G510S 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 7
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 Delay Setting 20
3.3.4 Face Recognition 21
3.3.5 Wiegand 23
3.3.6 RFID Copy Prevention 24
3.4 Alarm Setting 25
3.4.1 Tamper Alarm 25
3.4.2 Door Magnetic Alarm 27
3.5 Internal Door Opening/Door Magnetic Setting 28
3.6 System Logs 29
3.6.1 Record 29
3.6.2 Logs and Packet Grabbing 30
3.7 System Settings 31
3.7.1 Language, Volume, and Time 31
3.7.2 Network Settings 34

3.7.3 Password Settings 35
3.7.4 Firmware Upgrade 36
3.7.5 Screen Settings 37
3.7.6 Restart and Reset 38
3.7.7 Modes Settings 39
3.7.8 Contacts Page Settings 41
3.7.9 Device screenshot 42
3.8 Advanced Settings 43
3.8.1 Connection Settings 43
3.8.2 Light Settings 44
3.8.3 RTSP and ONVIF Settings 44
3.8.4 Audit Tracker 47
3.8.5 Factory Testing 48
4 IDMC Configuration 49
4.1 IDMC Platform Login 49
4.2 Space Management 50
4.3 Device Management 51
4.3.1 Adding Devices 51
4.3.2 Device Unlocking 52
4.3.3 Device Operation 53
4.3.4 Device Configuration 53

5 NexSmart Cloud Platform Settings 55
5.1 NexSmart Cloud Platform Login 55
5.2 Project Management 56
5.2.1 Project Management 56
5.2.2 Space Management 57
5.3 Device Management 58
5.3.1 Add Device 58
5.3.2 Device Unlocking 59
5.3.3 Device Configuration 61
5.4 Cloud Platform App Usage 62
5.4.1 Set Permission Group 62
5.4.2 Add New User 62
5.4.3 Device Unlocking 64
5.4.4 Monitoring Device 66

1 Product Overview

1.1 Product Introduction

G510S is a 5-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

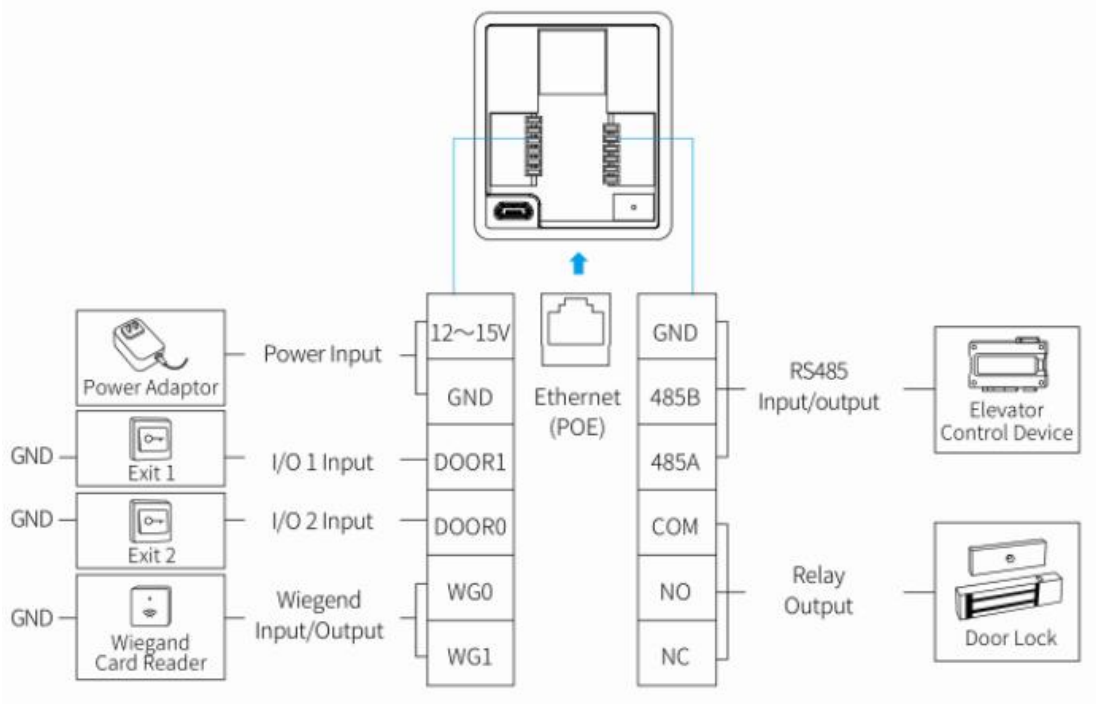
NO/COM/NC: Relay control port

RS485A/B: RS485 port

DOOR0/GND: Internal door opening

DOOR1/GND: Input port

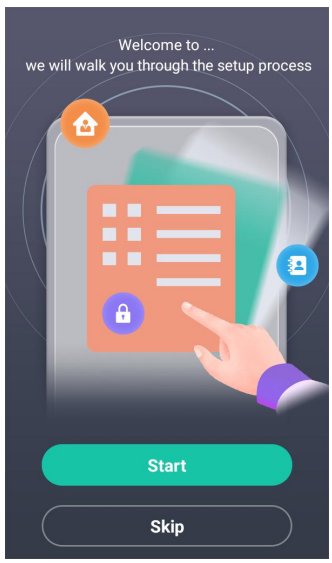
WG0/WG1/GND: Wiegand interface

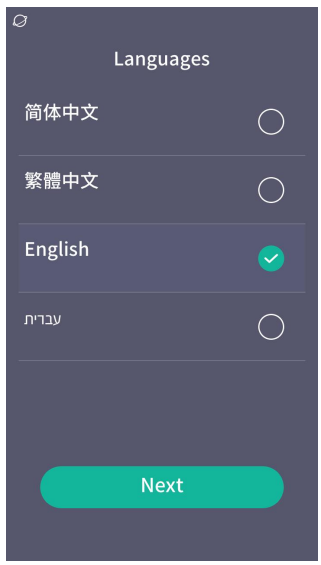


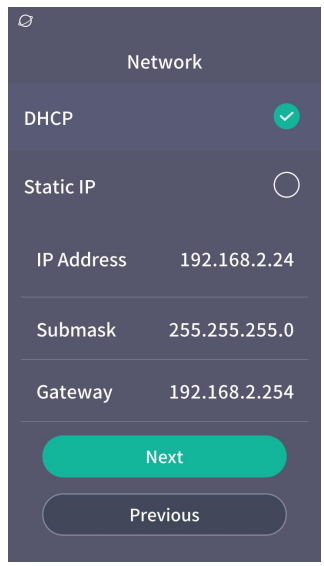
2 User Guide

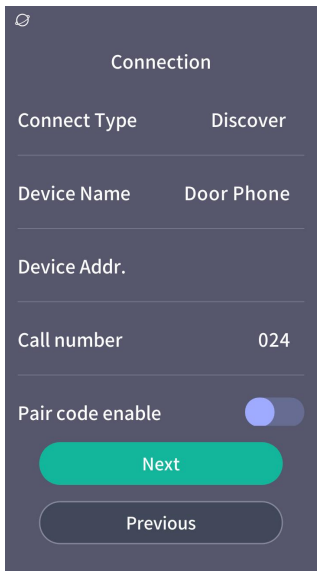
2.1 First configuration

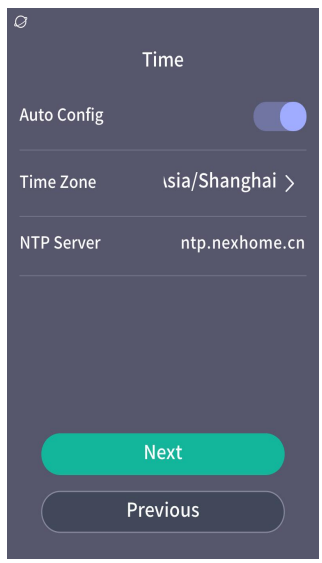
When starting the device for the first time, the user must perform language configuration (Simplified Chinese, Traditional Chinese, English,Hebrew), network configuration (DHCP, static IP), connection type setting (Discovery,Cloud), and mode selection (General mode, Doorbell mode, Access mode, Directory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

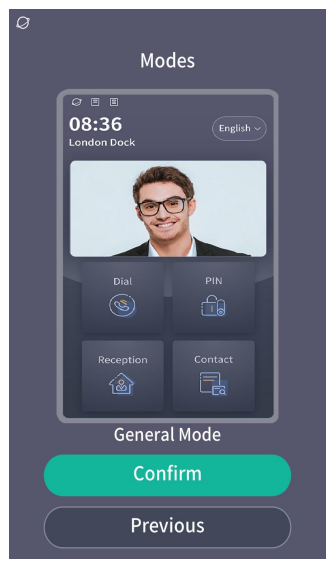










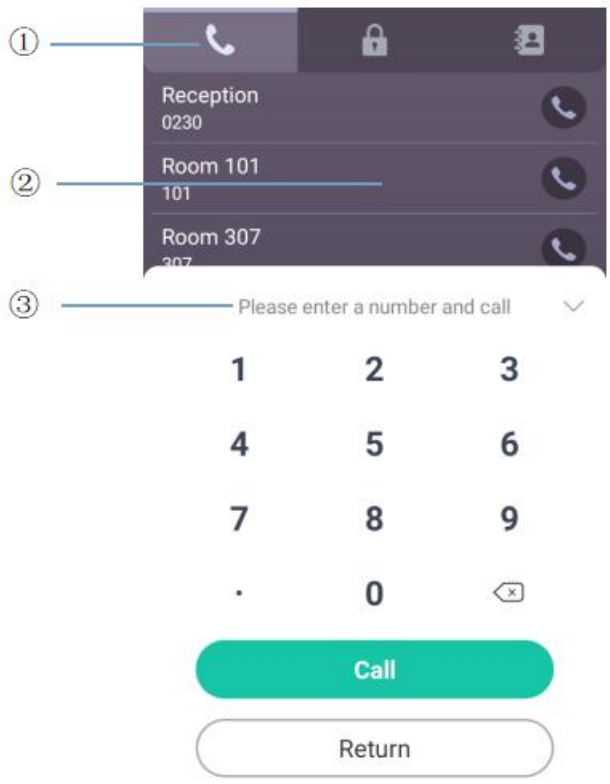


2.2 Dialing

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.

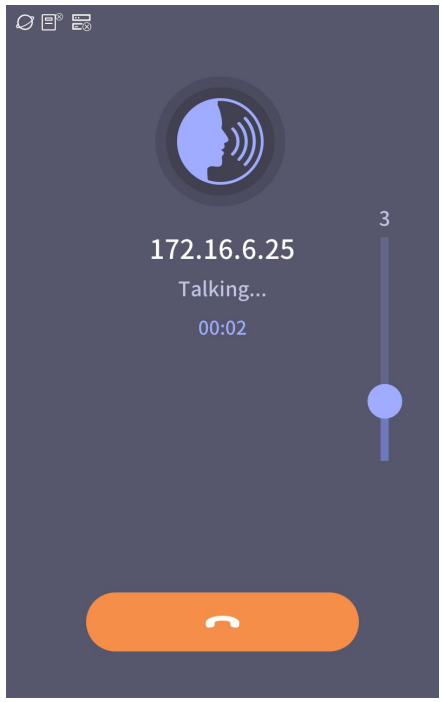


2.2.2 Incoming Calls

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

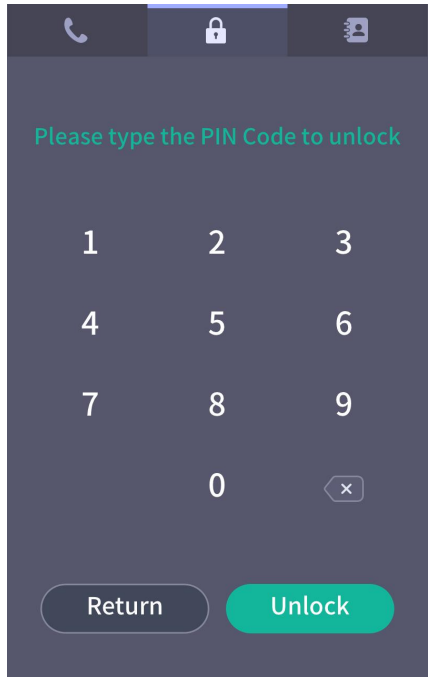
After clicking the green button to answer, enter the call interface. The volume bar on the right can adjust the call volume. Clicking the red button at the bottom of the interface will end the call.



2.3 Unlocking

2.3.1 Password Unlocking

Click on the **PIN** button on the main screen and enter the password,then click **Unclock** botton 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.

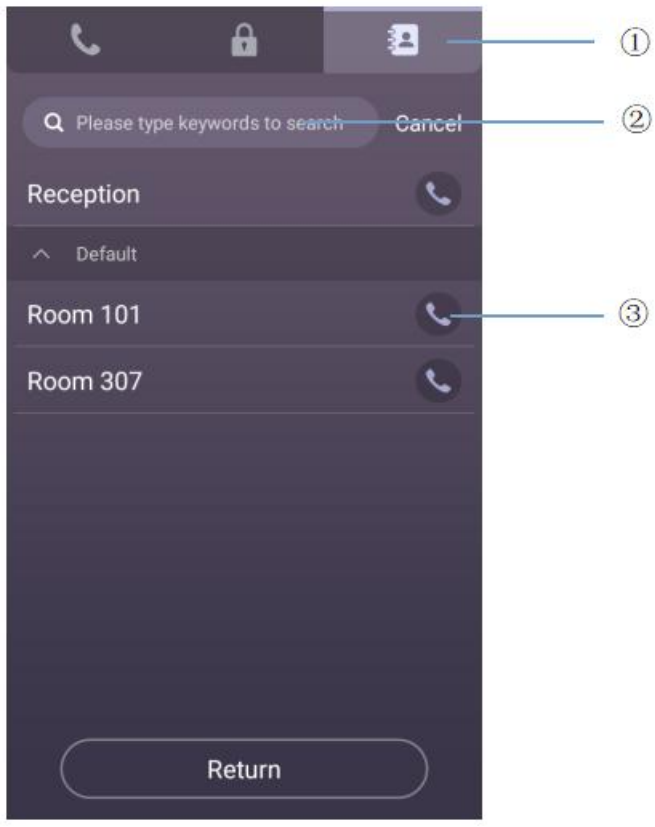
2.3.5 QR code Unlocking

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

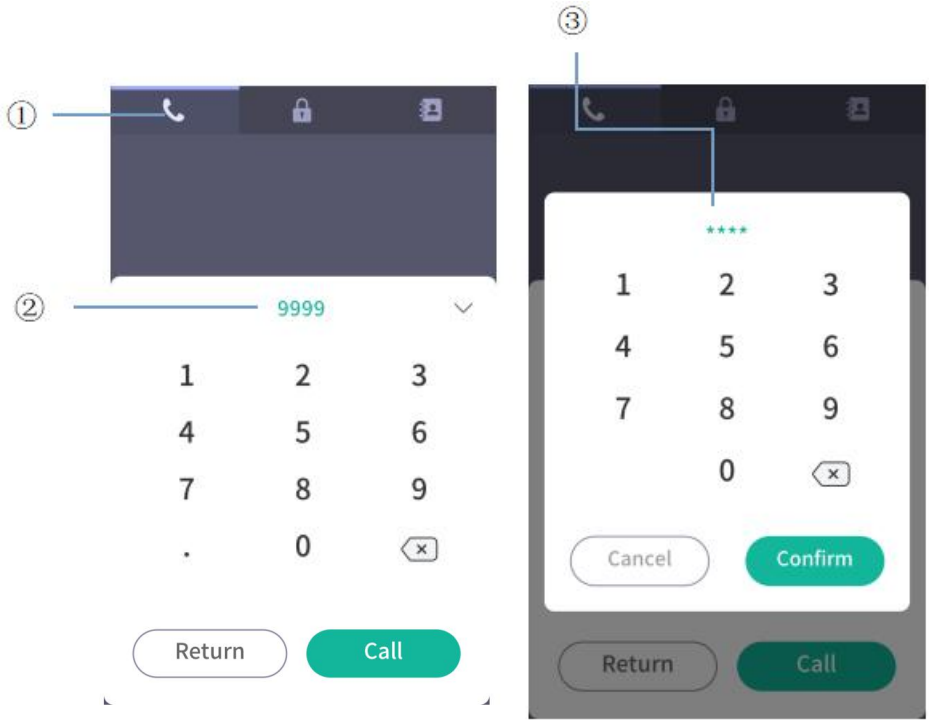
3.1 Accessing the Backend Interface

3.1.1 Accessing the Device-side Backend

①Click on daling button on the main interface.

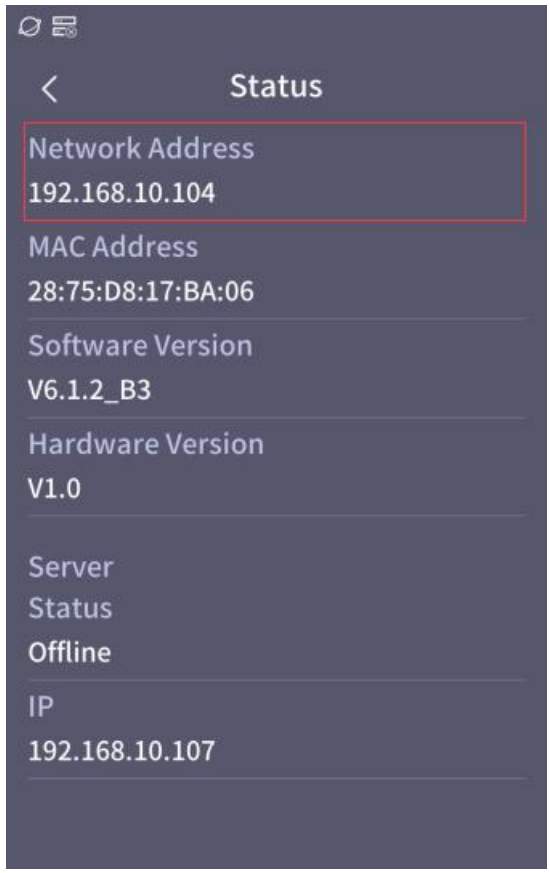
②Enter 9999 and call to pop up the project password menu.

③Enter the password 3888 and click OK to enter the device backend interface.



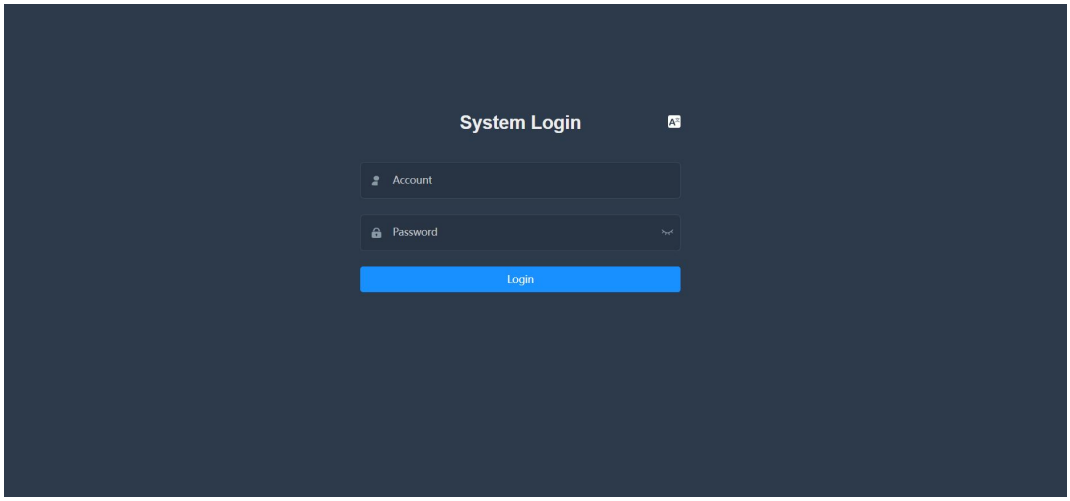
3.1.2 Checking the Device IP Address

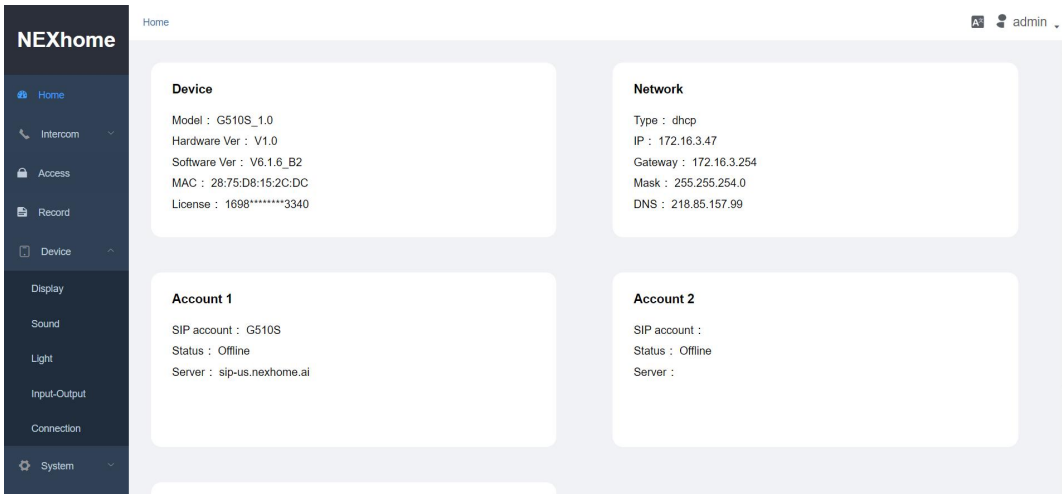
After entering the device backend, click the status information button to view the device's network address, version information and connection status.



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.

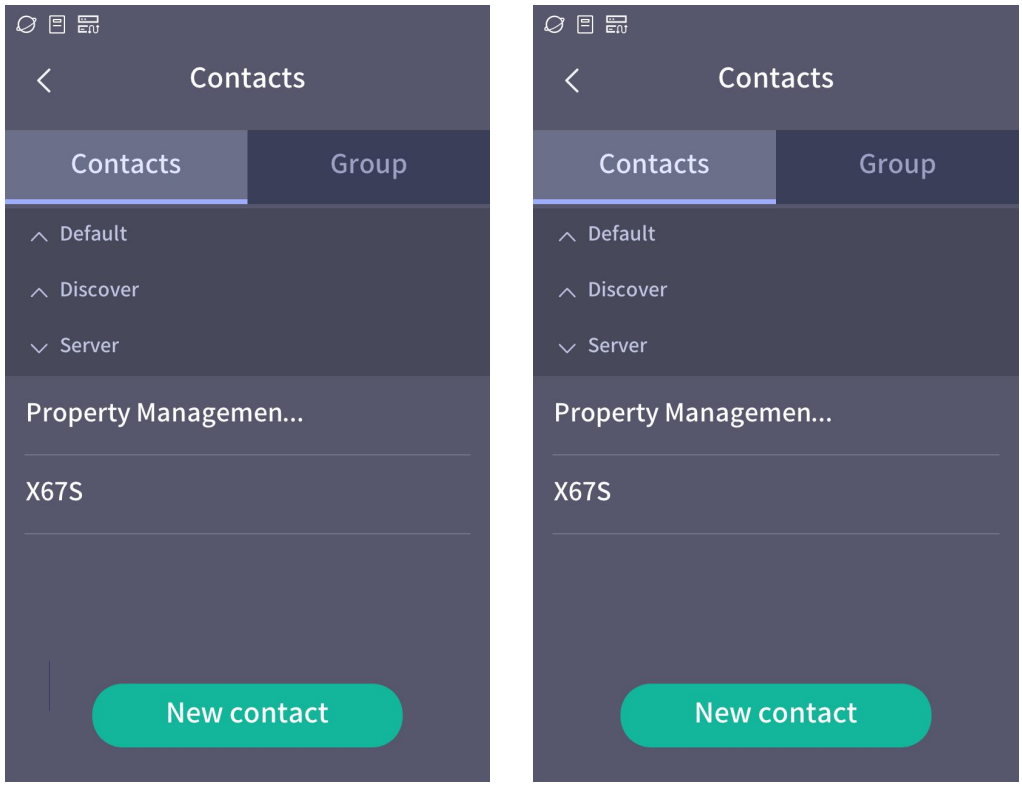




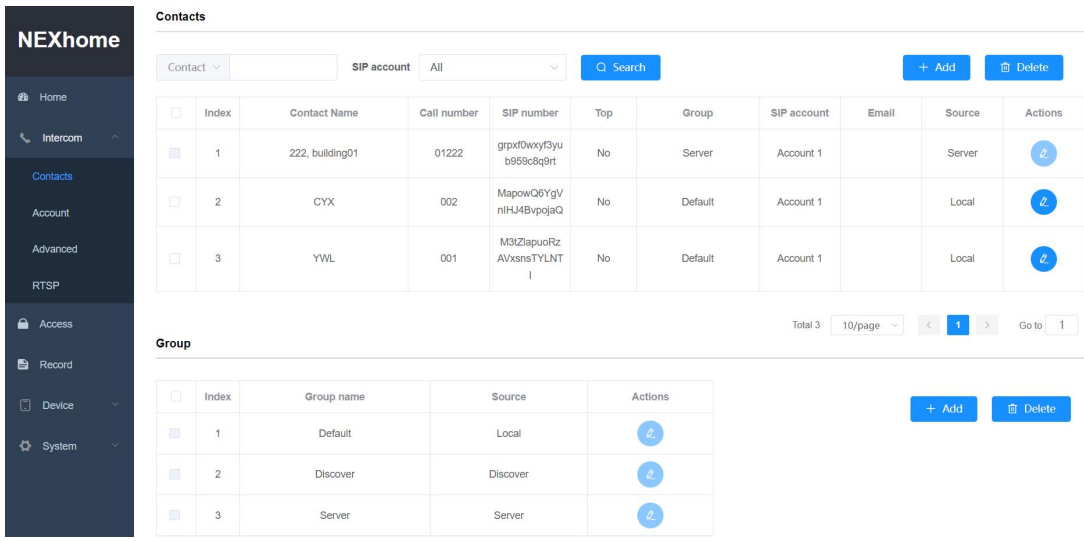
3.2 Intercom Configuration

3.2.1 Address Book Setting

In the device engineering settings interface, you can add, modify, and delete local contacts and local contact groups in **Contacts**.



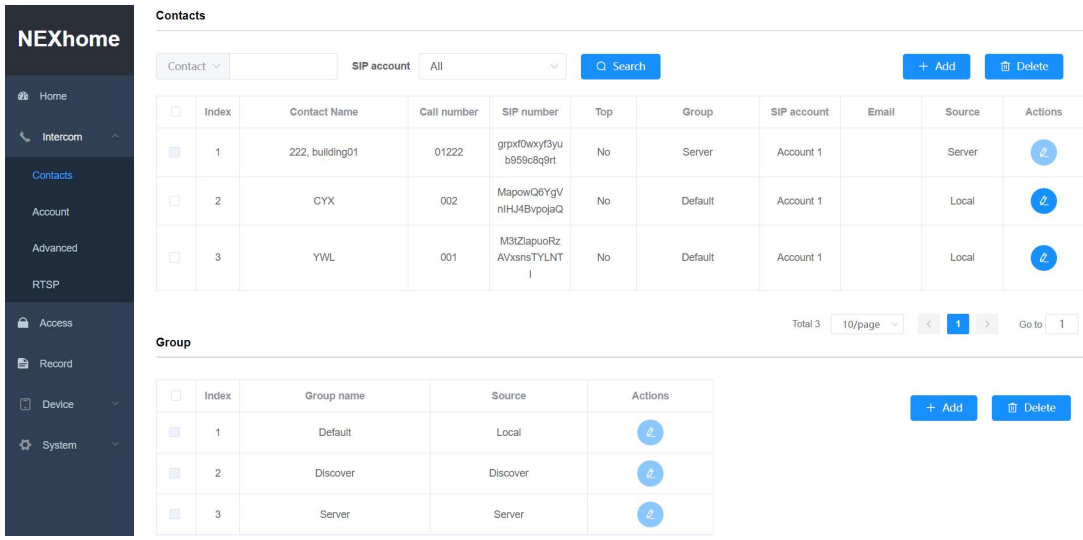
In the web backend, you can view existing address books in the intercom address book, and you can click the add button at the top right to add new contacts. The add button at the bottom right can create a new contact group. When creating a new contact, it is necessary to fill in the contact's display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

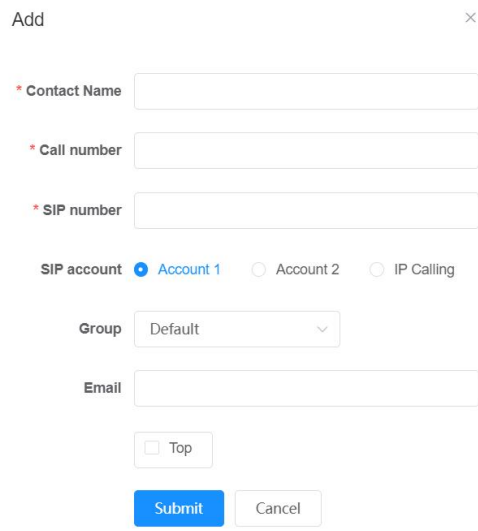


After selecting a contact on the left side of the contact list, you can click the delete button in the upper right corner to delete the local contact; After selecting a contact group on the left side of the contact list, you can also click the corresponding delete button on the right side to delete the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

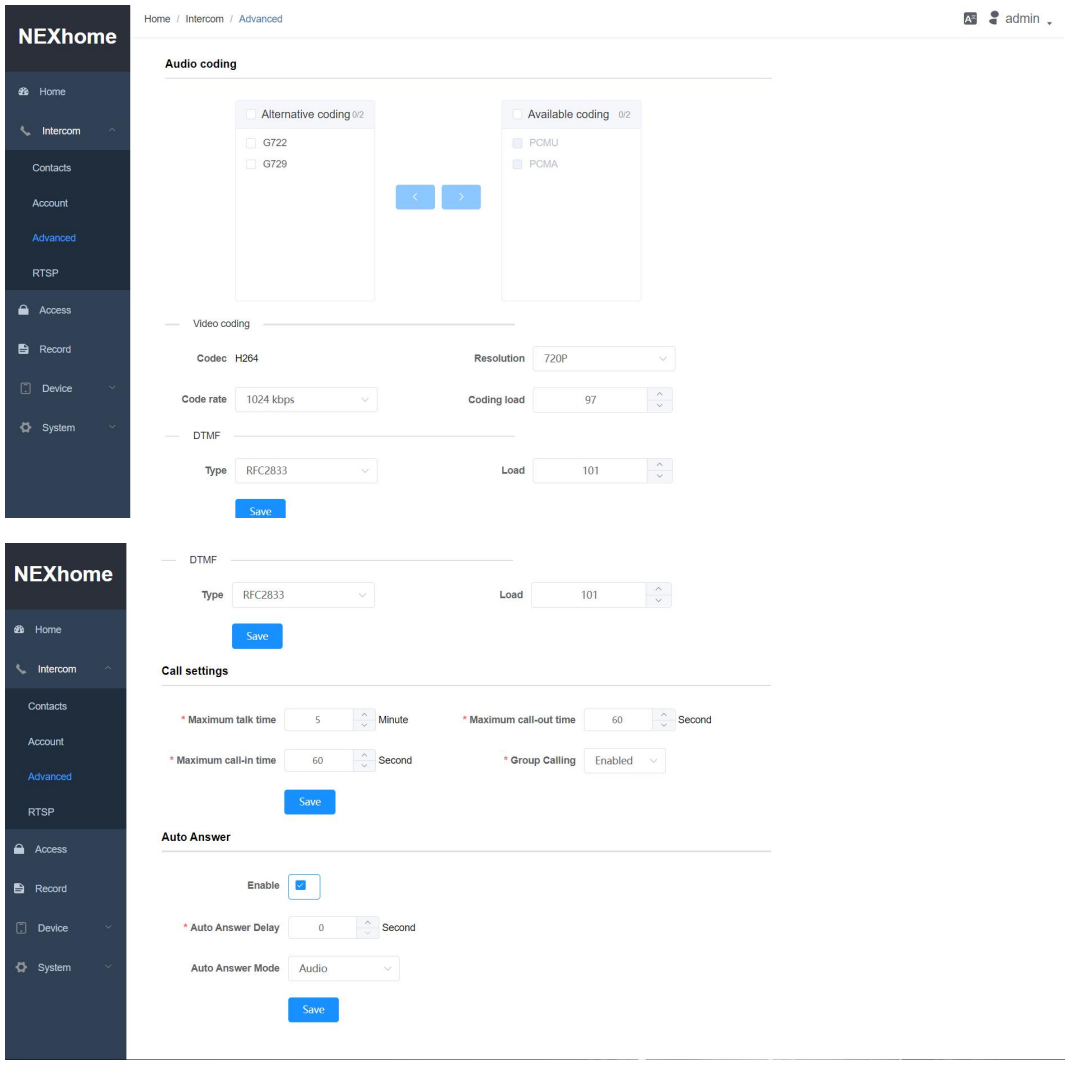
Edit the group name to modify the group name displayed in the device address book interface.





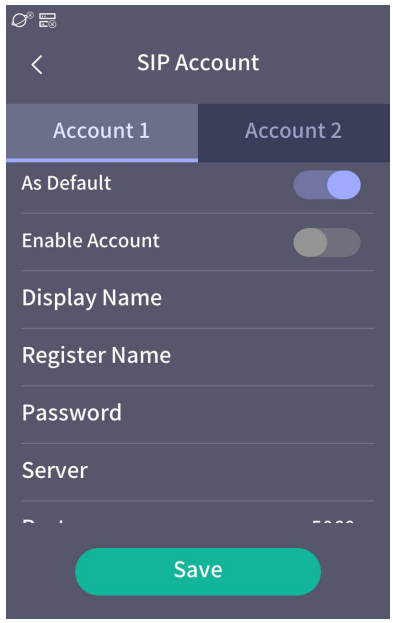
3.2.2 Call Setting

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.

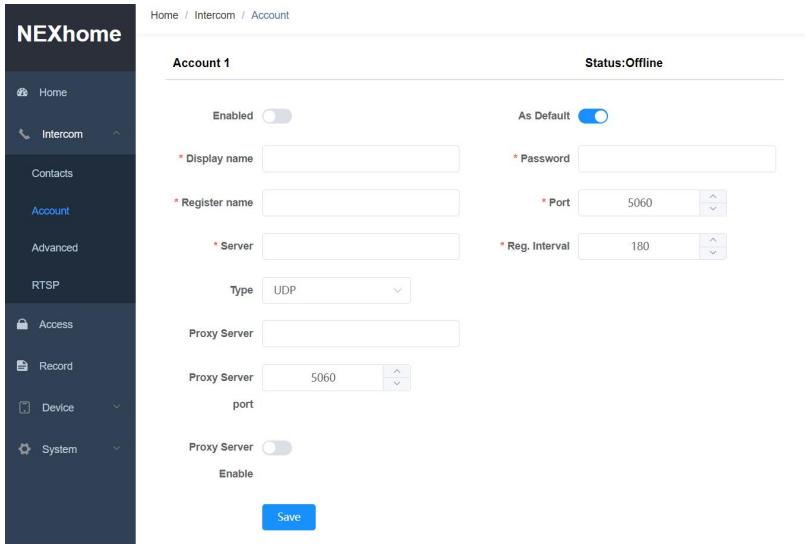


3.2.3 SIP Account Setting

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

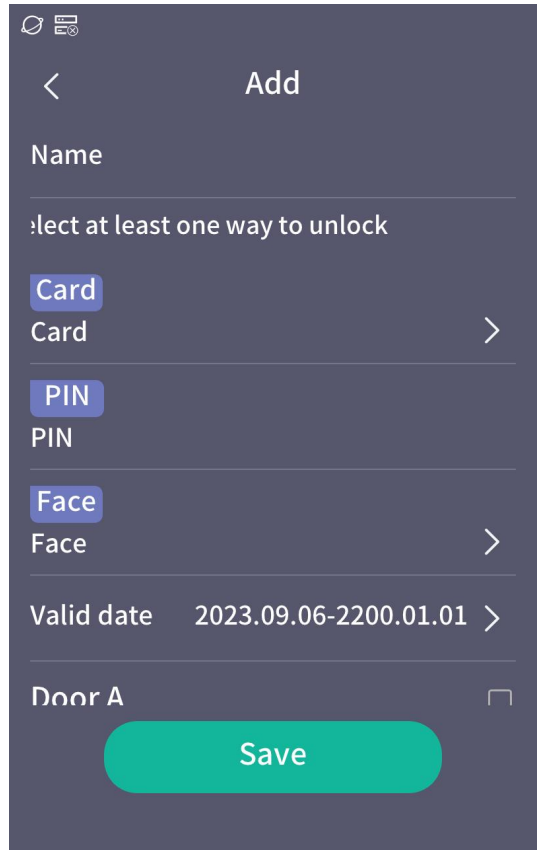


In the web backend, you can set up a SIP account in the intercom account.



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

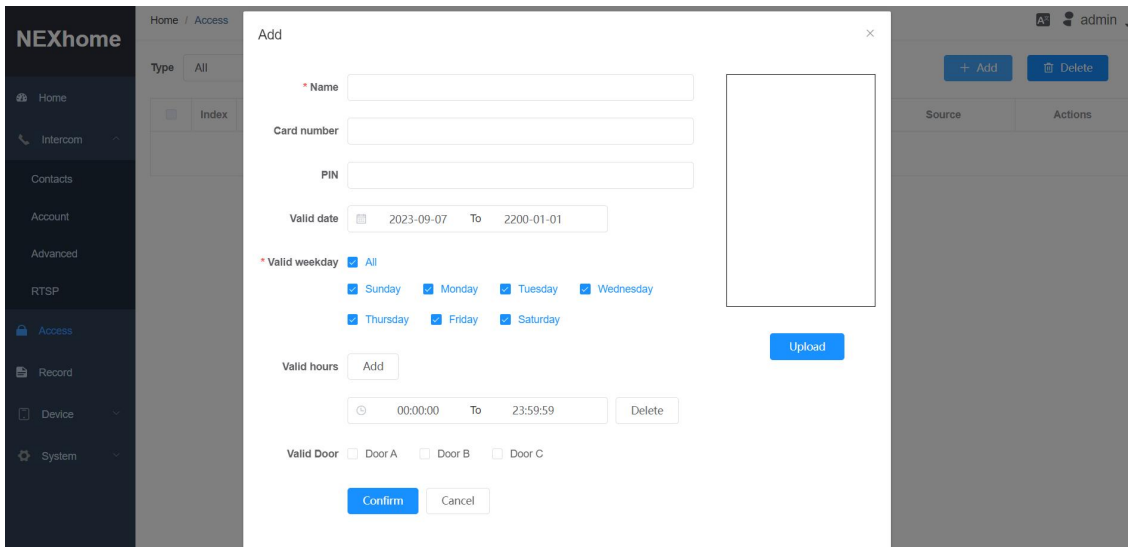
PIN: Access control password

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

Valid weekday: Card effective period, mu

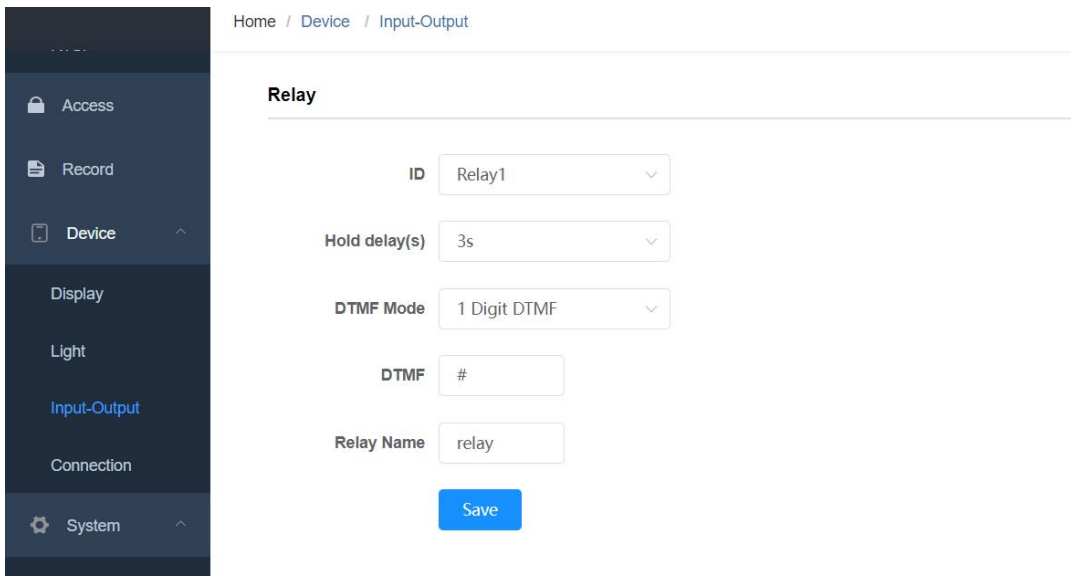
Valid hours: The effective period of the card, default to 00:00 to 23:59,can set multiple

Upload photos: Upload photos to the device for facial recognition



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.

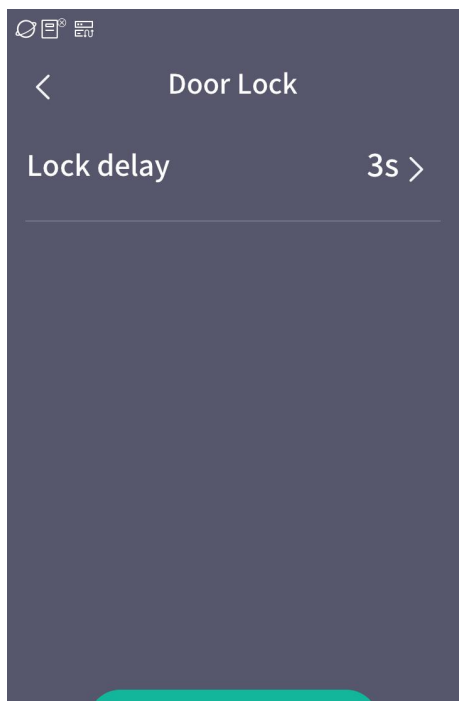
Hold delay: The relay remains in the triggered state for a certain period of time before resetting, i.e. the door opening hold time

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

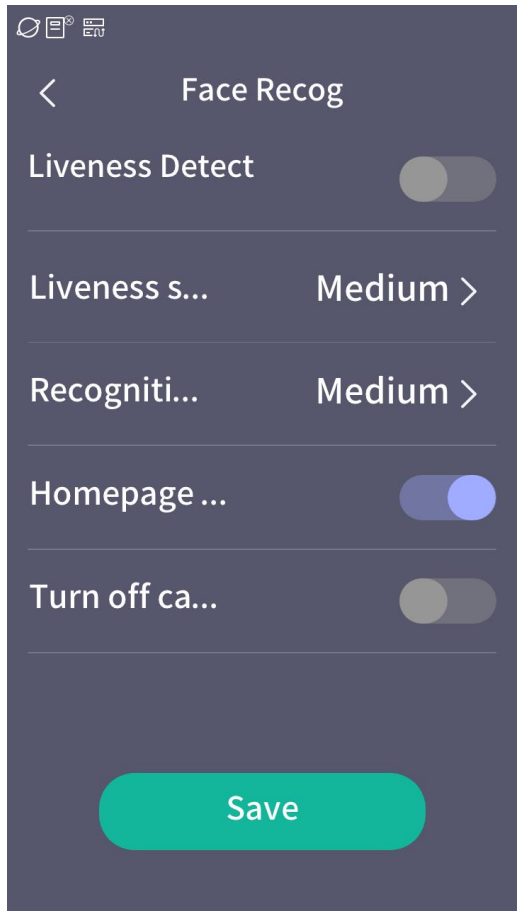
3.3.3 Door Lock Delay Setting

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

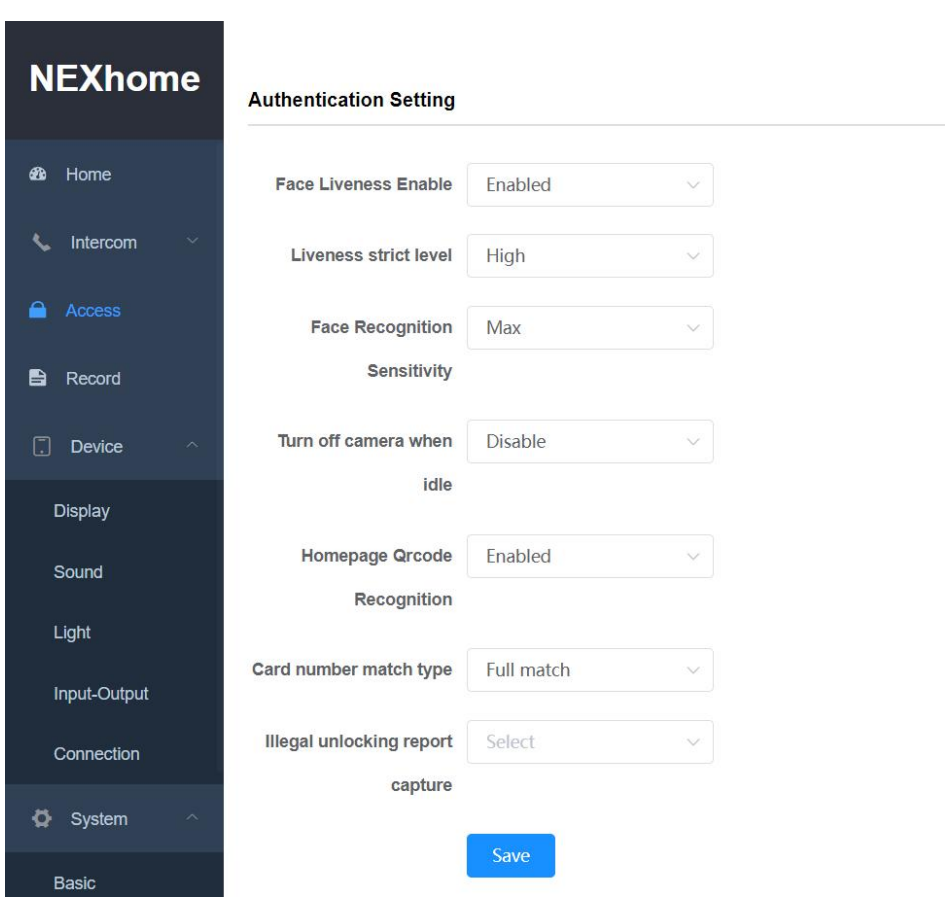


3.3.4 Face Recognition

In the device backend, enter the facial recognition interface to enable or disable liveness detect and configure recognition sensitivity. You can turn on or off the QR code recognition on the home screen, as well as enable or disable the camera off function.

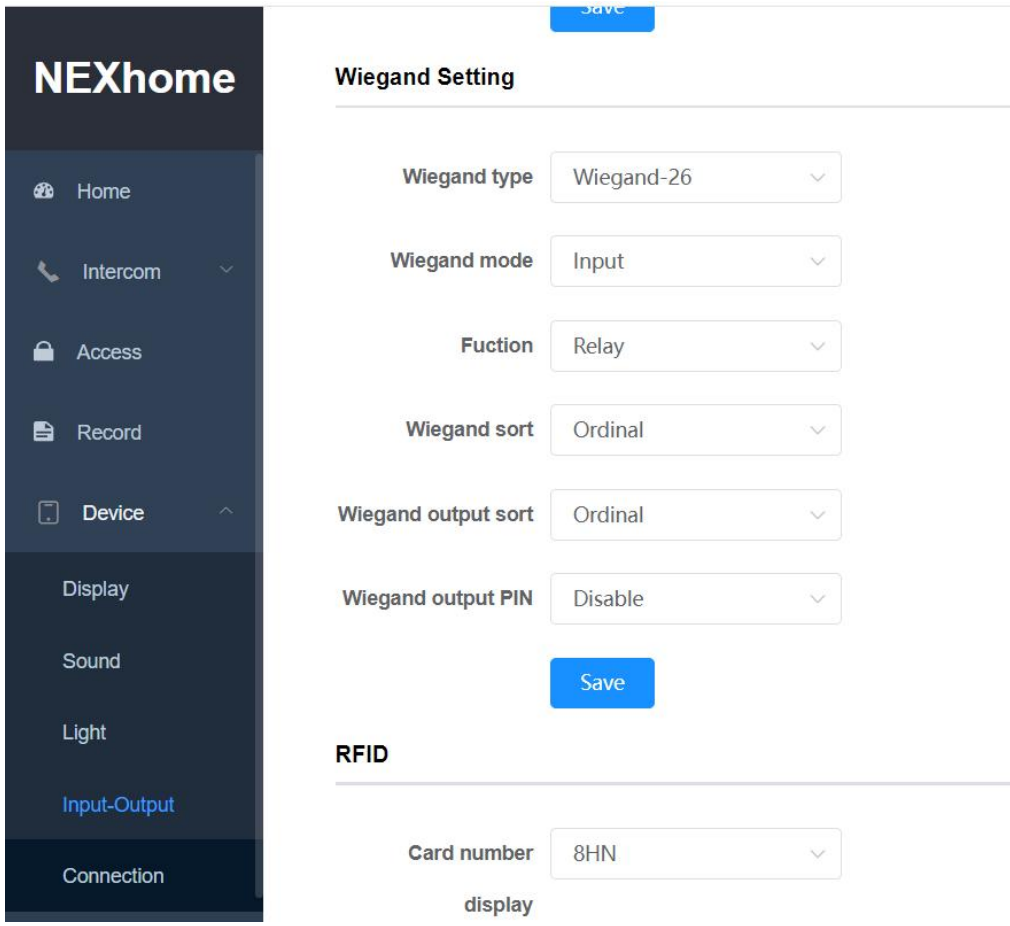


In the device's web backend,in **Access-Authentication Setting**, enable or disable face liveness detect, set the liveness detect strictness level, face recognition sensitivity, face recognition resolution, enable or disable the QR code recognition on the homepage, configure the card number matching mode, and select the unlocking type of illegal unlocking report snapshot.



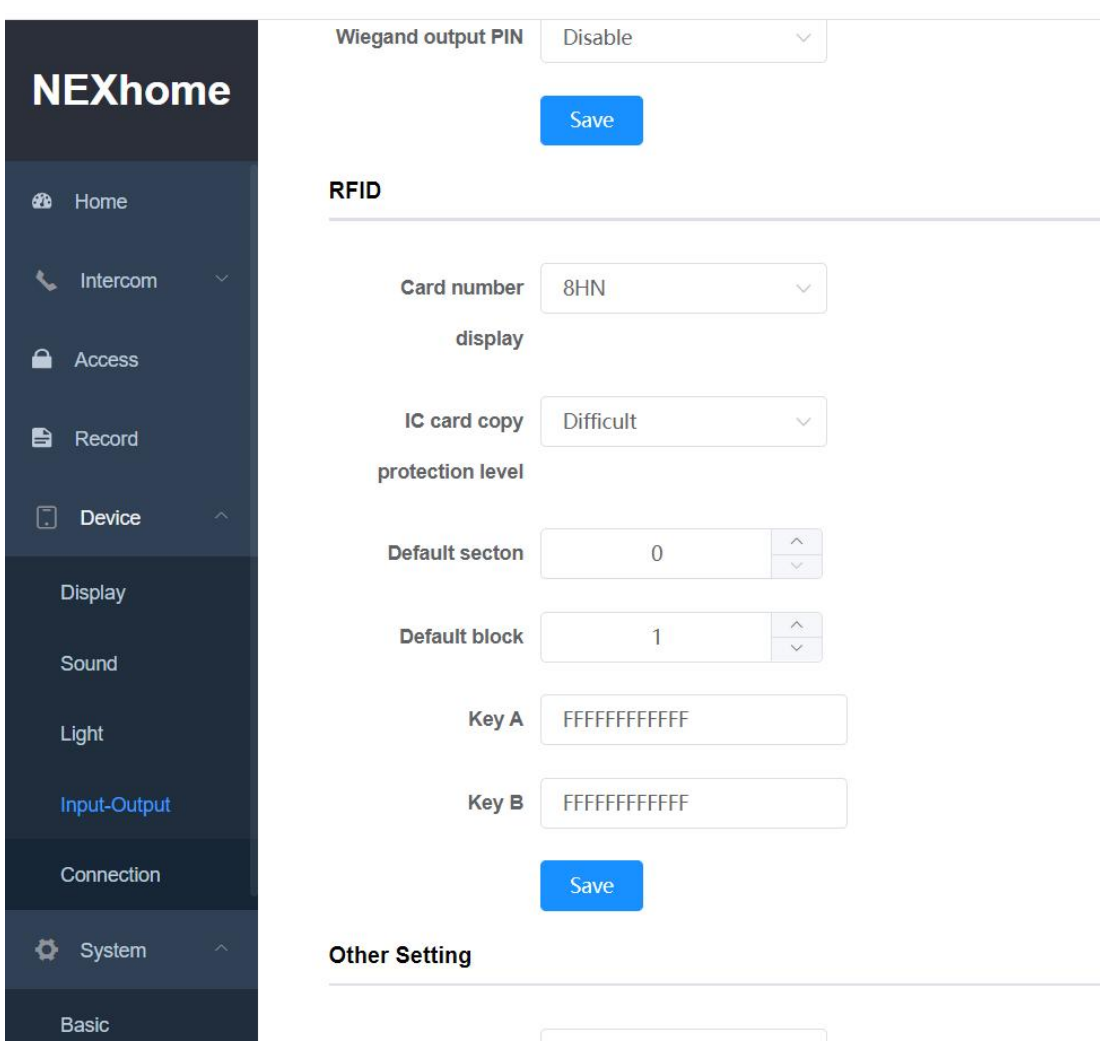
3.3.5 Wiegand

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.



3.3.6 RFID Copy Prevention

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**.

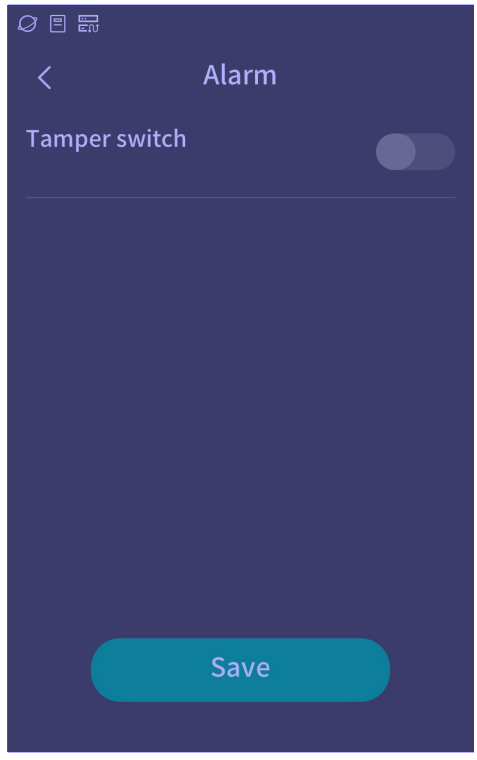


3.4 Alarm Setting

3.4.1 Tamper Alarm

In the device backend, click the **Alarm** button 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.

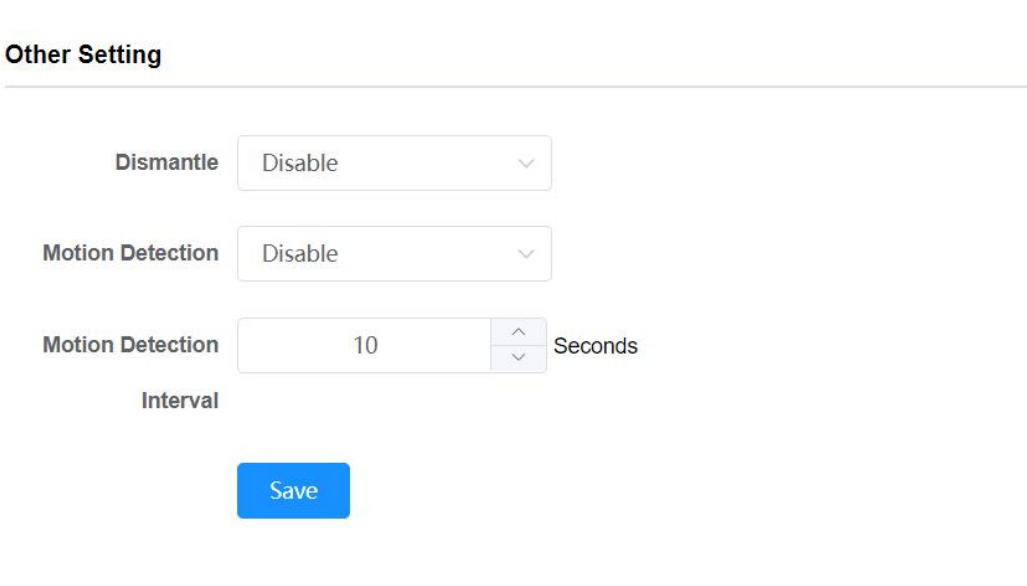
You can enable or disable motion detection and configure the reporting interval for trigger events.



In the device's web backend, in the **Device - Input/Output**

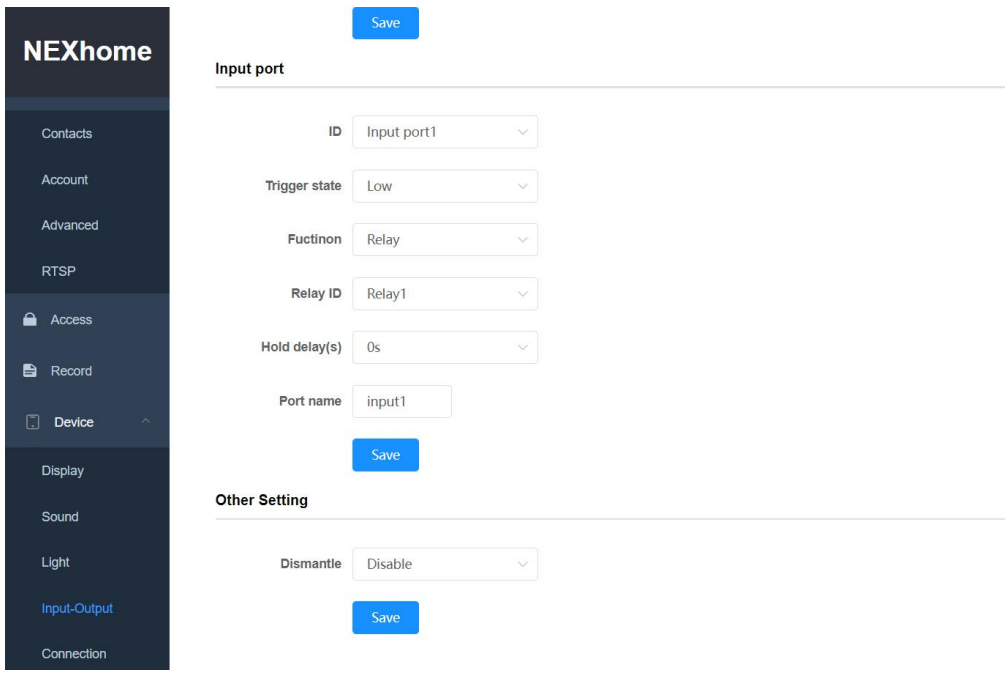
Setting - Other section, you can enable or disable the tamper-proof alarm. To deactivate the tamper-proof alarm, simply press the black protruding button located on the right side of the device's back.

You can enable or disable motion detection and configure the reporting interval for trigger events.



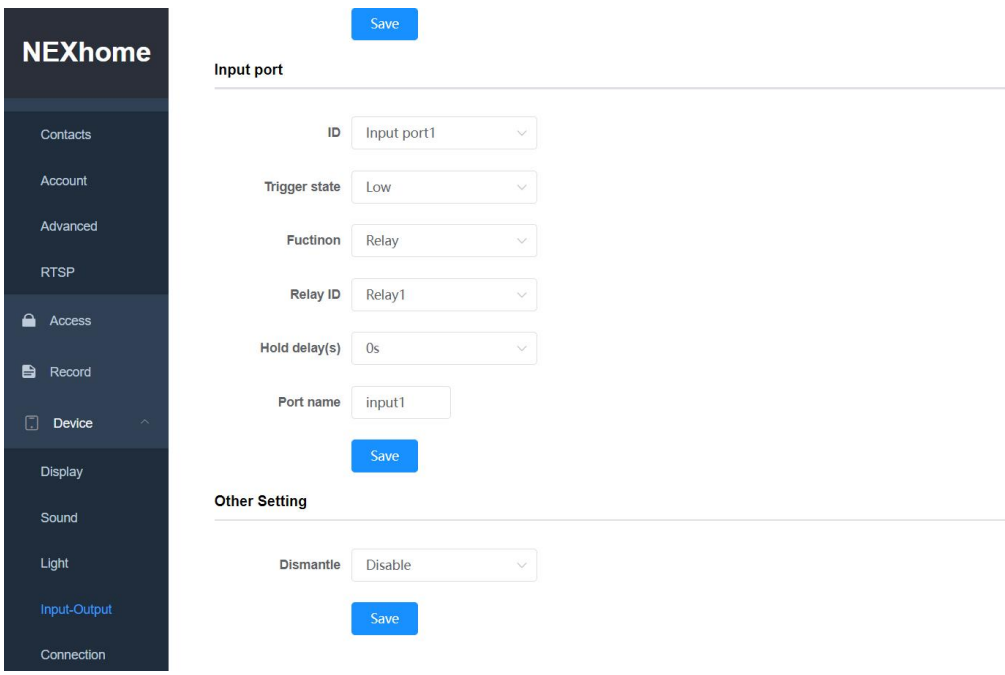
3.4.2 Door Magnetic Alarm

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.



3.5 Internal Door Opening/Door Magnetic Setting

In the backend of the web side, you can select the function to set the internal door opening for the relay in the input port section of Device-Input-Output Setting, and you can configure the ID, trigger state, function, hold relay time and name of the input port. Select the function as door magnet, you can configure the number, door magnet type, holding delay and input port name.



3.6 System Logs

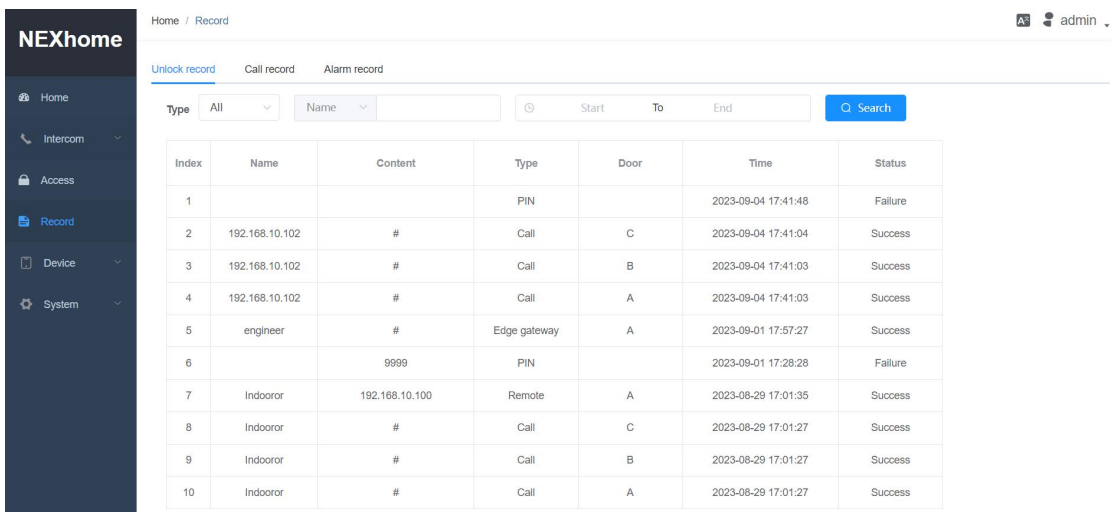
3.6.1 Record

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 and snapshots.

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

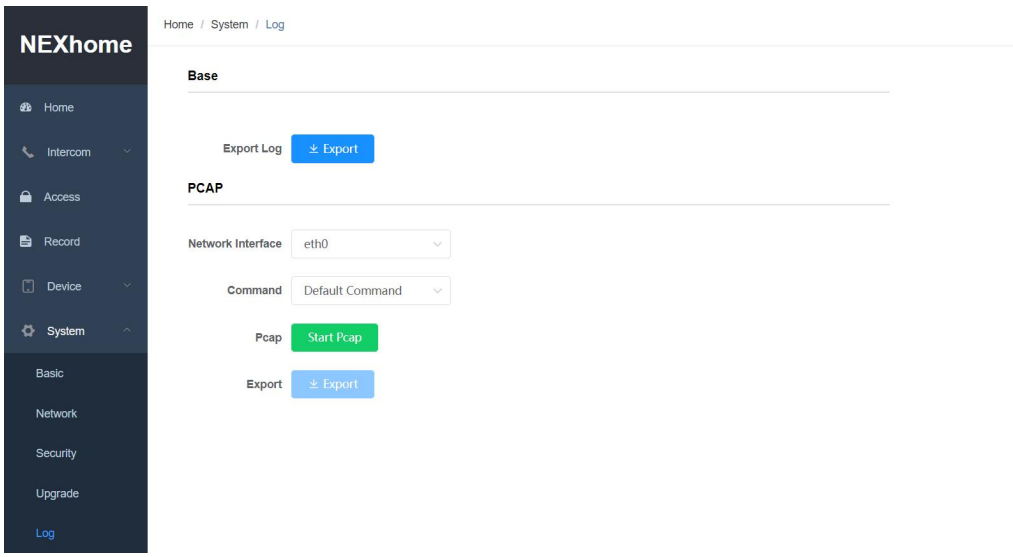
Alarm Record: Device alarm record including magnet alarm and dismantle alarm



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

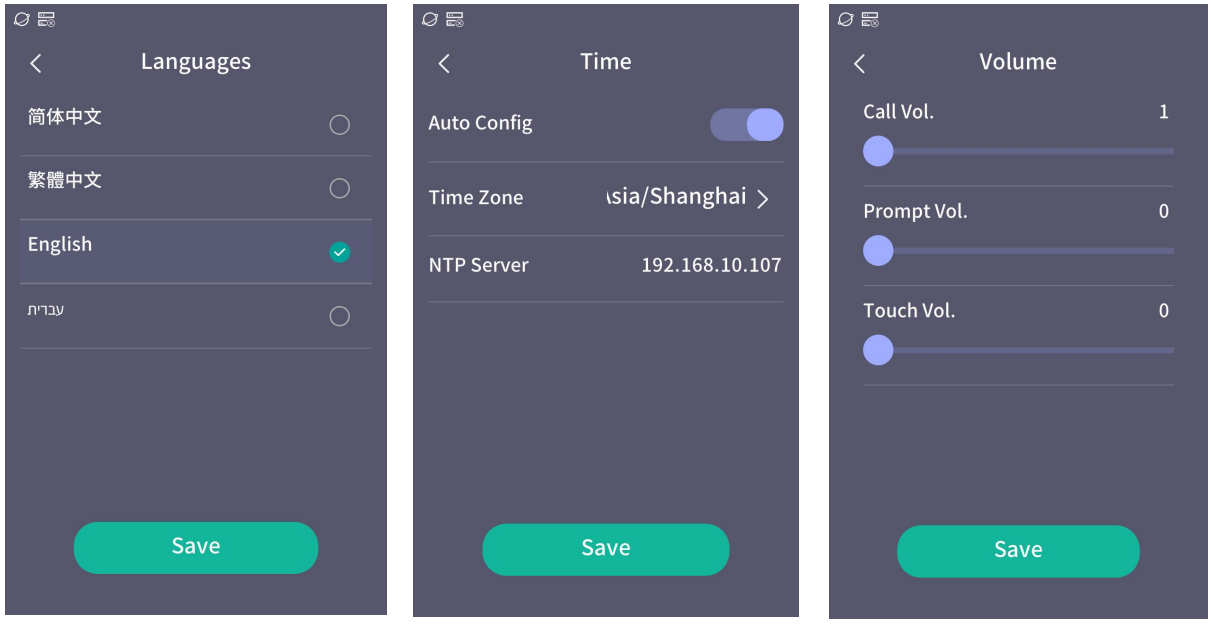


grabbed.

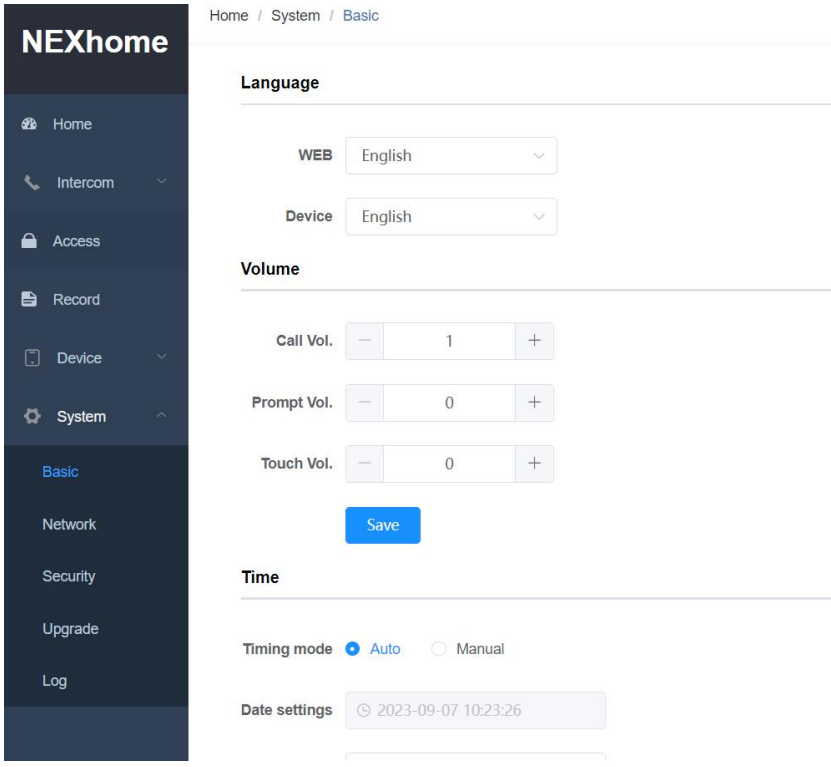
3.7 System Settings

3.7.1 Language, Volume, and Time

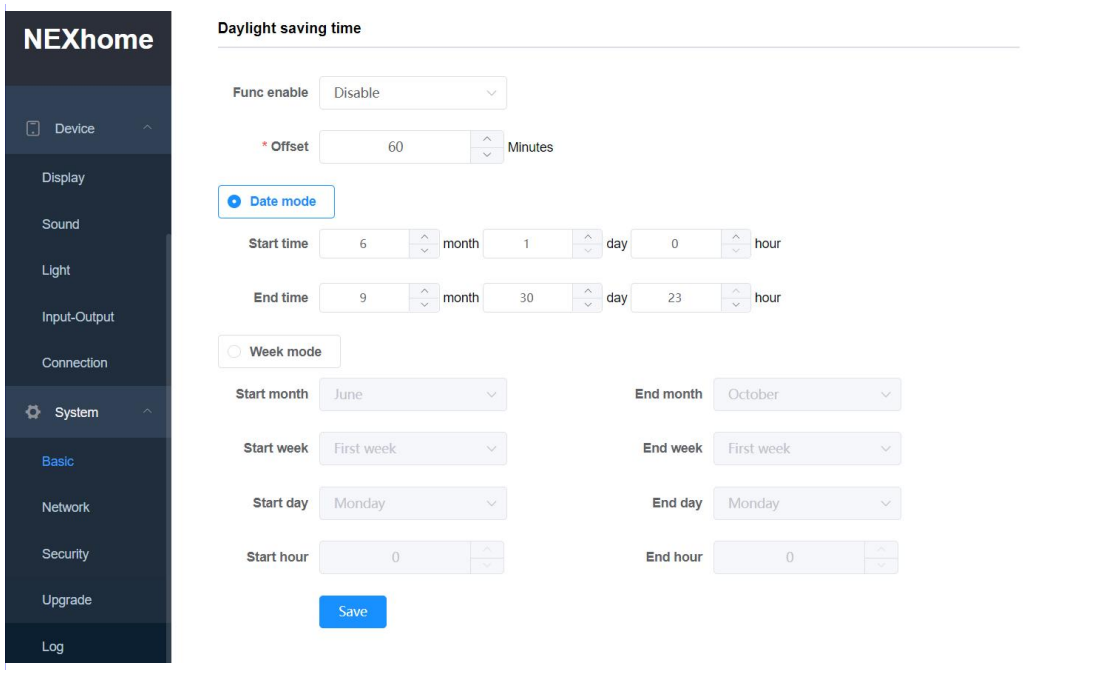
On the device backend page, click on **Language** settings to change the device display language. Currently, it supports Simplified Chinese, Traditional Chinese, English, and Hebrew. Click on the **Volume** settings to set the call volume, prompt volume, touch volume and alarm volume. Click on **Time** 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.

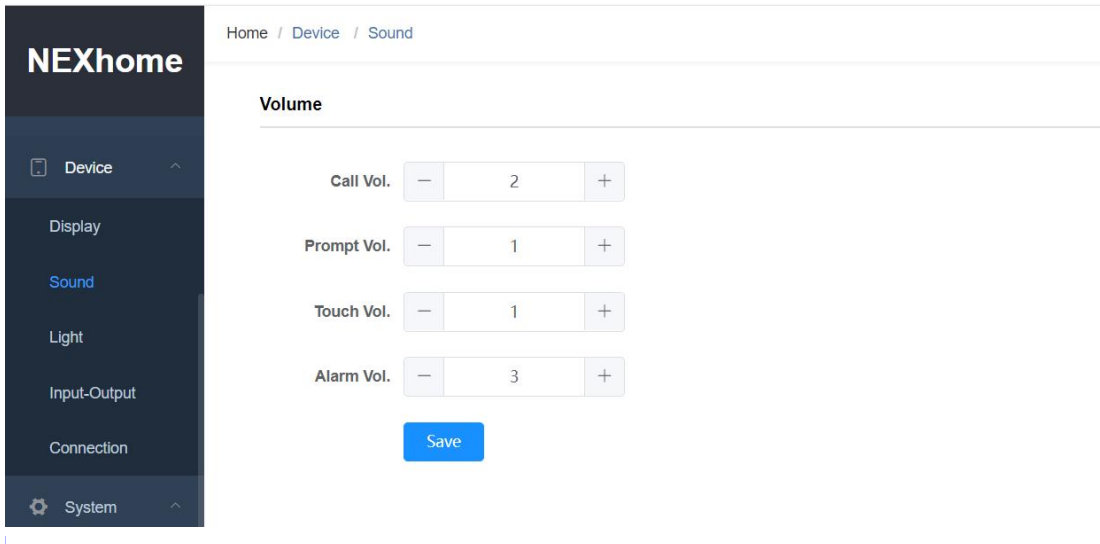


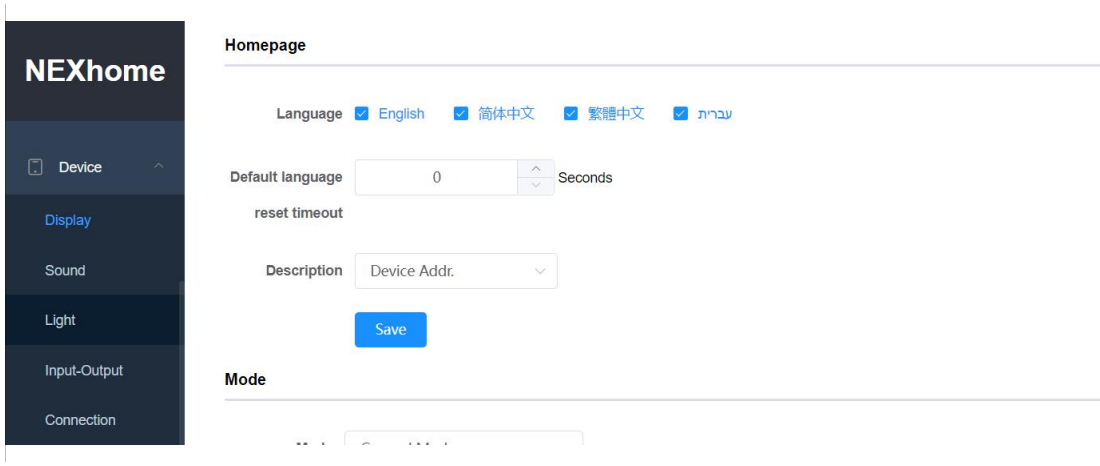
In the web side, you can set the language of the web in the upper right corner of the page, which supports Simplified Chinese, Traditional Chinese and English. In System-Basic Settings, you can set the language of web and device, and you can also set the Time zone and NTP server, also there are two ways of automatic time calibration and manual time calibration. In addition, you can set daylight saving time. In Device-Sound Settings, you can set the call volume, prompt volume, touch volume and alarm volume. In Device-Display Settings, You can set the home page language options, the



it.

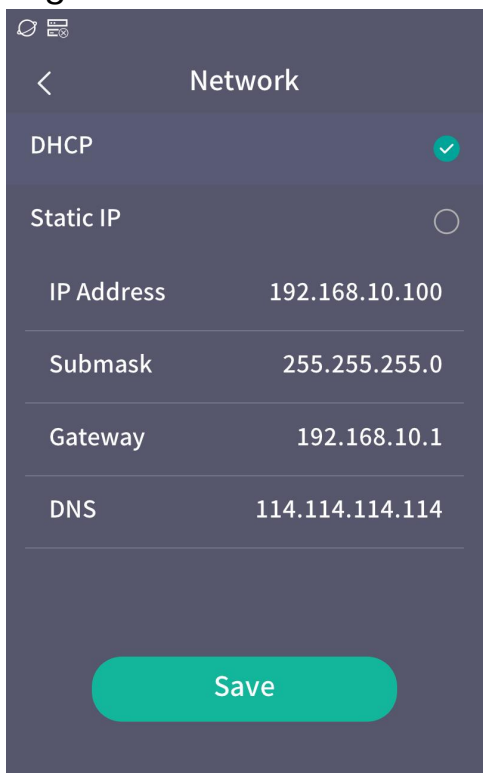

NEXhome
Device
Display
Sound
Light
Input-Output
Connection
System
Basic
Network
Security
Upgrade
Log
Daylight saving time
Func enable
Disable
* Offset
60
Minutes
Date mode
Start time
6
month
1
day
0
hour
End time
9
month
30
day
23
hour
Week mode
Start month
June
End month
October
Start week
First week
End week
First week
Start day
Monday
End day
Monday
Start hour
0
End hour
0
Save


NEXhome
Home / Device / Sound
Device
Display
Sound
Light
Input-Output
Connection
System
Volume
Call Vol.
2
Prompt Vol.
1
Touch Vol.
1
Alarm Vol.
3
Save

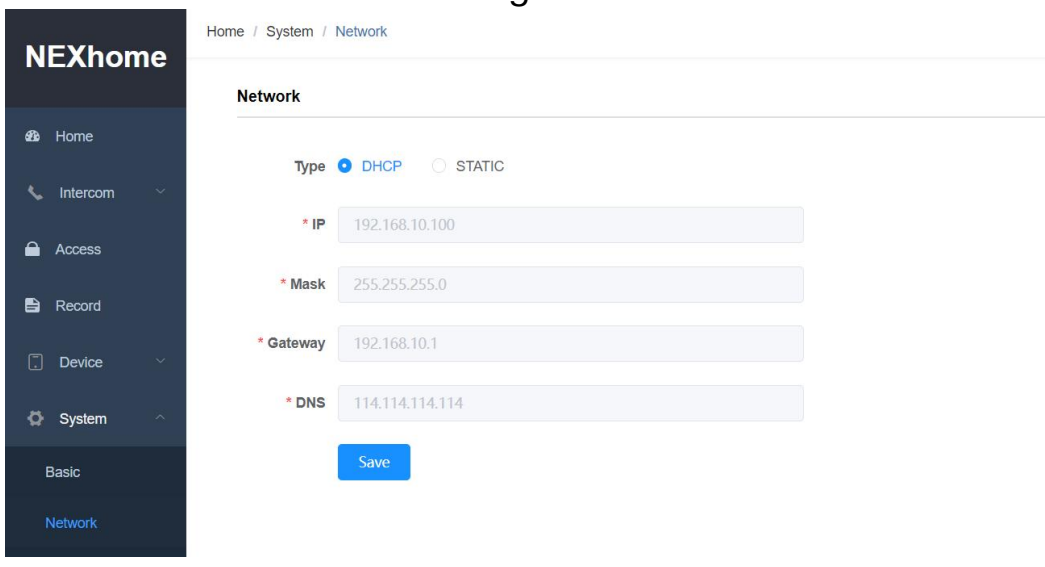

NEXhome
Device
Display
Sound
Light
Input-Output
Connection
Homepage
Language
English
简体中文
繁體中文
עברית
Default language reset timeout
0
Seconds
Description
Device Addr.
Save
Mode

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.

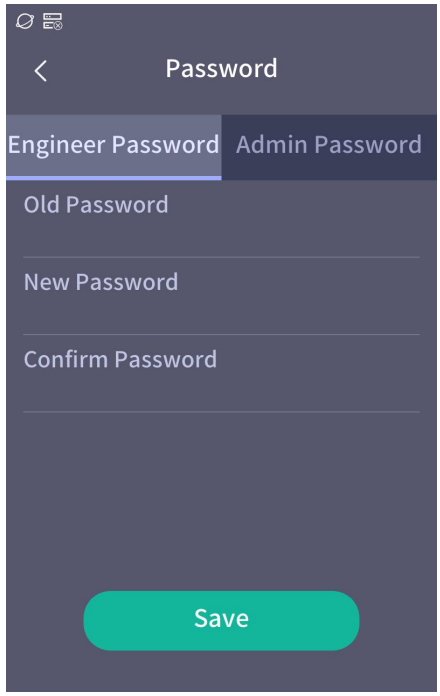


In the **System-Network** settings on the web side, you can also choose DHCP or static IP settings.



3.7.3 Password Settings

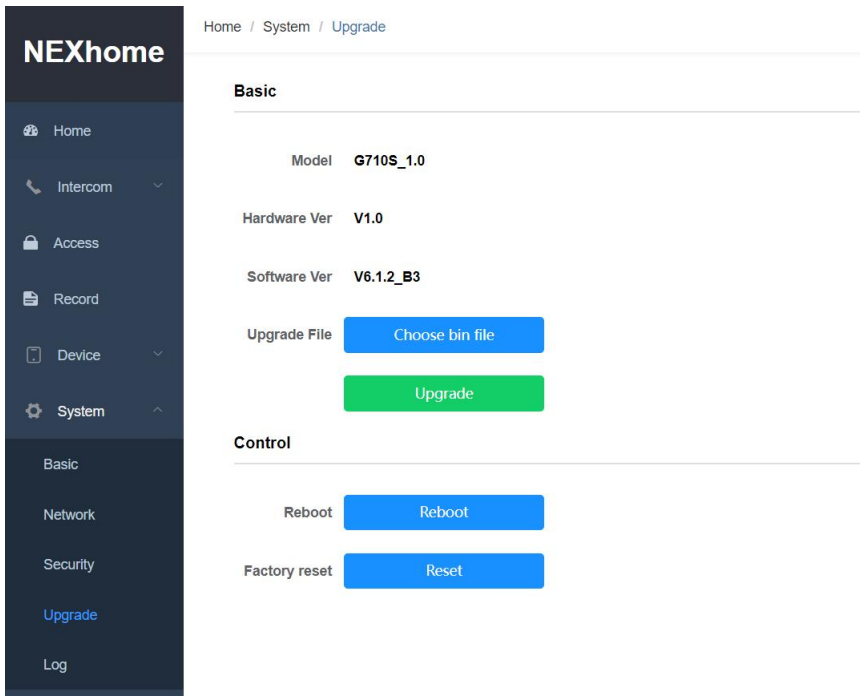
In the device backend, click the **Password** button to change the password for logging in to the engineering interface and logging in to the web interface.



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

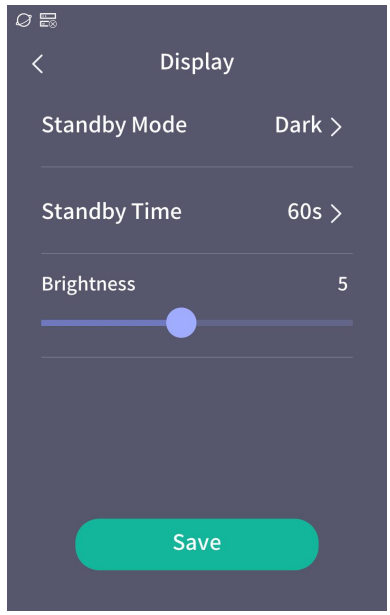
3.7.4 Firmware Upgrade

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.

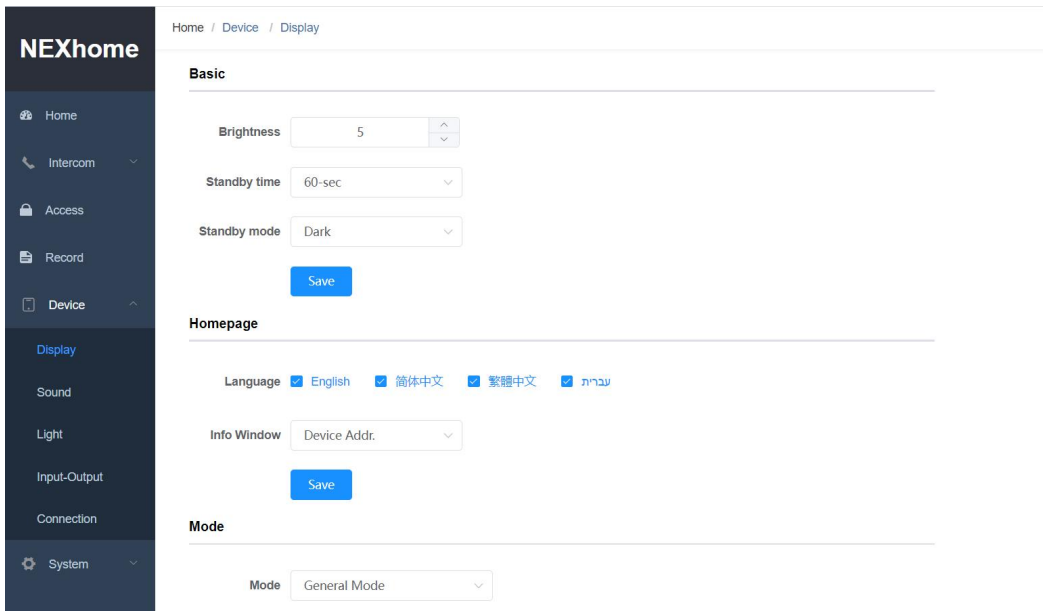


3.7.5 Screen Settings

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

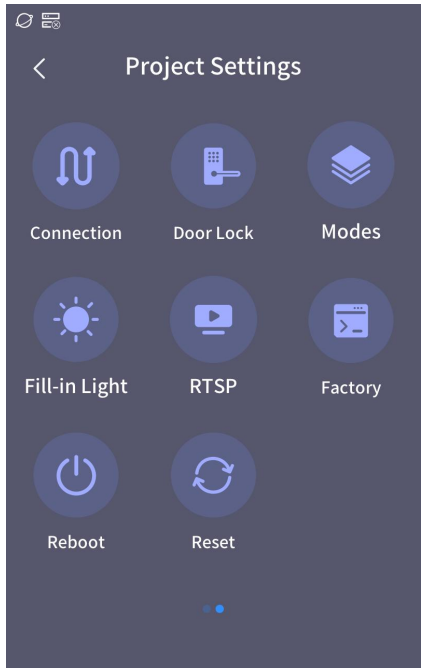


In Device - Display Settings - Basic of the web side backend,you can also set the brightness of the device screen, the standby time and the standby mode.

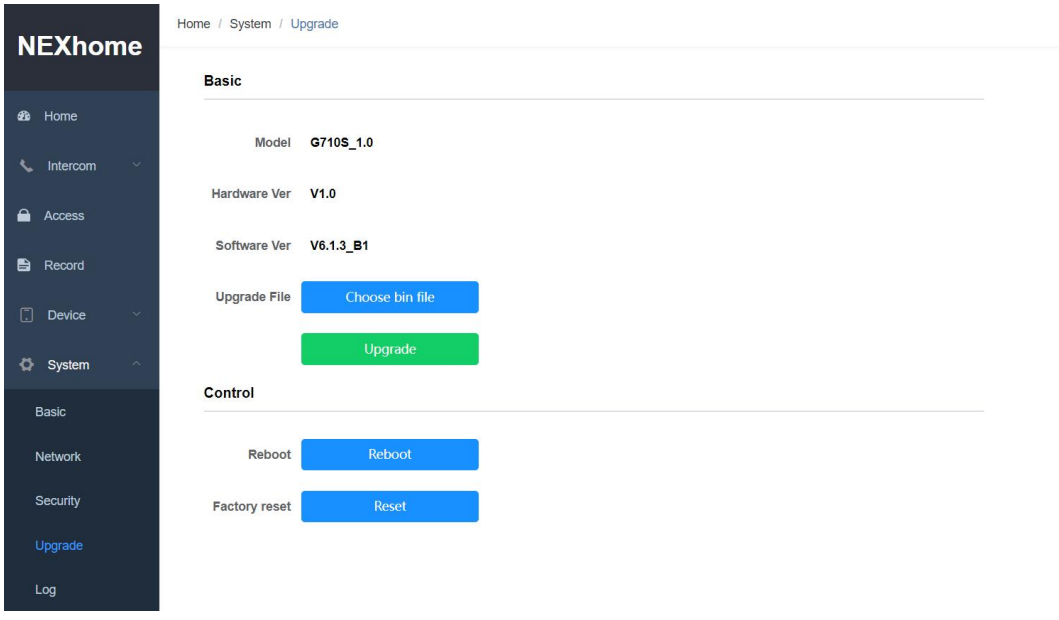


3.7.6 Restart and Reset

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.

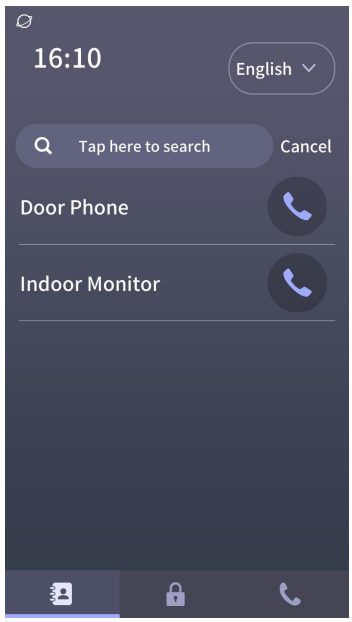


3.7.7 Modes Settings

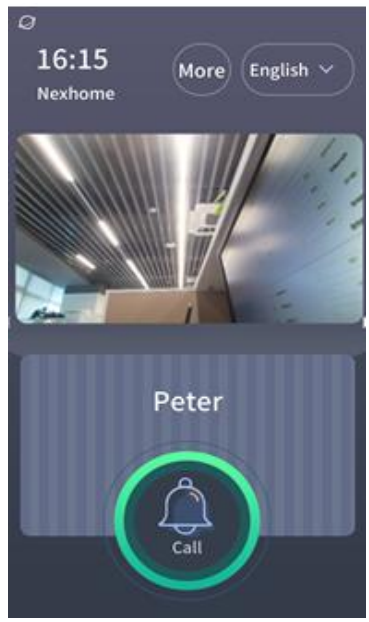
In the backend on the device side, click the Mode button to display the different main menus of the device, including General Mode, Access Mode, Doorbell Mode, and Directory Mode.

General Mode

Access Mode



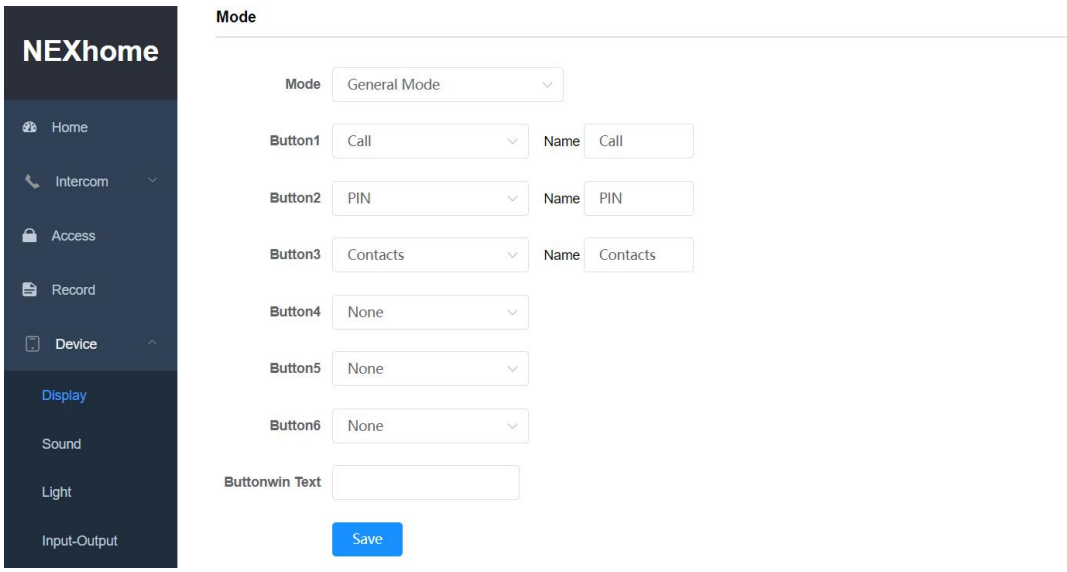
Directory Mode



Doorbell mode

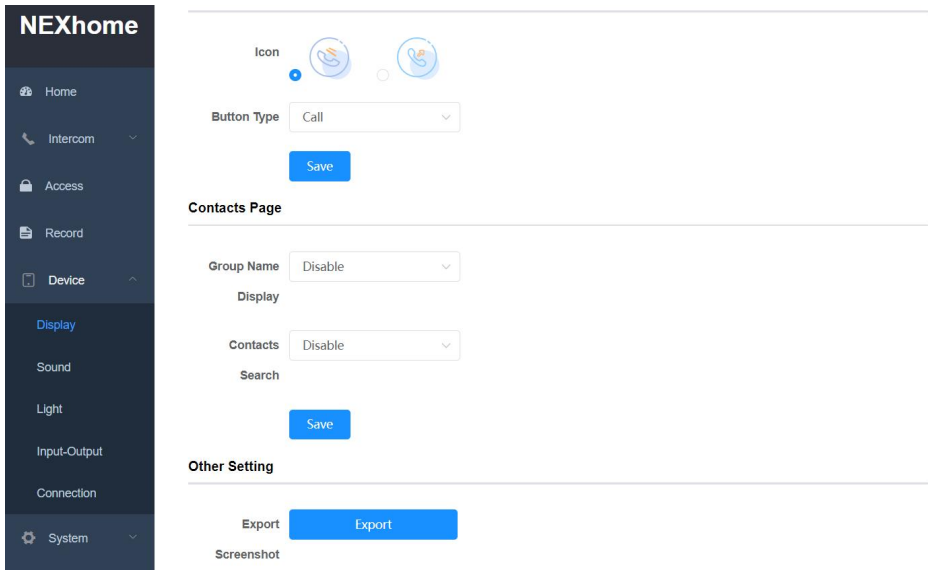
In the Device-Display-Mode of the web side,the different main menus of the device can also be selected,again including General, Access, Doorbell and Directory modes.

In the button icon, you can choose to set the dial, password, address book, QR code button icon.



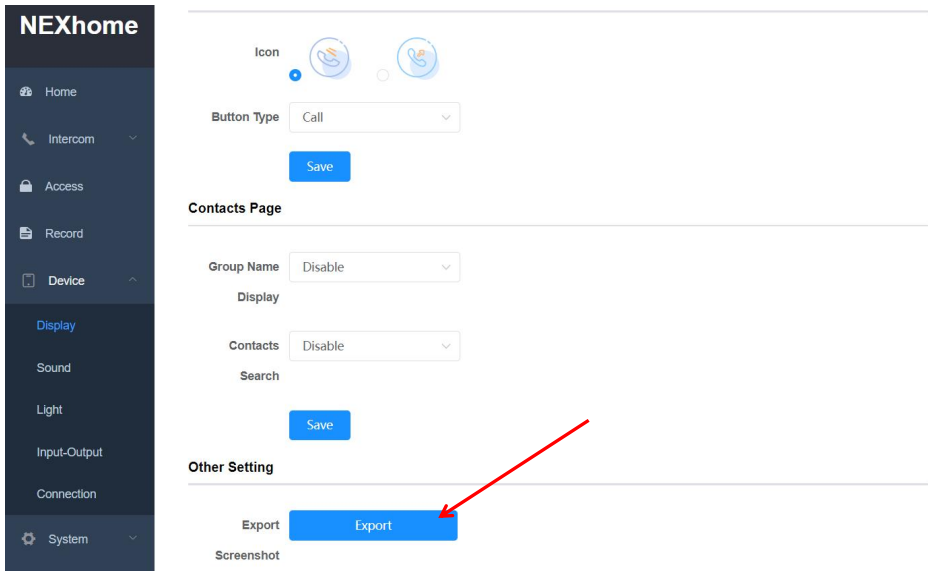
3.7.8Contacts Page Settings

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.



3.7.9Device screenshot

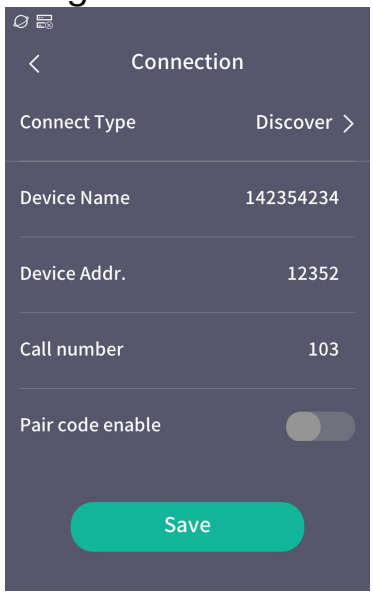
In the Device-Display Settings of the web side backend, in the Other Setting section, click the Export screenshot button to export the image of the current interface of the device.



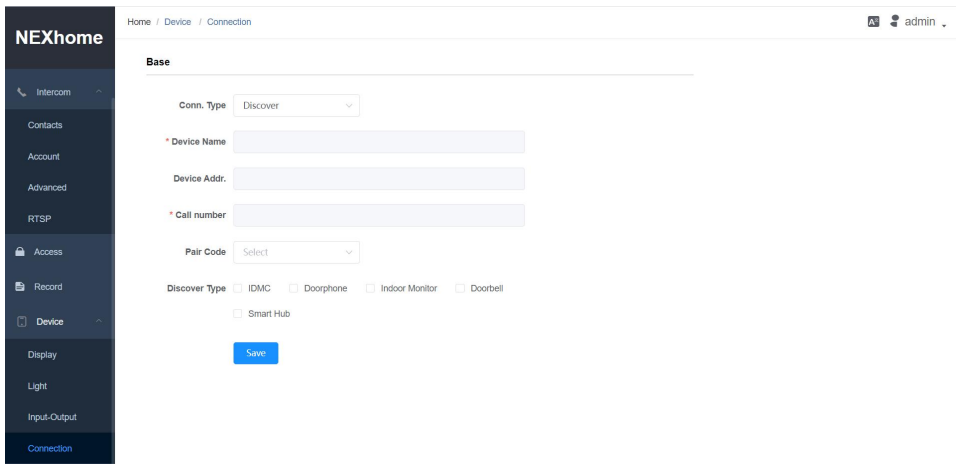
3.8 Advanced Settings

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.

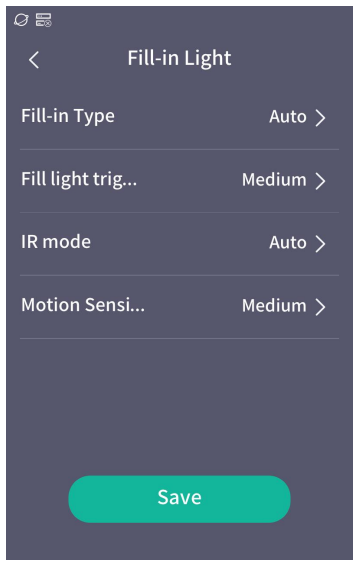


In the web backend, you can also change the device's connection settings by clicking **Device-Connection** Settings.

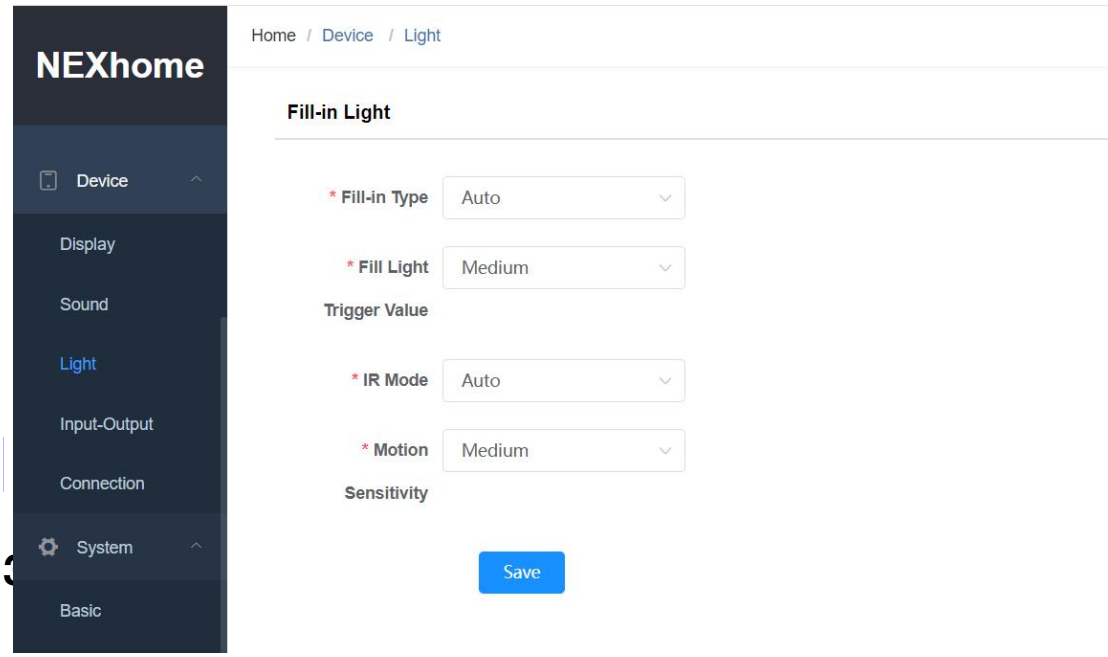


3.8.2 Light Settings

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

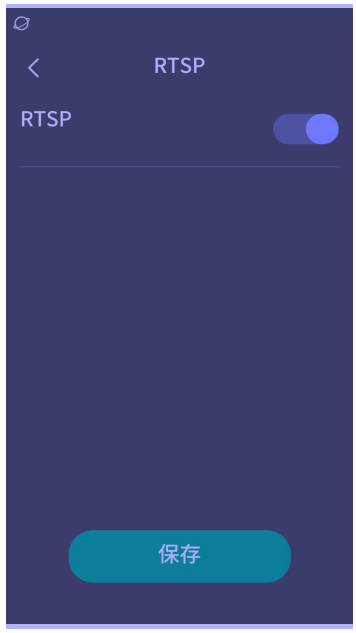


In the web backend, you can also change the device's lighting settings by clicking on **Device-Light** Settings.

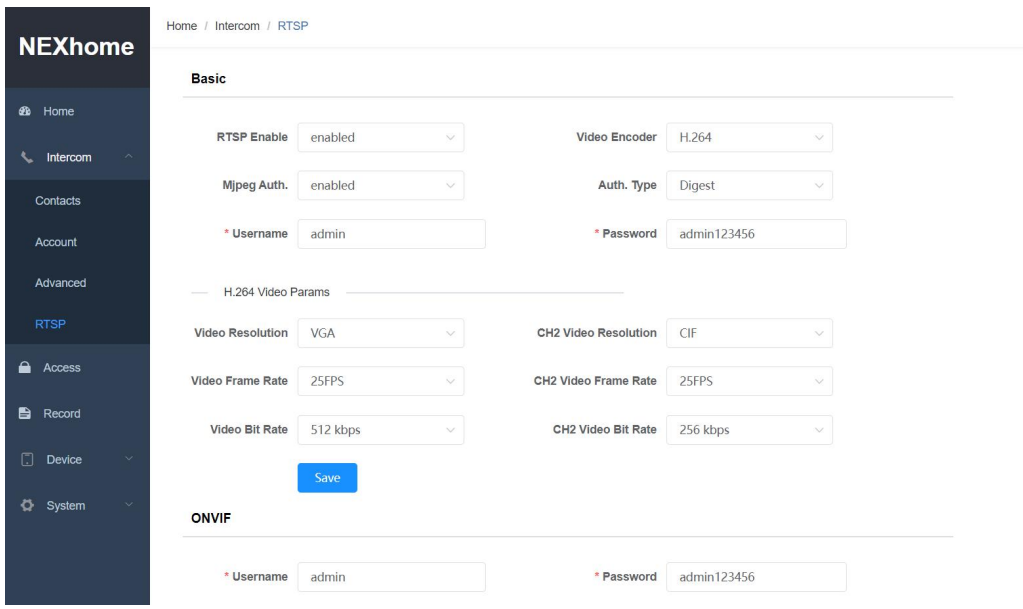


In the backend of the device side, click the **RTSP** button to

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

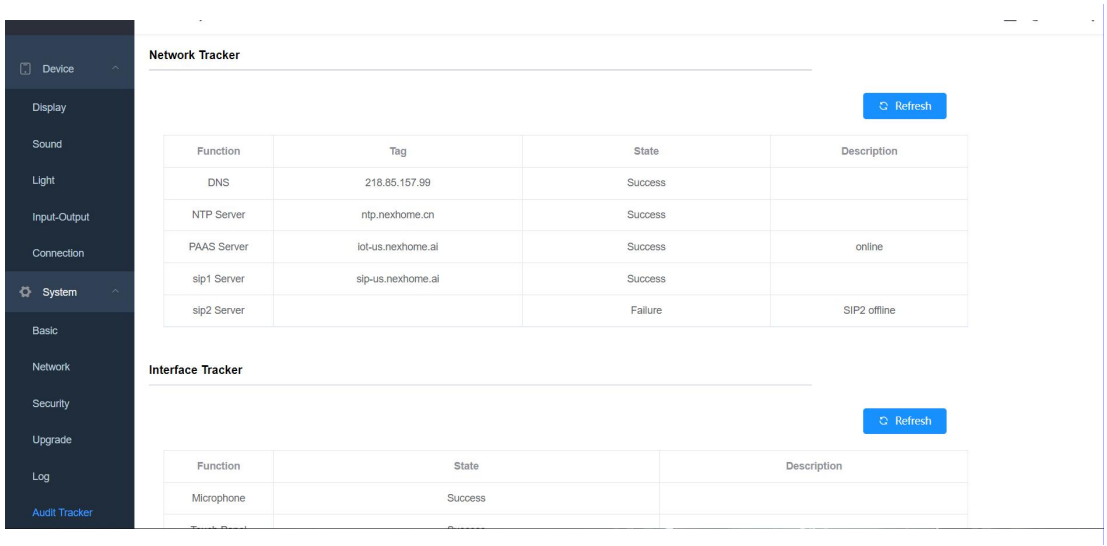
ONVIF User name and Password: default and rtsp user name and password are the same, when Mjpeg authentication is on,

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.

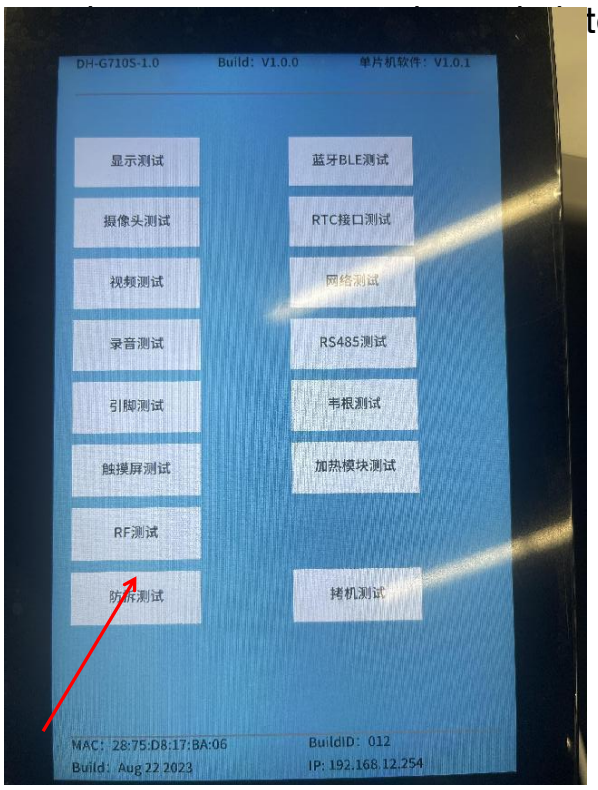
3.8.4 Audit Tracker

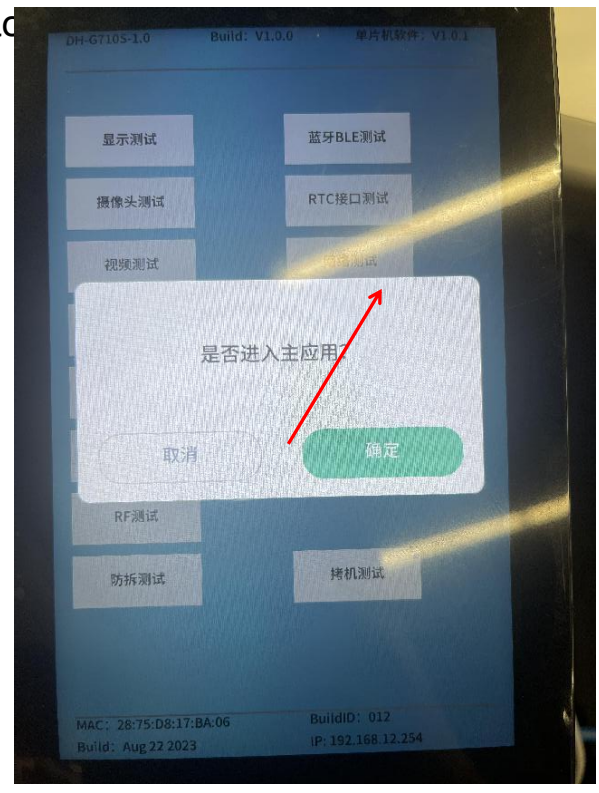
In the web backend, click on **System-Audit Tracker** to view various inspection results



3.8.5 Factory Testing

On the backend status information interface of the device end, click the MAC Address area three times in a row to select to enter the Factory Test, then enter the password 002396 to enter the Factory Test interface. The factory testing interface is used to detect hardware issues with device and is limited to professional technicians. Please do not enter the factory for testing during normal configuration. If you accidentally enter the Factory Test interface, simply quickly click on the "Mac" character in the bottom left corner. When a window pops up, select the right





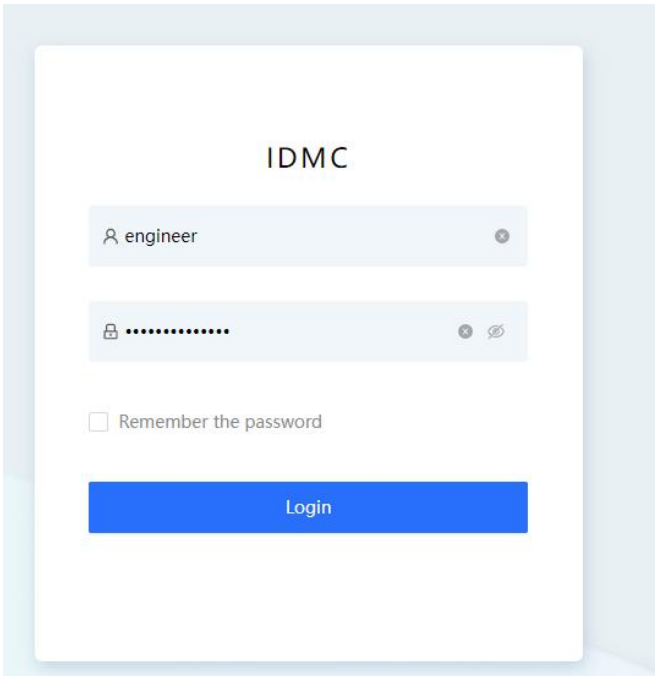
4 IDMC Configuration

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

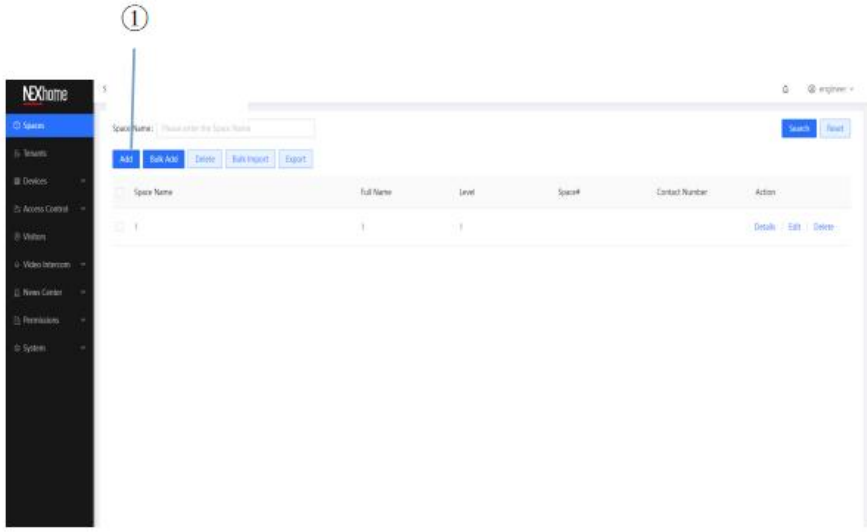
After installing the IDMC platform, double-click to open IDMC.exe and enter the IDMC platform webpage.

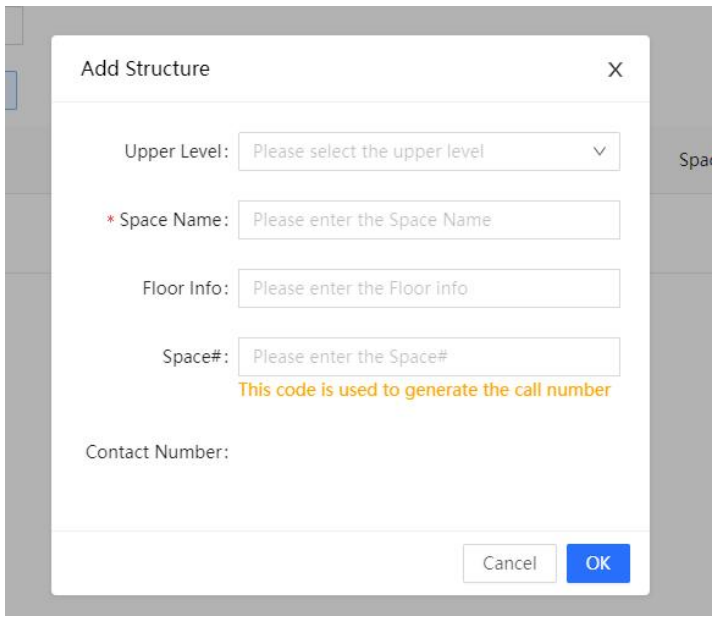
Enter account: engineer ;password: StarNetNexhome, click on Login to enter the IDMC platform interface.



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

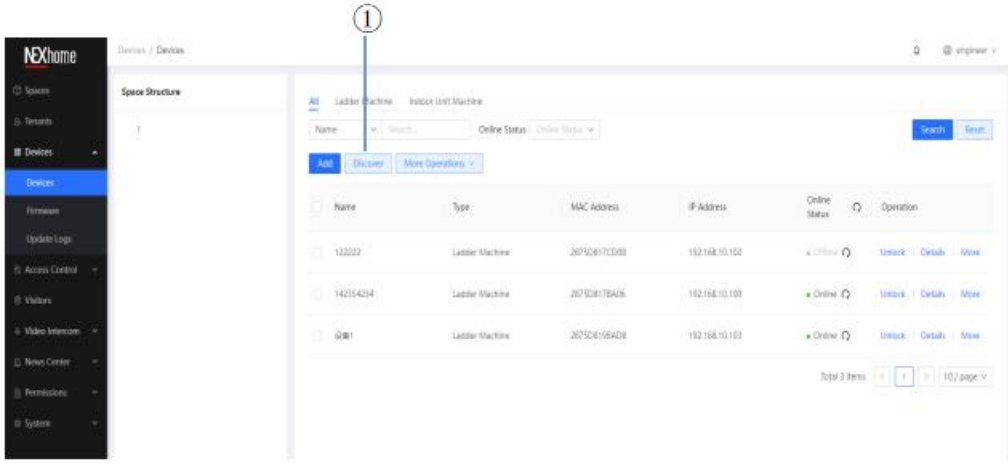
4.3.1 Adding Devices

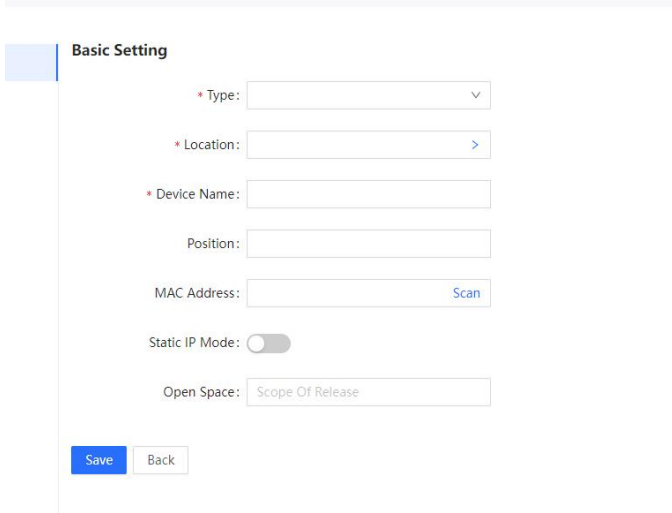
In the **Devices-Devices** section of the IDMC platform, click the **Discover** button ① and the system will automatically search for devices under the same local area network. Click the add button to the right of the device name to add, set the associated space and device name for the device, and click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

When adding a new device, you can fill in the device MAC, and the device can automatically register online when the network in the local area network is available.

The device can enable the 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 IP can be allocated automatically by turning on the DHCP function in the IDMC system management -DHCP configuration.

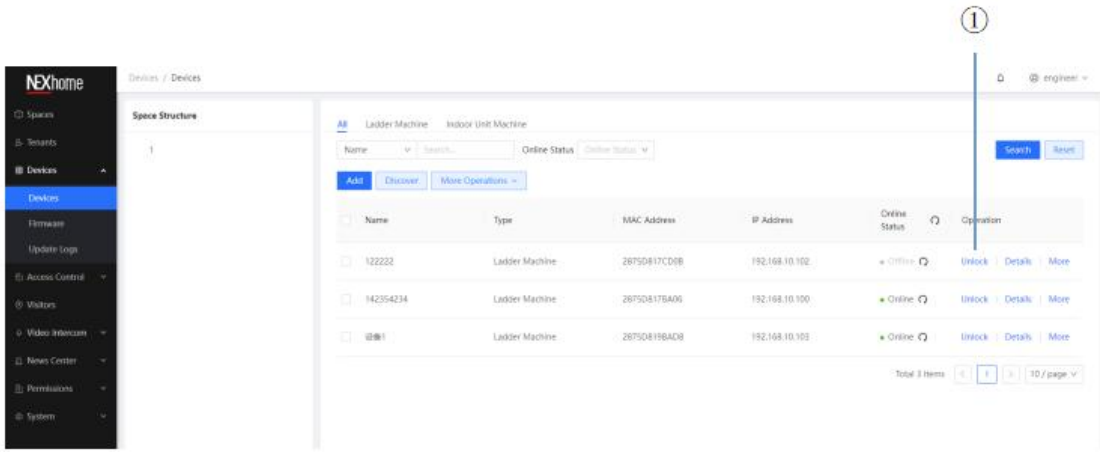




4.3.2 Device Unlocking

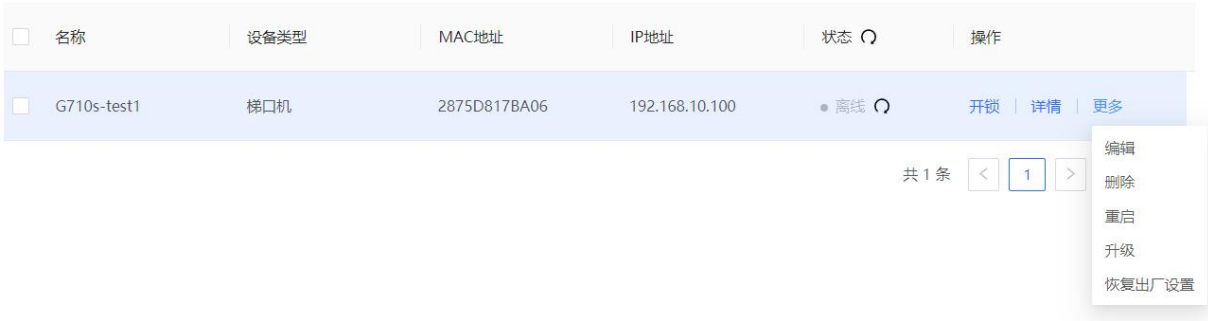
In the **Devices - Devices** section of the IDMC platform, click **Unlock** button①on the right side of the corresponding device, and the device will automatically unlock, device unlocking (access control unlocking or remote unlocking) supports capturing and uploading IDMC.

You can use the access control certificate issued by the IDMC to unlock the lock.



4.3.3 Device Operation

In the Device - Device section of the IDMC platform, click on the **More** button on the right side of the corresponding device to edit, delete, restart, upgrade, and restore production to the device. You can operate to resynchronize the address book and access control certificate.



4.3.4 Device Configuration

Add a configuration set to the IDMC Platform System Management-Device Configuration, modify the configuration in the configuration set, and select the associated devices that need to be synchronized.

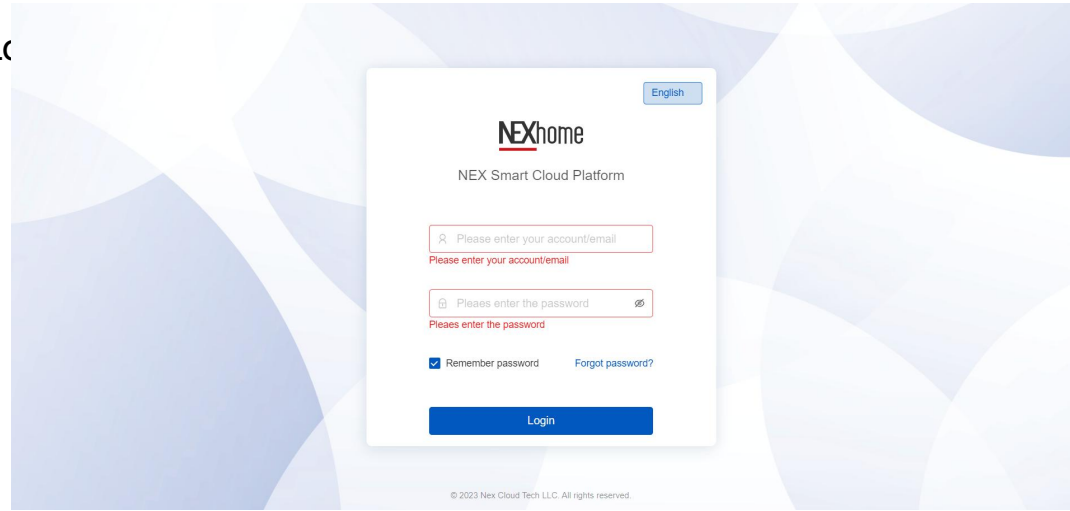
空间管理
用户管理
设备管理
门禁管理
访客管理
梯控管理
可视对讲
消息中心
信息发布
权限管理
员工管理
系统管理
系统配置
设备配置
操作记录
服务日志查看
DHCP配置
配置集
搜索...
创建时间:
开始日期
结束日期
更新时间:
开始日期
结束日期
查询
重置
设备小类:
设备厂商:
新增
配置集
设备小类
设备厂商
创建者
创建时间
更新时间
操作
G710S
梯口机
星网天合
nexhome-admin
2024-07-11 11:04:22
2024-07-11 11:04:22
修改配置
关联设备
同步记录
删除
共 1 条
1
10 条/页

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

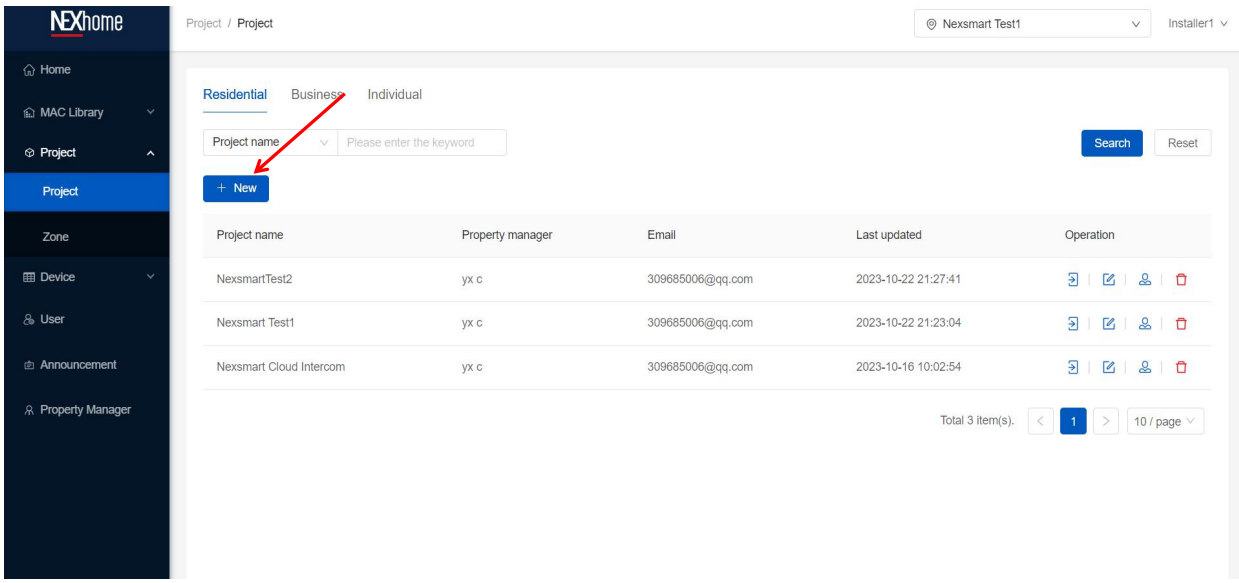
In the upper right corner of the login page, you can set the language of the cloud platform, and in the lower left corner, you can choose to remember your password, if you forget your password, you can click the lower right corner to reset your password. Enter the correct username and password and click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



5.2 Project Management

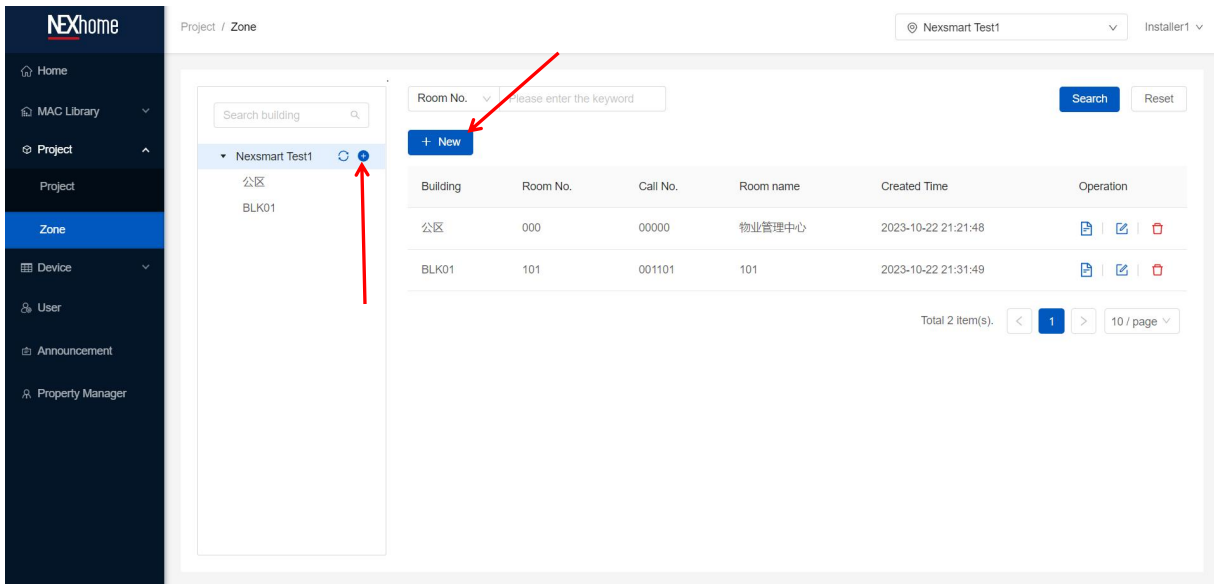
5.2.1 Project Management

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.



5.2.2 Space Management

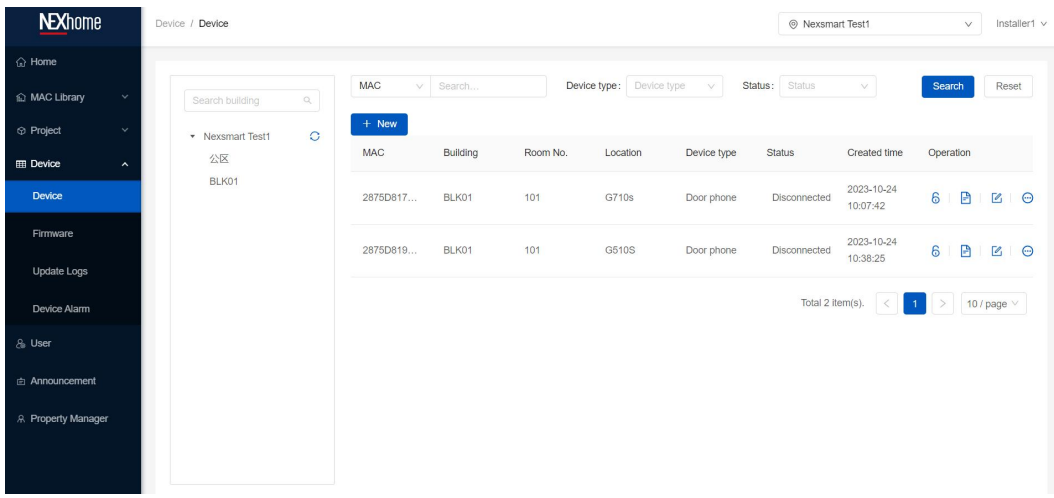
Log in to your installer account, and in Project Management - Space Management of NexSmart Cloud Platform, you can add new buildings and spaces under the project. Click the plus button on the left side to add a new building, and click the add button on the right side to add a new space under the building.



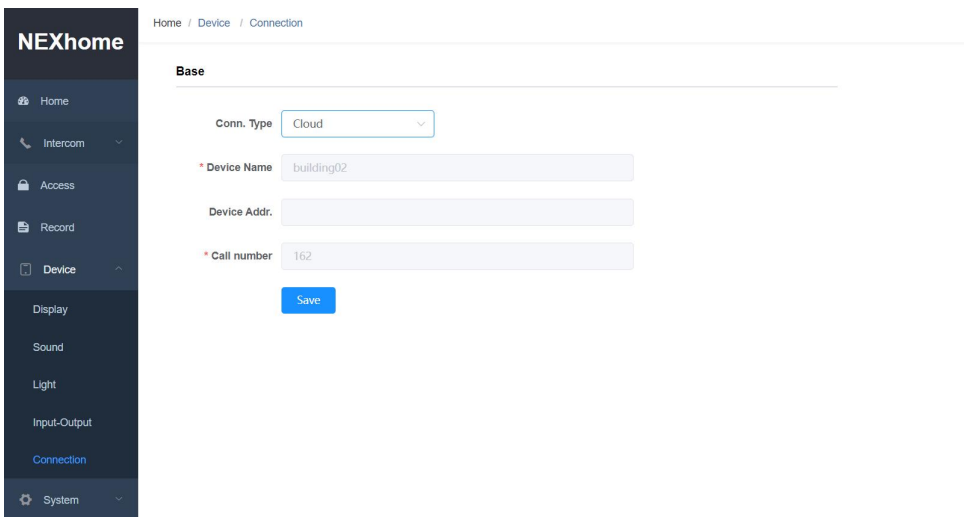
5.3 Device Management

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.



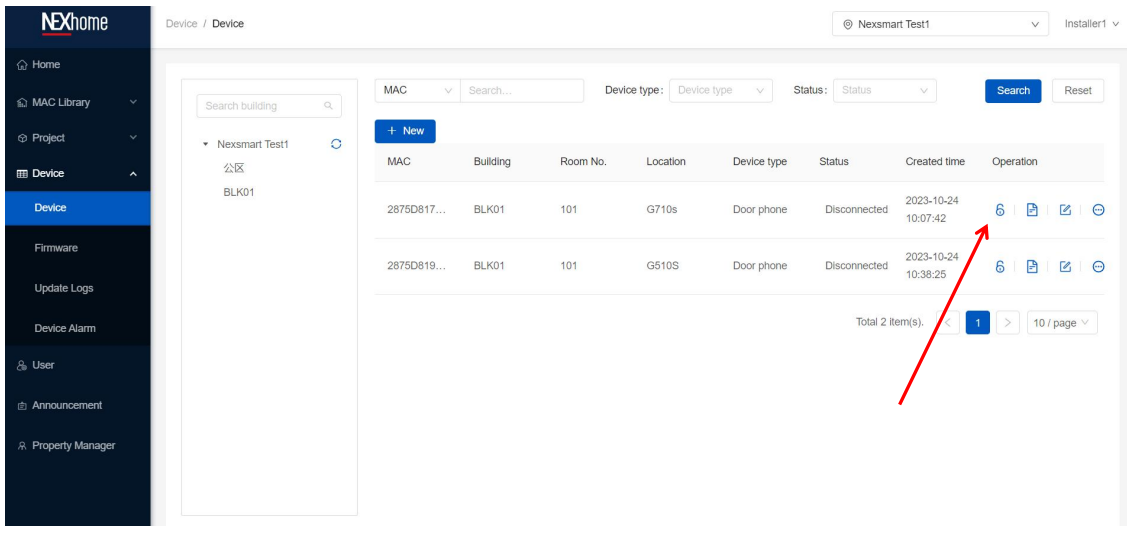
For added devices, you need to change the mode to cloud mode in the connection settings on the device side (web or device backend) in order to connect to the Nex Smart cloud platform.

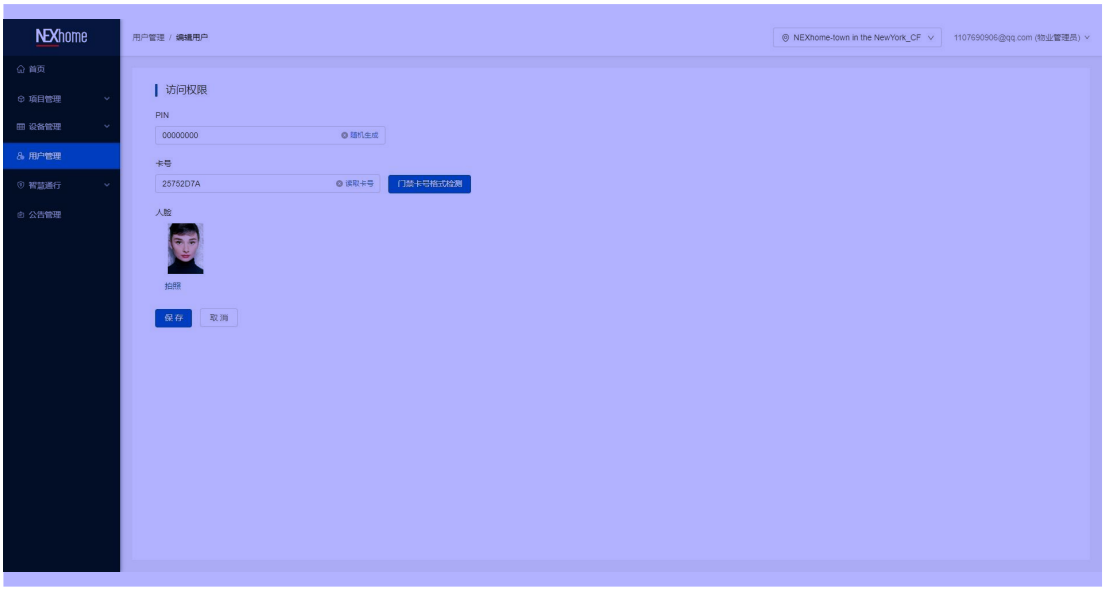


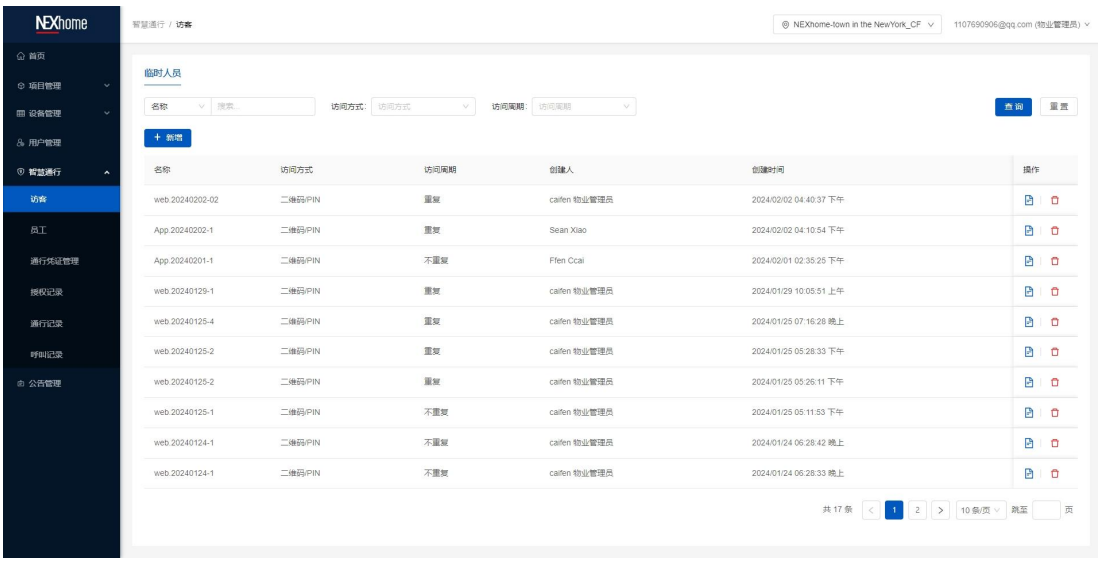
5.3.2 Device Unlocking

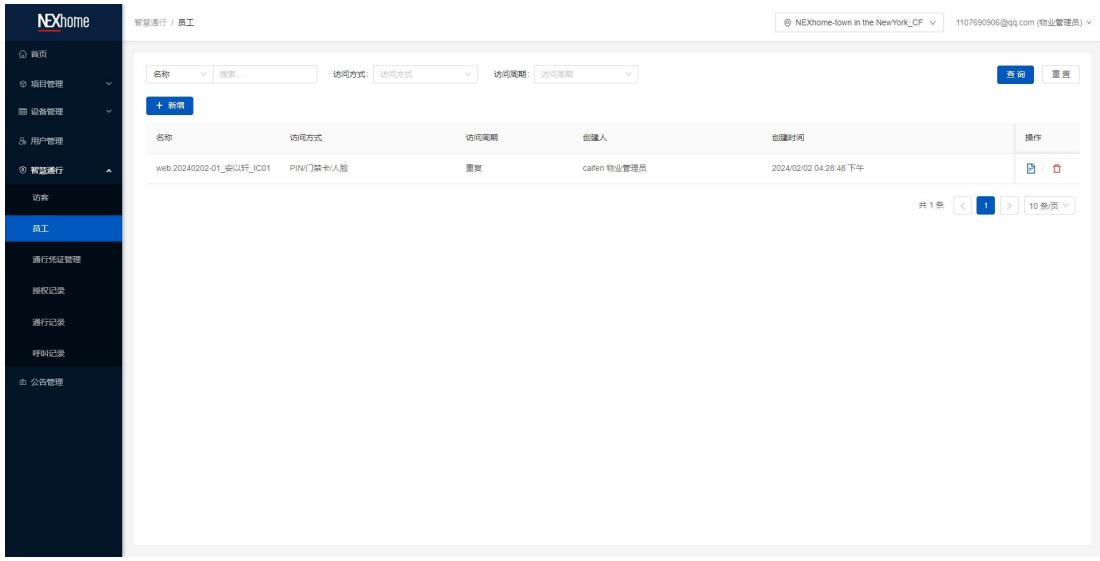
Log in to the installer account or property manager account, and in the NexSmart Cloud Platform's Device - Device, click the Unlock button on the right side of the corresponding device to control the device to unlock remotely.

Log in to the property manager's account. In the User Management interface, edit the user and click the Next button then you can set the user access control password, access control card, access control face. In the Smart Pass - Visitor interface, you can add a visitor access control, generate an access control password and an access control QR code, and send an email to the visitor mailbox. In the Smart Pass-Employee interface, you can add employee access control, access control cards, access control faces and access control passwords, and send emails to employee mailboxes.



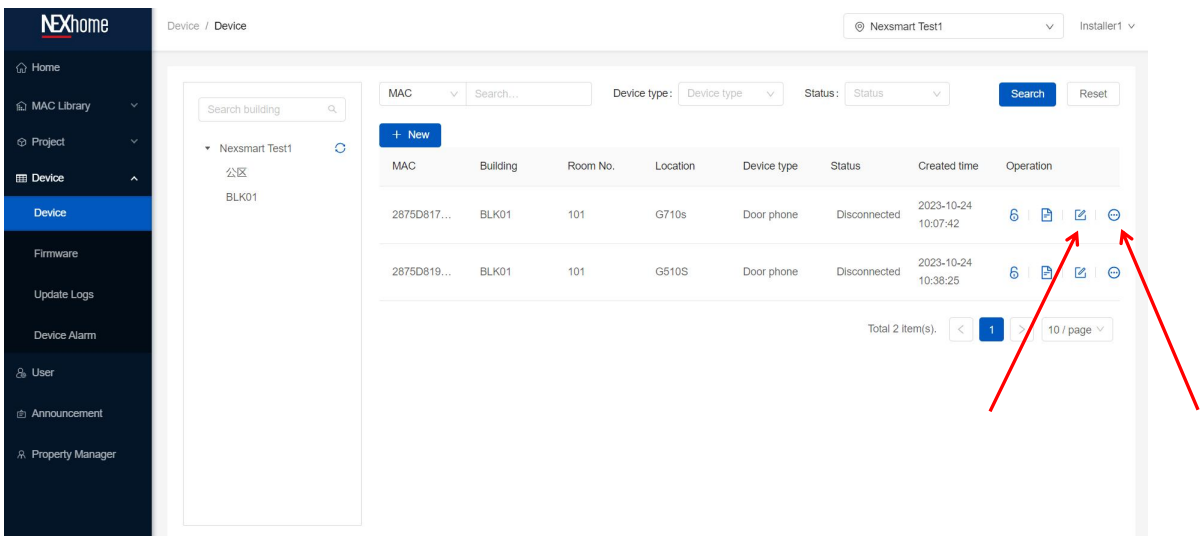

NEXhome
用户管理 / 编辑用户
NEXhome-town in the NewYork_CF
1107690906@qq.com (物业管理员)
首页
项目管理
设备管理
用户管理
智慧通行
公告管理
访问权限
PIN
00000000
随机生成
卡号
25752D7A
读取卡号
门禁卡号格式检测
人脸
拍照
保存
取消


NEXhome
智慧通行 / 访客
NEXhome-town in the NewYork_CF
1107690906@qq.com (物业管理员)
首页
项目管理
设备管理
用户管理
智慧通行
访客
员工
通行凭证管理
授权记录
通行记录
呼叫记录
公告管理
临时人员
名称
访问方式:
访问周期:
查询
重置
新增
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
App.20240202-1 二维码/PIN 重复 Sean Xiao 2024/02/02 04:10:54 下午
App.20240201-1 二维码/PIN 不重复 Ffen Ccai 2024/02/01 02:35:25 下午
web.20240129-1 二维码/PIN 重复 caifen 物业管理员 2024/01/29 10:05:51 上午
web.20240125-4 二维码/PIN 重复 caifen 物业管理员 2024/01/25 07:16:28 晚上
web.20240125-2 二维码/PIN 重复 caifen 物业管理员 2024/01/25 05:28:33 下午
web.20240125-2 二维码/PIN 重复 caifen 物业管理员 2024/01/25 05:26:11 下午
web.20240125-1 二维码/PIN 不重复 caifen 物业管理员 2024/01/25 05:11:53 下午
web.20240124-1 二维码/PIN 不重复 caifen 物业管理员 2024/01/24 06:28:42 晚上
web.20240124-1 二维码/PIN 不重复 caifen 物业管理员 2024/01/24 06:28:33 晚上
共 17 条
10 条/页
跳至
页



5.3.3 Device Configuration

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 Set Permission Group

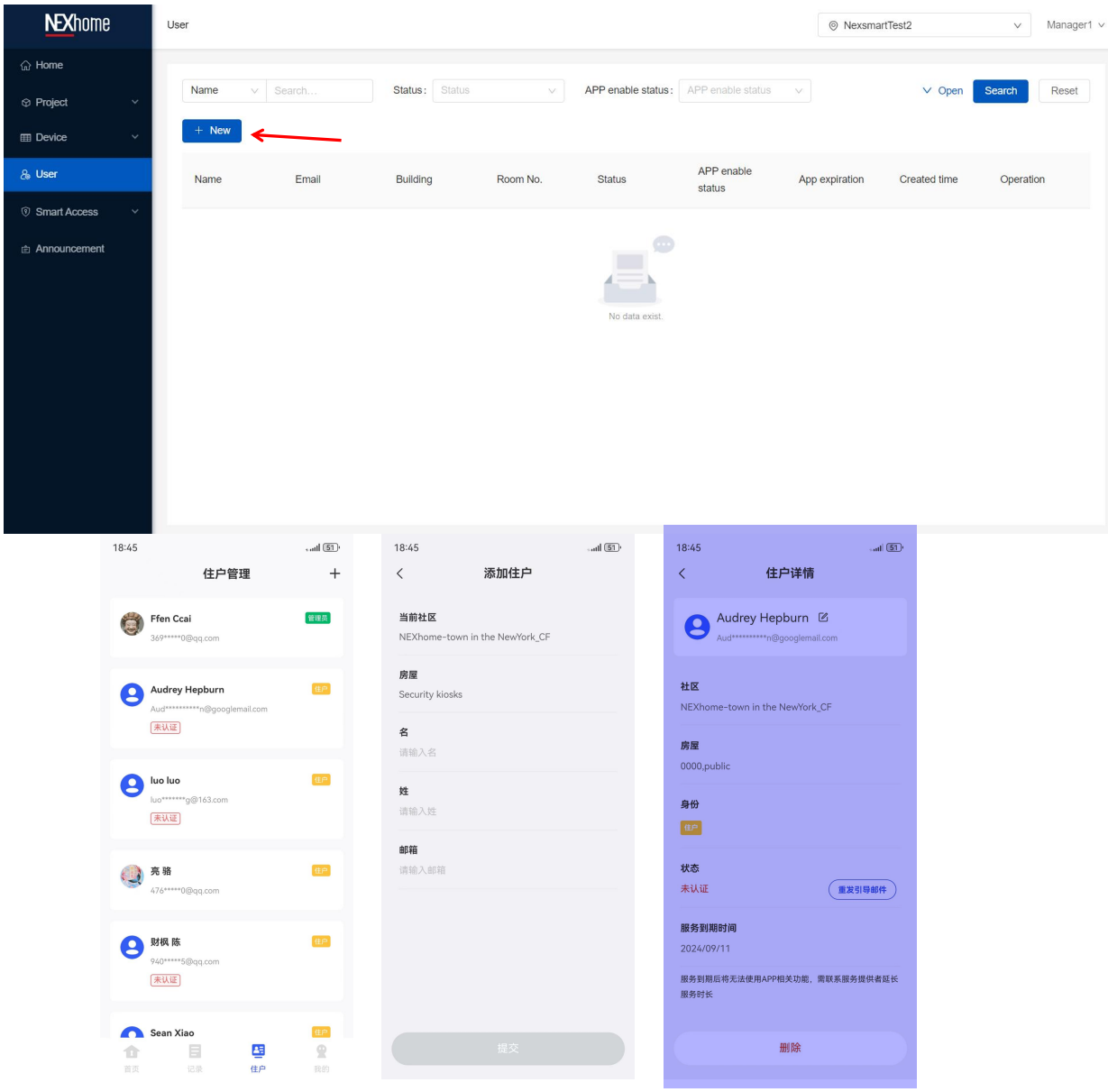
Log in to the installer account or property administrator account, in the Smart Pass - Permission Group of NexSmart Cloud Platform, add and set permission group name, repetitive pattern, passable period, select device rules, and accessible device. You can add users and associated homes.

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.

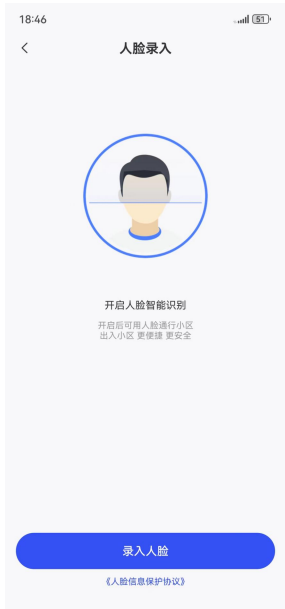
Housekeepers can add and delete tenants through the APP.

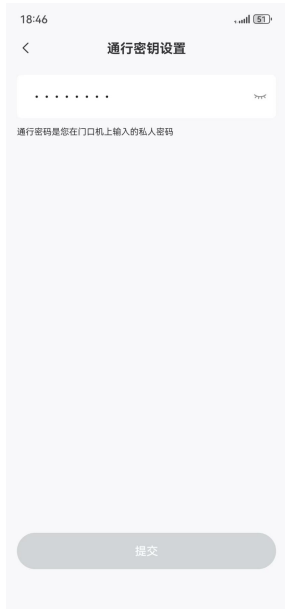


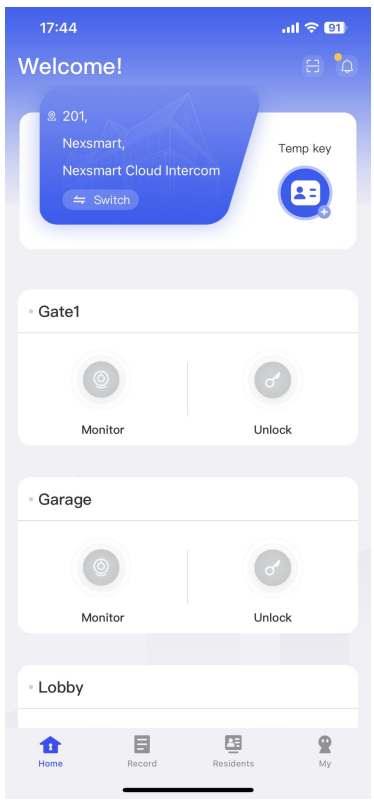
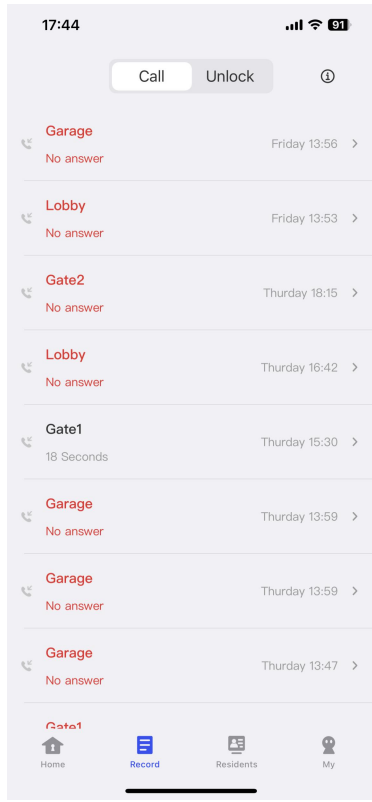
5.4.3 Device Unlocking

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 create a temporary secret key for visitors, generate an access control QR code and an access control password, and send an email to the visitor's mailbox.

In my interface, you can authorize face entry and set the unlock password.


18:46
人脸录入
开启人脸智能识别
开启后可用人脸通行小区
出入小区 更便捷 更安全
录入人脸
《人脸信息保护协议》


18:46
通行密钥设置
通行密码是您在门口机上输入的私人密码
提交

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.