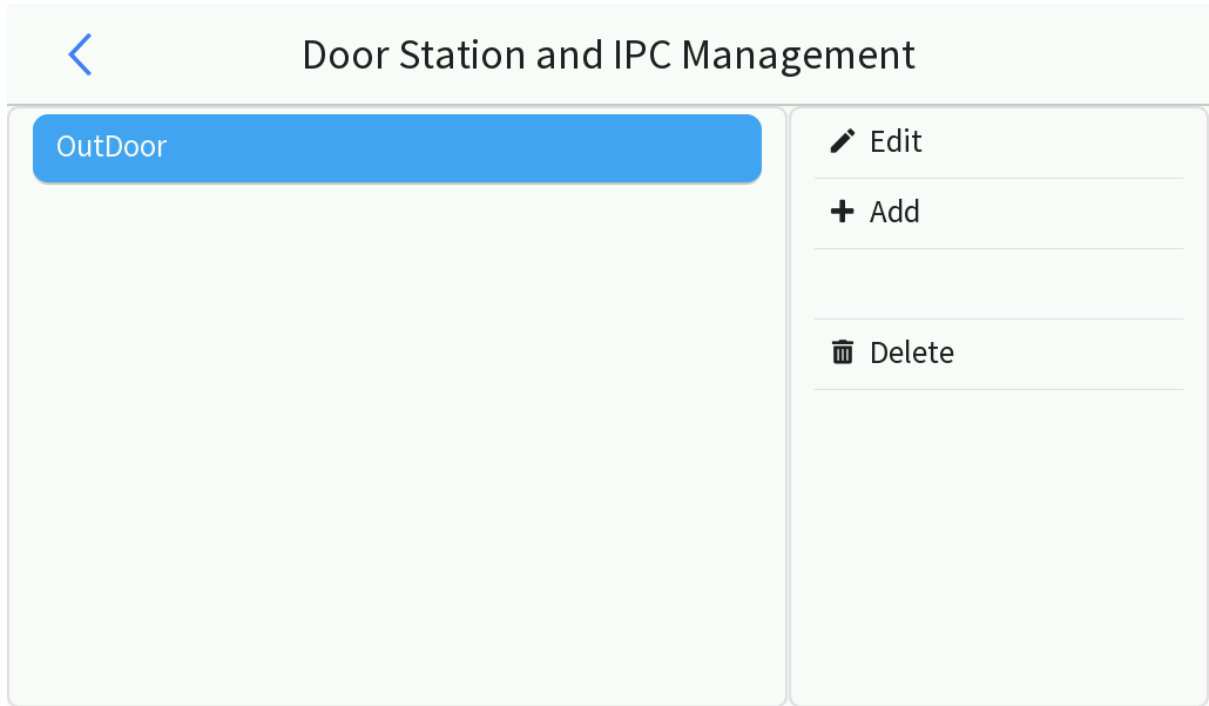
Set a face recognition terminal/door station/network camera so the indoor station can intercom with it, control it remotely, and open the door remotely. See [Live View](#) for details.

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

The [Door Station Auto Search](#) screen can automatically search for available door stations.

Tap , go to **Administration Configuration > Device Mgmt**, and tap  beside **Door Station and IPC Management**.

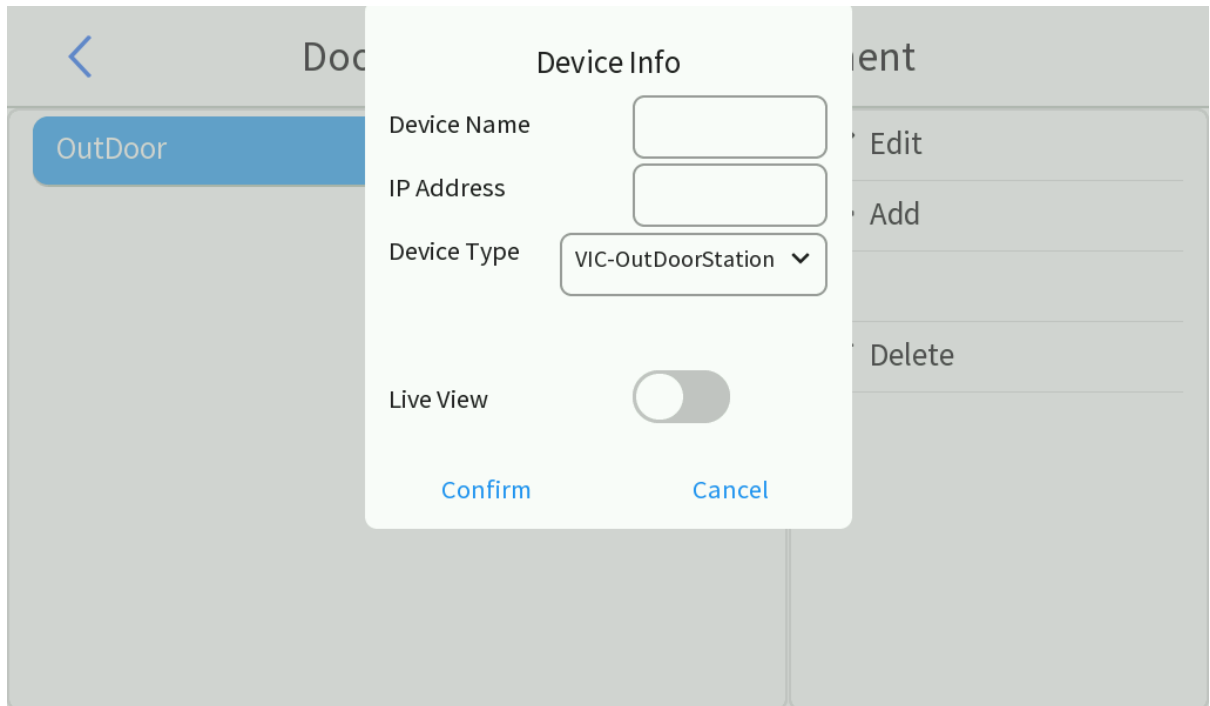
Figure 9-16: Door Station and IPC Management





Add

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

Figure 9-17: Add Door Station



2. Input device information. Some parameters are described below.
 - IP Address: Required. The IP address of the face 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 **VIC-OutDoorStation** for the face recognition terminal and door station; select **IPC** for the network camera.
 - Device Password (required only for **Device Type** as **VIC-OutDoorStation**): The password used to log in to the IPC's Web interface.

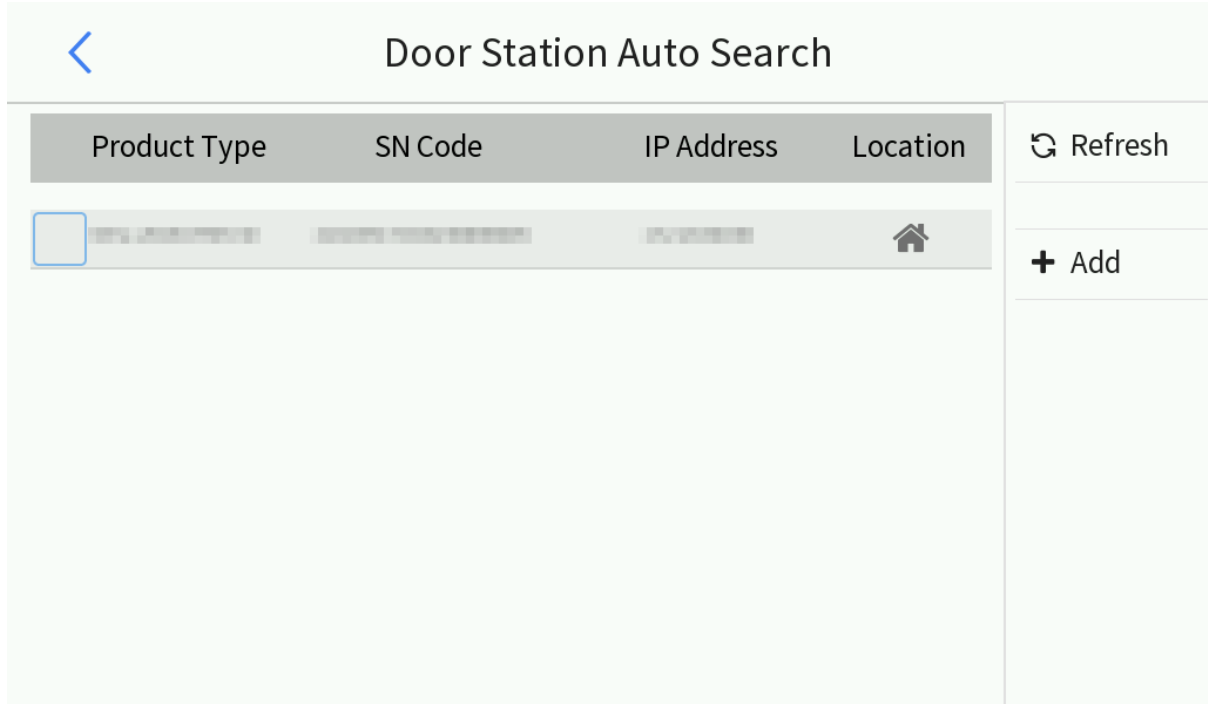
 **Note:**

- This function is available to the main indoor station.
- You can add door stations manually in [Door Station and IPC Management](#).

1. Tap , go to **Administration Configuration > Device Mgmt**, and tap  beside **Door Station Auto Search**.

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

Figure 9-20: Door Station Auto Search



2. Select the device you want to add.
3. Tap the IP address of the device(s) to be added, and set the corresponding network information, 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 9-21: Network Settings, Username, and Password

NetWork Settings

IP Address

Subnet Mask

Default Gateway

Username

Password

Confirm Cancel


4. Tap  beside the device to be added, and set the corresponding location information.
 - 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).
 - To add the device to the door station, set **Room** to 1 and make sure the extension number is unique.

Figure 9-22: Device Location


Device Location

Village Name Extension Number

District Building Unit Room


Confirm Cancel

5. Tap **Add**. A success message means the device has been added. You can view the added door stations in [Door Station and IPC Management](#), and added extensions in [Indoor Station Management](#). The added devices are named as **OutDoor** by default.

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

9.4.3 Main 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 [Device Mgmt.](#)

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

Figure 9-23: Main Station

The screenshot shows the 'Administration Configuration' screen. At the top, there is a back arrow and the title 'Administration Configuration'. Below this is a list of configuration items. The 'Main Station' item is highlighted in blue. It has a home icon and the label 'IP Address' next to an empty text input box. Below this, there is an 'Administrator Password' section with an empty text input box and a blue 'Apply' button to its right. At the bottom, there is a 'Device Maintenance' section.

2. Set the main station's name in the **Area** text box, with 1 to 32 characters.
3. Enter the main station's IP address.
4. 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 9-24: Administrator Password

The screenshot shows the 'Administration Configuration' screen. At the top, there is a back arrow and the title 'Administration Configuration'. Below this is a list of configuration items. The 'Administrator Password' item is highlighted in blue. It has a gear icon and the label 'Old Password' next to an empty text input box. Below this, there is a warning message: 'A strong password is required (9 to 32 characters including all three elements: digits, letters, and special characters)'. Below the warning, there are two more text input boxes: 'New Password' and 'Confirm', both with gear icons. At the bottom right, there is a blue 'Apply' button.

2. Enter the old password, new password, and confirm the password as required.

 **Note:** The new password must be 8 to 32 characters, containing at least three of the following types: uppercase letters, lowercase letters, digits, underscores, and hyphens.

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

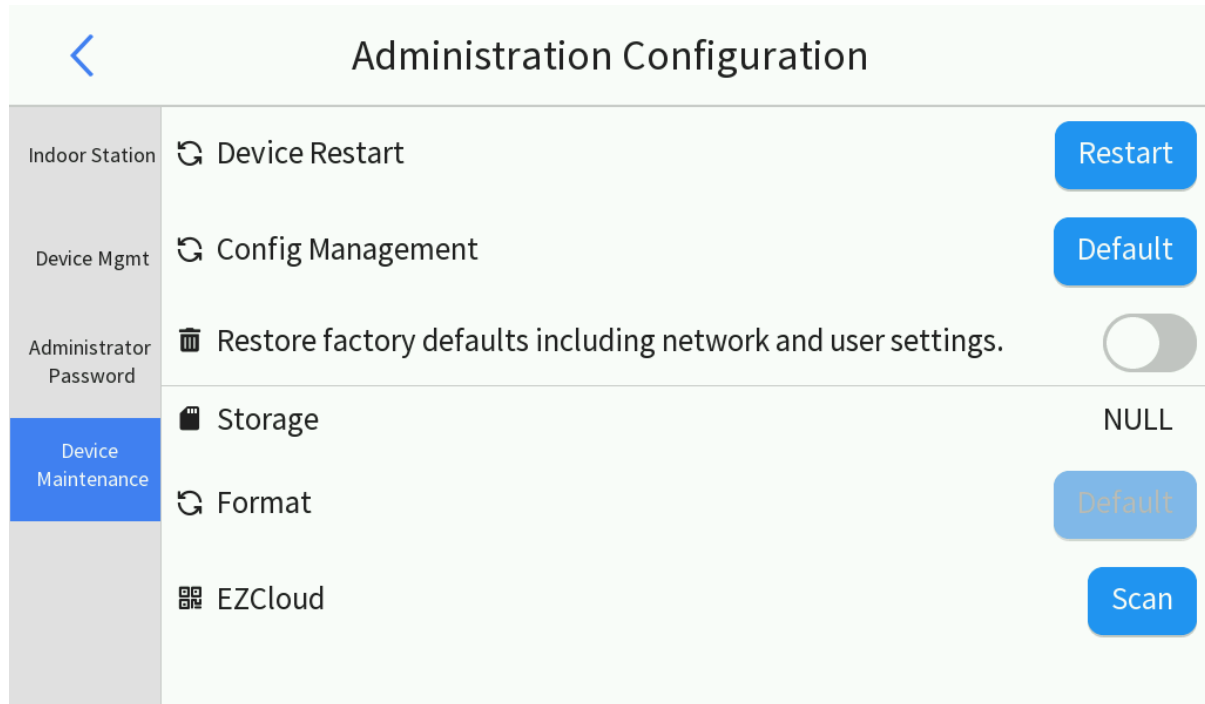
9.4.5 Device Maintenance



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 9-25: Device Maintenance



- Device Restart: Restart the indoor station. Tap , and then tap **Confirm** in the pop-up window to restart the indoor station.
- Config Management: 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 memory card is inserted into the device, the screen will display the memory card capacity. To set storage parameters, please see [Storage](#).
- Format: After a memory card is inserted into the device, tap **Default** to format the card.

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.

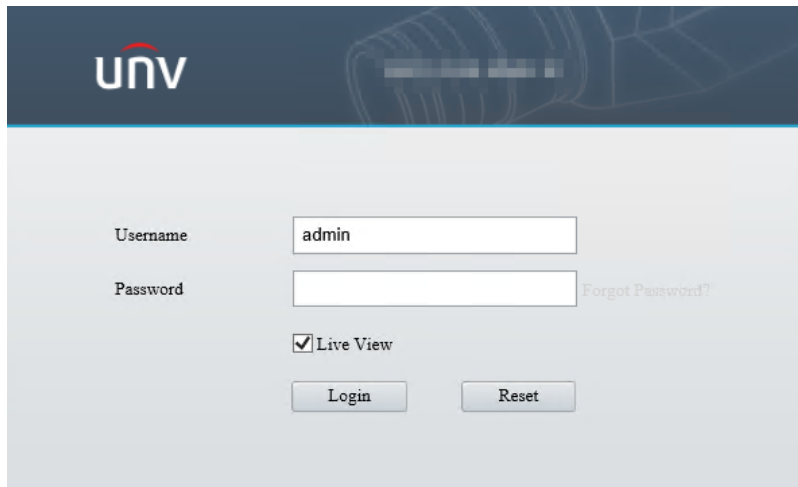
Log in to Web

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. For the indoor station, 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 password: 8 to 32 characters, including digits, letters, and special characters.
 - 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


<input checked="" type="checkbox"/> Parameter...	<input checked="" type="checkbox"/> Live View	<input checked="" type="checkbox"/> Playback	<input checked="" type="checkbox"/> Snapshot	<input checked="" type="checkbox"/> Two-way A...
<input checked="" type="checkbox"/> PTZ Control	<input checked="" type="checkbox"/> Event Subs...	<input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/> Maintenance	<input checked="" type="checkbox"/> 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

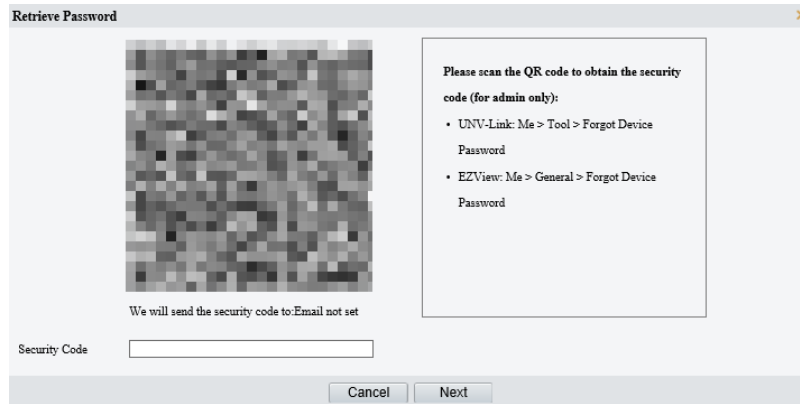
Forgot Password

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: Forgot 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.


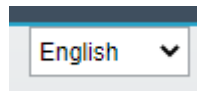

 **Note:** This function is only available to the indoor station.

Figure 10-7: Change Language



10.2 Live View

Play live video and audio.





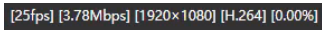



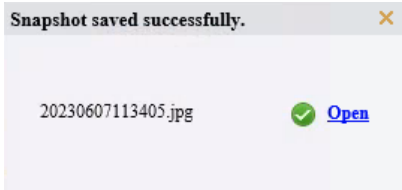

-  **Note:**
- This function is only available to the door station.
 - To view the live video, complete the following operations:
 - Select **Live View** on the **Login** page.
 - Follow the on-screen instructions to install a plug-in and run it successfully.








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"> • Scale: Displays 16:9 images. • Stretch: Displays images according to the window size (stretch images to fit the window). • Original: Displays images with original size.
Main Stream/Sub Stream	Select a live video stream according to the device.
Image & General Parameters	<p>Set General Parameters on the right to improve the live video effect.</p> <p>To view detailed parameters information or set more image parameters, click Image in the upper-right corner to enter the Image 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> Note: To set the output sound volume of the door station, please see Volume Control.</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 Open to view the folder where the snapshot is saved.</p>  <p> Note: See Local Parameters 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 Open to view the folder where the recording is saved.</p>  <p> Note: See Local Parameters 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"> • Left click and hold on the live view window and drag your mouse to specify the area (rectangular area) to be magnified. • Slide the mouse wheel up to zoom in on the image.
	<p>Enter full screen mode.</p> <p>To exit full screen mode, double-click in the live view window again or press Esc.</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

Add Person Library

Person Library Type: Employee Library

Person Library Name:

Check Template: None

Verify Success Linkage Configuration

Open door Voice Prompt

Verify Failure Linkage Configuration


Voice Prompt

OK Cancel


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 persons 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
Firmware Version			User
Hardware Version	A		
Boot Version	V2.3		
Serial No.			
Status			
System Time	2023/6/7 03:30:36		
Operation Time	0 Day(s) 1 Hour(s) 29 Minute(s)		
<input type="button" value="Refresh"/>			

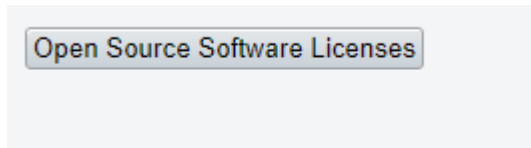
Common Configuration: Click the icon or text to quickly access the four common functions, including [Wired Network](#), [Time](#), [OSD](#), and [User](#).

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.

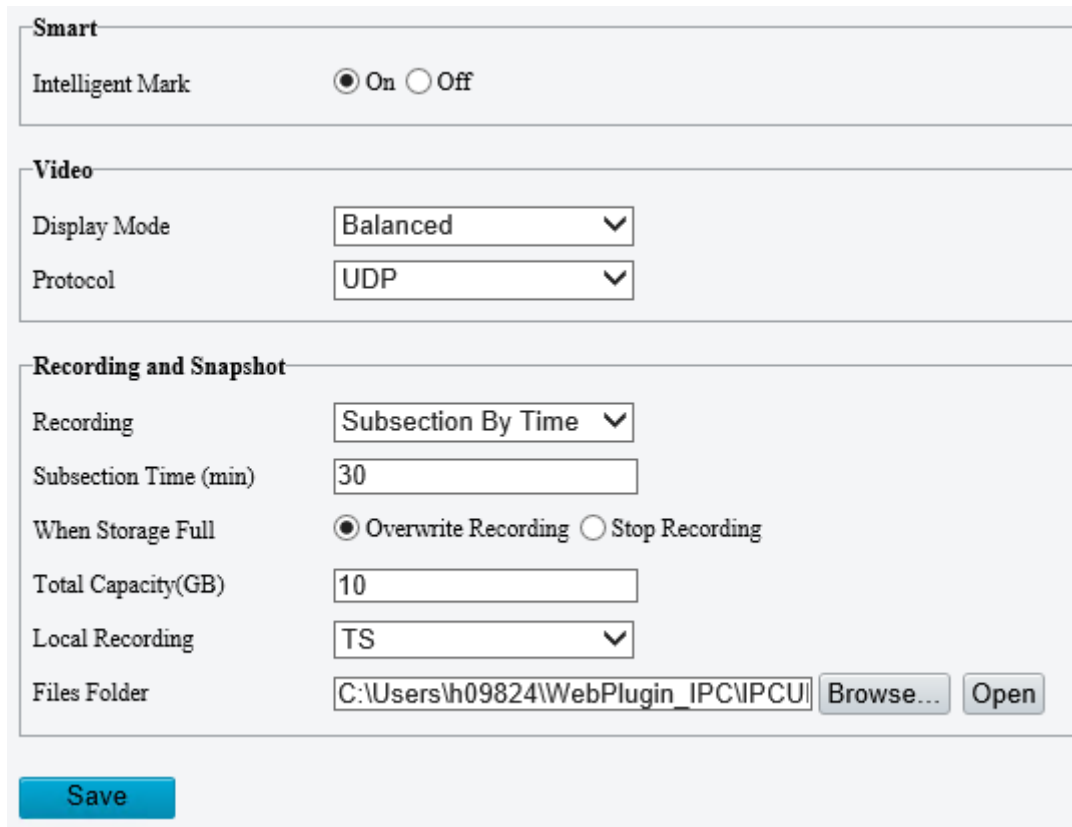
10.4.1.2 Local Parameters

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



2. Set the parameters as needed.

Parameter		Description
Video	Display Mode	Set the video display mode according to the network status including Min. Delay , Balanced (default), and Fluent (from low delay to high delay). You may also customize the display mode as needed.
	Protocol	Set the protocol used to transmit media streams. <ul style="list-style-type: none">• 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.• 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.

Parameter		Description
Recording and Snapshot	Recording	Mode to store the recording. <ul style="list-style-type: none"> Subsection By Time (default): Save recording files of the set subsection time. Subsection By Size: Save recording files of the set subsection size.
	Subsection Time (min)/ Subsection Size (MB)	<ul style="list-style-type: none"> Subsection Time (min): Available when Subsection By Time is selected. Range: [1-60], default: 30. Subsection Size (MB): Available when Subsection By Size is selected. Range: [10-1024], default: 100.
	When Storage Full	<ul style="list-style-type: none"> Overwrite Recording (default): When the local recording capacity is full, the oldest recordings are overwritten automatically. Stop Recording: When the local recording capacity is full, recording stops automatically.
	Total Capacity (GB)	Allocate storage capacity for local recording. Range: [1-1024], default: 10. The greater the value, the more the allocated recording storage capacity.
	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

The screenshot displays the 'Wired Network' configuration page. It is organized into three main sections: IPv4, IPv6, and Basic. In the IPv4 section, the 'Obtain IP Address' dropdown is set to 'DHCP'. The IPv6 section shows the 'Mode' dropdown set to 'DHCP'. The Basic section contains three fields: 'MTU' is a text input with '1500', 'Port Type' is a dropdown set to 'FE Port', and 'Operating Mode' is a dropdown set to 'Auto-negotiation'. At the bottom left, there is a prominent blue 'Save' button.

2. Configure wired network parameters.


Parameter		Description
IPv4	Obtain IP Address	<ul style="list-style-type: none"> Static: Configure a static public network IP address for the device manually. Set Obtain IP Address to Static, and enter the IP address, subnet mask, and default gateway. 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. Configure PPPoE (Point to Point Protocol over Ethernet) to assign the device a dynamic IP address to establish network connection. Set Obtain IP Address to PPPoE, and enter the username and password provided by your ISP (Internet Service Provider).
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 DHCP and Manual. The default mode is DHCP.</p>
Parameter	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>
	Operating Mode	<ul style="list-style-type: none"> 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. 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. (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.

3. Click **Save**.

10.4.1.4 Time

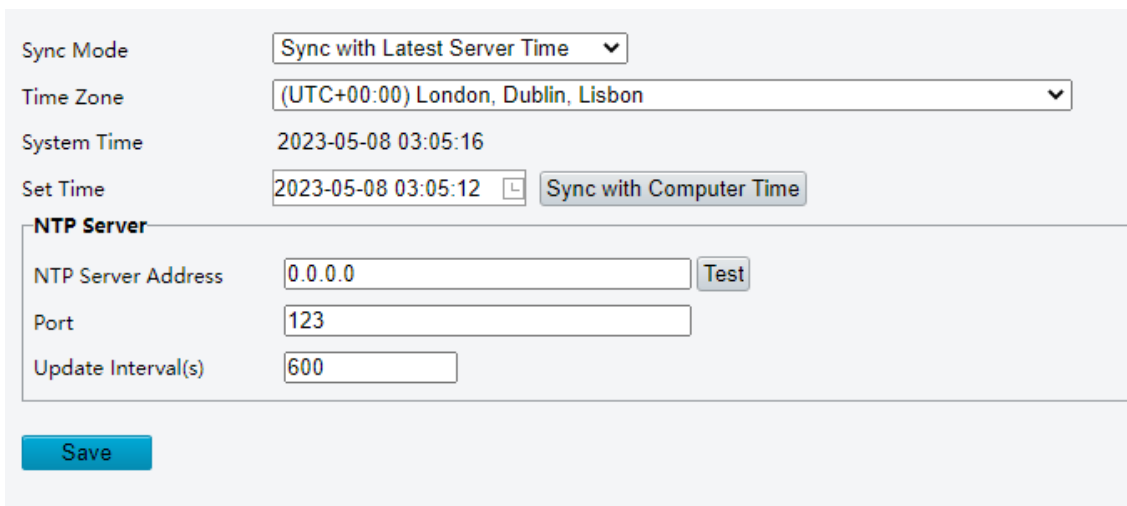
10.4.1.4.1 Time

Set the device time.

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

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

Figure 10-17: Time



Sync Mode: Sync with Latest Server Time

Time Zone: (UTC+00:00) London, Dublin, Lisbon

System Time: 2023-05-08 03:05:16

Set Time: 2023-05-08 03:05:12

NTP Server


NTP Server Address: 0.0.0.0

Port: 123

Update Interval(s): 600

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.
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: 5px 0;"> <p>NTP Server</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"> • NTP Server Address: Enter the NTP server address and click Test to check the network communication. A success message will appear if the NTP is verified successfully. • Port: Range: [1-65535], integer only, default: 123. • Update Interval (s): Range: [30-86400], integer only, default: 600.
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 EZCloud .

(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

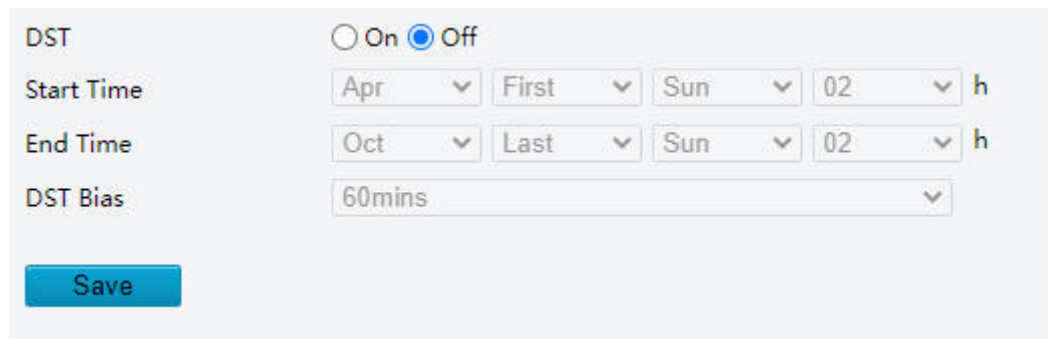
DST (Daylight Saving Time) is a local time system designed to make full use of daytime to save energy, which sets clocks forward by one hour in summer months.

By default, this function is disabled.

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

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

Figure 10-18: DST



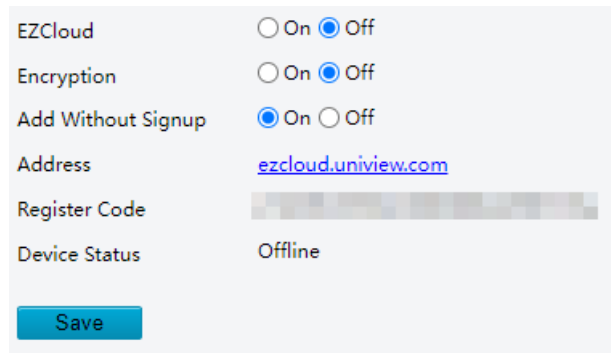
2. Enable **DST**.
3. Set the start time, end time, and DST bias.
4. Click **Save**.

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.

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

Figure 10-19: Indoor Station



EZCloud	<input type="radio"/> On <input checked="" type="radio"/> Off
Encryption	<input type="radio"/> On <input checked="" type="radio"/> Off
Add Without Signup	<input checked="" type="radio"/> On <input type="radio"/> Off
Address	ezcloud.uniview.com
Register Code	[Blurred]
Device Status	Offline

Save

Figure 10-20: Door Station



EZCloud	<input type="radio"/> On <input checked="" type="radio"/> Off
Encryption	<input type="radio"/> On <input checked="" type="radio"/> Off
Add Without Signup	<input checked="" type="radio"/> On <input type="radio"/> Off
Address	en.ezcloud.uniview.com
Register Code	[Blurred]
Device Status	Offline
Scan	

Save

1. Enable **EZCloud**.
2. Click **Save**.
3. Enter en.ezcloud.uniview.com in the address bar of a web browser, and then enter the **Login** page.
4. Click **Sign Up** and follow the on-screen instructions to create an account.
5. Log in to the EZCloud. Go to **Device Management > My Cloud Devices**, click **Add**, and then enter the register code.
6. Check device status.
 - EZCloud website: Go to **Device Management > My Cloud Devices** to check whether the device is online.
 - Device's Web interface: Go to **Setup > Network > EZCloud** to check whether the device is online.

10.4.1.6 OSD

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

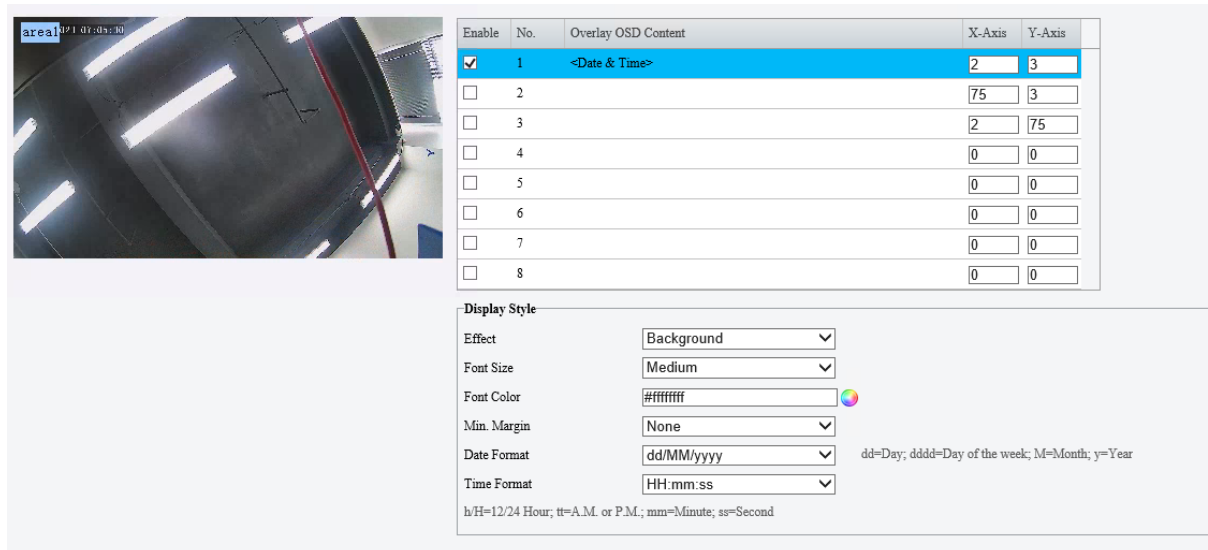


Note:

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

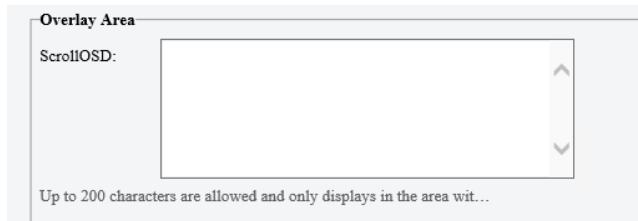
1. Go to **Setup > Common > OSD**.

Figure 10-21: OSD



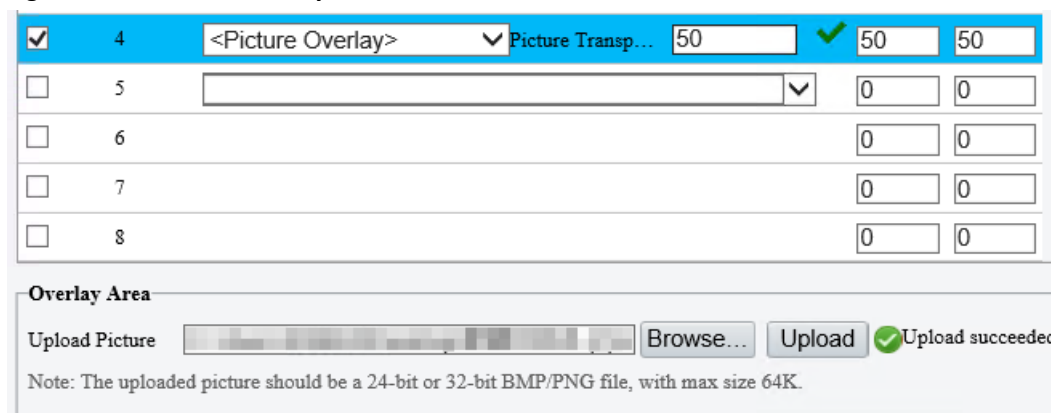
- To enable an OSD, select the check box in the **Enable** column, and then the OSD area will be displayed on the live video (OSD name format: area + OSD number, for example, area 1).
- Set the OSD content you want to overlay.
 - Custom: 0 to 40 characters are allowed.
 - Date & Time/Time/Date: Overlay 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 10-22: 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 10-23: Picture Overlay



- 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.
- 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.

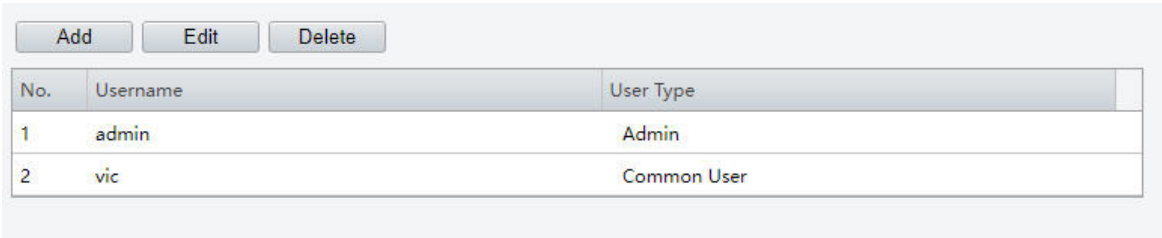
The user types are described below.

- 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 10-24: User



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

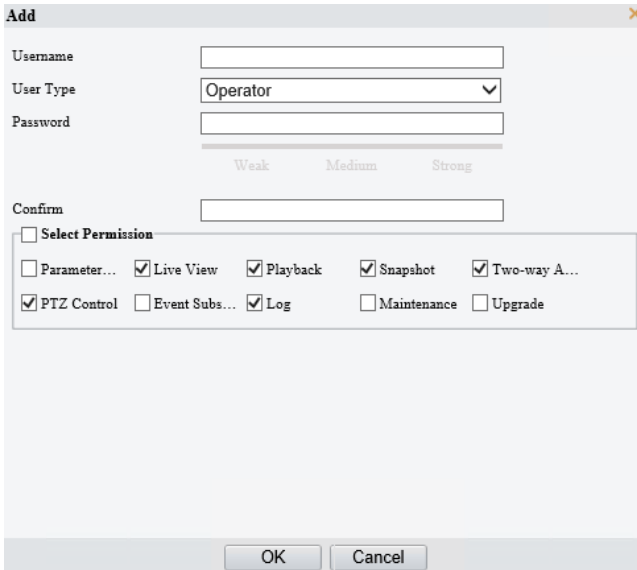
Add User

 **Note:**

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

1. Click **Add**.

Figure 10-25: Add Operator



Add

Username:

User Type:

Password:

Weak Medium Strong

Confirm:

Select Permission

Parameter... Live View Playback Snapshot Two-way A...

PTZ Control Event Subs... Log Maintenance Upgrade


OK Cancel

Figure 10-26: 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.
- Permissions:** Two sub-checkboxes: "Live View" (checked) and "Playback" (unchecked).
- 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 via 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**.

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.

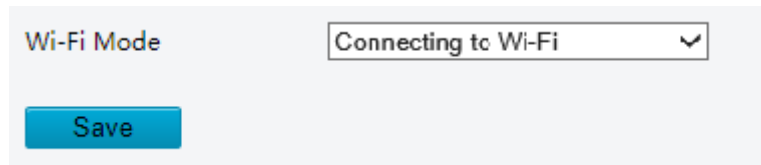
10.4.2.1.2 Wi-Fi

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

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


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

Figure 10-27: Wi-Fi



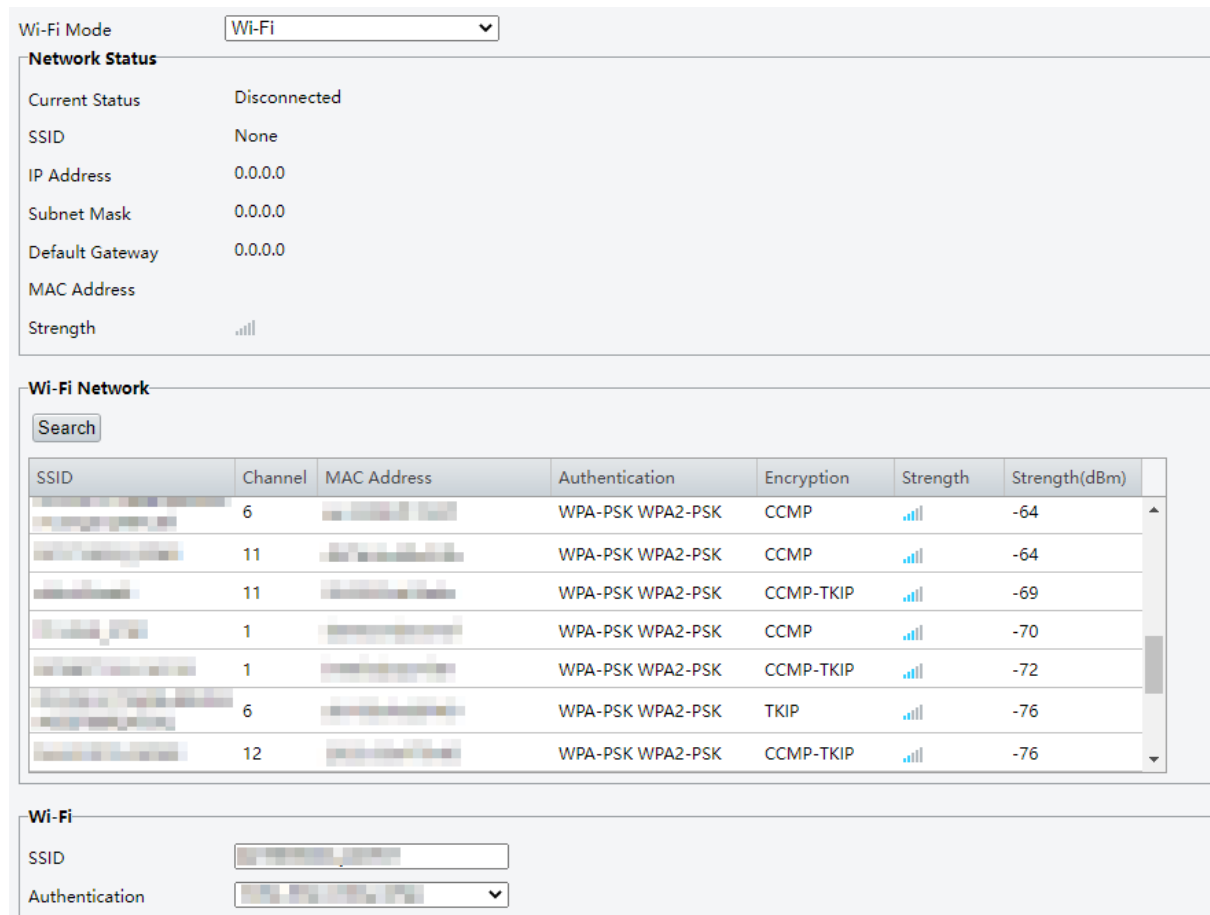
The Wi-Fi mode is **Connecting to Wi-Fi** by default, so as to prompt the user to connect to Wi-Fi

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 10-28: Wi-Fi



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 10-29: Select Wi-Fi

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

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

Figure 10-30: 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 10-31: Connected Wi-Fi

Network Status	
Current Status	Connected
SSID	thd2
IP Address	...
Subnet Mask	...
Default Gateway	...
MAC Address	...
Strength	...

Enable Wi-Fi Hotspot

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

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

Figure 10-32: 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 10-33: 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 10-34: 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 10-35: 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.
 - MyDDNS: Enter a domain name, and then click **Test** to check its validity.
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 10-36: 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 10-37: Port Mapping

Port Mapping On Off

Save

2. Enable **Port Mapping**.

Figure 10-38: Enable Port Mapping

Port Mapping On Off

Mapping Type

UPnP Mapping


Port Type	External Port	External IP Address	Status
HTTP Port	80	0.0.0.0	Inactive
RTSP Port	554	0.0.0.0	Inactive
HTTPS Port	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 10-39: 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**.

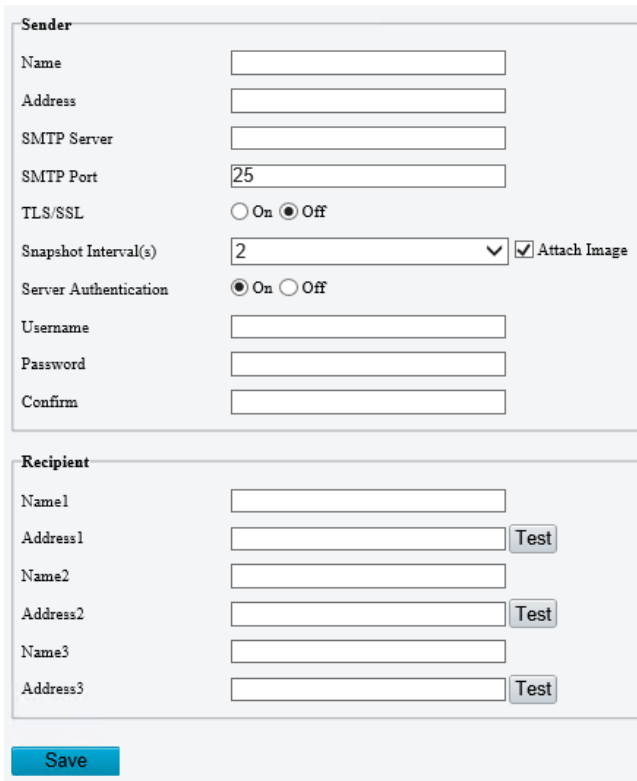
10.4.2.2 Service Config

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 10-40: 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 10-41: 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 10-42: 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

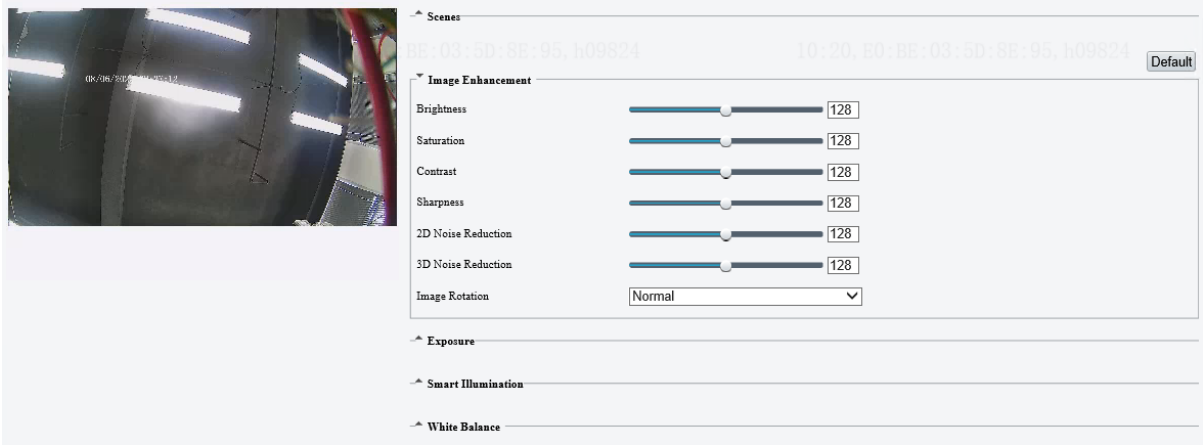
10.4.3.1 Image

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 10-43: Image



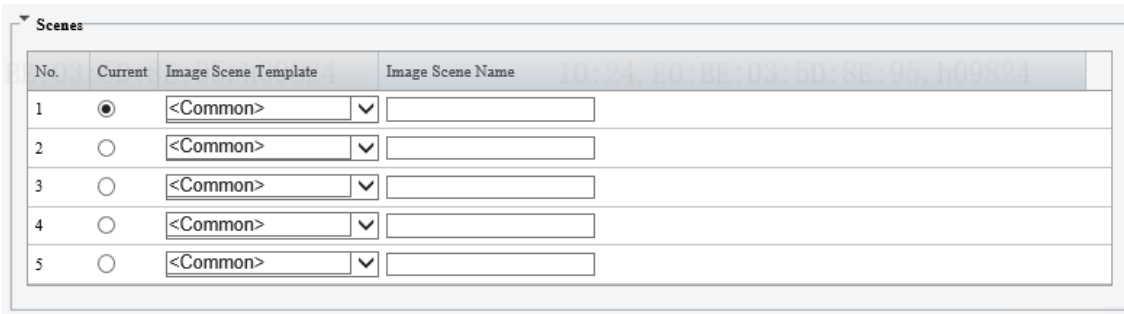
2. Set the image scenes.

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 10-44: 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.


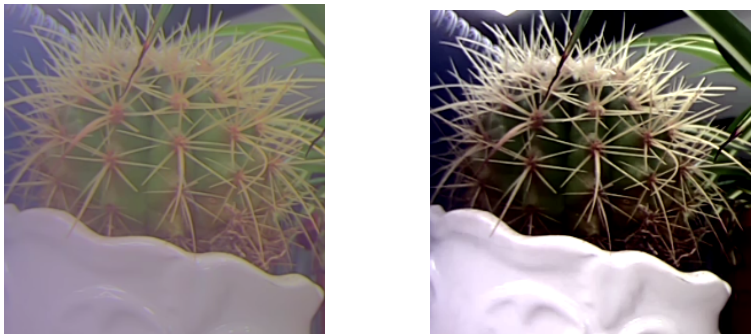
(3) Set the image scene name, which will be used in [Image Scene Switch](#).






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	The overall lightness or darkness of the image.
	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;">  <p>Low brightness</p> </div> <div style="text-align: center;">  <p>High brightness</p> </div> </div>

Parameter		Description
	Saturation	The intensity or vividness of colors in the image.
		 <p style="text-align: center;">Low saturation High saturation</p>
	Contrast	The black-to-white ratio in the image, that is, the gradient of color from black to white.
	Sharpness	 <p style="text-align: center;">Low contrast High contrast</p>
		The definition of edges in the image.
	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"> • Automatic: The door station automatically adjusts the exposure parameters based on the environment. • Custom: User can set exposure parameters as needed. • Shutter Priority: The device adjusts shutter as priority to adjust the image quality. • Indoor 50Hz/60Hz: Reduce stripes by limiting shutter frequency. • Manual: Fine-tune image quality by setting shutter and gain manually.

Parameter	Description
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> Note:</p> <ul style="list-style-type: none"> This parameter is configurable when Exposure Mode is set to Manual. The minimum and maximum time can be configurable when Exposure Mode is set to Custom. If Slow Shutter is disabled, the reciprocal of the shutter speed must be greater than the frame rate.
Gain	<p>Control image signals so that the device can output standard video signals in different light conditions.</p> <p> Note: This parameter is configurable when Exposure Mode is set to Manual or Custom. The minimum and maximum gain value can be configurable when Exposure Mode is set to Custom.</p>
Slow Shutter	<p>When enabled, the device can improve image brightness in low light conditions.</p>
Slowest Shutter	<p>Set the slowest shutter speed for exposure.</p>
Compensation	<p>Adjust the compensation value as required to achieve the desired image effect. The valid range is -100 to 100. The default is 0.</p> <p> Note: This parameter is configurable when Exposure Mode is not set to Manual.</p>
Metering Control	<p>Set how the door station measures the intensity of light.</p> <ul style="list-style-type: none"> Center-Weighted Average Metering: Measure light mainly in the central part of the image. Evaluative Metering: The device measures light mainly in the central part of the image. Face Metering: The device adjusts the image quality in poor lighting or backlighting conditions by controlling the brightness of captured faces in face scenes. Smart Metering: The device obtains an accurate exposure by weighting according to the exposure and importance of each area on the whole image. <p> Note: This parameter is configurable when Exposure Mode is not set to Manual.</p>
Day/Night Mode	<ul style="list-style-type: none"> Automatic: The device automatically switches between day mode and night mode according to the ambient lighting condition to output optimum images. Day: The device outputs high-quality images in daylight conditions. Night: The device outputs high-quality images in low-light conditions. 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 N.O., the device is on the day mode; if the alarm type is set to N.C., the device is on the night mode.
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> Note: This parameter is configurable when Night Mode is not set to Manual.</p>

Parameter		Description
	Day/Night Switching(s)	Set the length of time before the camera switches between day mode and night mode after the switching conditions are met.  Note: This parameter is configurable when Day/Night Mode is set to Automatic .
	WDR	Enable WDR to ensure clear images in high contrast conditions.  Note: This parameter is configurable when Exposure Mode is not set to Manual .
	WDR Level	When WDR is enabled, you can adjust the WDR level to improve image quality. The valid range is 1 to 9. The default is 5.  Note: 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.
	WDR Open/Close Sensitivity	When WDR is set to Automatic , adjust the parameter to change the WDR switching sensitivity. The valid range is 1 to 9. The default is 5.
Smart Illumination	Illumination Mode	Infrared: The device uses infrared light illumination.
	Control Mode	Global Mode: The device automatically adjusts illumination and exposure to achieve the balanced image effect. Some areas might be overexposed if you select this option. This option is recommended if you focus on the monitoring range and image brightness.
	Illumination Level	Default: 500. The greater the value, the higher the intensity.
White Balance	White Balance	<ul style="list-style-type: none"> • Auto/Auto 2: Automatically adjust the red and blue gains according to the lighting conditions. If there are still color casts in Auto mode, try Auto 2 mode. • Outdoor: Recommended for outdoor scenes where the color temperature varies widely. • Fine Tune: Allows user to manually adjust red and blue offsets. • Fine Tune (Base on night mode): Allows user to adjust red and blue offsets manually to adapt to poor lighting conditions. • Sodium Lamp: Automatically adjust the red and blue gains for optimal color reproduction in sodium light sources. • Locked: Keep the current color temperature.
	Red/Blue Offset	Adjust the red offset or blue offset manually.  Note: This parameter is configurable when White Balance is set to Fine Tune .

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 10-45: 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<>

Save

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.

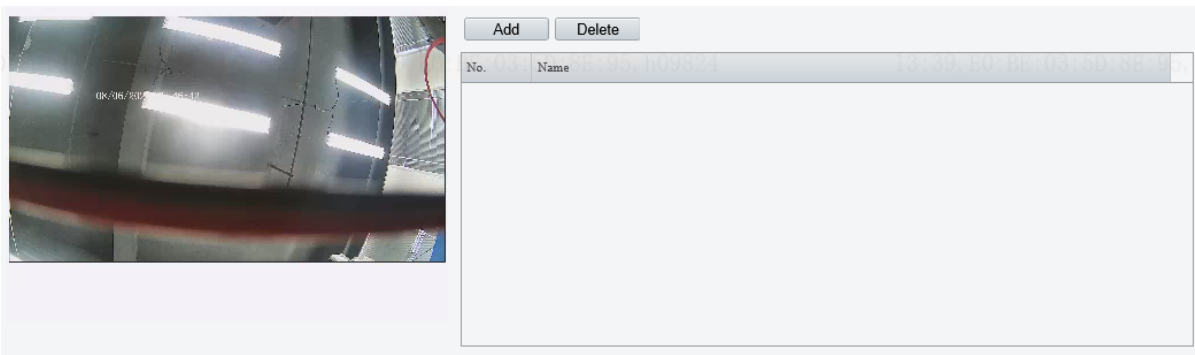
10.4.3.3 Privacy Mask

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 10-46: 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 10-47: Check Template


The screenshot shows the 'Check Template' configuration page. On the left, there is a list of templates with 'default' selected. The main area is titled '*Template Name' and shows a table with columns for days of the week (Mon, Tue, Wed, Thu, Fri, Sat, Sun). Below the table, there are eight rows for 'Time Interval1' through 'Time Interval8'. Each row has two time input fields (e.g., '00:00:00' and '23:59:59') and a dropdown menu for authentication mode (e.g., 'Card'). At the bottom, there is a 'Copy To' section with checkboxes for each day and a 'Copy' button. A 'Save' button is at the bottom left.

Add

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

Figure 10-48: Empty Check Template


The screenshot shows the 'Empty Check Template' configuration page. It is similar to Figure 10-47 but with an empty template selected. The table for Time Intervals and authentication modes is present but mostly empty. The 'Copy To' section has checkboxes for each day, with 'Mon' checked. A 'Copy' button is at the bottom right. 'Save' and 'Cancel' buttons are at the bottom left.

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 10-49: Time Template

Enable time template verific... On Off

Refre... Add Delete

default

*Template Name default

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

EnableException Date

Save

Add

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

Figure 10-50: Empty Time Template

*Template Name

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

EnableException Date

Save Cancel

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 10-51: 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 10-52: 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 10-53: 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

10.4.5.1 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 10-54: Tamper Alarm

Alarm Name

Alarm ID

Alarm Type

Alarm Input On Off

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. 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 **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 10-55: Storage

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

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

4. 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.

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

Figure 10-56: HTTPS

2. Enable **HTTPS**.
3. 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**.

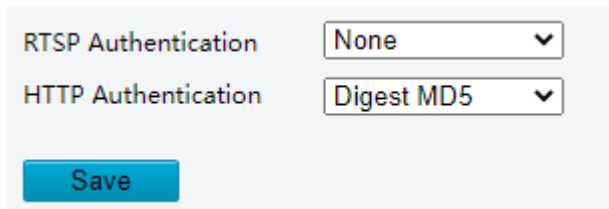
10.4.7.2.2 Authentication

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 10-57: Authentication



2. Choose an authentication mode.

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

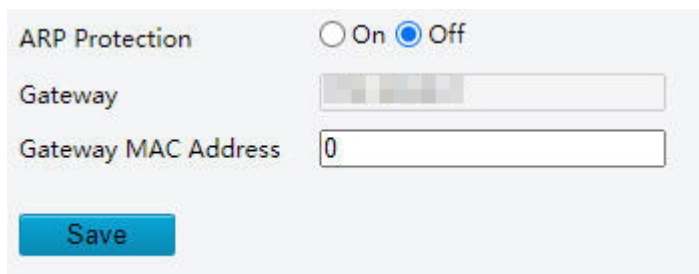
3. Click **Save**.

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 10-58: ARP Protection



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 10-59: 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 10-60: 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 10-61: Certificate Management

The screenshot displays the Certificate Management interface, divided into two main sections: "Certificate" and "CA Certificate".

Certificate Section:

- Buttons: Create Self-Signed Certificate, Create Certificate, Import Certificate, Export Certificate, Delete Certificate, Certificate Properties.
- Table:

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:

- Buttons: Import Certificate, Delete Certificate, Certificate Properties.
- Table:

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 10-62: Create Self-Signed Certificate

Create Self-Signed Certificate [Close]

Certificate Name

Public Key

Country Example:CN

Domain Name/IP

Valid Period(day)

Province

City

Organization

Organizational Unit

Email

[OK] [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 10-63: Create Certificate

Create Certificate [Close]

Country Example:CN

Domain Name/IP

Province


City

Organization

Organizational Unit

Email

[OK] [Cancel]

 **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 10-64: Import Certificate

Import Certificate

Import Format: Certificate+Private Key

Certificate Name:

Certificate: Browse...

Private Key: Browse...

Private Key Password:

OK Cancel

- 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 10-65: Import Certificate

Import Certificate

Certificate Name:

Certificate: Browse...

OK 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

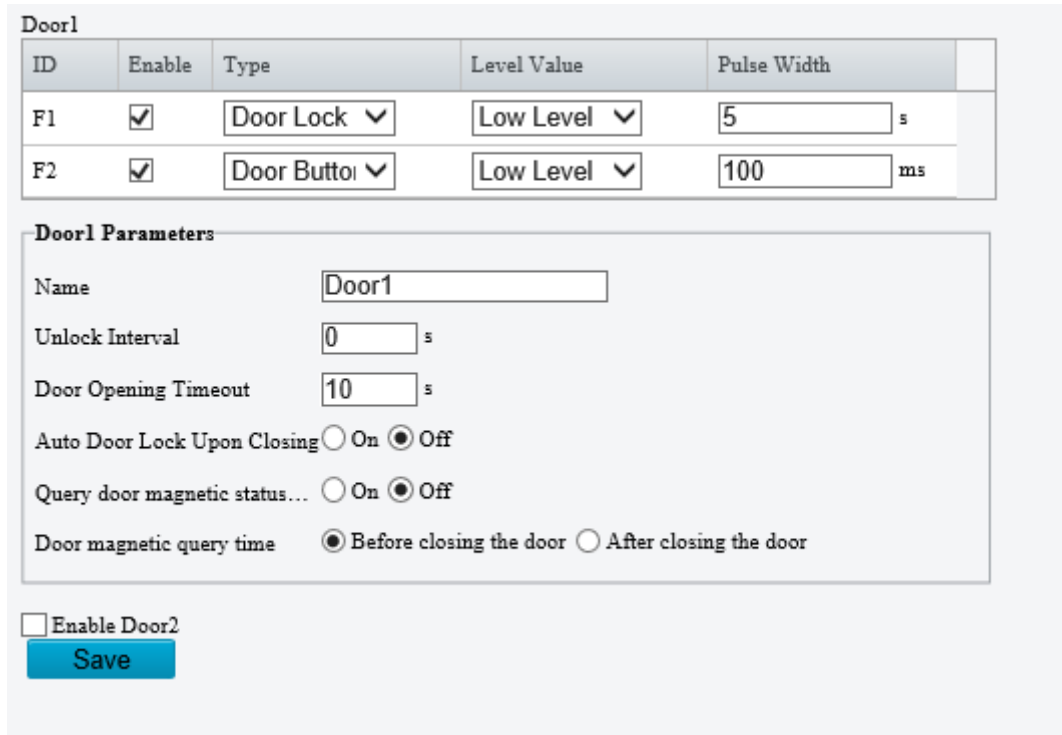
 **Note:** This function is only available to the door station.

10.4.8.2.1 General Config

Configure door locks, door buttons, and alarm output devices connected to the door station.

1. Go to **Setup > System > Ports & Devices > General Config**.

Figure 10-66: General Config



ID	Enable	Type	Level Value	Pulse Width
F1	<input checked="" type="checkbox"/>	Door Lock	Low Level	5 s
F2	<input checked="" type="checkbox"/>	Door Button	Low Level	100 ms

Door1 Parameters

Name:

Unlock Interval: s

Door Opening Timeout: s

Auto Door Lock Upon Closing: On Off

Query door magnetic status...: On Off

Door magnetic query time: Before closing the door After closing the door

Enable Door2

2. (Optional) **Door Lock**, **Door Button**, and **Alarm Output** are enabled by default. To disable these functions, clear the corresponding check box(es).
3. Set the level value. It must be consistent with the input and output signal level value of the external device.
4. Set the pulse width.
 - Door lock pulse width: The duration of a single door opening. The door lock automatically locks when the door opening time exceeds the set time.
Range: [1-300]s, integer only. Default: 5s.
 - Door button pulse width: The door button outputs a door opening signal after being pressed for the set time.
Range: [0-20000]ms, integer only. Default: 100ms.
 - Alarm output pulse width: The duration of the alarm output signal.
Range: [0-20000]ms, integer only. Default: 100ms.
5. Configure other parameters.
 - Name: **Door 1** by default. It can be named as needed, and must be unique.
 - 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.

6. To enable the second door, select **Enable Door2**, and configure other parameters as the above description.
7. Click **Save**.

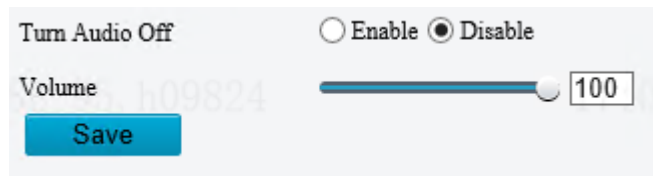
10.4.8.2.2 Volume Control

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 10-67: Volume Control



2. Select whether to turn audio off. If **Turn Audio Off** is disabled, you can adjust the volume. Range: [0-100], integer only. Default: 100.
3. Click **Save**.

10.4.8.3 Maintenance

10.4.8.3.1 Maintenance

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

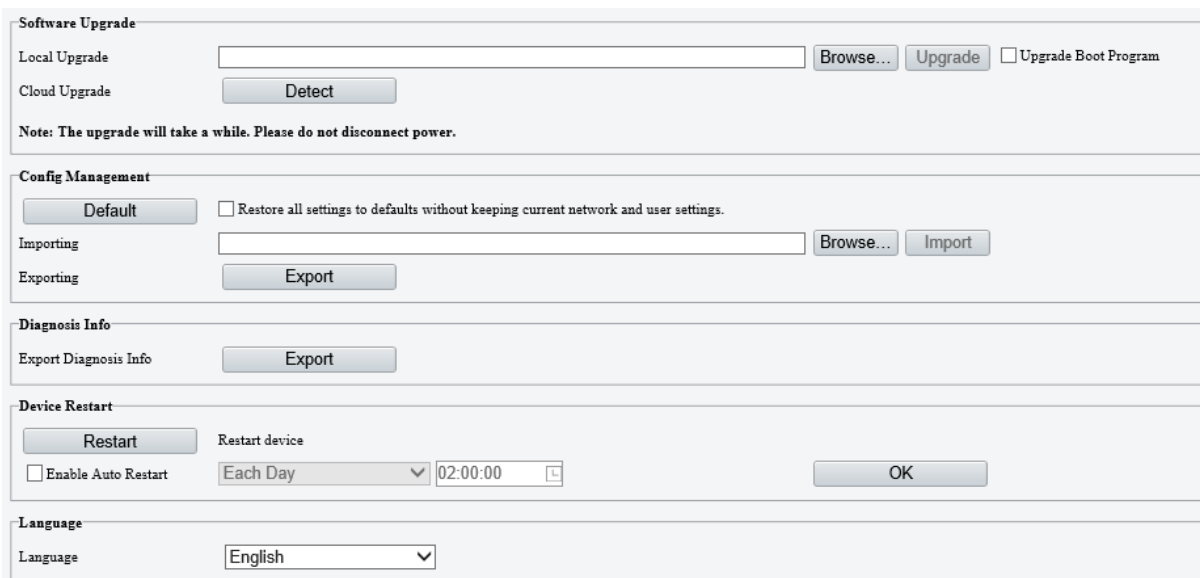
 **Note:**

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

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

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

Figure 10-68: Indoor Station



Note: 1. Software upgrade, system restart, restore default configuration, import configuration, import personnel library operation and change system language operation will restart the device.
2. Restarting the device will interrupt the connection to the device.

Figure 10-69: Door Station

Software Upgrade

Local Upgrade Upgrade Boot Program

Cloud Upgrade

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

Config Management

Restore all settings to defaults without keeping current network and user settings.

Importing

Exporting

Storage Medium

Diagnosis Info

Export Diagnosis Info

Collect Image Debugging Info

Device Restart


Restart device

Enable Auto Restart

Note:
 1. Software upgrade, device restart, restoration to defaults or configuration import will restart the device.
 2. Restarting the device will interrupt the connection to the device.

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 10-70: 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.

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 10-71: Indoor Station

Config Management

Restore all settings to defaults without keeping current network and user settings.

Importing

Exporting

Figure 10-72: Door Station

Config Management

Restore all settings to defaults without keeping current network and user settings.

Importing


Exporting

Storage Medium

- 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 10-73: Indoor Station

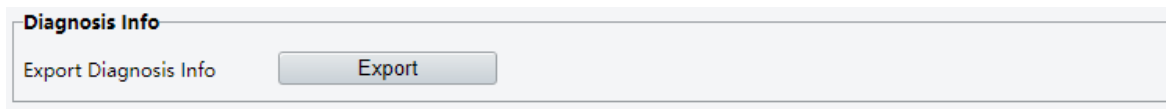


Figure 10-74: Door Station



- 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.


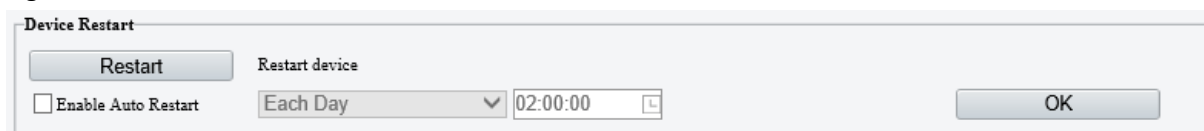
 **Note:** Restarting the device will interrupt the ongoing services.

Figure 10-75: Device 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.

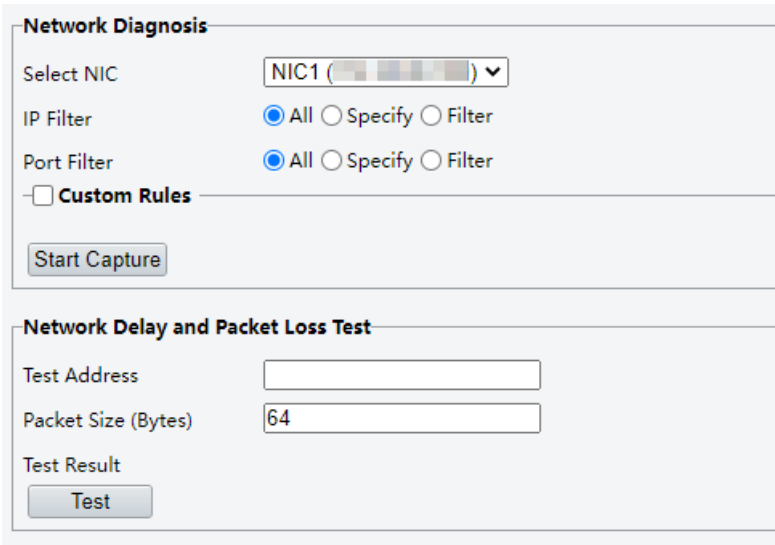
1. Select **Chinese Simplified** from the **Language** drop-down list.
2. Click **OK** to confirm the selection.

10.4.8.3.2 Network Diagnosis

Diagnose the NIC and network latency.

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

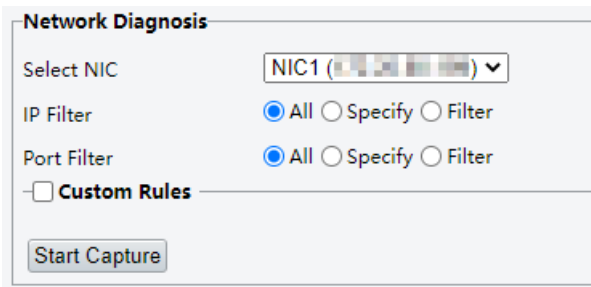
Figure 10-76: Network Diagnosis




Network Diagnosis

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

Figure 10-77: Network Diagnosis



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 10-78: Packet Loss Test


Network Delay and Packet Loss Test

Test Address

Packet Size (Bytes)

Test Result

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 10-79: Log


Time ~

Main Type Sub Type

Operation

No.	Type	Sub Type	Date	Time	Username	IP	Result
Total . << < 1 / > >>							

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.