



G710S Doorphone User Manual

1 Product Overview	1
1.1 Product Introduction	1
1.2 Interface Introduction	2
2 User Guide	3
2.1 First configuration	3
2.2 Dialing	4
2.2.1 Outgoing Calls	4
2.2.2 Incoming Calls	5
2.2.3 During a call	6
2.3 Unlocking	7
2.3.1 Password Unlocking	7
2.3.2 Card Unlocking	8
2.3.3 Face Unlocking	8
2.3.4 DTMF Unlocking	8
2.3.5 QR code Unlocking	8
2.4 Address Book Search	9
3 Configuration Tutorial	10
3.1 Accessing the Backend Interface	10
3.1.1 Accessing the Device-side Backend	10
3.1.2 Checking the Device IP Address	11
3.1.3 Accessing the Web-side Backend	12

3.2 Intercom Configuration	13
3.2.1 Address Book Setting	13
3.2.2 Call Setting	16
3.2.3 SIP Account Setting	17
3.3 Access Control Configuration	18
3.3.1 Adding New Passwords	18
3.3.2 Relay Setting	19
3.3.3 Door lock/Door magnetic delay setting	21
3.3.4 Face Recognition	22
3.3.5 Wiegand	24
3.3.6 RFID anti duplication	25
3.4 Alarm Setting	26
3.4.1 Tamper Alarm	26
3.4.2 Door Magnetic Alarm	28
3.5 Internal Door Opening/Door magnetic Setting	29
3.6 System Logs	30
3.6.1 Record	30
3.6.2 Logs and Packet Grabbing	31
3.7 System Settings	32
3.7.1 Language, Volume, and Time	32
3.7.2 Network Settings	35

3.7.3 Password Settings	36
3.7.4 Firmware Upgrade	37
3.7.5 Screen Settings	38
3.7.6 Restart and Reset	39
3.7.7 Modes Settings	40
3.7.8 Contacts Page Settings	41
3.7.9 Dialing interface settings	42
3.7.10 Device screenshot	43
3.8 Advanced Settings	44
3.8.1 Connection Settings	44
3.8.2 Light Settings	45
3.8.3 QR Code Settings	46
3.8.4 RTSP and ONVIF Settings	47
3.8.5 Audit Tracker	49
3.8.6 Factory Testing	50
4 IDMC Configuration	51
4.1 IDMC Platform Login	51
4.2 Space Management	52
4.3 Device Management	53
4.3.1 Adding Devices	53
4.3.2 Device Unlocking	54

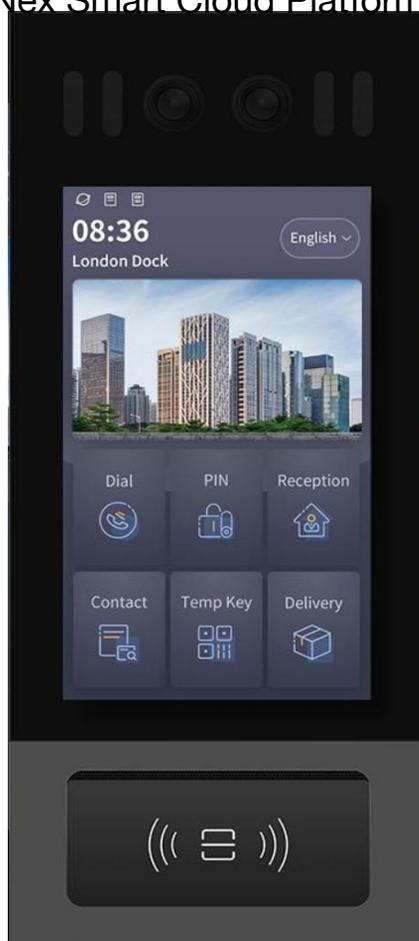
4.3.3 Device Operation	55
4.3.4 Device Configuration	55
5 NexSmart Cloud Platform Settings	57
5.1 NexSmart Cloud Platform Login	57
5.2 Project Management	58
5.2.1 Project Management	58
5.2.2 Space Management	59
5.3 Device Management	60
5.3.1 Add Device	60
5.3.2 Device Unlocking	61
5.3.3 Device Operation	63
5.4 Cloud Platform App Usage	64
5.4.1 Setting Permission Groups	64
5.4.2 Add New User	64
5.4.3 Device Unlocking	66
5.4.4 Monitoring Device	68

1 Product Overview

1.1 Product Introduction

G710S is a 7-inch touchscreen network doorphone with audio and video intercom, access control, monitoring and alarm functions. It can be used in applications such as villas, residential buildings, and more.

This product supports four configuration methods: direct hardware configuration, backend configuration, IDMC configuration and Nex Smart Cloud Platform Configuration.



1.2 Interface Introduction

Ethernet (POE) : Provides both power and network connectivity

12V-15V/GND: External power input

NO/COM/NC: Relay control port

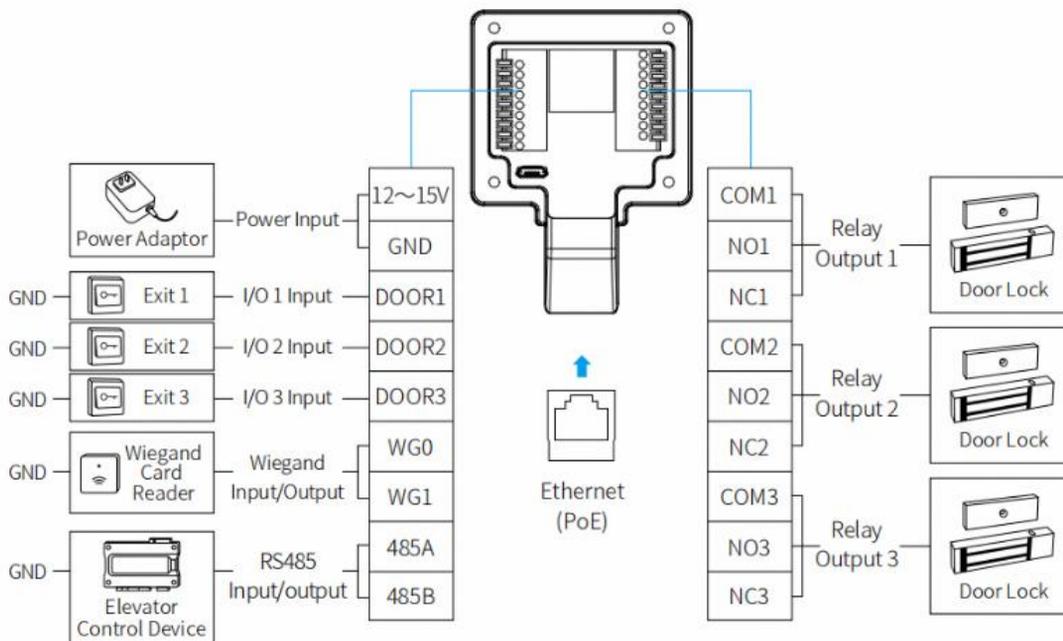
RS485A/B: RS485 port

DOOR1/GND: Internal door 1

DOOR2/GND: Internal door 2

DOOR3/GND: Internal door 3

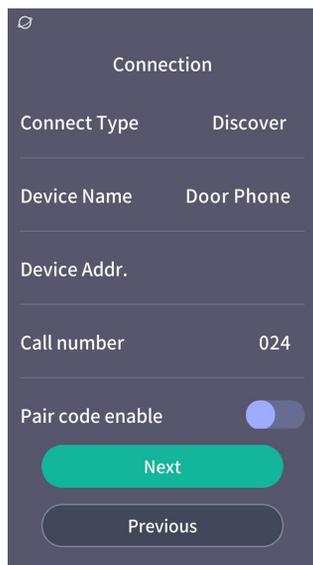
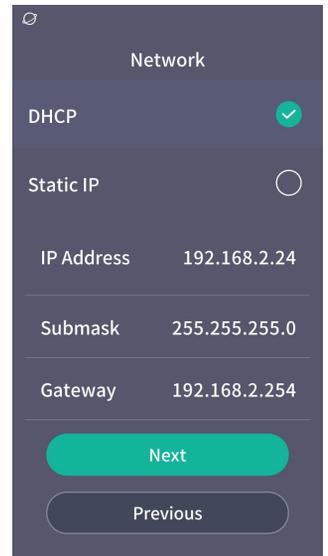
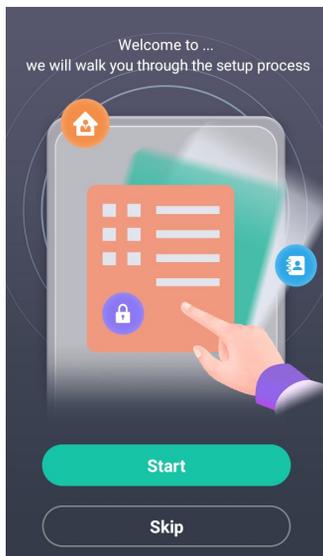
WG0/WG1/GND: Wiegand interface



2 User Guide

2.1 First configuration

When starting the device for the first time, the user must perform language configuration (Simplified Chinese, Traditional Chinese, English, Hebrew), network configuration (DHCP, static IP), connection type setting (Discovery, Cloud), and mode selection (General mode, Doorbell mode, Access mode, Directory mode).

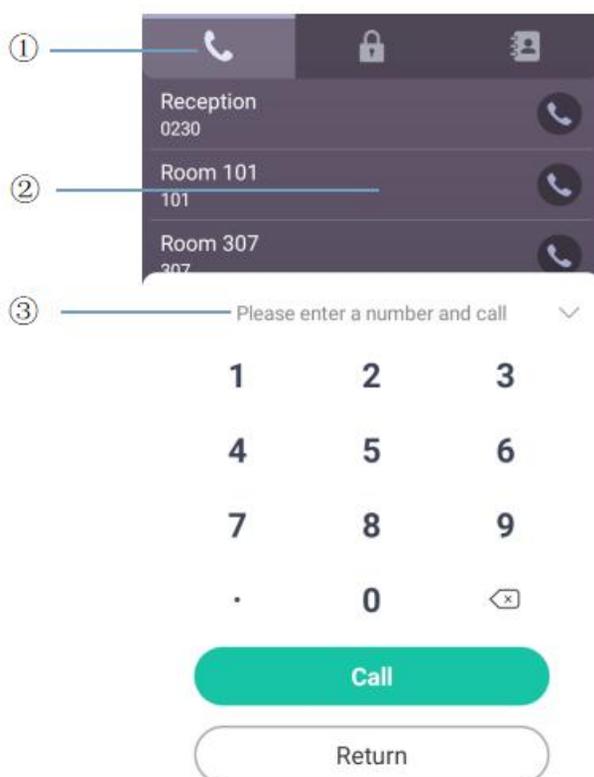


2.2 Dialing

2.2.1 Outgoing Calls

By clicking the dial button on the main screen, you can enter the call interface. You can directly click the dial button to start the call, or enter the call number or SIP account on the keyboard and click the call button to make the call. Alternatively, you can click on the address book on the main screen and select the device you want to call from the list to initiate the call.

This device supports group calling function, which means it can simultaneously call multiple indoor units. Simply select the group you want to call from the address book



2.2.2 Incoming Calls

When there is an incoming call and automatic answer is not enabled on the web, click the green answer button on the screen to answer the conversation, and click the red hang up button to hang up the call.



2.2.3 During a call

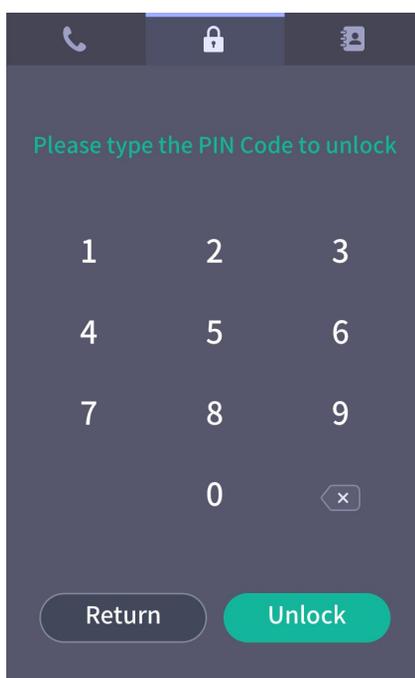
After clicking the green button to answer, enter the call interface. The volume bar on the right can adjust the call volume. Clicking the red button at the bottom of the interface will end the call.



2.3 Unlocking

2.3.1 Password Unlocking

Click on the **PIN** button on the main screen and enter the password, then click **Unlock** button to unlock.



2.3.2 Card Unlocking

Place the entered card in the card sensing area of the device, and the door lock will automatically open.

2.3.3 Face Unlocking

Directly approach the face to the screen, and if the face is valid, the device will prompt for successful door opening

2.3.4 DTMF Unlocking

Call the other party, and after the other party answers, enter the DTMF code (default is the "#" key), and the device prompts that the door has been opened successfully.

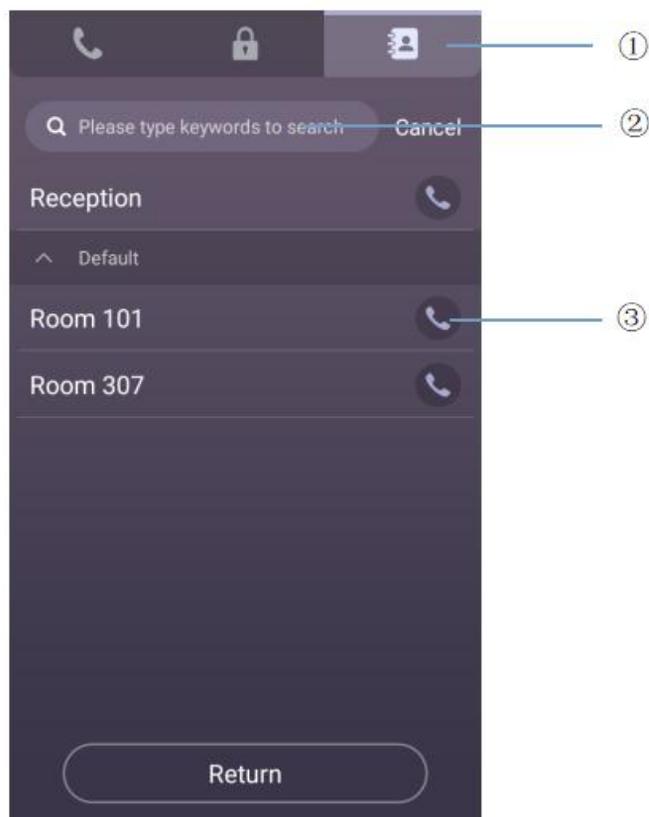
2.3.5 QR code Unlocking

Use a recognizable access control QR code. If the QR code is within its validity period, place it close to the screen and unlock it.

2.4 Address Book Search

Click on the address book button① on the main screen to enter the address book

- Enter numbers or letters in the input box to search②, support fuzzy search.
- Scroll up and down the list to select a contact, and click the contact tab or the call button.③

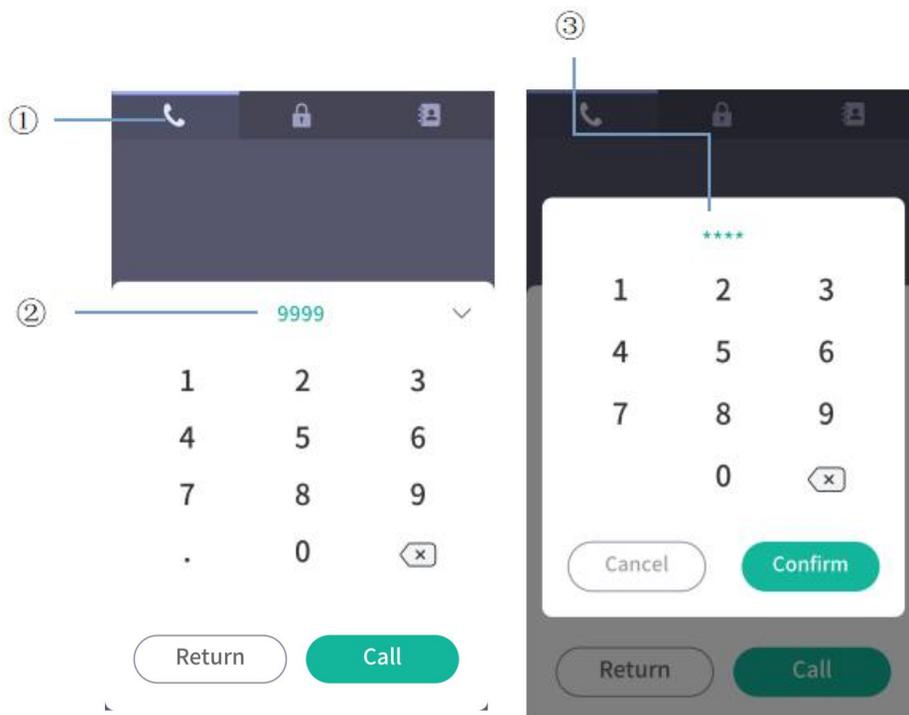


3 Configuration Tutorial

3.1 Accessing the Backend Interface

3.1.1 Accessing the Device-side Backend

- ① Click on dialing button on the main interface.
- ② Enter 9999 and call to pop up the project password menu.
- ③ Enter the password 3888 and click OK to enter the device backend interface.



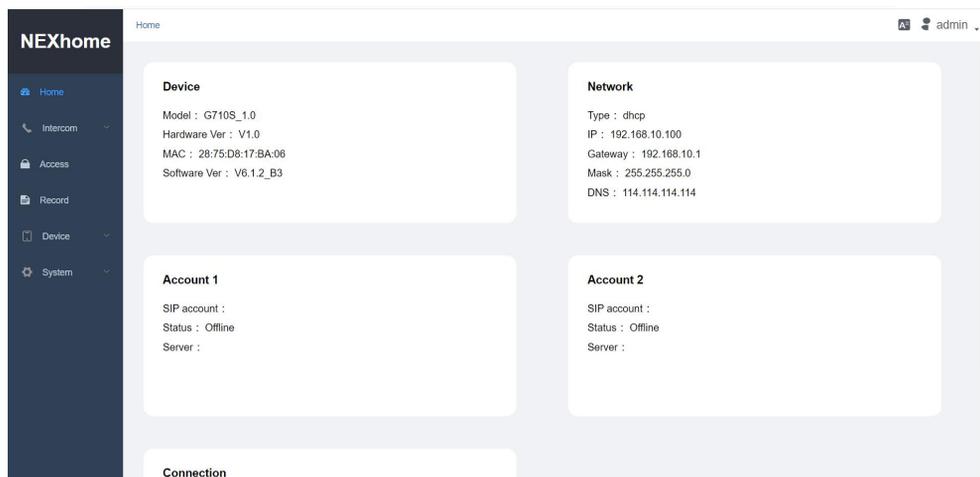
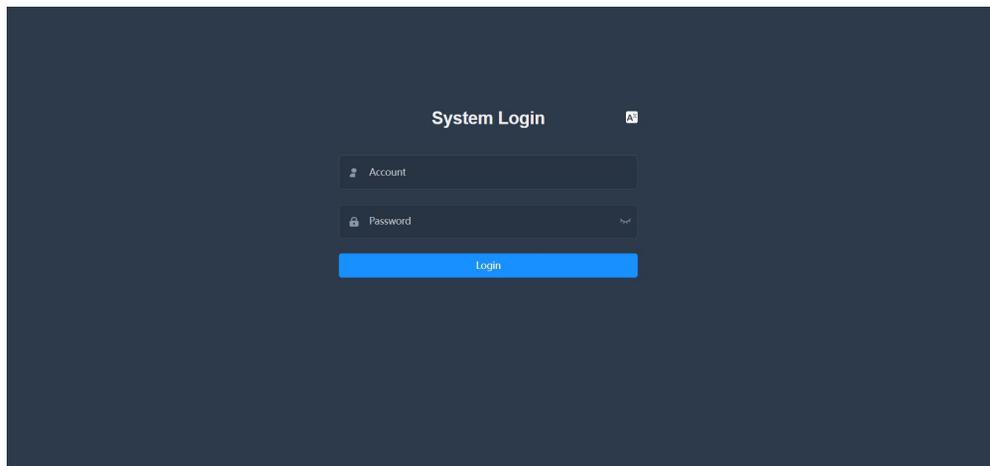
3.1.2 Checking the Device IP Address

After entering the device backend, click the status information button to view the device's network address, version information, and connection status.



3.1.3 Accessing the Web-side Backend

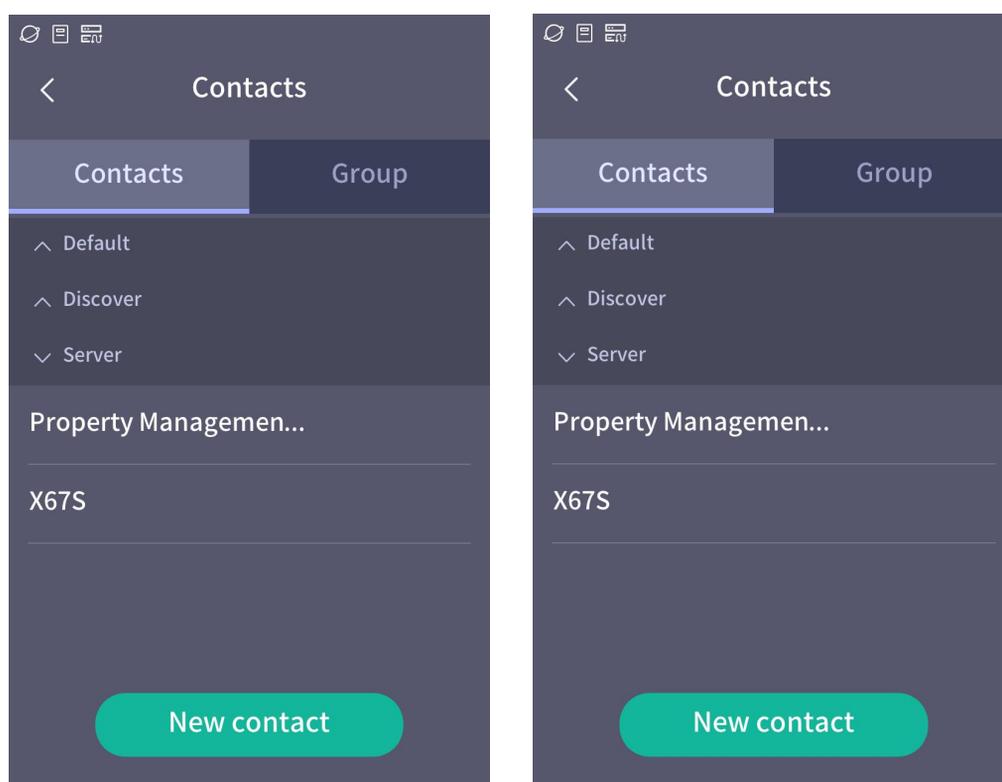
Enter the network address of the device on the webpage, click Enter to enter the web backend login interface, enter the account (default is admin) and password (default is 123456), and click Login to enter the web backend.



3.2 Intercom Configuration

3.2.1 Address Book Setting

In the device engineering settings interface, you can add, modify, and delete local contacts and local contacts in the address book.



In the web backend, you can view existing address books in the intercom address book, and you can click the add button at the top right to add new contacts. The add button at the bottom right can create a new contact group. When creating a new contact, it is necessary to fill in the contact's display name, call number, and SIP number.

The screenshot displays the NEXhome web interface. On the left is a dark sidebar with navigation options: Home, Intercom, Contacts (selected), Account, Advanced, RTSP, Access, Record, Device, and System. The main content area is titled 'Contacts' and features a search bar, filters for 'Contact' and 'SIP account' (set to 'All'), and '+ Add' and 'Delete' buttons. Below this is a table with 11 columns: Index, Contact Name, Call number, SIP number, Top, Group, SIP account, Email, Source, and Actions. Three contacts are listed, each with a delete icon in the Actions column. Below the table is a pagination control showing 'Total 3', '10/page', and 'Go to 1'. The 'Group' section below has a table with 5 columns: Index, Group name, Source, and Actions. Three groups are listed: Default (Local), Discover (Discover), and Server (Server), each with a delete icon in the Actions column. '+ Add' and 'Delete' buttons are also present for the Group section.

Index	Contact Name	Call number	SIP number	Top	Group	SIP account	Email	Source	Actions
1	222, building01	01222	grpxf0wxyf3yu b959c8q9rt	No	Server	Account 1		Server	
2	CYX	002	MapowQ6YgV nIHJ4BvpojaQ	No	Default	Account 1		Local	
3	YWL	001	M3lZlapuoRz AVxsnsTYLNT I	No	Default	Account 1		Local	

Index	Group name	Source	Actions
1	Default	Local	
2	Discover	Discover	
3	Server	Server	

After selecting a contact on the left side of the contact list, you can click the delete button in the upper right corner to delete the local contact; After selecting a contact group on the left side of the contact list, you can also click the corresponding delete button on the right side to delete the contact group, which supports batch deletion.

To edit a contact or contact group, you can enter the editing interface by clicking the edit button at the far right of the list.

Edit group call names to modify the group names displayed on the device address book interface.

The screenshot displays the NEXhome web interface. On the left is a dark sidebar with navigation options: Home, Intercom, Contacts (selected), Account, Advanced, RTSP, Access, Record, Device, and System. The main content area is titled 'Contacts' and features a table with columns: Index, Contact Name, Call number, SIP number, Top, Group, SIP account, Email, Source, and Actions. There are three contacts listed. Below the table is a 'Group' section with a table containing columns: Index, Group name, Source, and Actions. There are three groups listed. At the bottom of the screenshot is a modal window titled 'Add' with fields for Contact Name, Call number, and SIP number, radio buttons for SIP account (Account 1 selected), a Group dropdown menu, an Email field, a checkbox for Top, and Submit/Cancel buttons.

Index	Contact Name	Call number	SIP number	Top	Group	SIP account	Email	Source	Actions
1	222, building01	01222	grpxt0wxy3yu p959c8q9rt	No	Server	Account 1		Server	
2	CYX	002	MapowQ6YgV nHJ4BvpojaQ	No	Default	Account 1		Local	
3	YWL	001	M3lZiapuRz AVxsnsTYLNT I	No	Default	Account 1		Local	

Index	Group name	Source	Actions
1	Default	Local	
2	Discover	Discover	
3	Server	Server	

3.2.2 Call Setting

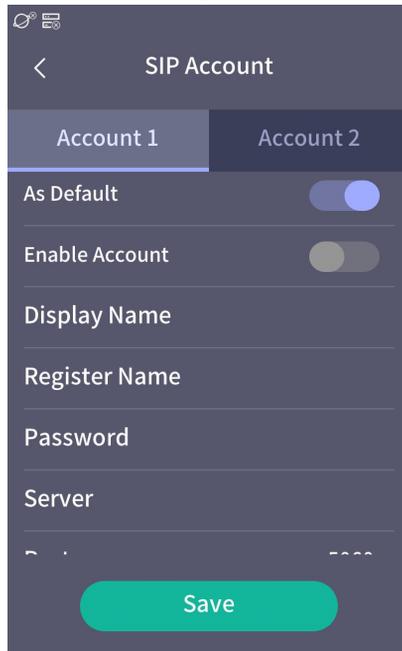
In the web backend, enter the Inertcom-Advanced section. You can check audio coding, set available coding, set video coding rate, resolution, coding load, and set DTMF type and load. You can also set the maximum talk time, maximum call-in time, and maximum call-out time, as well as whether to enable automatic answering and the delay time for automatic answering.

The screenshot displays the NEXhome web interface for configuring call settings. The interface is divided into several sections:

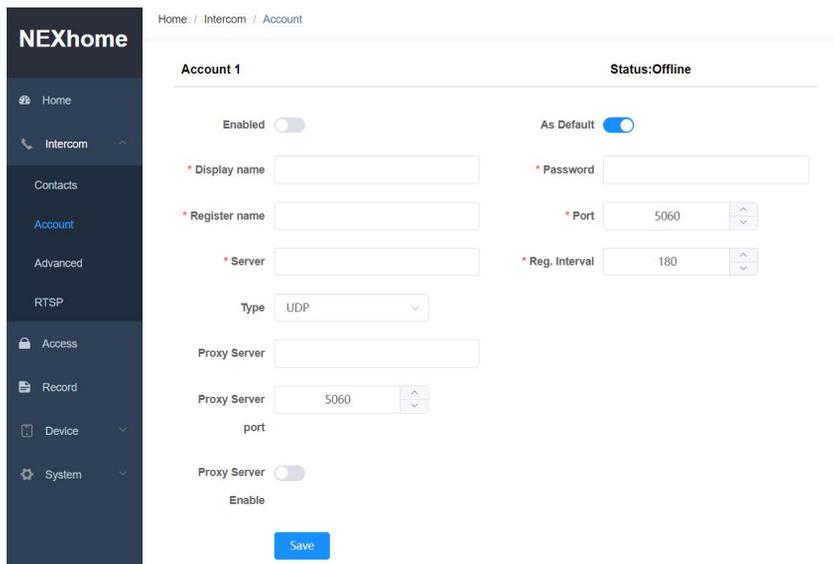
- Audio coding:** This section allows for selecting alternative and available coding schemes. The 'Alternative coding' panel includes checkboxes for G722 and G729. The 'Available coding' panel includes checkboxes for PCM/U and PCMA. Navigation arrows are provided between the panels.
- Video coding:** This section includes settings for Codec (H264), Resolution (720P), Code rate (1024 kbps), and Coding load (97).
- DTMF:** This section includes settings for Type (RFC2833) and Load (101). A 'Save' button is present below the settings.
- Call settings:** This section includes settings for Maximum talk time (5 Minute), Maximum call-in time (60 Second), Maximum call-out time (60 Second), and Group Calling (Enabled). A 'Save' button is present below the settings.
- Auto Answer:** This section includes an 'Enable' checkbox (checked), Auto Answer Delay (0 Second), and Auto Answer Mode (Audio). A 'Save' button is present below the settings.

3.2.3 SIP Account Setting

In the device backend, click the **SIP Account** button to set the SIP account information. It can also automatically synchronize settings after binding to the server.



In the web backend, you can set up a SIP account in the intercom account.



3.3 Access Control Configuration

3.3.1 Adding New Passwords

In the device backend, after clicking on **Credentials** button, you can view or edit all current access control and their effective dates. By clicking the "Add" button, you can add a new access card, password, or facial access control. You can choose to apply access control to three different doors A, B, and C.

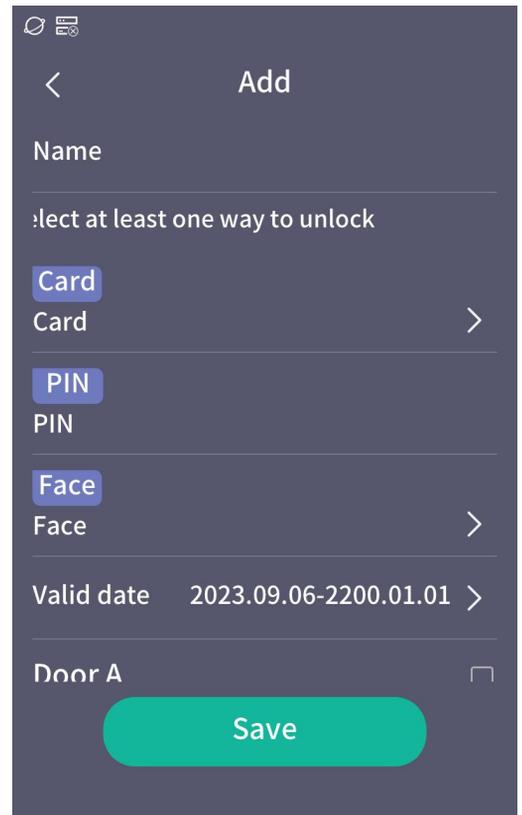
In the web backend, in the **Access** section, you can click the "Add" button to add a new access control. The following is the relevant information that needs to be filled in:

Name: Customer Name

Card number: IC card number, please swipe the card once first to obtain the card number record

PIN: Access control password

Valid date: The effective date of the card, which defaults to 2200 years from the current day



Valid weekday: Card effective period, mu

Valid hours: The effective period of the card, default to 00:00 to 23:59,can set multiple

Upload photos:Upload photos to the device for facial recognition

The screenshot shows the 'Add' form in the NEXhome web interface. The form is titled 'Add' and has a close button 'X'. It contains the following fields and options:

- Name:** A text input field with a red asterisk indicating it is required.
- Card number:** A text input field.
- PIN:** A text input field.
- Valid date:** A date range selector showing '2023-09-07' to '2200-01-01'.
- Valid weekday:** A section with a checked 'All' option and checkboxes for 'Sunday', 'Monday', 'Tuesday', 'Wednesday', 'Thursday', 'Friday', and 'Saturday', all of which are also checked.
- Valid hours:** A section with an 'Add' button and a time range selector showing '00:00:00' to '23:59:59', with a 'Delete' button.
- Valid Door:** A section with checkboxes for 'Door A', 'Door B', and 'Door C', all of which are unchecked.
- Upload:** A blue button for uploading a photo, located next to a large empty rectangular area.
- Confirm/Cancel:** Two buttons at the bottom of the form.

3.3.2 Relay Setting

In the web backend, enter **Device-Input-Output-Relay** can set the relays.

Number: Relay number, including relay 1, relay 2, and relay 3.

ID: Relay number, including relay 1, relay 2, and relay 3

Mode: Normal, Normally Open, Normally Closed

Hold delay(s): The relay remains in the triggered state for a certain period of time before resetting, i.e. the door opening hold time

Trigger interval(s): The time difference between each unlock trigger. If the current trigger time minus the last trigger time is less than the trigger interval, the unlock fails

DTMF mode: The input digit of the DTMF code, defaults to 1 digit

DTMF: The input DTMF code, which defaults to #, is used

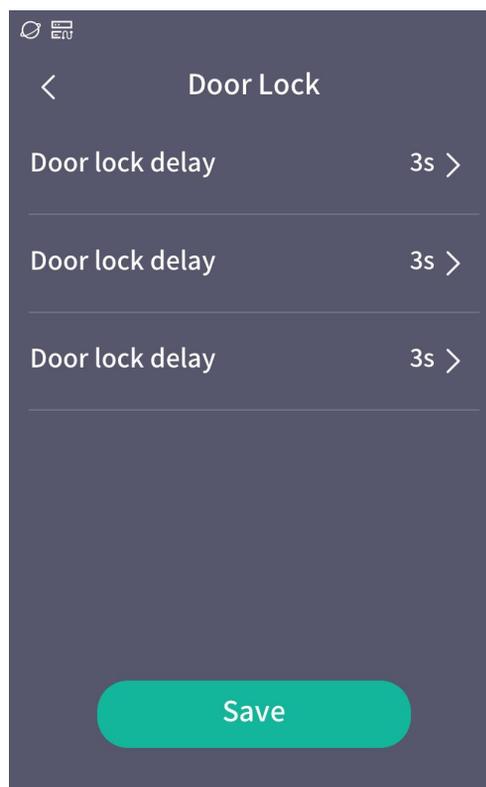
for remote door opening

Relay Name: Default is relay

Status: On/Off

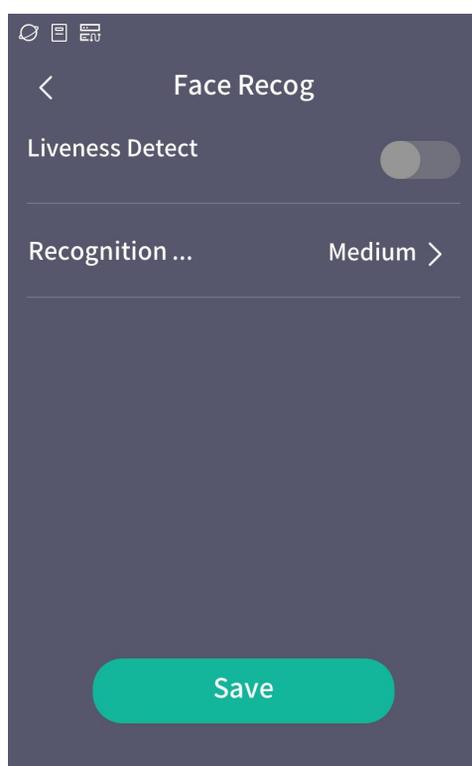
3.3.3 Door lock/Door magnetic delay setting

In the device backend, click the **Door Lock** button to set the door lock delay time.



3.3.4 Face Recognition

In the device backend, enter the facial recognition interface to enable or disable liveness detect and configure recognition sensitivity. Turn on or off homepage QR code recognition, turn on or off camera.



In the device's webside backend ,in **Access-Authentication Setting** ,it is possible to enable or disable facial liveness recognition, set the liveness severity level, facial recognition sensitivity, facial recognition resolution, enable or disable homepage QR code recognition, set card number matching

mode, and select the unlocking type for illegal unlocking reporting and capture.

The screenshot shows the NEXhome mobile application interface. On the left is a dark sidebar menu with the following items: Home, Intercom, Access, Record, Device, Display, Sound, Light, Input-Output, Connection, System, and Basic. The main content area is titled "Authentication Setting" and contains several configuration options, each with a dropdown menu:

- Face Liveness Enable: Enabled
- Liveness strict level: High
- Face Recognition Sensitivity: Max
- Turn off camera when idle: Disable
- Homepage Qrcode Recognition: Enabled
- Card number match type: Full match
- Illegal unlocking report capture: Select

A blue "Save" button is located at the bottom of the settings area.

3.3.5 Wiegand

In the device's web backend, in the **Device - Input/Output - Wiegand** section, you can configure the Wiegand type (26/34), Wiegand mode, functions, Wiegand sequence, Wiegand output sequence. If the mode is set to output, you need to enable the Wiegand output PIN.

The screenshot shows the NEXhome web interface. On the left is a dark sidebar with the NEXhome logo and a menu with items: Home, Intercom, Access, Record, Device, Display, Sound, Light, Input-Output (highlighted), and Connection. The main content area is titled 'Wiegand Setting' and contains several dropdown menus: 'Wiegand type' (Wiegand-26), 'Wiegand mode' (Input), 'Fuction' (Relay), 'Wiegand sort' (Ordinal), 'Wiegand output sort' (Ordinal), and 'Wiegand output PIN' (Disable). A blue 'Save' button is located below these settings. Below the 'Wiegand Setting' section is an 'RFID' section with a 'Card number' dropdown menu set to '8HN' and the text 'display' below it.

3.3.6 RFID anti duplication

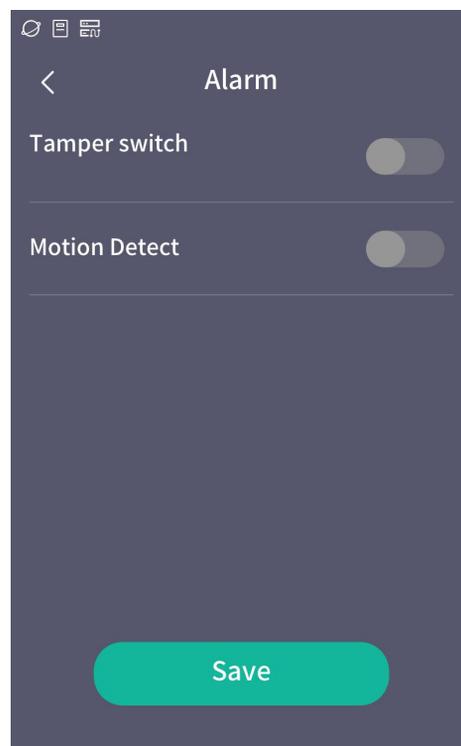
In the web backend of the device, you can set the card number display type (the same as the card number display type in **Access** interface), IC card anti duplication level, and read-write sector in the **Device -Input/Output- RFID**.

The screenshot displays the NEXhome web interface. On the left is a dark sidebar with the 'NEXhome' logo and a menu containing: Home, Intercom, Access, Record, Device, Display, Sound, Light, Input-Output (highlighted in blue), Connection, System, and Basic. The main content area shows the 'Wiegand output PIN' set to 'Disable' with a 'Save' button below it. The 'RFID' section is titled and contains the following settings: 'Card number display' set to '8HN', 'IC card copy protection level' set to 'Difficult', 'Default section' set to '0', and 'Default block' set to '1'. Below these are two text input fields for 'Key A' and 'Key B', both containing 'FFFFFFFFFFFF'. A 'Save' button is located at the bottom of the RFID section. The 'Other Setting' section is partially visible at the bottom.

3.4 Alarm Setting

3.4.1 Tamper Alarm

In the device backend, click the **Alarm** to set the tamper alarm on or off. Click the black protruding button on the right side of the device back to release the tamper alarm.



In the web backend of the device, you can turn on or off the anti disassembly alarm in **Device-Input/Output-Other Setting**. Press the black raised button on the right side of the device back

to release the anti disassembly alarm.

Mobile monitoring can be turned on or off, and trigger time intervals can be set to report records.

Other Setting

Dismantle

Motion Detection

Motion Detection **Seconds**
Interval

Save

3.4.2 Door Magnetic Alarm

In the web backend, you can configure the door magnet alarm in the **Device-Input-Output**, in the Input Port section, select the function as Magnetism.

The screenshot displays the NEXhome web interface for configuring a door magnetic alarm. On the left is a dark sidebar menu with the NEXhome logo at the top and various settings categories: Contacts, Account, Advanced, RTSP, Access, Record, Device (highlighted with a caret), Display, Sound, Light, Input-Output, and Connection. The main content area is titled 'Input port' and contains several configuration fields: ID (dropdown menu with 'Input port1'), Trigger state (dropdown menu with 'Low'), Fuctionon (dropdown menu with 'Relay'), Relay ID (dropdown menu with 'Relay1'), Hold delay(s) (dropdown menu with '0s'), and Port name (text input field with 'input1'). A blue 'Save' button is located below these fields. Below the 'Input port' section is the 'Other Setting' section, which includes a 'Dismantle' dropdown menu set to 'Disable' and another blue 'Save' button.

3.5 Internal Door Opening/Door magnetic Setting

In the backend of the web end, you can select the function of "relay setting internal door opening" in the input port section of the device input/output settings. Specific configurations include number, trigger status, relay number, hold delay, input port name, etc.

Select the function as door magnet, which can be configured with a specific number, door magnet type, hold delay, and input port name.

The screenshot displays the NEXhome web interface. On the left is a dark sidebar with the 'NEXhome' logo and a menu containing: Contacts, Account, Advanced, RTSP, Access, Record, Device (with a dropdown arrow), Display, Sound, Light, Input-Output, and Connection. The main content area is white and contains two sections. The 'Input port' section has a 'Save' button at the top and the following fields: ID (dropdown menu with 'Input port1'), Trigger state (dropdown menu with 'Low'), Fuctionon (dropdown menu with 'Relay'), Relay ID (dropdown menu with 'Relay1'), Hold delay(s) (dropdown menu with '0s'), and Port name (text input field with 'input1'). A 'Save' button is located below these fields. The 'Other Setting' section has a 'Dismantle' dropdown menu with 'Disable' selected and a 'Save' button below it.

3.6 System Logs

3.6.1 Record

In the web backend, various records of the device can be viewed in the **Record**, including the following:

Unlock record: various methods such as card swiping, facial recognition, password, and DTMF for door opening records

Call record: Record of the calling party and the record of being called

Alarm Record: Device alarm record including magnet alarm and dismantle alarm

Home / Record

admin

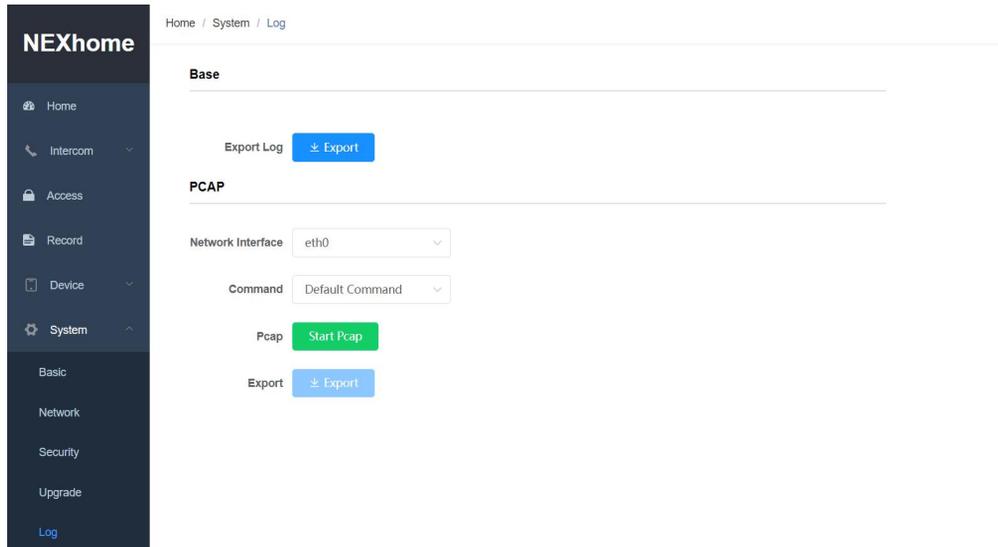
Unlock record | Call record | Alarm record

Type: All | Name: | Start: | To: | End: | Search

Index	Name	Content	Type	Door	Time	Status
1			PIN		2023-09-04 17:41:48	Failure
2	192.168.10.102	#	Call	C	2023-09-04 17:41:04	Success
3	192.168.10.102	#	Call	B	2023-09-04 17:41:03	Success
4	192.168.10.102	#	Call	A	2023-09-04 17:41:03	Success
5	engineer	#	Edge gateway	A	2023-09-01 17:57:27	Success
6		9999	PIN		2023-09-01 17:28:28	Failure
7	Indooror	192.168.10.100	Remote	A	2023-08-29 17:01:35	Success
8	Indooror	#	Call	C	2023-08-29 17:01:27	Success
9	Indooror	#	Call	B	2023-08-29 17:01:27	Success
10	Indooror	#	Call	A	2023-08-29 17:01:27	Success

3.6.2 Logs and Packet Grabbing

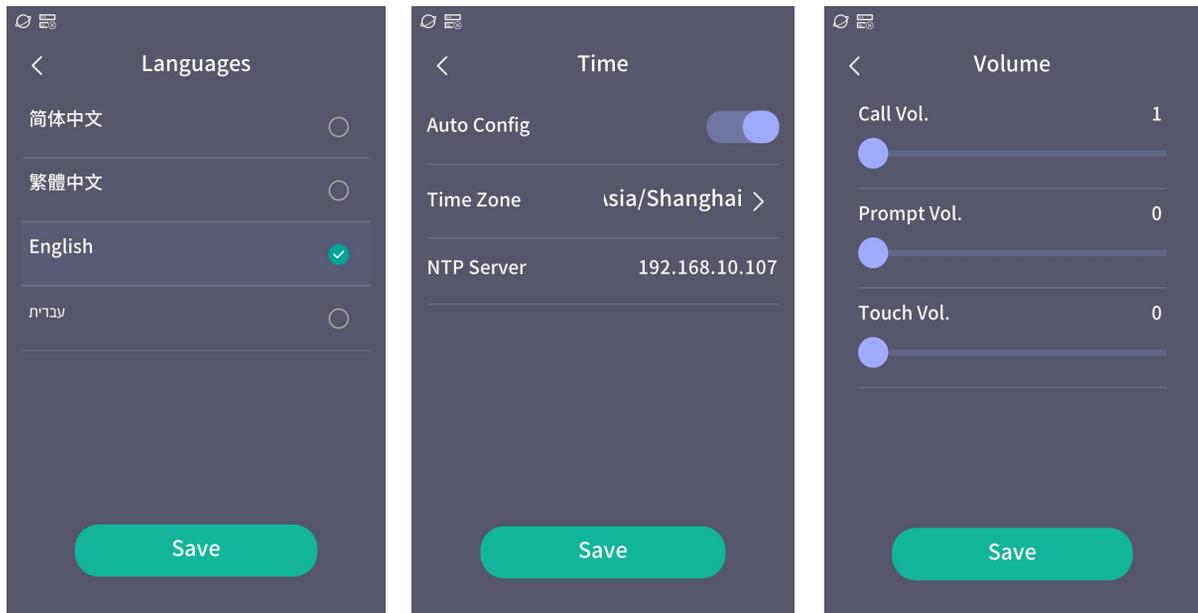
In the backend of the web side ,enter System - Log setting, you can export the logs in .tgz zip format which can also be



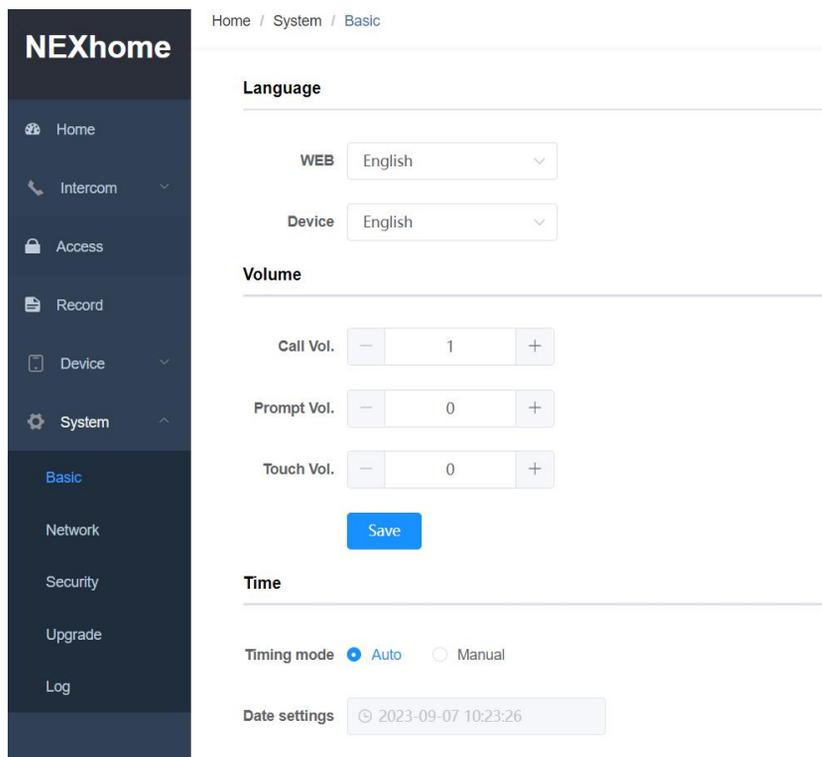
3.7 System Settings

3.7.1 Language, Volume, and Time

On the device backend page, click on **Language** settings to change the device display language. Currently, it supports Simplified Chinese, Traditional Chinese, English, and Hebrew. Click on the **Volume** settings to set the call volume, prompt volume, touch volume and alarm volume. Click on **Time** settings to set the time zone and the time server to connect to. You can also cancel automatic settings and manually set the device time instead.



In the web side, you can set the language of the web in the upper right corner of the page, which supports Simplified Chinese, Traditional Chinese and English. In System-Basic Settings, you can set the language of web and device, and you can also set the Time zone and NTP server, also there are two ways of automatic time calibration and manual time calibration. You can also set up fluorescent lamps to save time. In Device-Sound Settings, you can set the call volume, prompt volume, touch volume and alarm volume. In the device display settings, you can set the homepage language option, default language reset time, and information bits.



NEXhome

- Home
- Intercom
- Access
- Record
- Device
- Display
- Sound
- Light
- Input-Output
- Connection
- System

Daylight saving time

Func enable

* Offset Minutes

Date mode

Start time month day hour

End time month day hour

Week mode

Start month End month

Start week End week

Start day End day

Start hour End hour

NEXhome

- Home
- Intercom
- Access
- Record
- Device
- Display
- Sound
- Light
- Input-Output
- Connection

Home / Device / Sound

Volume

Call Vol.

Prompt Vol.

Touch Vol.

Alarm Vol.

NEXhome

- Home
- Intercom
- Access
- Record
- Device
- Display
- Sound
- Light
- Input-Output
- Connection

Homepage

Language English 简体中文 繁體中文 עברית

Default language Seconds

reset timeout

Description

Mode

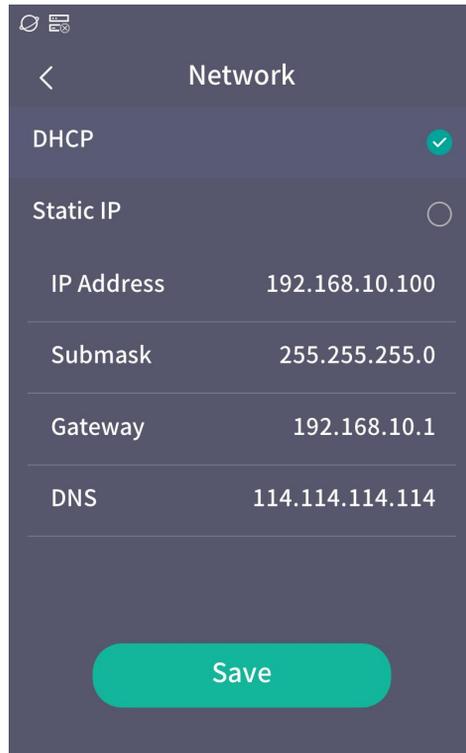
Mode

Button1 Name

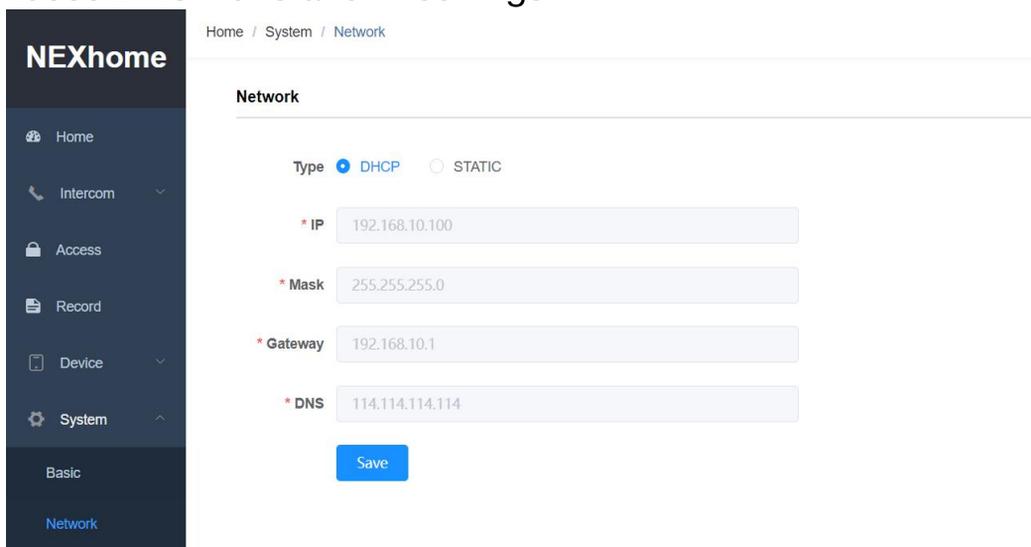
Button2 Name

3.7.2 Network Settings

In the device backend, click on **Network** setting to change the current network settings and select DHCP or static IP settings.

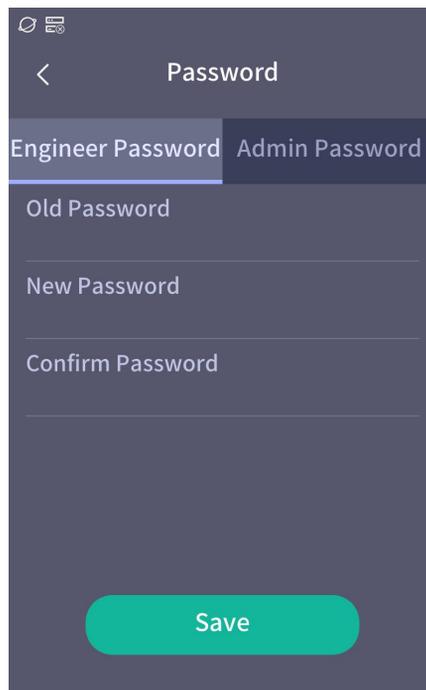


In the **System-Network** settings on the web side, you can also choose DHCP or static IP settings.



3.7.3 Password Settings

In the device backend, click the **Password** button to change the password for logging in to the engineering interface and logging in to the web interface.



In the **System-Security** settings on the web side, the password for logging into the web interface can be changed.

Home / System / Security

Change Password

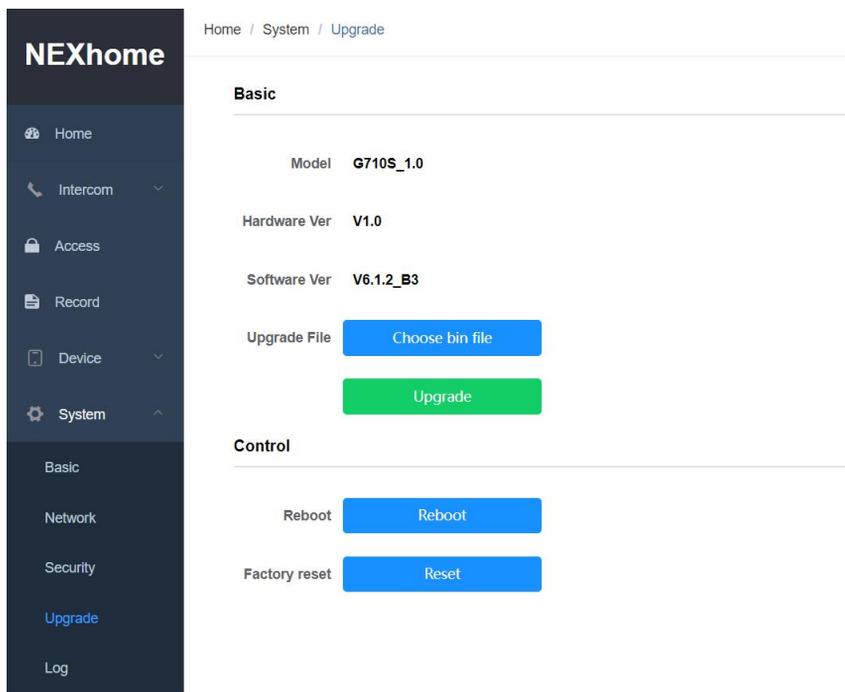
* Old password

* New password

* Confirm password

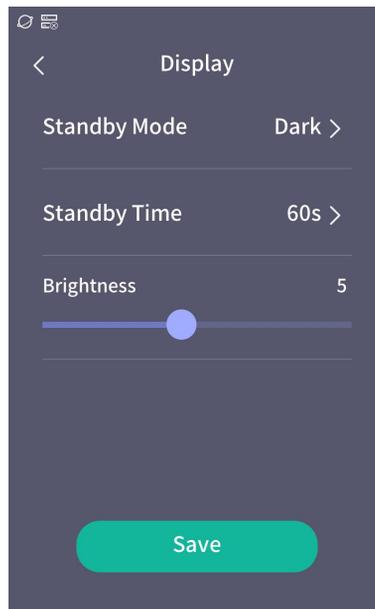
3.7.4 Firmware Upgrade

In the **System-Upgrade** of the web side, you can view the current version number of the device and use the .bin file to upgrade the device software.

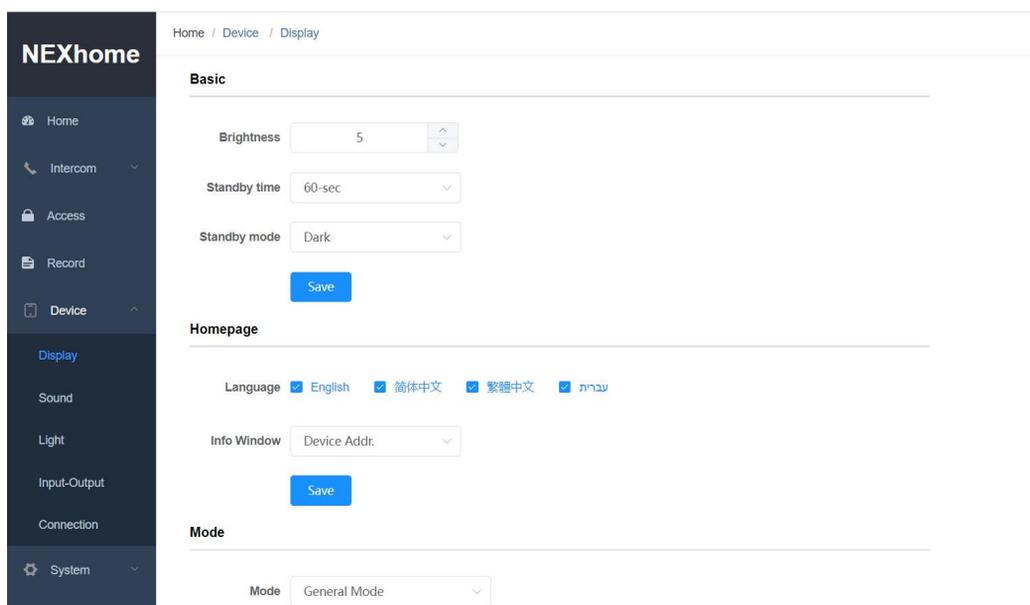


3.7.5 Screen Settings

On the backend of the device side, click the **Display** button to set the standby mode and standby time of the device, and also to change the brightness of the screen.

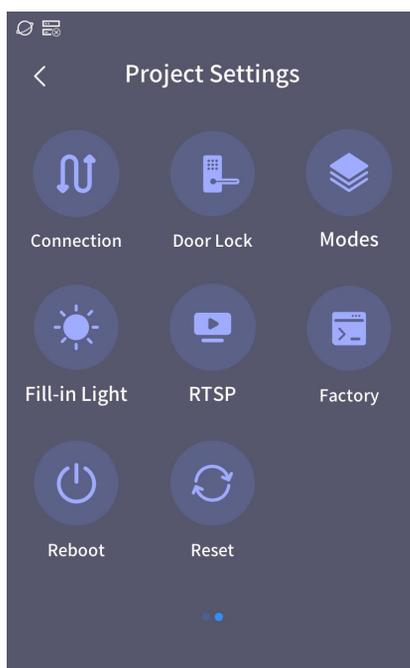


In Device - Display Settings - Basic of the web side backend, you can also set the brightness of the device screen, the standby time and the standby mode.

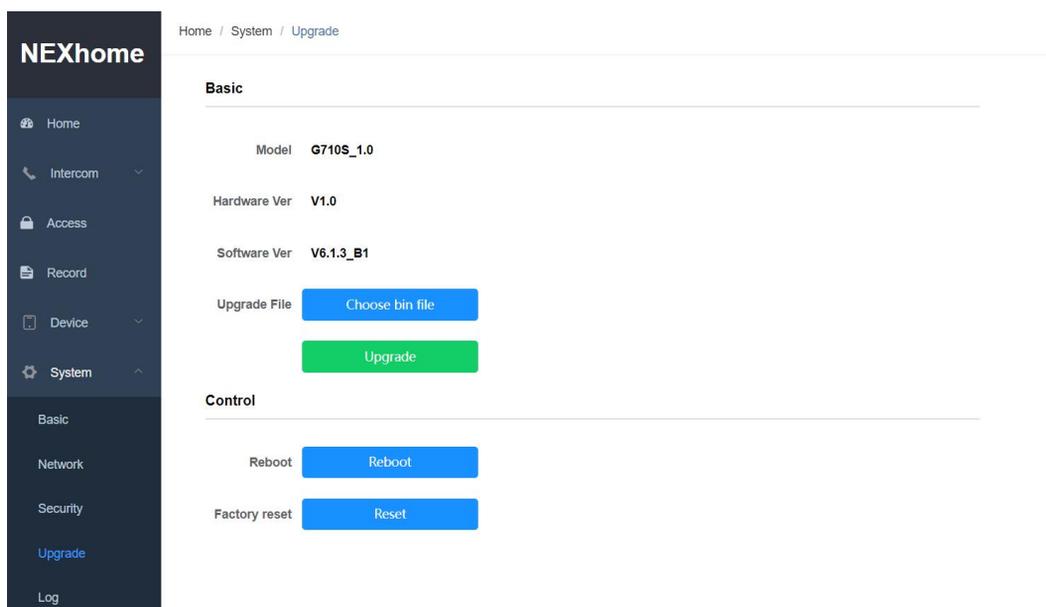


3.7.6 Restart and Reset

In the device backend, click the **Reboot** button to restart the device, and click the **Reset** button to reset the device.

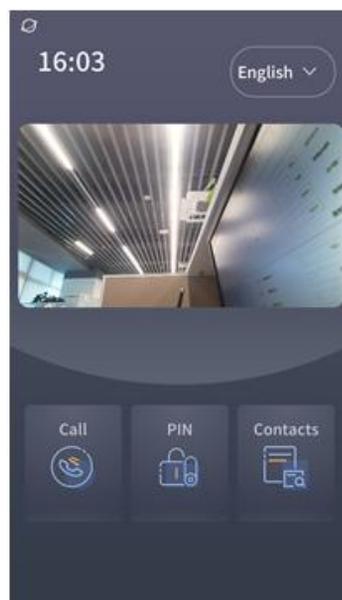


In the System-Upgrade section on the web side, the device can be reboot or reset.



3.7.7 Modes Settings

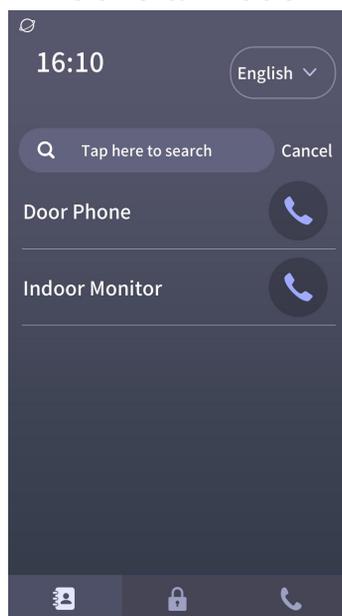
In the backend on the device side, click the Mode button to display the different main menus of the device, including General Mode, Access Mode, Doorbell Mode, and Directory Mode.



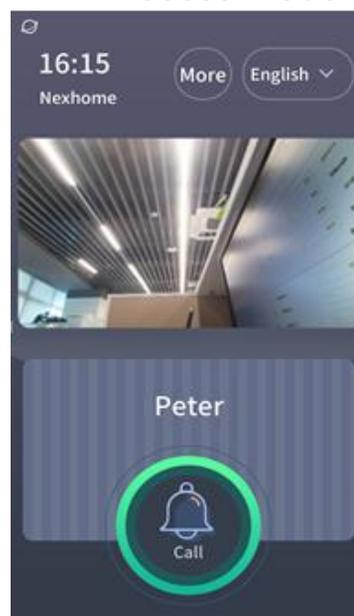
General Mode



Access Mode



Directory Mode



Doorbell mode

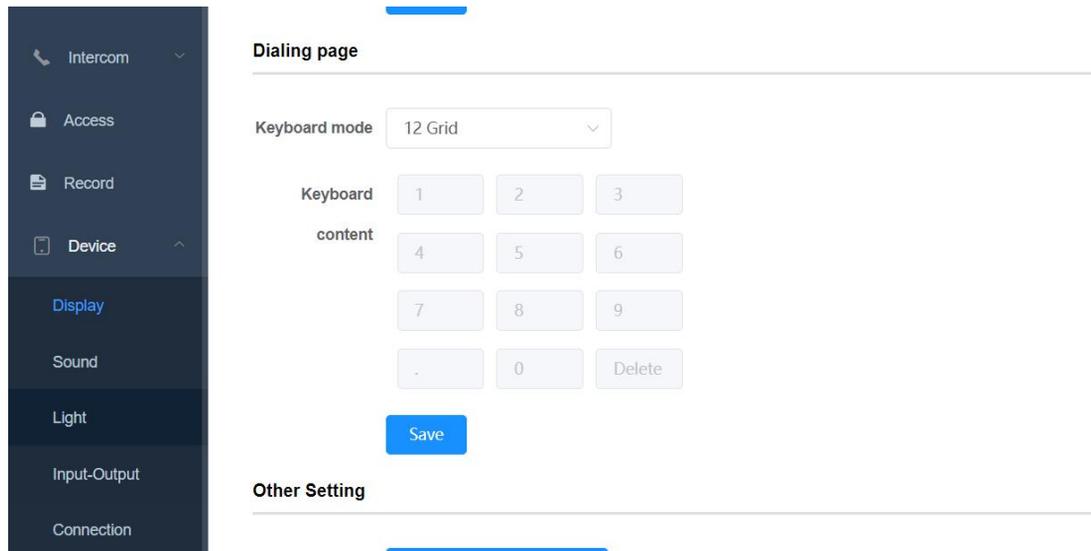
In the Device-Display-Mode of the web side, the different main menus of the device can also be selected, again including General, Access, Doorbell and Directory modes.

3.7.8 Contacts Page Settings

In the **Device-Display** on the web side, You can choose whether to display the group name in the address book, You can also choose whether to enable the address book search function.

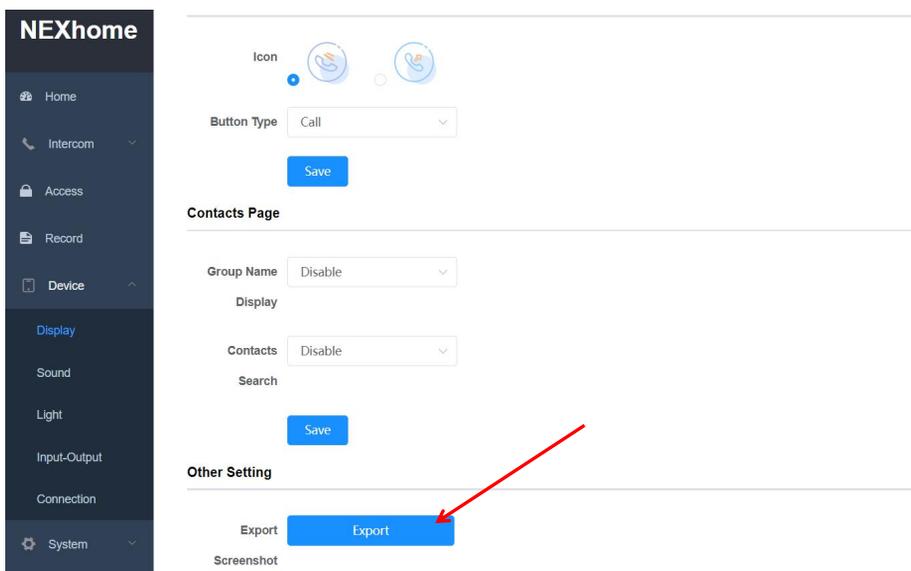
3.7.9 Dialing interface settings

In the **Device-Display** of the web backend, you can choose the keyboard format displayed on the dialing interface.



3.7.10 Device screenshot

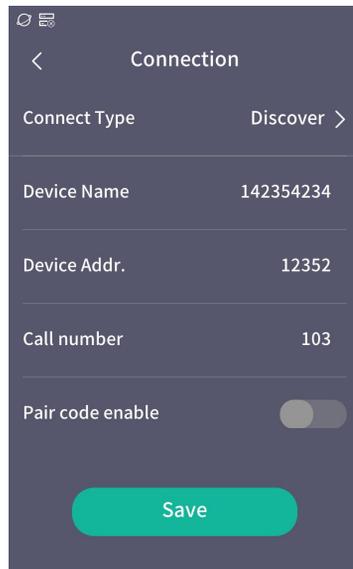
In the Device-Display Settings of the web side backend, in the Other Setting section, click the Export screenshot button to export the image of the current interface of the device.



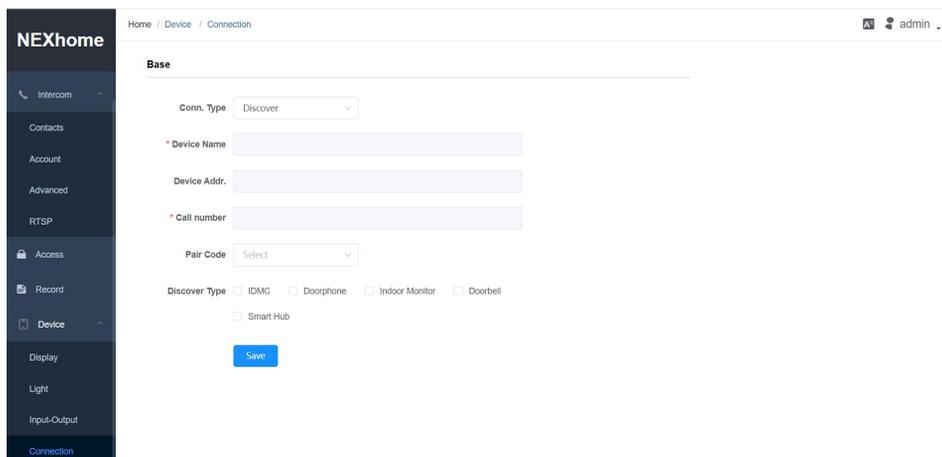
3.8 Advanced Settings

3.8.1 Connection Settings

In the device backend, click the **Connection** Settings button, select the type of connection (usually self discovery mode), modify the device name, address, call number, and select whether to enable pairing codes.

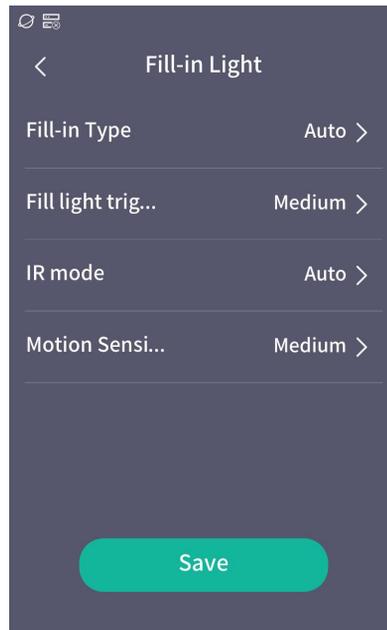


In the web backend, you can also change the device's connection settings by clicking **Device-Connection** Settings.

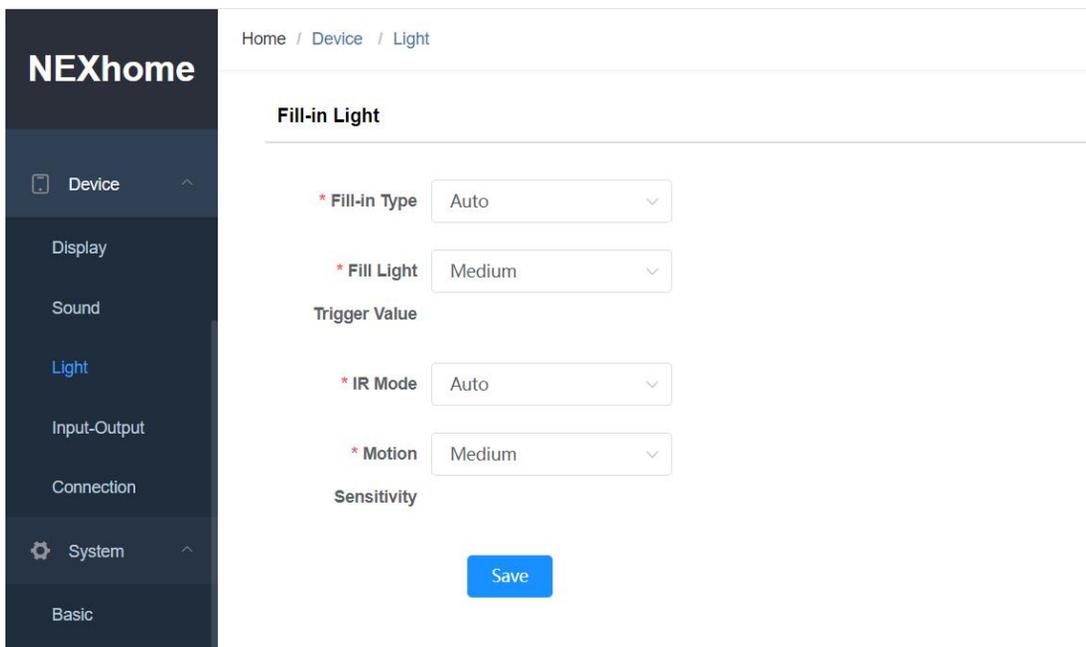


3.8.2 Light Settings

In the device backend, click the **Fill-in Light** button to set the fill light type and infrared light mode.



In the web backend, you can also change the device's lighting settings by clicking on **Device-Light** Settings.



3.8.3 QR Code Settings

On the backend interface of the device, click the QR code button to view the binding QR code and scan code binding.

In the web backend, click on the **Device-connection** to set the content of the application QR code, or set the corresponding application binding QR code content.



Qrcode

Content

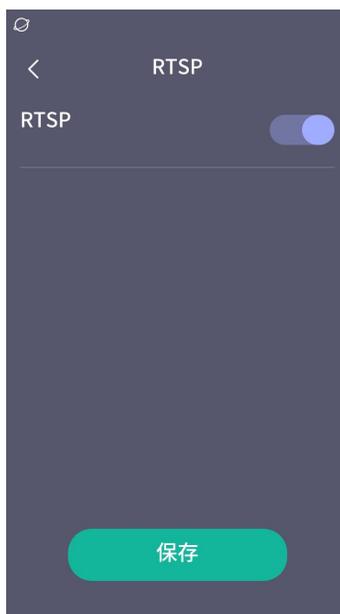
Update

Please use the app to scan the QR code to bind

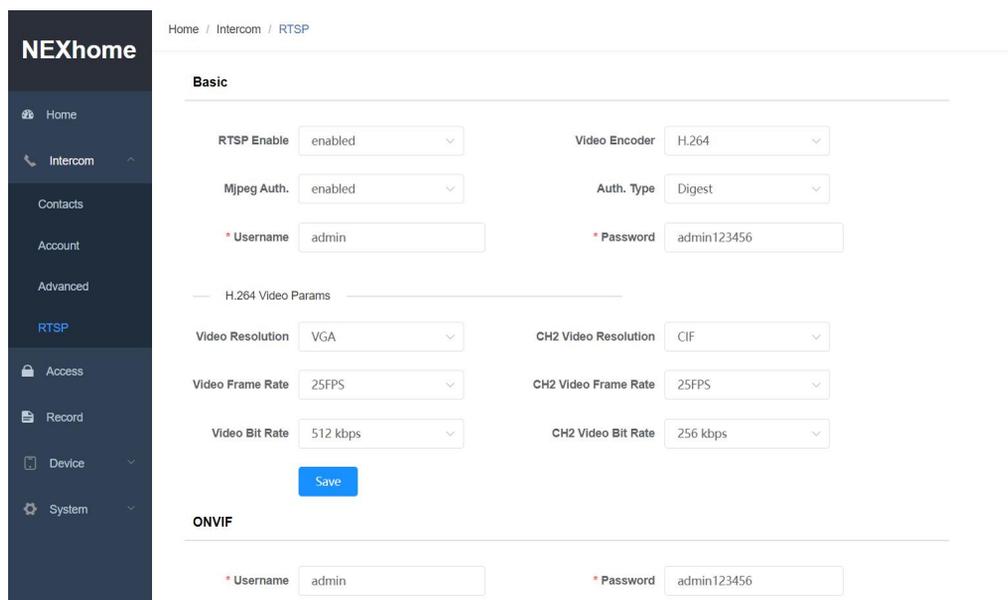


3.8.4 RTSP and ONVIF Settings

In the backend of the device side, click the **RTSP** button to choose whether to enable RTSP



In the web backend, click on **Intercom-RTSP** to set RTSP related parameters.



RTSP enable: After enabling, the computer's vlc, ffplay, and other clients can play RTSP video streams from the device

Mjpeg authentication: Enter username and password

User name: To play the device's rtsp video stream, confirm the user name

Password: To confirm the password for playing rtsp video streams on the device

RTSP Video Streaming

Video encoder: The video encoding is in H.264 format

Video resolution: default 720P, with QCIF, QVGA, CIF, VGA, 720P options

Video frame rate: default 25FPS

Video bitrate: default to 1024kbps, with options of 128kbps, 256kbps, 512kbps, 1024kbps, and 2048kbps

Playing RTSP video streams from devices

You can play rtsp video streams from devices using clients such as vlc and ffplay on your computer,

Main stream address: rtsp://Device IP address:
5541/stream/main

Secondary stream address: rtsp://Device IP address:

5541/stream/sub

ONVIF User name and Password: default and rtsp user name and password are the same, when Mjpeg authentication is on, ONVIF user name and password need to be the same as rtsp's.

IP Visible: Enable **IP Visible**, you can use ONVIF Device Manager tool, enter the device username and password, onvif tool can automatically search the device, you can click to monitor.

3.8.5 Audit Tracker

In the web backend, click on **System-Audit Tracker** to view various inspection results.

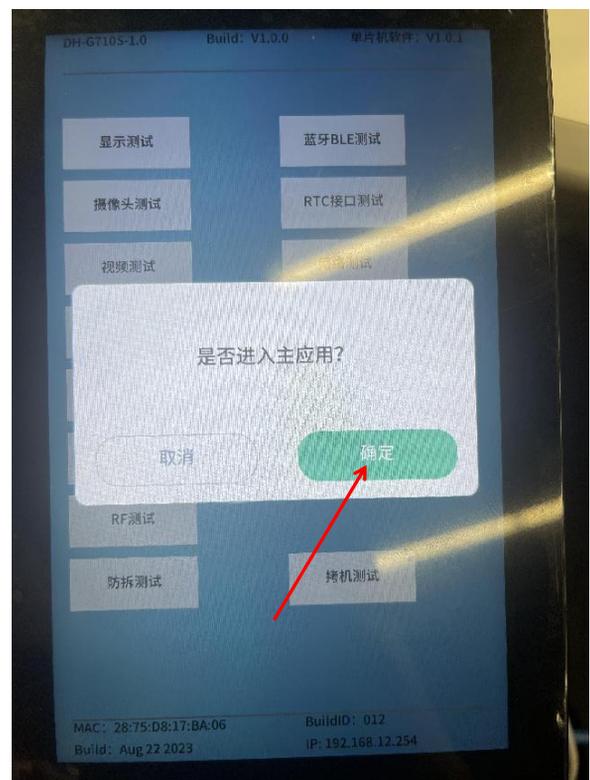
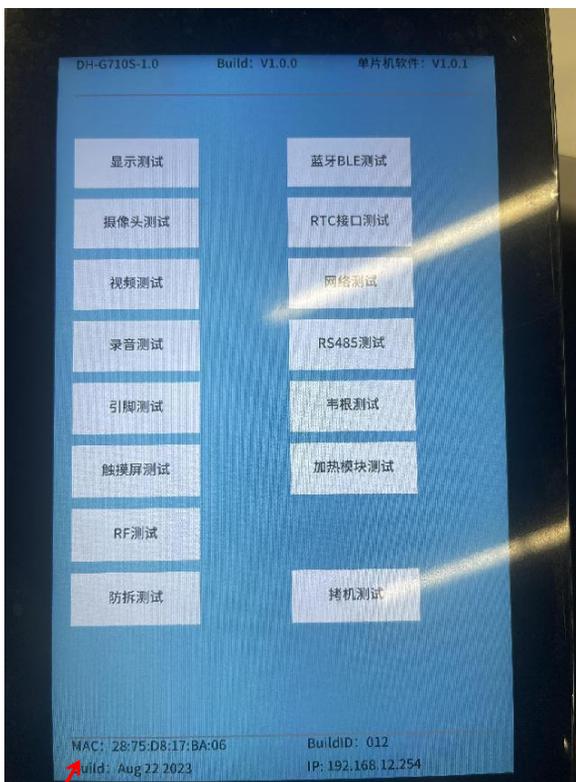
The screenshot shows a web interface with a dark sidebar on the left containing navigation options: Device, Display, Sound, Light, Input-Output, Connection, System (selected), Basic, Network, Security, Upgrade, Log, and Audit Tracker. The main content area is divided into two sections: 'Network Tracker' and 'Interface Tracker'. Each section has a 'Refresh' button and a table of inspection results.

Function	Tag	State	Description
DNS	218.85.157.99	Success	
NTP Server	ntp.nexhome.cn	Success	
PAAS Server	lol-us.nexhome.ai	Success	online
slp1 Server	slp-us.nexhome.ai	Success	
slp2 Server		Failure	SIP2 offline

Function	State	Description
Microphone	Success	

3.8.6 Factory Testing

On the backend status information interface of the device, click on the MAC address area three times in a row to enter the factory test. Enter the password 002396 to enter the factory test interface. The factory test interface is used to detect hardware issues of the device and is only for professional technicians. Please do not enter the factory test during normal configuration. If you accidentally enter the factory testing interface, simply quickly click on the "Mac" character in the bottom left corner, and when the "Enter Main Application" window pops up, select "Yes" to return to the



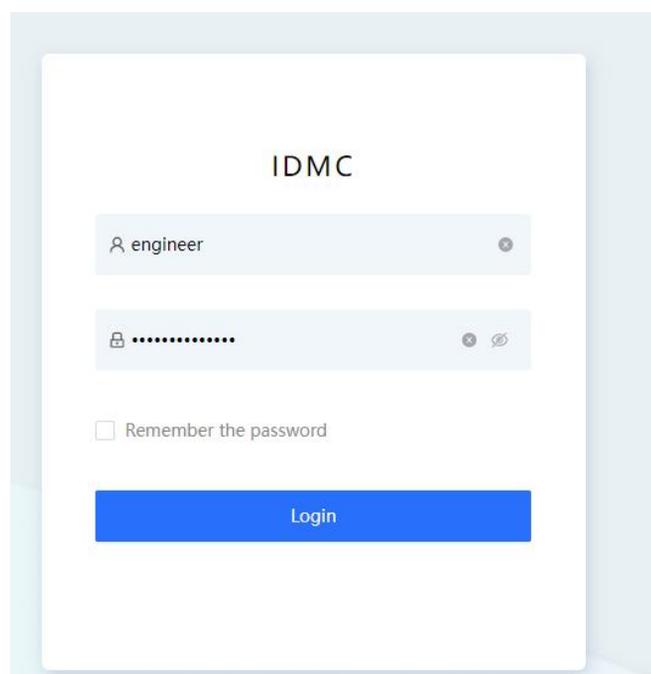
4 IDMC Configuration

IDMC (Device Management Center Based on SIP Protocol) is mainly used for community resident management centers. The IMDC platform is deployed in a local area network, allowing administrators to manage buildings, personnel, device, access control, intercom, and information comprehensively.

4.1 IDMC Platform Login

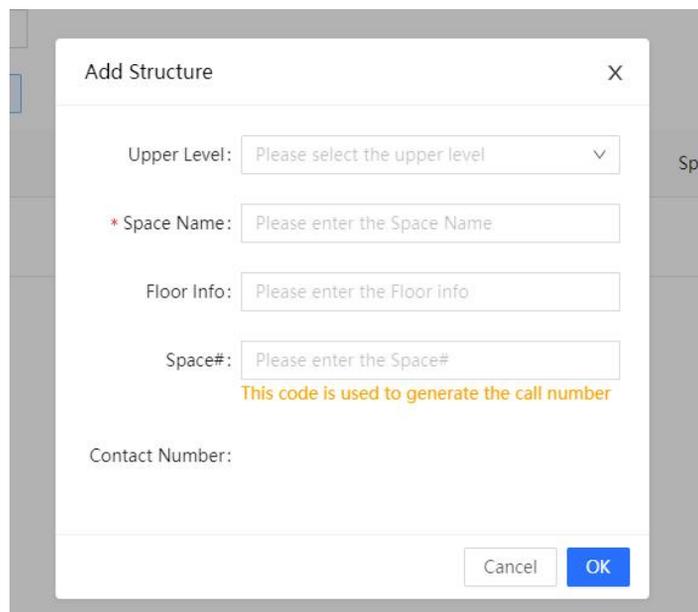
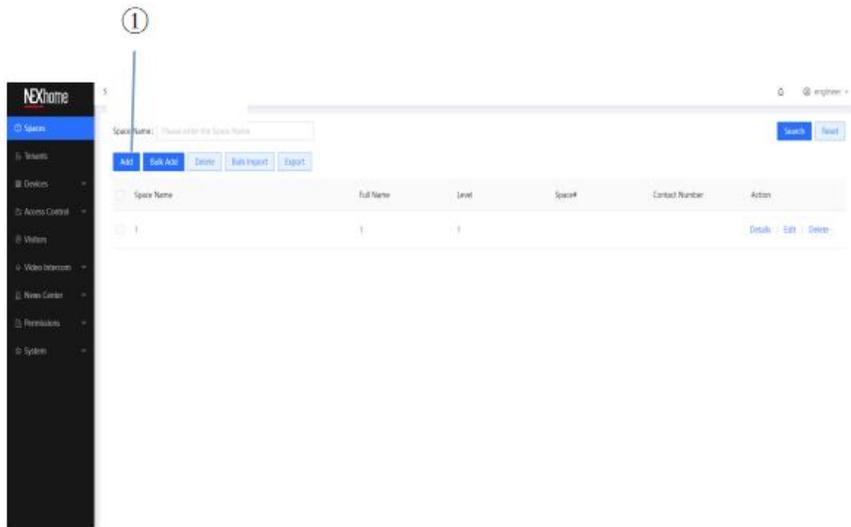
After installing the IDMC platform, double-click to open IDMC.exe and enter the IDMC platform webpage.

Enter account: engineer ;password: StarNetNexhome, click on Login to enter the IDMC platform interface.



4.2 Space Management

In the space management of the IDMC platform, click the **Add** button, fill in the space name and other information, and click to confirm the creation of the space.



4.3 Device Management

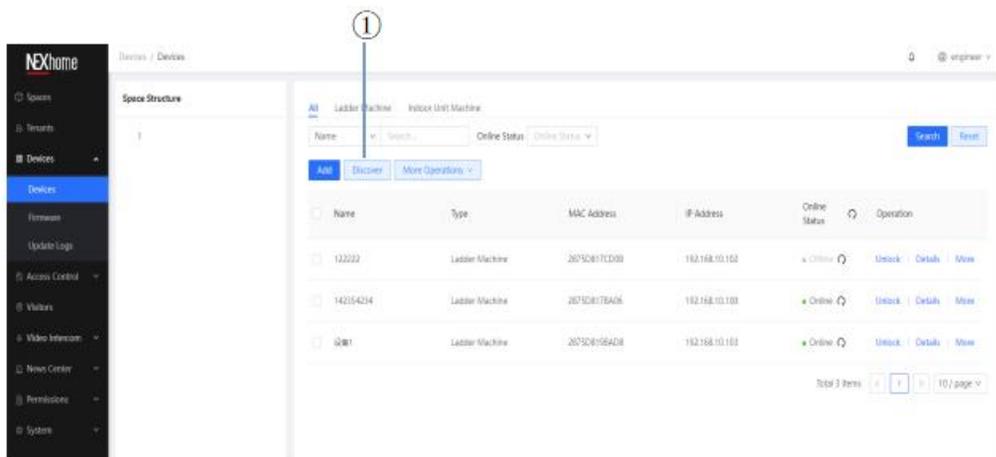
4.3.1 Adding Devices

In the **Devices-Devices** section of the IDMC platform, click the **Discover** button ① and the system will automatically search for devices under the same local area network. Click the add button to the right of the device name to add, set the associated space and device name for the device, and click save to add the device to that space.

When adding a device, the device MAC can be filled in, and the device can automatically register online when the network is accessible within the local area network.

The device can enable pairing code and fill in the location code and target IP in the connection settings, or register online.

The device is connected to a three-layer network environment and can be automatically assigned an IP address by enabling DHCP function in IDMC system management DHCP configuration.



Basic Setting

* Type:

* Location:

* Device Name:

Position:

MAC Address: [Scan](#)

Static IP Mode:

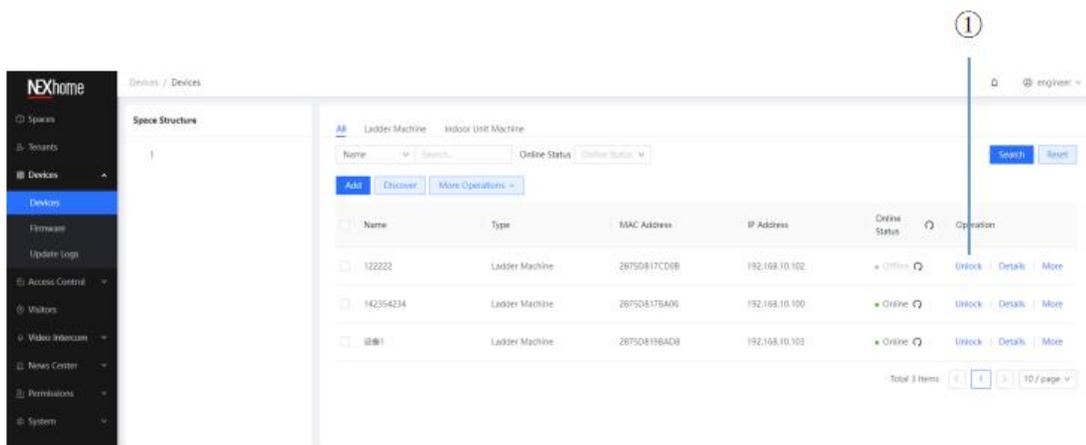
Open Space:

[Save](#) [Back](#)

4.3.2 Device Unlocking

In the **Devices - Devices** section of the IDMC platform, click **Unlock** button ① on the right side of the corresponding device, and the device will automatically unlock, device unlocking (access control unlocking or remote unlocking) supports capturing and uploading IDMC.

You can use the access credentials issued through IDMC to unlock.



4.3.3 Device Operation

In the Device Management section of the IDMC platform, click the "More" button on the right side of the corresponding device to edit, delete, restart, upgrade, and restore production of the device. You can operate to resynchronize the address book and access credentials in the device details.

<input type="checkbox"/>	名称	设备类型	MAC地址	IP地址	状态 ⌵	操作
<input type="checkbox"/>	G710s-test1	梯口机	2875D817BA06	192.168.10.100	● 离线 ⌵	开锁 详情 更多

共 1 条 < 1 >

- 编辑
- 删除
- 重启
- 升级
- 恢复出厂设置

4.3.4 Device Configuration

Add a configuration set in the IDMC platform system management device configuration, modify the configuration in the configuration set, and select the associated devices that need to be synchronized.

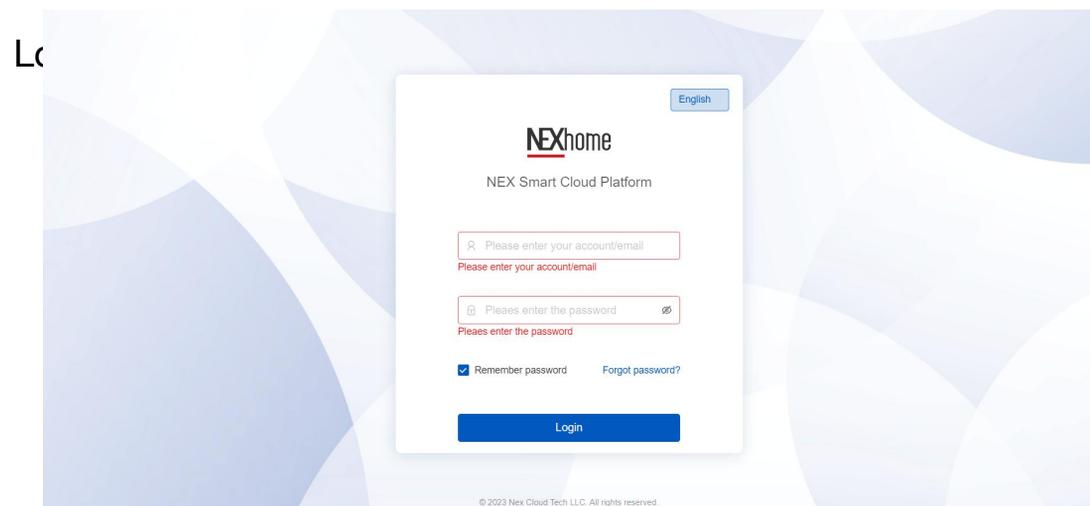
The screenshot displays the NEXhome management interface. On the left is a dark sidebar with navigation options: 空间管理, 用户管理, 设备管理, 门禁管理, 访客管理, 梯控管理, 可视对讲, 报警中心, 信息发布, 权限管理, 员工管理, and 系统管理. The '设备管理' (Device Management) option is highlighted in blue. The main content area features a search bar with '配置集' (Configuration Set) and '搜索...' (Search...). Below the search bar are filters for '设备小类' (Device Category) and '设备厂商' (Device Manufacturer). A '新增' (Add) button is located above a table. The table has columns for '配置集' (Configuration Set), '设备小类' (Device Category), '设备厂商' (Device Manufacturer), '创建者' (Creator), '创建时间' (Creation Time), '更新时间' (Update Time), and '操作' (Action). One device is listed: 'G710S' (Configuration Set), '梯口机' (Device Category), '星网天合' (Device Manufacturer), 'nexhome-admin' (Creator), '2024-07-11 11:04:22' (Creation Time), and '2024-07-11 11:04:22' (Update Time). The '操作' column contains links for '修改配置' (Modify Configuration), '关联设备' (Associate Device), '同步记录' (Sync Record), and '删除' (Delete). At the bottom right of the table area, it shows '共 1 条' (Total 1 item) and a pagination control for '1' out of '10 条/页' (10 items/page).

5 NexSmart Cloud Platform Settings

The NexSmart cloud platform consists of four parts: device, cloud server, management background and APP. It is used for community residents' management services. The management background is used for unified management of assets, devices, users and access control rights, and an APP is provided to facilitate owners to remotely open doors, cloud intercom and other operations. The APP supports both iOS and Android systems.

5.1 NexSmart Cloud Platform Login

In the upper right corner of the login page, you can set the language of the cloud platform, and in the lower left corner, you can choose to remember your password, if you forget your password, you can click the lower right corner to reset your password. Enter the correct username and password and click



5.2 Project Management

5.2.1 Project Management

Log in to your installer account, and in Project Management - Project Management in the NexSmart Cloud Platform, click New, fill in the project name and other information, and click OK to create the project.

Project / Project

Nexsmart Test1 Installer1

Residential Business Individual

Project name Please enter the keyword Search Reset

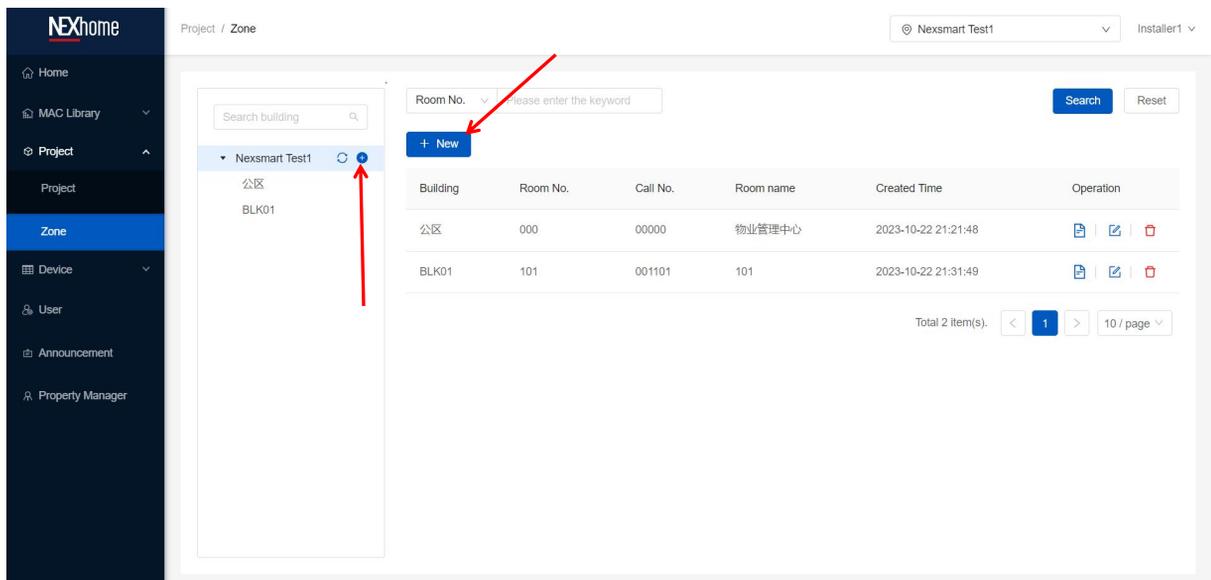
+ New

Project name	Property manager	Email	Last updated	Operation
NexsmartTest2	yx c	309685006@qq.com	2023-10-22 21:27:41	↻ ✎ 👤 🗑️
Nexsmart Test1	yx c	309685006@qq.com	2023-10-22 21:23:04	↻ ✎ 👤 🗑️
Nexsmart Cloud Intercom	yx c	309685006@qq.com	2023-10-16 10:02:54	↻ ✎ 👤 🗑️

Total 3 item(s). 1 10 / page

5.2.2 Space Management

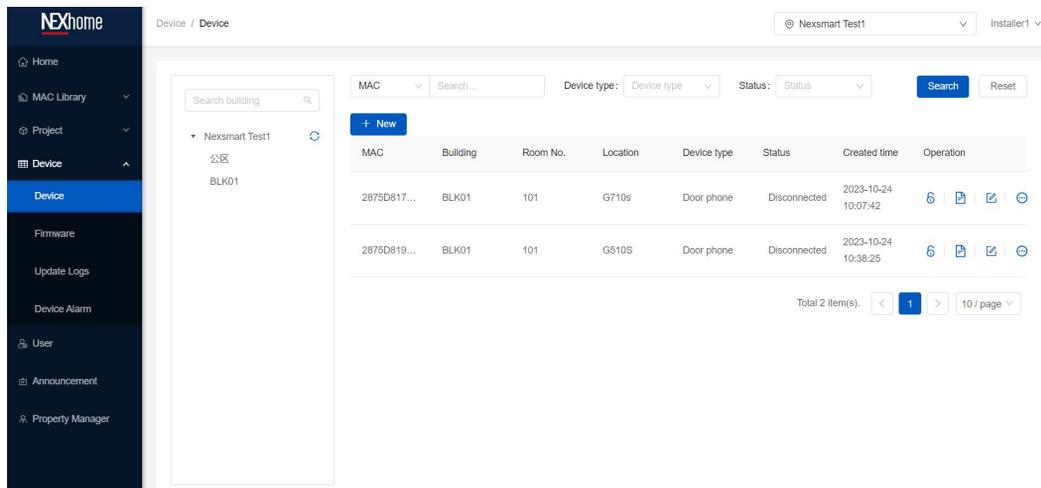
Log in to your installer account, and in Project Management - Space Management of NexSmart Cloud Platform, you can add new buildings and spaces under the project. Click the plus button on the left side to add a new building, and click the add button on the right side to add a new space under the building.



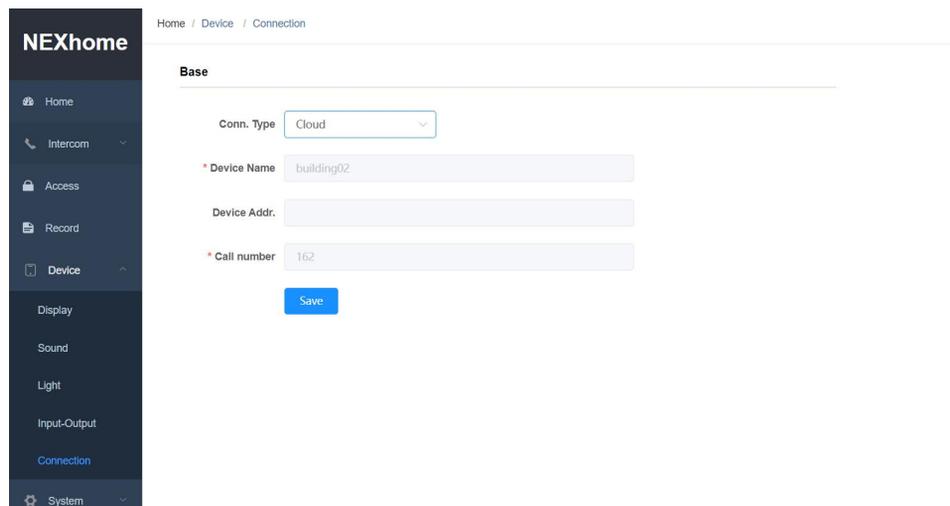
5.3 Device Management

5.3.1 Add Device

Log in to your installer account, and in NexSmart Cloud Platform's Device- Device, click Add on the right side, fill in the device type, space, and other information, and click OK to add a new device to the space.



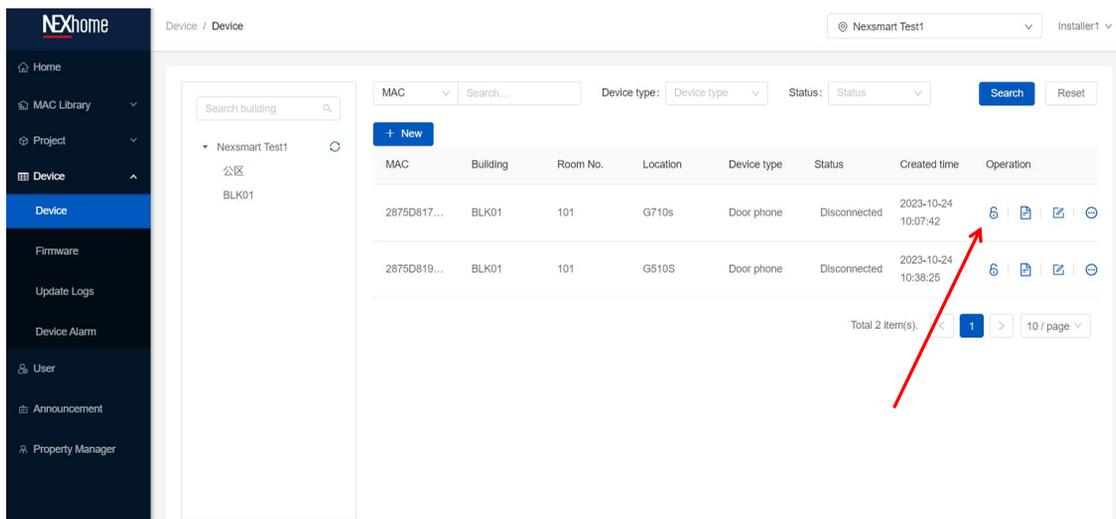
For added devices, you need to change the mode to cloud mode in the connection settings on the device side (web or device backend) in order to connect to the Nex Smart cloud platform.



5.3.2 Device Unlocking

Log in to the installer account or property manager account, and in the NexSmart Cloud Platform's Device - Device, click the Unlock button on the right side of the corresponding device to control the device to unlock remotely.

Log in to the property administrator account, in the user management interface, edit the user and click next to set the user's access password, access card, and access face. In the Smart Pass - Visitor interface, visitor access control can be added, access passwords and QR codes can be generated, and emails can be sent to the visitor's email. In the Smart Pass Employee interface, employee access control can be added, including access cards, access faces, and access passwords, and emails can be sent to the employee's email.



用户管理 / 编辑用户

访问权限

PIN: 00000000

卡号: 25752D7A

人脸

拍照

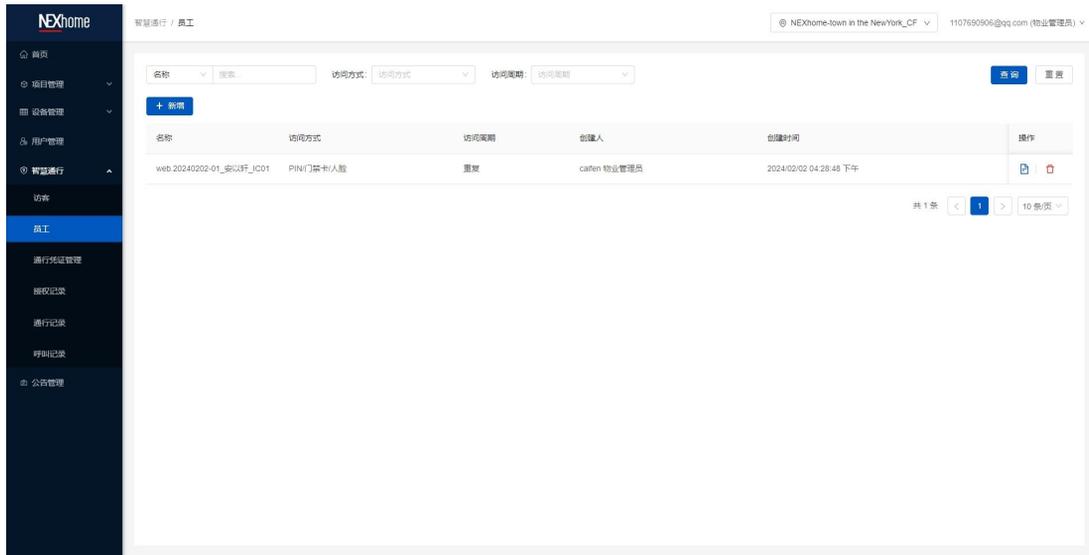
智慧通行 / 访客

临时人员

名称: 搜索: 访问方式: 访问周期:

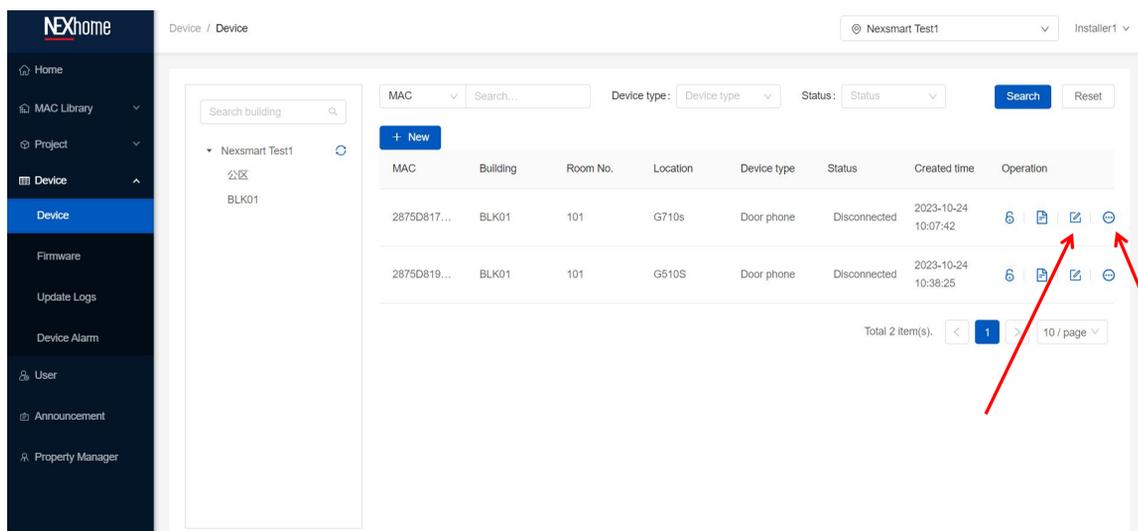
名称	访问方式	访问周期	创建人	创建时间	操作
web-20240202-02	二维码/PIN	重复	caifen 物业管理员	2024-02-02 04:40:37 下午	<input type="button" value="编辑"/> <input type="button" value="删除"/>
App-20240202-1	二维码/PIN	重复	Sean Xiao	2024-02-02 04:10:54 下午	<input type="button" value="编辑"/> <input type="button" value="删除"/>
App-20240201-1	二维码/PIN	不重复	Ffen Cai	2024-02-01 02:35:25 下午	<input type="button" value="编辑"/> <input type="button" value="删除"/>
web-20240129-1	二维码/PIN	重复	caifen 物业管理员	2024-01-29 10:05:51 上午	<input type="button" value="编辑"/> <input type="button" value="删除"/>
web-20240125-4	二维码/PIN	重复	caifen 物业管理员	2024-01-25 07:16:28 晚上	<input type="button" value="编辑"/> <input type="button" value="删除"/>
web-20240125-2	二维码/PIN	重复	caifen 物业管理员	2024-01-25 05:28:33 下午	<input type="button" value="编辑"/> <input type="button" value="删除"/>
web-20240125-2	二维码/PIN	重复	caifen 物业管理员	2024-01-25 05:26:11 下午	<input type="button" value="编辑"/> <input type="button" value="删除"/>
web-20240125-1	二维码/PIN	不重复	caifen 物业管理员	2024-01-25 05:11:53 下午	<input type="button" value="编辑"/> <input type="button" value="删除"/>
web-20240124-1	二维码/PIN	不重复	caifen 物业管理员	2024-01-24 05:28:42 晚上	<input type="button" value="编辑"/> <input type="button" value="删除"/>
web-20240124-1	二维码/PIN	不重复	caifen 物业管理员	2024-01-24 05:28:33 晚上	<input type="button" value="编辑"/> <input type="button" value="删除"/>

共 17 条



5.3.3 Device Operation

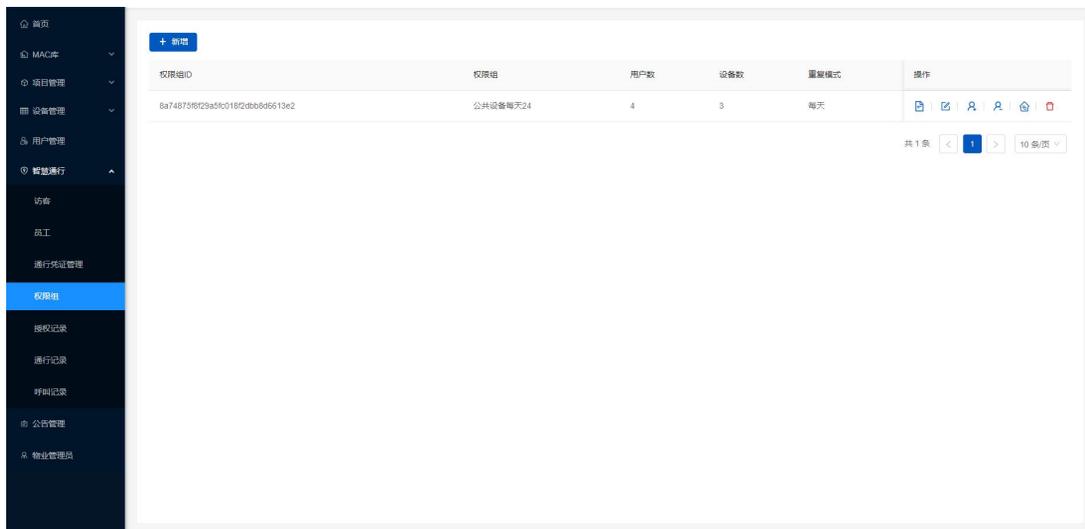
Log in to the installer's account, and in the Device - Device of NexSmart Cloud Platform, click the Edit button on the right side of the corresponding device to modify the basic information of the device, and click the More button next to it to delete, upgrade, reboot, and restore factory settings of the device.



5.4 Cloud Platform App Usage

5.4.1 Setting Permission Groups

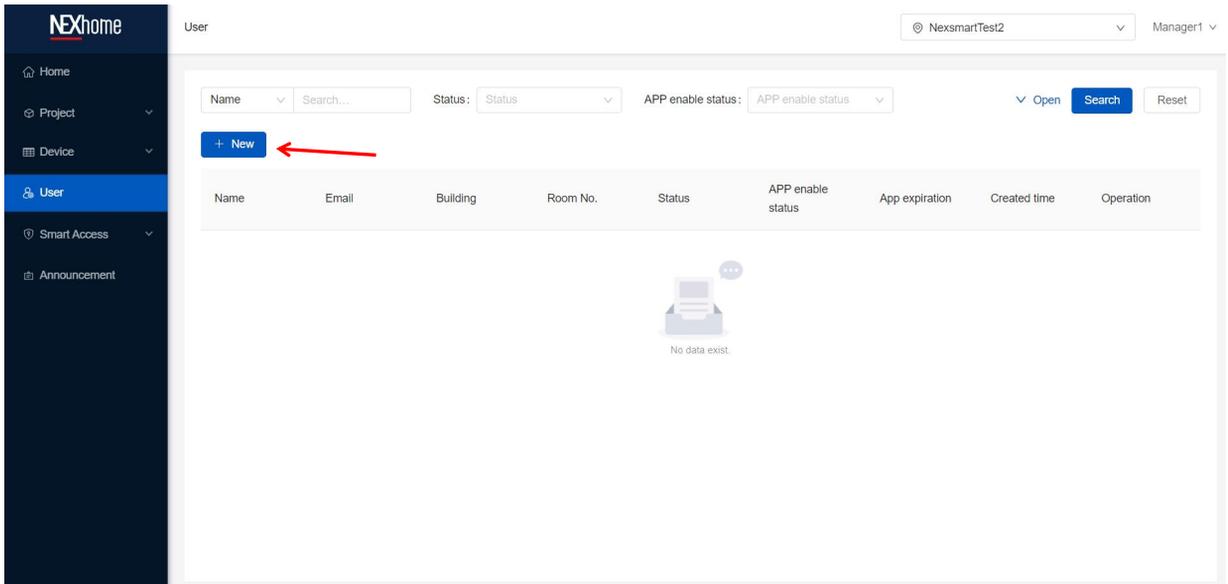
Log in to the installer account or property administrator account, and in the Smart Access Permission Group of Nex Smart Cloud Platform, add and set the permission group name, repeat mode, available time period, device selection rules, and accessible devices. Users and associated houses can be added.



5.4.2 Add New User

Log in to the installer account or property manager account, in the **User** section of NexSmart Cloud Platform, click the Add button, fill in the house number, user name, email and other information, select Enable app, click Save, and then you can add a new user.

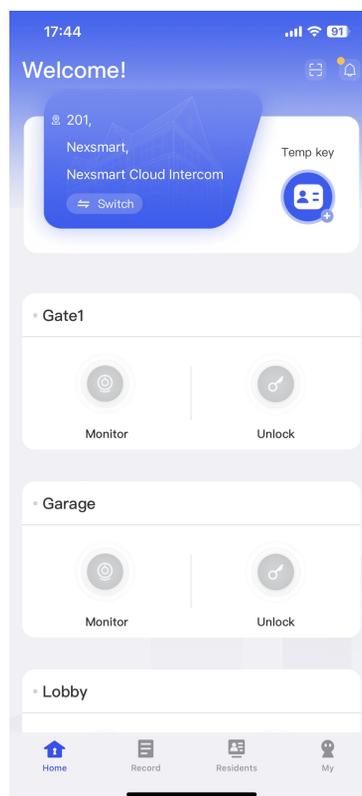
Email will receive an email for app authentication, and the mobile app will scan the authentication code, and after authentication, you can operate the device in the app.

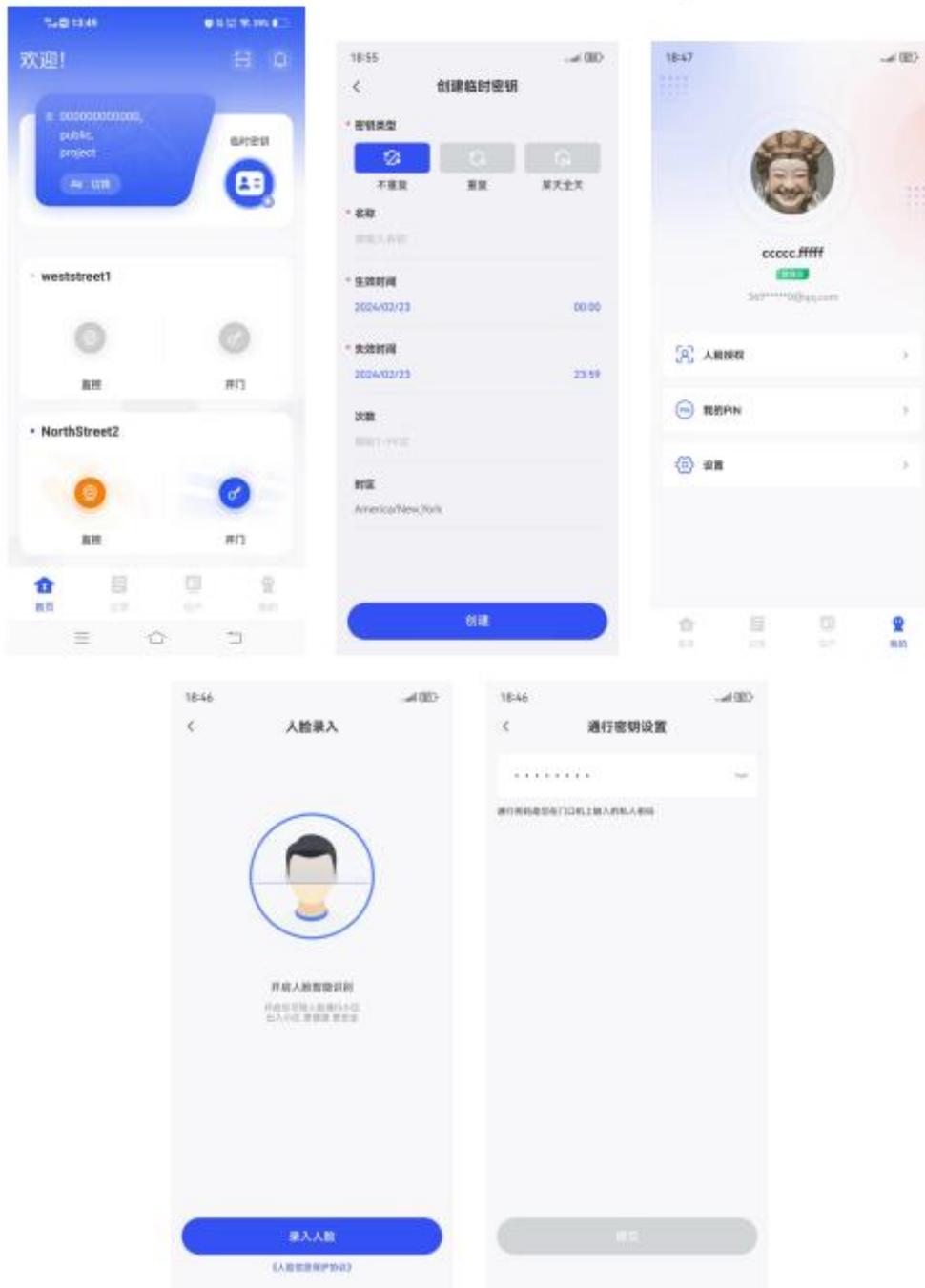


5.4.3 Device Unlocking

The user logs into the app, and on the homepage, can control the unlocking of the device by clicking the unlock button of the corresponding device.

You can authorize facial recognition and set unlock passwords on my interface.





5.4.4 Monitoring Device

Users log in to the app, and on the homepage, they can monitor the device by clicking on the monitoring button of the corresponding device, or by clicking on the incoming call record of the corresponding device in the call log.

