KIT1021

User Guide

Kingtent

Kingtent

Website: https://www.Kingtent.com

About This Document

This document describes the functions and basic operations of the body worn camera KIT1021.

Product Version

This document is applicable to the KIT1021 of the following versions.

Product Name	Product Version
KIT1021	

Intended Audience

This document is intended for:

- Common user
- System engineers
- Field engineers

Organization

1 Change History

This chapter describes changes between document versions.

2 Safety Information

This section contains important information pertaining to the operating instructions of your device. It also contains information about how to use the device safely. Read this information carefully before using your device.

3 Product Description

This chapter describes the appearance, buttons, indicators, specifications, certifications, and accessories of the KIT1021.

4 Hardware Installation

This chapter describes how to install the hardware of the KIT1021.

5 Software Commissioning

This section describes how to commission the KIT1021.

6 Operation and Maintenance

This chapter describes the operation and maintenance of the KIT1021 and how to use it.

7 Security Management

This section describes the product security of the KIT1021 and related security configurations.

8 Appendix

The appendix provides related information for your reference.

Conventions

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
⚠ DANGER	Indicates a hazard with a high level of risk which, if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a hazard with a medium level of risk which, if not avoided, could result in death or serious injury.
⚠ CAUTION	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.

NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
NOTE	Supplements the important information in the main text. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

General Conventions

The general conventions that may be found in this document are defined as follows.

Convention	Description
Times New Roman	Normal paragraphs are in Times New Roman.
Boldface	Names of files, directories, folders, and users are in **boldface**. For example, log in as user **root**.
Italic	Book titles are in *italics*.
Courier New	Examples of information displayed on the screen are in Courier New.

Command Conventions

The command conventions that may be found in this document are defined as follows

Convention	Description
Boldface	The keywords of a command line are in **boldface**.
Italic	Command arguments are in *italics*.
[ ]	Items (keywords or arguments) in brackets [ ] are optional.

{ x | y | ... }	Optional items are grouped in braces and separated by vertical bars. One item is selected.
[x | y | ...]	Optional items are grouped in brackets and separated by vertical bars. One item is selected or no item is selected.
{ x | y | ... }*	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[x | y | ...]*	Optional items are grouped in brackets and separated by vertical bars. Several items or no item can be selected.

GUI Conventions

The GUI conventions that may be found in this document are defined as follows.

Convention	Description
Boldface	Buttons, menus, parameters, tabs, window, and dialog titles are in **boldface**. For example, click **OK**.
>	Multi-level menus are in **boldface** and separated bythe ">" signs. For example, choose **File** > **Create** > **Folder**.

Keyboard Operations

The keyboard operations that may be found in this document are defined as follows.

Format	Description
Key	Press the key. For example, press **Enter** and press **Tab**.
Key 1+**Key 2**	Press the keys concurrently. For example, pressing **Ctrl**+**Alt**+**A** means the three keys should be pressed concurrently.
Key 1, **Key 2**	Press the keys in turn. For example, pressing **Alt**, **A** means the two keys should be pressed in turn.

Mouse Operations

The mouse operations that may be found in this document are defined as follows.

Action	Description
Click	Select and release the primary mouse button without moving the pointer.
Double-click	Press the primary mouse button twice continuously and quickly without moving the pointer.
Drag	Press and hold the primary mouse button and move the pointer to a certain position.

Contents

1 Safety Information

This section contains important information pertaining to the operating instructions of your device. It also contains information about how to use the device safely. Read this information carefully before using your device.

Medical Device

- Follow rules and regulations set forth by hospitals and health care facilities. Do not use your device when using the device is prohibited.

- Implantable medical devices, such as pacemakers, implanted cochleas, and hearing aids may be affected by radio waves generated by this device. If you are using such medical devices, consult their manufacturers for related restrictions. Pacemaker manufacturers recommend that a minimum distance of 15 cm be maintained between your device and a pacemaker to prevent potential interference with the pacemaker. If you are using a pacemaker, use the device on the opposite side of the pacemaker and do not carry the device in your front pocket.

Safety of Children

- Comply with all precautions with regard to children's safety. Letting the child play with your device or its accessories, which may include parts that can be detached from the device, may be dangerous, as it may present a choking hazard. Ensure that children are kept away from the device and accessories.

Potentially Explosive Atmosphere

- Power off your device in any area with a potentially explosive atmosphere, and comply with all signs and instructions. Triggering of sparks in such areas could cause an explosion or a fire, resulting in bodily injuries or even deaths. Do not power on your device at refueling points such as service stations.

- Comply with restrictions on the use of radio equipment in fuel depots, storage, and distribution areas, and chemical plants. In addition, adhere to restrictions in areas where blasting operations are in progress. Before using the device, watch out for areas that have potentially explosive atmospheresthat are often, but not always, clearly marked. Such locations include areas below the deck on boats, chemical transfer or storage facilities, and areas where the air contains chemicals or particles such as grain, dust, or meta powders. Ask the manufacturers of vehicles using liquefied petroleum gas (such as propane or butane) whether this device can be safely used in their vicinity. Do not store or transport the device and accessories in the same container as combustible or explosive gas, liquid or materials.

Traffic Security

- Do not use your device while flying in an aircraft. Power off your device before boarding an aircraft. Using wireless devices in an aircraft may cause danger to the operation of the aircraft and interrupt the wireless telephone network. It may also be considered illegal.

Operating Environment

- Do not use or charge the device in dusty, damp, and dirty places or places with magnetic fields. Otherwise, it may result in a malfunction of the circuit.
- On a stormy day with thunder, do not use your device to prevent any danger caused by lightning.
- Power off your device if using the device is prohibited.
- If the ambient temperature is over high or low, the device may be faulty.

Disposal and Recycling Information

The device (and any included batteries and accessories) should not be disposed of as normal household garbage. Local laws and regulations on the disposal and recycle of such objects should be followed.

Accessories

Use ONLY original batteries, chargers, and accessories supplied by the device manufacturer. The use of any other type of battery, charger, or accessory may invalidate any warranty for the device, may be in violation of local rules or laws, and may be dangerous.

Battery and Charger

- Use ONLY the original charger to charge the battery and equipment.
- Unplug the charger from the electrical plug and the device when not in use.
- Do not connect two poles of the battery with conductors, such as metal materials, keys, or jewelries. Otherwise, the battery may be short-circuited and may cause burns and other bodily injuries.
- Do not place the battery or device near any heating device, such as a microwave oven, an oven, or a radiator. Battery overheat may result in a fire, explosion or other hazard.
- Do not modify or remanufacture, attempt to insert foreign objects into the battery, immerse or expose it to water or other liquids, Otherwise, it may lead to battery leakage, overheat, fire or explosion.

- If battery electrolyte leaks out, ensure that the electrolyte does not touch your skin or eyes. If the electrolyte touches your skin or splashes into your eyes, wash your eyes and skin with clean water immediately and consult a doctor.

- If there is a case of deformation, color change, or abnormal heating while the battery is being used, charged or stored, remove the battery immediately and replace it. Otherwise, it may lead to battery leakage, overheating, explosion, or fire.

- If the power cable is damaged, or the plug loosens, stop using the cable at once. Otherwise, it may lead to an electric shock, a short circuit of the charger, or a fire.

- Do not dispose of batteries in fire as they may explode. Batteries may also explode if damaged.

- A battery subjected to extremely low air pressure that may result in an explosion or the leakage of flammable liquid or gas.

Cleaning and Maintenance

- Keep the device and accessories dry. Do not use microwave oven or other heaters to dry the device.

- Do not place your device, battery, and charger in places where they can get damaged because of collision. Otherwise, it may lead to battery leakage, device malfunction, overheating, fire, or explosion.

- Do not leave your device, battery, and charger in a place with an extreme high or low temperature. Otherwise, they may become faulty, and fire or explosion may be caused.

- Do not place sharp metal objects such as pins near the earpiece. The earpiece may attract these objects and hurt you when you are using the device.

- Do not use any strong chemical detergent, powder, or other chemical agents (such as alcohol and benzene) to clean the device and the charger. Otherwise, parts of the device may be damaged or a fire can be caused. You can clean the device and the charger with a piece of damp and soft antistatic cloth. Power off the device before cleaning or maintenance, and disconnect the charger from the device. Secure the interface cover, and battery cover.

- Do not dismantle the device or accessories. Otherwise, the warranty on the device and accessories is invalid and the manufacturer is not liable to pay for the damage.

- If the device screen is broken by colliding with hard objects, do not touch or try to remove the broken part. In this case, stop using the device immediately, and then contact an authorized service center in time.

- Avoid dropping, knocking, or vibrating the device. Otherwise, the internal circuit and structure may be damaged. If the device or battery is dropped, especially on a hard surface, and the user suspects damage, contact the device manufacturer.

- Keep the port plug and battery cover installed tightly.
- Clear the water from the surface and loudspeaker of the device if it is exposed to water.

2 Product Description

About This Chapter

This chapter describes the appearance, buttons, indicators, specifications, certifications, and accessories of the KIT1021.

2.1 Application Scenarios

This section describes the application scenarios of the KIT1021.

2.2 Appearance

This section describes the appearance of the KIT1021.

2.3 Button Description

This section describes the buttons on the KIT1021.

2.4 Indicators

This section describes the status of indicators on the KIT1021.

2.5 Specifications

This section describes specifications of the KIT1021.

2.1 Application Scenarios

This section describes the application scenarios of the KIT1021.

The KIT1021 is a body worn camera based on the 5G SoC solution. It uses the Android 10.0 open platform to implement 4K HD recording and AI intelligent identification, supporting also the capability to detect and store frontal faces (blacklist faces for matching and recognition) from the body worn camera while performing HD recording, meeting the requirements of low power consumption and long standby time. It can connect to a third-party video platform in compliance with the ONVIF protocol. The KIT1021, with a 2.4-inch touchscreen, supports main and auxiliary cameras and has built-in acceleration sensors, NFC and GIS capabilities, meeting the requirements of routine policing service expansion.

It is widely used in standardizing government law enforcement, such as public security, traffic control, transportation, energy, emergency handling, policing, city management, and market supervision. For example, industry scenarios can be public security law enforcement by civilian police officers, road inspection by traffic police officers, highway law enforcement by road administration personnel, major event security assurance by special police forces, dangerous personnel identification at stations, electric power line inspection, and coal mine blasting inspection.

KIT1021 accesses the online dispatching system through the operator's 3G/4G//5G VPDN to implement services such as real-time online video dispatching, PoC group calls, and GIS positioning.

2.2 Appearance

This section describes the appearance of the KIT1021.

Figure 2-1 shows the appearance of the KIT1021.

Figure 2-1 Appearance of the KIT1021

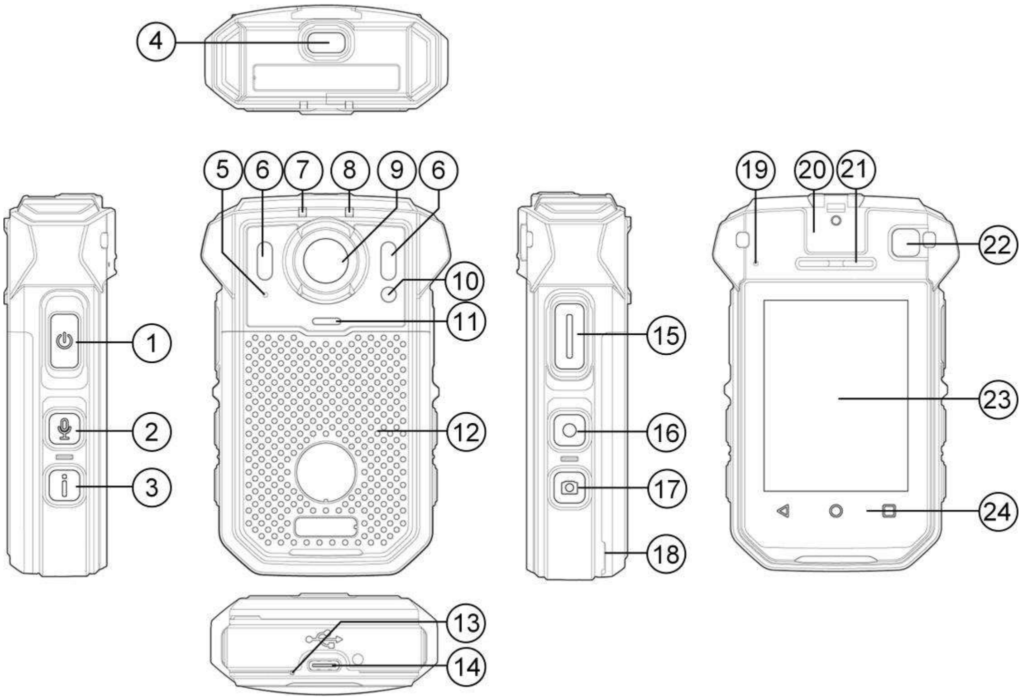


Table 2-1 describes the components of the KIT1021.

Table 2-1 KIT1021 description

No.	Item
1	Power button
2	Voice recording button

3	Mark button
4	Multi-function button (Voice assistant/SOS/Emergency call)
5	Microphone
6	Infrared LED light
7	Indicator 1
8	Indicator 2
9	Main camera
10	Light sensor
11	White LED light
12	Rear cover/Battery
13	Microphone
14	USB port
15	PTT button
16	Video recording button
17	Shutter button
18	Rear cover notch
19	Air escape hole
20	Back clip
21	Speaker
22	Secondary camera
23	Screen
24	Navigation bar

2.3 Button Description

This section describes the buttons on the KIT1021.

Table 2-2 describes the buttons on the KIT1021. For details about the button positions, see **2.1 Appearance**.

Table 2-2 Button description

Item	Press	Press and Hold
Power button	Turn the screen on/off.	● Power on or off the device. ● Press and hold this button for 10seconds to forcibly reset the device.
Video recording button	Start/End a video recording.	Default: Start/End locking the buttons. Optional: Start/End video sending.(Configured through the upper computer/OTA and the body worn camera needs to be restarted to take effect.)
Voice recording button	Start/End a voice recording.	Turn on/off the white light.
Shutter button	Take a photo.	Perform intelligent law enforcement.
Mark button	Add/Cancel a tag to/ from a file.	Turn on/off the infrared light. (Set **Infrared** to **Manual**.)
PTT button	—	Initiate a voice group call.
Multi-purpose button	In compliance with software configurations	In compliance with software configurations
Keyboard	Back/Home/Function key	—

2.4 Indicators

This section describes the status of indicators on the KIT1021.

Table 2-3 describes the status of indicators on the KIT1021. For details about the indicator positions, see **2.1 Appearance**.

Table 2-3 Indicator status

Item	Indicator Status	Description
Indicator 1	Steady green	Charging status: high battery level
	Steady yellow	Charging status: medium battery level
	Steady red	● Charging status: low battery level ● Low battery ● Full storage space
	Blinking yellow	Identification alarm
Indicator 2	Steady green	Power-on/P2P video calling in progress
	Steady red	Video sending/surveillance in progress
	Blinking red	Video recording in progress
	Blinking yellow	Voice recording in progress

2.5 Specifications

This section describes specifications of the KIT1021.

Table 2-4 describes hardware specifications of the KIT1021.

Table 2-4 Hardware specifications

Item	Specifications
Dimensions (H xW x D)	97.8 mm (H) x 63.8 mm (W) x 27.7 mm (D)

Weight	190 g (without back clip)
Screen	2.4-inch color LCD touchscreen
Resolution	240 x 320
Battery capacity	3400 mAH (During battery replacement of 3 min to 5 min, the ongoing recording is not interrupted.)
Camera	● Main camera: 8 megapixels ● Auxiliary camera: 2 megapixels ● Video recording resolution: 3840*2160 (main) 1920*1080(auxiliary) ● Photographing: 64MP
Angle of view	125° (horizontal), 68° (vertical), and 160° (diagonal)
White balance	Supported
Flash	Supported
Infrared night vision	Recognition within 3 m and visibility within 10 m
Storage	4GB RAM + 64GB/128GB/256GB ROM
Speaker power	2 W
Microphone	Dual microphones
Motor	Supported
Positioning	Joint positioning GNSS (including GPS, GLONASS, BDS and GALILEO)
Wi-Fi	2.4 GHz/5 GHz, IEEE802.11 a/b/g/n/ac
Bluetooth	Bluetooth 5.1
NFC	Card mode and reader mode
5G/4G frequencyband	● 5G NR: n1/3/28/41/77/78/79 ● FDD-LTE: B1/B2/B3/B4/B5/B7/B8/B12/B17/B18/B19/B20/B26/B28

	● TDD-LTE: B34/B38/B39/B40/B41
3G/2G frequencyband	● WCDMA: B1/B2/B5/B8 ● GSM: 850/900/1800/1900MHz
Power class	3GPP compliance
Sensitivity	3GPP compliance
External port	Type C USB3.0
SIM card	Physical SIM card (single slot, nano SIM)
Input Voltage	≤ 9V 2A
Operating time (single battery)	Video Recording ≥ 10 hours (30FPS)

Table 2-5 describes software services of the KIT1021.

Table 2-5 Software service functions

Type	Function	Description
Basic functions	OS	Android 10
	Photographing	Takes photos in one press and saves them in JPG format.
	Audio recording	Records audios in one press and saves them in WAV format.
	Video recording	● Records videos in one press and saves them in MP4 format. ● During video recording, you can press a single button to take a snapshot, which does not affect normal video recording.
	Key file flagging	You can press the mark key to mark key files during video recording.

	Browsing and playback	Allows users to browse, retrieve, and play back local video files, audio files, and photos by timeline.
	Operation prompt	Supports operation indication in the form of sound or motor motion and supports indicator status display.
	Alarm reporting	Generates alarms for battery undervoltage and storage overflow. This body worn camera notifies you of the alarms through audio or text prompts.
Wireless Service	GIS service	Supports location information reporting, track playback, and SOS emergency reporting.
	PoC group call	Supports group calls with LTE trunking terminals and other body worn cameras.
	Video sending	● Supports video sending over the 3G/4G/5G wireless network. Encoding format: H.264/H.265. Video sending formats: 4K/25 FPS, 2K/25 FPS, 1080p/25 FPS, 720p/25 FPS, D1/25 FPS, and CIF/25FPS.
	P2P video call	Supports P2P video call.
	P2P voice call	Supports P2P voice call.
AI service	Basic alert deployment with AI face cutouts	Allows a recorder to upload image streams for alert deployment.
	Front-end AI solution	Includes facial recognition and post-recognition processing.

Table 2-6 describes the audio encoding of the KIT1021.

Table 2-6 Audio encoding description

Local voice recording	WAV file, not involving audio encoding

Local video recording	MP4 file, audio encoding AAC
Video sending/Voice intercom	AMR

Table 2-7 describes the environmental and reliability specifications of the KIT1021.

Table 2-7 Environment and reliability specifications

Item	**Specifications**
Operating temperature	–30°C to +55°C
Storage temperature	Main body: –40°C to +60°C Battery (within three months): –20℃ to +45℃
Humidity	Relative humidity: 5% to 95% (non condensing)
IP rating	IP68
Mean time between failures (MTBF)	50,000 hours

3 Hardware Installation

This chapter describes how to install the hardware of the KIT1021.

Replacing the Battery

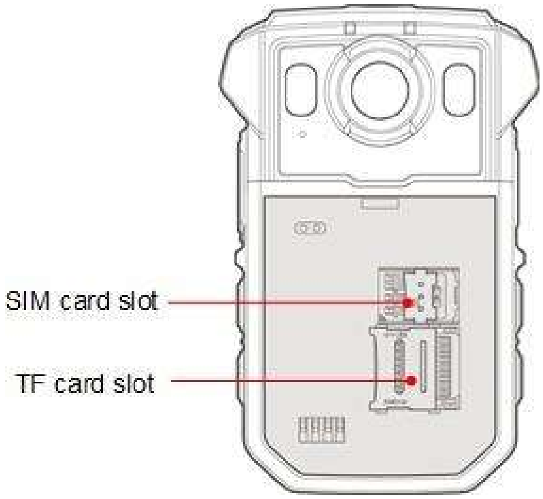
- When replacing the battery, remove the rear cover from the handle and replace the battery. Ensure that the rear cover is properly installed after the new battery is inserted.
- Do not use sharp objects to poke the air escape hole. Otherwise, the water-proofing performance will be affected.
- In order to extend the battery life, the battery needs to be charged regularly. The battery must be charged at least once within three months. Otherwise, the battery may be damaged.

Installing the SIM Card and the TF card

Figure 3-1 shows the position of the KIT1021 card slots.

Attention: TF card slot: used only as an encryption card, which is customized and need working with the specific software.

Figure 3-1 Position of the KIT1021 card slots



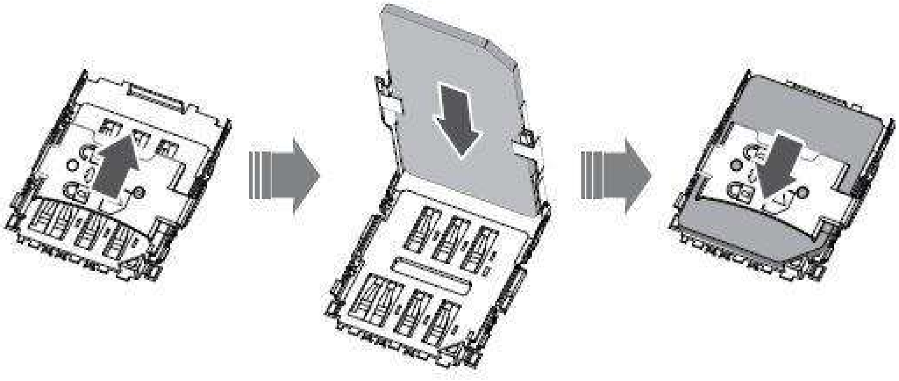
⚠ **CAUTION**

Exercise caution when installing a SIM/TF card. The direction must be correct. Otherwise, the card slot may be damaged.

- Power off the device, remove the battery, and remove the SIM card fastener and the TF card fastener.
- Make sure that the small notch in the corner of the SIM card matches the one in the SIM card slot so that it fits properly. Fasten the card fastener, as shown in **Figure 3-2**.

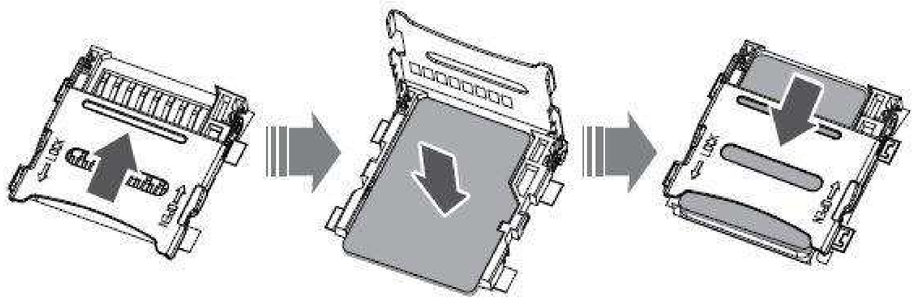
  (The following figure is for reference only. Install the SIM card according to the actual situation. The other SIM card does not need to be inserted into the fastener. Place the SIM card in the slot and fasten the fastener again.)

  Figure 3-2 Inserting a SIM Card



- Make sure that the small notch in the corner of the SIM card matches the one in the SIM card slot so that it fits properly. Fasten the card fastener, as shown in **Figure 3-3**.

Figure 3-3 Inserting a TF Card



Charging with a Charging Stand

When charging the body worn camera with the charging stand, connect it to the charging stand using the power cable delivered with the main equipment.

Table 3-1 describes the indicator status of the charging stand.

Table 3-1 Charging stand indicator description

Indicator Status	Description
Blinking green slowly (blinking once per second)	Ongoing charging
Steady green	Full charge
Steady red	Standby mode
Blinking red (blinking three times per second)	Fault

4 Software Commissioning

About This Chapter

This section describes how to commission the KIT1021.

📖 **NOTE**

Registration and login are required only for online services.

4.1 Scenario Description

The body worn camera solution supports the data collection scenario and online service scenario.

4.2 Initial Passwords

This section describes the initial passwords of the KIT1021 and related systems.

4.3 Commissioning in Online Scenario

This section describes how to commission the KIT1021 in online scenarios.

4.1 Software Commissioning

The body worn camera solution supports the data collection scenario and online service scenario.

Data Collection Scenario

The KIT1021 is connected to the collection station and management background. In this scenario, there is no online service on the bodyworn camera.

- The collection station supports data collection, data clearing, charging, time calibration, as well as the local caching of audio and video data of the body worn camera and upload of these data to the management center.

- The background management system is usually deployed in the data center. This system connects to the collection stations deployed in branches to manage all collection stations, body worn cameras, and users. The background management system automatically obtains the audio and video data stored on the collection station, as well as stores and manages it.

Online Service Scenario

The KIT1021 implements real-time online video dispatching, PoC group call, and GIS positioning after connecting to the online dispatching system.

4.2 Initial Passwords

This section describes the initial passwords of the KIT1021 and related systems.

Initial device and system passwords

Table 4-1 lists the initial passwords of a body worn camera.

Table 4-1 Initial passwords of the body worn cameras

Device Model	Description	Initial Password
KIT1021	Common users: ● Entered when replay device stores files (optional, configured on the upper computer) ● Upper computer software connection and configuration	None. It needs to be configured by the user.
	Administrator: ● Upper computer software connection and configuration	888888 When a body worn camera needs to connect to the software, the password cannot be changed.

NOTE

To ensure system security, change the initial password in a timely manner after the system commissioning and remember the new password.

During routine maintenance, change the password periodically and remember the new password.

4.3 Commissioning in Online Scenario

This section describes how to commission the KIT1021 in online scenarios.

NOTE

Before commissioning in online scenarios, ensure that all network-side devices have been commissioned and all services are running properly. For example, P2P calls, group calls, and video sending can be performed between terminals that have been commissioned on the same network.

4.3.1 Registration on the Network

This section describes how to register the KIT1021 with the dispatching system.

Context

- On the network, register the body worn camera with the dispatching system.
- The following table describes the differences when the body worn camera accesses networks of different versions.

Table 4-2 Accessing networks of different versions

User type	**Mobile Terminal Users**
Service capability (terminal user)	● Select the options based on site requirements. ● Select **Login ThroughPublic Network UEs**.

Procedure (Using a Public Network SIM Card or Wi-Fi)

Step 1: Register a terminal.

1. Log in to the dispatching system
2. Choose **Registration > Terminal Management > UE**. The **UE** page is displayed.
3. Click **New**. Set related parameters
4. Click **OK**. A message is displayed, indicating that the operation is successful.
5. Click **Confirm**

Step 2: Register a user.

1. Log in to the dispatching system
2. Choose **Registration > User Management > Mobile Terminal Users**. The **Mobile Terminal Users** page is displayed.
3. Click **New**. Set related parameters
4. Click **Confirm**

---End

4.3.2 Application Login

This section describes how to log in to the Application. When the Application runs on the device, you must log in to the Application.

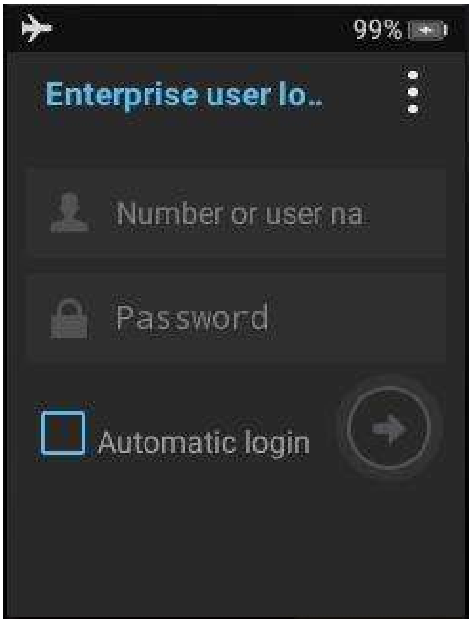
Context

- Before using trunking services, you must log in to the system.
- Ensure that you have connected to the network during login.
  - Using a public SIM card to access: The public SIM card can properly access the carrier network and use data functions. In addition, public network access configurations have been completed on the application server.
  - Using other Wi-Fi access points to access: The device accesses the network through other Wi-Fi access points, and related configurations have been completed on the application server.

Procedure

Step 1 On the main screen of the device, click the app icon to start application. Figure 4-1 shows the login page.

Figure 4-1 Login dialog box



Step 2 Touch⋮, select Server Settings and set parameters for the authentication server. You can set the Primary IP Address and Secondary IP Address. The Primary IP Address must be filled in. Table 4-3 describes the parameters.

Table 4-3 Parameters related to the authentication server

Parameter	**Description**
IP address or domain	Specifies the IP address or domain name of the authentication server. Set this parameter based on the actual condition.
Port number	Specifies the port ID. Set this parameter based on the actual condition. The default value is **8013**.

Step 3 Enter login parameters, which are described in Table 4-4.

Table 4-4 Login parameters

Parameter	Description
Number or user name	A valid short number or user name that has been registered in the system.
Password	A login password that corresponds to the user name.
Automatic login	When this option is selected, automatic login is allowed next time.

Step 4 Touch → to login.

----End

- If the user name and password are correct, the application page is displayed.
- If the password of a user name is incorrectly entered for five consecutive times, the user name will be locked for 30 minutes by default. The lockout times and time period are configurable on the server.
- If you forget your password, contact the network administrator to reset the password.

5 Operation and Maintenance

About This Chapter

This chapter describes the operation and maintenance of the KIT1021 and how to use it.

5.1 Home Screen and Apps

This section describes the home screen and apps of the KIT1021.

5.2 General Recording Settings

This section describes general recording parameter settings of the KIT1021.

5.3 Photographing

This section describes how to use the KIT1021 to take a photo.

5.4 Voice Recording

This section describes how to use the KIT1021 to perform voice recording.

5.5 Video Recording

This section describes how to use the KIT1021 to perform video recording.

5.6 Online Evidence Archiving

This section describes how to set online evidence archiving on the KIT1021.

5.7 Setting Replay Password

This section describes how to set the replay password of the KIT1021.

5.8 Setting Positioning Mode

This section describes how to set the positioning mode of the KIT1021.

5.9 Application Operations

This section describes how to perform the Application services.

5.10 Smart Services

This section describes smart services provided by the KIT1021 and related operations.

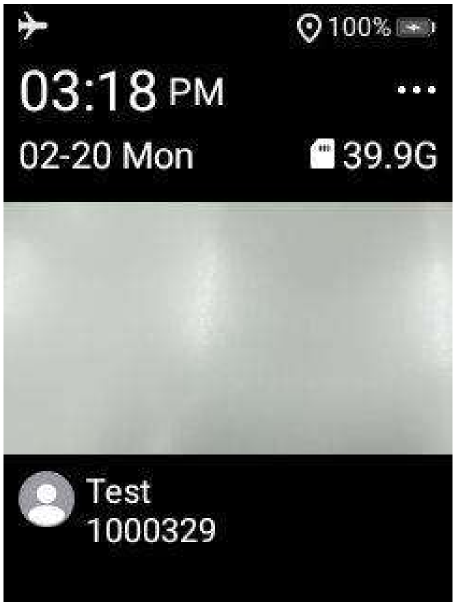
5.11 Remote Configuration

5.1 Home Screen and Apps

This section describes the home screen and apps of the KIT1021.

Figure 5-1 shows the home screen of an KIT1021.

Figure 5-1 KIT1021 home screen



5.2 General Recording Settings

This section describes general recording parameter settings of the KIT1021.

Table 5-1 describes the general recording parameter settings.

Table 5-1 General recording parameter settings

Item	Description
Settings > **Shooting** > **Video Recording**	After the switch is turned on, the video is uploaded and recorded simultaneously.
Settings > **Shooting** > **Facial/License Plate Recognition**	After the switch is turned on, AI identification is performed simultaneously with video recording.

Item	Description
Settings > **System >Voice settings**	After the switch is turned on, there are voice prompts when you take photos or record videos.
Settings > **Shooting > Watermark**	Watermark information can be set. Photos and videos will be automatically watermarked.

5.3 Photographing

This section describes how to use the KIT1021 to take a photo.

Prerequisite

The home screen is running properly

Context

The related parameters are as follows:

Settings > **System >Camera Settings**	Set the camera mode used in different scenarios. The options are **Ultra-long Standby Time**, **Image Stabilization** and **Ultra-wide angle**.
Settings > **Shooting** **> More > Photo size**	Set the photo resolution. The options are **8M**, **16M**, **24M**, **32M** and **64M**, which correspond to 3840 × 2160,5312 × 2988, 6528 × 3672, 7552 × 4248 and 10688 × 6012.

Settings > Shooting **> More > Delayed photograph**	Set the delay time for taking photos. The options are **Disable**, **3 seconds** and **5 seconds**.

Procedure

- Taking photos

Press 📷 on the body worn camera to take a photo.

- Viewing photos

  a. Return to the system home page and click the application icon to start the Replay

  b. (Optional) Enter the password of a common user.

5.4 Voice Recording

This section describes how to use the KIT1021 to perform voice recording.

Prerequisite

The home screen is running properly

Procedure

- Recording the voice

  Press 🎙 on the body worn camera to start voice recording.
  Press the button again to stop recording.

- Viewing voice recording files

  a. Return to the system home page and click the application icon to start the Replay.

b. (Optional) Enter the password of a common user.

c. Select **Voice** in the drop-down options.

5.5 Video Recording

This section describes how to use the KIT1021 to perform video recording.

The following describes the storage usage of each recorder, which relates to different resolutions and compression mode.

Assuming 8 hours per shift, the storage usage is about:

Video resolution	Compression mode	
	H264	H265
2k	30 GB	15 GB
1080p	15 GB	7.5 GB
720p	7.5 GB	3.8 GB

Prerequisite

The home screen is running properly

Context

The related parameters are as follows:

Settings > **System >Camera Settings**	Set the camera mode used in different scenarios. The options are **Ultra-long Standby Time**, **ImageStabilization** and **Ultra-wide angle**.
Settings > **Shooting > Encoding format**	Set the encoding format for video recording. The options are **H.264(good compatibility)** and **H.265(high compression rate)**.
Settings > **Shooting > Resolution**	Set the video resolution. The options are **D1, 720P,1080P**, **2K** and **4K**.

Settings > Shooting >More > Frame rate	Set the video frame rate. The options are **25** and **30**.
Settings > Shooting > File segmentation	Set the time segment according to which a video is saved during video recording. If the segment duration exceeds the preset threshold or the file size reaches 3.6 GB, the video is stored in multiple files. The options are 5 minutes, 10 minutes, 20 minutes, 30 minutes and 60 minutes.
Settings > Shooting > More > Pre-record	Set the pre-recording duration, specifically, the duration from the time when the recording starts to the time when you press the video recording button. The options are Disable, 5 seconds, 10 seconds, 15 seconds, 30 seconds, 60 seconds and 120 seconds (When the resolution is set to 4k, the pre- recording time of 120s is not provided).
Settings > Shooting > More > Delayed record	Set the delayed recording duration, specifically, the duration from the time when you press the video recording button to the time when the recording stops. The options are Disable, 3 seconds, 5 seconds, 10 seconds, 15 seconds, 30 seconds, 60 seconds and 120 seconds.
Settings > Shooting > More > Video compression	After the switch is turned on, the video compression efficiency is improved by 10%, but the key frame interval is increased to more than 3s. During video playback, you can only drag the key frame at an interval of 3s.

Procedure

- Recording the video

Press on the body worn camera to start recording videos.

Press the button again to stop recording.

Locking the buttons

During video recording, press and hold the video recording key to enable the lock key.

- To prevent accidental touch, short presses of the video/voice recording buttons do not take effect.
- Control by voice control or other means is not affected by the lock buttons function.
- When the lock buttons takes effect, press and hold the video recording key again to exit the lock buttons.

Marking important video time points

During video recording, important events such as events transmitted by bluetooth, SOS, emergency, and AI alarms, can be marked. In addition, the dotting information can be played on the evidence management software.

- The **Video Dotting Switch** needs to be enabled on the upper computer software. The switch is disabled by default.
- Ensure that the video recording service has been started.

Viewing videos

a. Return to the system home page and click the application icon to start the Replay.

b. (Optional) Enter the password of a common user.

c. Select **Video** in the drop-down options.

d. If there is a dotting event, the dotting information will be displayed on the progress bar when replaying.

e. On the video playback page, touch the menu icon in the upper right corner and you can select a speed (0.5x, 1x (default), 2x, 4x, 8x, 16x, 32x,or 64x).

5.6 Online Evidence Archiving

This section describes how to set online evidence archiving on the KIT1021.

NOTE

This section describes only the operations performed on the body worn camera. This function can be used only with the centralized evidence management platform. The standalone collection software is not supported.

Context

- Online evidence archiving allows you to upload evidence files in real time without connecting to the collection station.
- The body worn camera can only archive trust list files online. If a file is not in the trust list, a notification is displayed and the file cannot be played. The current trust list file format is MP4, XML, GPI, M4A, WAV, and JPG.

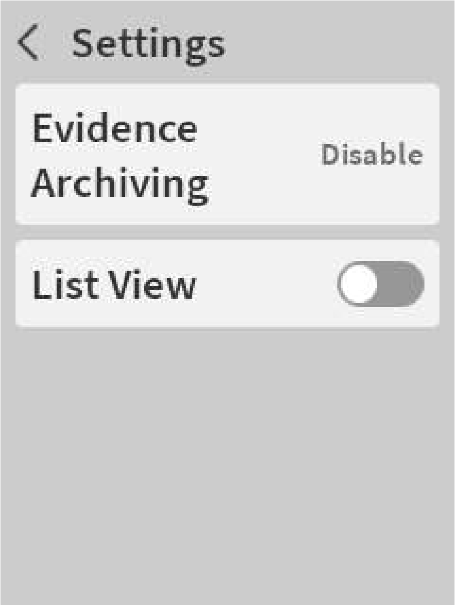
Procedure

Step 1 Click the **Replay** on the system home page.

Step 2 (Optional) Enter the password of a common user.

Step 3 Click the setting icon in the upper right corner. The option is displayed as shown in **Figure1 The option of evidence archiving**.

Figure 5-2 The option of evidence archiving



Settings

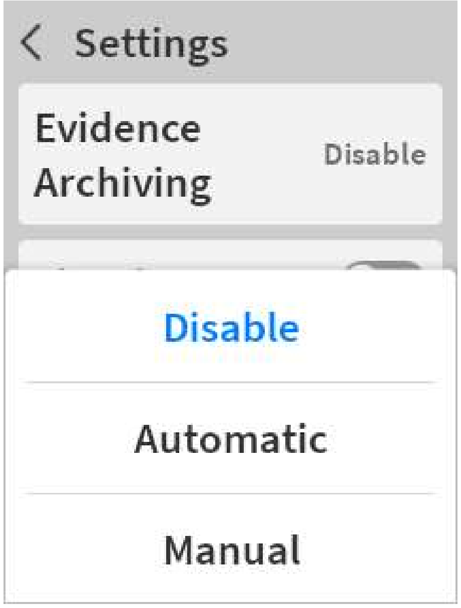
Evidence Archiving Disable

List View ○

Step 4 Click **Evidence Archiving** and select **Disable, Automatic**, or **Manual** as required.

As shown in Figure **5.3**.

Figure 5-3 Set the parameter



Settings

Evidence Archiving: Disable

----End

Temperature Control

The KIT1021 supports temperature control for online evidence archiving. When the internal temperature is higher than a certain level, online evidence archiving is suspended. After the temperature decreases to the specified level, online evidence archiving starts again.

The temperature control function is enabled by default. You can set the temperature control switch, temperature level, and hysteresis time on the upper computer software.

When the remaining storage space of the body worn camera is less than 2 GB, the temperature control mechanism is automatically stopped.

5.7 Setting Replay Password

This section describes how to set the replay password of the KIT1021.

Context

The following table lists the initial passwords of a body worn camera.

Table 5-2 Initial passwords of the body worn cameras

Device Model	Description	Initial Password
KIT1021	Common users: ● Entered when replay device stores files (optional, configured on the upper computer) ● Upper computer softwareconnection and configuration	None. It needs to be configured by the user.
	Administrator: ● Upper computer software connection and configuration	888888 When a body worn camera needs to connect to the software, the password cannot be changed.

Body Worn Camera Operations

The common user password cannot be changed on the body worn camera by default. However, if the **Evidence Password Setting Switch** is enabled on the upper computer software, the common user password needs to be entered for replaying files, and the password can be set as follows:

- When you log in to the Replay for the first time, you can set a common user password.
- Choose **Change Password** from the menu in Replay.

Upper Computer Software Operations

- After logging in to the upper computer software, a common user can change the password.
- After logging in to the upper computer software, an administrator can reset the password of a common user.

5.8 Setting Positioning Mode

This section describes how to set the positioning mode of the KIT1021. The

KIT1021 supports joint positioning.

- You can set the positioning mode by the upper computer or OTA. For details, see **Location mode.**
- You can choose **Settings > System > Positioning** on the body worn camera to view the current positioning mode.

5.9 Application Operations

This section describes how to perform the Application services.

NOTE

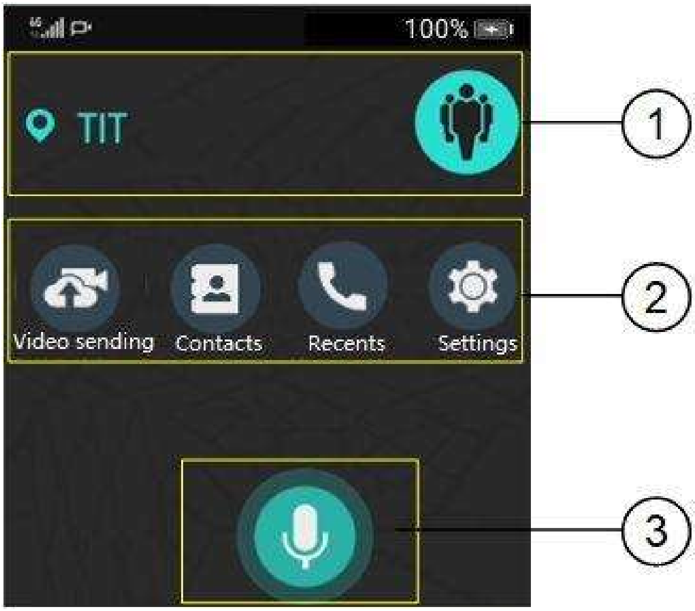
- The icons and parameters in this document may be different from those of the actual situation due to the upgrade of product software. In this case, operation and maintenance should be based on the actual software environment.
- Some functions are controlled by the network side through the authority. Please refer to the actual software environment.
- The function of the **soft PTT key** can also be realized through the **PTT key** on the recorder body.

5.9.1 Application Home Screen

This section describes the Application home screen.

Figure 5.4 shows the Application home screen.

Figure 5.4 Home screen of the Application



1 Group function module
2 Application shortcuts
3 Soft Push To Talk (PTT) key

5.9.2 Application Settings

This section describes how to customize Application settings.

On the home screen of the Application, click ⚙.

Account

The Application can be used by different users. An account is required to authenticate with the network side to perform services.

- Select **Settings**>**Account**, You can view the current account's details, or set the current account's status. The user status is **online** or **offline**. When the user's status is **online**, other status values can be set. Status values are distributed by the serving network.

- Click **Change the password** to change the current account password.
- Turn on **Remember me**. If you do not log out, you do not need to enter the **username** and **password** next time.
- Click **Logout** to log out the current account.

Heavy-traffic service reminder on a mobile network

General > Heavy-traffic service reminder on a mobile network: After this switch is turned on, a dialog box is displayed each time a heavy-traffic service is initiated. After this function is disabled, no confirmation reminder is displayed when a heavy-traffic service is initiated.

The mobile network is used preferentially

General > The mobile network is used preferentially: After this switch is turned on, if both the mobile network and Wi-Fi are available, the mobile network is preferred, which may cause high mobile data usage.

Voice and Vibration

- **General** > **Voice**: If you turn on the switch, there will be a voice when there is an incoming call or a new message. The voice is controlled by the terminal system at the same time.
- **General** > **Vibration**: If you turn on the switch, the phone will vibrate when there is an incoming call or new message.

Skip Non-scanned Group

- **General > Skip Non-scanned Group**: this switch is turned off by default, non-scanned groups are not skipped during group switching. After this switch is turned on, non-scanned groups are skipped during group switching.

Enable HD P2P video call

- **General** > **Enable HD P2P video call**: When the terminal initiates a video call, after you turn the switch on, the phone will support 720P video call, which takes effect only for the dispatching console and video conference. After this function is enabled, frame freezing and artifacts may occur due to limited device performance.

About

- Version update: check the current software version and update it to the latest version.
- General: including log uploading, notification of heavy-traffic services on mobile networks, and preferential use of mobile networks.
- Trunking service statement: view the statement of the trunking service.

5.9.3 Voice Service

This section describes how to perform voice services using the Application.

5.9.3.1 PTP Voice Call

This section describes operations related to PTP calls performed on Application.

Procedure

Receiving a PTP Voice Call

a. When a PTP voice call is incoming, the home screen of a Application displays call initiator information. Click 📞 to receive the PTP voice call.

b. After a call is connected, you can set the following parameters: Mute.

c. After a PTP voice call is complete, click 📞 on the home screen to terminate the call.

Making a PTP Voice Call

a. On the Application screen, click 📞.

b. Making a PTP Voice Call using one of the following methods:

- Enter **Dialer** and enter a call number, then click 📞 on the homescreen to initiate a PTP voice call.
- Enter **Recents** and select a PTP voice call record for redialing.
- Enter **Recents**, select a call record, and then click ⓘ to view the details and touch a phone number to initiate a PTP voice call.
- Enter **Contacts**. select a contact number to view the details and initiate a PTP voice call.

c. After the PTP voice call is connected, you can set the call-related parameters.

d. After a PTP voice call is complete, click ☎ on the home screen to terminate the call.

5.9.3.2 Group Call

This section describes operations related to trunking group calls performed on Application in trunking mode.

Selecting a Group

Before making a group call, a user must select a group. After a user logs in to the Application, the user joins the default group automatically.

The group scanning list of the Application is enabled by default. The Application scans groups in the list and listens to the group with the highest priority.

(Optional) Group Category Switching

If group categories are configured, the current group category switching can be performed.

On the home screen of the Application, click 👤 to switch the group category.

Making a Group Call

- Hold down the **soft PTT key** to initiate a group call when Application is in standby state. Upon initiating a group call, you own the floor by default as the call initiator. Release the **soft PTT key** to release the floor.

- When your Application is listening to a group call, hold down the **soft PTT key** to request the floor:

  - If no one is speaking in the group, you can speak after the floor is granted. Release the **soft PTT key** to release the floor.

  - If someone is speaking in the group, your request will be rejected if your priority is lower than the speaker, or else you can speak after the floor is granted if your priority is higher than the speaker. Release the **soft PTT key** to release the floor.

Receiving a Group Call

The Application in standby state or listening to a group automatically receives calls in a subscribed group. When receiving a group call, the Application's home screen displays group and speaker information. Or when the Application is in the talk state, if there is a high priority group call in the account groups, the group call can also be accepted.

5.9.4 Video Service

This section describes the operations of the video service on the Application.

5.9.4.1 Video Call

This section describes operations related to video calls performed on Application.

Procedure

Answering a Video Call

a. When a video call is incoming, click the home screen icon ☎ to receive the video call.

b. After a call is connected, you can set the following parameters: Mute, close local video.

c. After a PTP video call is complete, click ☎ on the home screen to end the call.

Making a Video Call

a. On the home screen, click ☎.

b. Use one of the following methods to make a PTP video call:

- Enter a call number on the **Dialer**, click ☎.
- Enter **Recents**. Select a PTP video call number for redialing.
- Enter **Recents**. Select a call record and click ⓘ to view details, click ☎.
- Touch **Contacts**. Select a contact number to view the details, click ☎.

c. After the PTP video call is connected, you can set the call-related parameters. For details, see **Answering a Video Call**.

d. After a PTP video call is complete, click ☎ on the home screen to terminate the call.

5.9.4.2 Video Sending

This section describes operations related to real-time video sending and local recording and uploading performed on Application.

Procedure

Real-time video sending

Step 1 On the home screen, click ⬆ to enter the video sending application. Icons in the operation bar are listed in Table 5-3.

Table 5-3 Icons in the operation bar

Icon	Function
⚙	Set video sending parameters.
⬆	Initiate video sending.
⭱🕒	View the video sending history.

Step 2 Click ⚙ to set video sending parameters. The parameters are described in Table5.4.

Table 5-4 Parameter descriptions

Parameter	**Description**
Automatic answer of video return	If the switch is turned off, you need to confirm when handheld terminal send a video surveillance request over your UE.
Sending number	● In the enhanced mode, the default number is configured on the dispatching system. If this parameter is not configured on the dispatching system, it is not displayed. In other modes, the default number is **99999500**. ● If you select **Archive video**, videos are directly uploaded to the recording server of the dispatching system. ◆ This parameter is unavailable when the network side does not support this function. ◆ On the dispatching system, set the dispatching console number by following the instructions provided in section *Configuring One-Click Upload* in *dispatching system Product Documentation*. Videos will be sent to the recording server connected to the dispatching system to which the dispatching console number is logged.
Resolution	Specify the resolution.
White balance	Specify the white balance.
Restore to defaults	Restore parameters to defaults.

Step 3 Click ● to initiate video sending.

----End

Local recording and uploading

Step 1 Turn on the **Recorder Local Recording Switch** (If this switch is not turned on, the related settings are invisible.)

Step 2 On the home screen, click to enter the video sending application. Icons in the operation bar are listed in **Table 5-5**.

Table 5-5 Icons in the operation bar

Icon	Function
⚙	Set video sending parameters.
	Initiate video sending.
	View the video sending history.
🖼	Local recording library, which allows to view and share local recordings.

Step 3 Click ⚙ to set local recording parameters. The parameters are described in **Table 5-6**.

Table 5-6 Parameter descriptions

Parameter	Description
Record if network abnormal	If the switch is turned on, local video recording is automatically performed when there is no network connection.
Display video label	If this switch is turned on, local recording can be performed.
Preferred Save Location	Set the preferred storage location of the file.

Step 4 On the video sending page, click **Video** to switch to the local recording page. Click ● to start local recording.

Step 5 Click 🖼 to view the local recording files. Click **Share** to upload the file.

----End

5.10 Smart Services

This section describes smart services provided by the KIT1021 and related operations.

5.10.1 AI Recognition

KIT1021 can perform AI recognition of faces and license plates. This section describes how to perform facial recognition as an example. The license plate recognition operations are similar.

Context

The requirements for the image files used as the base library files are as follows:

Table 5-7 Base library photo requirements

Category	**Requirement**
Image format	.bmp, .dib, .jpe, .jpeg, .jpg, .png
File size	35 KB to 60 KB
Color depth	Minimum 8-bit grayscale image
Image quality	The face in the image is clear, and the image is not blurred due todefocus or motion. The face is not covered by sunglasses, masks, scarves, or other objects. The face resolution is between 80 x 80 and 200 x 200 pixels. The distance between eyes must be at least 60 pixels. A distance over 90 pixels is recommended.
Posture	PTZ rotation angle/Tilt angle/Posture angle: –10° to +10°.

Glasses	Eyes are not blocked due to reflection of glasses or thick frames.
Illumination	The ambient illumination is at least 300 lux. The light is even. No backlight exists.
Accessories	The accessories should not block the face.
Facial expression	The facial expression is normal, and there is no laugh expression on the face.

The classification of the recognition result is as follows:

Table 5-8 Classification prompt description

Level	**Audible and visual prompt**	**Description**
Level 1 (Urgent)	Beep tone + vibration + red light blinking + white light steady on	● Sound, vibration, and light blinking: Stop after 10s or after the user views the notification message. ● White light: The indicator is turned off after 10 seconds or after the user presses and holds the recording button.
Level 2 (Important)	Beep tone + vibration + yellow light blinking	Sound, vibration, and light blinking: Stop after 10s or after the user views the notification message.
Level 3 (Minor)	Beep tone + green light blinking	Sound and light blinking: Stop after 10s or after the user views the notification message.
Level 4 (Prompt)	vibration	vibration: Stop after 10s or after the user views the notification message.

NOTE

In the local recognition scenario, the recognition result prompt levels is set on the base library files and the default level is 4. In the cloud recognition scenario, the prompt levels is set on the server.

Procedure

This section uses the local facial recognition as an example.

Step 1 Prepare the image file in the base library: Use the Excel template tool to fill in information, generate the file index file, and compress the file index file and photo file into a .zip file (other formats than .zip are not supported).

- Ensure that the base library files are packaged directly without subfolders. For example, face.zip -> base library file, but not face.zip -> face -> base library file.
- A maximum of 2000 face images can be imported into the face library.
- Contact technical support to obtain the Excel template.

Step 2 Configure parameters on the upper computer software. Click **System Settings**, select **Smart Service Parameters**, and click **Edit** in the upper right corner to set the parameters.

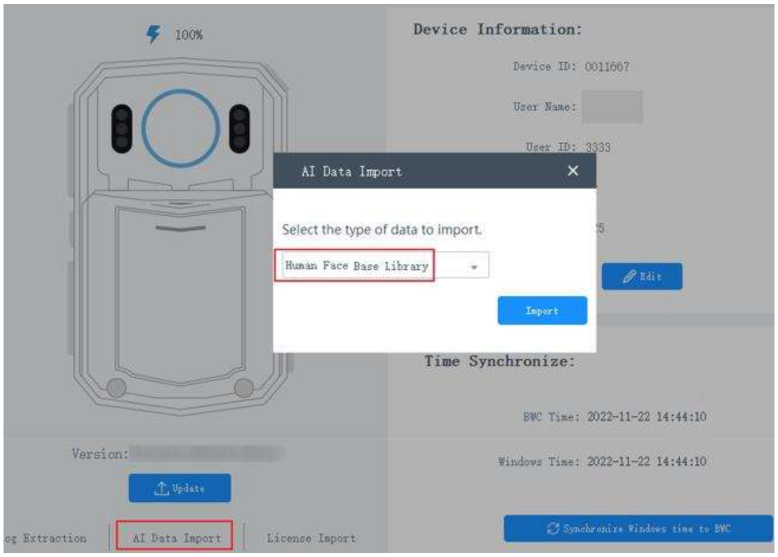
Table 5-9 Parameter Description

Parameter Name	Value
AI Recognition Mode Menu	Display
AI Recognition Mode	Local
Local Recognition Type	Facial recognition
Face list type	Set the value to **Blacklist** or **Whitelist** as required.
Face whitelist alarm threshold (%)	Set the value as required.
Face blacklist alarm threshold (%)	Set the value as required.

Step 3 Use the upper computer to import the face whitelist or blacklist image file to the body worn camera.

- Connect the upper computer to the body worn camera and log in to the upper computer software. Choose **AI Data Import** from the menu and select **Human Face library** for the file type, as shown in Figure 5-5.

Figure 5-5 Importing the image file - Human Face library



100%

Device Information:

Device ID: 0011667

User Name:

User ID: 3333

AI Data Import

Select the type of data to import.

Human Face Base Library

Time Synchronize:

BWC Time: 2022-11-22 14:44:10

Windows Time: 2022-11-22 14:44:10

Version: [redacted]

Step 4 On the body worn camera, you can set AI recognition parameters as follows:

- On the system home page of the body worn camera, choose **AI** function**, select Recognition Mode** (Ensure that AI Recognition Mode Menu is set to Display).

Step 5 On the body worn camera, perform the following operations to enable facial recognition.

- Press and hold the camera button to enable automatic recognition.
- On the screen, enable **AI-based Law Enforcement**.

On the screen, you can view the recognition result in the alarm list.

- Whitelist: A whitelist notification is triggered when the similarity between the locally recognized face and that in the whitelist is higher than this threshold.
- Blacklist: A danger alarm is triggered when the similarity between the locally recognized face and that in the blacklist is higher than this threshold.

----End

5.11 Remote Configuration

This section describes how to query and modify the parameter settings of specified KIT1021.

Prerequisites

- The specified KIT1021 is in the service area of an enterprise network and works properly.
- The dispatching system server works properly, and terminal management client can connect to the server properly.

Procedure

Step 1 Log in to the terminal management client.

Step 2 On the menu bar, choose **OTA** > **UE Config Query And Modify**. The **UE Config Query And Modify** page is displayed.

- Set **Type** to **Platform** or **App**.
- Enter the short number of the body worn camera to be queried in the textbox.

Step 3 Click **Query**.

Step 4 Select and modify the parameters to be reconfigured and click **Send**.

🕮 **NOTE**

Only the checked parameters are delivered to the terminal. The unchecked parameter settings are invalid.

Step 5 After the configuration parameters are downloaded, the configuration takes effect immediately. Modifying some parameters may cause body worn camera services to be interrupted.

----End

6 Security Management

About This Chapter

This section describes the product security of the KIT1021 and related security configurations.

6.1 Product Security

This section describes the product security of the KIT1021.

6.2 Security Configuration

This section describes security configuration of the KIT1021.

6.1 Product Security

This section describes the product security of the KIT1021.

User Data and Sensitive Data Protection

- KIT1021 does not remove user data in upgrades or updates. Instead, the application software performs smooth processing for the existing data.
- The log collection function of KIT1021 may involve user personal data (such as short numbers and IP addresses) due to product maintenance requirements.

Transmission Channel Encryption

- Device authentication, user authentication, and user management of KIT1021 are implemented over HTTPS to ensure data security.
- KIT1021 login is implemented over HTTPS.
- Video services of KIT1021 are transmitted over the SIP/RTP/RTCP standard protocol, and the protocols support encryption.
- Push channels of KIT1021 are transmitted over the TLS-encryption-based XMPP protocol.

Password Management

- Administrator Password and Replay Password of KIT1021 meet the password complexity requirements.
- Application user names and passwords for login are encrypted and stored in KIT1021. When a user attempts to change the password, the user must enter the old password. The password complexity rules are as follows:
  - A password must contain 6 to 18 characters.
  - The password must combine two or more types of characters among uppercase letters, lowercase letters, numbers, and special characters.
  - Spaces, consecutive percent signs (%%), and special characters such as " ' , ; = & are not allowed in a password.
- Brute-force cracking prevention for login: The administrator password, replay password, or cluster account will be locked if the number of failed the application software login attempts by this account exceeds a specified threshold.

Privacy Tips

The KIT1021 supports the ambience listening function. The administrator can remotely initiate the function through the dispatching console without the user's perception to listen to the environmental sound of the KIT1021.

Others

If user uses a third-party root brushing machine or uses an unauthorized operating system to update the operating system, there will be risks for the operating system.

6.2 Security Configuration

This section describes security configuration of the KIT1021.

Enabling/Disabling Permissions on Trunking Services

Administrators enable or disable permissions on trunking services using the dispatching system. The permissions include GIS reporting, initiating video uploading, SIP encryption, and SRTP encryption.

After permissions on trunking services are disabled, trunking services are unavailable to the KIT1021.

After permissions on trunking services are enabled, trunking services are available to the KIT1021.

Usage Declarations

GIS information reporting: For production scheduling purposes, the organization or enterprise where a user belongs can collect user location information when the location service is disabled after the user is informed of the user through the employment contract or company rules and regulations. In addition, when a subscriber is in an emergency, the location information of the subscriber is automatically reported when the subscriber makes a call in emergency mode. Please comply with local laws and regulations when using.

Using information about the IMEI, IMSI, and short number: The enterprise that provides the enterprise network service can view information about the KIT1021, such as the IMEI or version information, on the enterprise server. The KIT1021 registers with the enterprise server together with the IMEI, IMSI, and short number of users. However, the information about users is used only for UE authentication, user authentication, UE permission update, and user permission update. You must comply with the local laws and regulations when using the information.

After an KIT1021 accesses the enterprise server, the server automatically allocates a device authentication code to the KIT1021. The KIT1021 must carry the device authentication code in later login to the enterprise server. If the carried authentication code is incorrect, the KIT1021 fails to access the enterprise network or view data related to the enterprise trunking. In this case, the user must request the enterprise administrator to reset the device authentication code.

If the default user login switch for an KIT1021 is turned on on the server, these default users cannot log out of the KIT1021 unless the enterprise administrator turns of the default user login switch.

An account can log in to only one KIT1021 at a time. If an account logs in to an KIT1021, it is forced to log out from the previous KIT1021. To clear data about an account on an KIT1021, enabled the account to log in to the KIT1021 and then log out from the KIT1021. Select the option of clearing user data when you perform the logout.