Smart Home Center

User’s Manual

V1.0.0

Foreword

General

This manual introduces the functions and operations of Smart Home Center (hereinafter referred to as "the Device").

Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

Signal Words	Meaning
DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
TIPS	Provides methods to help you solve a problem or save you time.
NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	May 2020

Interface Declaration

This manual mainly introduces the relevant functions when you use the device. The interfaces used for manufacture, returning to the factory for inspection, and locating fault are not described in this manual. Please contact technical support if you need information about these interfaces.

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the

electronic version shall prevail.

- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

This section introduces the proper handling of the Device, hazard prevention, and property damage prevention. Read the manual carefully before using the Device, follow the instructions when using the Device, and keep the manual well for future reference.

Operating Requirements

- Do not place or install the Device in a place exposed to sunlight or near the heat source.
- Keep the Device away from dampness, dust or soot.
- Keep the Device installed horizontally on the stable place to prevent it from falling.
- Do not drop or splash liquid onto the Device, and make sure that there is no object filled with liquid on the Device to prevent liquid from flowing into it.
- Place the Device in a well-ventilated place, and do not block the ventilation.
- Use the Device within the rated range of power input and output.
- Do not dissemble the Device randomly.
- Transport, use and store the Device under the allowed humidity and temperature range.
- Do not hot swap the SD card and SSD; otherwise the data might be lost or damaged.
- Use the recommended SD card and SSD to ensure storage reliability.
- Keep the Device away from microwave equipment to avoid the effect on wireless communication.
- Press the Home button for ≥ 6 seconds, and the Device will be forcibly restarted. Be cautious.

Power Requirements

- Improper battery use might result in fire, explosion, or inflammation.
- When replacing the battery, make sure that the same model is used.
- Use the recommended power cables in the region and use them under the rated specification.
- Use the power adapter provided with the Device; otherwise, it might result in people injury and device damage.
- The power source shall conform to the requirements of the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited power Source requirement according to IEC60950-1. Note that the power supply requirement is subject to the device label.
- Connect the Device (type-I structure) to the power socket with protective earthing.
- The appliance coupler is a disconnection device. Keep a convenient angle when using it.

The figures in the manual are for reference only, and the actual interface shall prevail.

IC RF Radiation Exposure 5G Statement:

The user manual for local area network devices shall contain instructions related to the restrictions mentioned in the above sections, namely that:

(i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

(ii) the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall comply with the e.i.r.p. limits specified for point-to-point and non point-to-point operation as appropriate.

(i)Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

(ii) le gain d'antenne maximal autorisé pour les appareils dans la bande 5725-5850 MHz doivent respecter le pire limites spécifiées pour le point-à-point et l'exploitation non point à point, le cas échéant.

Users should also be advised that high-power radars are allocated as primary users (i.e. priority users) of the bands 5725-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

Les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5725-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

FCC Supplier’s Declaration of Conformity

Brand name / model number

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Suppliers Name

Suppliers Address (USA)

Suppliers phone number and / or internet contact information

Table of Contents

1 Product Overview

1.1 Introduction

The Device is designed for civil use, and it serves as the household security control center. It can connect to Wi-Fi cameras, battery-powered cameras, doorbells, smart locks, video intercoms, household sensors (magnetic contacts, PIRs, and flood detectors), and many other surveillance products.

The Device adopts a 7" touchscreen which can be directly used for controlling devices and live view. It integrates offline speech recognition, MIC control and privacy masking to protect family privacy; it provides intelligent speaker through Bluetooth 5.0, high-fidelity sound chamber and other modules;

1.2 Packing List

When you receive the product, check whether there is obvious damage to the packing box. Unpack the box, and check whether the components are complete against the following packing list.

Table 1-1 Packing list

Name	Quantity
Power adapter	1
Warning label	1
Warranty card	1
smart home insert	1
Network cable	1
Plastic bag	1
Quick Start Guide	1
QR code	1

1.3 Structure

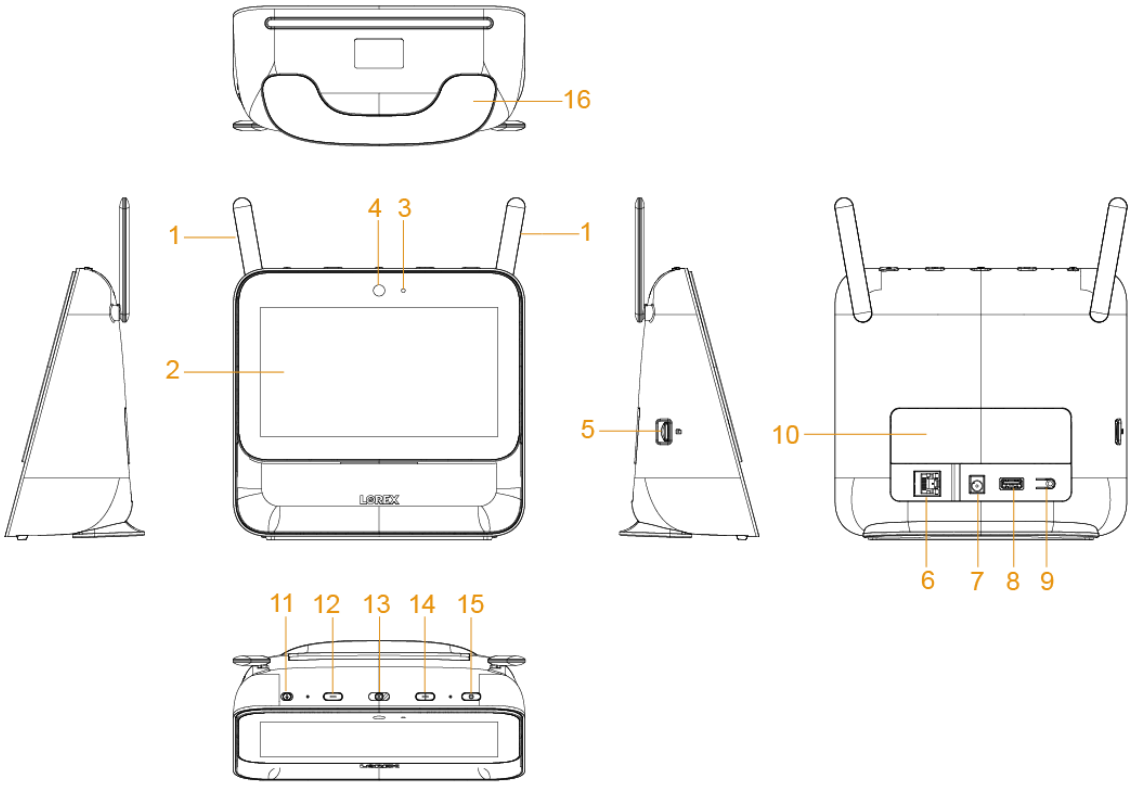


Table 1-2 Structure

No.	Description	No.	Description
1	Antenna	9	Pairing button
2	Touchscreen	10	SSD protective cover
3	Photosensitive sensor	11	Muting switch
4	Camera	12	Volume down
5	SD card slot	13	Camera switch
6	Network port	14	Volume up
7	Power port	15	Home button
8	USB port	16	Base

2 First-Time Setup

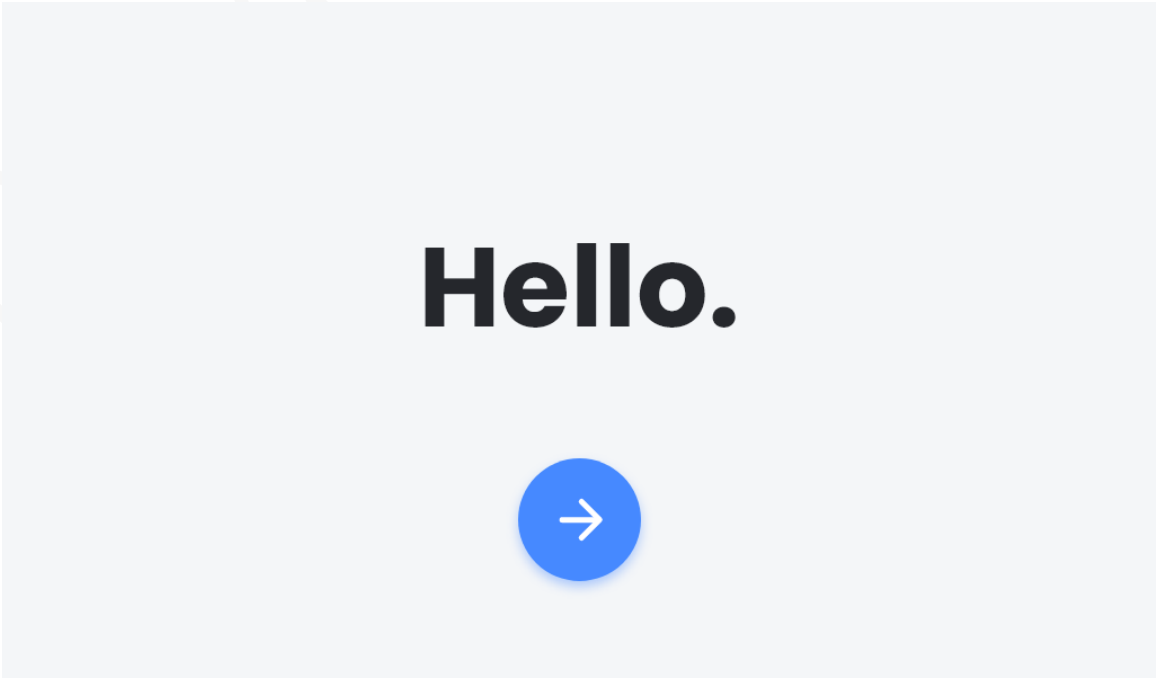
For first-time use or after you have restored the Device to default settings, finish the setup with the following steps.

2.1 Startup

Step 1 Connect the power supply to start the Device, and then the initial interface is displayed.

Figure 2-1 Initial interface

Figure 2-2 Hello



2.2 Initialization

2.2.1 Password Settings

Step 1 On the **Hello** interface, tap  .

The **Create a Passcode** interface is displayed.

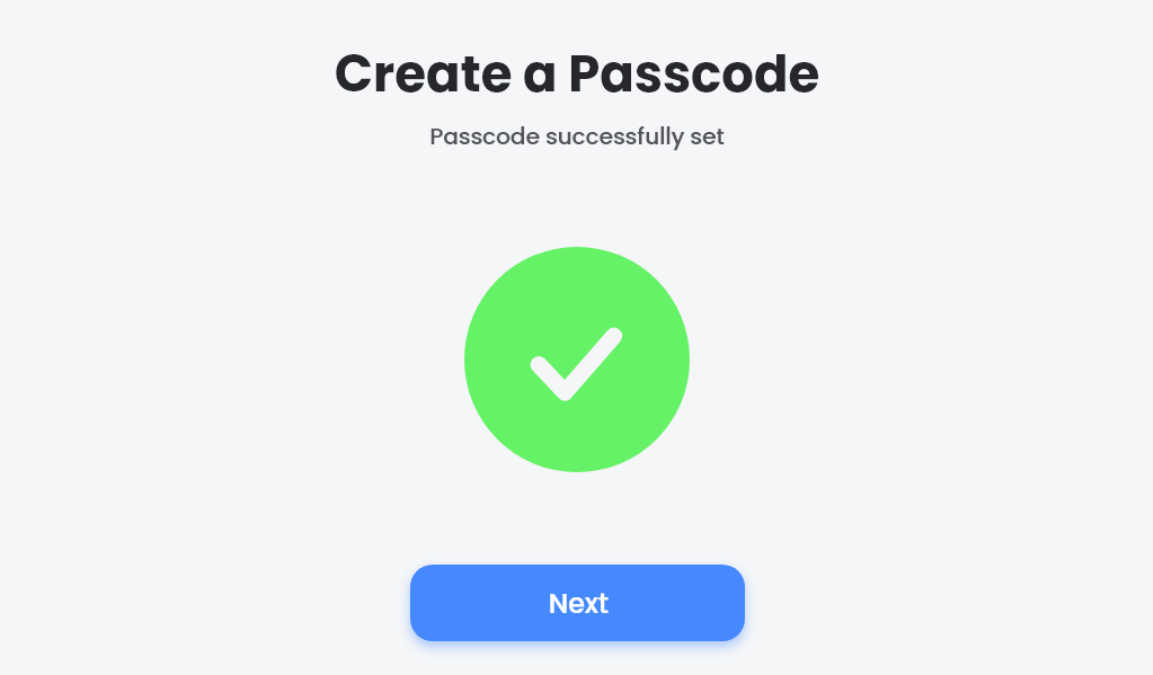
- If you want to skip this step, tap **Set Up Later**, and the face unlock setting step will also be skipped.
- The passcode is used to unlock the Device and arm sensors.

Figure 2-3 Create a passcode

Step 2 Set a passcode with 6 digits, and then the **Confirm Passcode** interface is displayed.

Step 3 Confirm the passcode, and the **Passcode successfully set** interface is displayed.

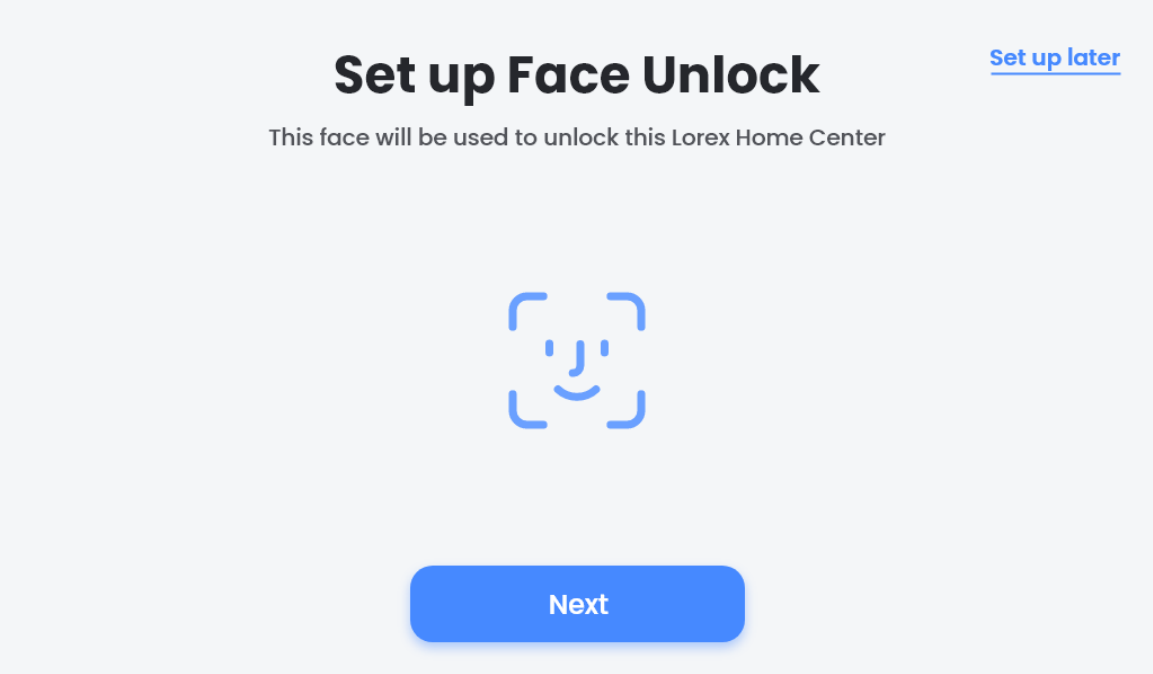
Figure 2-4 Passcode successfully set



Step 4 Tap **Next**, and the **Set up Face Unlock** interface is displayed.

If you want to skip this step, tap **Set up later**.

Figure 2-5 Set face unlock



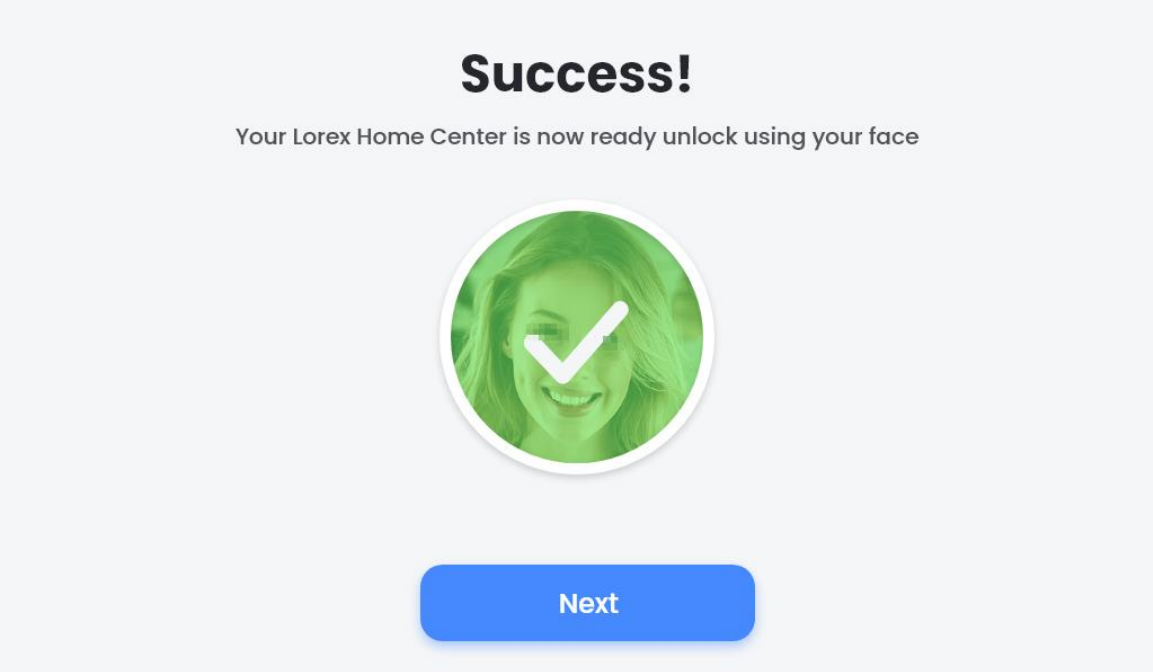
Step 5 Tap **Next**, and the face recognition interface is displayed.

Position your face within the frame, and face picture can be captured.

If the camera is not open, there will be a prompt on the interface.

Step 6 After the face is captured, the **Success** interface is displayed.

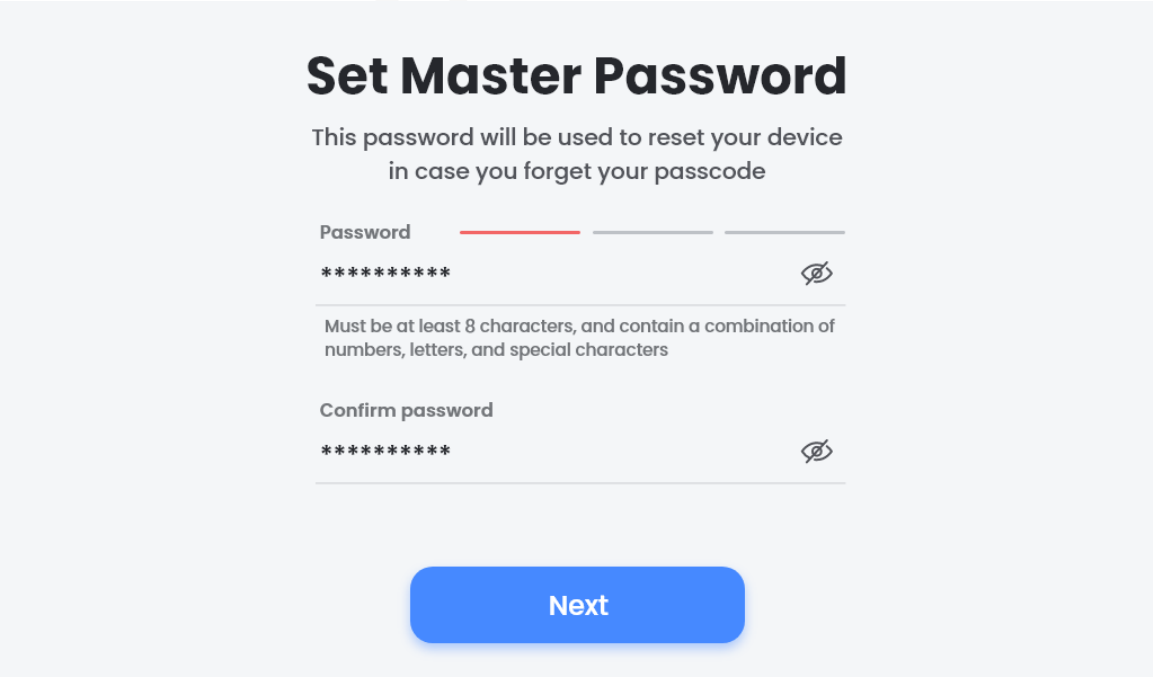
Figure 2-6 Face capture success



Step 7 Tap **Next**, and the **Set Master Password** interface is displayed.

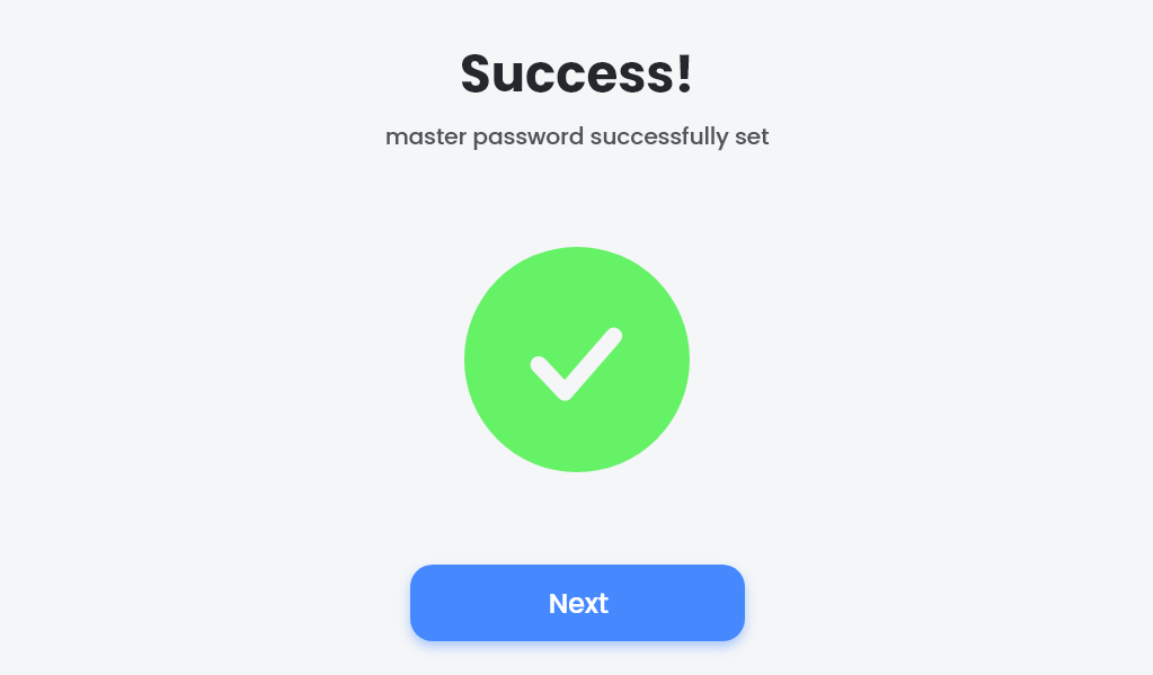
- The password should consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special characters (excluding ' " ; : &). Set a high security password according to the prompt of password strength.
- The password is used to reset the Device in case that you forget the passcode.

Figure 2-7 Set master password



Step 8 Set a strong password, and then tap **Next**.
The **Success** interface is displayed.

Figure 2-8 Success



2.2.2 Network Settings

Step 1 Tap **Next** after you set the master password.
The **Network Setup** interface is displayed.

Figure 2-9 Network setup

Step 2 Select a connection method from Wired Connection, Wireless Connection, and Use Offline.

- Wired Connection

1) Tap **Wired Connection** on the **Network Setup** interface, and then tap **Next**.
2) Connect the Device to the router with a network cable, and then tap **Continue**.

The connecting interface is displayed.

DHCP is the default setting and the IP address can be obtained automatically.

Figure 2-10 Connecting network

3) The prompt interface is displayed if connection is successful.

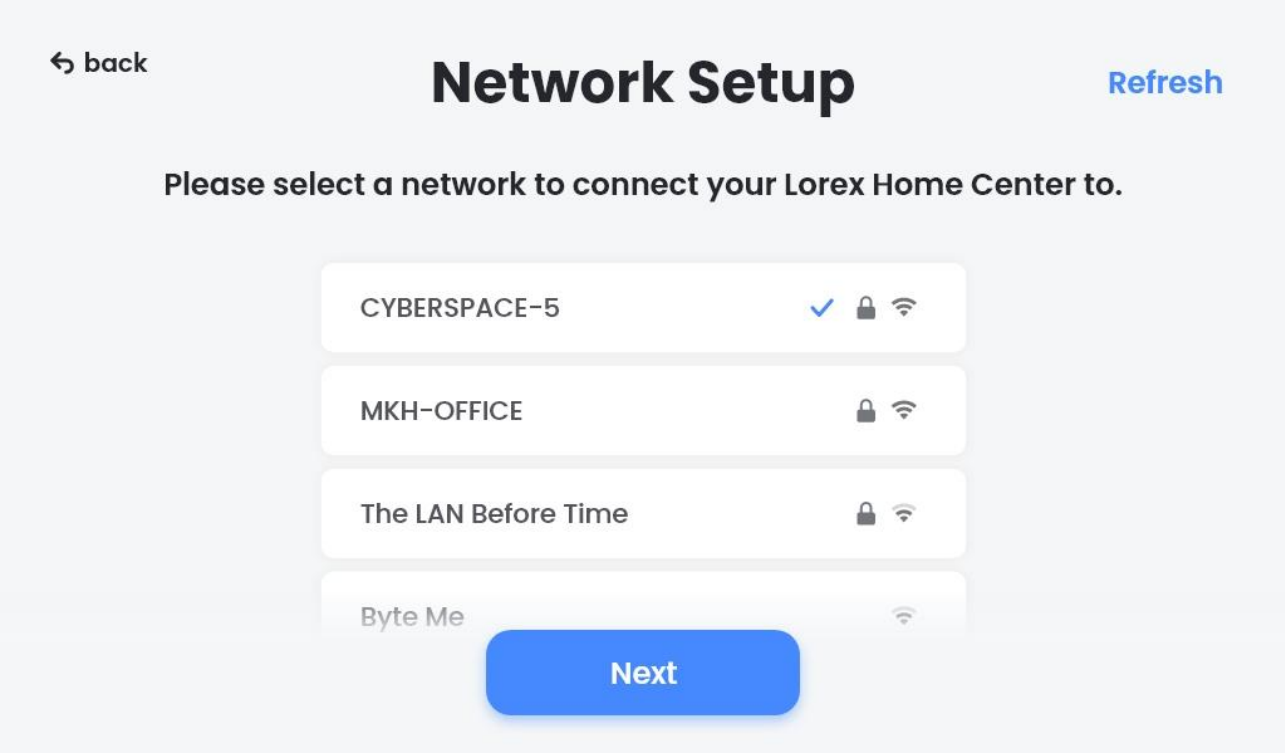
- Wireless Connection

1) Tap **Wireless Connection** on the **Network Setup** interface, and then tap **Next**. The **5 GHz Network Required** prompt is displayed.

The Device uses 5 GHz. Make sure that your router supports dual-band Wi-Fi, and that 5 GHz network is enabled.

2) Tap **PROCEED**, and the searched Wi-Fi hotspots are displayed based on the signal strength.
3) Select a network, enter the password of the network if any, and then tap **Connect**. The connecting interface is displayed.
4) The icon ✓ will be displayed next to the network if it is connected successfully.

Figure 2-11 Successful connection



- Use Offline

1) Tap **Use Offline** on the **Network Setup** interface, and then tap **Next**.
   The **Offline Mode** prompt is displayed.

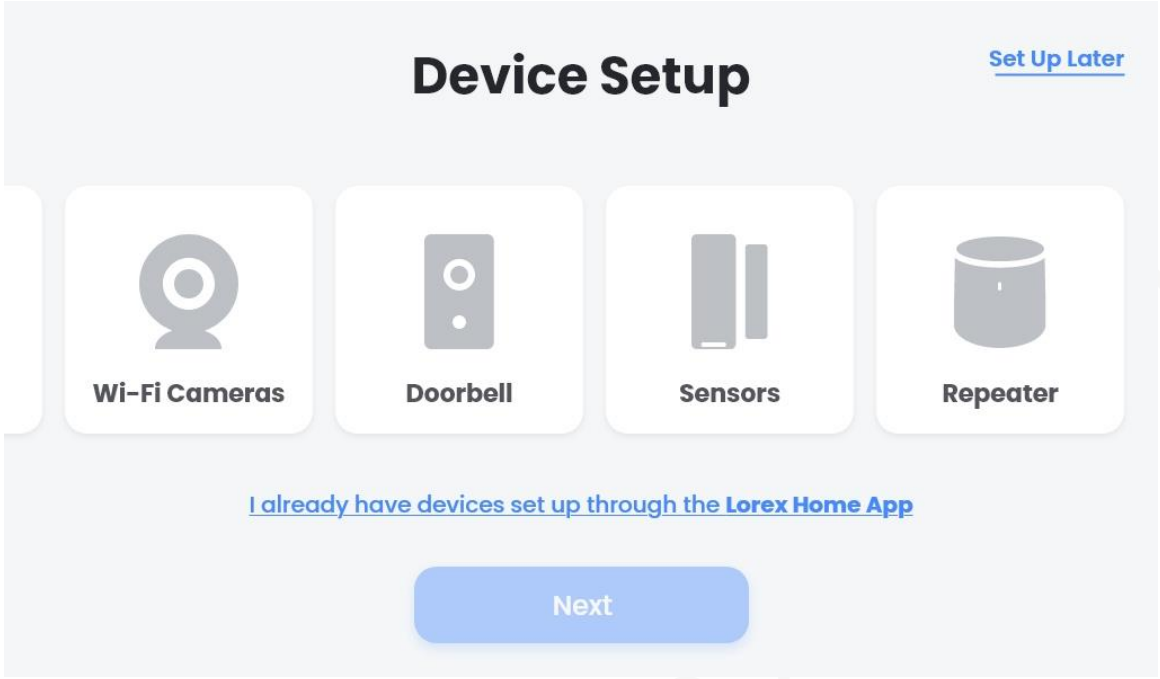
   - If you select this mode, network features will be disabled, including remote viewing, cloud backup, and software upgrade. You cannot connect the Device to App either, but the Device can be connected with 2.4G cameras through AP method.
   - If you want to connect to a network later, go to **Settings > Network Settings**.

2) Tap **PROCEED**, and the **Device Setup** interface is displayed.

2.2.3 Adding Devices

On the **Device Setup** interface, you can add Wi-Fi cameras, doorbells, sensors and repeaters. This section takes adding a Wi-Fi camera as an example.

Figure 2-12 Device setup



Step 1 On the **Device Setup** interface, select **Wi-Fi Cameras**, and then tap **Next**.
The **Wi-Fi Camera Setup** interface is displayed.

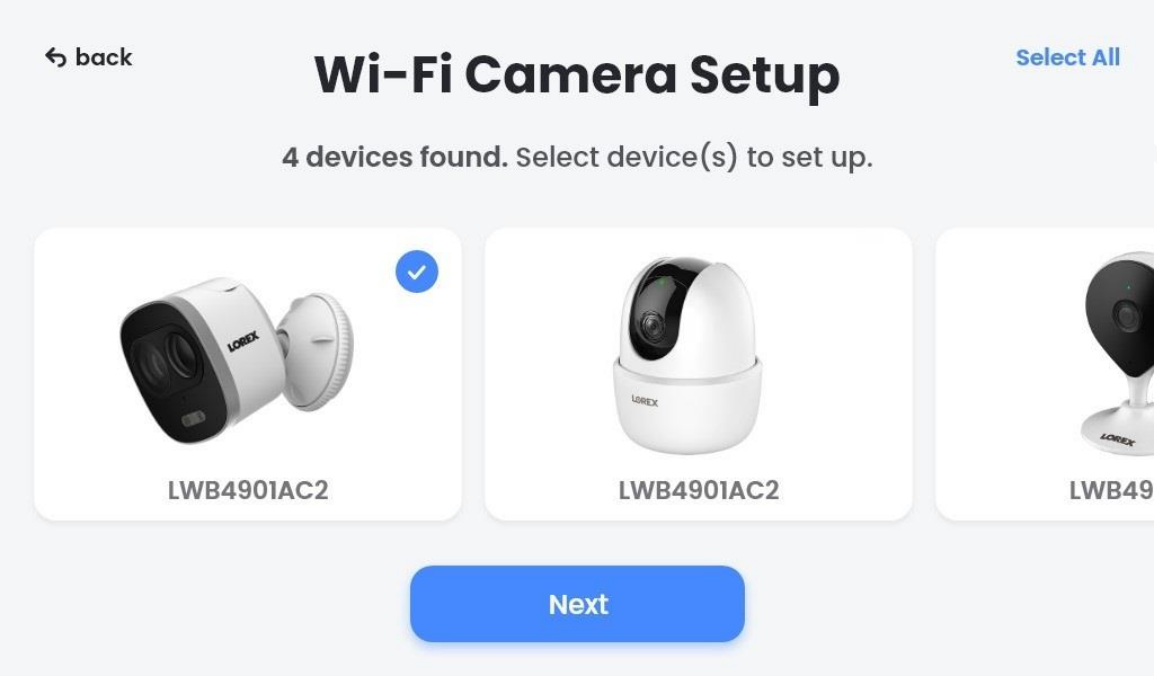
Figure 2-13 Wi-Fi camera setup

Step 2 Power on your camera, and then tap **Next**.
The Device starts to search for cameras, and then the searched cameras are displayed.

If the camera cannot be found, there will be a prompt on the screen, and you can tap **Troubleshooting** to find the solution.

Step 3 Tap the camera you want to add, and is displayed at the upper right corner of the camera picture.

Figure 2-14 Searching results



Step 4 Tap **Next**, and then name the camera to be added.

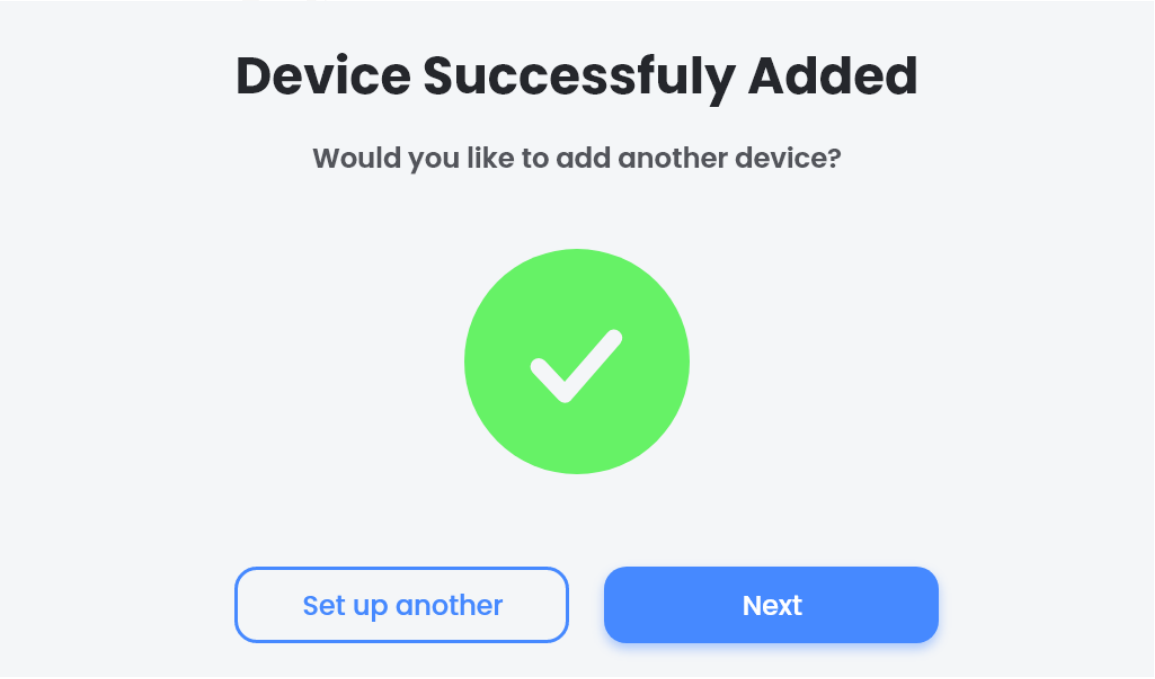
It is recommended to select one name listed below the name field, such as **Front Door**. If you use a custom name, the voice recognition accuracy might be affected.

Step 5 Tap **Save**, select **Indoor** or **Outdoor**, and then tap **Next**.

The **Device Successfully Added** interface is displayed.

Tap **Set up another** to add more devices.

Figure 2-15 Device successfully added



Step 6 Tap  , the gesture guidance video is displayed, and then the homepage is displayed.

The initialization is completed.

3 Basic Operations

3.1 Gestures

- Slide from the left border to the right to return to the previous page.
- Slide from the top to open the drop-down menu.
- Slide from the bottom to return to the homepage.

3.2 Drop-Down Menu

Figure 3-1 Drop-down menu

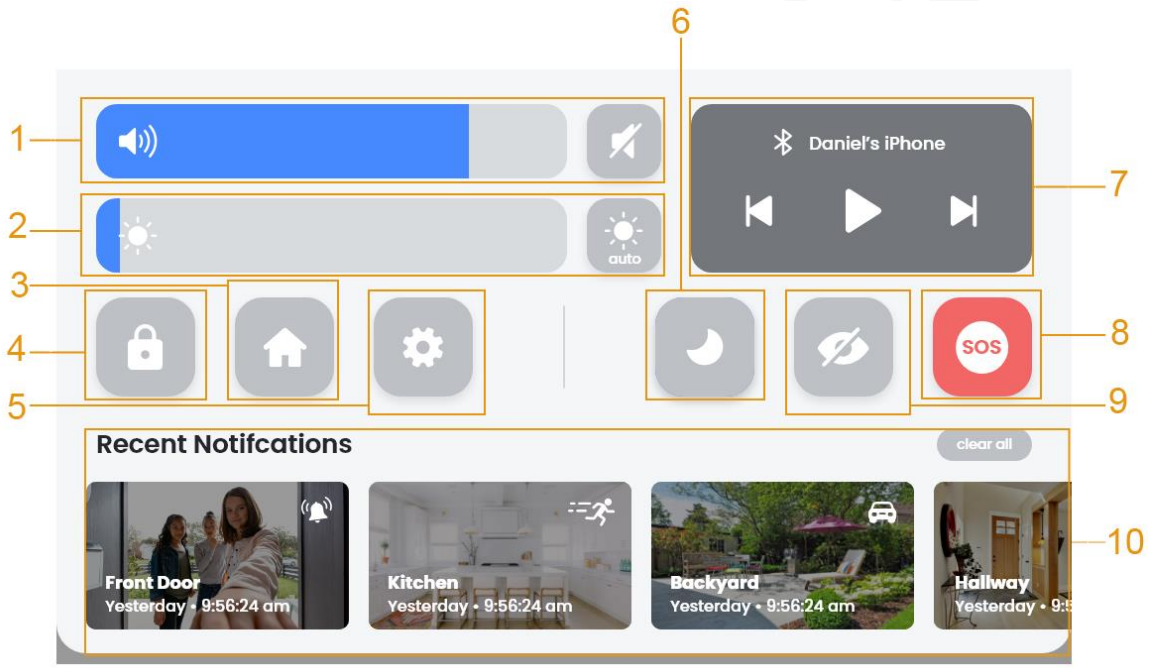


Table 3-1 Drop-down menu description

No.	Description
1	Drag to adjust the speaker volume. Tap to mute the Device.
2	Drag to adjust the brightness of the screen. Tap to adjust the brightness automatically.
3	Tap to go to the homepage.
4	Tap to go to the screen saver.
5	Tap to go to the device settings interface.
6	Tap to enable or disable DND mode. If the DND mode is enabled, no messages will be displayed in the notication section; no message sound will be played; the indicator light will not flash with color; no message will be displayed on the screensaver interface. And alarm information will only be saved in message center.

No.	Description
7	Control music play of the mobile phones connected through Bluetooth.
8	Panic button used to enable or disable all sounds and lights of the cameras connected. Long press the panic button for 5 seconds to enable all sounds and lights of the cameras. Tap again to disable them.
9	Tap to enable or disable global privacy mode of all cameras.
10	Display recent notifications, including device name, alarm time and alarm type. Tap one notification to see details; tap **clear all** to delete all notifications.

3.3 Login

When you restart the Device after initialization or have not operated the Device for a while, you need to unlock the Device. There are two unlocking methods: Face ID and passcode.

Face Unlock

You can use the face to unlock the Device.

- When the screen is dark, face recognition is not supported. Only after you press the Home button to wake up the Device and it is in locked status, the face recognition is supported to unlock the Device.
- After 5 wrong face inputs, the Device will be locked for 1 minutes. After that, the Device will be locked for 5 minutes for one wrong input. If there is no face input for 10 minutes, the wrong number will be cleared.
- If face unlock fails, the system goes to passcode unlock interface.

Passcode Unlock

You can enter the 6-digit passcode to unlock the Device.

- After 5 wrong passcode inputs, the Device will be locked for 5 minutes. After that, the Device will be locked for 5 minutes for one wrong input. If there is no input for 10 minutes, the wrong number will be cleared.
- Tap **Cancel** to go to face unlock if it has been set.

3.4 Homepage

Figure 3-2 Homepage (1)

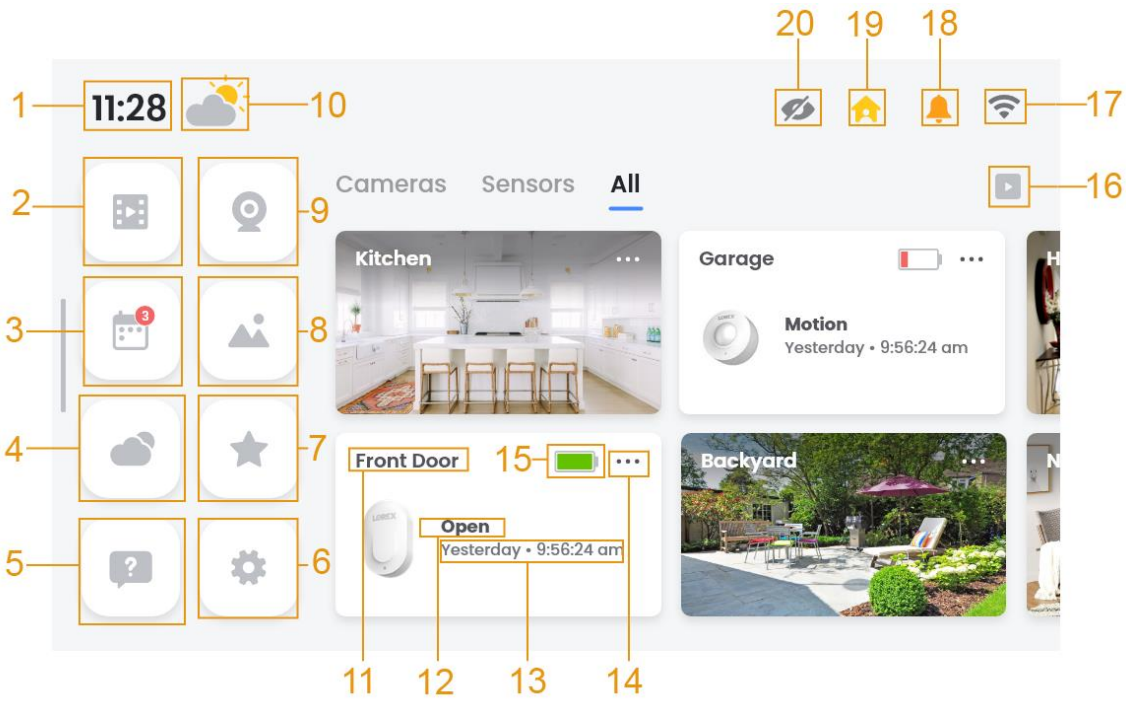


Table 3-2 Homepage description (1)

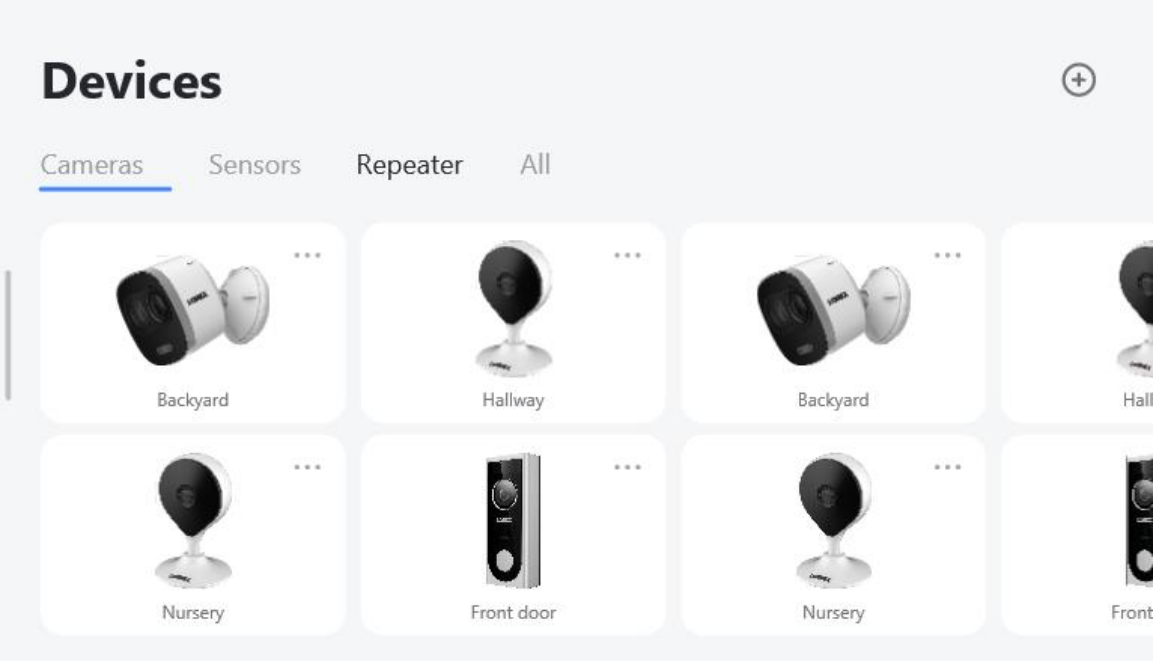
No.	Description
1	Display the current time.
2	Play back videos.
3	Events.
4	Weather settings.
5	Voice prompts.
6	Device settings.
7	Faviourites
8	Photos.
9	Device management.
10	Display the current weather.
11	Display the name of the corresponding device.
12	Display the notification type.
13	Display the push time of the last notification.
14	Set the corresponding device.
15	Display the battery level of the corresponding device.
16	Play live videos of all channels.
17	Display network signal status.
18	Enable or disable notifications for added devices; displays only when cameras have been added.
19	Arming settings; displays only when sensors have been added.

No.	Description
20	Enable or disable privacy mode for added devices; display only when cameras have been added.

3.4.1 Device Management

Tap on the homepage, and the **Devices** interface is displayed. The added devices are divided into cameras, repeaters, and sensors. And you can view all devices in the **All** tab.

Figure 3-3 Devices



3.4.1.2 Operations

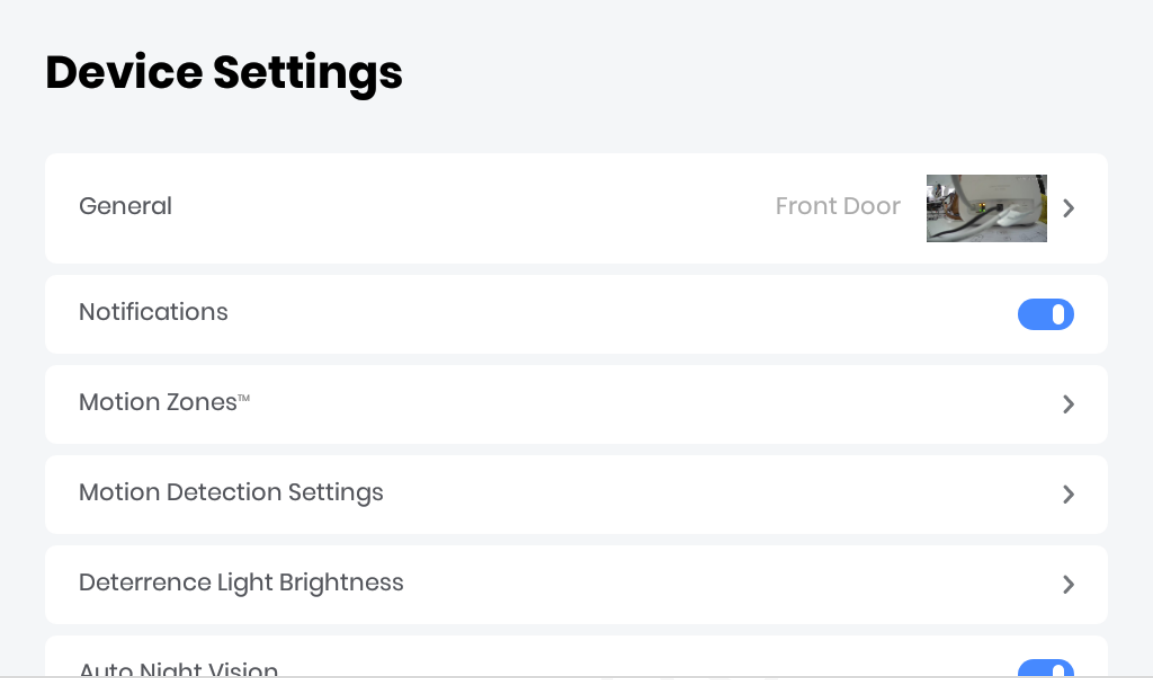
- Tap to add devices. For details, see "2.2.3 Adding Devices."
- Tap the device pictures to see the details, including live view.
- Tap and hold devices, and then drag them to adjust the order. After that, the devices will be displayed on the homepage in the adjusted order.
- Tap to go to the **Device Settings** interface.

3.4.1.3 Device Settings

On the **Device Settings** interface, you can set the device name, device location, notifications, motion detection, deterrence light brightness, privacy mode, audio recording, and so on. This section takes LNW16XF camera as an example.

The functions that can be set on this interface vary with the added devices, and the actual interface shall prevail.

Figure 3-4 Device settings



General Settings

- On the **General** interface, you can see the device photo, type, and ID, but cannot modify them.
- You can modify the name of the added device by tapping **Device Name**.

It is recommended to select one name listed below the name field, such as **Front Door**. If you use a custom name, the voice recognition accuracy might be affected.

- Tap **Device Location** to set the location to **Indoor** or **Outdoor**.

Notifications

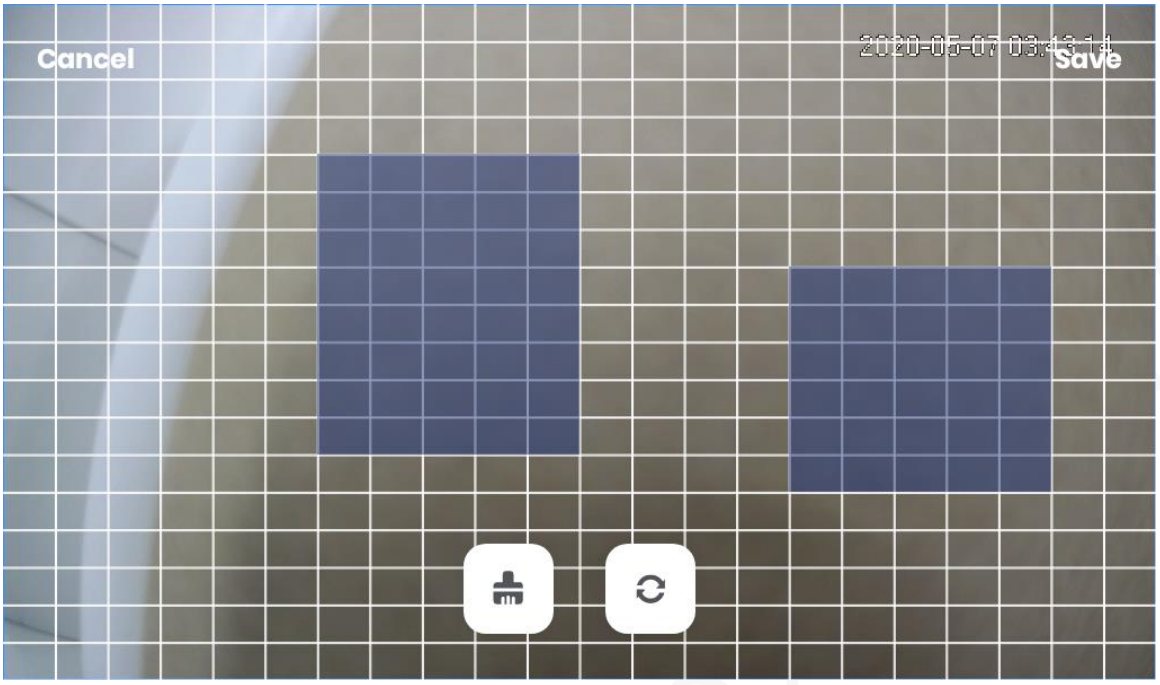
Tap to enable or disable notifications. The setting here applies to the homepage.

Motion Zones™

You can set motion zones to enable motion detection in the drawn areas. When motion is detected in these areas, alarm events will be triggered.

Step 1 Tap **Motion Zones™** on the **Device Settings** interface, and the motion zone setting interface is displayed.

Figure 3-5 Motion zone setting



Step 2 Tap and draw on the zone setting interface. The selected area will be highlighted in blue.

- Tap to clear all drawn areas.
- Tap to select the whole screen.

Step 3 Tap **Save**.

Motion Detection Settings

- **Motion Detection**: Tap to enable the function, and then when moving objects appear and move fast enough to reach the preset sensitivity value, alarms will be triggered. The function is enabled by default.
- **Motion Sensitivity**: Select the sensitivity of motion detection from 1 to 5. 3 is selected by default.
- **Activate Deterrence Light on Motion**: When motion is detected, the deterrence light of the camera is activated automatically if the function is enabled.

Deterrence Light Brightness

You can set the brightness of the deterrence light. The value ranges from 1 to 4 (selected by default).

Auto Night Vision

With auto night vision enabled, when in low-light conditions (for example, at night), the camera enters black-and-white mode to ensure the image is clear. If the function is disabled, the

camera will be in color mode all the time. In this case, when light is insufficient, the image might be blurry.

Privacy Mode

You can enable or disable privacy mode for the added camera. If this mode is enabled, notifications, video streaming and recording on this camera will be turned off.

Audio Recording

You can enable or disable audio recording when video is recorded for the camera. The function is enabled by default.

Camera Status LED

On the added camera, there is an indicator light. You can enable or disable it here.

Image Rotation

After the function is enabled, the camera stream will be rotated by 180°. If the camera is installed upside down, it is recommended to enable the function.

Firmware

Tap **Firmware** on **Device Settings** interface, and **Firmware Update** interface is displayed. You can manually check whether there is new version available. The Device automatically checks for new version when the added camera is restarted and connected to it.

When there is new version, the new version number and modified content will be displayed.

Do not power off the camera or disconnect the network during the upgrading process.

Restarting and Deleting Devices

Tap **Reboot Device** or **Remove Device** to restart or delete the camera.

3.4.1.4 Video Doorbell

After the video doorbell is connected, when someone presses the doorbell, there will be a ringtone prompt on the Device, and the screen automatically switches to the doorbell video. At the same time, a screenshot will be taken and saved to the **Visitor photos** album; an alarm information will be generated for you to manage the alarm video.

Figure 3-6 Doorbell ring

- Tap  to answer the doorbell and start video call. After answering the call, you can tap  to mute the call. In this case, the person who presses the doorbell cannot hear your voice.

After the person presses the doorbell, the information will also be pushed to the App (if you have connected the Device to the app). You can choose to answer it on the Device or on the app. If you have answered the call on one of them, there will be a prompt.

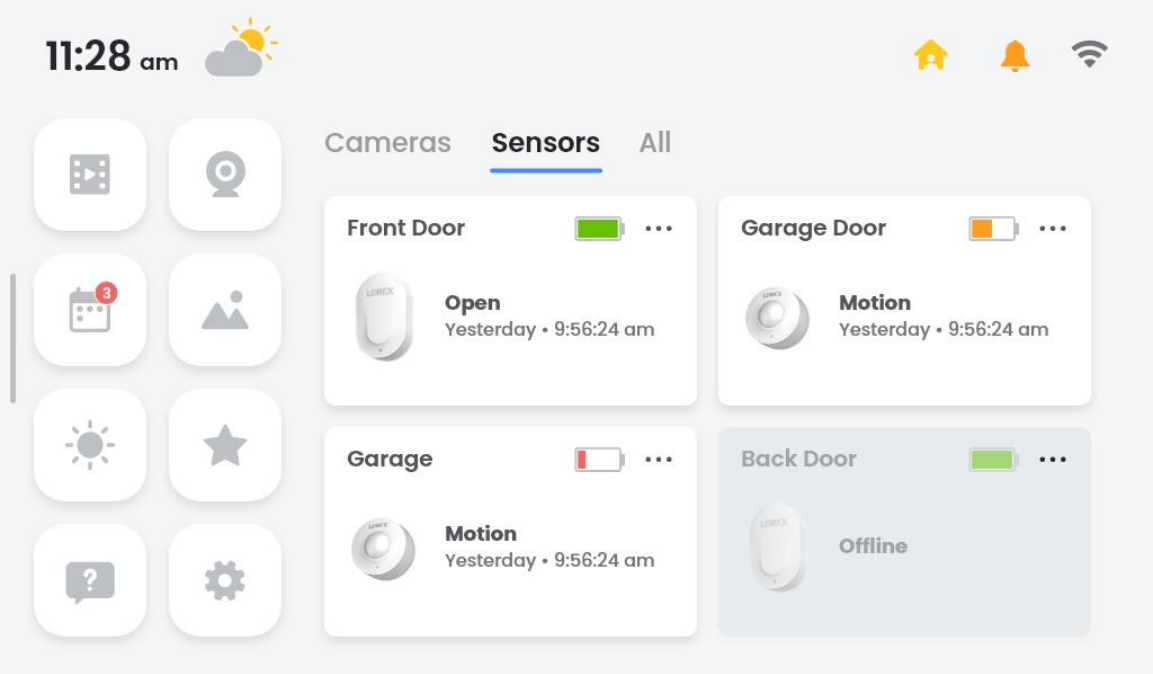
- Tap  to hang up the call.

3.4.1.5 Sensor

Tap the **Sensors** tab on the homepage, and the name of the sensor, the picture of sensor, battery level, sensor status (online or offline), and last alarm information (alarm type and alarm time) are displayed.

Up to 20 pieces of alarm information can be displayed on the **Sensors** interface.

Figure 3-7 Sensors



- When sensors are added alone, you can receive messages when certain events occur.
- When sensors are connected with cameras, you can view the linked video when an alarm is triggered.
- Three types of devices are supported: PIR sensors, door magnets, and flood detectors. Here are the supported alarm types for each type of device.
  - ◇ PIR sensor: Motion, and low battery.
  - ◇ Door magnets: Open, close, and low battery.
  - ◇ Flood detector: Inflow, and low battery.

Operations

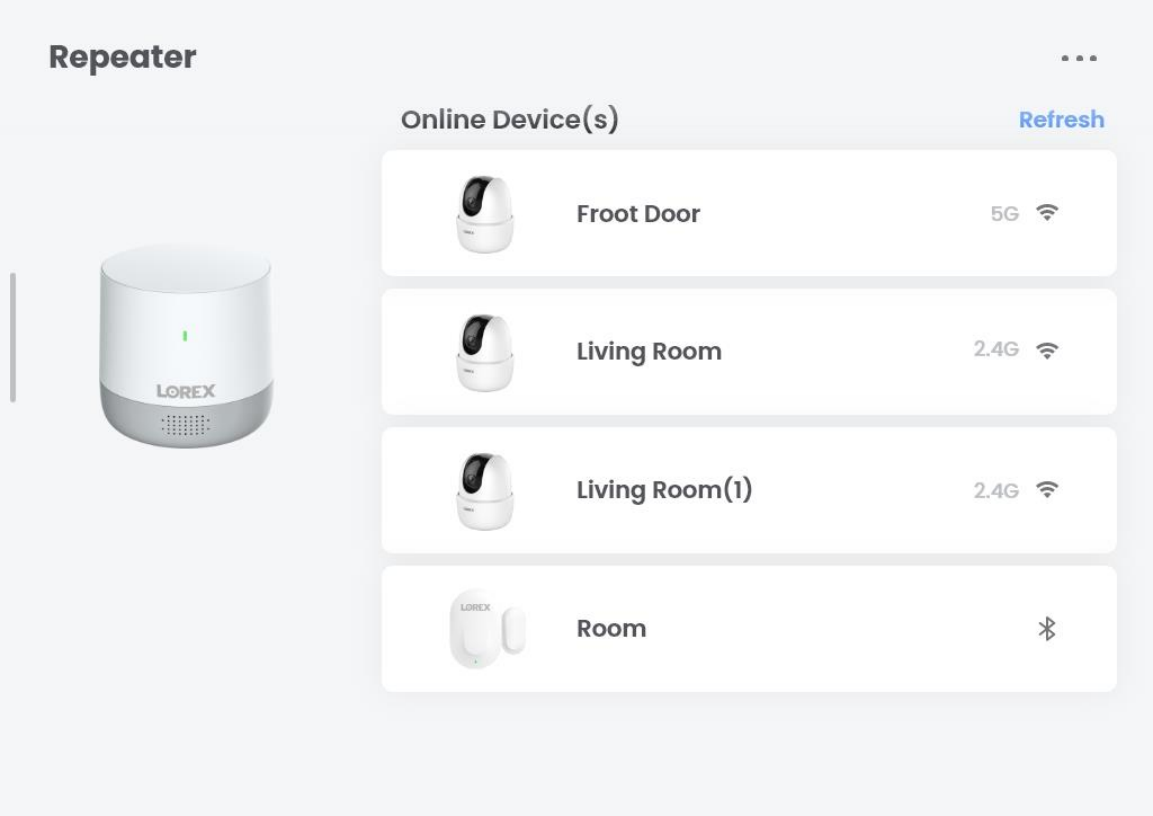
- Tap a sensor to view the alarm information.
- If the sensor has been connected to a camera, tap the alarm information to watch the linked video.
- If you tap the latest alarm information when the alarm recording is going on, there will be a prompt on the screen, and you will go to the live view interface.

3.4.1.6 Repeater

If the home area is more than 200 square meters, due to distance, wall, wireless interference and other factors, the Wi-Fi and Bluetooth coverage might be insufficient. In this case, the Repeater can be used for wireless signal relay. Moreover, the Repeater can also serves as a speaker of the Device. When there is an alarm or the doorbell rings, the Repeater will play the sound to inform you.

Tap the **Repeater** tab on the homepage, and the online devices that are connected to the Repeater are displayed on the **Repeater** interface.

Figure 3-8 Repeater



Operations

- Click **Refresh** to display the connected devices in real-time.
- Tap ··· at the upper right corner, and then you can view device information, do sound settings, LED setting, firmware upgrading, rebooting and device removing on the **Device Settings** interface.

3.4.2 Live View

You can tap an added device on the homepage to watch the live video. You can also select multiple or all devices to watch the live videos.

- If privacy mode has been enabled for the device, video stream cannot be pulled, and there will be a prompt on the interface.
- The live view interface varies with the added devices, and the actual interface shall prevail.

3.4.2.1 Single View

Tap the picture of an added device on the homepage, and the live view interface is displayed.

Figure 3-9 Live view

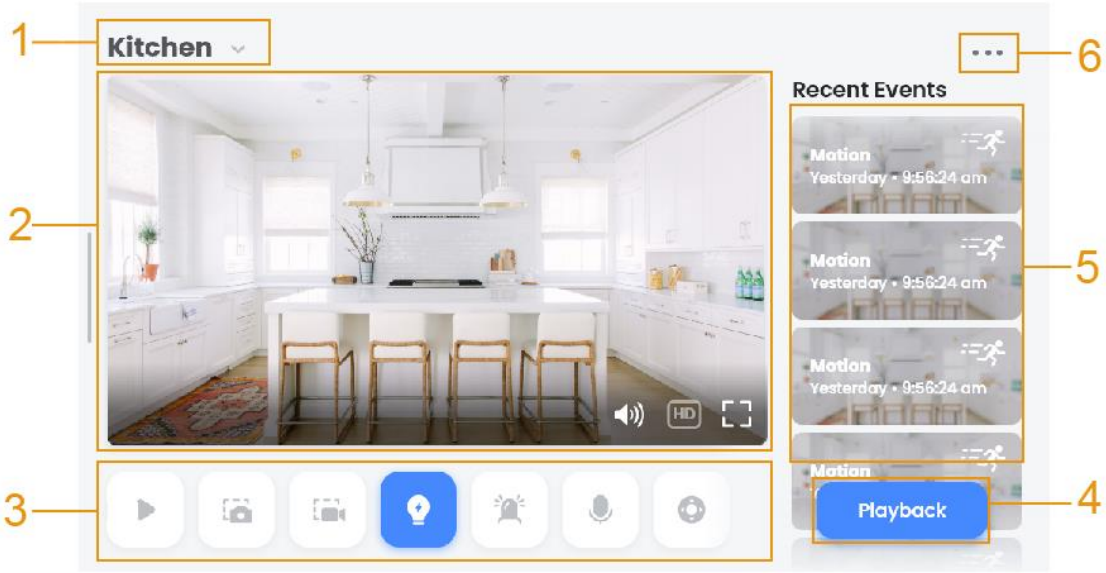


Table 3-3 Live view description

No.	Description	No.	Description
1	Device name	4	Playback
2	Video play	5	Push notifications
3	Functions	6	Device settings.

Device Name

Tap to switch device(s) or channel(s).

Video Play

- Tap to disable audio in the live view video.
- Tap to switch to SD mode. In HD mode, main stream is acquired; in SD mode, sub stream is acquired. HD is selected by default.
- Tap display the live view in full screen, and the buttons on the screen will be hidden after three seconds. Tap again on the full screen, and the buttons will be displayed again.
- Tap to exit full screen.

Functions

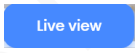
Table 3-4 Functions description

Button	Function
/	Tap to play/pause the live view video.

Button	Function
	Tap to capture a picture which will be displayed at the lower-left corner with the capturing sound, and disappeared after 3 minutes.
	Tap to capture a video. Tap again to stop capturing, and there will be a thumbnail of the video displayed at the lower-left corner. The minimum recording time is 3 seconds. When the video is being captured, returning to another interface, switching to another channel, switching between HD and SD mode, or playing/pausing the live view video will stop the recording.
	Tap to enable two-way audio with the device. Two-way audio conflicts with the talk function of the App, which means when the App and the Device acquire the same video stream, if audio is enabled for one of them, this function will be disabled automatically on another.
	For devices with light, you can tap the button to turn on the light. The light will be turned off automatically after 10 seconds. You can also tap the button to turn off it immediately.
	For devices supporting siren, you can tap the button to enable the siren. The siren will be turned off automatically after 10 seconds. You can also tap the button to turn off it immediately.
	For devices supporting PTZ, you can tap the button to control the PTZ.
	Tap the button to stop acquiring video streams.

Push Notifications and Playback

Up to 20 alarm videos of the recent events are displayed on the live view interface in reverse chronological order. You can see the alarm thumbnail, alarm type, and alarm time on the interface.

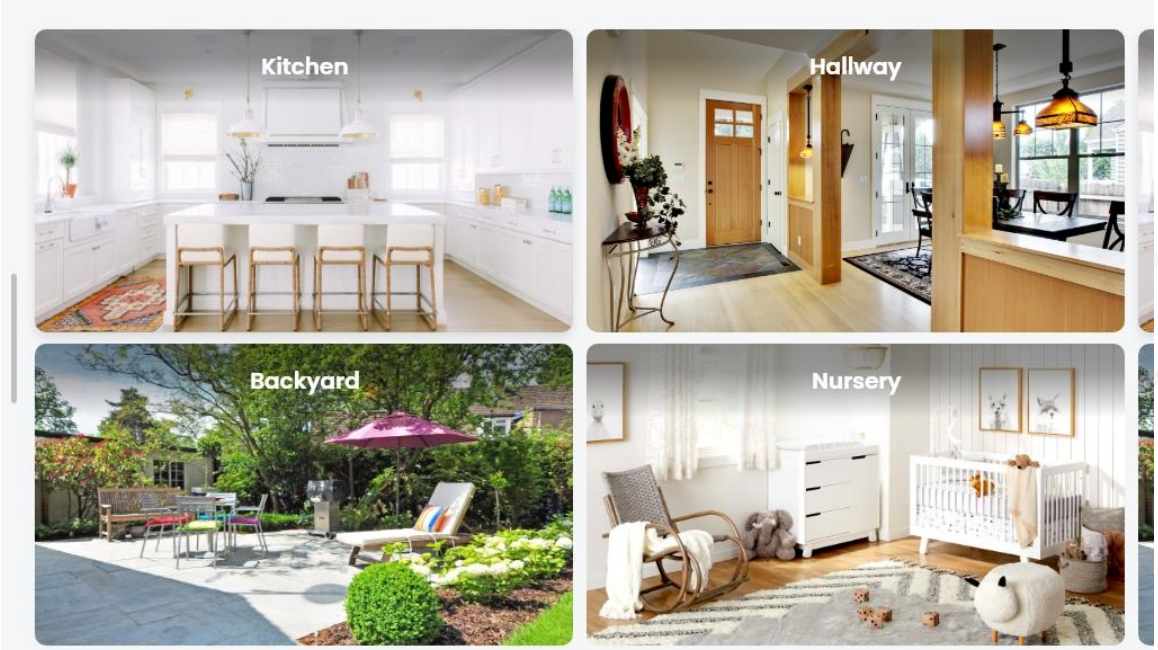
- Tap the alarm video to play back the video directly.
- Tap  to return to the live view interface.

Tap to go to the **Device Settings** interface. For more details, see "3.4.1.3 Device Settings."

3.4.2.2 Split View

Tap  on the homepage to play live videos of all channels. 4 small windows will be displayed on one screen. You can swipe to left or right to switch to other channels if there are more than 4 channels.

Figure 3-10 Split view



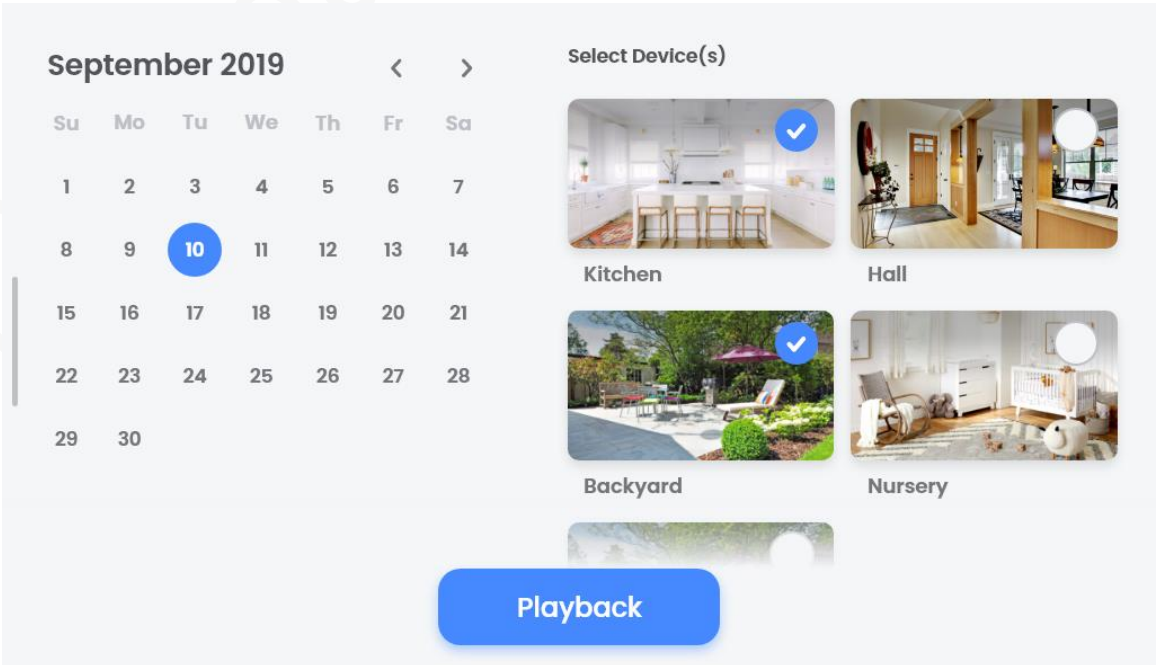
Double-tap one channel to display the window in full screen. And then you can use capturing, voice talk, and other functions.

3.4.3 Playback

You can play back the recordings of the Device, and quickly search for the videos when certain events occur.

Step 1 Tap on the homepage, and the playback interface is displayed.

Figure 3-11 Playback interface



Step 2 Select the date and the device, and then tap Playback.

The playback video of all selected devices will be displayed.

Up to 4 devices can be selected at the same time.

Step 3 Double-tap to view the playback of a single device.

For buttons description, see Table 3-5.

Figure 3-12 Playback of a device

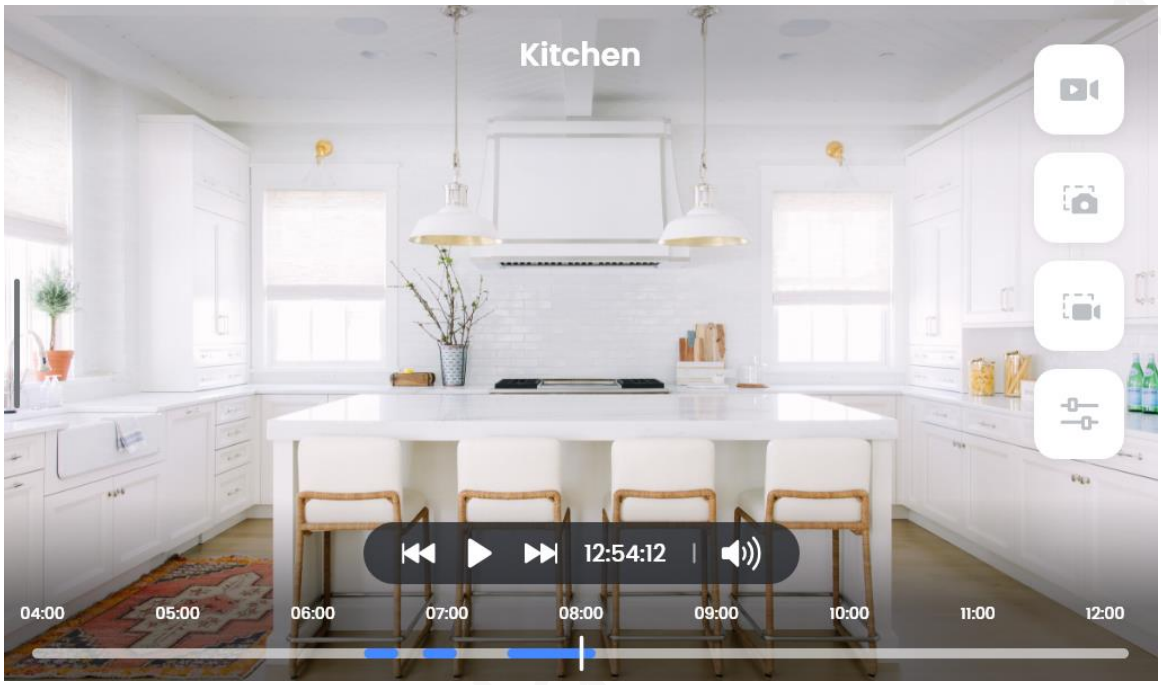


Table 3-5 Buttons description

Button	Description
	Tap to play the video.
,	Tap to slow-forward or fast-forward the video play.
	Tap to mute the video.
	Tap to filter the playback video. You can filter by date or event type.
	Drag on the progress bar to play back the video from a certain time point.
	Tap to go to the live view interface.
	Tap to take a snapshot of the current view.
	Tap to capture a recording.

- If no operation is performed on the playback interface for 3 seconds, all buttons will be hidden.

- Pinch your fingers on the playback screen to zoom in or out.

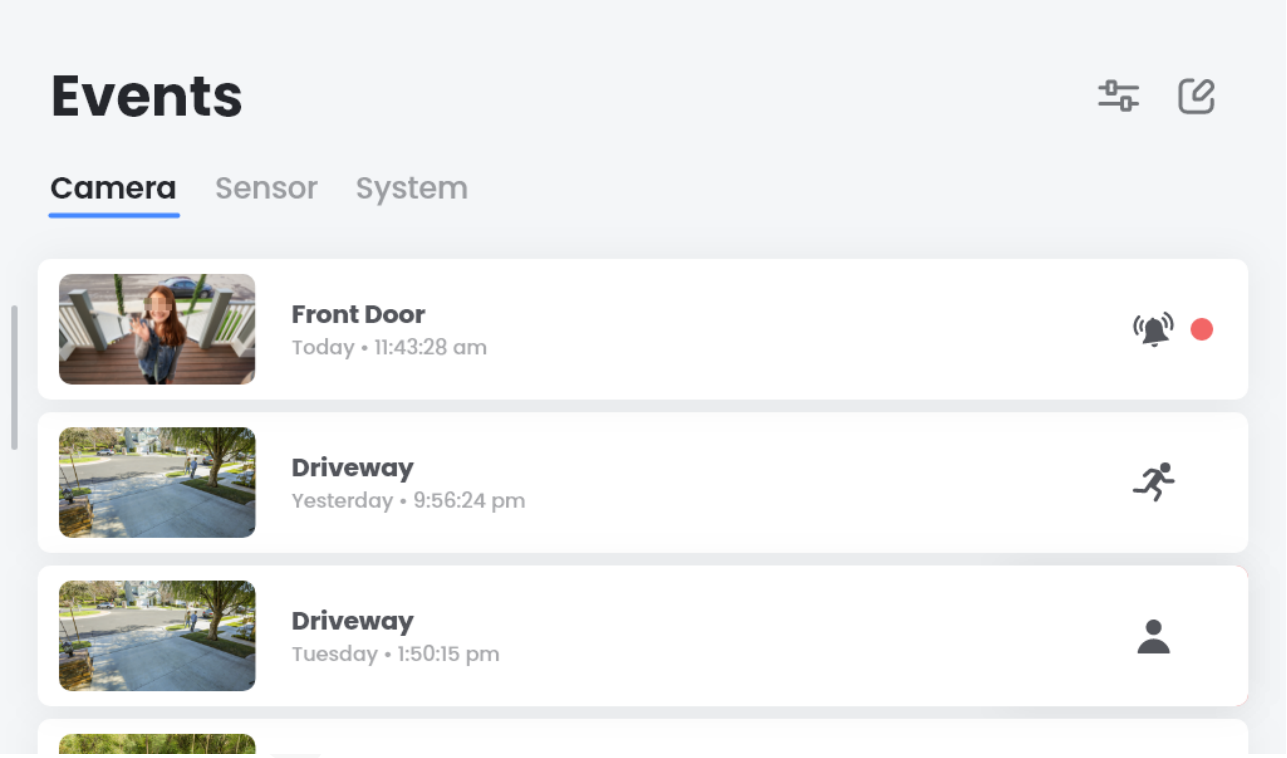
3.4.4 Message Center

You can view the alarm information of the added devices and the Device to know the running status of the whole system.

Procedure

Step 1 Tap on the homepage, and the **Events** interface is displayed.

Figure 3-13 Events



Step 2 Tap a piece of alarm information to view it.

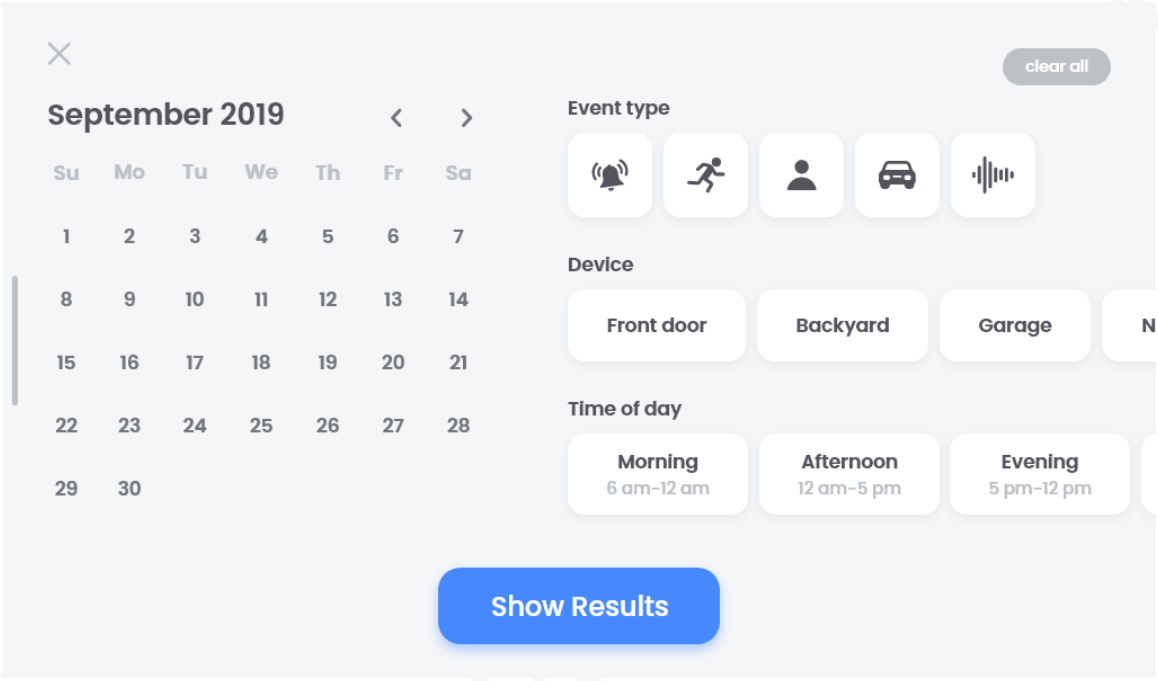
There are three types of alarm information: **Camera**, **Sensor**, and **System**.

- For each alarm information, device name, alarm time, and alarm screenshot will be displayed. If there is a red dot on the information, it means the information have not been read.
- For cameras and doorbells, when you tap the alarm information, a captured video will be displayed.
- For sensors, if you have connected them to cameras, tap the alarm information to play back the linked video. If you haven not connected them to cameras, the picture of the alarm status will be displayed.
- The alarm information is displayed in reverse chronological order, which means the latest event is displayed at the top of the list.

Operations

- Tap  to mark one piece of or all alarm information as read or delete them.
- Tap  to filter the alarm information.

Figure 3-14 Filter alarm information



  - ◇ You can search for the alarm information by event type, device or time of day.
  - ◇ You can select one or more filtering condition. After you select a filtering condition, it turns blue. Tap it again to cancel the selection. You can tap  to clear all selections.
- Swipe left on a message, and then tap **Delete** to delete it.

If you want to delete multiple messages at the same time, tap  and follow the onscreen instructions.

Supported Event Types

The supported event types vary with devices, and the actual product shall prevail.

- For cameras, motion, person, vehicle, sound, and call are supported.
- For sensors:
  - ◇ The event types of door magnets include open, close, low battery (lower than 20%), and so on. If such devices are armed, event types will be generated every time the door is opened or closed.
  - ◇ The event types of flood detectors include inflow, low battery (lower than 20%), and so on. Such devices are armed all the time.

◇ The event types of PIR include motion and low battery (lower than 20%).

- For system, abnormal network (disconnected and connected), abnormal storage (SSD abnormal and SD card full), power on record, and other events are supported.

Figure 3-15 Camera events

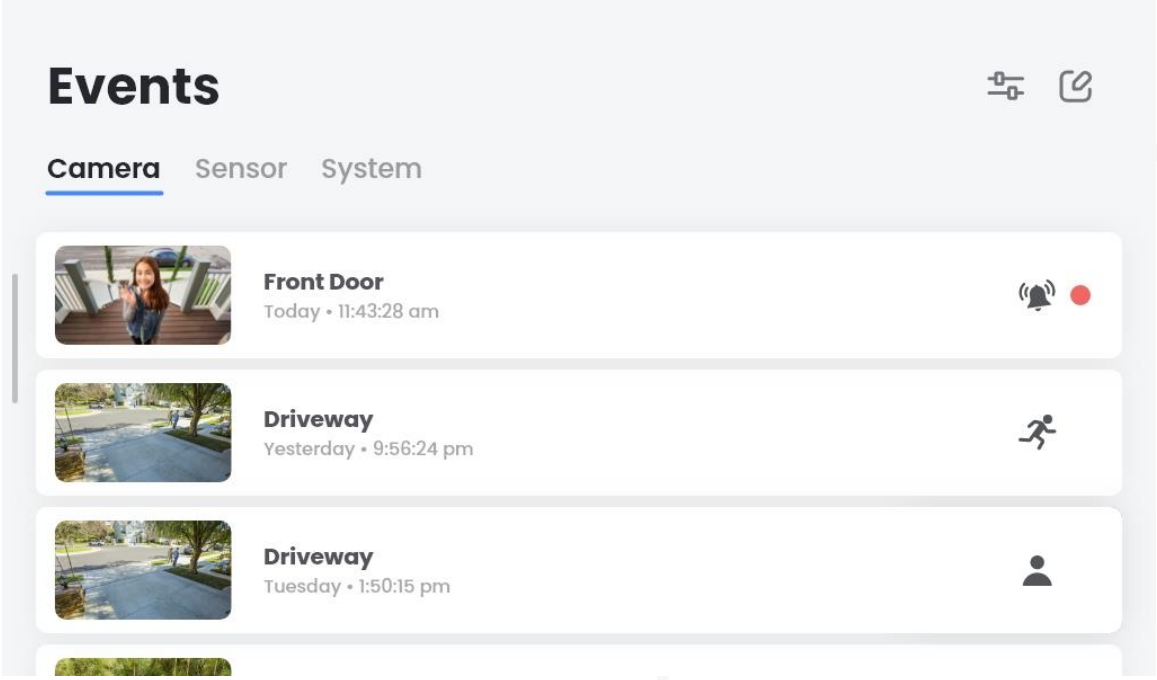


Figure 3-16 Sensor events

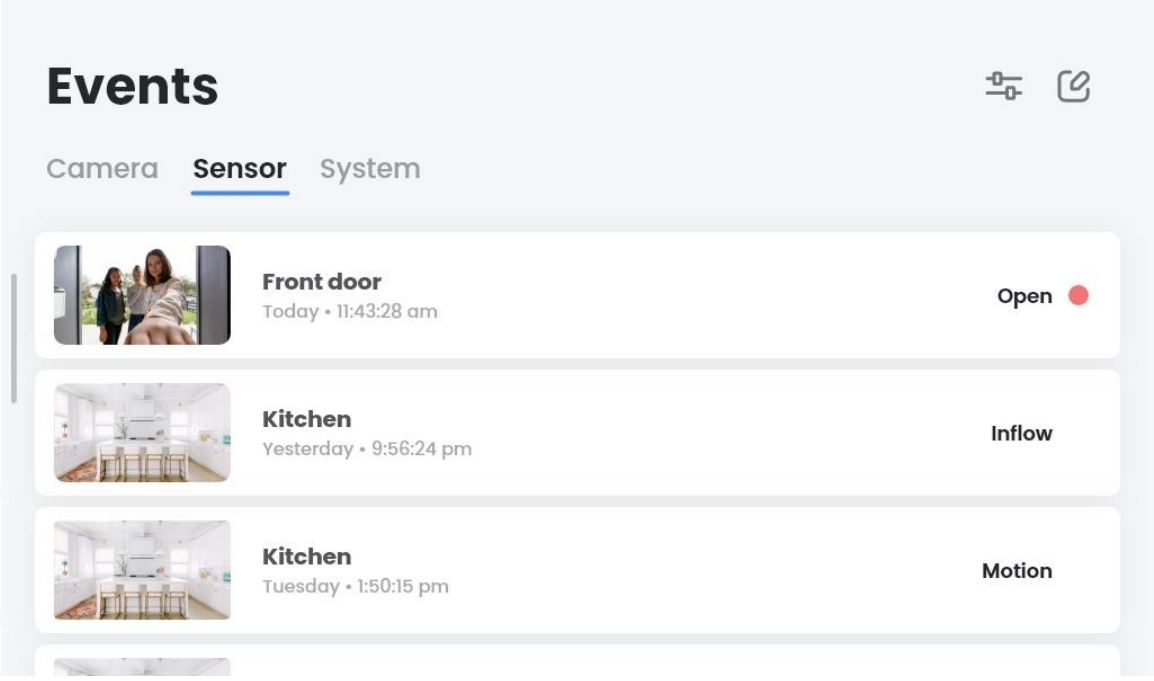
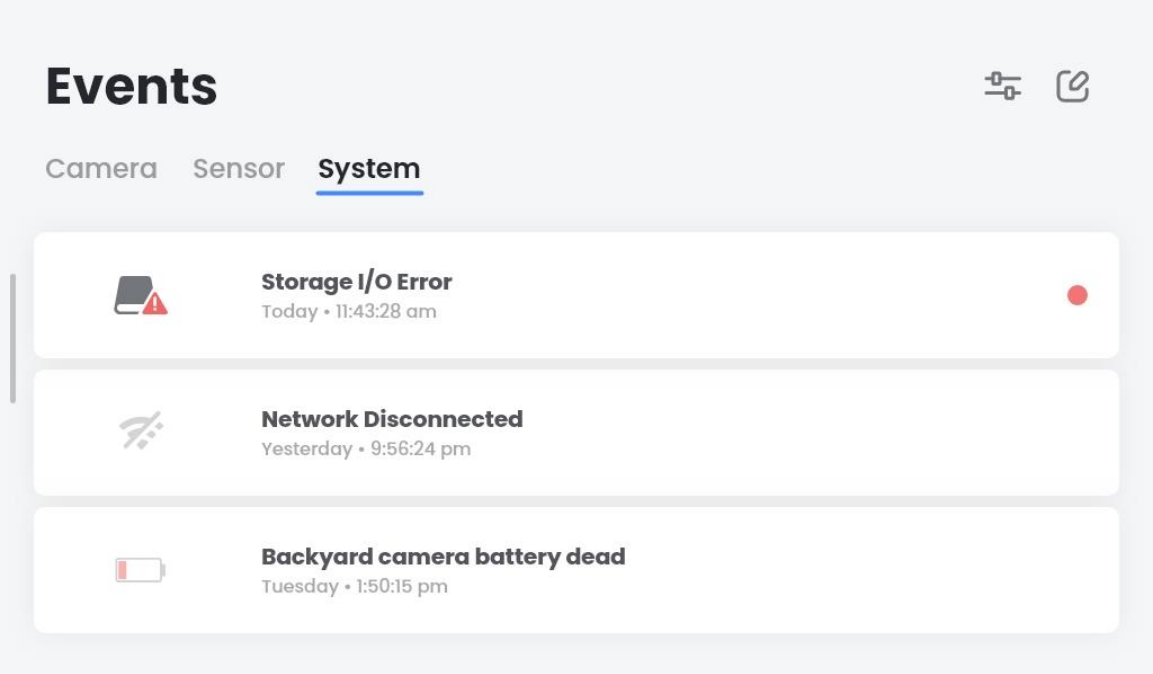


Figure 3-17 System events



3.4.5 Photos

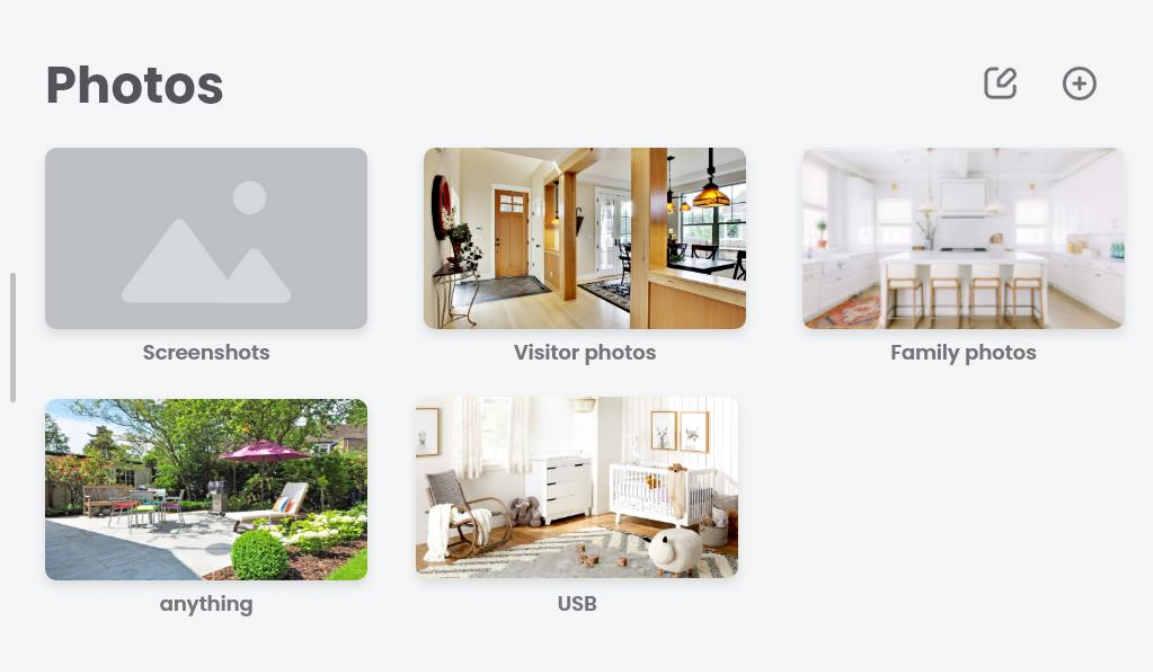
You can save the needed videos and pictures in standard format on the Device, and export these files through USB cable. You can also import the family album to the Device to set the photos as screen savers.

3.4.5.1 Albums

Creating New Albums

Step 1 Tap on the homepage, and the **Photos** interface is displayed.

Figure 3-18 Photos



There are three default albums: **Screenshots**, **Visitor photos**, and **Family photos**. These albums cannot be deleted or renamed.

- Screenshots and captured videos in live view and playback are saved in **Screenshots** album.
- Screenshots taken when the doorbell is pressed are saved in **Visitor photos** album.
- **Family photos** album can be used to store family photos, and there are five photos provided by default for screen saver.
  - ◇ Supported video formats include mp4, mkv, MPEG, and AVI. The captured videos in live view and playback are in mp4 format.
  - ◇ Supported picture formats include jpg, png, bmp, and jpeg. The screenshots taken in live view and playback, and when the doorbell is pressed are in jpg format.

Step 2 Tap , enter the album name, and then tap **Save**.

The new album is created.

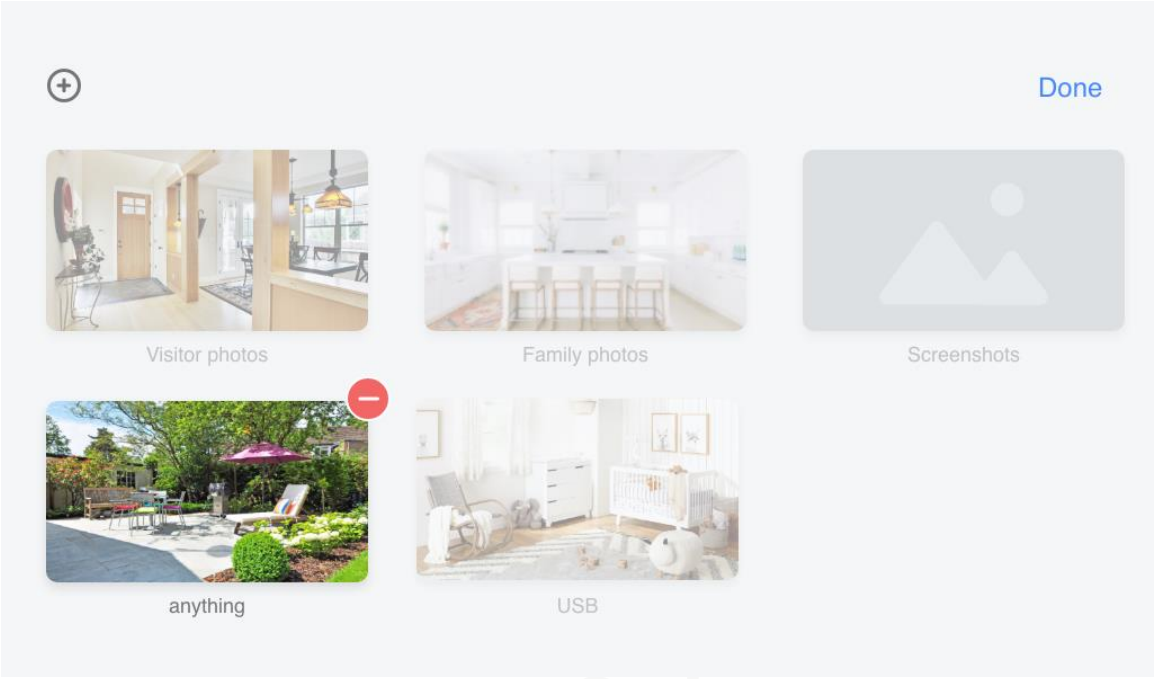
The album name length is limited to 32 English characters, and for special characters, only underline is allowed.

Editing Albums

Step 1 On the **Photos** interface, tap to enter the edit mode.

You can delete the albums except the three default albums as needed.

Figure 3-19 Delete albums



Step 2 Tap **Done** to exit the edit mode.

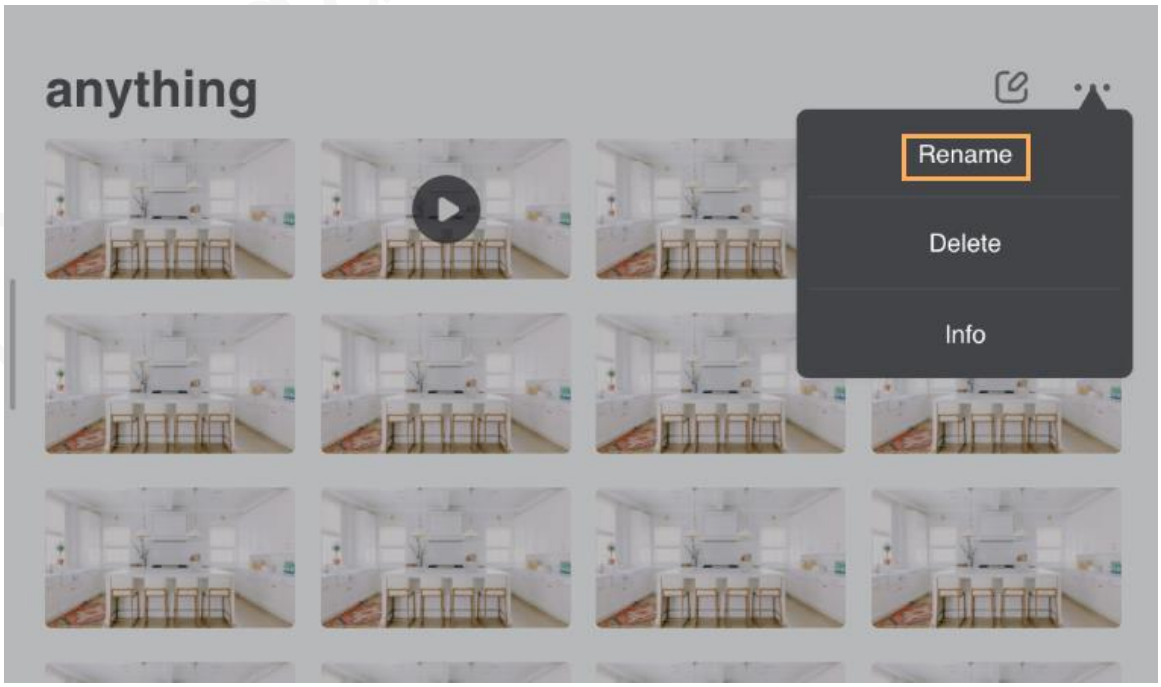
On the editing interface, you can also tap to create new albums.

Renaming Albums

Step 1 Tap an album, and the album details interface is displayed.

Step 2 Tap , and then tap **Rename**.

Figure 3-20 Rename albums



Step 3 Enter the new name, and then tap **Save**.

The new name comes into effect.

3.4.5.2 Files

Viewing Files

Tap an album, and then you can view the pictures or videos in it.

- For pictures, you can view them in a list or in full screen.
- For videos, you can play and pause the video, drag the progress bar to play the video from a certain point, and mute the video play.

Exporting Files

Step 1 Tap an album to enter the details interface.

Step 2 Tap , select the files you want to export, and then tap **Export**.

Tap **Select All** if you want to export all files.

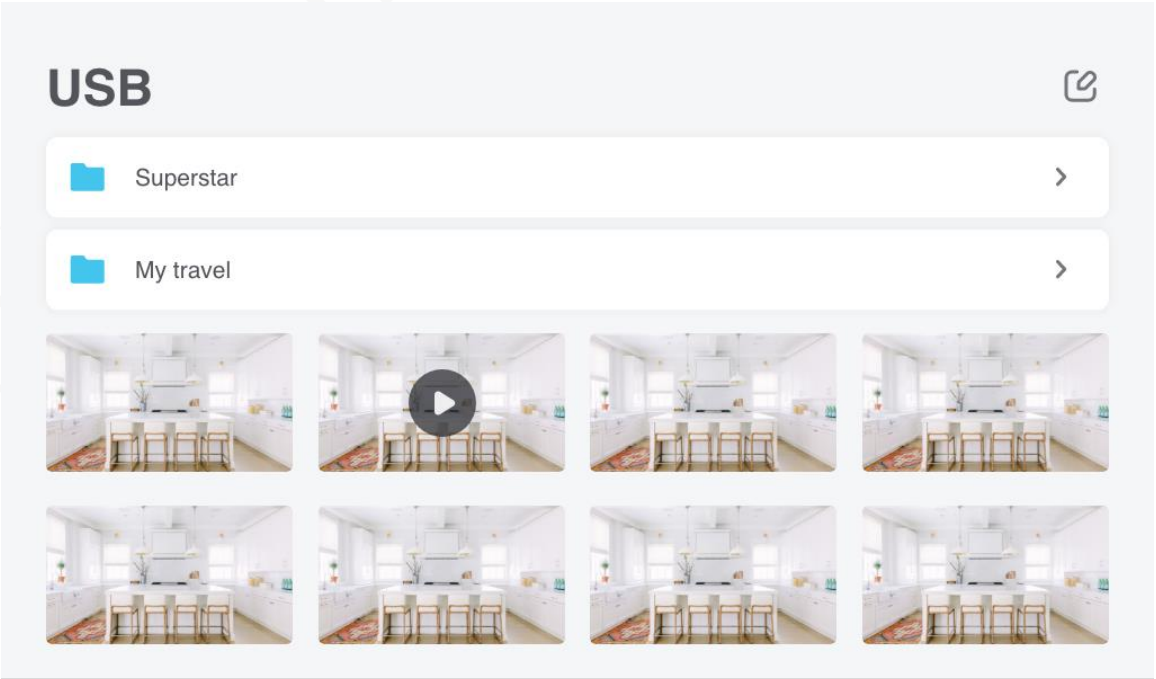
Importing Files

Step 1 Insert the USB flash drive.

The folders and files will be displayed.

You can view or delete the files in the USB flash drive.

Figure 3-21 USB



Step 2 Select the files you want to import to the Device, tap **Import**, select the albums you want to import the files to, and then tap **Import** again.

The progress bar will be displayed. An onscreen prompt is displayed when the import is completed.

3.4.6 Favourites

The function serves as the shortcut for **Snapshots and Recordings** albums in **Photos** section.

You can tap to view the captured pictures and videos quickly.

3.4.7 Voice Command

The Device supports voice recognition, and you can wake it up with voice command.

Tap on the homepage, and the five categories of the supported voice commands are displayed.

Figure 3-22 Voice commands

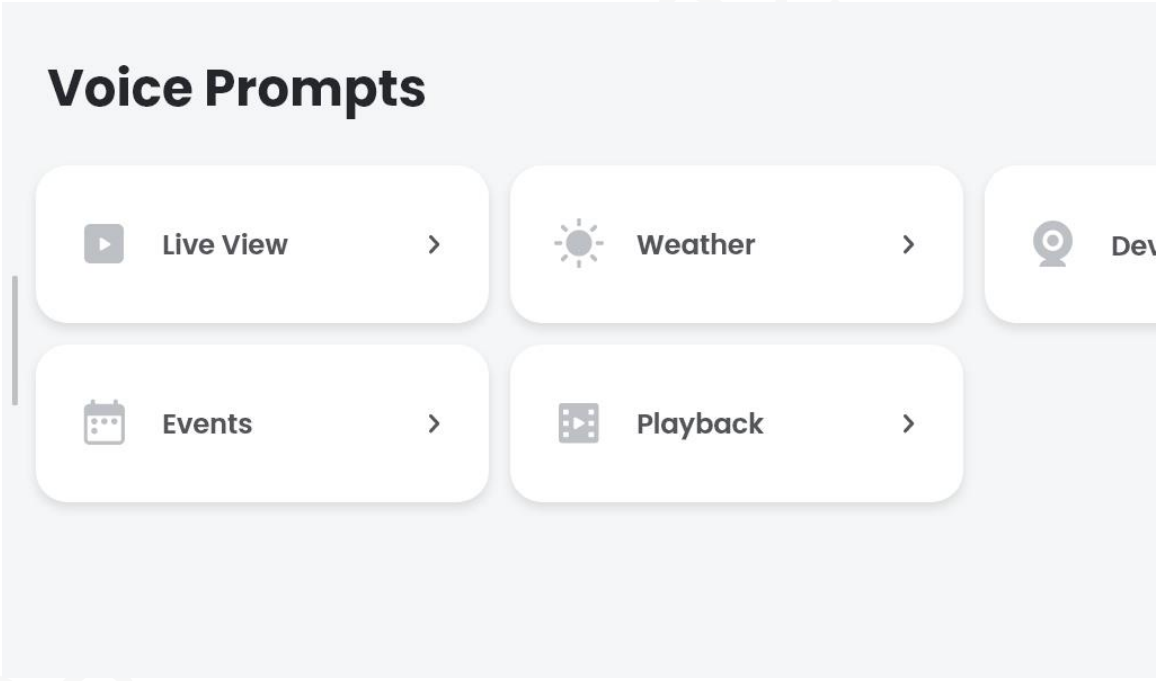


Table 3-6 Supported voice commands

Category	Examples of Supported Voice Commands
Live View	Imou, show me the Basement camera. Imou, show men all indoor cameras.
Weather	Imou, show me what's the weather right now. Imou, show me what's the temperature is it outside now.
Device Settings	Imou, turn on panic mode on all cameras. Imou, turn privacy mode on for living room.
Events	Imou, play motion recording of the Basement camera from 3pm onwards. Imou, show me all people at the camera yesterday.

Category	Examples of Supported Voice Commands
Playback	Imou, go slower. Imou, maximum volume.

3.4.8 Weather

Internet Connected

The Device can obtain the weather of the current place based on IP address. If connected to network, the Device obtains weather information of five days (starting from today) every three hours, and displays it on the homepage and screen saver.

- Tap on the homepage, and the weather interface is displayed. You can see the date, weather, and temperature.
- Tap the city name at the upper left corner to search for the city for viewing the corresponding weather information.
- Tap °C or °F to see the temperature displayed in the corresponding unit.

Figure 3-23 Weather with Internet connected

Internet Disconnected

If Internet is not connected, the following interface will be displayed. You can tap **Refresh** or **Network Settings** to fix the issue.

Figure 3-24 Weather with Internet disconnected (1)

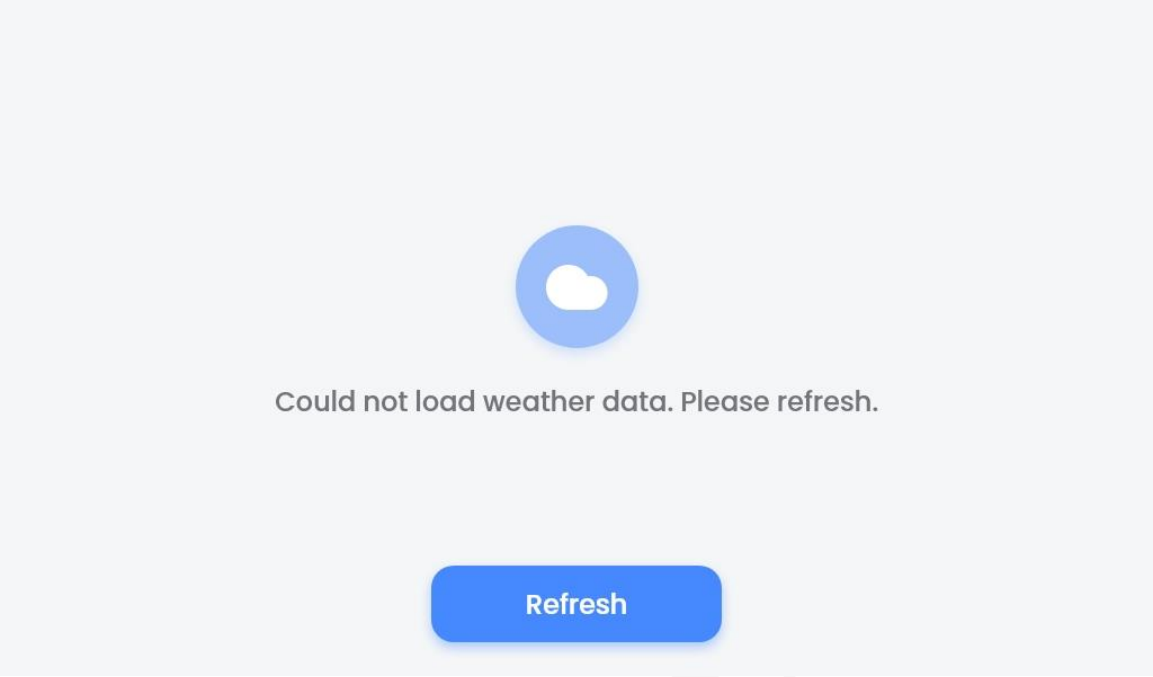
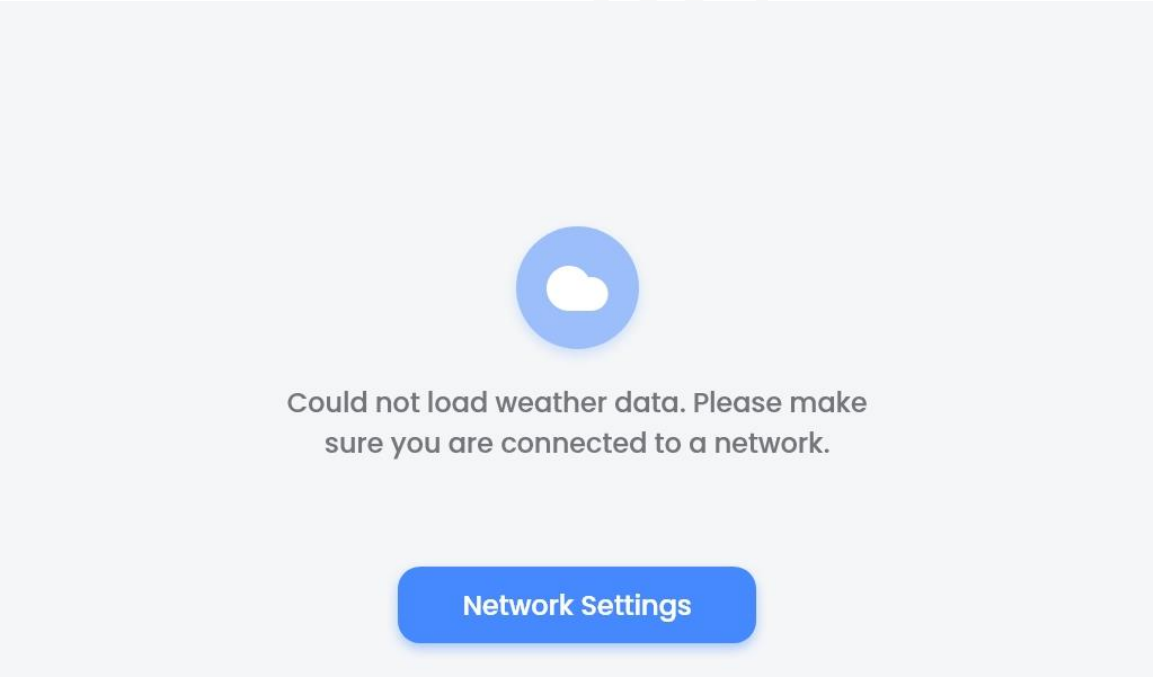


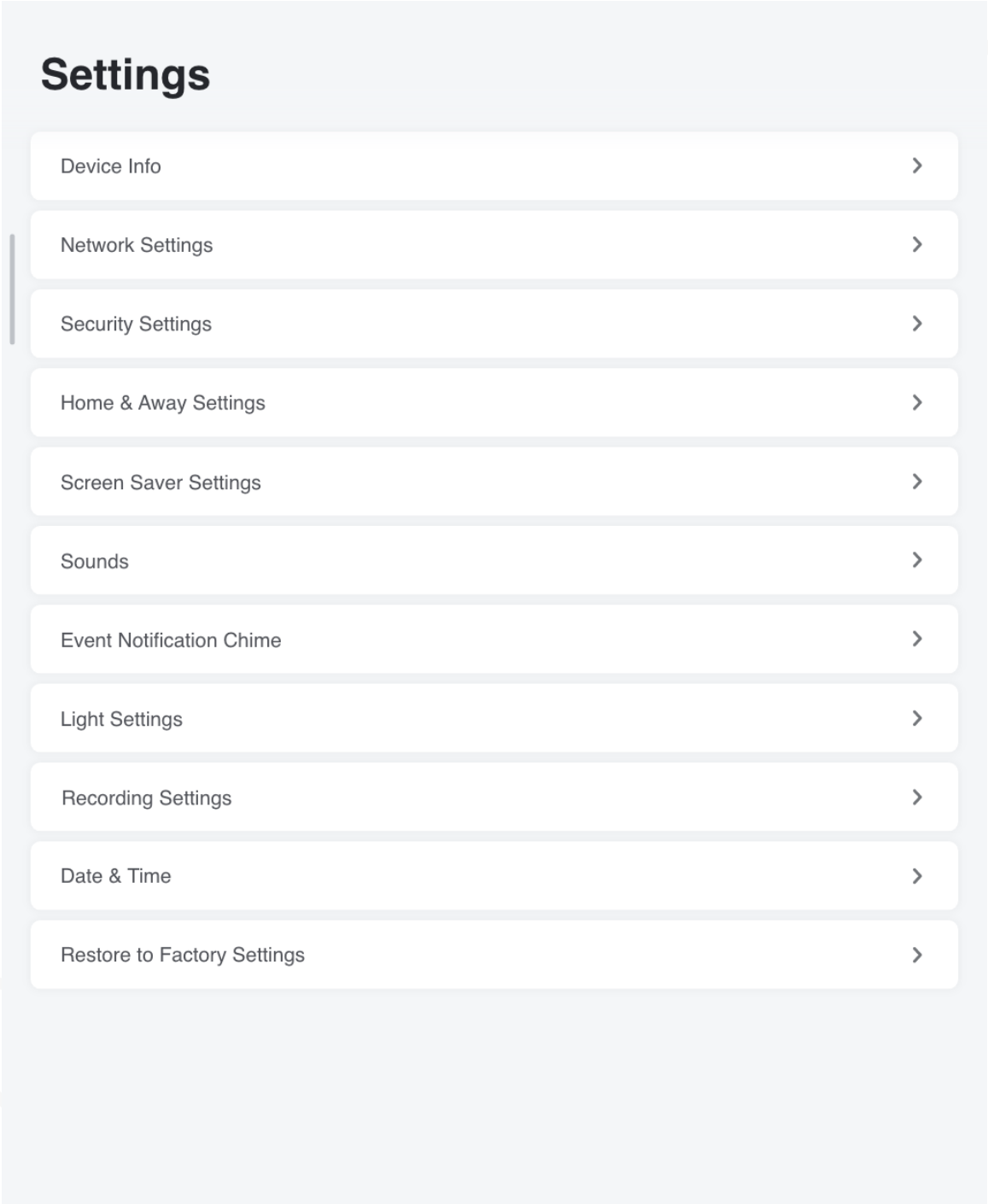
Figure 3-25 Weather with Internet disconnected (2)



4 System Settings

Tap on the homepage, and the **Settings** interface is displayed.

Figure 4-1 Settings

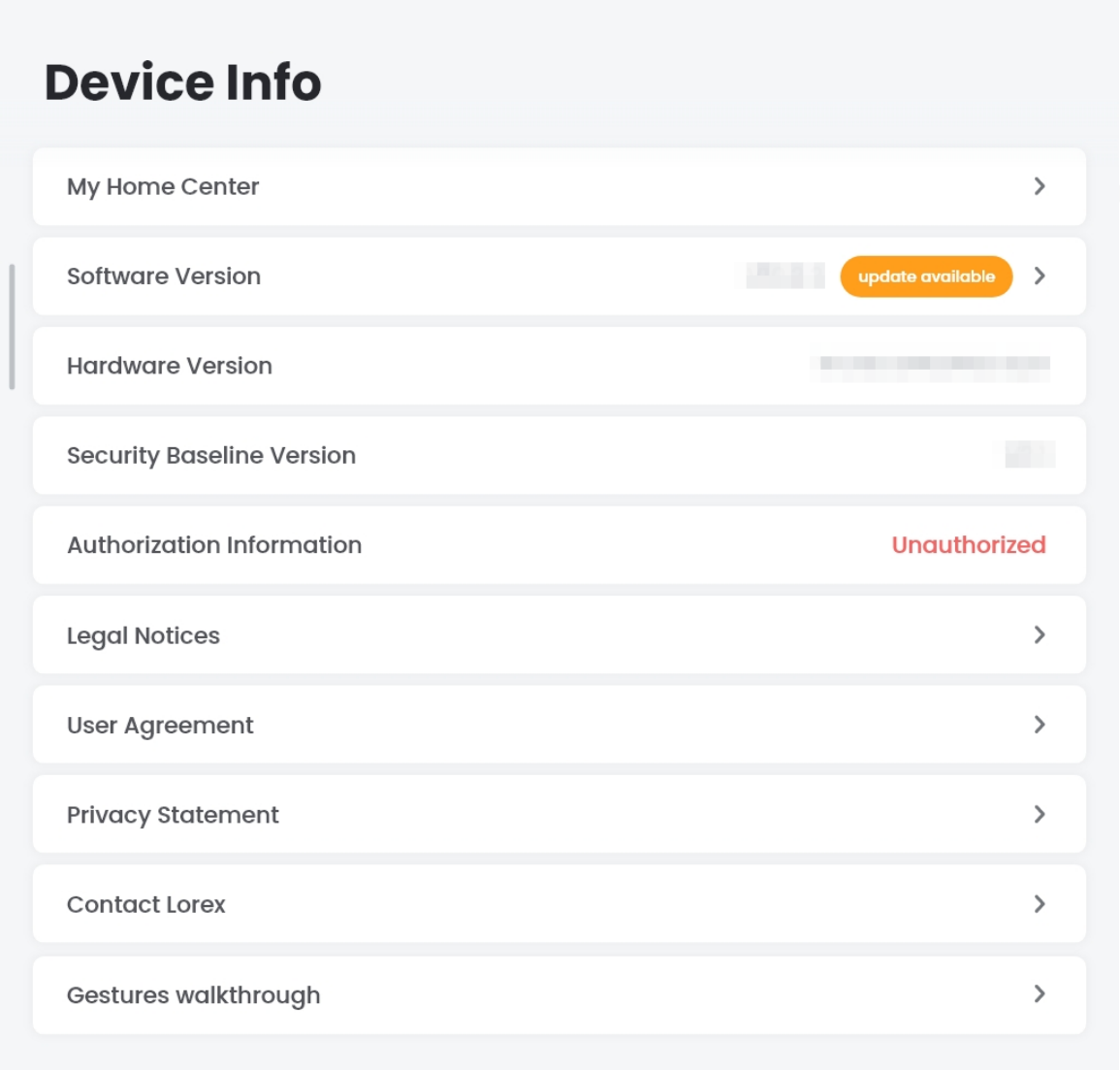


4.1 Device Information

Tap **Device Info** on the **Settings** interface, and you can see the device name, software version, hardware version, security baseline version, authorization information, legal notices, user

agreement, privacy statement, contact information of the customer service, and the gestures walkthrough.

Figure 4-2 Device info



Device Name

Tap the device name (for example, My Home Center in Figure 4-2), and you can see the device name, device type, and device ID.

You can tap the device name to modify it. The maximum length of the name is 32 characters.

Software Version

If there is a new software version available, there will be a prompt on the screen. Here are the upgrading steps.

Step 1 Tap **Software Version**, and the **Software Version** interface is displayed.

Step 2 Tap **Update now**, and the **Device Update** interface is displayed.

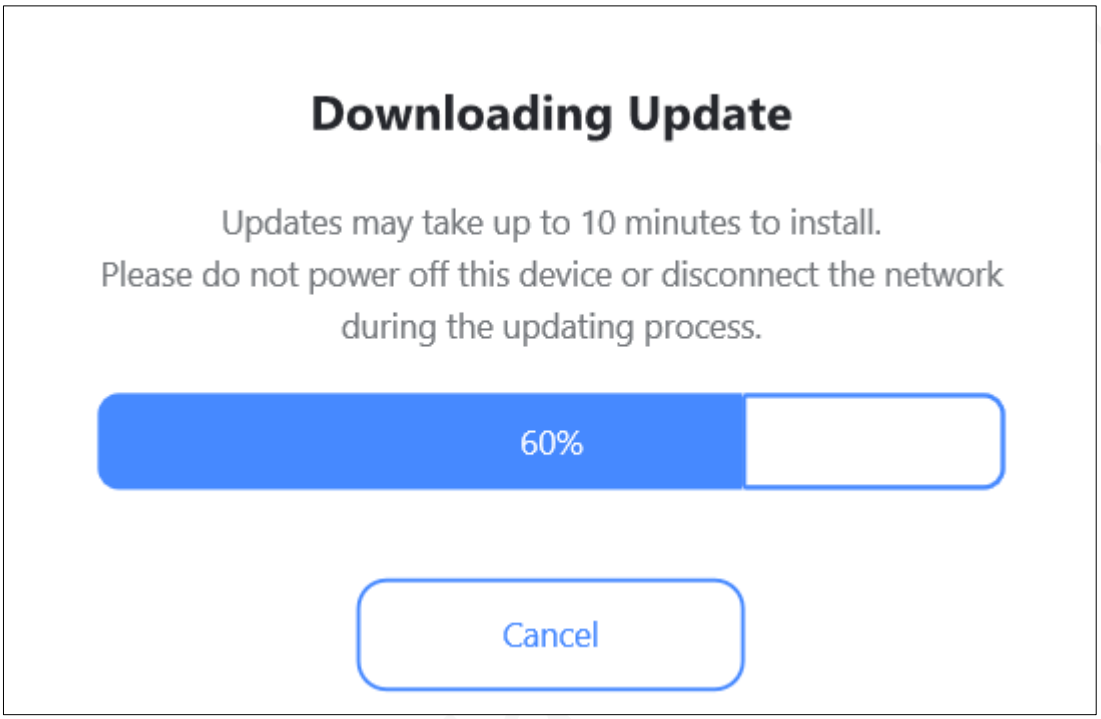
Do not disconnect the power or network during the upgrade process. It will take up to 10 minutes to complete the upgrade.

Step 3 Tap **Update**, and there will be another prompt to let you know the upgrade will start after 5 seconds.

You still can cancel the upgrade at this time.

Step 4 After 5 seconds, the upgrade progress bar will be displayed.

Figure 4-3 Progress bar



Step 5 After the installation package is downloaded, the system will check it.

- If the verification fails, there will be a failure prompt, and the downloaded file will be cleared.
- If the verification is successful, there will be a prompt to remind you not disconnect the power or network. After the installing is completed, the Device will be restarted automatically.

You can also upgrade the software through TF card. After you insert the TF card, the system will detect if there is a new version. If new version is available, tap to start the upgrade.

Authorization Information

The current authorization status of intelligent algorithm is displayed. If authorized, **Authorized** is displayed in grey; if not authorized, **Unauthorized** is displayed in red.

Gestures Walkthrough

Tap **Gestures Walkthrough** on the **Device Info** interface, and a short video is displayed, demonstrating how to operate the Device through gestures, which is the same as the guide after device initialization.

4.2 Network Settings

You can configure Wi-Fi and Wired network. Wi-Fi and wired network cannot be used at the same time. When you select Wi-Fi, the wired network will be disabled automatically, and vice versa.

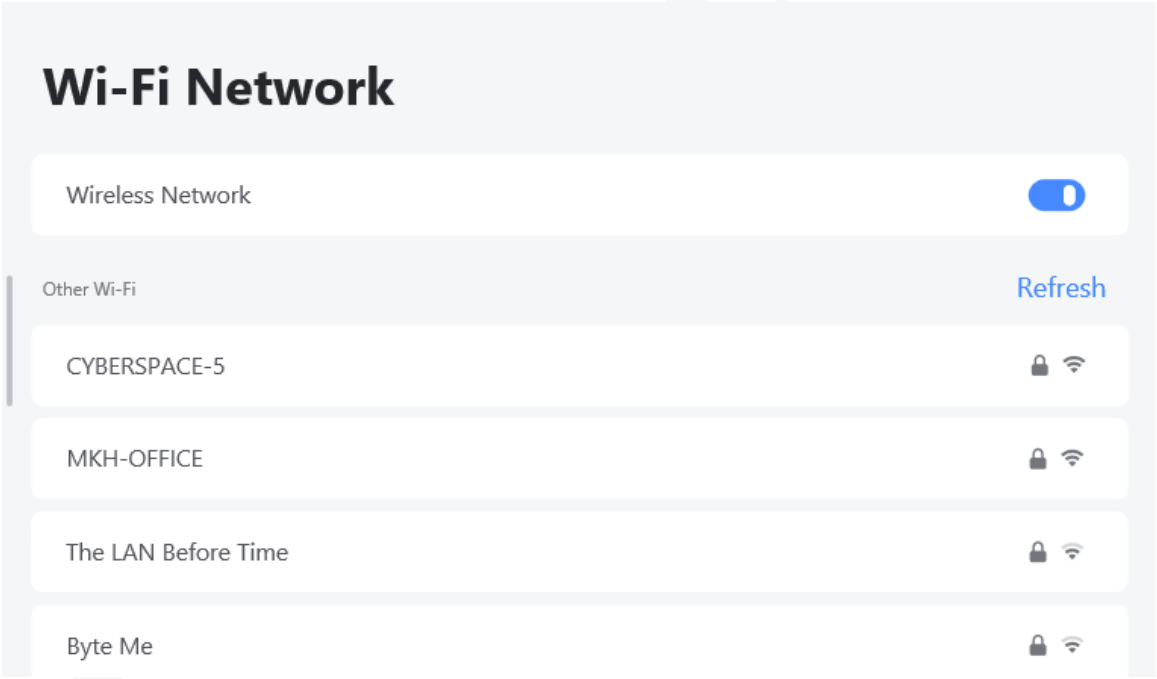
4.2.1 Configuring Wi-Fi

Step 1 Tap **Network Settings** on the **Settings** interface.
The **Network Settings** interface is displayed.

Step 2 Tap **Wi-Fi Network**, and then enable **Wireless Network**.
The available Wi-Fi hotspots are displayed.

If wired network has been connected, there will be prompt on the screen. Tap **Continue**.

Figure 4-4 Wi-Fi network

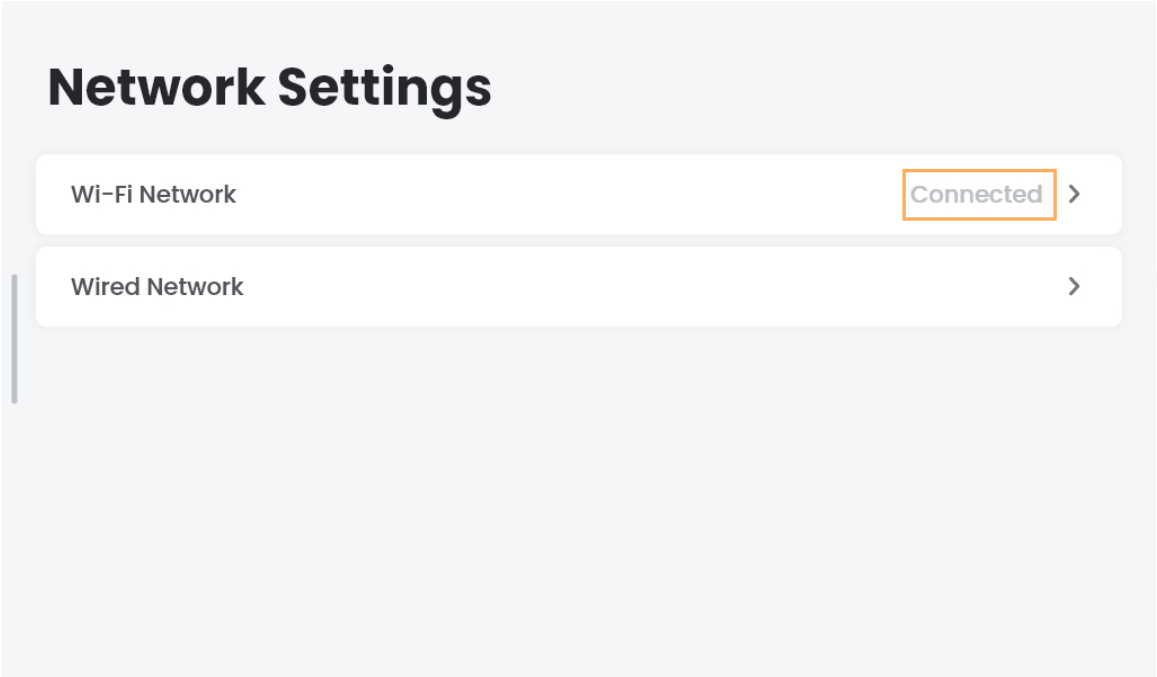


- The wireless network is enabled by default.
- Only 5G network can be searched by the Device.

Step 3 Tap the hotspot you want to connect, enter the password, and then tap **Connect**.

- If the hotspot is the one you have successfully connected before, and the saved password has not changed, the Device can connect the hotspot directly.
- If Wi-Fi network is connect successful, **Connected** is displayed, and is displayed on the homepage and screen saver.

Figure 4-5 Wi-Fi network connected

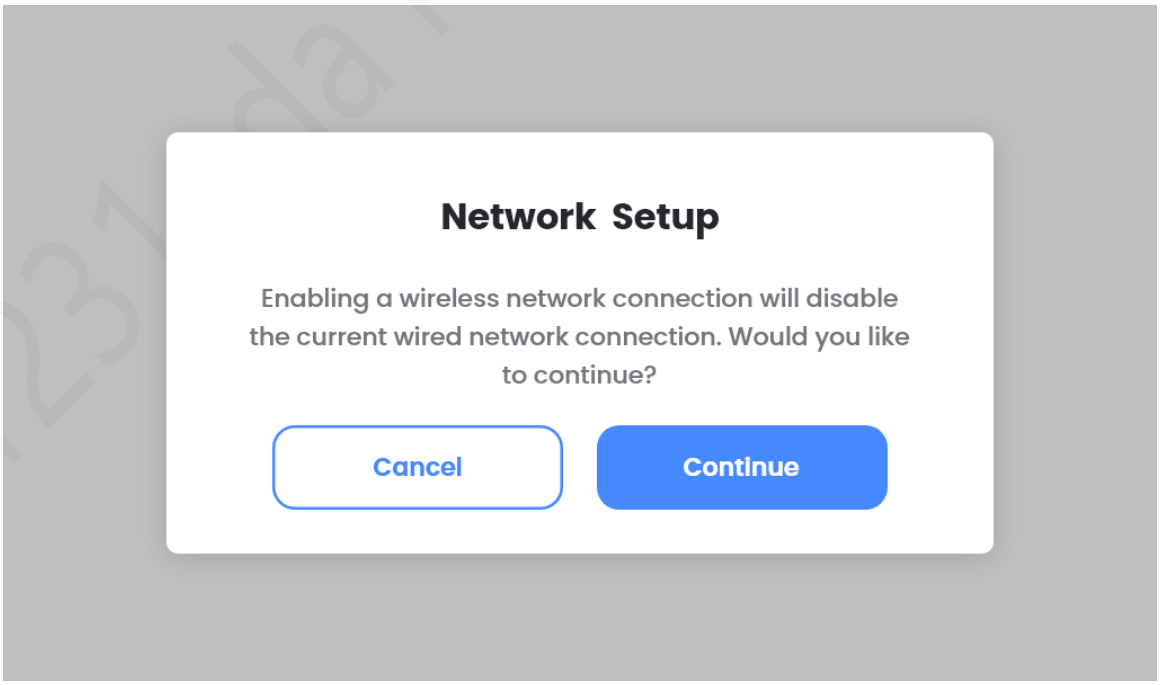


4.2.2 Configuring Wired Network

Step 1 Tap **Network Settings** on the **Settings** interface.
The **Network Settings** interface is displayed.

Step 2 Tap **Wired Network**, and then enable **Wired Network**.
The **Network Setup** prompt is displayed.

Figure 4-6 Network setup prompt (1)



Step 3 Tap **Continue**, and then select **DHCP** or **Static IP**.

- If you select **DHCP**, the Device will obtain IP address automatically. If the IP address is obtained, the IP address, subnet mask, gateway, and DNS will be displayed. If no IP address is obtained, there will be a failure prompt.
- If you select **Static IP**, you need to configure the IP address, subnet mask, gateway, and DNS manually. The system will verify the information you entered. If the information is invalid, there will be a failure prompt.

Step 4 Tap **Save**, and there will be another prompt to remind you to connect the network cable.

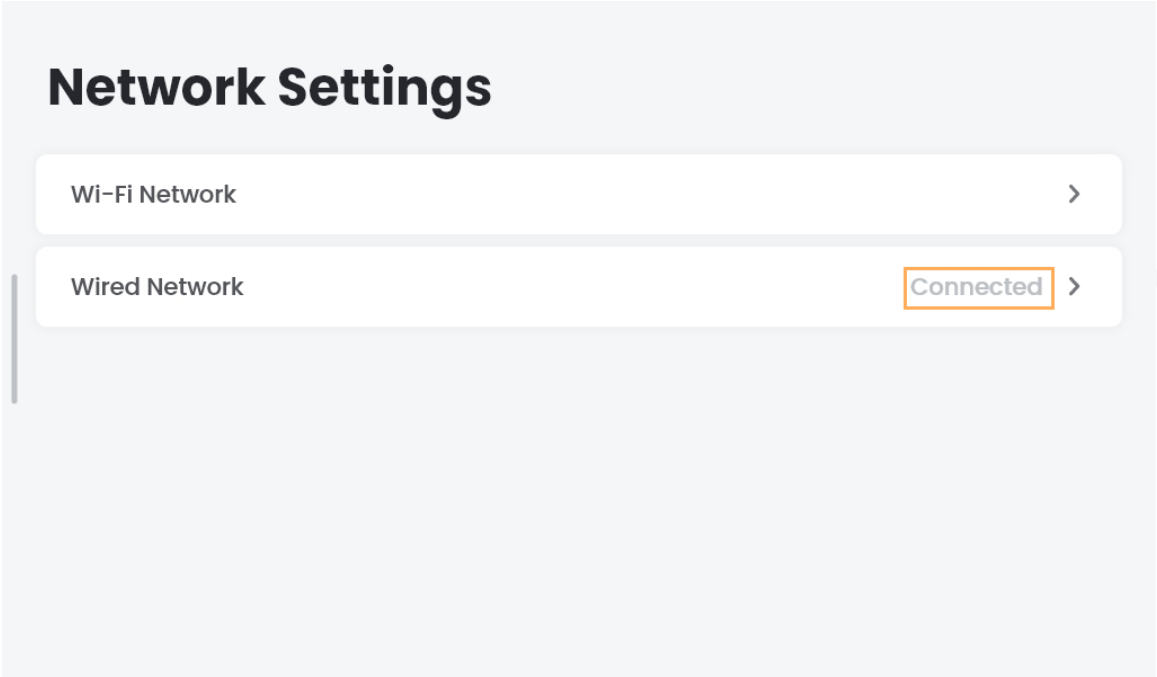
Figure 4-7 Network setup prompt (2)

Step 5 Tap **Continue**, and the connecting starts.

- If the connection is successful, tap **Complete** on the prompt interface.
- If the connection fails, tap **Try Again** or **Back**.

If wired network is connect successful, **Connected** is displayed.

Figure 4-8 Wired network connected

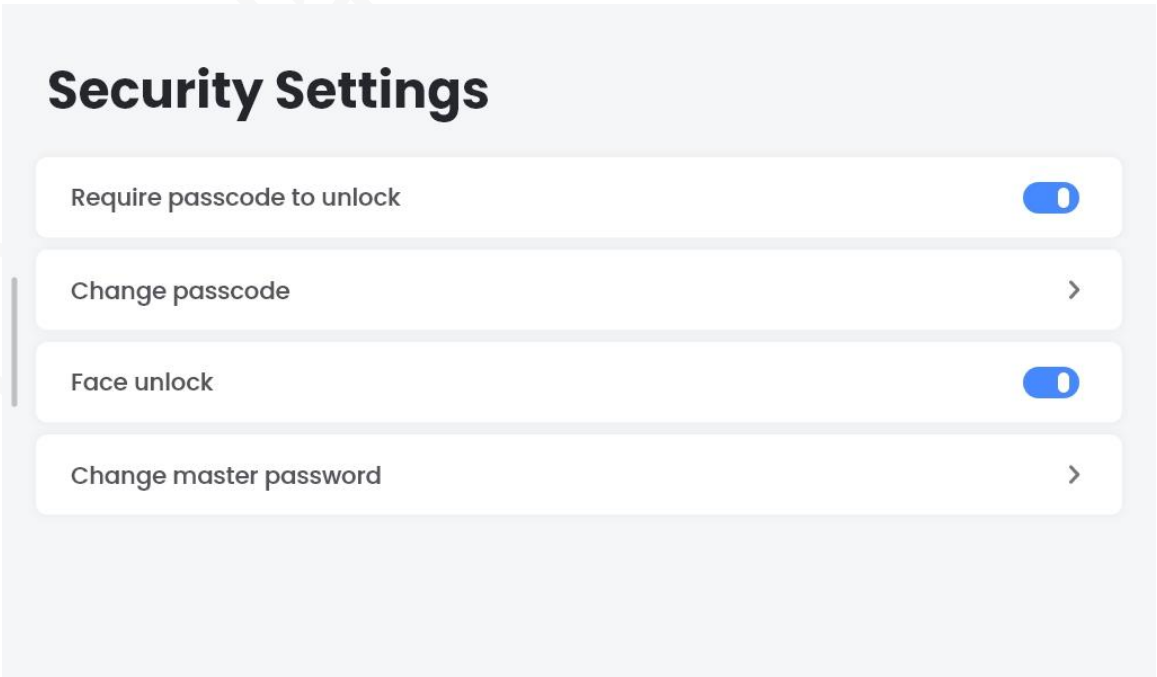


4.3 Security Settings

You can set password to protect your data on the Device, and you can enable or disable password protection.

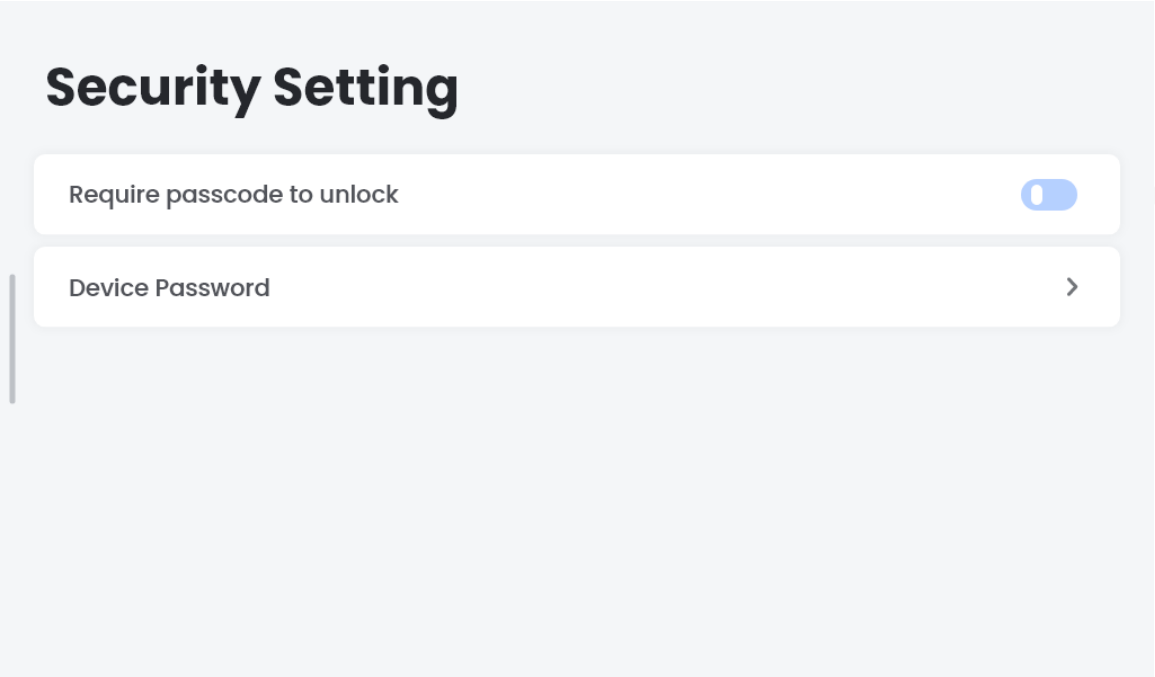
- If you have enabled password protection, on **Security Settings** interface, you can disable password protection, change passcode, enable or disable face unlock, and change master password.

Figure 4-9 Security setting (1)



- If you have not enabled password protection, on **Security Settings** interface, you can only change master password.

Figure 4-10 Security setting (2)



For password settings, see "2.2.1 Password Settings."

If you forget the passcode, long press the pairing button on the back of the Device for 10 seconds to restore to factory defaults. All data will be cleared if you restore the Device to defaults. Be cautious.

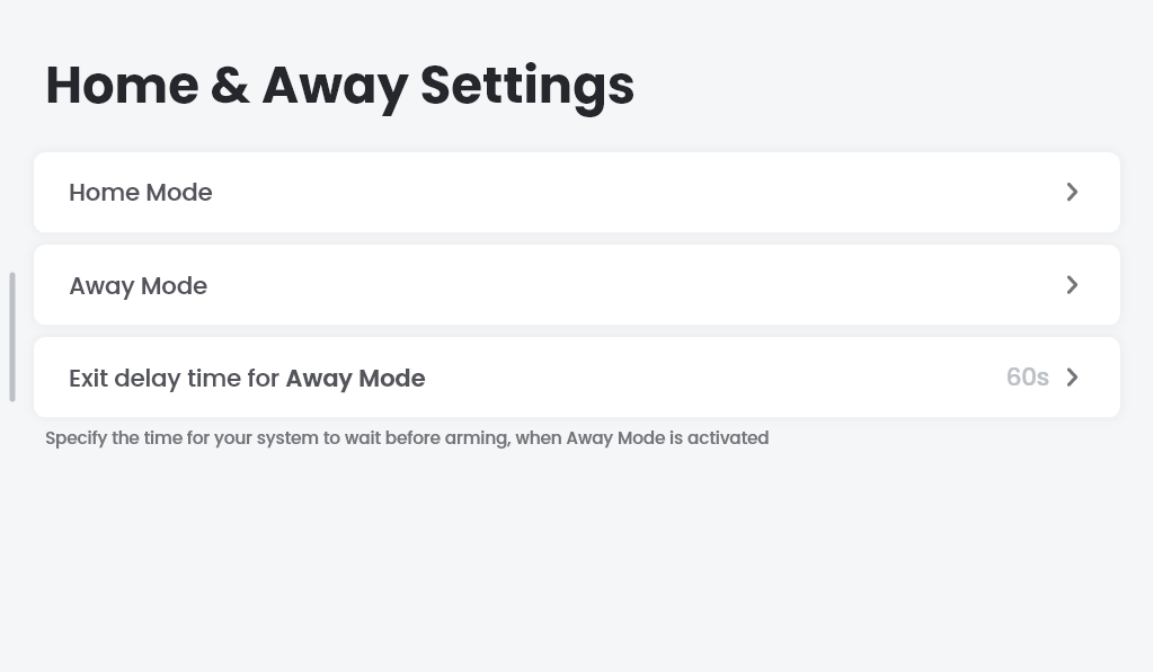
4.4 Home & Away Settings

You can arm or disarm different devices when you are at home or away from home.

Step 1 Tap **Home & Away Settings** on the **Settings** interface.

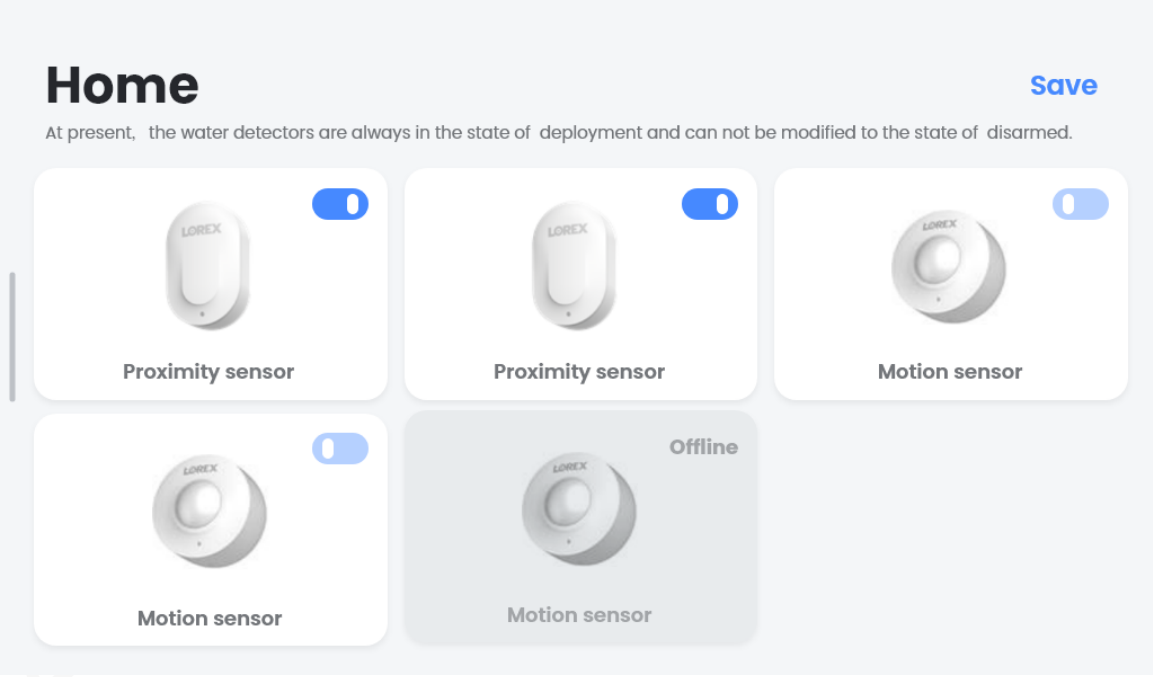
The **Home & Away Settings** interface is displayed.

Figure 4-11 Home and away settings



Step 2 Tap **Home Mode**, and **Home** interface is displayed.

Figure 4-12 Home mode



Step 3 Tap to arm or disarm the corresponding device.

- For offline devices, you cannot arm or disarm them.
- Flood detectors are armed after they are powered on by default, and you cannot disarm them.

Step 4 Tap **Save**.

Step 5 Tap **Away Mode** to arm or disarm devices.

The configuration is the same as that of the home mode.

- In **Home** mode, outdoor devices are armed and indoor devices are disarmed by default.
- In **Away** mode, all devices are armed by default. You can modify the default settings.

Step 6 Tap **Exit delay time for Away Mode** to set the time for the Device to wait before arming after the **Away** mode is enabled.

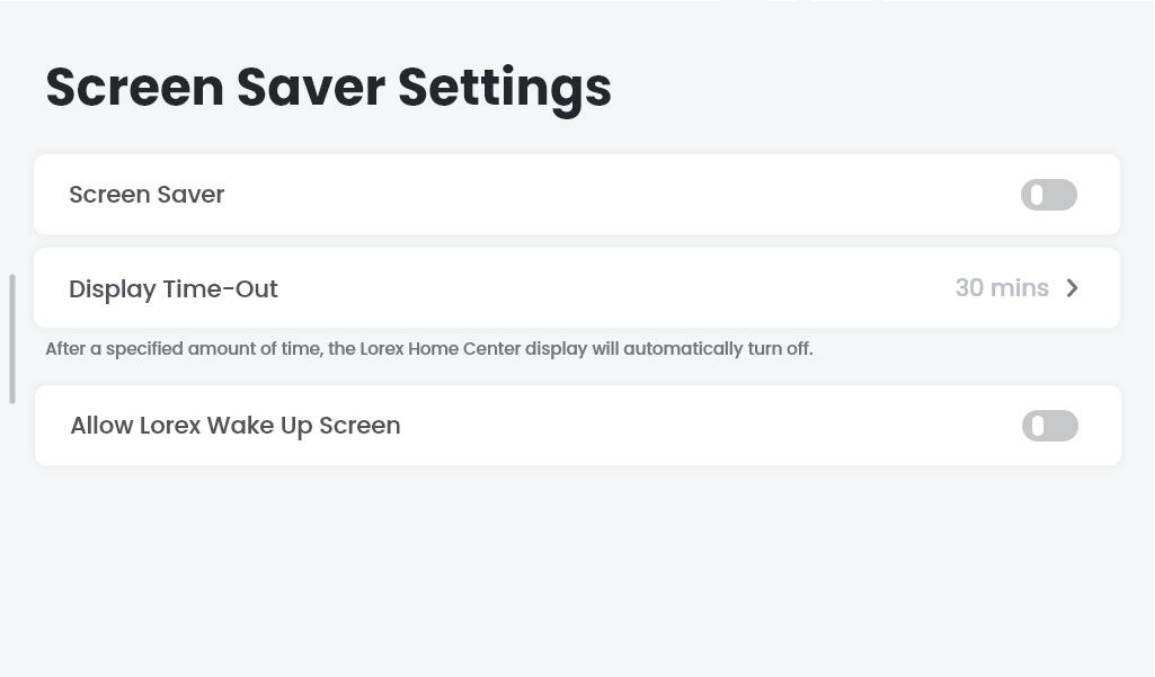
4.5 Screen Saver Settings

After you enable the screen saver, if there is no operation after a specified amount of time, the Device enters the screen saver automatically.

Step 1 Tap **Screen Saver Settings** on the **Settings** interface.

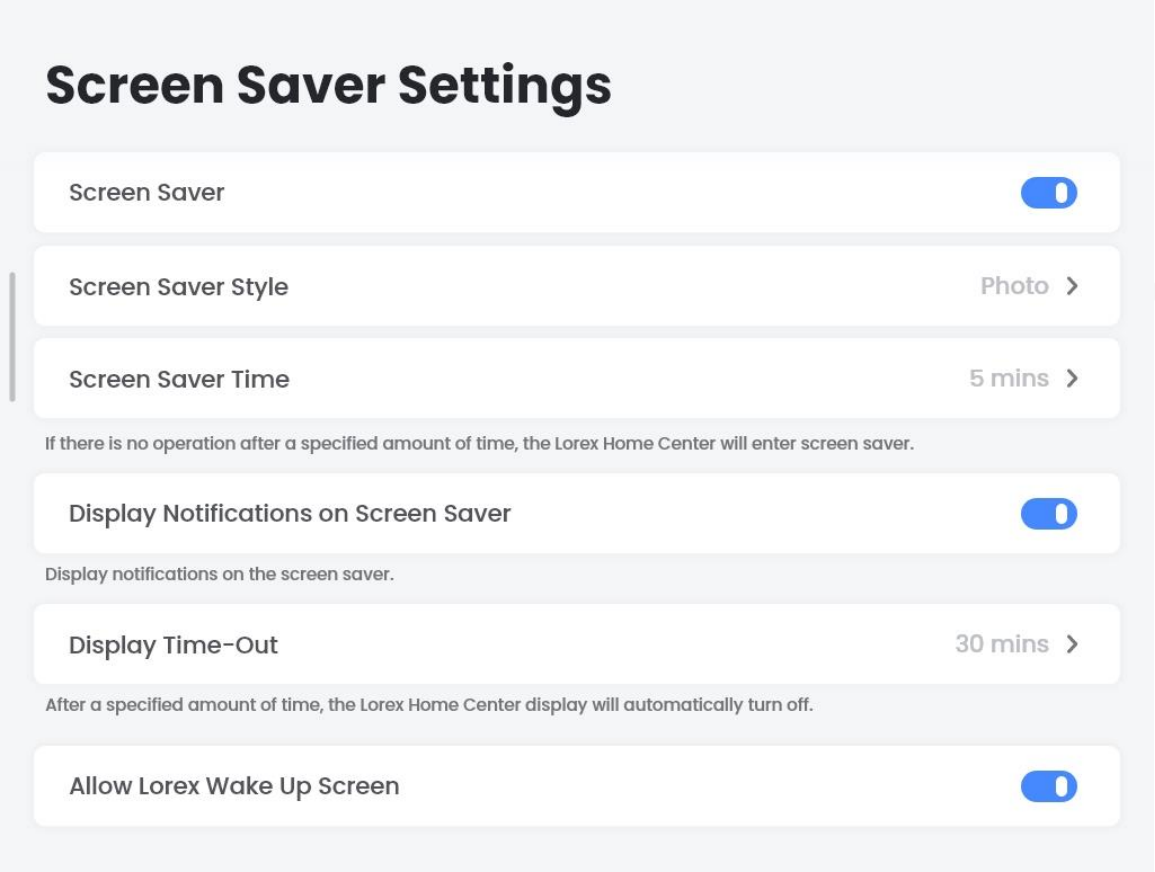
The **Screen Saver Settings** interface is displayed.

Figure 4-13 Screen saver settings



Step 2 Tap next to **Screen Saver Settings** to enable the function, and more options are displayed.

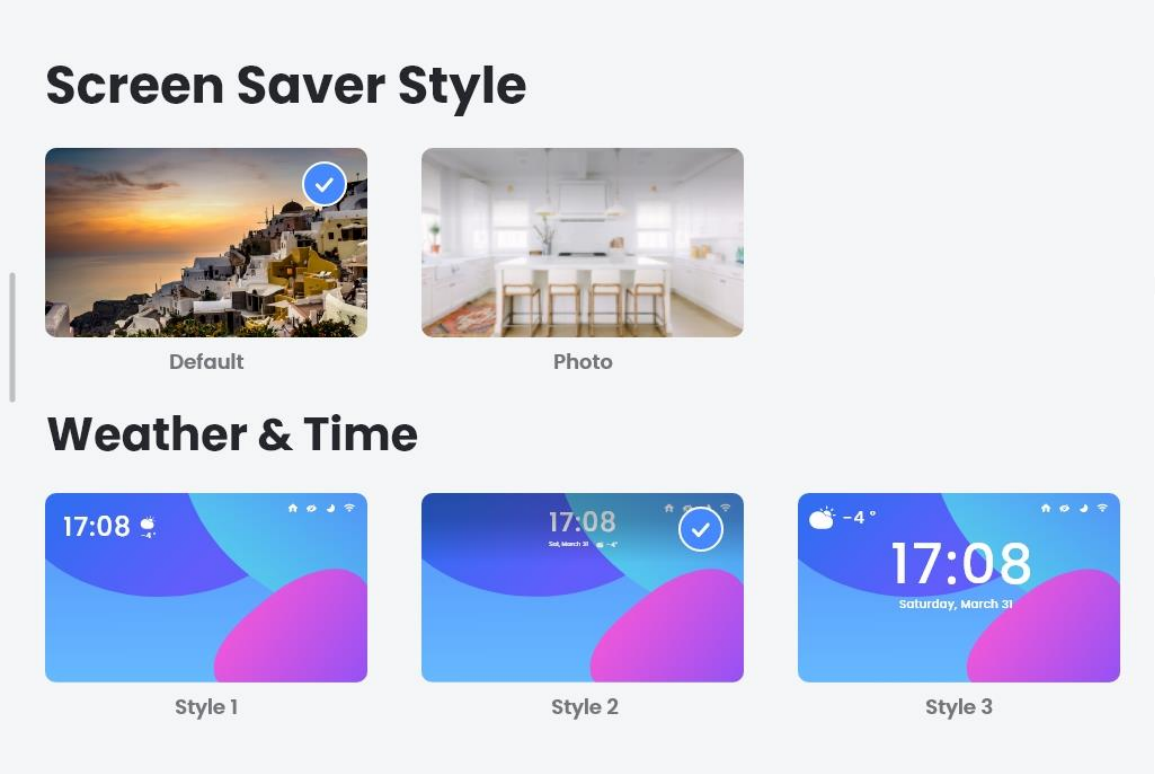
Figure 4-14 More options



Step 3 Tap **Screen Saver Style** to select a style.

Tap **Photo** to customize the screen saver. You can select an album or a folder to set picture carousel as the screen saver. You can also select one picture as the screen saver.

Figure 4-15 Screen saver style



Step 4 Swipe right on the **Screen Saver Style** interface, and then tap **Screen Saver Time**. You can select **30s**, **1 minute**, **5 minutes**, **10 minutes**, or **30 minutes**.

- If no operation is performed during the set time, the Device will enter screen saver.
- When live view, playback, video play or video talk is going on, the Device will not enter screen saver even if the set time reaches.

Step 5 Tap next to **Display Notifications on Screen Saver** to enable or disable the function.

- If you have enabled the function, there will be notifications displaying on the screen saver.
- The function is enabled by default.

Step 6 Tap **Display Time-Out** to select **30s**, **1 minute**, **5 minutes**, **10 minutes**, **30 minutes** or **Never**.

- If no operation is performed during the set time, the display will automatically turn off.
- When the Device is in screen saver or the display turns off, you can tap the screen or press the home button to wake up the Device, and then enter the passcode or use you face to unlock it.

Step 7 Tap next to **Allow Imou Wake Up Screen** to enable or disable the function. If you have enabled the function, you can wake up the Device with voice command.

4.6 Light Settings

You can set the multi-color light on the front panel of the Device. Tap **Light Settings** on the **Settings** interface, and then enable the light as needed. After you enable the light, the corresponding light will flicker once for demo.

Figure 4-16 Light settings

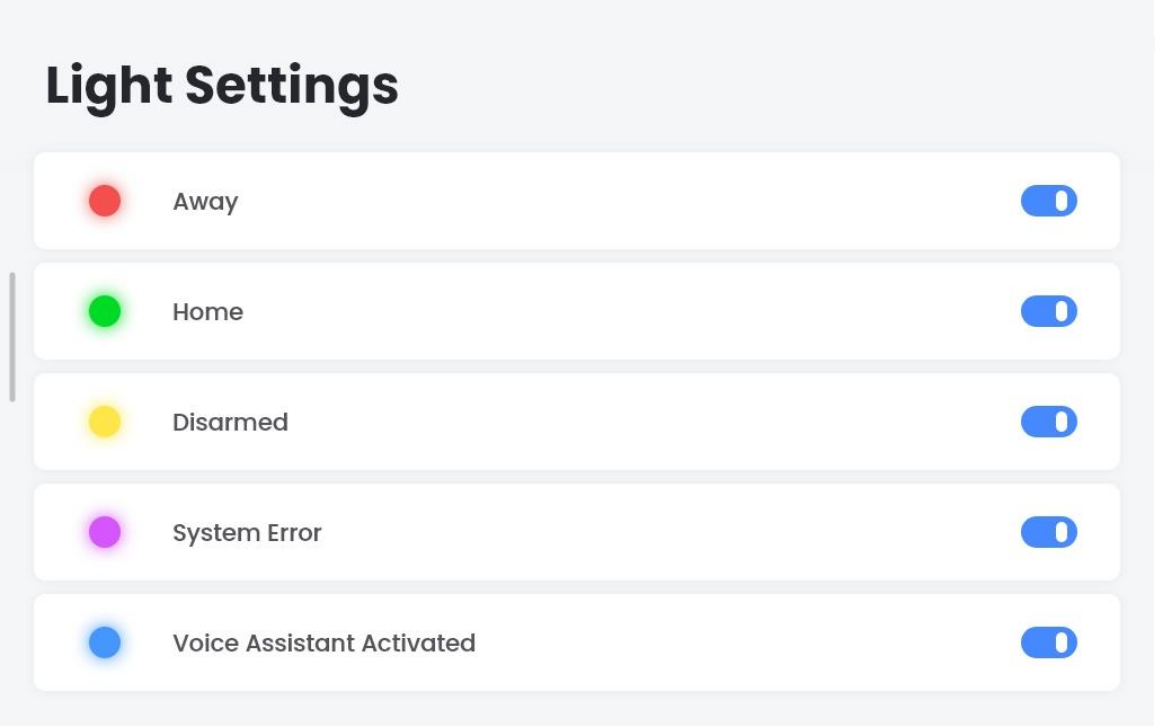


Table 4-1 Light description

Light Status	Description
Red light on	Away mode.
Yellow light on	Disarmed mode.
Green light on	Home mode.
Purple light flashing	Abnormality alarms, such as system error.
Blue light flashing	Voice assistant is activated.

For the priority, lights flashing is higher than lights on.

4.7 Sound Settings

Tap **Sounds** on the **Settings** interface, and then you can set the siren tone and doorbell chime.

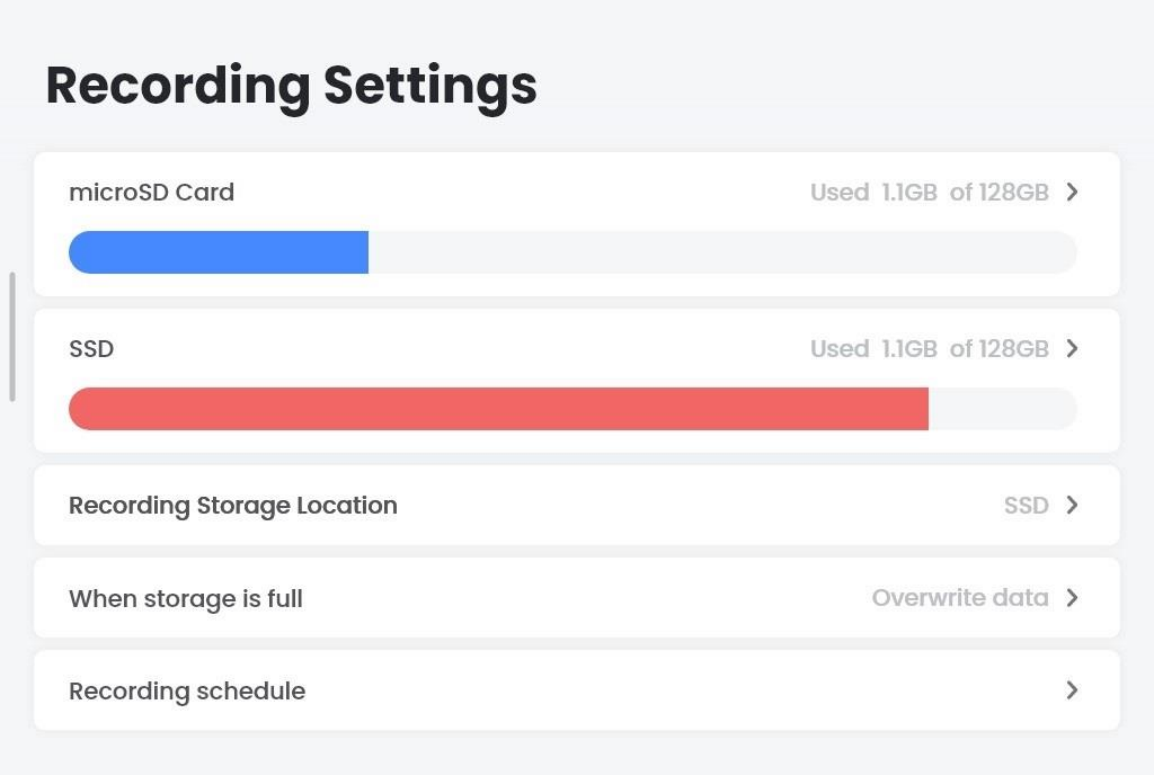
- After you set the siren tone, it will be played when alarms are triggered. You can select from the ringtones on the Device, or set the ringtone as **None**; you cannot record audios as ringtones.

- After you select the sound, it will be played once, which means that the sound has been set successfully. If an alarm is triggered when the sound is played, the sound will be interrupted, and then started over.
- Doorbell chime is the sound played when someone presses the doorbell. The sound will be played in loop until you answer the doorbell, or the time is out.

4.8 Recording Settings

You can set the video storage on the Device. Tap **Recording Settings** on the **Settings** interface, and the **Recording Settings** interface is displayed.

Figure 4-17 Recording settings



- On the **Recording Settings** interface, you can see the current use of the storage space which includes micro SD card and SSD. If no SD card or SSD is available, a prompt will be displayed; otherwise the used space and the total space are displayed.
- You can format the SD card and SSD on the Device.

Recording Storage Location

You can set the storage location as **SSD** or **SD Card**, and **SSD** is selected by default.

- For the SD card, you need to buy it separately, and up to 128 GB is supported.
- For the SSD, it is 256 GB by default, and 2 TB at most.
- If the used space reaches 90%, the used portion will be highlighted in red.
- If the SSD or SD card is damaged, a prompt will be displayed.

When Storage is Full

You can select to overwrite data or stop recording when the storage is full.

- **Overwrite data**: When the storage space is 1 GB left, a prompt will be displayed. You can select to overwrite the earliest video or change the storage location.
- **Stop recording**: When the storage space is 1 GB left, a prompt will be displayed. You can select to stop recording or change the storage location.

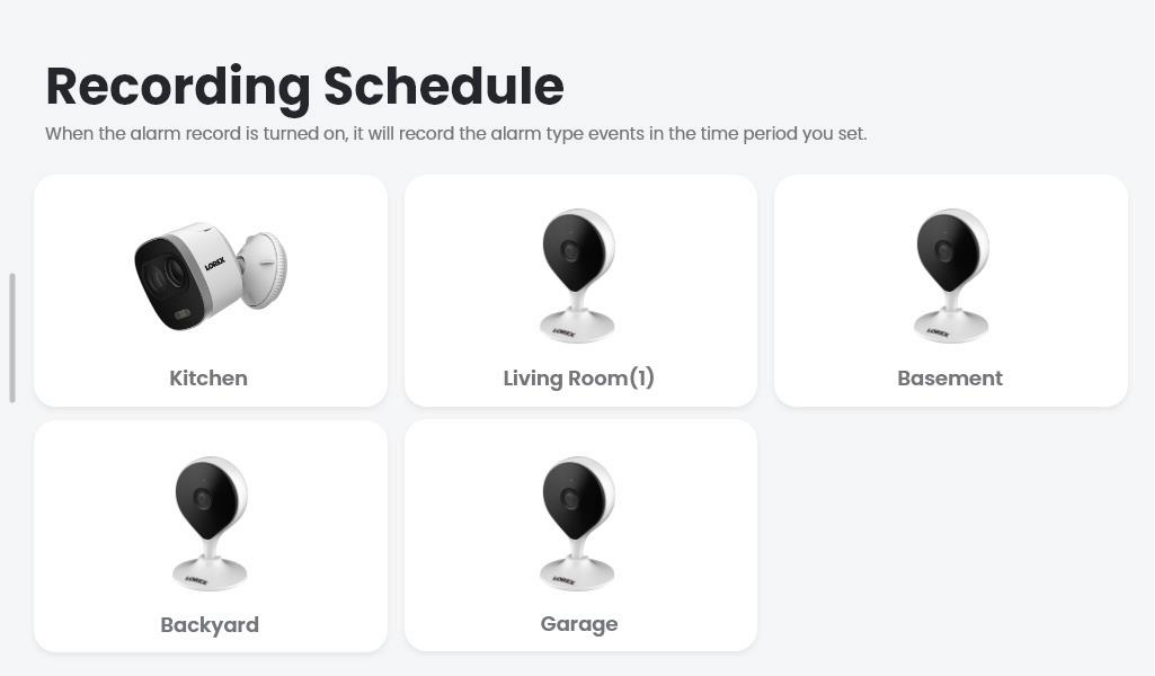
Recording Schedule

After you set the recording schedule, the Device will record the alarm events in the period you set.

Step 1 Tap **Recording schedule** on the **Recording Settings** interface.

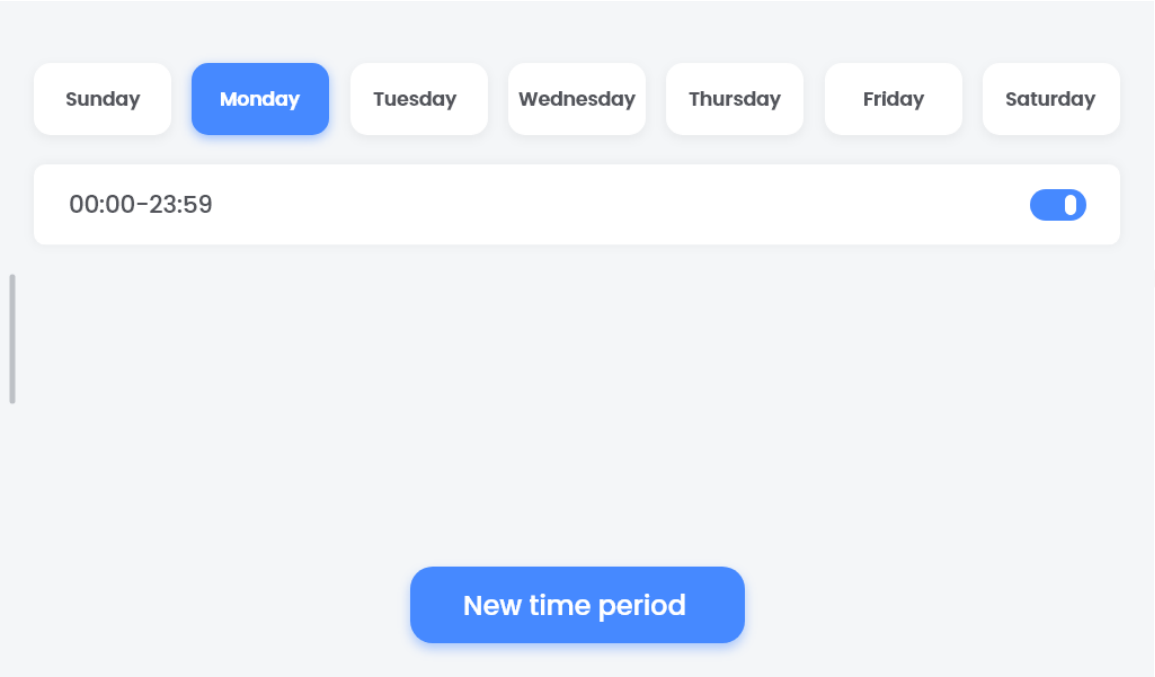
The **Recording Schedule** interface is displayed.

Figure 4-18 Recording schedule



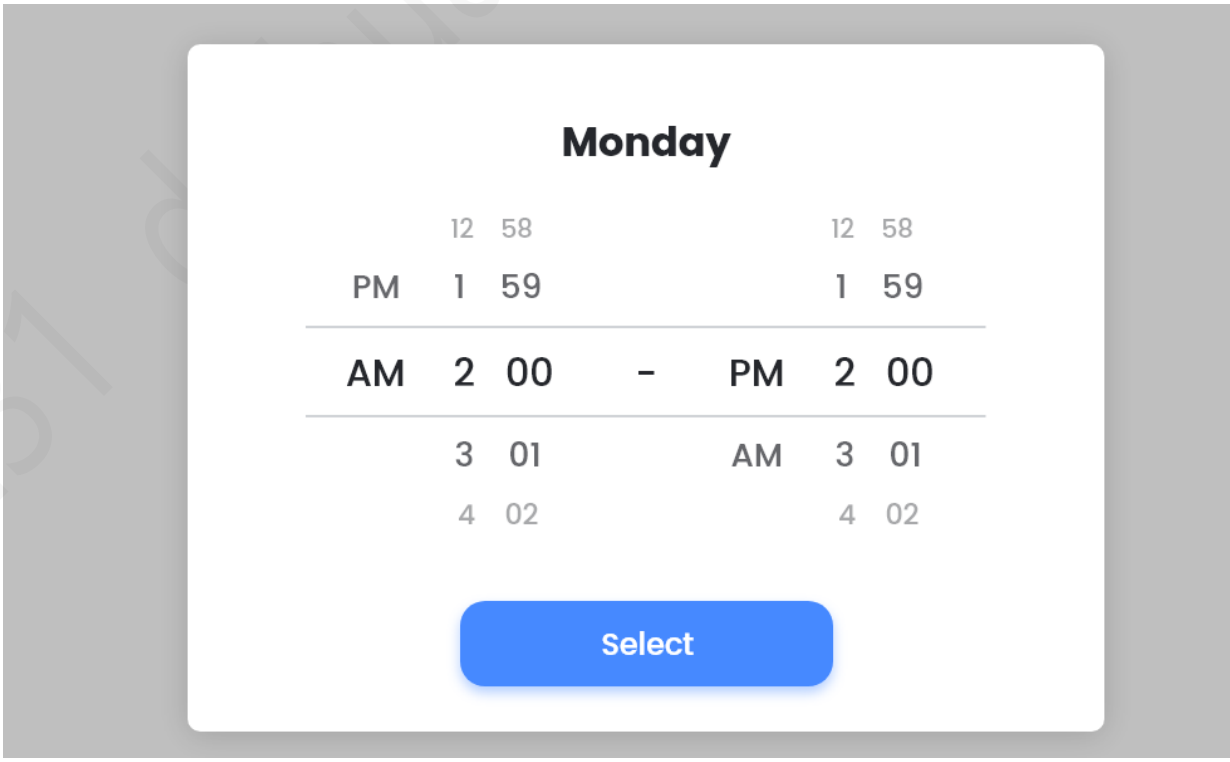
Step 2 Select the device that you want to set recording plan, and then the arming period setting interface is displayed.

Figure 4-19 Arming period setting



Step 3 Select a day that you want to record videos, and then tap New time period to set arming period. The arming period is enabled by default.

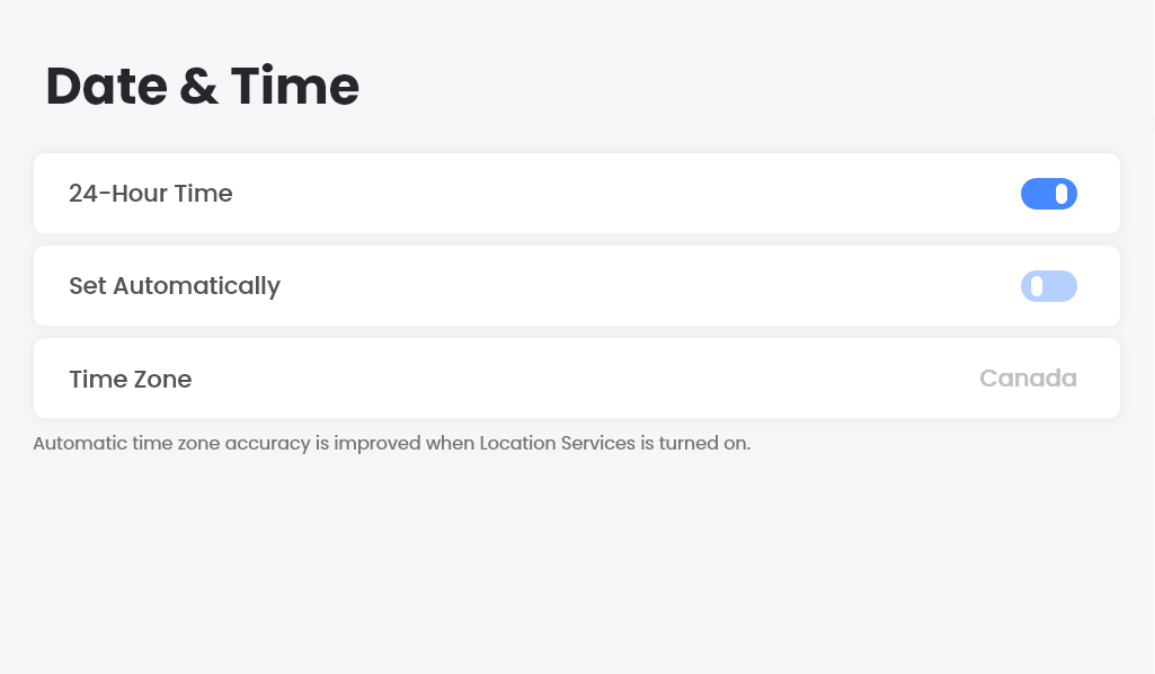
- You can set several recording plan for one day.
- The arming period is 24 hours every day by default, and the Device records videos for all motions.



4.9 Date and Time

You can set the date and time of the Device by tapping **Date & Time** on the **Settings** interface.

Figure 4-20 Date and time settings



- Both 24-hour mode and 12-hour mode are supported. If you disable **24-Hour Time**, then 12-hour mode is applied.
- The Device obtains network time automatically based on the IP address, and synchronizes time every one hour.
- You can disable **Set Automatically** to select the time zone, date and time manually.

4.10 Restoring to Factory Settings

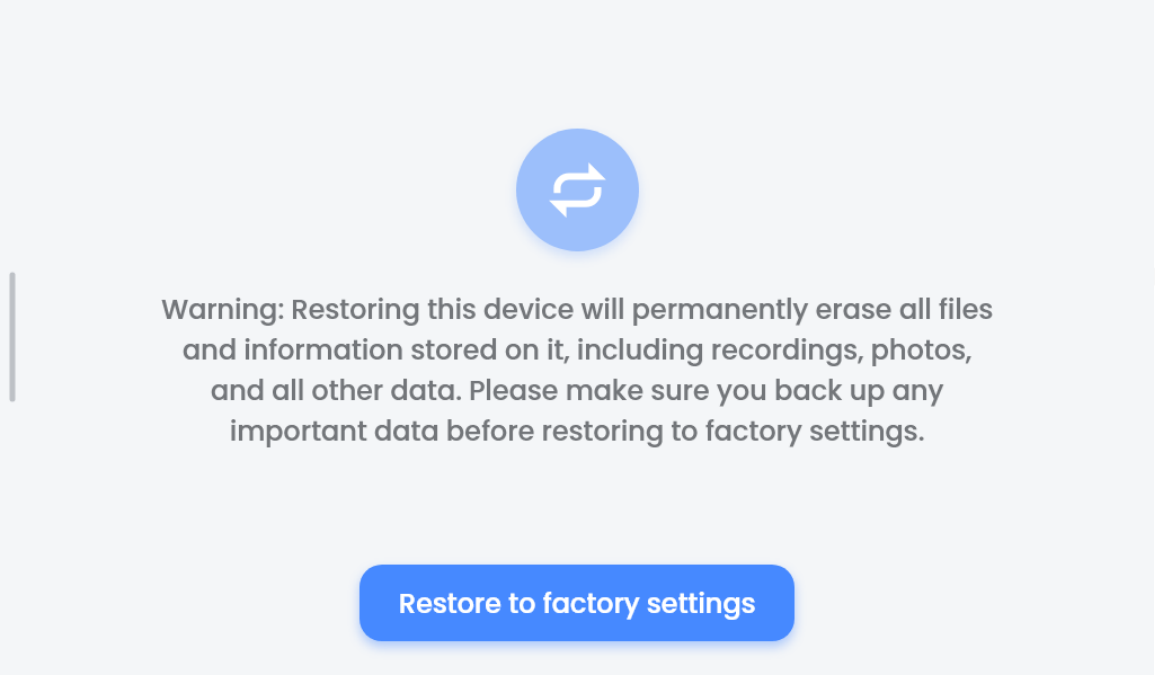
You can restore the Device to factory defaults.

If you use the function, all data on the Device will be cleared. Be cautious.

Step 1 Tap **Restore to Factory Settings** on the **Settings** interface.

A warning will be displayed.

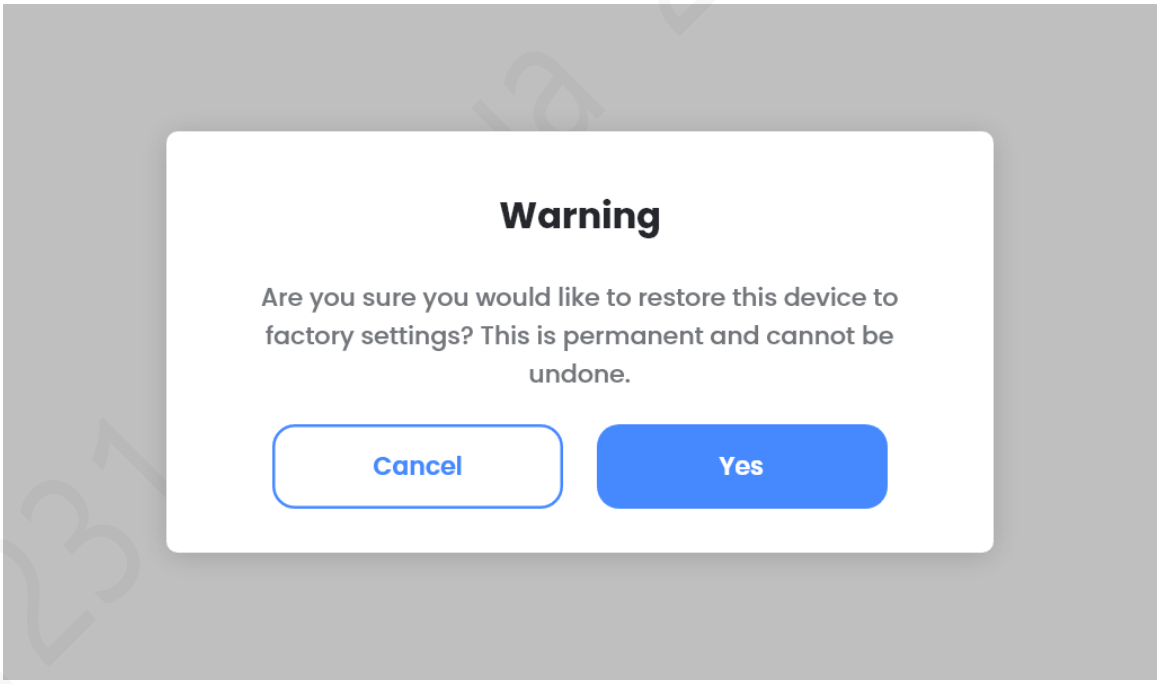
Figure 4-21 Warning (1)



Step 2 Tap **Restore to factory settings**.

Another warning is displayed.

Figure 4-22 Warning (2)



Step 3 Tap **Yes**, and the restoring process begins.

Step 4 After the restoring process is completed, the Device will be restarted.

And you need to finish the initialization before using the Device.

Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic equipment network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
   - Do not contain the account name or the account name in reverse order;
   - Do not use continuous characters, such as 123, abc, etc.;
   - Do not use overlapped characters, such as 111, aaa, etc.;

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your equipment network security:

1. **Physical Protection**

   We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The equipment supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **Enable Whitelist**

   We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.

8. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

9. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

10. **Disable Unnecessary Services and Choose Secure Modes**

    If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

    If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

    - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
    - SMTP: Choose TLS to access mailbox server.
    - FTP: Choose SFTP, and set up strong passwords.
    - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

11. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

12. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

13. **Network Log**

    Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

14. **Construct a Safe Network Environment**

    In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is

suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.

- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.