Mobile Portable Terminal

Quick Start Guide

V1.0.2

Foreword

General

This manual introduces the structure, operations and maintenance of the Mobile Portable Terminal (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.
📖 NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.2	Added safety precautions for batteries and refine the whole manual.	July 2020
V1.0.1	Updated the titles of Section 3.4.2 and 3.6.2.	November 2018
V1.0.0	First release.	October 2017

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.
- Install 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.
- Transport, use and store the Device under the allowed humidity and temperature range.

Power Requirements

- Improper battery use might result in fire, explosion, or inflammation.
- When replacing 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 requirements 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.

Table of Contents

1 Product Introduction

1.1 Overview

The Device adopts forensic technology, and integrates audio and video recording, and snapshot taking in one mobile portable terminal. It facilitates the work of public security police and other law enforcement departments in a variety of environments.

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 according to the packing list. For details, see Table 1-1.

Table 1-1 Packing list

Name	Quantity
Device	1
Shoulder mark clip	1
Back clip	1
USB cable	1
Micro USB to Mini USB cable	1
Battery	1
Power adapter	1
Quick Start Guide	1
QR code	1

2 Structure

2.1 Structure

Figure 2-1 Front and rear panel

White light
IR
Laser Light
MIC Hole
HD Camera

White light
IR
Sensor
MIC Hole

Home   Return
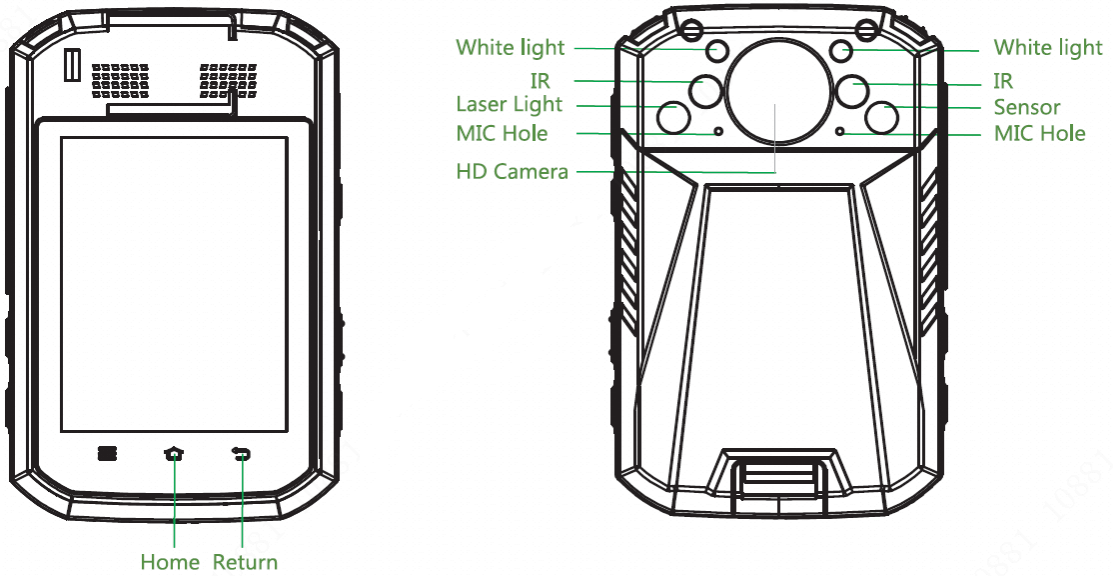
Figure 2-2 Left and right panel

Multi-Function
Composite Port

Screw Hole

Up/Enable Laser Light

Down/Enable White
Light

Bidirectional Talk

Record Audio

Record Video

Snapshot
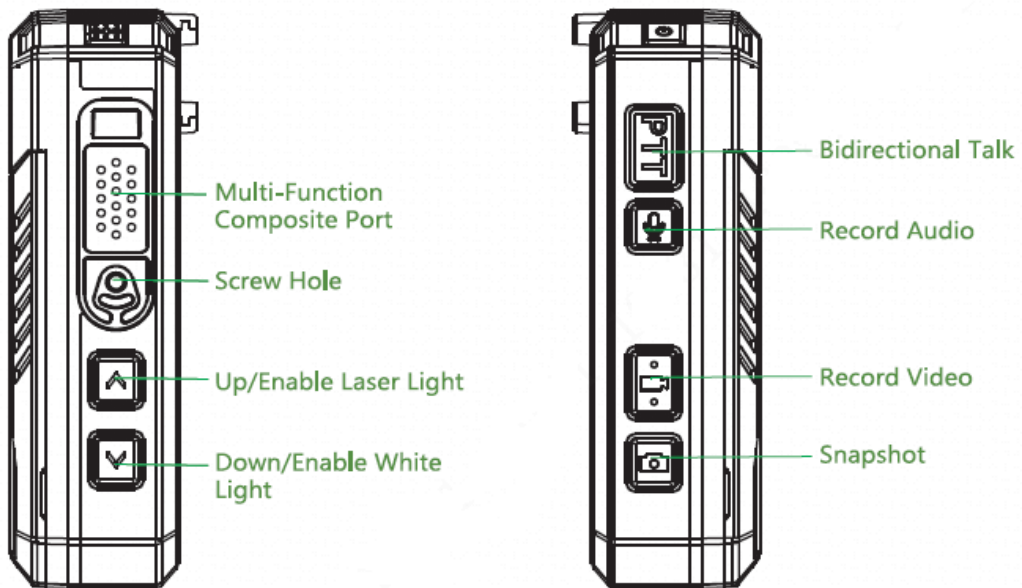
Figure 2-3 Top and bottom panel

Alarm Indicator Light   Power

USB Port/Recharge Port
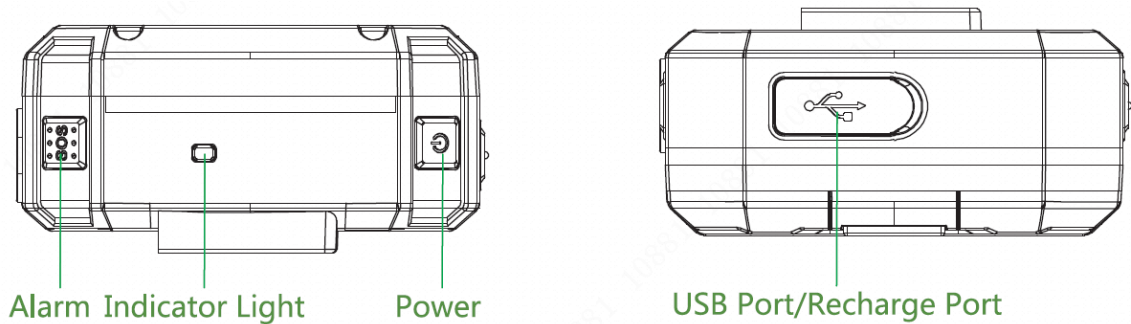
2.2 Indicator Status

When the Device is in different working states, the indicator lights have different statuses. For details, see Table 2-1.

Table 2-1 Indicator status

Working State	Indicator Status	Working State	Indicator Status
Standby.	Green light is on.	Recording audios.	Yellow light flickers.
Standby when the battery level is less than 5%.	Red light is on.	Charging.	Red light is on.
Recording videos.	Red light flickers.	Full charge.	Green light is on.
Taking pictures.	Red light flickers	Pull stream.	Blue light flickers.

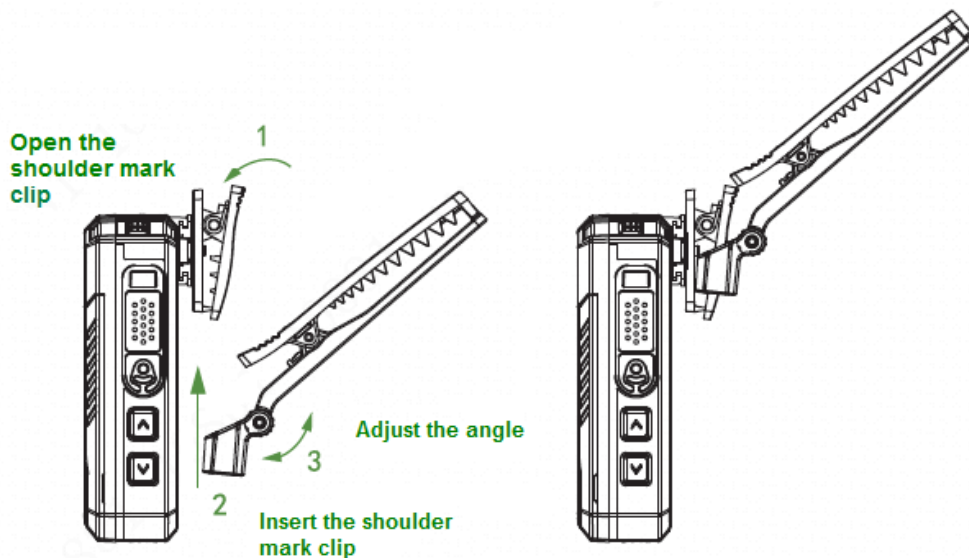## 2.3 Back Clip and Shoulder Mark Clip Installation

Step 1   Install the back clip.

Figure 2-4 Back clip installation
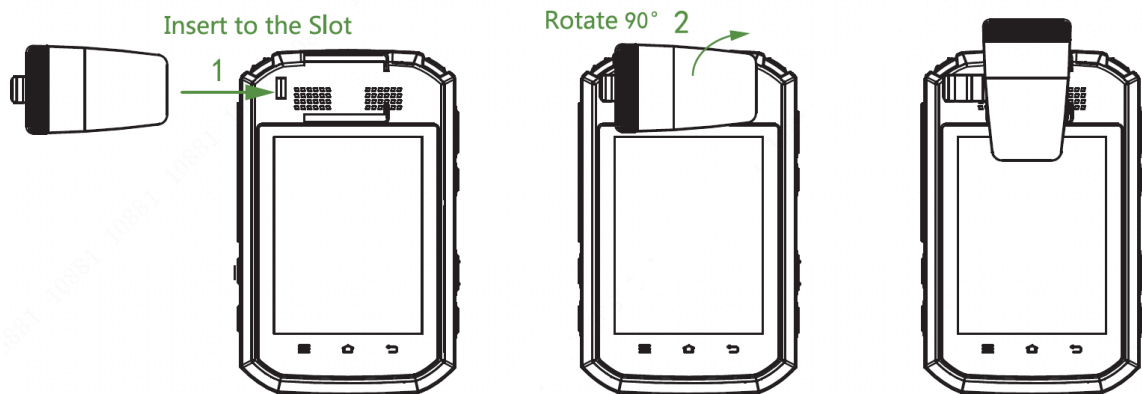
Step 2   Install the shoulder mark clip.

Figure 2-5 Shoulder mark clip installation

Step 3   Clip the installed shoulder mark clip onto the shoulder mark.

3 Basic Operations

3.1 Powering On or Off

Press the [⏻] on the top panel to power on or off, restart or hibernate the Device.

- When the Device has been shut down, press and hold [⏻] to start it.

- When the Device is running, press and hold [⏻], select **Power off**, and then click **OK** on the **Power off** interface, the Device will be shut down.

- When the Device is running, press and hold [⏻], select **Reboot**, and then click **OK** on the **Reboot** interface, the Device will be restarted.

- When the Device is running, press [⏻] to hibernate the Device. Press again to wake up the Device.

- When the Device is running, press and hold [⏻] for 10 seconds to force restart it.

3.2 Device Initialization

For first usage, you need to set the login password, and at least three security questions. If you forget the password, go to **Settings > System > Modify Password**, click **Forgot password**, and then answer the security questions to reset login password.
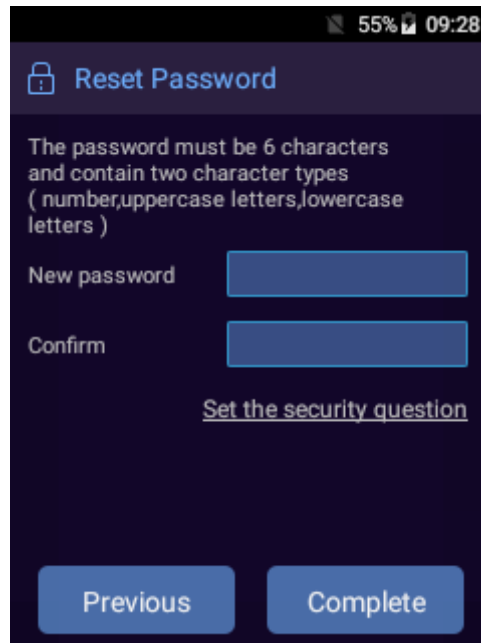
Step 1 When the Device has been shut down, press and hold [⏻] to start it.

The **Language Setting** interface is displayed.

Step 2 After selecting the language, click **Next**.

The **Reset Password** interface is displayed.
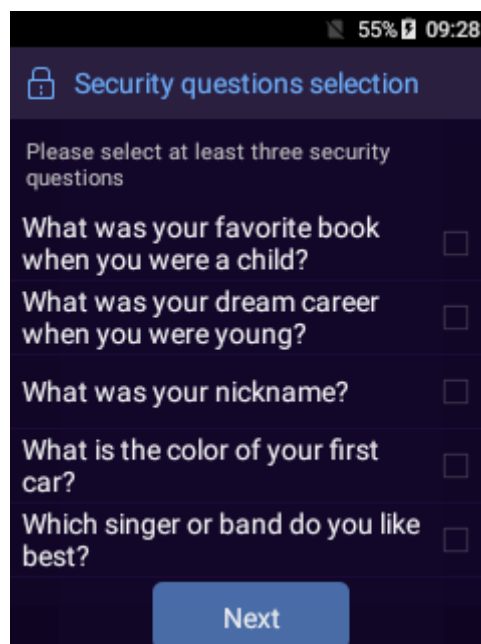
Figure 3-1 Resetting the password

Step 3 Enter the new password, and then confirm it.

Step 4 Click **Set the security question**.

The **Security questions selection** interface is displayed.

Figure 3-2 Security questions selection

Step 5 Select at least three security questions, and then click **Next**.

Step 6 Enter the answers to the security questions, and then click **Save**.

The system prompts **Successfully set security answers**, and then goes back to the **Reset Password** interface.

Step 7 Click **Complete** on the **Reset Password** interface.

The system prompts **Successfully modified password**, and the live view interface is displayed.
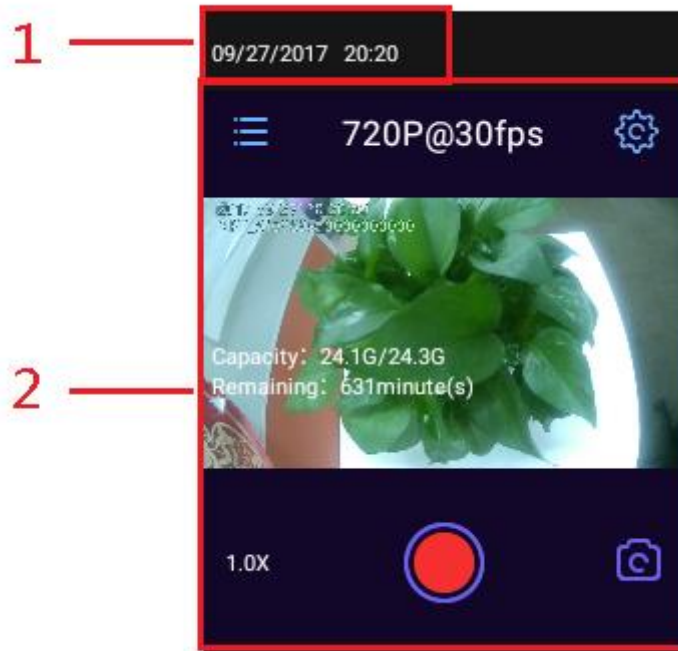
Figure 3-3 Live view interface

Table 3-1 Live view interface description

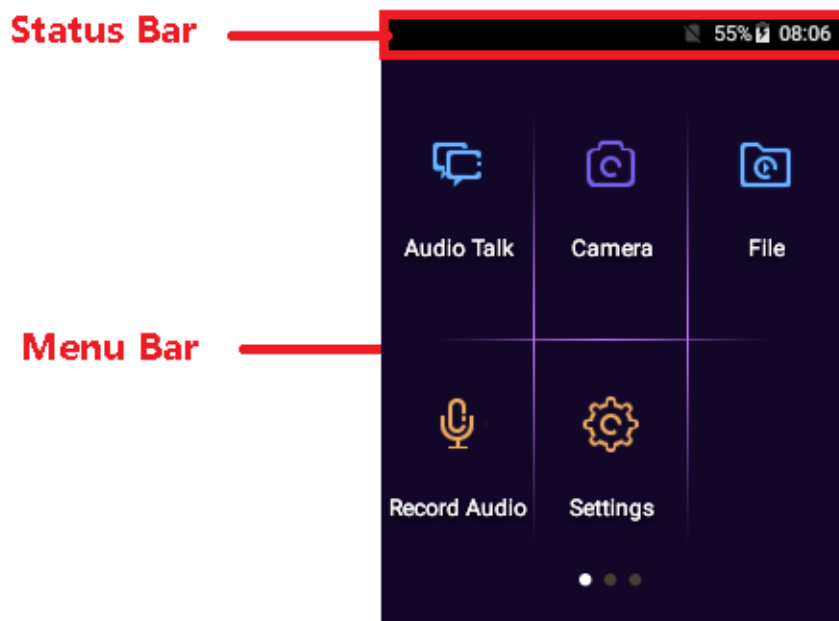| No.	Name
1	Displays the current time of the Device.
2	Live view

3.3 Main Interface

On the live view interface, tap ⌂ or ↩ to go back to the main interface.

Figure 3-4 Main interface

- The status bar is to display message, working status and the carrier. Tap the status bar and slide down to view the time, date and battery. Tap ⚙ to go to the **Settings** interface quickly.
- Slide left or right on the menu bar to go to the previous or next page.

3.4 Videos

3.4.1 Recording Videos

After you initialize the Device, it enters live view interface by default after being started. For the interface, see Figure 3-5. For the parameter description, see Table 3-2.

Press 🎥 to start recording. Press 🎥 again to stop recording.

Figure 3-5 Live view interface

Table 3-2 Live view parameter description

No.	Description
1	Tap the icon, and enter login password to manage files.
2	Displays video quality when recording videos. 📖 Displays image resolution when taking snapshots.

| No.	Description
3	Tap the icon to set parameters. ● When recording videos, you can tap the icon to set video quality, pre-recording time, and post-recording time. ● When taking snapshots, you can tap the icon to set photo resolution, continuous shot, and snap sound.
4	Tap the icon to switch to the snapshot taking mode. 📖 In snapshot taking mode, tap to switch to the video recording mode.
5	Tap the icon to start recording videos; tap it again to stop recording. 📖 In snapshot taking mode, tap to take snapshot.
6	Tap the screen, and the zoom slider is displayed. Drag the slider to zoom in or out from 1.0 to 8.0 times.
7	Displays the remaining capacity/total capacity, and the remaining recording time. 📖 ● With different video resolutions, the remaining recording period is not the same. ● Displays the remaining capacity/total capacity, and the remaining snapshot time in snapshot taking mode.
8	Displays the date, time, serial number, police officer number, and GSP information. 📖 ● To display police officer number, you need to set the number with PCTool first. ● To display GPS information, make sure that you have enabled location function and GPS OSD. Go to **Settings > Network > Location** to enable location function, and go to **Settings > Device > OSD > GPS OSD** to enable GPS function.
9	Displays customized OSD information. 📖 ● You can display two customized OSD messages on the interface. Before this, you need to use the PCTool to set OSD information and enable customized OSD information. ● Use USB cable to connect the Device and PC, run PCTool, enter and confirm the password, and then set the OSD information (the length shall be less than 40 bits). ● Go to **Settings > Device > OSD > Custom Info** to enable or disable customized OSD information.

3.4.2 One Tap to Record Videos

Press to start recording videos and enter live view interface when the Device has been hibernated. Press again to stop recording.

3.4.3 Zoom

On the live view interface or when recording videos, press and hold [icon] or [icon], or tap the screen, and the zoom slider is displayed. Drag the slider to zoom in or out 1.0 to 8.0 times.

3.4.4 Marking Important Videos

When recording videos, press and hold [icon] to mark important videos. The videos marked with stars will have IMP filename extensions.

Yellow stars will be displayed at the top right corner of the screen.

Figure 3-6 Marking important videos
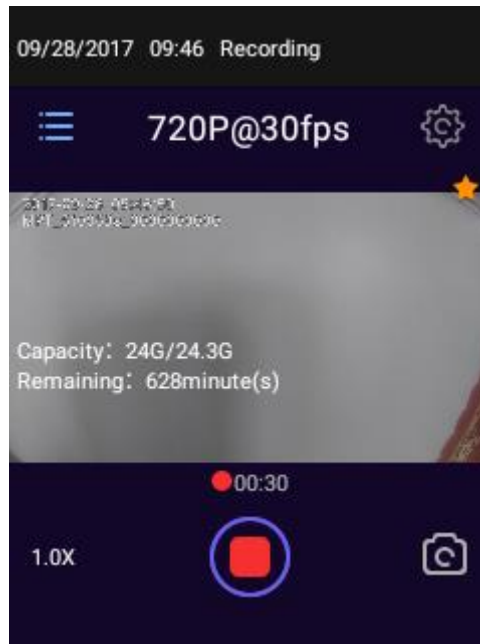
3.5 Snapshots

3.5.1 Taking Snapshots

On the live view interface, press [icon] or tap [icon], and you will hear the shutter sound. The working indicator flickers with red light, and then a snapshot is taken.

3.5.2 One Tap to Take Snapshots

Press [icon] to start taking snapshots, and enter the live view interface when the Device has been hibernated.

3.6 Audios

3.6.1 Recording Audios

On any interface, press ![icon] to start recording audios. Or tap ![icon] on the main interface. The recording interface is displayed. See Figure 3-7. For the parameter description, see Table 3-3.

Figure 3-7 Recording audios
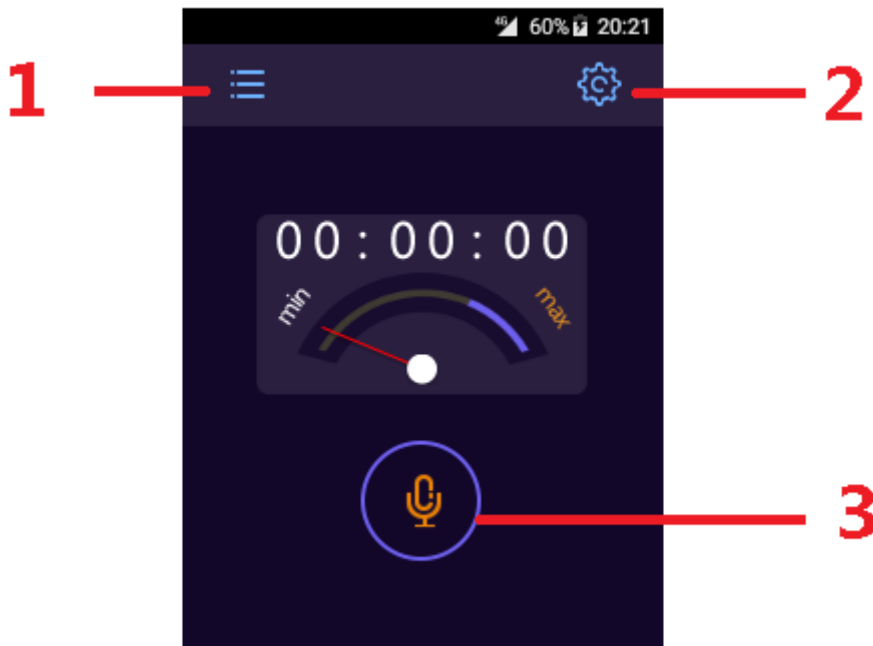
Table 3-3 Audio recording parameter description

No.	Description
1	Tap the icon, and enter login password to manage files.
2	Tap the icon to set audio format and file type. ● Audio formats: **AAC**, **G.711A**, and **AMR**. ● File types: **dav**, and **aac**. 📖 When you are recording audios, icon 1 and 2 are hidden.
3	Tap the icon to start recording audios; tap ![icon] to stop recording. The system prompts **Audio record is over and saved**.

3.6.2 One Tap to Record Audios

Press ![icon] to start recording audios when the Device has been hibernated. Press ![icon] again to stop recording.

3.7 One Tap to Switch

In video settings, **Record Video & Audio** is disabled by default, and you can switch between audio and video by one tap.

- When videos are recorded, press to stop recording videos and switch to audio recording.

- When audios are recorded, press to stop recording audios and switch to video recording.

3.8 Recording Audio & Video at the Same Time

Before using the function, you need to go to **Device > Video**, and then enable **Record Video&Audio.**

- When videos are recorded, press to start recording videos and audios at the same time.

- When audios are recorded, press to start recording audios and videos at the same time.

3.9 Data Transmission

The Device can upload data through PCTool and acquisition station.

After the USB cable is inserted, all wireless functions will stop, and white light and IR light will be turned off, and cannot be turned on again. Current audio or video recording will automatically stop. After stopping USB connection, audio or video recording will not automatically resume.

- When the Device is started, connect it to the PC through USB cable, and then run PCTool. Enter and confirm the password, and then you can download the data.
- When the Device is started, connect it to the USB port of the proper data acquisition station. The data on the Device can be automatically uploaded to data acquisition station. If the data on the Device is not properly displayed, disconnect and then connect the USB cable again.

4 Battery and Maintenance

The Device supports 5V/2A DC power. When the battery level is low, charge the Device in time.

- When the Device has the main battery, the voltage of the main battery is displayed on the interface.
- After the main battery is taken out, the system prompts "The main battery has been removed". In this case, the white light and IR light cannot be enabled. And the WLAN, location, Bluetooth, NFC settings become grey. After installing the main battery, the system prompts the battery restores.

⚠

- Recharge the battery if the Device will not be in use for a long time.
- The system triggers low voltage alarm when the device voltage is ≤5%.
- The Device automatically shuts down when the power runs out.
- If the device will not be used for a week or more, charge it to 60%, take the battery out of the Device, and store it in a clean, dry and ventilated room with ambient temperature of 20±5°C.
- Charge the battery once every four months during storage.
- The battery is a consumable accessory. It is recommended to replace it after one year of use.

4.1 Installing SIM Card

⚠

- The SIM card and external accessories do not support hot swap. The installation comes into effect after the Device is restarted.
- Shut down the Device before installing the SIM card; otherwise the Device might be damaged.

Step 1 Use one hand to pull down the battery cover lock on the back of the Device, and use the thumb of the other hand to hold the tray on any side of batter cover. Follow the directions on Figure 4-1 to remove the battery cover.

Figure 4-1 Take out the battery cover

Hold the thumb here

Battery cover lock
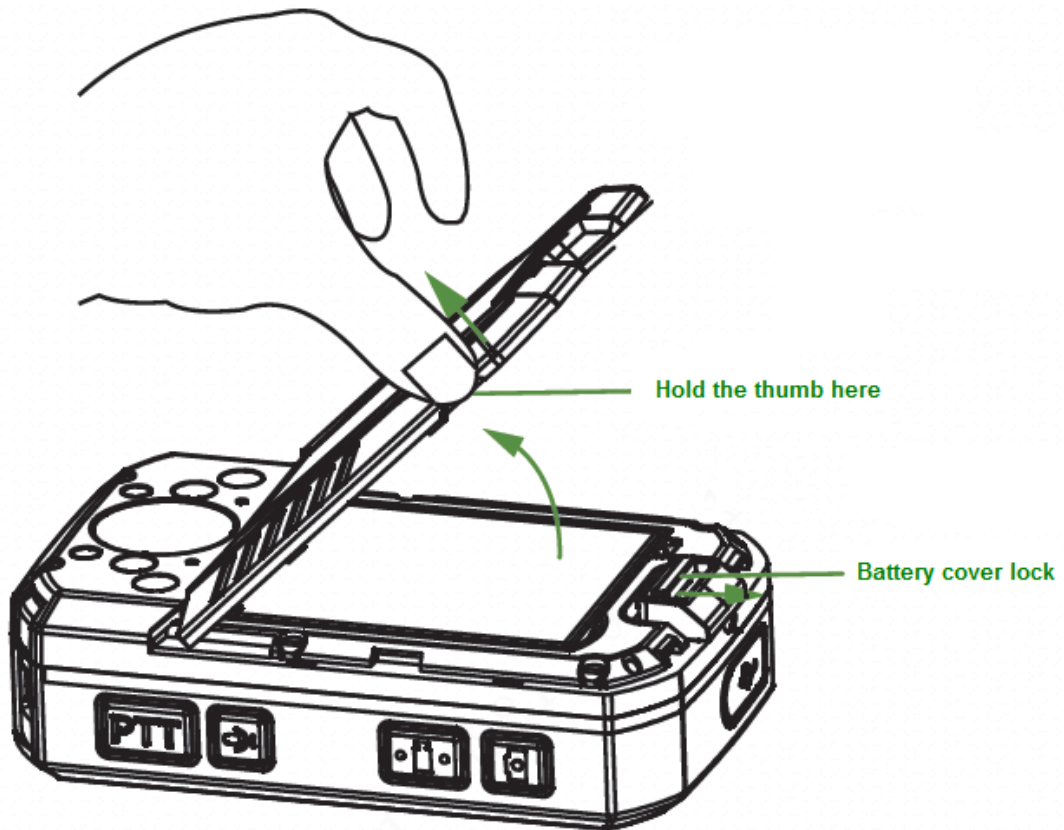
Step 2　Take out the main battery.

Figure 4-2 Take out the main battery.
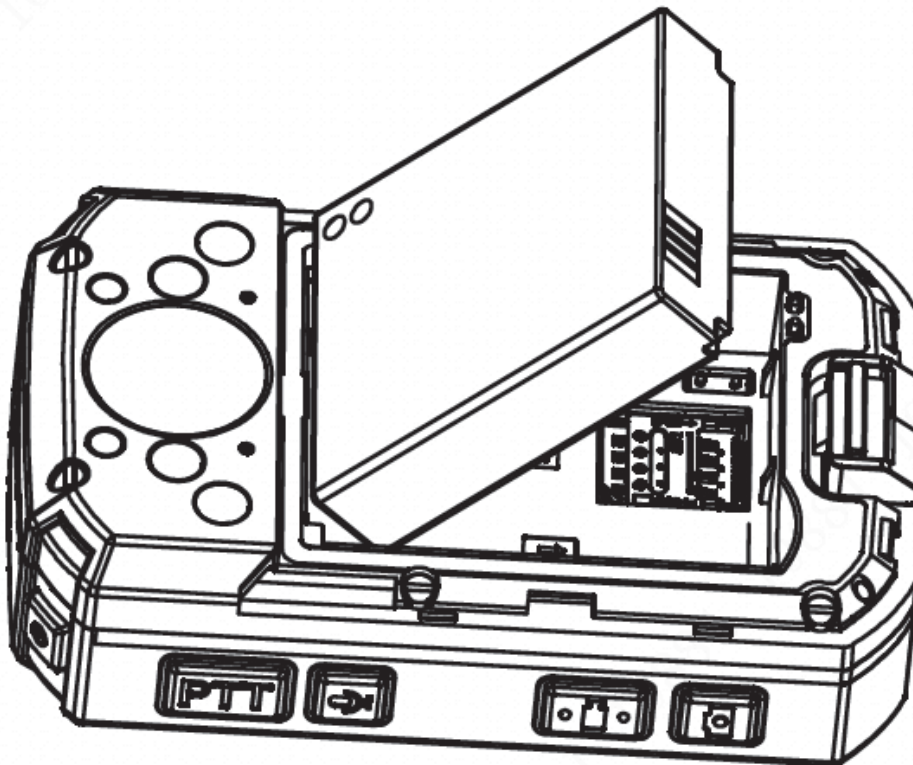
Step 3　Make sure that the metal contact of the SIM card is facing downwards. Follow the directions on Figure 4-3 to push the SIM card to the tray until the SIM card is firm.

Figure 4-3 Install the SIM Card
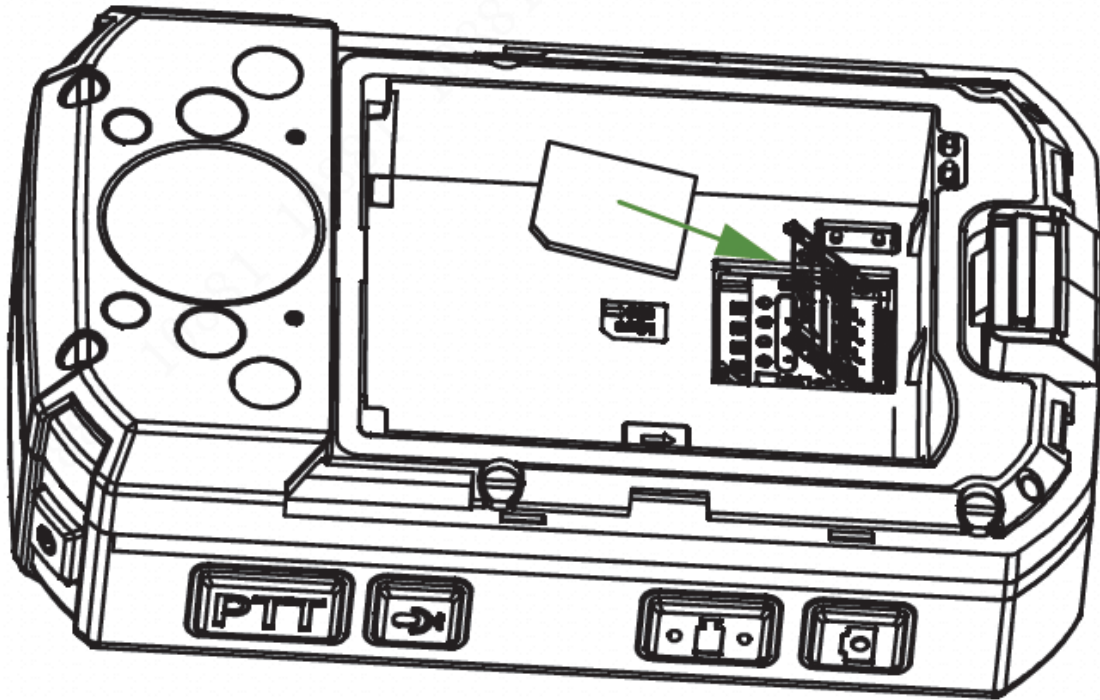
Step 4 Install the main battery.

📖

Install the SIM card first, and then install the main battery in case the battery jams the tray and results in tray damage.

Step 5 Pull down the battery cover lock on the back of the Device to install the battery cover.

4.2 Replacing the Main Battery

For details, see Step 1, Step 2, Step 4 and Step 5 in "4.1 Installing SIM Card."

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.
- It is recommended that you enable your device's firewall or blacklist and whitelist feature to reduce the risk that your device might be attacked.