

Video Intercom Main Station

User Manual

V1.00

Contents

Disclaimer and Safety Warnings.....	1
Preface.....	1
Legal Statement.....	2
Safety Warnings.....	3
1 Defaults.....	6
2 Introduction.....	6
3 Call.....	7
3.1 Call Main Station.....	7
3.2 Call Resident.....	8
3.3 Call Records.....	10
4 Answer.....	10
5 Live View.....	11
5.1 View Live Video of Unit Door Station.....	11
5.2 View Live Video of Zone Station.....	13
6 Message.....	14
6.1 Alarm.....	14
6.2 Snapshot.....	15
7 Settings.....	15
7.1 Personalization.....	15
7.2 Volume Settings.....	16
7.3 User Settings.....	19
7.4 Administrator Configuration.....	19
7.4.1 Administrator Password.....	20
7.4.2 Network Settings.....	20
7.4.3 System Maintenance.....	21
7.5 System Language.....	22
7.6 Date & Time Settings.....	22
7.7 System Information.....	22

Disclaimer and Safety Warnings

Preface

The purpose of this section is to ensure that users correctly utilize the product to prevent dangers caused by improper operation or property damage. Before using this product, please read this manual carefully and keep it properly for future reference.

About This Manual

- This manual is for use with multiple product models; we apologize for not listing the appearance and functions of each product individually. Please refer to your actual product for use.
- This manual is compatible with multiple software versions. The product interface and functions should be based on the actual software.
- Despite our best efforts, the content of this manual may contain technical or printing errors. Final interpretation resides solely with us.
- Please follow the operating instructions in this manual. Any losses caused by not following the guidance in this manual are the responsibility of the user.
- We reserve the right to modify the content of this manual without notice. Due to product version upgrades or regulatory requirements in relevant regions, the content of this manual will be updated periodically, and the updated content will be reflected in the new version.
- This manual will be updated in real time according to the laws and regulations of relevant regions. Please refer to the product's paper copy, QR code, or official website for details. If there is any inconsistency between the paper copy and the electronic version, the digital version shall prevail.

About the Product

If the product you have chosen is a video product, please strictly adhere to the applicable laws and regulations. You can visit our official website to inquire about the relevant content.

User Guidelines

- This document serves as a guide for use only. All statements, information, and suggestions in this document do not constitute any express or implied warranty.
- We assume no responsibility for any special, incidental, consequential, or indirect damages resulting from the use of this manual or the use of our products, including but not limited to loss of business profits, loss of data or documents, and abnormal product operation or information leakage caused by cyber-attacks, hacker attacks, or virus infections.
- Due to uncertain factors such as the physical environment, there may be discrepancies between the actual values of some data and the reference values provided in the manual. If there are any questions or disputes, our final interpretation shall prevail.

Formatting Conventions

The UI formatting conventions used in this document are as follows:

Format	Meaning
>	Indicate a sequence of actions, e.g., click Device Management > Add Device, which means first click Device Management, and then click Add Device.

Symbol Conventions

This document uses various distinctive symbols to highlight contents that require special attention during the operation process. The meanings of these symbols are as follows:

Symbol	Meaning
	NOTE: Provides tips and additional information related to the operation and use of the product.
	CAUTION: Alerts to matters that require attention during operation, as improper handling may lead to product damage, data loss, or functional abnormalities.
	WARNING: The annotations following this symbol demand extra attention, as improper handling could potentially cause personal injury.

Legal Statement

Copyright Statement

2026 Zhejiang Uniview Technologies Co., Ltd. All rights reserved.

The copyright of any part of this document, including text, images, graphics, etc., belongs to Zhejiang Uniview Technologies Co., Ltd (referred to as Uniview, we, us, our company, hereafter). Without our written permission, no organization or individual may copy, reproduce, translate, modify any part or all of the content of this manual without authorization, nor may they disseminate it in any form.

The product described in this manual may contain proprietary software owned by our company and its possible licensors. Unless permitted by 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.

Trademark Acknowledgements

 are trademarks or registered trademarks of Uniview.

All other trademarks, products, services and companies in this manual or the product described in this manual are the property of their respective owners.

Export Compliance Statement

We comply with applicable export control laws and regulations worldwide, including that of the People's Republic of China and the United States, and abide by relevant regulations relating to the export, re-export and transfer of hardware, software and technology. Regarding the product described in this manual, we ask you to fully understand and strictly abide by the applicable export laws and regulations worldwide.

Disclaimer of Liability

- To the extent allowed by applicable law, in no event will we be liable for any special, incidental, indirect, consequential damages, nor for any loss of profits, data, and documents.
- The product described in this manual is provided on an "as is" basis. Unless required by applicable law, this manual is only for informational purpose, and all statements, information, and recommendations in this manual are presented without warranty of any kind, expressed or implied, including, but not limited to, merchantability, satisfaction with quality, fitness for a particular purpose, and noninfringement.
- Users must assume total responsibility and all risks for connecting the product to the Internet, including, but not limited to, network attack, hacking, and virus. We strongly recommend that users take all necessary measures to enhance the protection of network, device, data and personal information. We disclaim any liability related thereto but will readily provide necessary security related support.
- To the fullest extent permitted by applicable law, in no event shall we, our employees, licensors, or affiliates be liable for any indirect, incidental, special, consequential, or punitive damages, including but not limited to loss of profits, loss of sales or business, loss of data, or costs of procurement of substitute goods or services, arising out of or related to your use or inability to use the product or service, even if advised of the possibility of such damages. Some jurisdictions do not allow the exclusion or limitation of liability for personal injury, or of incidental or consequential damages, so the above limitations may not apply to you.
- To the extent allowed by applicable law, in no event shall our total liability to you for all damages for the product described in this manual exceed the amount of money that you have paid for the product.

- When using this product, please strictly adhere to the applicable laws and regulations to avoid infringing upon the rights of third parties, including but not limited to intellectual property rights, data rights, or other privacy rights. You must also not use this product for the purposes of developing or facilitating the use of weapons of mass destruction, biological or chemical weapons, nuclear weapons, or for any other purposes that violate international norms and regulations.

Privacy Protection Reminder

Uniview complies with applicable privacy protection laws and is committed to protecting user privacy. You may want to read our full privacy policy at our website and get to know the ways we process your personal information.

Please be aware, using the product described in this manual may involve the collection of personal information such as face, fingerprint, license plate number, email, phone number, GPS. Please abide by your local laws and regulations while using the product.

Safety Warnings

The device must be installed, serviced and maintained by a trained professional with necessary safety knowledge and skills. Before you start using the device, please read through this guide carefully and make sure all applicable requirements are met to avoid danger and loss of property.

Storage, Transportation, and Use

- Store or use the device in a proper environment that meets environmental requirements, including and not limited to, temperature, humidity, dust, corrosive gases, electromagnetic radiation, etc.
- Make sure the device is securely installed or placed on a flat surface to prevent falling.
- Unless otherwise specified, do not stack devices.
- Ensure good ventilation in the operating environment. Do not cover the vents on the device. Allow adequate space for ventilation.
- Prevent water or other liquids from entering the device. It may cause device damage and risks such as electric shock and fire.
- Make sure the power supply provides a stable voltage that meets the power requirements of the device. Make sure the power supply's output power exceeds the total maximum power of all the connected devices.
- Verify that the device is properly installed before connecting it to power.
- Do not remove the seal from the device body without consulting us first. Do not attempt to service the product yourself. Contact a trained professional for maintenance.
- Always disconnect the device from power before attempting to move the device.
- Take proper waterproof measures in accordance with requirements before using the device outdoors.
- Warning: Operating this device in a residential environment may cause radio interference.

Power Requirements

- Install and use the device in strict accordance with your local electrical safety regulations.
- Use the recommended cordset (power cord) in accordance with the specified ratings.
- Only use the power adapter supplied with your device.
- Use a mains socket outlet with a protective earthing (grounding) connection.
- Ground your device properly if the device is intended to be grounded.

Battery Safety

Please use batteries properly; otherwise, there is a risk of fire or explosion.

- Warning: Using incorrect battery models can lead to explosion.
- If you need to replace the battery, it is recommended that you go to an authorized service center or have it replaced under professional supervision. We shall not be held responsible for any issues arising from unauthorized battery replacement.

- When replacing the battery, be sure to use a battery of the same type as the original. Using the wrong model for replacement (such as certain types of lithium batteries) may cause safety protection to fail.
- Batteries must not be exposed to overheat environments such as sunlight, fire, as this may lead to fire, explosion, or combustion.
- Do not dispose of batteries in fire or heating appliances. Do not squeeze, bend, or cut batteries, as it may cause explosion.
- Do not expose batteries to extremely high or low temperatures, or to very low-pressure environments, as this may cause explosion or leakage of flammable liquid/gas.
- For products or the included remote control containing a button cell battery: Do not ingest the battery-chemical burn hazard! If swallowed, a button cell battery can cause severe internal burns within 2 hours and may be fatal. Precautions (including but not limited to):
 - Keep new and used batteries away from children.
 - Stop using the product and keep it away from children if the battery compartment is not securely closed.
 - If you suspect that a battery may have been swallowed or inserted inside any part of the body, seek immediate medical attention.

Network Security

Please take all necessary measures to enhance network security for your device.

The following are necessary measures for the network security of your device:

- **Change the default password and set a strong password:** You are strongly recommended to change the default password after your first login and set a strong password of at least nine characters including all three elements: digits, letters and special characters.
 - Do not include the account name or the reverse of the account name.
 - Avoid using consecutive characters, such as 123, abc, etc.
 - Do not use overlapping characters, such as 111, aaa, etc.
- **Keep firmware up to date:** It is recommended that your device is always upgraded to the latest version for the latest functions and better security. Visit our website or contact your local dealer for the latest firmware.

The following are recommendations for enhancing network security of your device:

- **Change password regularly:** Change your device password on a regular basis and keep the password safe. Make sure only the authorized user can log in to the device.
- **Enable HTTPS/SSL:** Use SSL certificate to encrypt HTTP communications and ensure data security.
- **Enable IP address filtering:** Allow access only from the specified IP addresses.
- **Minimum port mapping:** Configure your router or firewall to open a minimum set of ports to the WAN and keep only the necessary port mappings. Never set the device as the DMZ host or configure a full cone NAT.
- **Disable the automatic login and save password features:** If multiple users have access to your computer, it is recommended that you disable these features to prevent unauthorized access.
- **Choose username and password discretely:** Avoid using the username and password of your social media, bank, email account, etc., as the username and password of your device, in case your social media, bank and email account information is leaked.
- **Restrict user permissions:** If more than one user needs access to your system, make sure each user is granted only the necessary permissions.
- **Disable UPnP:** When UPnP is enabled, the router will automatically map internal ports, and the system will automatically forward port data, which results in the risks of data leakage. Therefore, it is recommended to disable UPnP if HTTP and TCP port mapping have been enabled manually on your router.
- **SNMP:** Disable SNMP if you do not use it. If you do use it, then SNMPv3 is recommended.
- **Multicast:** Multicast is intended to transmit video to multiple devices. If you do not use this function, it is recommended you disable multicast on your network.
- **Check logs:** Check your device logs regularly to detect unauthorized access or abnormal operations.
- **Physical protection:** Keep the device in a locked room or cabinet to prevent unauthorized physical access.

- **Isolate video surveillance network:** Isolating your video surveillance network with other service networks helps prevent unauthorized access to devices in your security system from other service networks.

You may also obtain security information under Security Response Center at Uniview's official website.

1 Defaults

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 dynamically, and you need to use the assigned IP address to log in.

2 Introduction

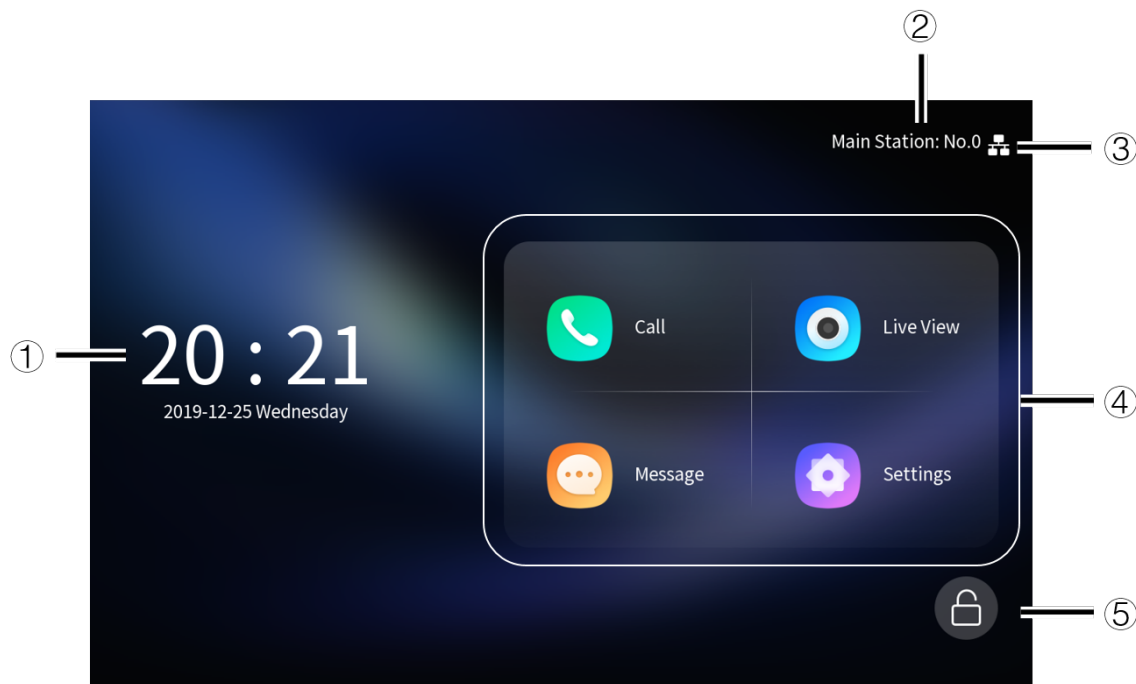
Power-on Configuration

The main station needs to be used with video intercom series products (indoor station, door station, etc.).

Please first add the main station and its associated video intercom devices on UNV Guard or EZTools (hereinafter collectively referred to as "the platform"), then complete the association.

Main Screen

After normal startup, the main screen will display the following content.

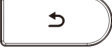


No.	Name	Description
1	Date, Time	Can be configured in Date & Time Settings .
2	Main Station ID	Assigned by the platform, also can be viewed in System Information .
3	Network Status	: Network connected : Network not connected

No.	Name	Description
4		Call other main stations in the same community, call residents bound to this device, view call records. For details, see Call .
		View live video of unit door stations and zone stations. For details, see Live View .
		- View and process Alarm. - View Snapshot.
		Background parameter configuration. For details, see Settings .
5		Click to lock screen. In screen-off state, click any position on the screen to light up. Also supports setting auto screen-off, for details see Personalization .

Buttons

Short press the button once.

Icon	Description
	During a call, decrease/increase volume.
	Return to main screen.
	Turn on speaker, turn off speaker.
	Return to previous unit.

3 Call

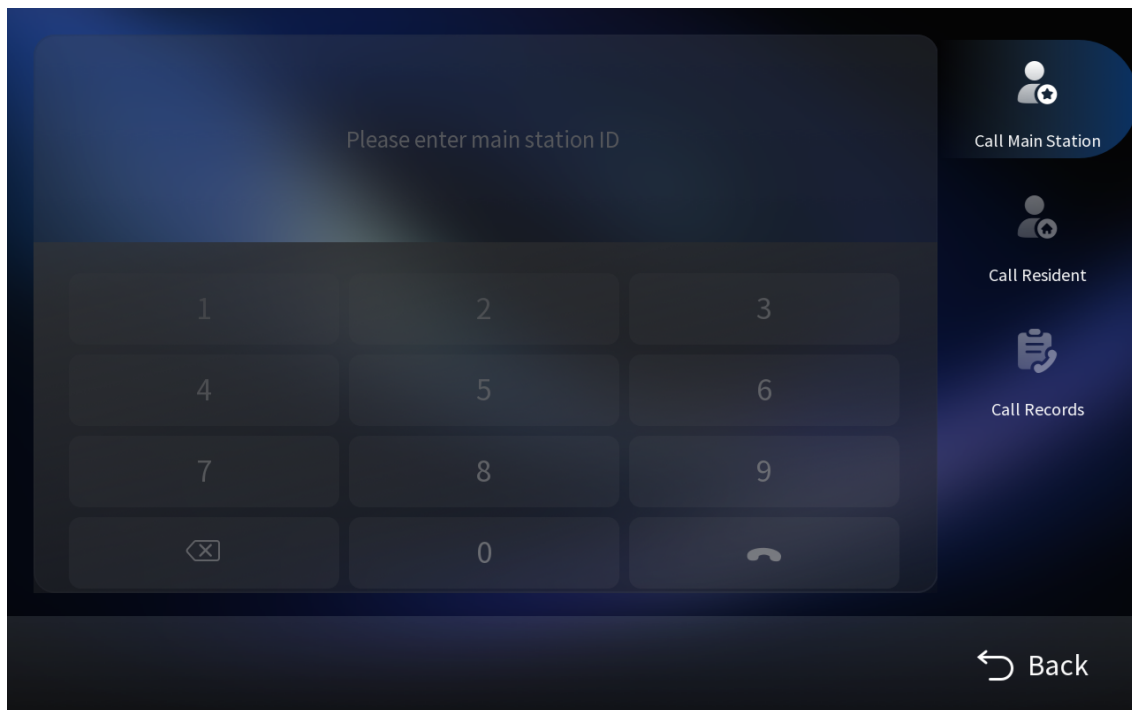
3.1 Call Main Station

Prerequisites

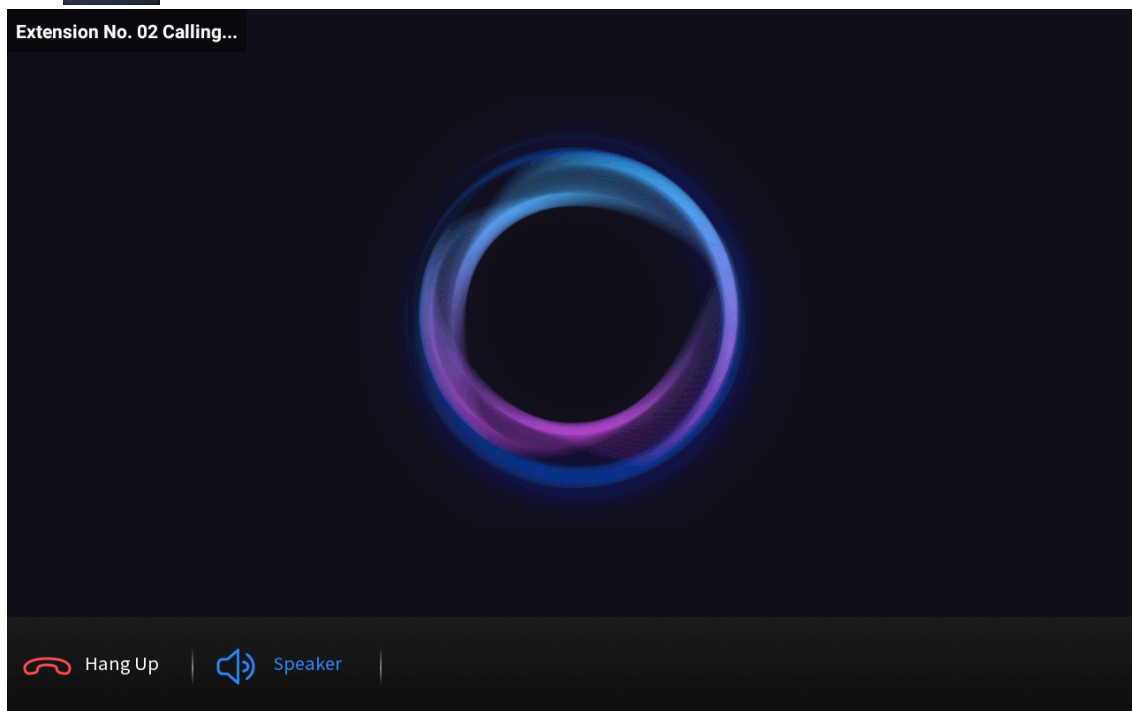
The called main station and this main station must be in the same community.

Procedure

1. Click . The Call Main Station screen opens by default.
2. Enter the main station ID (i.e., the ID in the upper-right corner of the main screen. Example: 01).



3. Click .



Click  to end the call.

Speaker is enabled by default. Click  to disable speaker.

3.2 Call Resident

Prerequisites

The resident room must be equipped with an indoor station, and the indoor station must be bound to the platform side and managed by this main station.

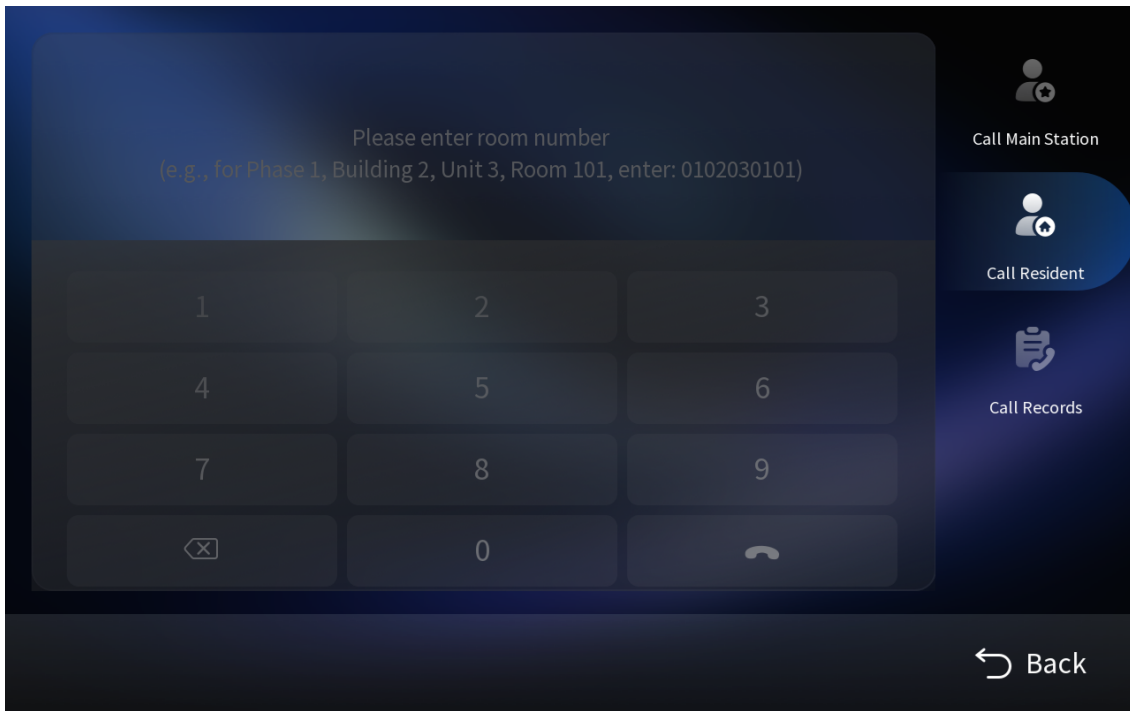
Procedure

1. Select  > **Call Resident**.

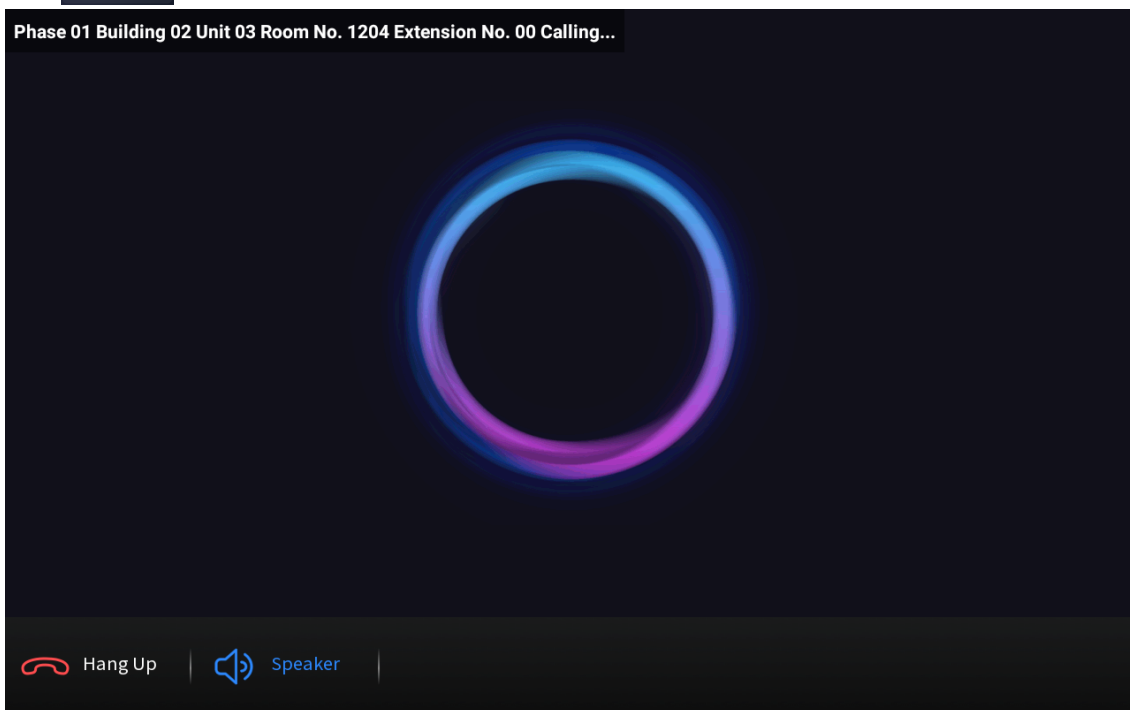
2. Enter the room number.

Example: For room 1204 in Building 2, Unit 3 of Phase 1, the room number is 0102031204.

 **Note:** If the room number is less than four digits, pad with leading zeros.



3. Click .

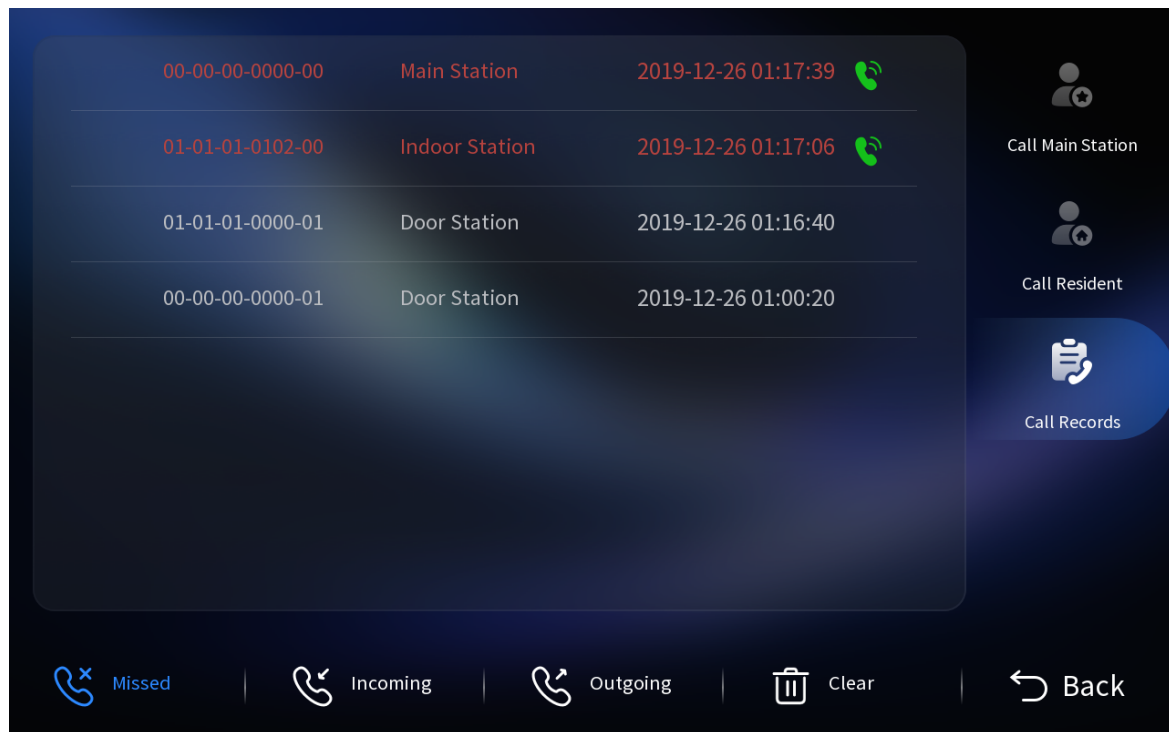


Click  to end the call.

Speaker is enabled by default. Click  to disable speaker.

3.3 Call Records

Select  > **Call Records**.



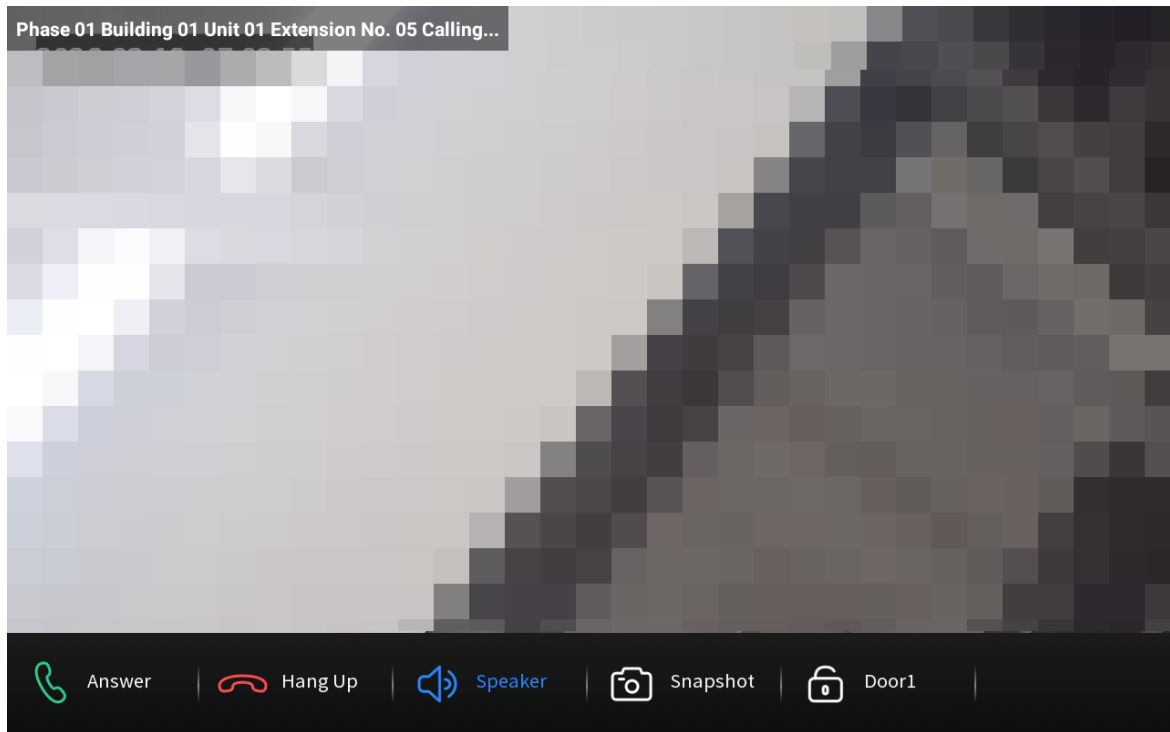
- Supports viewing the latest 200 call records (total records from the three lists: missed, incoming, outgoing).
- If there are missed calls, a badge will appear on the icon, e.g., , where the number indicates the count of missed calls. In the missed calls list, red text indicates unread message. After viewing the call record, the badge disappears.
- Callback: Only the main station and indoor station support this function. A  will appear on the right side of some call records. Tap it to quickly initiate a callback to the corresponding device.
- Delete multiple call records: Click **Delete**, select the records to delete, click **Delete**, enter the admin password in the pop-up, then click **OK**.
- Clear **all** call records: Click **Clear**, enter the admin password in the pop-up, then click **OK**.

4 Answer

The main station can answer calls from other main stations, zone stations, and unit door stations.

After a call comes in, the following screen is displayed, with the calling device information shown in the upper right corner.

Tap  to answer, tap  to decline.



Other operations:

-  : Enable speaker. Tap the icon again to turn it off.
-  : Capture the current screen. After capturing, you can view it in [Snapshot](#).
-  : Control the device to remotely open the door.

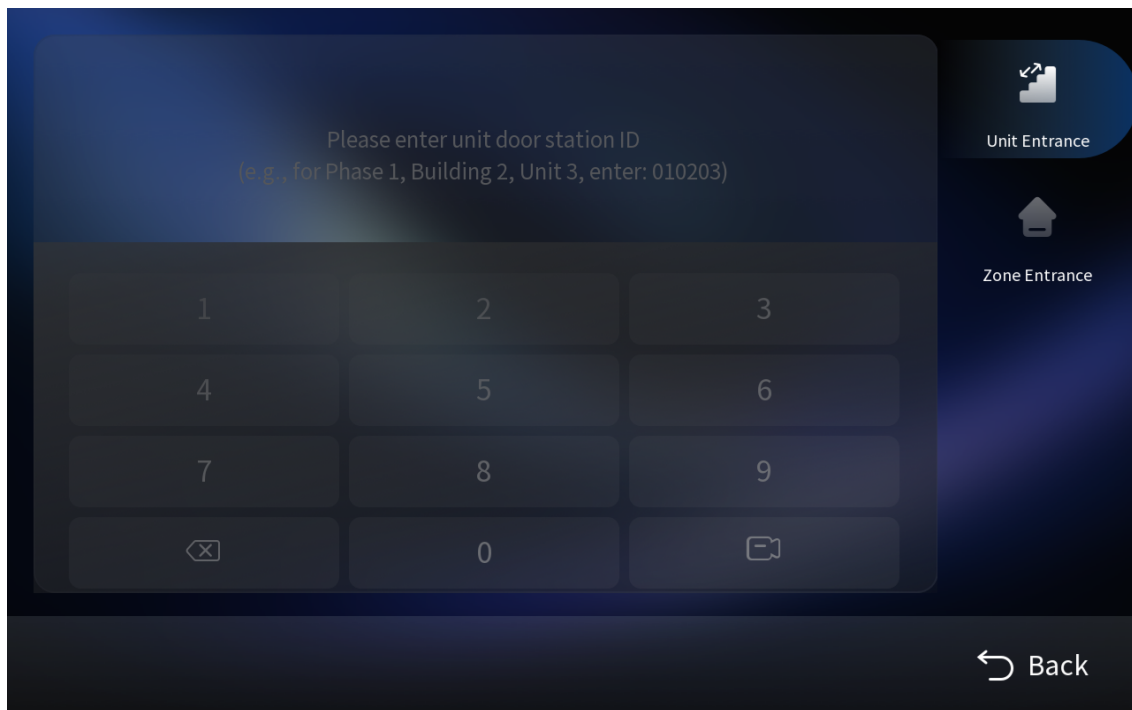
5 Live View

The main station can display the live video from unit door stations and zone stations that **have been bound on the platform** .

5.1 View Live Video of Unit Door Station

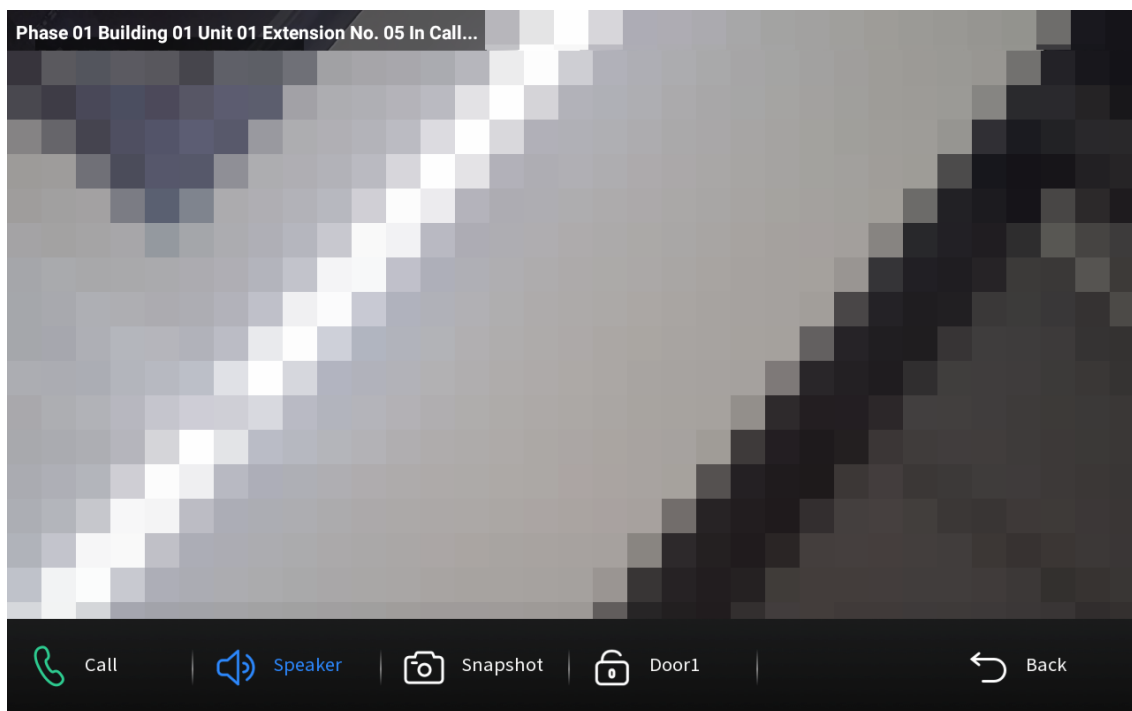
Unit door station: A door station deployed at the entrance of a building unit.

1. Tap  to enter the unit door station live view operation screen by default.



2. Enter the unit door station ID.
Example: Phase 1, Building 2, Unit 3, then the ID is 010203.
3. Tap  to view the live video.

 **Note:** If the live video is continuously viewed for 60 seconds without any operation, the live video will automatically end.



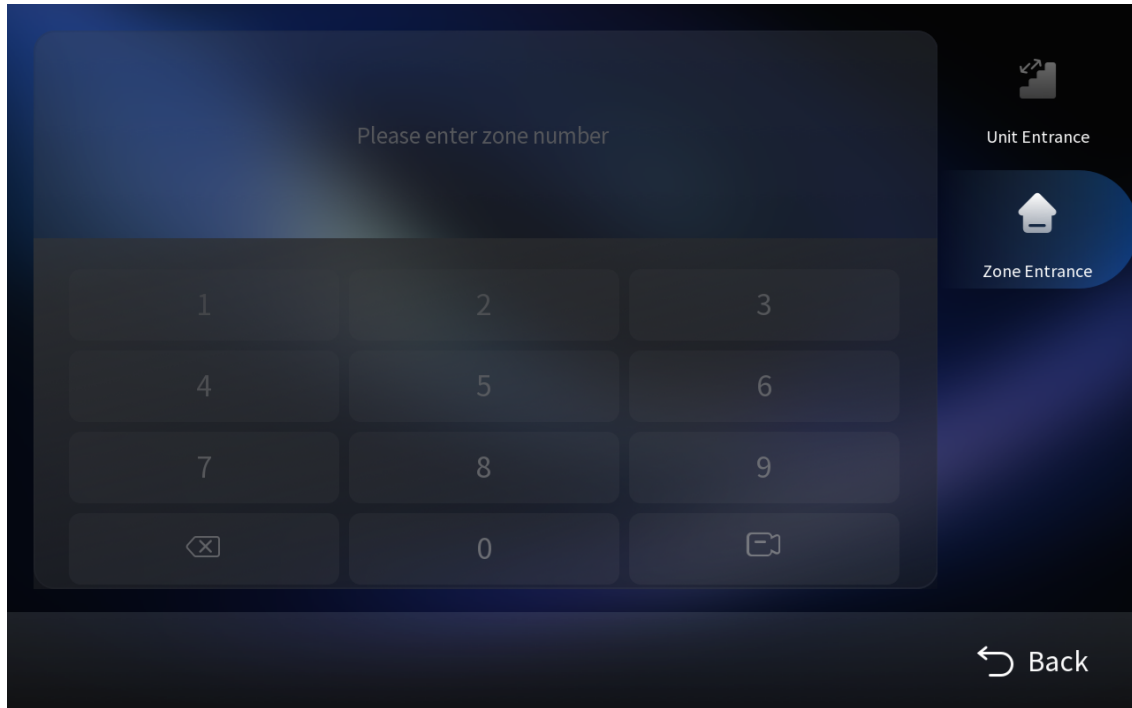
-  : Initiate a call. After answering, tap  to end the call.
-  : Enable speaker. Tap the icon again to turn it off.
-  : Capture the current screen. After capturing, you can view it in [Snapshot](#).

-  : Control the device to remotely open the door.

5.2 View Live Video of Zone Station

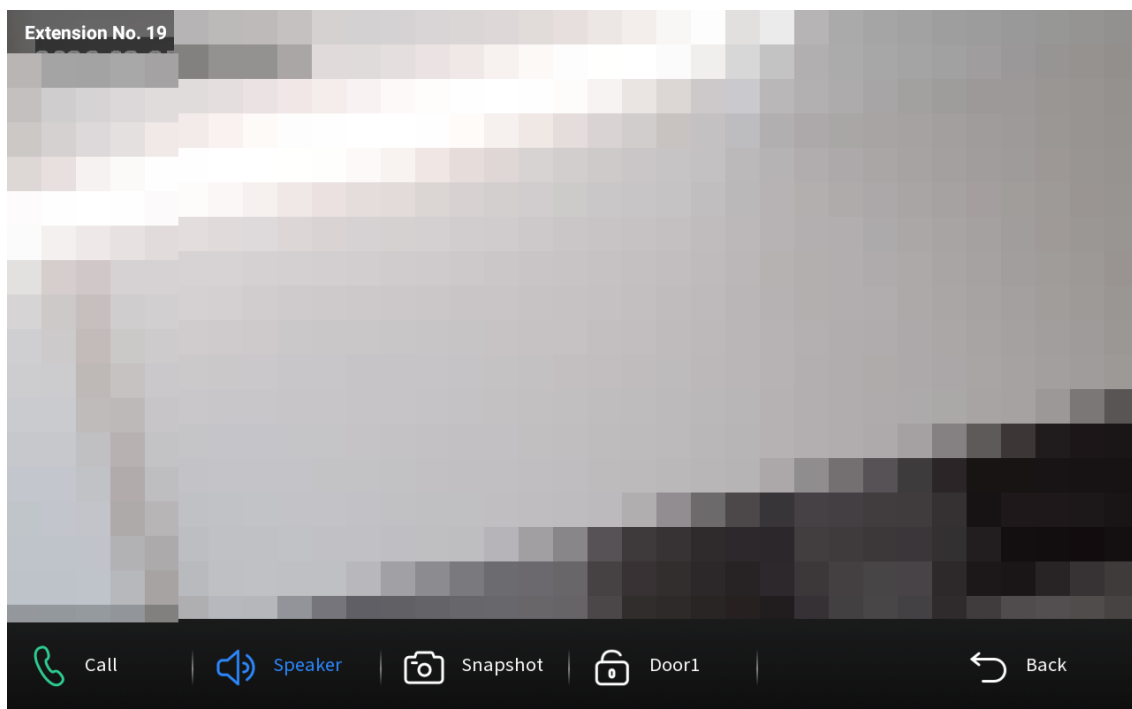
Zone station: A door station deployed at the entrance/exit of a residential community.

1. Go to  > **Zone Station Live**.



2. Enter the zone station ID.
3. Tap  to view the live video.

 **Note:** If the live video is continuously viewed for 60 seconds without any operation, the live video will automatically end.



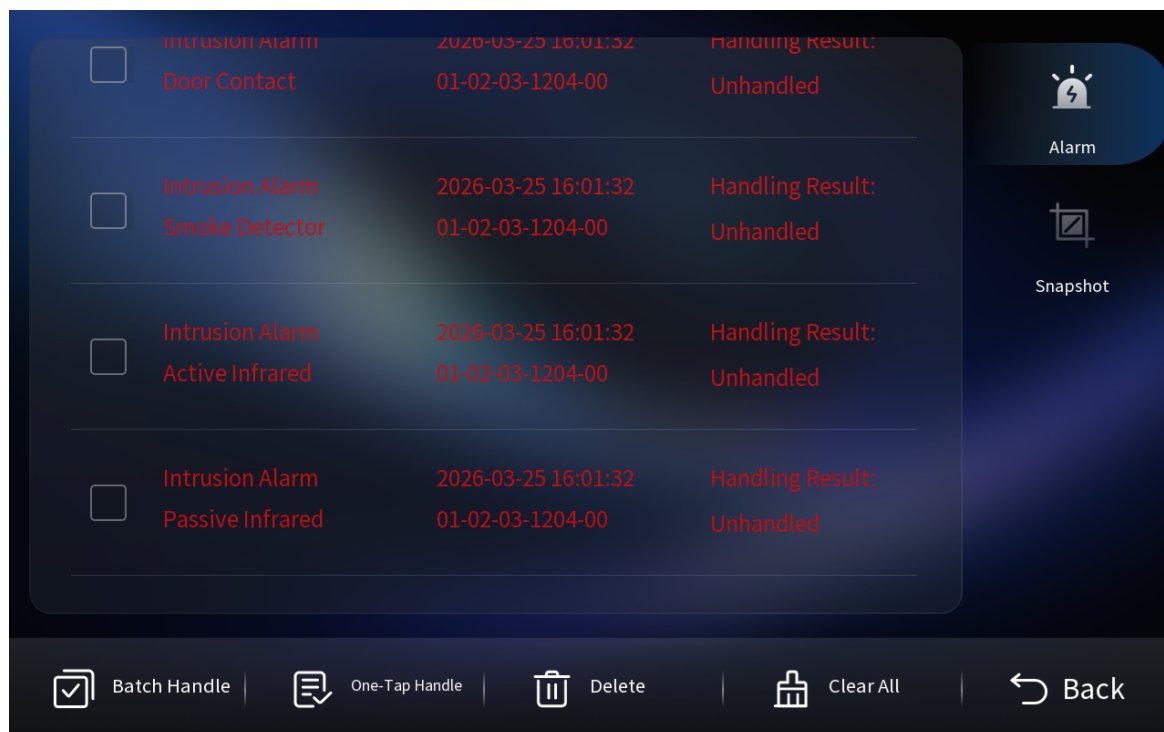
Other operations are the same as [View Live Video of Unit Door Station](#).

6 Message

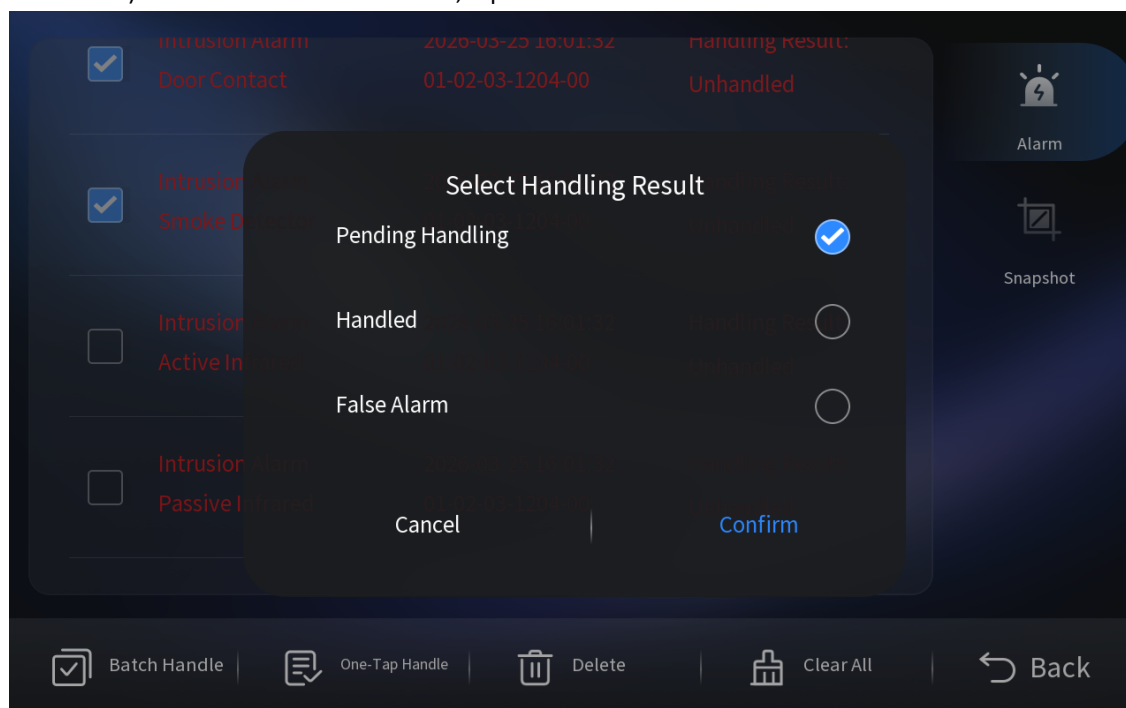
6.1 Alarm

Summarizes alarms reported by indoor stations.

Tap  to enter the alarms screen by default. Red text indicates pending handling; white text indicates handled alarms.



- Batch Handling: Select the alarm, tap **Batch Process**, select the handling result (pending handling/handled/false alarm) based on the actual situation, tap **OK**.



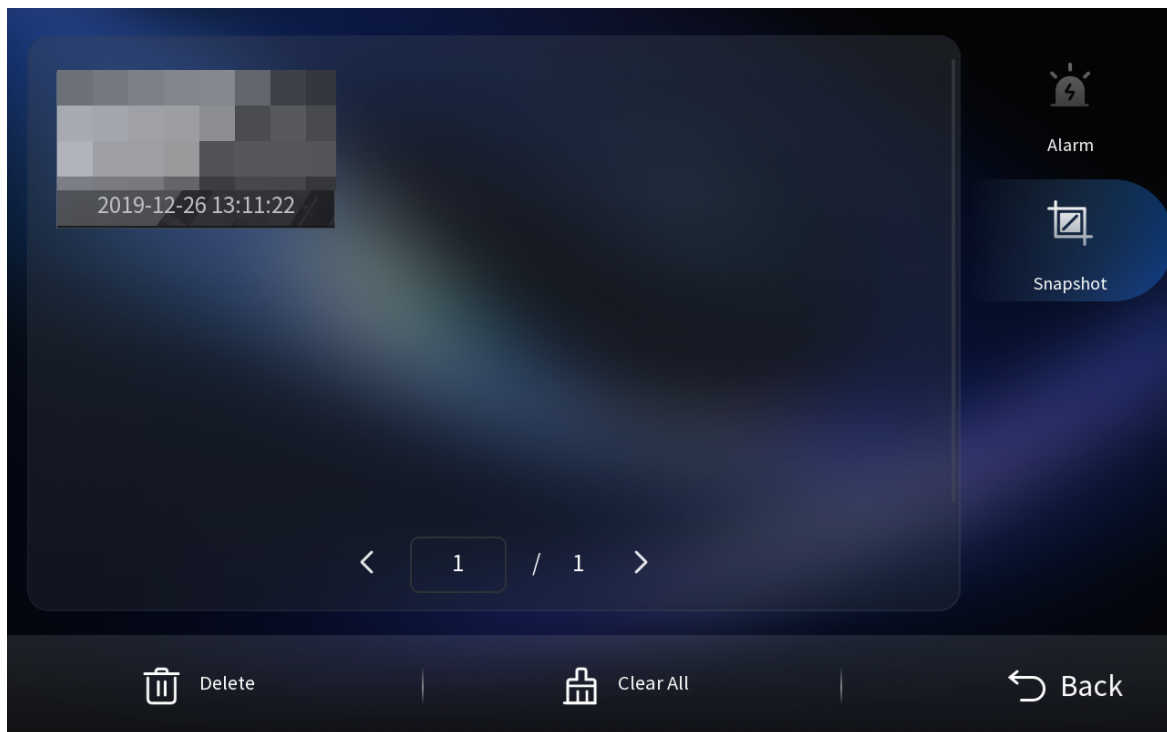
- One-Tap Handle: Tap One-click **Handle**, all alarms in red will be selected, select the handling result (pending handling/handled/false alarm) based on the actual situation, tap **OK**.
- Delete a specific alarm: Tap the corresponding checkbox, tap **Delete** below, enter the admin password in the pop-up window, tap **OK**.
- Clear all alarms: Tap **Clear** at the bottom, enter the admin password in the pop-up window, tap **OK**.

6.2 Snapshot

The snapshot screen summarizes images captured during answering, calling, and conversation.

Up to 100 images can be stored. If the storage limit is reached, the earliest stored images will be automatically overwritten.

Go to  > **Snapshot**. Snapshots are displayed in descending order of capture time.



- View snapshots: Tap a photo to display it in full screen; tap anywhere on the screen to exit full-screen mode.
- Delete a snapshot: Tap the checkbox in the upper-left corner of the photo, tap **Delete** below, enter the admin password in the pop-up window, tap **OK**.
- Clear all snapshots: Tap **Clear** at the bottom, enter the admin password in the pop-up window, tap **OK**.

7 Settings

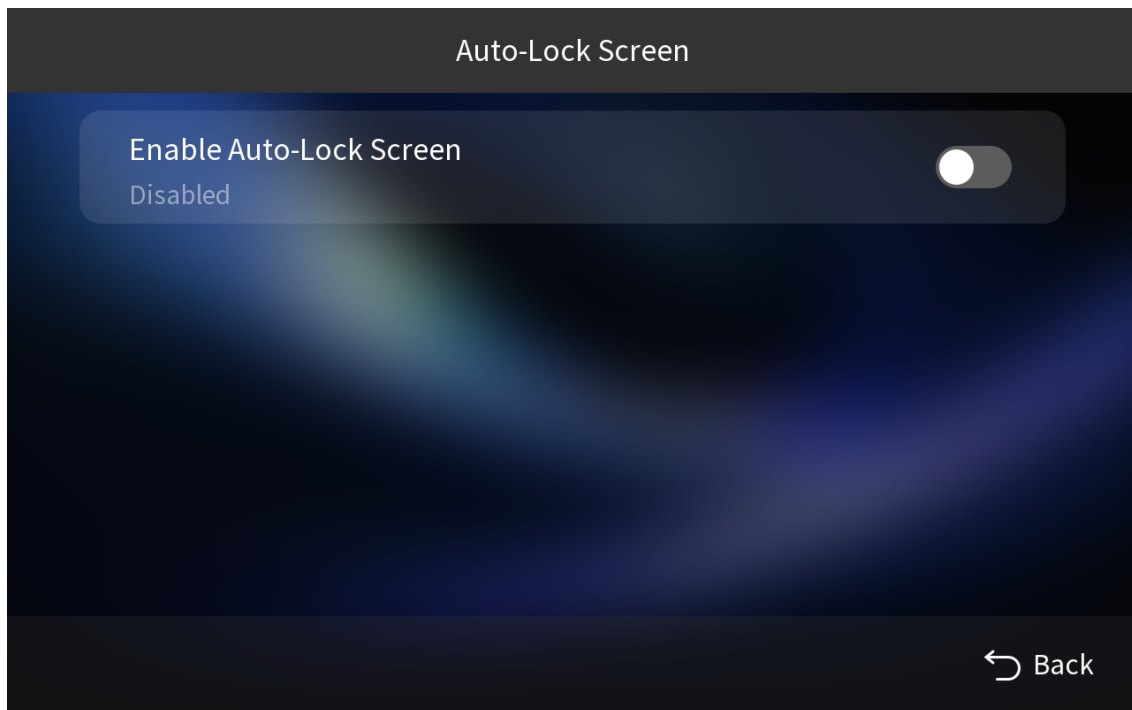
7.1 Personalization

Set auto-lock screen parameters.

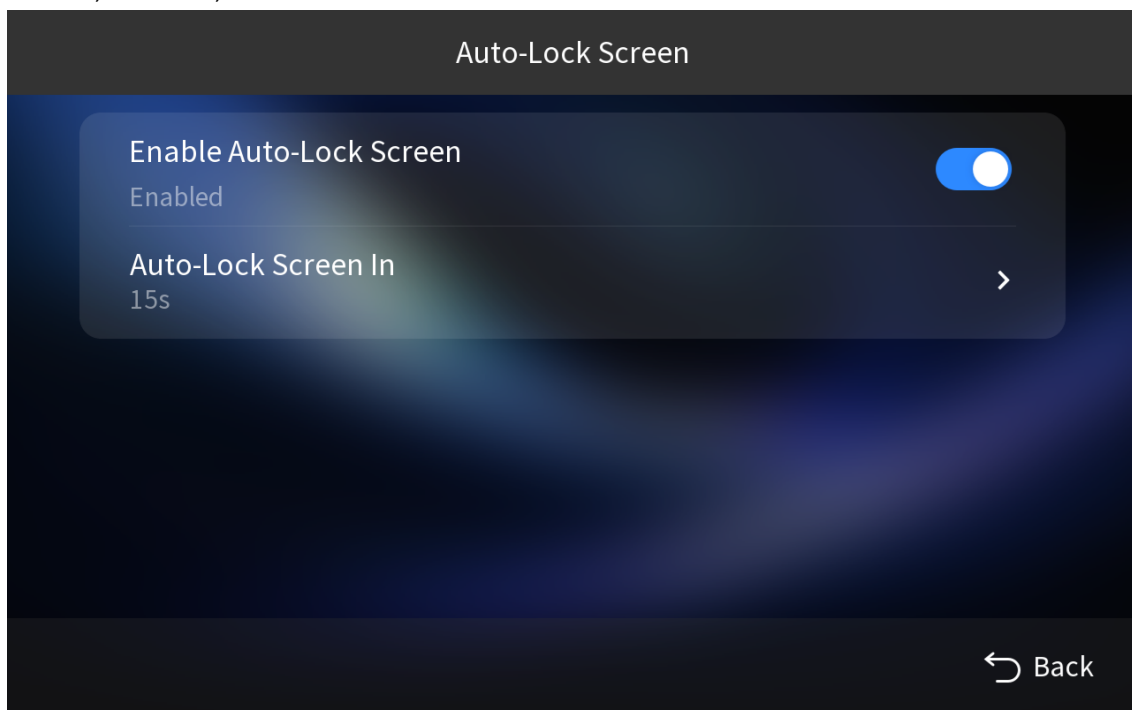
After the function is enabled, if no operation is performed on the main station within the set auto-lock screen time and the main station does not receive a call request, the screen will turn off automatically; tap anywhere on the screen to cancel screen lock.

While this function is enabled, manual screen lock is also supported. For details, see [Main Screen](#).

1. Go to  > **Personalization** > **Auto-Lock Screen**.



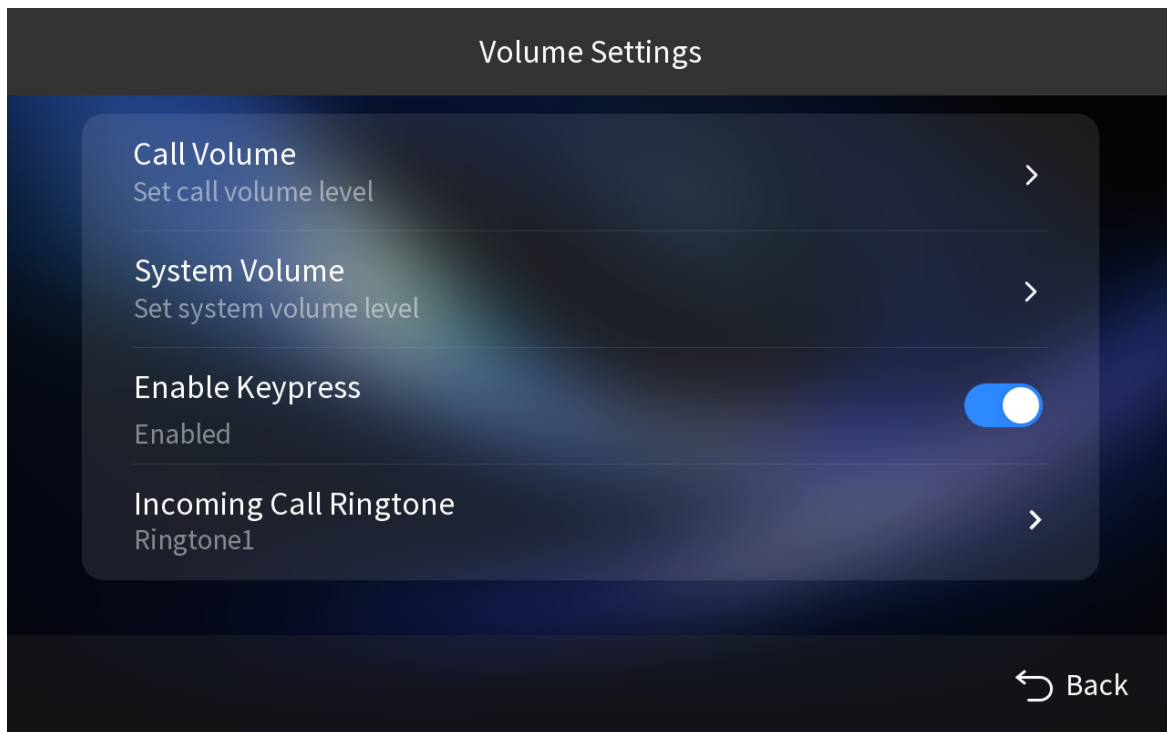
2. Tap  to enable the auto-lock screen, tap **OK**.
3. Set the auto-lock screen time. Default: 15 seconds; options include: 15 seconds, 30 seconds, 1 minute, 2 minutes, 5 minutes, 10 minutes.



4. Tap **OK**.

7.2 Volume Settings

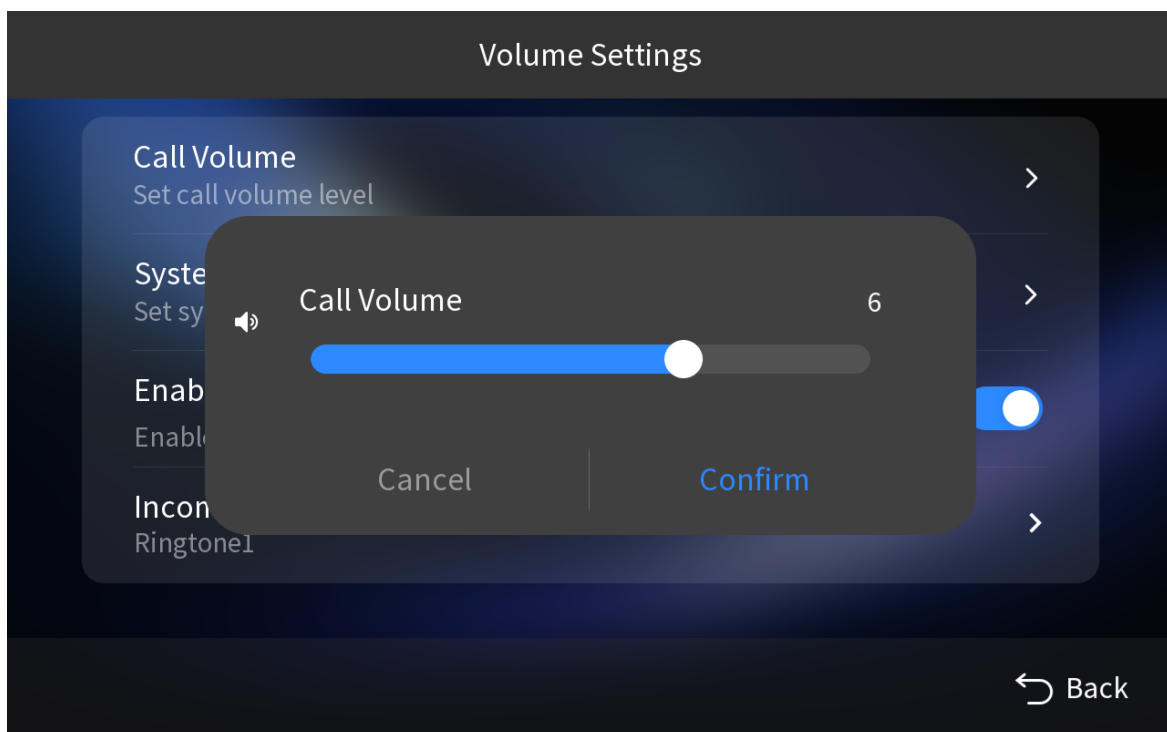
Go to  > **Volume Settings**].



Call Volume

Set the default volume level during calls. Physical buttons can be used to adjust volume during calls. For details, see [Buttons](#).

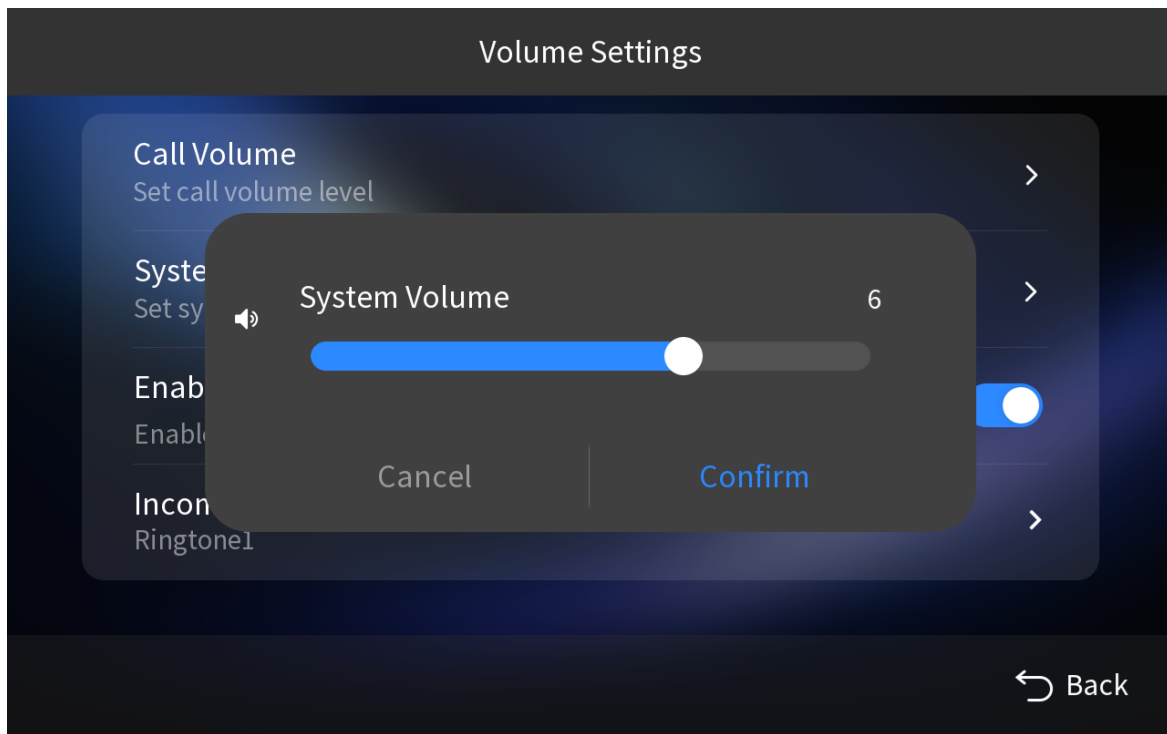
Drag the slider to set the volume level. Tap **OK** to save.



System Volume

Set the volume for incoming calls and keypress tones.

Drag the slider to set the volume level. Tap **OK** to save.



Enable Keypress Tone

The sound emitted when a button on the screen is tapped, to confirm a successful press.

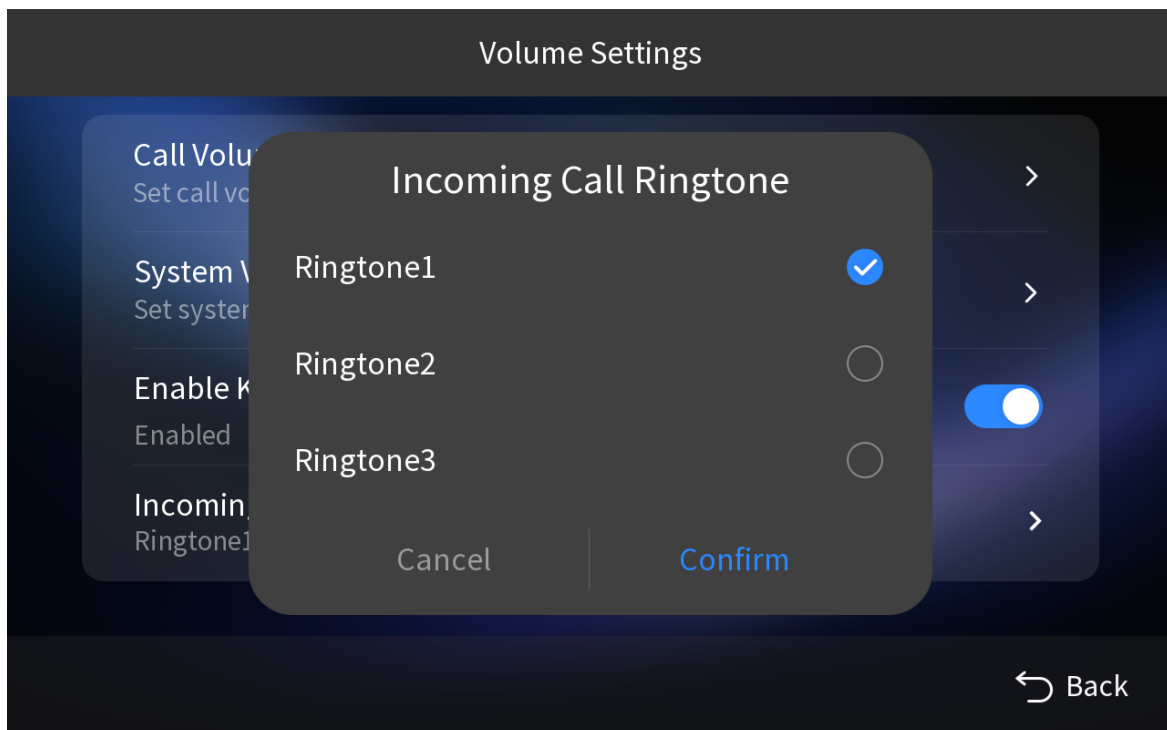
Tap  to enable.

Ringtone

The music that rings when the main station receives a call.

Three ringtones are provided by default.

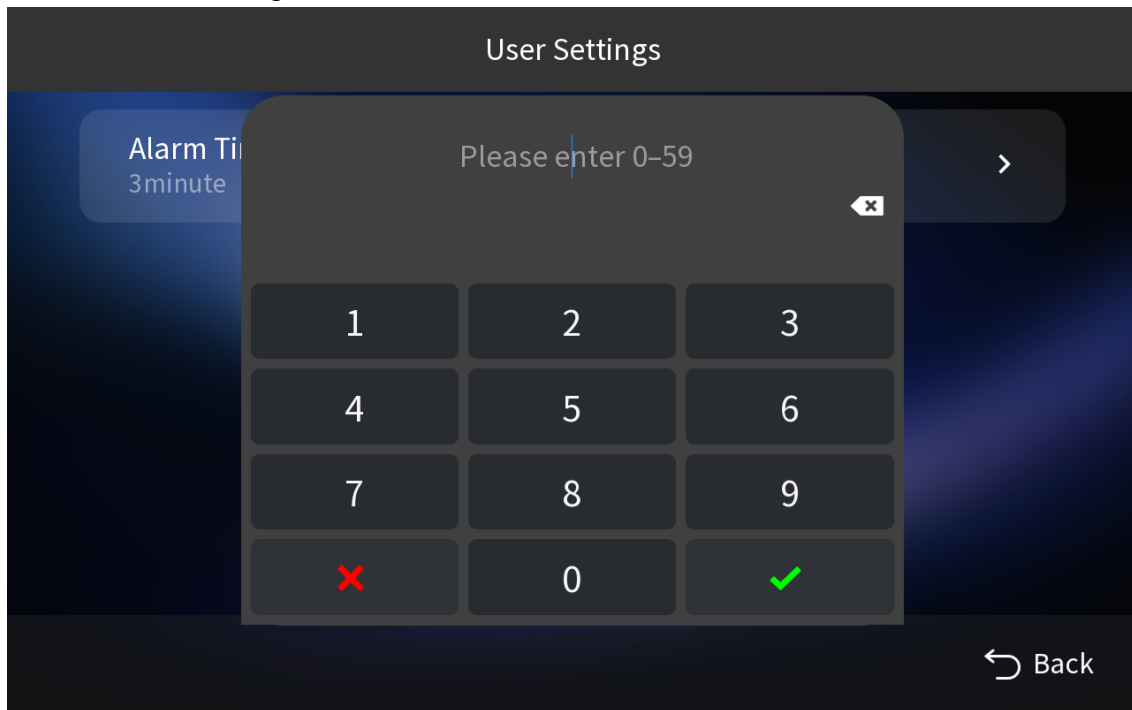
Tap to switch ringtones, tap **OK** to save.



7.3 User Settings

Set the duration for which an alarm persists after being triggered. Default: 3 minutes.

1. Select  > **User Settings** > **Alarm Time**.
2. Enter the time. Valid range: 0-59.

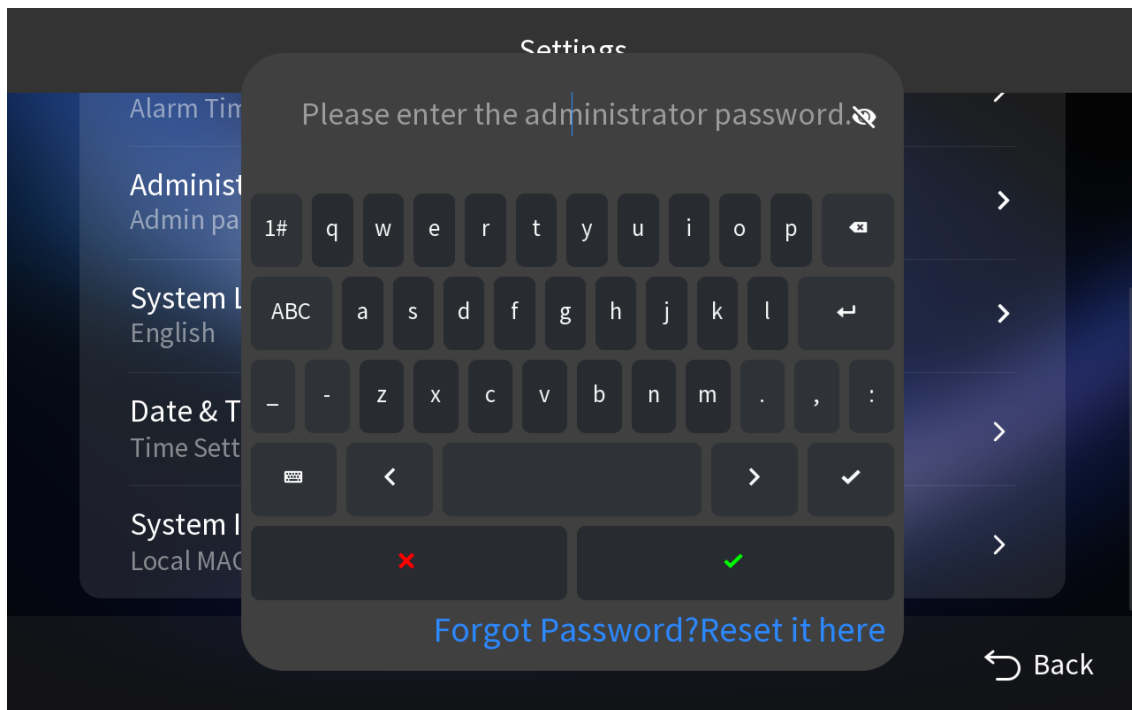


3. Tap ✓.

7.4 Administrator Configuration

1. Go to  > **Administrator Configuration**.
2. Enter the admin password in the pop-up window. Default: 123456.

 **Note:** If you forget the password, tap the hint in the lower-right corner of the pop-up window, follow the on-screen instructions to obtain a security code, reset the password, and then log in.



7.4.1 Administrator Password

Reset the admin password.

1. Go to  > **Administrator Configuration** > **Administrator Password**.

 A screenshot of the 'Set Administrator Password' screen. It features two input fields: 'New Password' and 'Confirm Password', both with 'Please Enter' placeholder text and a visibility toggle icon. Below the fields is a text block stating: 'A strong password is required (9 to 32 characters including all three elements: digits, letters, and special characters).' At the bottom, there are two buttons: 'Cancel' and 'Confirm'.

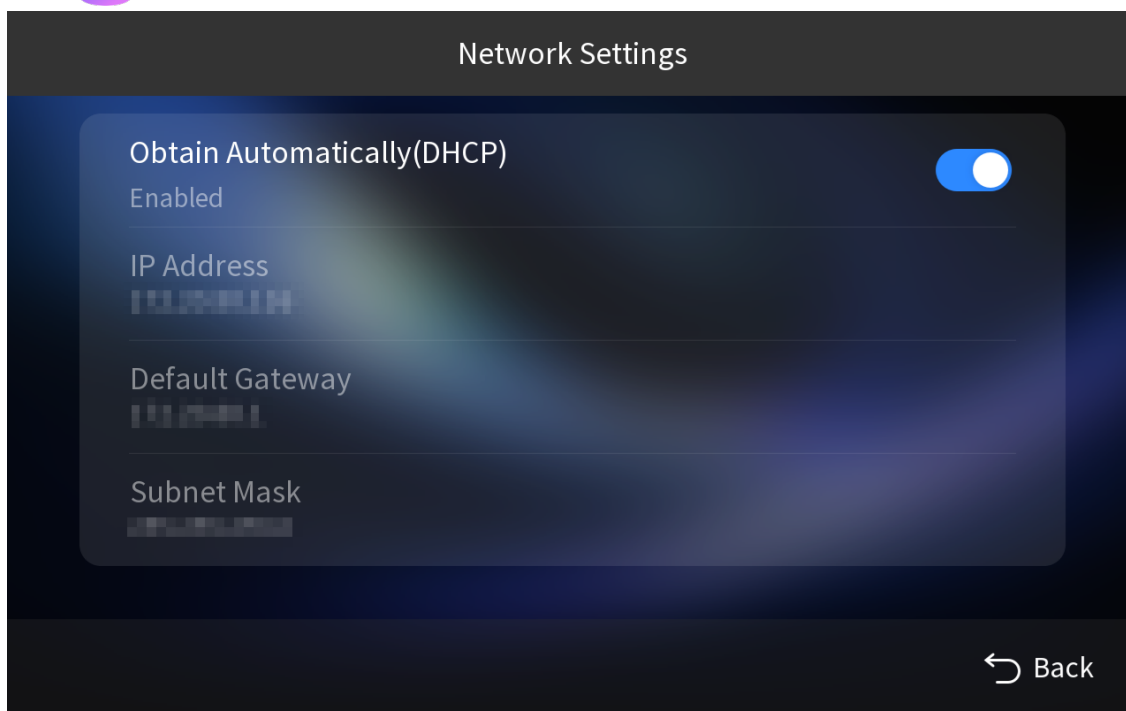
2. Enter the new password, then enter it again for confirmation.
Password requirements: 9-32 characters, must include digits, letters, and special characters.
3. Tap **OK**.

7.4.2 Network Settings

Two methods are available.

- Obtain Automatically (DHCP): If a DHCP (Dynamic Host Configuration Protocol) server exists in the network environment, the main station can automatically obtain an IP address from the DHCP server.
- Static IP: A long-term, fixed IP address assigned to the main station. When switching the IP obtainment method to **Static IP**, you also need to configure the corresponding IP address, subnet mask, and default gateway.

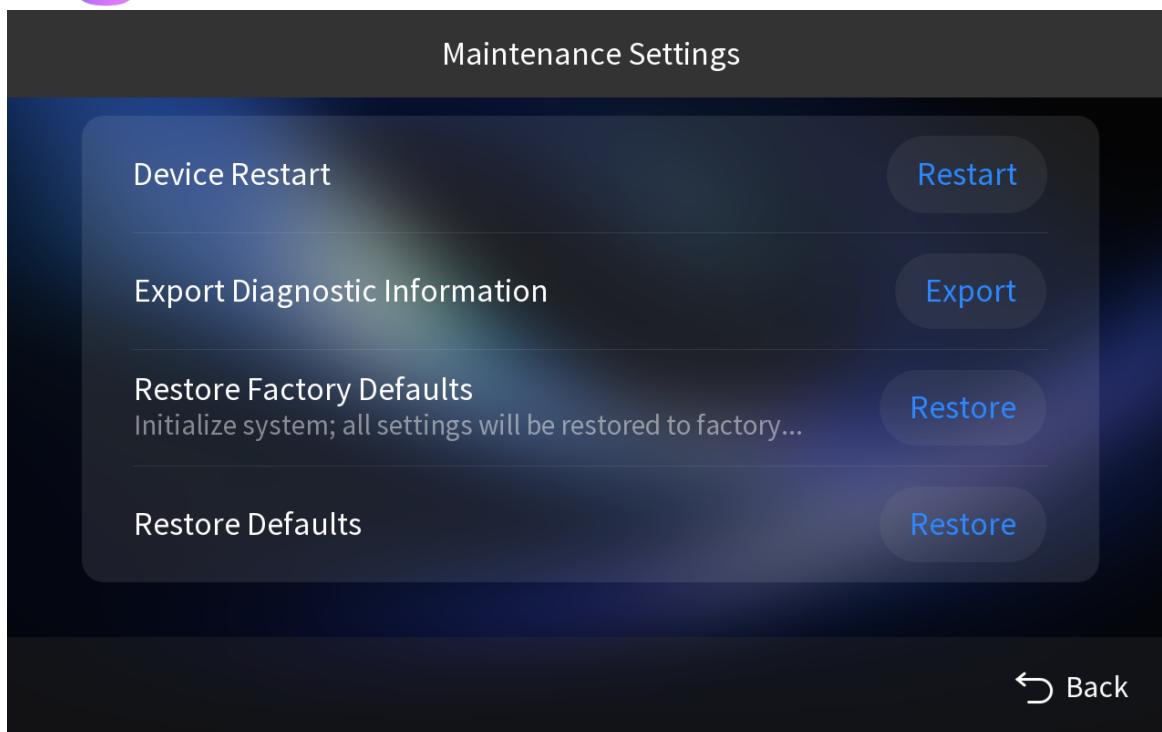
1. Go to  > **Administrator Configuration > Network Settings.**



2. DHCP is enabled by default. To switch to static IP, tap , then configure the static IP parameters.

7.4.3 System Maintenance

- Go to  > **Administrator Configuration > System Maintenance.**



Device Restart

Restart the main station. After tapping **Restart**, a confirmation window pops up; tap **OK**, and the main station will automatically restart.

Export Diagnostic Information

Prerequisite: Insert a USB flash drive into the main station first.

Tap **Export**; the exported file is named in the format “lvgl_logs_date_time.zip”.

Example: lvgl_logs_20260318_105106.zip

Restore Factory Defaults

All configurations will be restored to default values. After restoration, the device automatically restarts.

Restore Defaults

All configurations except the admin password and network settings will be restored to default values. After restoration, the device automatically restarts.

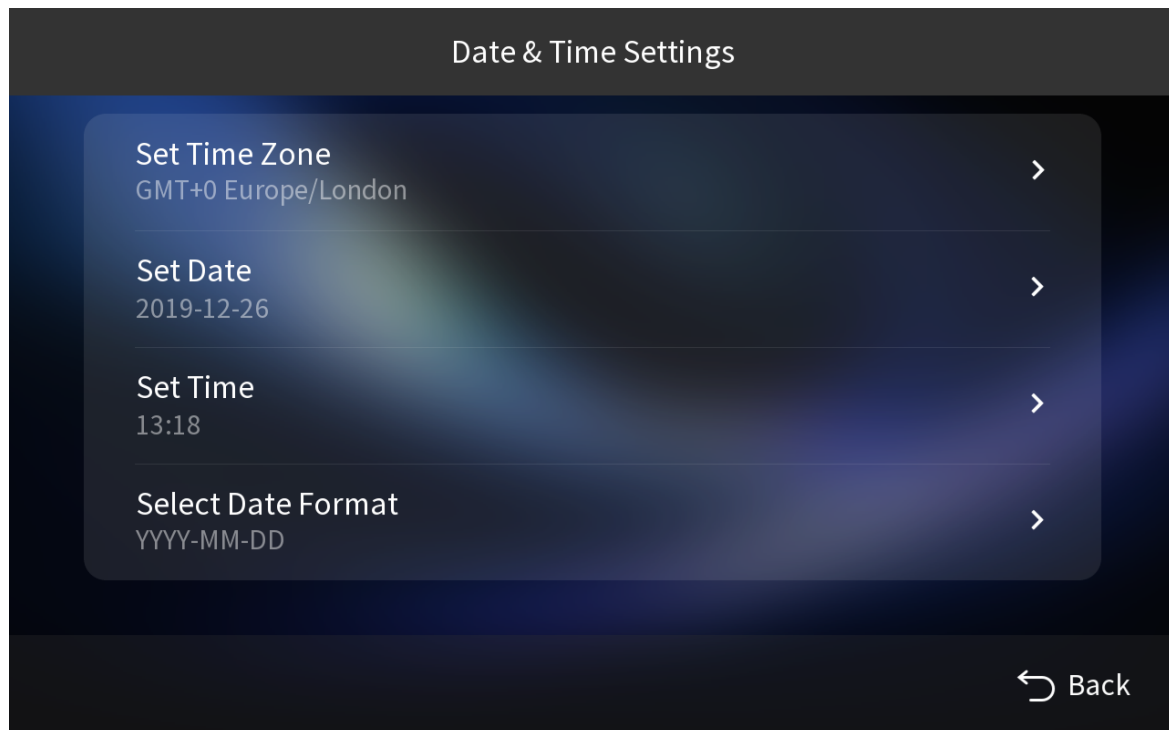
7.5 System Language

Currently only English is supported.

7.6 Date & Time Settings

You can set the time zone, date, time, and date format.

Go to  > **Date and Time Settings**.



7.7 System Information

You can view the device’s network information, uptime, etc.



System Information

Main Station

Device MAC Address
08:00:27:00:00:00

Management Platform

[← Back](#)