Body Camera MPT230

User Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V2.1.1

Foreword

General

This manual introduces the functions and operations of the Body Camera MPT230 (hereinafter referred to as "the Device"). Read carefully before using the device, and keep the manual safe for future reference.

Symbols

The following symbols might appear in the manual.

Symbol	Description
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, reductions in performance, or unpredictable results.
ESD	Electrostatic Sensitive Devices. Indicates a device that is sensitive to electrostatic discharge.
ELECTRIC SHOCK	Indicates dangerous high voltage. Take care to avoid coming into contact with electricity.
LASER RADIATION	Indicates a laser radiation hazard. Take care to avoid exposure to a laser beam.
MOVING FAN BLADES	Indicates dangerous moving parts. Take care to keep away from fan blades.
MECHANICAL INJURY	Indicates device parts might cause mechanical injury.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V2.1.1	• Added picture-in-picture function. • Added battery maintenance. • Added AI Always-On. • Added verify to stop recording function and verify to shutdown or restart function. • Added force retransmission by TCP.	May 2026
V1.1.1	Updated the location services.	October 2025
V1.1.0	• Added the update server, KMS server and user verification server in platform settings. • Added the docking mode. • Updated the AI functions. • Added the stealth mode. • Added the SOS broadcast. • Added the platform update.	April 2025
V1.0.0	First release.	November 2024

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

Intelligent Product Usage Statement

Intelligent products utilize AI technology to effectively enhance security. The intelligent recognition and alarm functions of the product might be affected by factors such as environmental lighting, camera angles, object obstructions, and network delays, potentially leading to false alarms, missed alerts, or response delays. This intelligent product is solely intended to be used as a security assistance tool. The results from performing identification are for reference only and do not constitute absolute guarantee of personal or property safety. Users need to combine these products with necessary physical security measures to enhance overall protection. Except as otherwise provided by laws or in the event of intentional or gross negligence on the part of the company, the company shall not be liable for any losses caused by the aforementioned factors not attributable to the company.

Interface Declaration

This manual mainly introduces the relevant functions of the device. The interfaces used in its manufacture, the procedures for returning the device to the factory for inspection and for locating its faults are not described in this manual. Please contact technical support if you need information on these interfaces.

About the Manual

- This manual is provided for general reference only. Discrepancies might exist between the product and this manual, including but not limited to printed, electronic, or any other editions.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. Specifications and documentation are subject to change without prior notice. For the latest versions, as well as legal notices, consult the printed manual, the product webpage, our official website, or scan the QR code to access the electronic edition.
- The manual will be updated as necessary to reflect product changes and applicable legal requirements. These updates will not diminish your statutory rights, nor will they remove or weaken the safety information or essential instructions provided at the time of purchase.
- Although we make every effort to ensure accuracy, errors or deviations in descriptions of functions, operations, or technical data might occur. If there is any uncertainty or controversy, we reserve the right of final explanation.
- All trademarks, registered trademarks and company names referenced in this manual are the property of their respective owners.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the Device, hazard prevention, and prevention of property damage. Read carefully before using the Device, and comply with the guidelines when using it.

Transportation Requirements

Transport the Device under allowed humidity and temperature conditions.

Storage Requirements

- Store the Device under allowed humidity and temperature conditions.
- To avoid short circuits caused by metal objects touching the battery anode and cathode, do not store the battery with other metals.
- If the Device will not be used for a week or longer, charge it to 60%, take the battery out of the Device, and store it in a clean, dry and ventilated room with an ambient temperature of 20 ± 5 °C.
- Charge the battery once every four months during storage.

Installation Requirements

- The Device must be installed in a location that only professionals can access. Non-professionals are not allowed to enter the installation area.
- The Device must be reliably grounded by professionals. They must install the grounding conductor in the building floor and verify the grounding connection of the output receptacle.
- When installing the Device, make sure that the power plug can be easily reached to cut off the power.

Operation Requirements

DANGER

Battery Pack Precautions

Preventive measures (including but not limited to):

- Do not transport, store or use the batteries in high altitudes with low pressure and environments with extremely high and low temperatures.
- Do not dispose the batteries in fire or a hot oven, or mechanically crush or cut the batteries to avoid an explosion.
- Do not leave the batteries in environments with extremely high temperatures to avoid explosions and leakage of flammable liquid or gas.

- Do not subject the batteries to extremely low air pressure to avoid explosions and the leakage of flammable liquid or gas.

WARNING

Use the power adapter and cables provided with the device. We assume no responsibility for injuries or damage caused by using the incorrect power adapter and cables.

- Use the Device under allowed humidity and temperature conditions.
- Do not continuously charge the battery for 24 hours or longer. When it is finished charging or it no longer needs charging, disconnect the adapter from the device, and unplug it from the power socket.
- Please be advised that your configurations will be lost after performing a factory reset.

Maintenance Requirements

DANGER

Replacing unwanted batteries with the wrong type of new batteries might result in explosion.

Preventive measures (including but not limited to):

- Replace unwanted batteries with new batteries of the same type and model to avoid the risk of fire and explosion.
- Dispose of the old batteries as instructed.

The battery is a consumable accessory. We recommend replacing it after it has been used for a year.

Table of Contents

Foreword I
Important Safeguards and Warnings IV
1 Product Introduction 1
2 Structure and Installation 2
2.1 Packing List 2
2.2 Device Structure 2
2.3 Indicator Lights 4
2.4 Back Clip 5
3 Basic Operations 7
3.1 Starting and Shutting Down 7
3.2 Initialization 7
3.3 Home Screen 11
3.4 User Management 11
3.4.1 Enabling Platform User Verification 11
3.4.2 Changing the Password 12
3.4.3 Changing the Unlock Pattern 12
3.4.4 Configuring the Account Security 13
3.5 Configuring the Device 14
3.5.1 Network 14
3.5.2 Device 30
3.5.3 System 40
3.6 System Maintenance 46
3.6.1 Online Update 46
3.6.2 Platform Upgrade 47
3.6.3 Local System Upgrade 47
3.6.4 Scan to Update 47
3.6.5 Network Test 47
3.6.6 Network Capture 48
3.6.7 Log Package 49
3.6.8 Signal Strength and Band 50
3.6.9 ADB Network Debugging 50
3.7 Audio Recording 50
3.7.1 Recording Audio 50
3.7.2 One Press to Record Audio 51
3.8 Video Recording 51
3.8.1 Recording Video 51
3.8.2 One Press to Record a Video 54

3.8.3 Focusing....54
3.8.4 Marking Important Videos....55
3.9 Pictures....55
3.9.1 Taking a Picture....55
3.9.2 One Press to Take a Picture....55
3.10 Files....55
3.10.1 Viewing Pictures....55
3.10.2 Playing Video....58
3.10.3 Playing Audio....60
3.10.4 Viewing AI Function Files....61
3.11 Switching between Video and Audio Recording....62
3.12 Light & Sound Icons....63
3.13 Data Transmission....63
3.14 Log....63
3.15 Creating and Joining Tasks....64
3.16 Scanning the QR Code....66
4 System Update....67
4.1 Updating on MPT Manager....67
4.2 Updating on Local Device....68
5 Platform Operations....69
5.1 Adding the Device to the Platform....69
5.2 Connecting to the Platform....71
6 Battery Maintenance....72
7 SIM Card and Battery Installation....73
7.1 Installing the SIM Card....73
7.2 Installing the Battery....74
8 FAQ....77
Appendix 1 Security Commitment and Recommendation....78

1 Product Introduction

This product is a mobile portable terminal for persons of public security, insurance, traffic police and more. It integrates audio/video record and snapshot together.

This product can record the data during the whole law enforcement process. It is light and has small compact design, easy to install. It is waterproof and shockproof. The built-in IR light can guarantee clear video at night. The recorded video supports onsite playback and prevents the file from being tampered. The recorded data is fair and can be recognized by the authorities to solve a case and provide as the evidence on the court.

2 Structure and Installation

2.1 Packing List

Table 2-1 Packing list

Name	Quantity
Device	1
Clip	1
USB cable	1
Battery	1
Power adapter	1
Quick start guide	1

2.2 Device Structure

The structure differs depending on the model you are using. The following figures are for reference only.

Figure 2-1 Front and rear panels

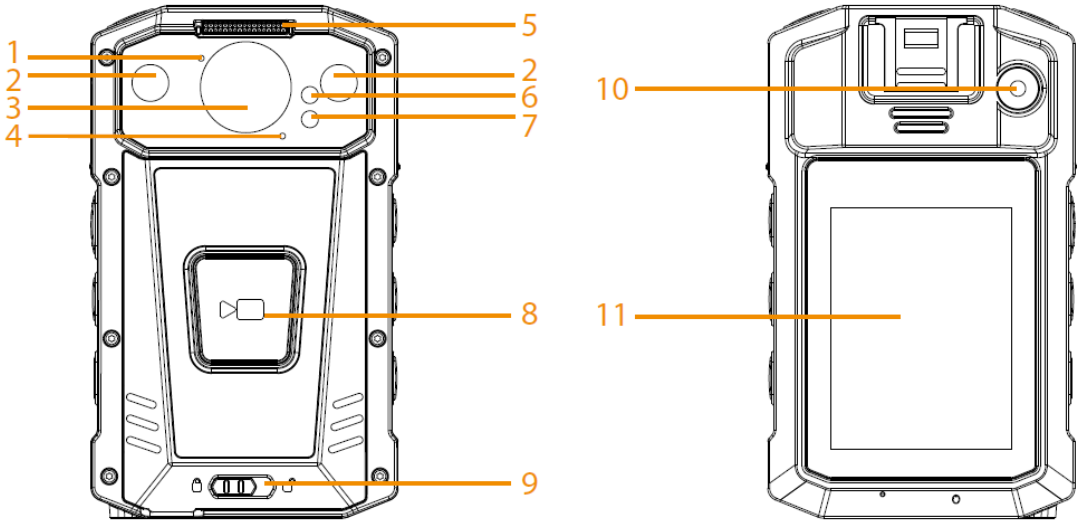


Table 2-2 Structure introduction

No.	Name
1	Indicator light
2	IR light
3	Rear camera

No.	Name
4	Mic in
5	Red and blue flashing light
6	Light perception
7	White light
8	Record video
9	Slider
10	Front camera
11	Main screen

Figure 2-2 Side panels

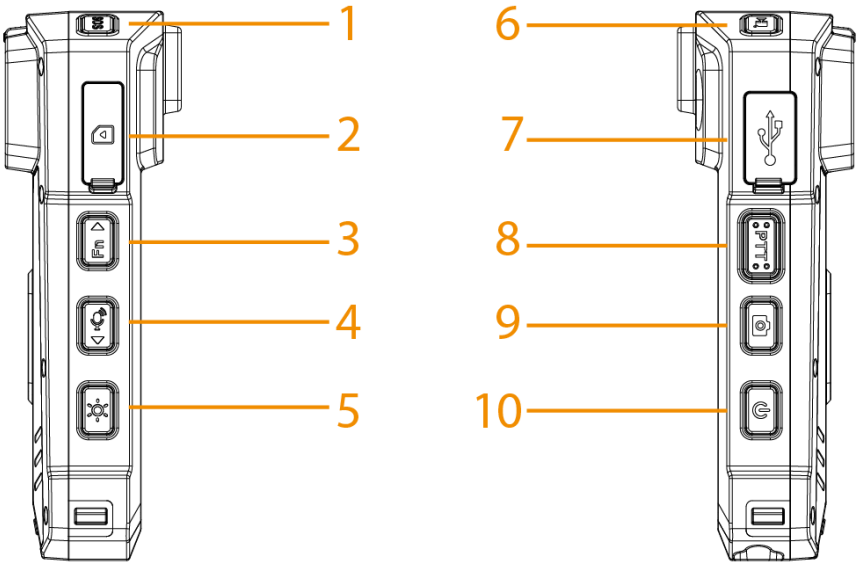


Table 2-3 Button introduction

No.	Name	No.	Name
1	SOS button	6	Record video
2	Sim card port	7	USB port and power input
3	Fn button	8	Voice talk
4	Record audio	9	Capture button
5	IR light button	10	Power button

Figure 2-3 Bottom and top panels

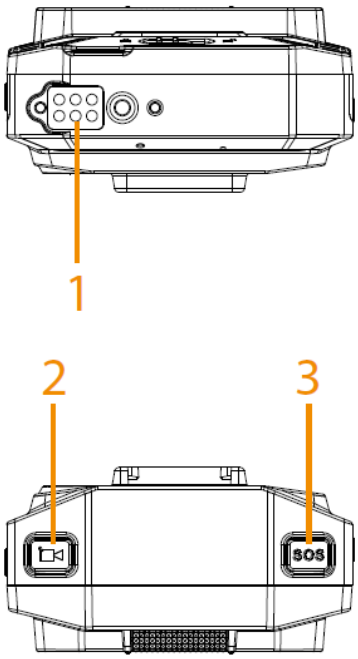


Table 2-4 Button introduction

No.	Name
1	Pogo pin interface
2	Record video
3	SOS button

2.3 Indicator Lights

The states of the indicator show different statuses of the Device.

Table 2-5 Indicator lights

Working Status	Indicator Light
Standby	Solid green
Standby (battery level ≤ 5%)	Solid red
Recording video	Flashes red
Snapshot	Flashes red
Alarm	Red and blue flashing light warning
Recording audio	Flashes yellow
Charging	Solid red
Battery fully charged	Solid green
Platform is pulling stream	Flashes blue

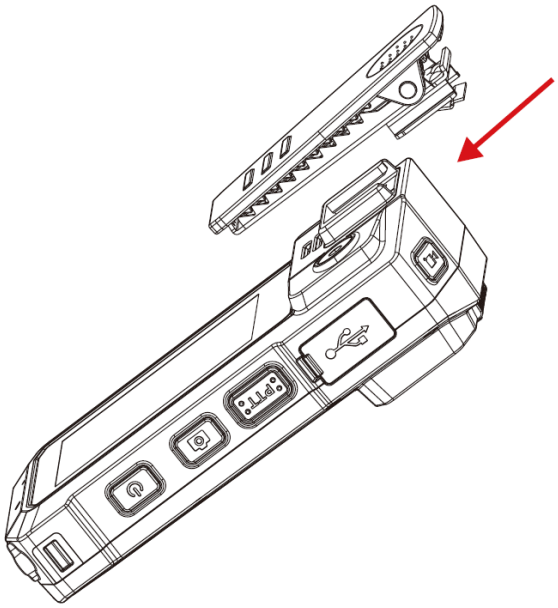
You can select **None** , **Red and Blue Flashing Light Warning** or **Sound and Light Active Deterrence** for the Fn button in **Settings** > **Device** > **FN key**. The default setting is red and blue flashing light.

2.4 Back Clip

Installing the clip

After aligning the slot, simply push the back clip in to install it.

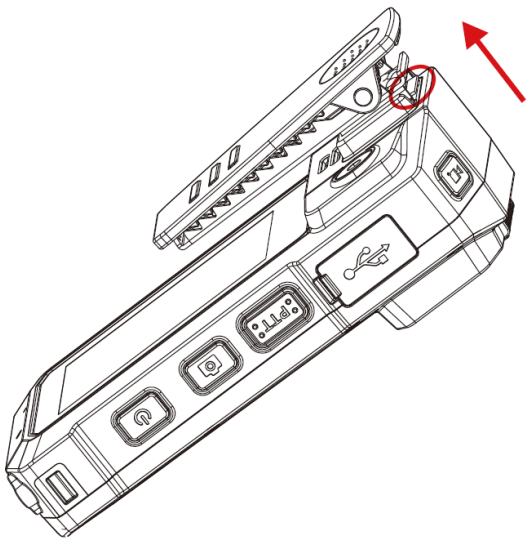
Figure 2-4 Install the clip



Removing the clip

Pinch upward with your hand and then pull outward to remove the back clip.

Figure 2-5 Remove the clip



3 Basic Operations

3.1 Starting and Shutting Down

The power supply automatically turns on when connected to power, even if it is turned off.

Press on the right side to start, shut down, restart or let the Device sleep.

- When the Device is shut down, press and hold to start the Device.
- When the Device is running, press and hold , and then tap **Power off** to shut down the Device.
- When Device is running, press and hold , and then tap **Restart** to restart the Device.
- When the Device is running, press and hold for 10 s to restart the Device forcibly.
- When the Device is running, press to let the Device sleep; press again to activate the Device.

3.2 Initialization

Background Information

For the first-time use, set device login password and at least 3 security questions. If you forget the password, tap **Forgot?** , and then answer the security questions, send verification code to your email, or tap **Help** to reset the login password.

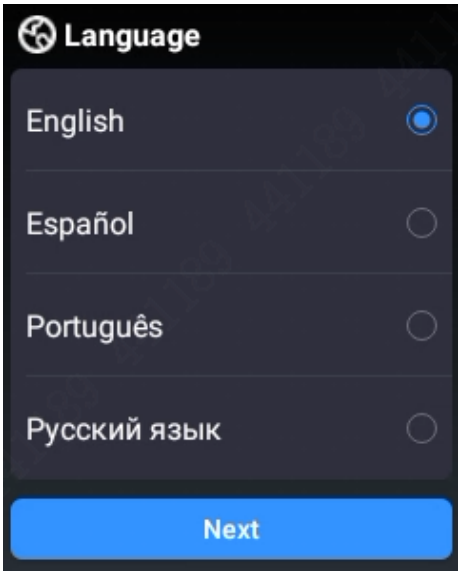
- The password resetting function is only available for admin user.
- Password resetting will delete the pattern lock. You need to set it again after resetting the password.
- If you forget the answers to the security questions or your mailbox is unavailable, please contact the technical support or the distributor for help.

Procedure

Step 1 When the Device is shut down, press and hold to start the Device.

Step 2 Select the language, checkbox of the end-user software license agreement and product privacy policy, select **I have read and agree** , and then tap **Next**.

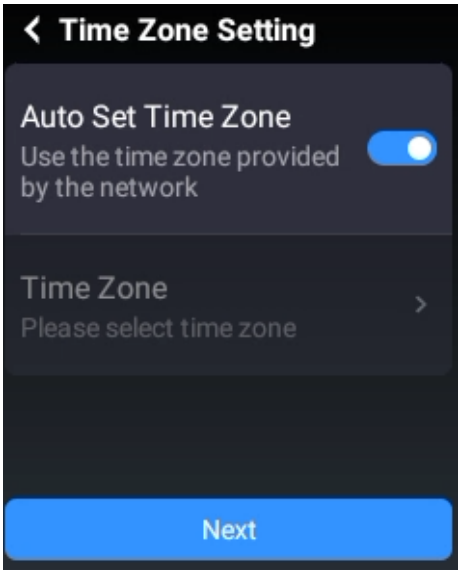
Figure 3-1 Select the language



You can select English, Spanish, Portuguese and Russian.

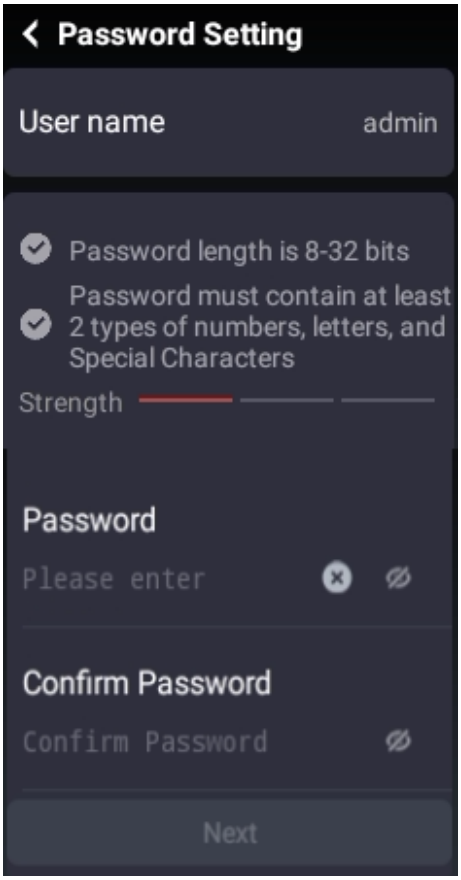
Step 3 Enable **Auto Set Time Zone** or select the time zone.

Figure 3-2 Set time zone



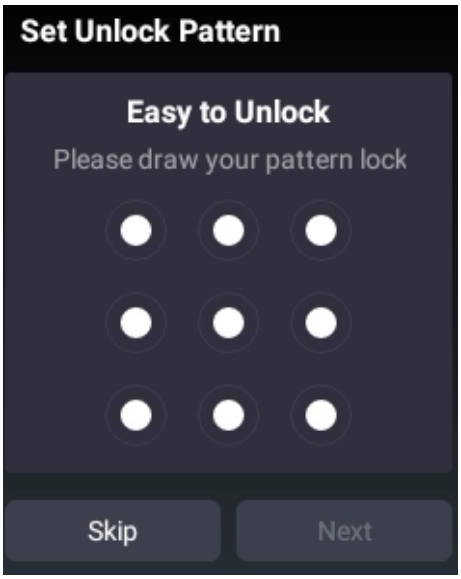
Step 4 Enter the new password and then confirm it.

Figure 3-3 Set password



Step 5 Set unlock pattern and click **Next**.

Figure 3-4 Set unlock pattern

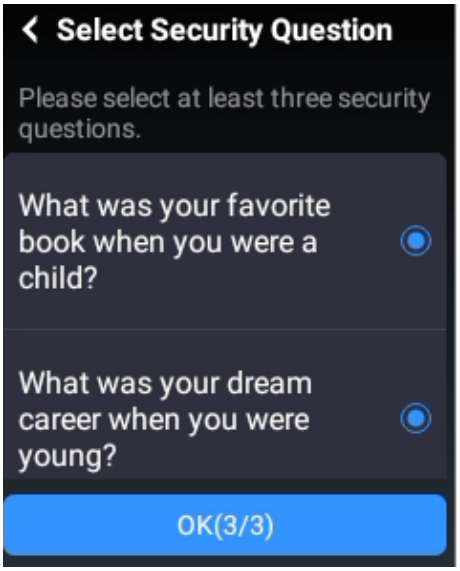


Step 6 Ensure the account security by setting security questions and binding your email.

- Set security questions

  1. Tap **Security Questions** to set security questions.
  2. Select at least 3 security questions, and then tap **OK(3/3)**.
  3. Enter the answers and then tap **Save**.

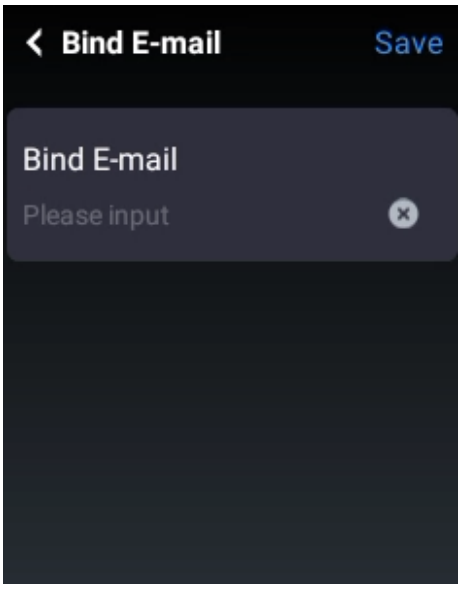
Figure 3-5 Select security questions



- Bind email

  Tap **Email** to input your email address, and then tap **Save**.

Figure 3-6 Bind email



Step 7 Tap **Done**.

If you tap **Skip** in the account security screen, you can only retrieve your password by contacting the distributor or technical support in the **Forgot?** or **Help** screen.

Step 8 Follow the on-screen instructions to learn gestures.

Results

The Device is initialized successfully.

3.3 Home Screen

- The notification bar displays message, working status, and operator status. Swipe down to view time and date, and select white light, IR light, sound and light active deterrence and red and blue flashing light warning.
- Swipe left or right on the home screen to switch the screen.

For the homepage drop-down menu, see "3.12 Light & Sound Icons".

3.4 User Management

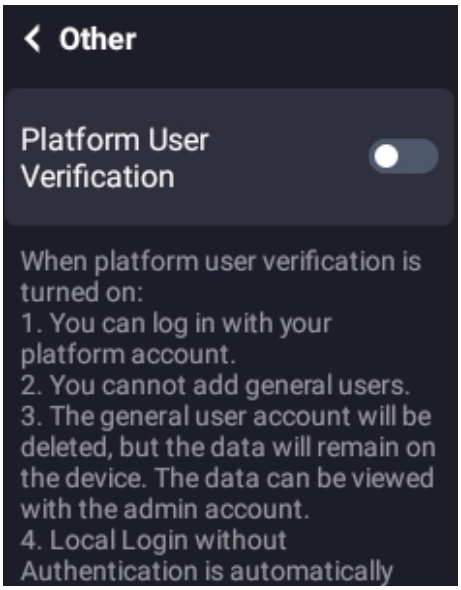
3.4.1 Enabling Platform User Verification

Procedure

Step 1 On the home screen, tap .

Step 2 Tap **Platform User Verification**.

Figure 3-7 Platform user verification



Step 3 Click and enter the login password.

Results

The platform user verification is enabled.

3.4.2 Changing the Password

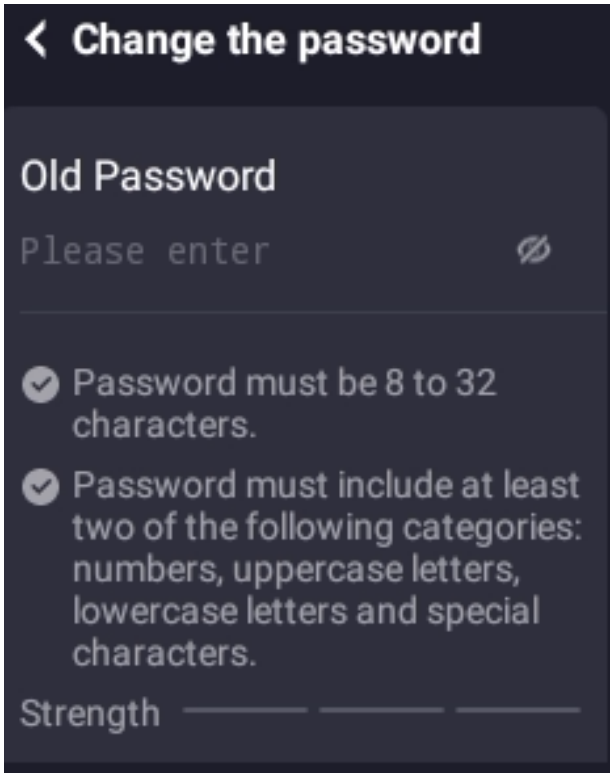
We recommend you change the password regularly to enhance the device security.

Procedure

Step 1 On the home screen, tap .

Step 2 Select the account whose password you want to change, and then tap **Change the password**.

Figure 3-8 Change the password



Step 3 Enter the old password, new password and confirm password.

Step 4 Set the password validity period.

Step 5 Tap **Confirm Modification**.

3.4.3 Changing the Unlock Pattern

Procedure

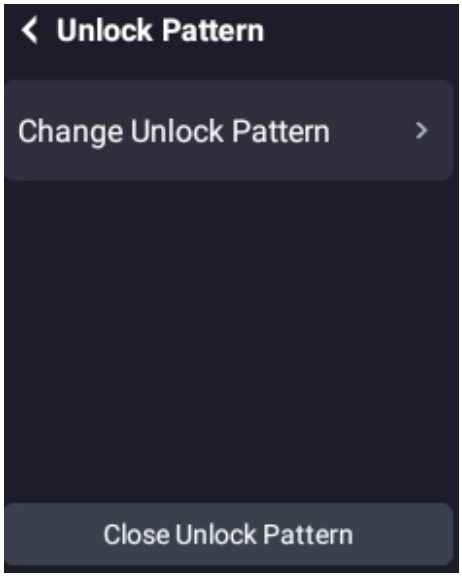
Step 1 On the home screen, tap .

Step 2 Select an account, and then tap **Unlock Pattern**.

Step 3 Enter the login password.

Step 4 Tap **Change Unlock Pattern**.

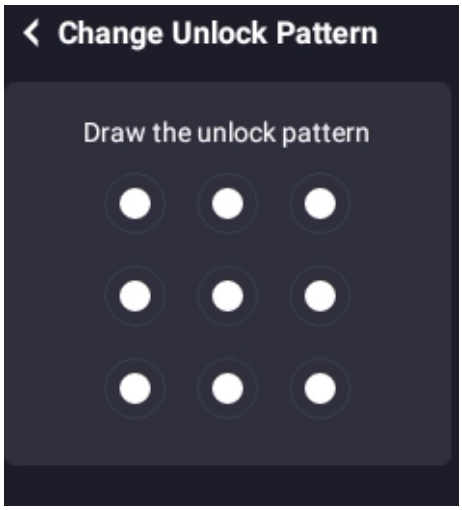
Figure 3-9 Unlock pattern



You can tap **Close Unlock Pattern** and the unlocking mode will be changed to password unlock.

Step 5 Draw the pattern lock.

Figure 3-10 Draw the unlock pattern



- An unlock pattern must contain at least 4 points.
- After you set the unlock pattern, the pattern unlock will be required on the login screen by default. If you have not set pattern lock, password is required on the login screen by default.

3.4.4 Configuring the Account Security

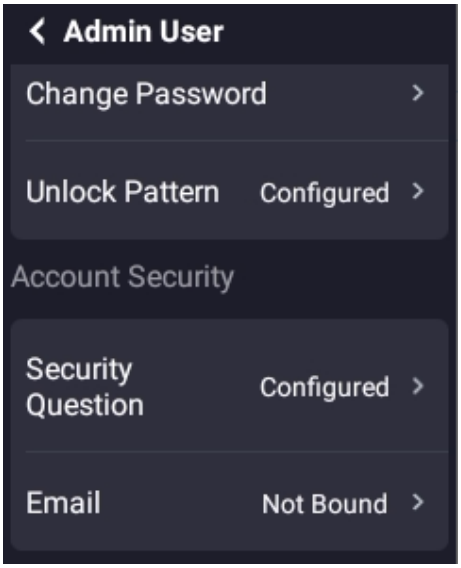
You can reset your security questions and bound email. This function is only for the admin user.

Procedure

Step 1 On the home screen, tap .

Step 2 Select an account, and then tap **Security Question** or **Email**.

Figure 3-11 Account security



Step 3 Enter the login password.

Step 4 Follow the on-screen instructions to configure your security questions and the bound email.

3.5 Configuring the Device

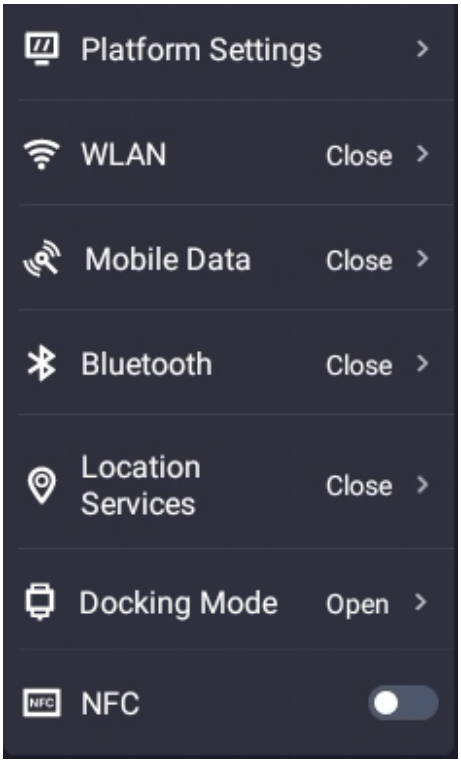
Before using the Device, configure recording parameters, camera parameters, network mode, and more.

3.5.1 Network

On the home screen, tap

to go to the **Network** screen.

Figure 3-12 Network



Tap an icon to go to the corresponding screen for configuration.

- close means that the function is disabled.
- open means that the function is enabled.

3.5.1.1 Platform Settings

You can add the Device to platform for remote management. You can configure platform connection, WLAN, location service and more.

Private protocol is enabled, otherwise you cannot configure the parameters successfully.

3.5.1.1.1 Auto Registration

You can manually register the device to the platform.

Procedure

Step 1 On the home screen, select Settings > **Network** > **Platform Settings** > **Auto Registration**.

Step 2 Tap to enable the auto registration function.

Step 3 Configure the parameters.

Figure 3-13 Auto Registration

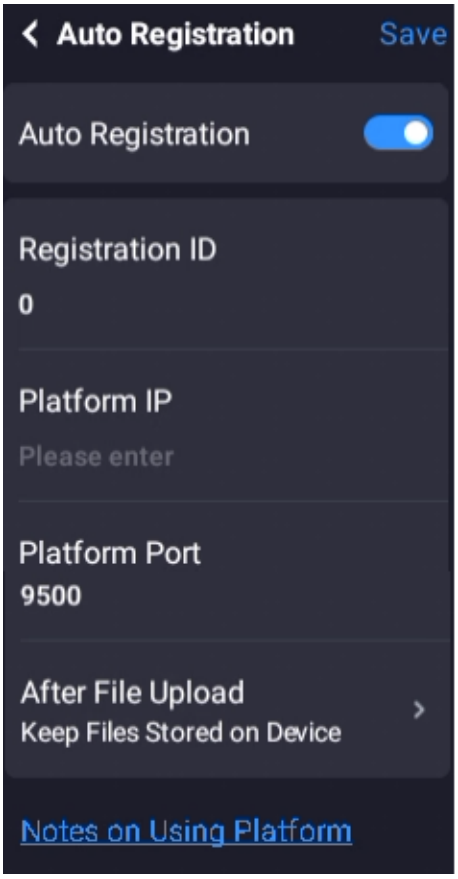


Table 3-1 Auto registration parameters

Parameter	Description
Registration ID	Enter an ID for registration. Make sure that the same ID is used when you add the Device to the platform.
Platform IP	Enter the IP address or the domain name of the platform server.
Platform Port	Enter the ARS (Active Register Server) port number of the platform.
After File Upload	• **Keep Files Stored on Device** : Files are stored on the device after you upload files to the platform. • **Auto Delete** : Files are automatically deleted on the device after you upload files to the platform.

Step 4 Tap **OK**.

3.5.1.1.2 Update Server

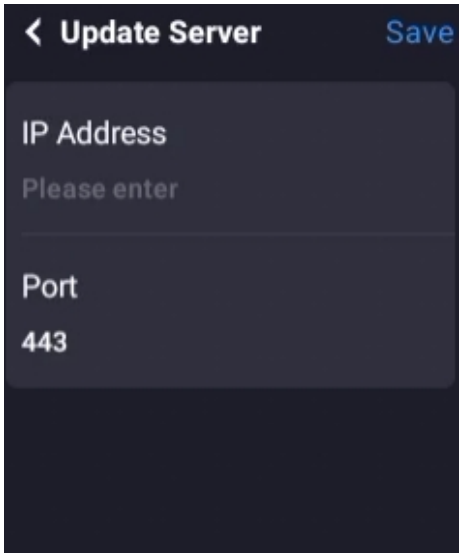
Used for updating the device on the platform.

Procedure

Step 1 On the home screen, select > **Network** > **Platform Settings** > **Update Server**.

Step 2 Configure the IP address and port.

Figure 3-14 Update server



The default port is 443.

Step 3 Click **Save**.

3.5.1.1.3 KMS Server

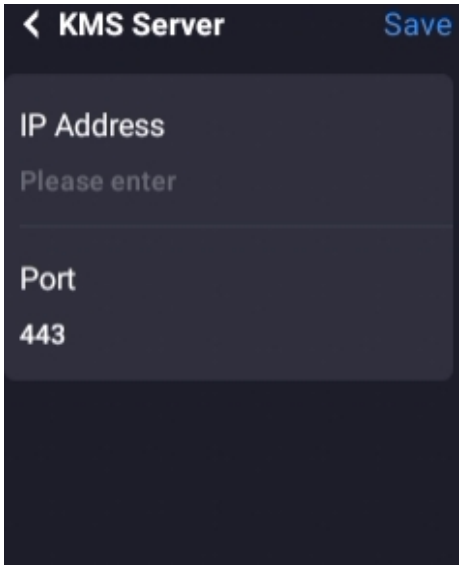
Used for file encryption.

Procedure

Step 1 On the home screen, select > **Network** > **Platform Settings** > **KMS Server**.

Step 2 Configure the IP address and port.

Figure 3-15 Update server



The default port is 443.

Step 3 Click **Save**.

3.5.1.1.4 User Verification Server

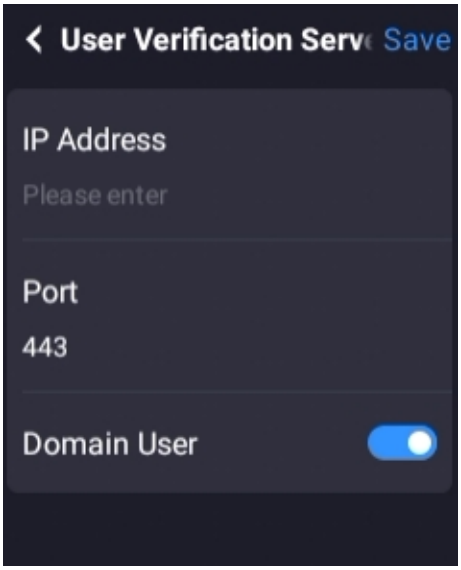
Used for verifying whether the user is a platform user.

Procedure

Step 1 On the home screen, select > **Network** > **Platform Settings** > **User Verification Server**.

Step 2 Configure the IP address and port.

Figure 3-16 User verification server



- The default port is 443.
- You can enable **Domain User** according to your actual needs.

Step 3 Click **Save**.

3.5.1.1.5 RTSP

Enables RTSP stream encryption by using TLS.

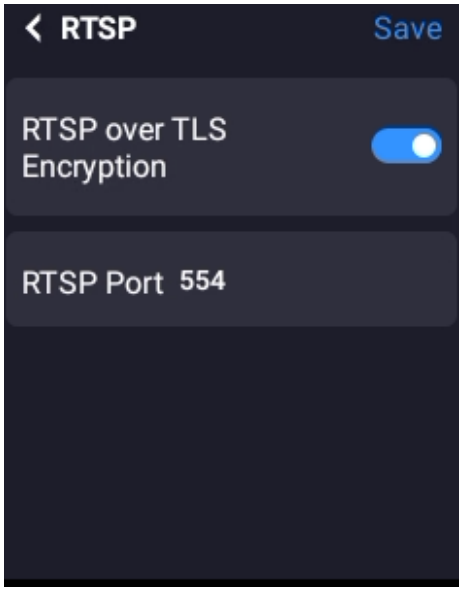
Procedure

Step 1 On the home screen, select > **Network** > **Platform** > **RTSP**.

Step 2 Tap to enable RTSP over TLS encryption.

Step 3 Enter the RTSP port and then tap **Save**.

Figure 3-17 RTSP



- There might be safety risk if this service is disabled.
- The RTSP port is 554 by default.

3.5.1.1.6 FTP

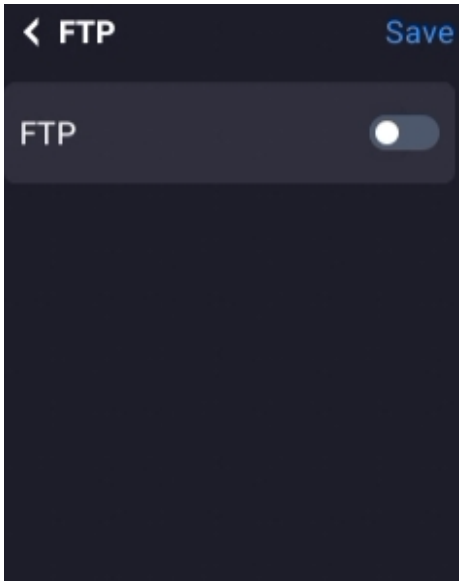
You can add the device to the FTP server.

Procedure

Step 1 On the home screen, select > **Network** > **Platform Settings** > **FTP**.

Step 2 Tap to enable the FTP settings.

Figure 3-18 FTP



Step 3 Enter address, port and storage path.

Step 4 Configure the parameters.

Figure 3-19 FTP parameters

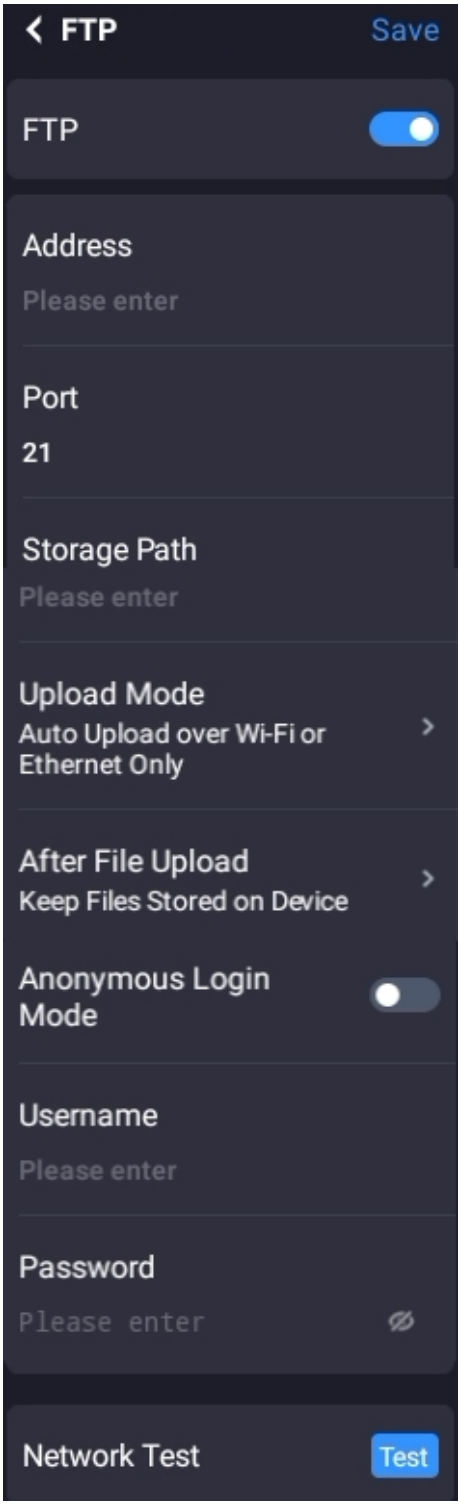


Table 3-2 FTP parameters

Name	Parameter
Upload Mode	• **Manual Upload** : Upload files manually. • **Auto Upload over WI-FI or Ethernet Only** : Only when the device is connected to Wi-Fi or Ethernet are files uploaded to the FTP platform automatically. • **Auto Upload** : Files are uploaded to the FTP platform automatically when the device is over 4G, 5G, WI-FI or Ethernet.
After File Upload	• **Keep Files Stored on Device** : After files are uploaded, files are stored on the device. • **Auto Delete** : After files are uploaded, files are automatically deleted from the device.
Anonymous Login Mode	When it is enabled, you can log in to the platform without username and password.

The FTP and platform register can be enabled simultaneously, but register will take priority.

3.5.1.2 WLAN

When WLAN is turned on, you can search for or add WLAN networks.

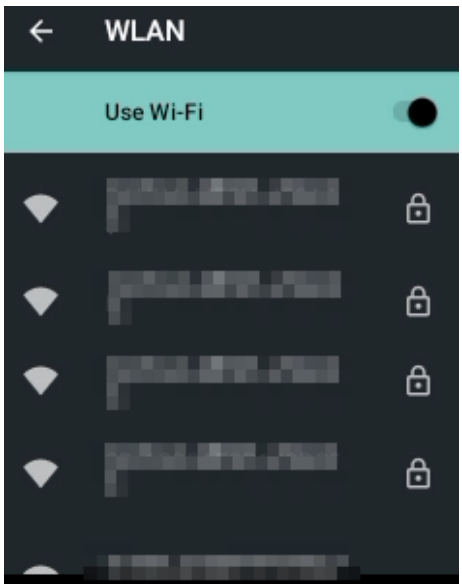
Procedure

Step 1 On the home screen, select Settings > **Network** > **WLAN**.

Step 2 Tap to enable the WLAN function.

Step 3 Select the Wi-Fi that you want to connect to, and then enter the password.

Figure 3-20 WLAN

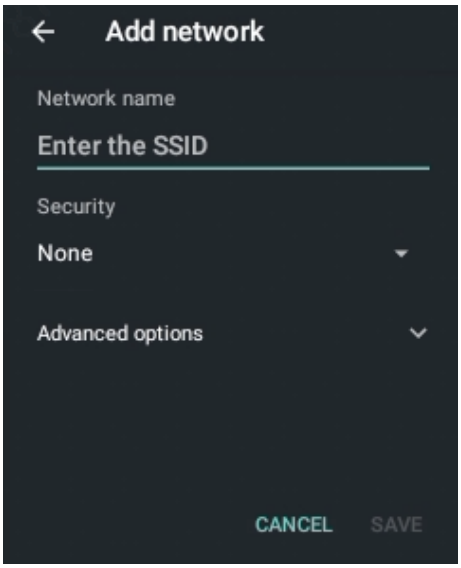


3.5.1.2.1 Adding Network

Procedure

Step 1 On the **Wi-Fi** screen, tap **Add network**.

Figure 3-21 Adding network



Step 2 Configure the parameters.

Table 3-3 Parameter description of adding network

Parameter		Description
Network name		Enter the router SSID (the name of the WLAN) that needs to be connected.
Security		Set security settings. ● If you select **None,** you do not need to enter a password to log in to the WLAN. ● If you select a different type, you need to enter a password or certificate.
Advanced Options	Hidden network	Choose whether the network you are adding is a hidden network. If it is a hidden network, select **Yes** to add it successfully.
	Metered	Select **Detect automatically** , **Treat as metered** and **Treat as unmetered**.
	Proxy	● **None** : Do not need proxy. ● **Manual** : Set the proxy server parameters manually. ● **Proxy Auto-Config** : The Device will automatically set proxy server parameters.

Parameter		Description
	IP settings	• **DHCP** : The Device automatically searches for WLAN IP. • **Static** : You need to manually configure the **IP address**, **Gateway**, **Network prefix length**, **DNS 1**, and **DNS 2**. ◇ IP address must be on the same segment as the router. ◇ Other parameters must be consistent with those on the router.
	Privacy	• **Use randomized MAC (default)** : The device uses a randomly generated MAC address when connecting to a Wi Fi network. • **Use device MAC** : The device uses its fixed and unique MAC address (i.e. the address of the device) to connect to the Wi Fi network.

Step 3 Tap **SAVE**.

3.5.1.2.2 Configuring Wi-Fi Preferences

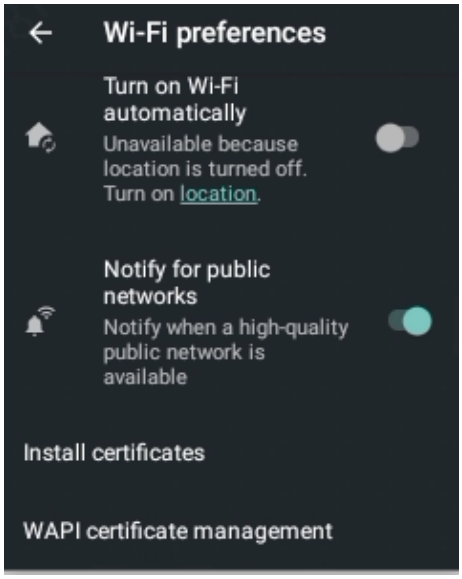
Prerequisites

WIFI direct connection requires location services to be enabled for use. For details, see "3.5.1.5 Location Services".

Procedure

Step 1 On the **Wi-Fi** screen, tap **Wi-Fi preferences**.

Figure 3-22 Wi-Fi preferences



Step 2 Configure the parameters.

Table 3-4 Parameters of Wi-Fi preferences

Parameter	Description
Turn on Wi-Fi automatically	Automatically enables Wi-Fi when the Device is on a saved high-quality Wi-Fi network. To use the function, you need to enable the location service. For details, see "3.5.1.5 Location Services".
Notify for public networks	Sends notifications when a high-quality public network is available.
Install certificates	After you upload the security certificate to your device, tap **Install certificates** to select and install the certificate.
WAPI certificate management	You can manage and maintain the security certificates used in the WAPI protocol.

3.5.1.2.3 Managing Saved Networks

Procedure

Step 1 On the **Wi-Fi** screen, tap **Saved networks**.

Step 2 You can view the networks that were connected or added.

Step 3 Select a network, and then tap **Forget** to remove the network.

3.5.1.3 Mobile Data

The Device can connect to network through mobile data.

Procedure

Step 1 On the home screen, select

> **Network** > **Mobile Data**.

Step 2 Configure the parameters.

Figure 3-23 Mobile data

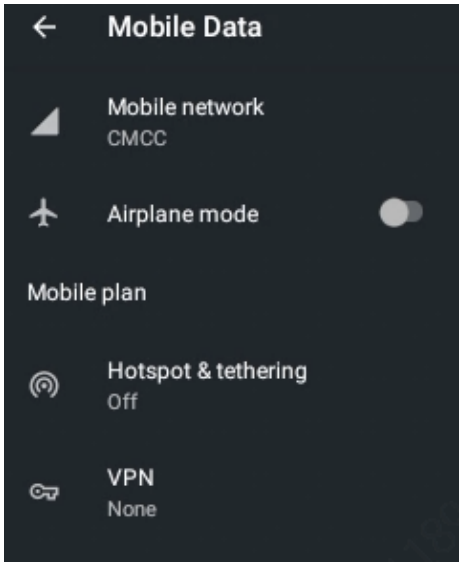


Table 3-5 Description of mobile data parameters

Parameter	Description
Mobile network Supports dual SIM card selection.	• SIM name & color: Tap to configure the SIM card's name and color used by compatible apps. • Mobile data: Enables mobile network. • Roaming: Enables the Device to connect to the mobile network service while roaming. • Data warning & limit: Configure the mobile data usage cycle, data warning and data limit. • 4G Calling: Uses 4G services to improve voice and other communication functions. This function is enabled by default. • Preferred networks: Select the preferred network in the list. • Advanced: ◇ Preferred network type: You can select 4G, 3G or 2G as the preferred network mode. 4G is recommended. ◇ Carrier video calling: Make high-quality video calls provided by mobile network operators. ◇ Automatically select network: The device automatically chooses the best available mobile network. ◇ Access Point Names: APN determines how the Device accesses the network.
Airplane mode	In airplane mode, cellular, Wi-Fi, and Bluetooth functions are disabled.

Parameter		Description
Hotspot & tethering		• Wi-Fi hotspot: Shares Internet connection or content with other devices. The hotspot can be accessed by entering a password. • USB tethering: Shares your mobile Internet connection over USB. • Bluetooth tethering: Shares your mobile Internet connection through Bluetooth. • Ethernet tethering: Shares phone's internet connection via USB Ethernet.
VPN		Add the appropriate VPN as needed. Click + to edit the VPN profile.
Advanced	Private DNS	You can select private DNS mode. • **Off** : The Device uses the default DNS. • **Automatic** : The Device selects the best private DNS server based on system settings. • **Private DNS provider hostname** : You can manually specify a trusted third-party DNS provider.

3.5.1.4 Bluetooth

When Bluetooth is enabled, a nearby device will be able to detect the Device, and then you can receive and share files through Bluetooth.

Procedure

Step 1 On the home screen, select Settings > **Network** > **Bluetooth**.

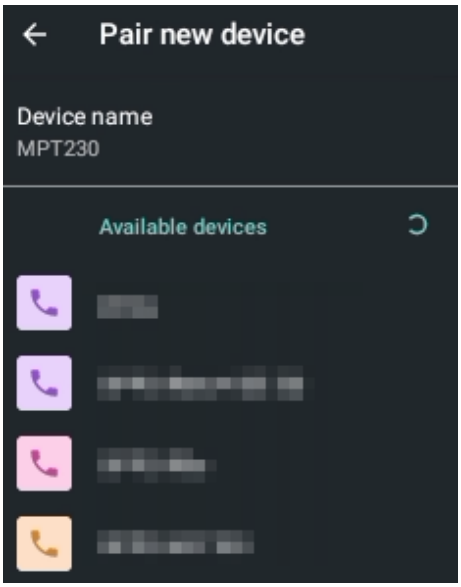
Step 2 Tap to enable Bluetooth.

Step 3 Tap **Pair new device**.

Step 4 Select the Bluetooth device to pair with, and then tap **Pair**.

After confirmation on both devices, pairing is successful.

Figure 3-24 Bluetooth



Related Operations

- To rename the Device, tap **Device Name**.
- To connect with devices that had been paired, tap the device that has been previously connected. The Device will connect with the previously paired device automatically.
- Tap to modify the device details.

3.5.1.5 Location Services

You can enable the satellite-based positioning service for the Device. After connecting the Device to the platform and enabling track record in **Network** > **Location Services**, the Device reports its location information to the platform.

Procedure

Step 1 On the home screen, select > **Network** > **Location Services**.

Step 2 Tap to enable the location services.

Step 3 Configure the parameters.

Figure 3-25 Location services

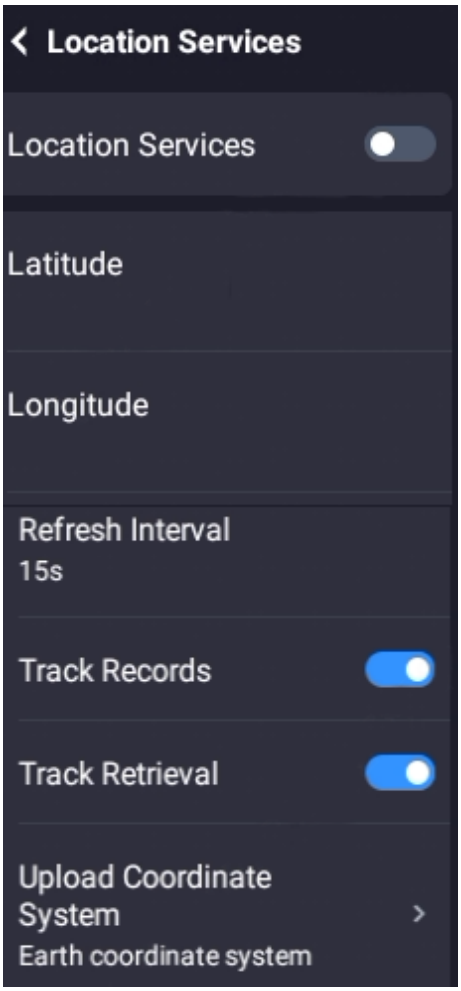


Table 3-6 Parameter description of location services

Parameter	Description
Location	Displays the latitude and longitude.
Refresh Interval	Select the interval at which the Device reports location information to the platform. The default value is 15 s.
Track Records	Enable the Device to keep track of its historical locations.
Track Retrieval	Enable the function, and the Device will cache. You can upload the location information to the platform.
Upload Coordinate System	Select the GPS Coordinate System from **Earth coordinate system** or **Mars coordinate system**. The selected coordinate system must be the same with the coordinate system on the platform.

3.5.1.6 Docking Mode

You can insert the MPT 230 into the docking base for charging, data upload and other functions.

Procedure

Step 1 On the home screen, select Settings > **Network** > **Docking Mode**.

Step 2 Tap to enable the docking mode.

Once the docking mode is enabled, when the MPT 230 is inserted into the base, the MPT will automatically enter the docking mode page.

Step 3 Configure the parameters.

Figure 3-26 Docking mode

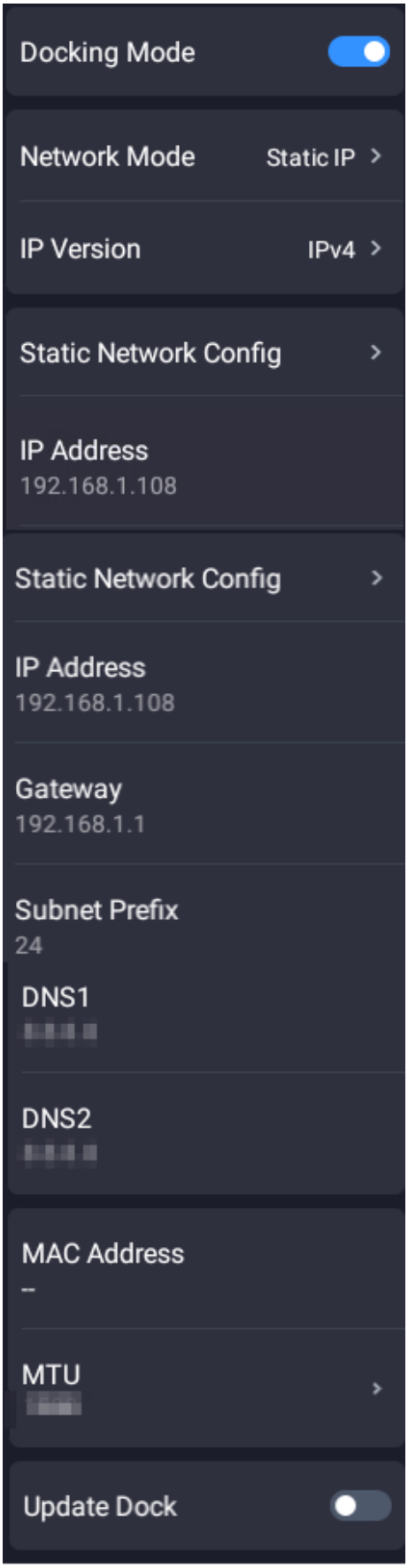


Table 3-7 Docking mode parameters

Parameter		Description
Network Mode		Select the network mode. • **Auto Obtain** : The device will automatically obtain an IP address from the network. • **Static IP** : You need manually configure a specific IP address for the device. Static Network Config is only available when you select **Static IP**.
IP Version		Select **IPv4** or **IPv6**. Both versions are supported for access.
Static Network Config	IP Address	Click **Static Network Config** to set the IP address, gateway, subnet prefix and DNS for the static IP of the device. IP address and gateway must be on the same network segment.
	Gateway	
	Subnet Prefix	
	DNS1	
	DNS2	
MAC Address		When the MPT 230 is connected to the docking base, you can view the MAC address of the base.
MTU		Set the MTU (Maximum Transmission Unit) value, ranging from 576 to 1500.
Update Dock		Enable the function to update the docking base.

3.5.1.7 NFC

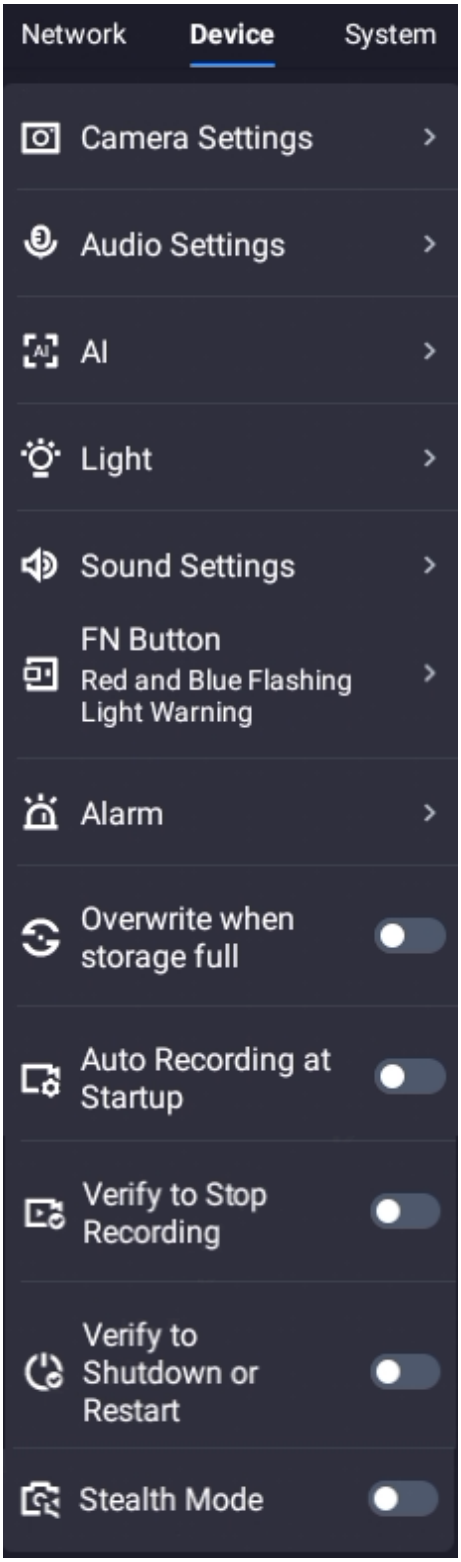
Enable the NFC function to allow for quick and secure data exchange between devices.

3.5.2 Device

On the home screen, tap

, and then tap the **Device** tab to configure camera settings, audio recording settings, and more.

Figure 3-27 Device



3.5.2.1 Camera Settings

Select **Device** > **Camera Settings** to configure camera settings.

The camera parameters might differ depending on the model you are using.

The configuration parameters for the front and rear cameras might differ.

Figure 3-28 Camera settings

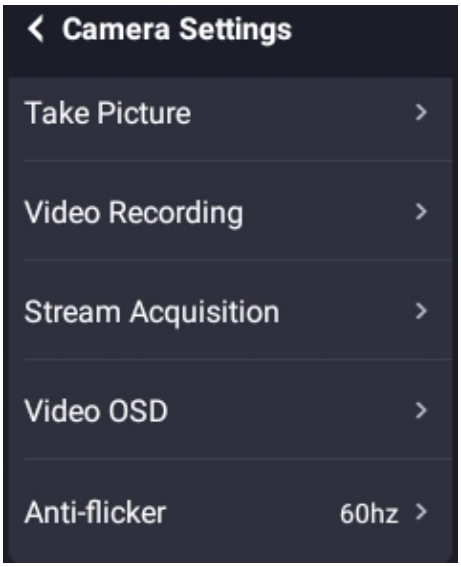


Table 3-8 Camera settings description

Parameter		Description
Take Picture	Resolution	Configure the image size of the rear camera, the front camera and picture-in-picture frame. The picture-in-picture image parameters cannot be configured and are grayed out, displaying 2M (1080x1920), which cannot be modified.
	Burst	Configure the number of continuous shooting.
Video Recording	Compression	Configure the encoding type of video.
	Resolution	Configure the video resolution. The higher the resolution, the higher the video quality, but meanwhile the more the storage space consumption.
	Frame Rate	Configure the frame rate of video. The higher the frame rate, the smoother the video.
	Bit Rate	Configure the bit rate of video.
	Pre-Record	Configure the pre-record time. For example, if you select 10 s, the 10 s video prior to recording will be saved automatically.
	Post-Record	Configure the post-record time. For example, if you select 10 s, 10 s video after the recording ends will be saved automatically.

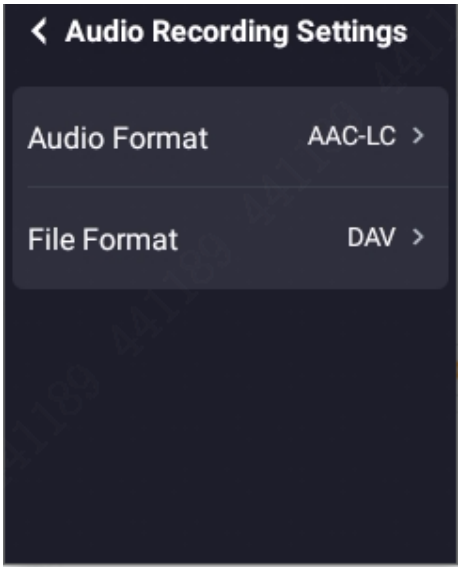
Parameter		Description
	EIS	Enable the function to reduce the effect from vibration and shaking on video quality. ● The AI functions, EIS and distortion correction cannot be enabled at the same time. ● When the resolution of the rear camera is set to 2K or above, EIS cannot be enabled. ● The AI functions, viewing videos and recording videos in 4MP cannot be enabled at the same time.
	Distortion Correction	Fix or reduce any distortions in images or videos, like lens or camera-related distortions, to make them look more accurate and true. The smart functions, EIS and distortion correction cannot be enabled at the same time.
	File Type	Select the file type of the videos. **Dav** and **Mp4** can be selected.
	Packaging Time	Configure the interval at which the recorded video is saved as a file. ● To avoid small files, the packaging time will fluctuate. For example, when you select 30 min, if the start time of recording is 10:26, the stop time will be 11:00; if the start time of recording is 10:14, the stop time will be 10:30. ● A single recorded video file cannot exceed 2 GB in size and is automatically repackaged if beyond the limit.
	Picture-in-Picture	You can enable the picture-in-picture function in the video recording process. When enabled, resolution, frame rate, and bitrate cannot be changed; video encoding can be changed. The main camera can be configured, and the secondary camera's position can be set (top-left, bottom-left, top-right, or bottom-right).
Stream Acquisition	Resolution	Configure the video resolution for network transmission. The higher the resolution, the higher the video quality, but meanwhile the more memory and CPU resources are occupied.
	Frame Rate	Configure the frame rate of video for network transmission. The higher the frame rate, the smoother the video.

Parameter		Description
	Bit Rate	Configure the bit rate of video for network transmission. The options available are different depending on the selected resolution and frame rate.
	Compression	Configure the encoding type of video for network transmission.
	Network Self-adaptive	Enable network adaptation so that the device can adjust the video quality automatically according to the actual network bandwidth situation.
	Force Retransmission by TCP	Enable the function, and then it can optimize video transmission smoothness in scenarios with poor network quality and a high likelihood of packet loss.
Video OSD		Configure whether to display device ID, user ID, time information, longitude&latitude information, task ID, custom information and OSD position and order on the live video image. ● You can select one of the items above to the top. ● **Top Left** , **Top Right**, **Bottom Left** and **Bottom Right** can be selected for the OSD position.
Anti-flicker		Avoids flashing lines of the target during video recording. ● 50 Hz (AC frequency in China). ● 60 Hz (AC frequency in countries such as Japan and United States).

3.5.2.2 Audio Recording Settings

Select **Device** > **Audio Recording Settings** to select the audio format and file format.

Figure 3-29 Audio recording settings



3.5.2.3 AI

Intelligent detection is to extract key information through image processing and analysis, and compare with the per-set detection rules. The device supports face detection by camera and ANPR by camera.

- When both face recognition by camera and ANPR by camera are enabled, the resolution of the rear camera cannot be set to 2K or above.
- Enabling any AI functions and setting the rear camera resolution to 2K or above will prevent live streaming from the rear camera.

3.5.2.3.1 ANPR

Prerequisites

Enable ANPR in **Settings** > **Device** > **AI** > **ANPR**.

Background Information

When the license plate is detected in the detection area, the detection result will be show on the right side of the screen and a record be kept in file management.

On the home screen, select **Camera**, and then put the license plate in the detection area. The detection result will be show on the right side of the screen.

- Enable **ANPR Database** to create the ANPR database.
- Enable **Vibrate** so that the device will vibrate after comparison finishes.
- The ANPR database is distributed by the platform.

3.5.2.3.2 Face Recognition

Prerequisites

Enable face detection by camera in **Settings** > **Device** > **AI** > **Face Recognition**.

Background Information

On the home screen, select **Camera**, and then put the face in the detection area. The detection result will be shown on the right side of the screen.

- Enable **Main Group** in **Face Comparison Database** so that the database is configured.
- Set the similarity ratio for face comparison in **Success Threshold**.
- Enable **Vibrate** so that the device will vibrate after comparison finishes.
- The face database is distributed by the platform.

- When the face images are detected in the face detection area, the detection result will be shown on the right side of the screen and a record be kept in the face detection of the file management. For details, see Figure 3-55 .
- The face recognition function will compare detected faces with those in the face database, and once the comparison is successful, the information will be saved in the face recognition section of the file management. For details, see "Face recognition results".

3.5.2.3.3 AI Always-On

Once the function is enabled, it will activate the corresponding AI algorithm in the background, regardless of whether the rear camera is turned on or not.

3.5.2.4 Light Settings

Configure light settings on the device as needed.

Select **Device** > **Light**.

Figure 3-30 Light settings

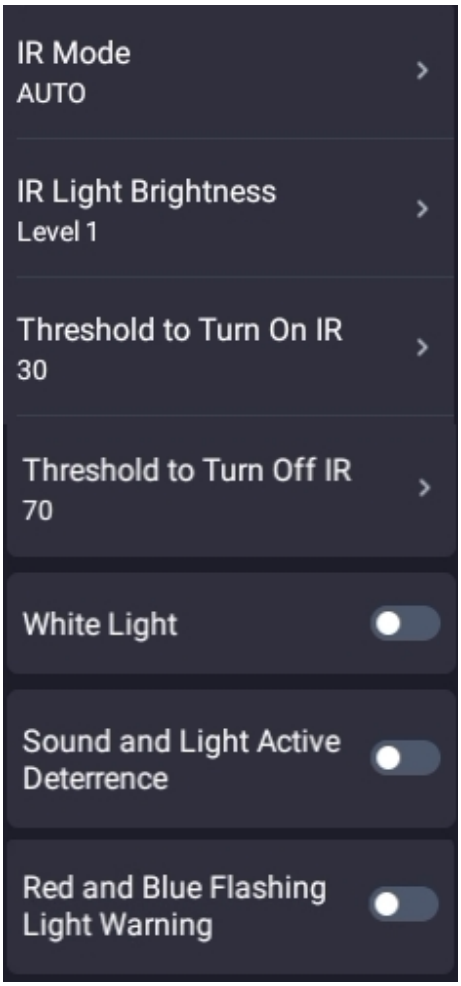


Table 3-9 Light settings

Parameter	Description
IR Mode	Night vision mode. Select the mode from **AUTO** , **OPEN**, and **CLOSE**. **CLOSE** is selected by default.
IR Light Brightness	Configure the brightness of the infrared light. You can set the level to Level 1, Level 2, Level 3, Level 4 and Level 5, and it is Level 1 by default.

Parameter	Description
Threshold to Turn On/Off IR	In the **AUTO** mode, set the threshold for the IR light to turn on and turn off. The default for the IR light to turn on is 30 and to turn off is 70.
White Light	Tap to turn on the white light.
Sound and Light Active Deterrence	Tap to use loud sounds and bright lights to serve as a warning.
Red and Blue Flashing Light Warning	Tap to turn on the red and blue flashing light.

3.5.2.5 Sound Settings

You can configure media and notification volume, enable or disable other sounds and vibrations.

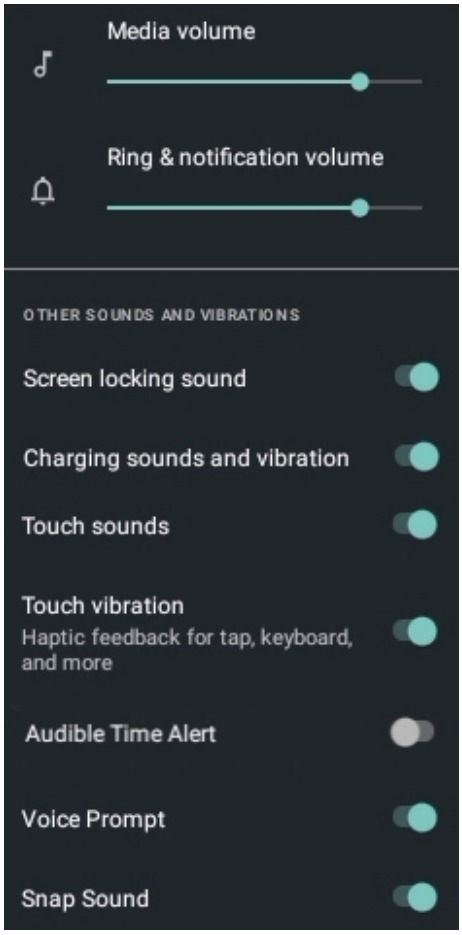
Procedure

Step 1 Select **Device** > **Sound Settings**, and then drag the slider to adjust the media and ring & notification volume.

- Media volume involves video and audio playback.
- Notification volume includes key tones, capture success sound, and more.

Step 2 Tap to enable other sounds and vibrations, including screen locking sounds, charging sounds and vibration, touch sounds, touch vibration, audible time alert, voice prompt and snap sound.

Figure 3-31 Adjust sound



3.5.2.6 FN Button

Select **Device** > **FN Button**, and then you can choose **None** , **Red and Blue Flashing Light Warning**, **Sound and Light Active Deterrence**, **White Light** and **Stealth Mode** associated with pressing the FN key for 2 seconds.

3.5.2.7 Alarm Settings

Select **Device** > **Alarm** to configure the alarm settings.

Figure 3-32 Alarm settings

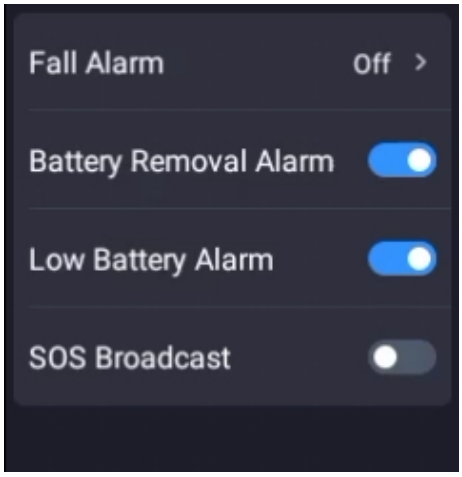


Table 3-10 Alarm setting parameters

Name	Parameter
Fall Alarm	An alarm is triggered when the device falls down to the ground and the rear camera starts recording videos. You can set the auto recording time from **1 min** , **3 min**, **5 min**, **10 min** or you can select **Manually Stop**.
Battery Removal Alarm	An alarm is triggered when the battery is removed.
Low Battery Alarm	An alarm is triggered when the battery gets low.
SOS Broadcast	A broadcast alarm is triggered when the device enables the SOS function. The nearby MPT 230, MPT230-P and MPT230-P/E devices will automatically start recording key videos via bluetooth.

When the over temperature protection is triggered, the Device will send a notification to prompt you to handle the temperature anomaly to avoid slow screen response, system failure or data exception.

When the temperature becomes too high, the device will automatically shut down.

3.5.2.8 Data Overwrite

Select **Device** > **Overwrite when storage full**, and then enter the password of the admin account to enable or disable data overwriting. After the function is enabled, the oldest non-key files will be overwritten when the storage space is full.

This function is only available for admin account.

3.5.2.9 Auto Recording at Startup

Select **Device** > **Auto Recording at Startup**, and then tap to enable the function. Enter the admin password and then tap **OK**. The device will start video recording automatically after system starts up.

This function only can be enabled by the admin user.

3.5.2.10 Verify to Stop Recording

Enable the function, click **Stop Recording** (including both physical buttons and on-screen buttons such as manual/auto stop buttons in the preview page and task page). An admin password or gesture password will first pop up for verification, and the recording will only stop after successful verification.

3.5.2.11 Verify to Shutdown or Restart

Enable the function, and then when holding down the power-off button and clicking to shut down/restart, a pop-up window will first require admin password or gesture verification. Only after successful verification will the shutdown/restart be permitted.

3.5.2.12 Stealth Mode

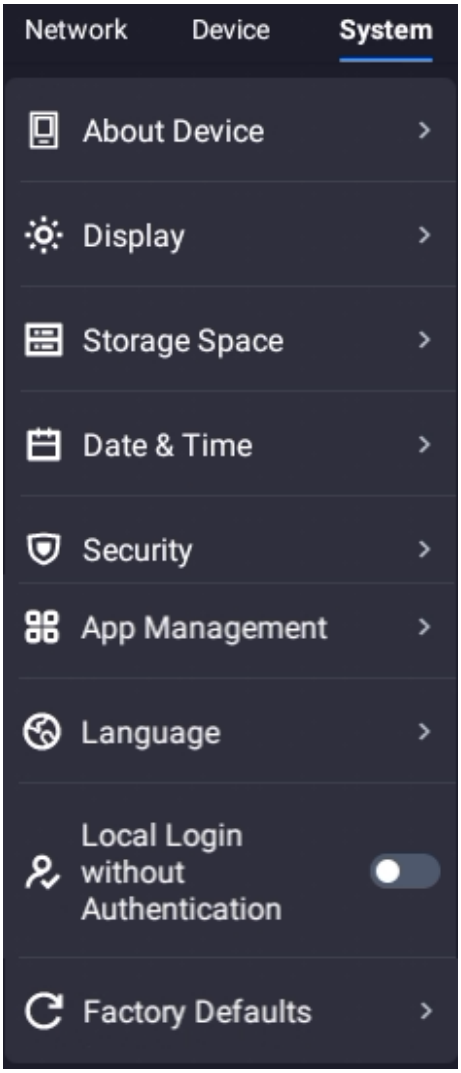
Select **Device** > **Stealth Mode**, and then tap to enable the function.

If it is enabled, the system will turn off vibration, sound and light during video recording, audio recording, photo taking, and intercom communication.

3.5.3 System

On the main screen, tap , and then select **System**. You can configure security, display, date and time, language, and more.

Figure 3-33 System



3.5.3.1 About Device

Select **System** > **About Device** to view device information such as device name, serial number, and Android version.

3.5.3.2 Display

Select **System** > **Display** to adjust the screen brightness and device hibernation time.

Figure 3-34 Display

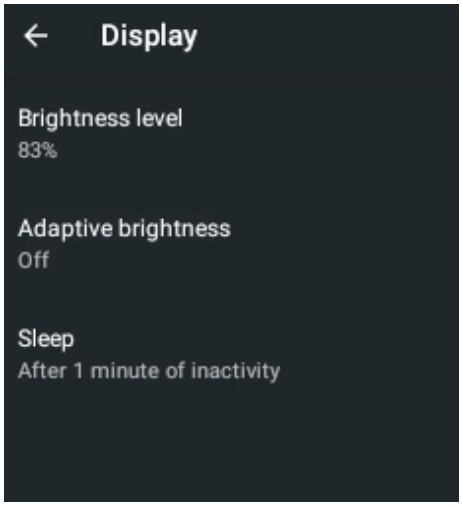


Table 3-11 Display parameters

Parameter	Description
Brightness level	Adjust the screen brightness.
Adaptive brightness	Automatically adjusts the screen brightness according to the environment and activity.
Sleep	Configure the hibernation time. The Device automatically hibernates after the predefined time of inactivity.

3.5.3.3 Storage Space

Select **System** > **Storage Space** to view the used and total storage space.

If you want to use an SD card, make sure to format it to FAT32 first. After you insert an SD card, the Device will display the used and total storage space of the SD card. If the format is wrong, you can format the card.

3.5.3.4 Date & Time

Select **System** > **Date & Time** to configure date and time settings.

Table 3-12 Date & Time parameters

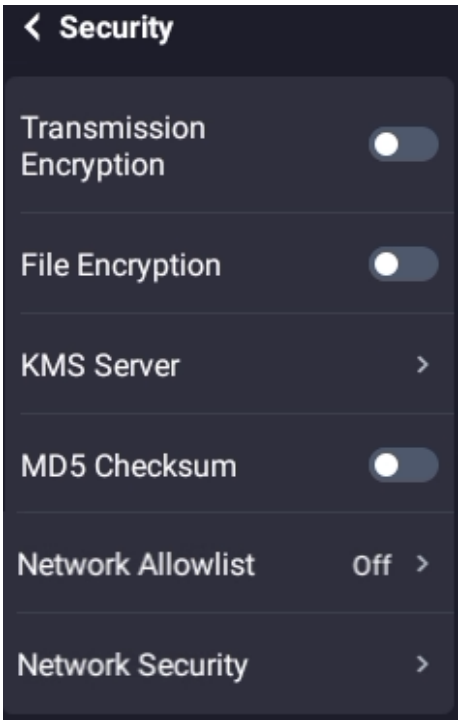
Parameter	Description
Time Sync	Sync device time with the network, platform or GPS satellite. ● To sync with the network time, ensure that the Device is connected to the network, such as a 4G or Wi-Fi. ● To sync with platform time, ensure that the Device is connected to the platform. ● The Device can also sync time through MPT Manager. ● To sync time through GPS satellite, ensure that **Location Service** is enabled. For details, see "3.5.1.5 Location Services".
Select time zone	You can select time zone when **Automatic time zone** is disabled or enable the automatic time zone to use network-provided time zone.

3.5.3.5 Security

Procedure

Step 1 Select **System** > **Security**.

Figure 3-35 Security



Step 2 Configure the parameters.

Table 3-13 Security parameters

Parameter	Description
Transmission Encryption	Enable encryption for transmission.

Parameter	Description	
File Encryption	Enable encryption for files. WAV and MP4 formats do not support file encryption.	
KMS Server	Configure the address of the file encryption server.	
MD5 Checksum	Enable it to verify if the file has changed during transmission or storage.	
Network Allowlist	To allow access of only trusted IPs, MACs and ports, enable **Network Allowlist** and then add the trusted IPs, MACs and ports.	
Network Security	Security Exception Alarm	Displays alarm information when an exception occurs.
	Login Authentication	Configure login mode. We recommend you turn on security mode to avoid security risks.
	Dynamic Multi-link	Enable it to set an independent link for each request. It is used during live view video, voice talk and playback.
	Private Protocol	Enable it to enhance security for data transmission.
	Security Authentication	Select **MD5** or **SHA256** for security authentication. • At least one item should be selected. • You can select **MD5** and **SHA256** simultaneously, and **SHA256** takes priority.

3.5.3.6 App Management

3.5.3.6.1 Viewing App Information

Select **System** > **App Management** > **App info**, enter the password, and then you can view the information on the apps.

Only the admin account has the permission to view the app information.

3.5.3.6.2 Configuring the Startup App

Select **System** > **App Management** > **Power On**, enter the password, and then you can set the startup app that runs automatically after the system starts up.

- Tap **Clear All** to remove all the startup settings.
- You can set only one startup app.
- Only the admin account has the permission to set the startup app.

3.5.3.6.3 Installing Platform Apps

Install the platforms apps that have been configured in advance.

Procedure

Step 1 Select **System** > **App Management** > **Platform app installation**.

Step 2 Select a pre-configured platform apk file.

The apk files are configured before the Device leaves the factory. Contact the technical support to get other apk files.

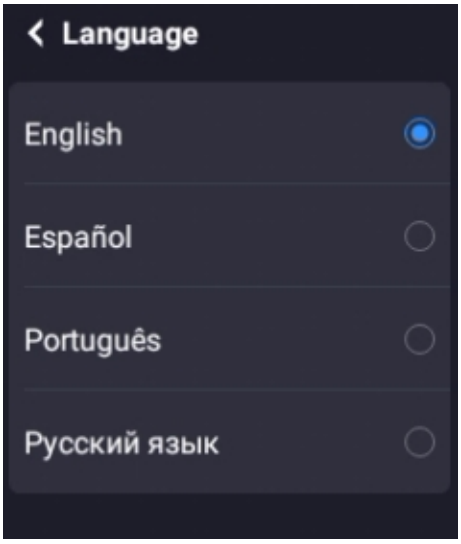
Step 3 Follow the on-screen instructions to install the app. The installed app will appear on the home screen.

3.5.3.7 Language

Select **System** > **Language** to configure the device language, keyboards and tools.

You can select English, Spanish, Portuguese and Russian.

Figure 3-36 Configure language



3.5.3.8 Login without User Verification

Select **System** > **Login without user verification**. Tap and click **Open** to enable the function. You do not need to enter the password for unlocking the Device or after the Device restarts up. The other related operation still needs to enter the password.

After this function is enabled, all users can directly access the Device.

3.5.3.9 Reset

Restore the Device to default settings.

- Restoring default settings will clear all data stored on your Device, including system, app data and settings and face and ANPR files. The Device still retains the serial number. You can select whether to clear video, audio and image data in the internal storage and micro SD card. Proceed with caution.
- Only the admin account has the permission to reset the Device.

Procedure

Step 1 Select **System** > **Reset**.

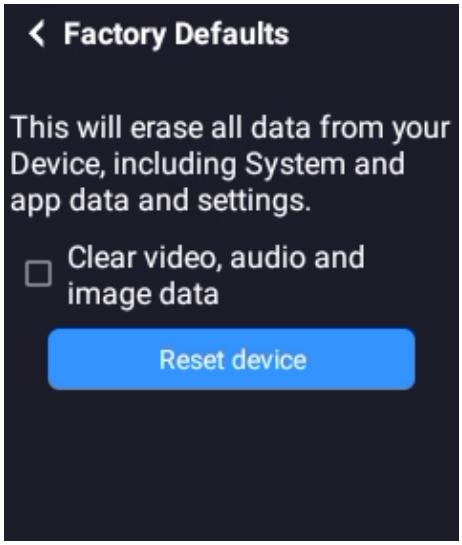
Step 2 Select **Clear video, audio and image data**.

This option is unchecked by default.

Step 3 Tap **Reset device** , and then tap **Erase everything**.

Step 4 Enter the password, and then tap **OK**.

Figure 3-37 Reset



3.6 System Maintenance

On the home screen, tap **Maintenance**, and then you can perform maintenance operations such as system update, and ping test.

3.6.1 Online Update

When the device is connected to the internet, it can be updated online. Before it is updated, you need to check whether there is the latest version. The version check can be done automatically or manually.

Procedure

Step 1 On the home screen, select **Maintenance** > **Online Update**.

Step 2 Check the version.

- Auto check: Tap to enable the **Auto check** function.
- Manual check: Tap **Manual check** to check whether there is the latest version.

Step 3 Tap to update the system.

If the page shows "You are using the latest version", you do not need to update the system.

3.6.2 Platform Upgrade

Upgrade the platform in the device.

Procedure

Step 1 On the home screen, select **Maintenance** > **Platform Upgrade**.

Step 2 Click to enter the update server page.

Step 3 Enter the IP address and port, and then click **Save**.

Subsequent updates will be pushed via the platform's upgrade package.

3.6.3 Local System Upgrade

On the home screen, select **Maintenance** > **Local System Upgrade**. The Device detects update package automatically. After local update package is detected, you can select the package to update the system.

3.6.4 Scan to Update

You can scan the QR code to get the update file and then update the system.

Procedure

Step 1 On the home screen, select **Maintenance** > **Scan to Update**.

Step 2 Scan the QR code that corresponds to the update file.

Step 3 Tap **Download** to download the update file.

Anonymous login is enabled by default. You can tap **SETTINGS** on the upper-right corner of the **Scan to Update** screen, disable anonymous login and then configure the FTP username and password.

Step 4 After the download is complete, tap **OK** to update immediately.

You can also use the update file to update the system later. For details, see "4.2 Updating on Local Device".

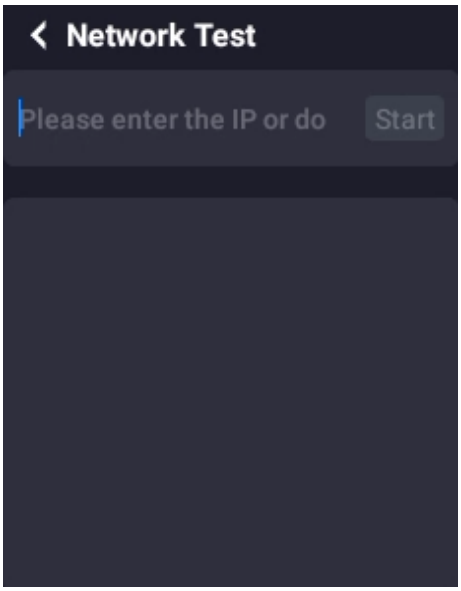
The Device suspends the download process when network breaks down and resumes downloading when network is recovered.

3.6.5 Network Test

You can test the network connection.

On the home screen, select **Maintenance** > **Network Test**, enter the target IP address or the domain name, and then tap **Start**.

Figure 3-38 Ping test



3.6.6 Network Capture

You can capture data packets and share them through Bluetooth. The packets help to diagnose and solve network problems.

Prerequisites

To share captured packet, you need to turn on Bluetooth. For details, see "3.5.1.4 Bluetooth".

Procedure

Step 1 On the home screen, select **Maintenance** > **Network Capture**.

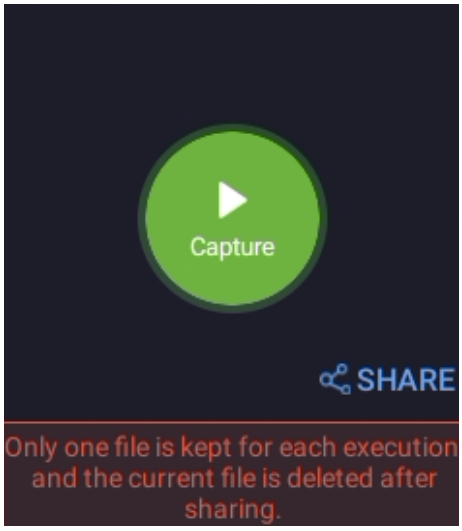
Step 2 Tap **Capture** to capture data packets.

Step 3 Tap **StopCap** to stop capturing data packets.

Step 4 Tap **SHARE** to send the captured packet to a Bluetooth device.

The shared file will be deleted automatically. If you tap **Capture** again, the previously captured packets will also be deleted automatically.

Figure 3-39 Network capture



3.6.7 Log Package

The logs record the information on the system operation, through which you can identify some abnormal operations. You can package the logs and share them through Bluetooth.

Prerequisites

To share log package, you need to turn on Bluetooth. For details, see "3.5.1.4 Bluetooth".

Procedure

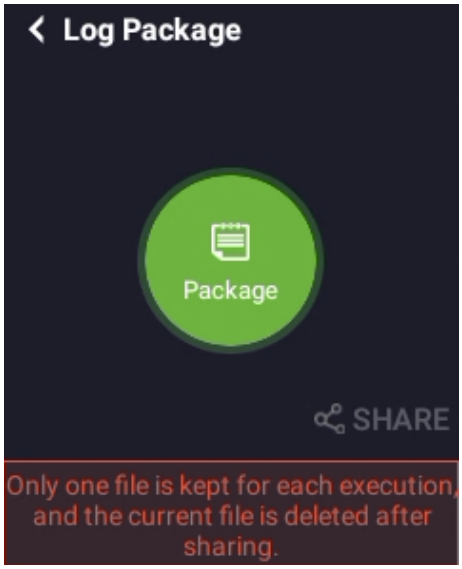
Step 1 On the home screen, select **Maintenance** > **Log Package**.

Step 2 Tap **Package** to compress logs into one package.

Step 3 Tap **SHARE** to send the log package to a Bluetooth device.

The shared file will be deleted automatically.

Figure 3-40 Log package



3.6.8 Signal Strength and Band

Check the signal and band of SIM card.

On the home screen, select **Maintenance** > **Signal Strength and Band**, the SIM card provider name, network information, mobile network type, signal intensity and band of SIM card will be displayed automatically.

Supports the dual-card configuration.

3.6.9 ADB Network Debugging

On the home screen, select **Maintenance** > **ADB Network Debugging**, and then tap . After the device connects to the network, you can debug the device through ADB network.

3.7 Audio Recording

3.7.1 Recording Audio

Press on any screen to record audio, or tap on the home screen, and then tap .

Figure 3-41 Record audio

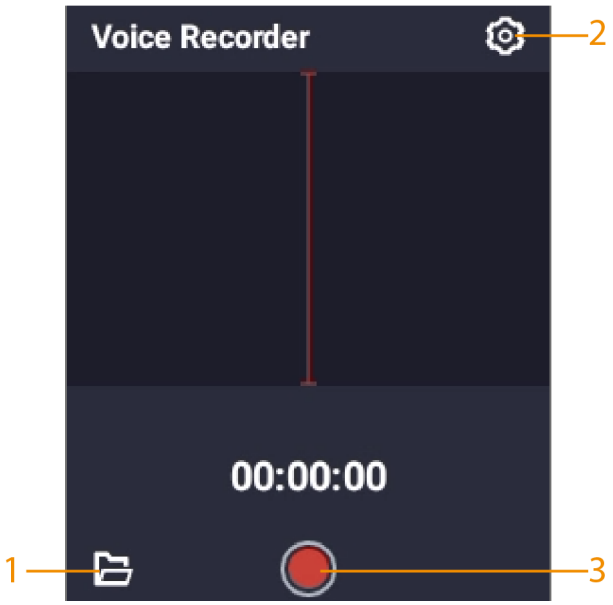


Table 3-14 Audio recording functions

No.	Function
1	Tap the icon and then enter password or unlock pattern to view and manage audio files.

No.	Function
2	Tap the icon to set audio format and file format. During recording audio process, icon 1 and 2 are hidden.
3	Tap the icon to start recording audio. Tap to stop. System prompts "Stop recording audio".

3.7.2 One Press to Record Audio

When the Device is sleeping, press to start recording audio. Press again to stop.

3.8 Video Recording

3.8.1 Recording Video

- To start recording, tap on the home screen, tap to start recording video, and then tap to stop recording.
- Press to start recording video, and then press again to stop recording.

Figure 3-42 Record video

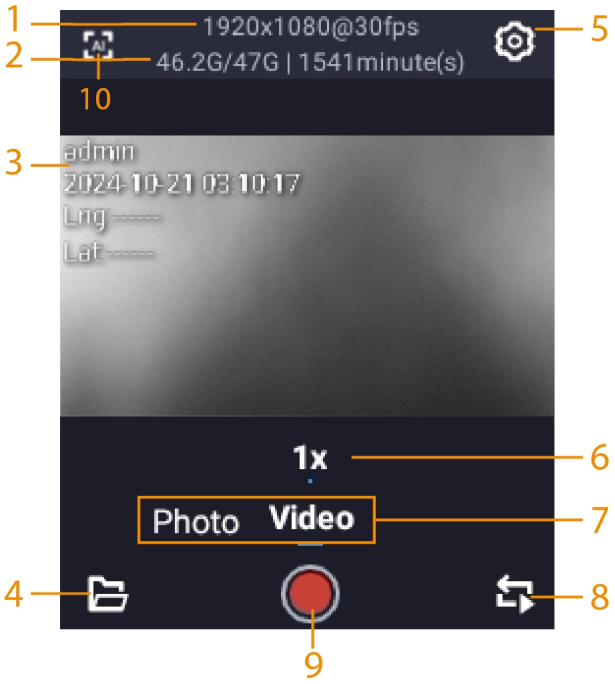
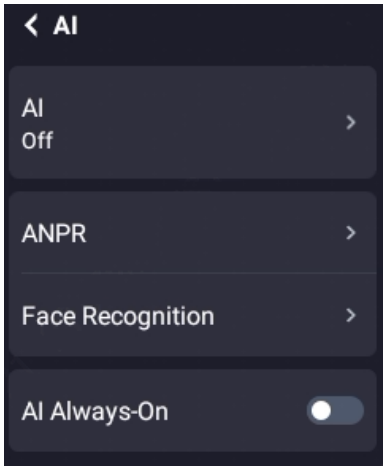
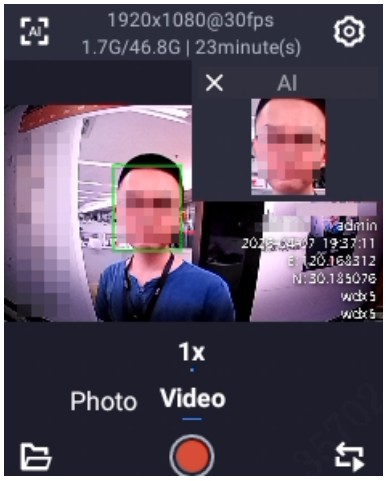
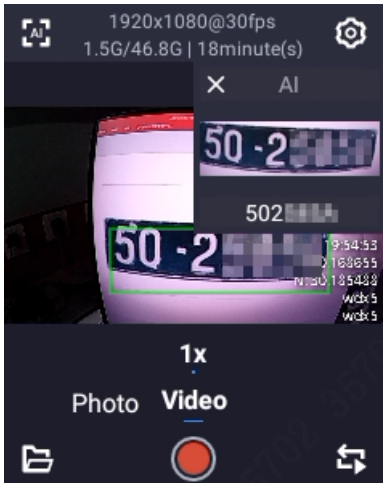


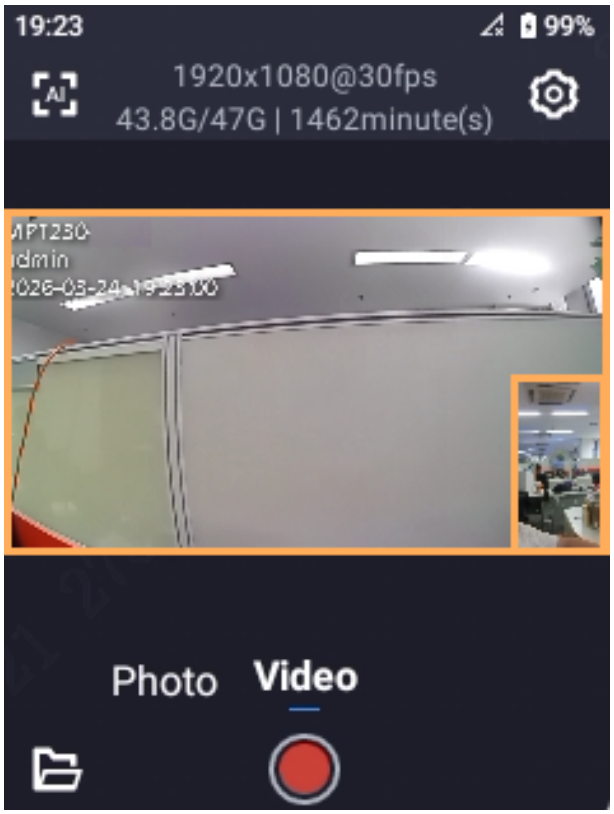
Table 3-15 Video recording functions

No.	Description
1	Video quality. Shows picture resolution when the Device is in capturing mode.
2	Remaining capacity/total capacity, and remaining recording time. ● The remaining recording time varies with video quality. ● Shows the remaining capacity/total capacity in capturing mode, and the remaining number of pictures that you can take.
3	Date, time, GPS information, and custom information. ● To show GPS information, make sure that location service and GPS display are enabled. Select > **Network** > **Location Service** to enable positioning; select > **Device** > **Camera Settings** > **Overlay** > **GPS OSD** to enable GPS display. ● Supports to configure the custom OSD information on local, and then enable custom information display in > **Device** > **Camera Settings** > **Overlay**.
4	Tap the icon and then enter password to view and manage video files.
5	Camera settings. For details, see "3.5.2.1 Camera Settings".
6	Tap to select the zooming degree. It can be zoomed at 1.0, 2.0, 4.0, 6.0 and 8.0 times.
7	Tap to switch between recording mode and capturing mode.
8	Tap the icon to switch between front camera and rear camera.
9	● When the Device is in recording mode, tap to start recording video and then tap to stop. ● When the Device is in capturing mode, tap to take a picture.

No.	Description
10	Click the AI icon to quickly enter the page of AI function configuration. Figure 3-43 AI  When the system detects a face or license plate, an AI prompt box will appear and collect facial or ANPR information. Figure 3-44 AI prompt box (face)  Figure 3-45 AI prompt box (ANPR) 

If you enable the picture-in-picture function, the video will display dual-screens.

Figure 3-46 Record video (picture-in-picture)



The device supports USB external cameras and HDMI-to-USB devices (also virtualized as cameras), enabling recording and streaming for these cameras. The HDMI cable allows input from another host (computer, drone, etc.) to the MPT device, displaying the input feed on the camera interface.

3.8.2 One Press to Record a Video

When the Device is sleeping, press to start recording video. The Device prompts "Start recording video" and the login screen is displayed with a recording icon in the notification bar.

Press again to stop recording video, and you can hear a sound prompt "Stop recording video".

If the device you are using has a recording button on the back, you can press the button to start recording a video.

3.8.3 Focusing

On the live view screen, tap the screen, and then you can select the zooming degree at X1.0, X2.0, X4.0, X6.0 and X8.0.

Front cameras, external cameras, and picture-in-picture do not support this function.

3.8.4 Marking Important Videos

When a fall alarm is triggered or SOS button is pressed, the Device automatically records videos which are marked as important files.

During recording videos, you can also mark a video as an important file by pressing and holding .

Tap to view files. The important files are marked with ★, and their names end with _IMP.

3.9 Pictures

3.9.1 Taking a Picture

On the live view screen, press or tap . The working indicator light flashes red and system prompts success.

3.9.2 One Press to Take a Picture

When the Device is sleeping, press to take a picture. If you have configured continuous shot, you can press once to take the defined number of pictures.

3.10 Files

You can view pictures, videos, audio files, face detection, face recognition, and ANPR files saved in your device.

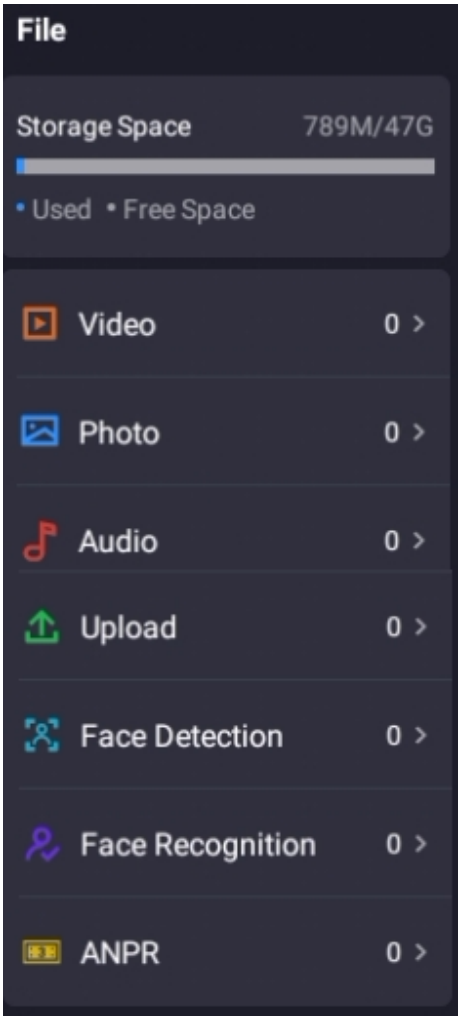
3.10.1 Viewing Pictures

Procedure

Step 1 On the home screen, tap .

Step 2 Draw the unlock pattern or enter your login password, and then tap **OK**.

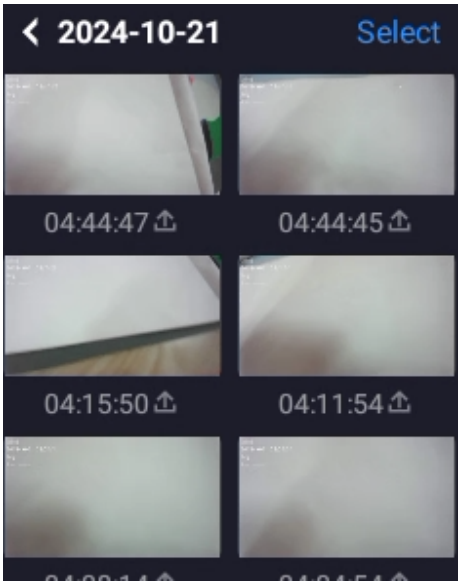
Figure 3-47 Files



Step 3 Tap **Photo**, select a folder, and then tap a picture to play.

The folders are displayed in chronological order, and the newest folder is on the top of the list.

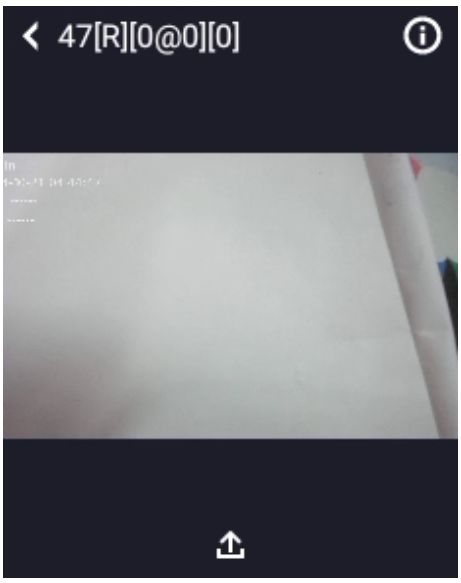
Figure 3-48 Select a picture



- To select a picture, tap and hold it, and appears on the right-bottom corner of the picture. means the picture has been selected.
- Tap All to select all the pictures in the current folder.
- Tap **Cancel** to unselect pictures.

Step 4 Tap a picture.

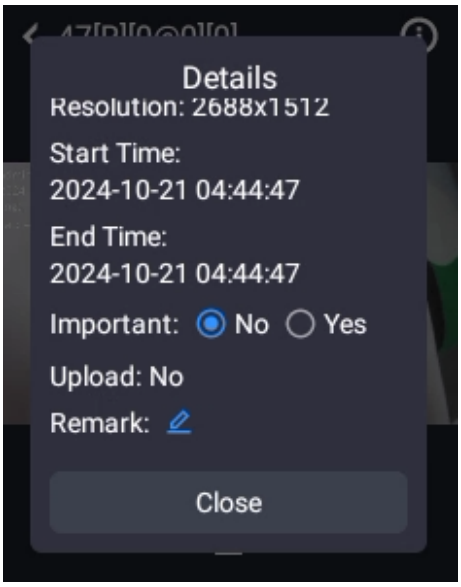
Figure 3-49 View a picture



- When viewing a picture, swipe left or right on the screen to see the previous or next pictures.
- Use two finger to zoom in or out the picture.
- When floating button is used for back operation, tap to go back to the picture list; when gesture is used, swipe left or right from the screen edge instead.

- Tap to view details of the selected picture, such as file type, size, and resolution. Tap **Yes** next to **Important** to mark the picture as an important file. Tap **No** to cancel the mark.

Figure 3-50 Details



- Tap to upload the picture to platform.

3.10.2 Playing Video

Procedure

Step 1 On the home screen, tap .

Step 2 Draw the unlock pattern or enter your login password, and then tap **OK**.

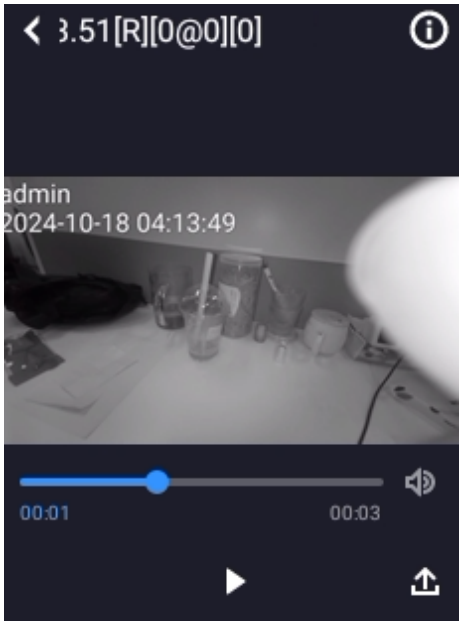
Step 3 Tap the **Video** tab.

Step 4 Select a folder.

The folders are displayed in chronological order, and the newest folder is on the top of the list.

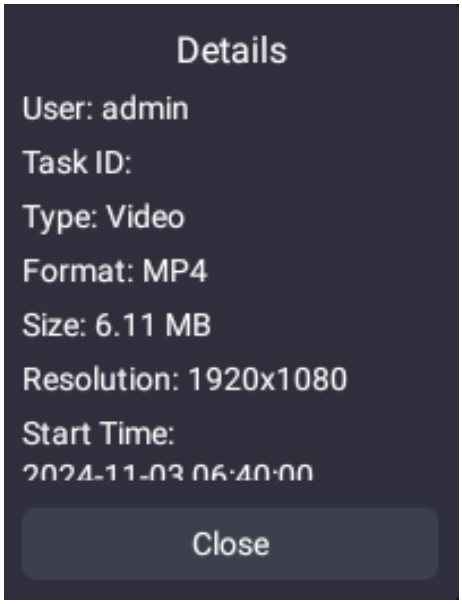
Step 5 Tap the video file to play.

Figure 3-51 Play video



- When viewing a video, swipe left or right on the screen to play the previous or next videos.
- Drag the progress bar to fast-forward or rewind.
- Tap to pause.
- Tap to adjust volume.
- When floating button is used for back operation, tap to go back to the video list; when gesture is used, swipe left or right from the screen edge instead.
- Tap to view video details.

Figure 3-52 Details



- Tap to upload the current video to the platform.

3.10.3 Playing Audio

Procedure

Step 1 On the home screen, tap .

Step 2 Draw the unlock pattern or enter your login password, and then tap **OK**.

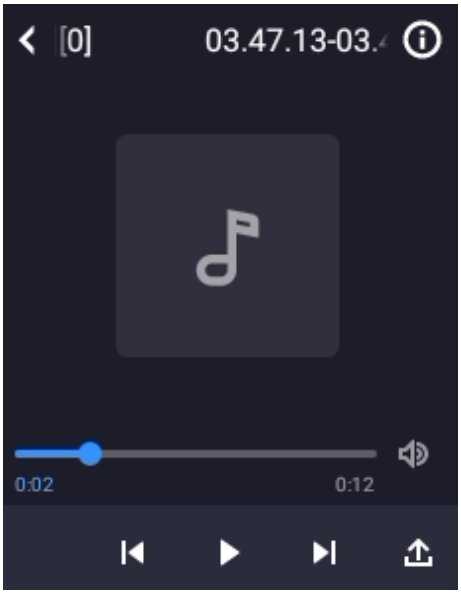
Step 3 Tap the **Audio** tab.

Step 4 Select a folder.

The folders are displayed in chronological order, and the newest folder is on the top of the list.

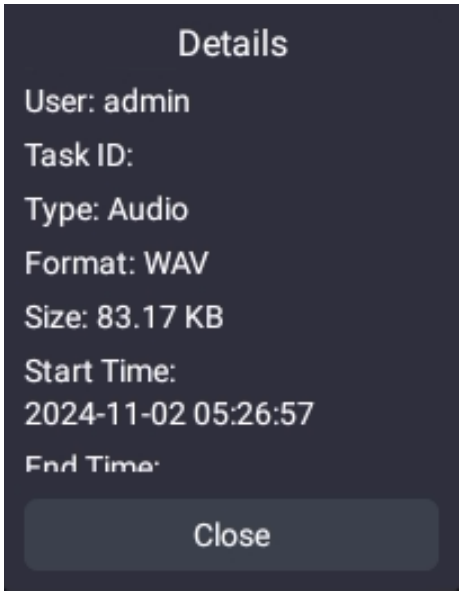
Step 5 Tap the audio file to play.

Figure 3-53 Play audio



- Tap or to play the previous or next audio in the folder.
- Drag the progress bar to fast-forward or rewind.
- Tap to pause.
- Tap to adjust volume.
- When floating button is used for back operation, tap to go back to the audio list; when gesture is used, swipe left or right from the screen edge instead.
- Tap to view audio details.

Figure 3-54 Details



- Tap to upload the current audio to the platform.

3.10.4 Viewing AI Function Files

You can view face detection, face recognition and ANPR files and select them to delete.

Procedure

Step 1 On the home screen, tap .

Step 2 Draw the unlock pattern or enter your login password, and then tap **OK**.

Step 3 Select **Face Detection** , **Face Recognition** or **ANPR** to view the corresponding files.

Figure 3-55 Face detection results

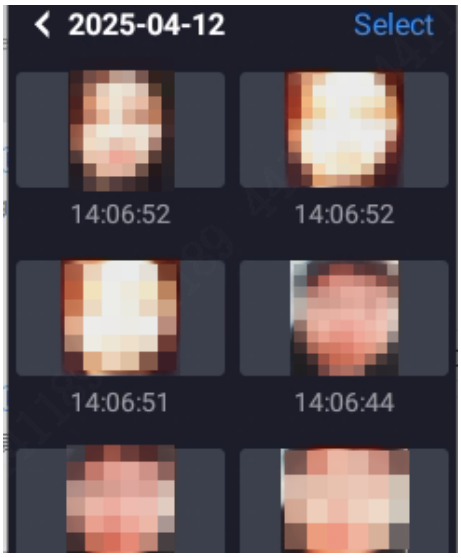


Figure 3-56 Face recognition results

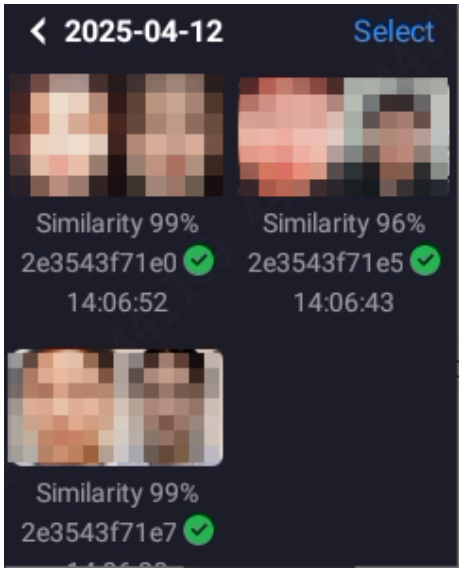
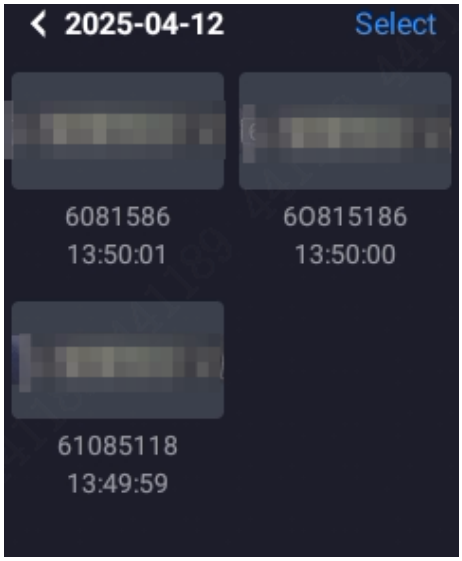


Figure 3-57 ANPR results



Related Operations

- Click **Select** to select some results to delete.
- Click **Select** and select **All** to delete all results.

3.11 Switching between Video and Audio Recording

You can switch between video and audio recording with a simple press.

- When the Device is recording video, press , or tap on the home screen and then tap to stop recording video and start recording audio.
- When the Device is recording audio, press , or tap on the home screen and then tap to stop recording audio and start recording video.

3.12 Light & Sound Icons

Light & sound can be used to assist in law enforcement at night or with low illuminance.

Swipe down the notification bar, and then tap the icons to open the light & sound indicators.

Table 3-16 Light icons

Icons	Description
	Flashlight
	IR light
	Red and blue flashing light with loud sound
	Red and blue flashing light without sound

The light & sound cannot be enabled when the battery level is lower than 5%.

3.13 Data Transmission

You can upload data from the Device to MPT Manager and data acquisition station.

- Make sure that the **Private Protocol** is enabled.
- After starting the Device, use USB cable to connect the Device to the PC, start MPT Manager, enter password, and then confirm to download the data.
- Start the Device, and connect it to a legal data acquisition station through the USB cable. For the first-time use, you need to enter the password, and then the data on the Device can be uploaded to data acquisition station. If the device information is not displayed on the interface, unplug USB and plug it again.

3.14 Log

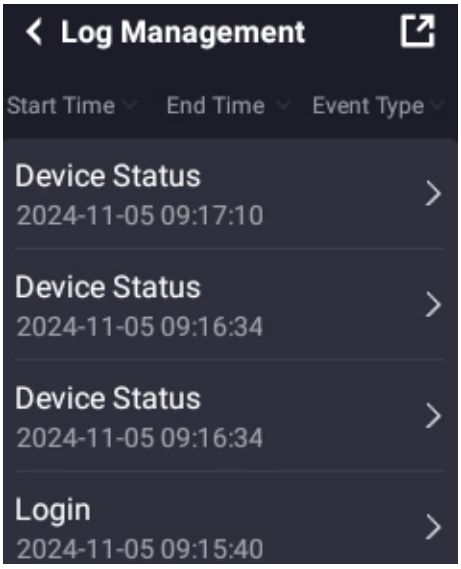
You can view the device log by selecting the start time, end time and event type.

Procedure

Step 1 Tap to enter the log management screen.

Step 2 Select the start time, end time and event type.

Figure 3-58 Log management



Results

The logs are displayed in the form of a list.

Related Operations

Click to share logs to other devices. You can select **TF card or root path** or **Bluetooth sharing** as the export mode.

3.15 Creating and Joining Tasks

You can create or join tasks in this device and track the tasks to be completed.

Procedure

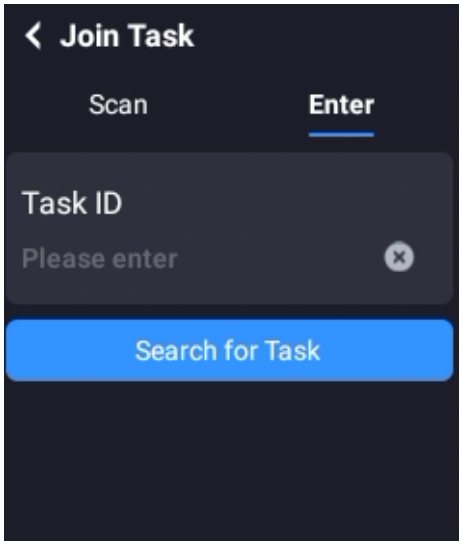
Step 1 Tap to enter the task list screen.

Step 2 Tap **+ Join Task**.

- Join by scanning the QR code: Scan the code generated by the task ID.
- Join by entering the task ID: Enter the task ID to create the new task ID, and then click **Search for Task**.

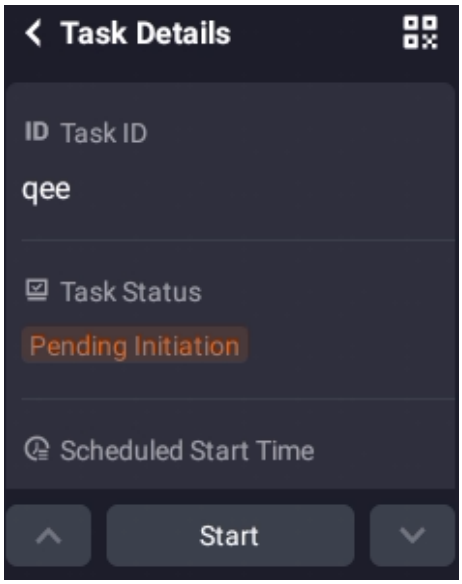
You can also locate the task ID you created through this way.

Figure 3-59 Join by ID



Step 3 Configure the task details as required.

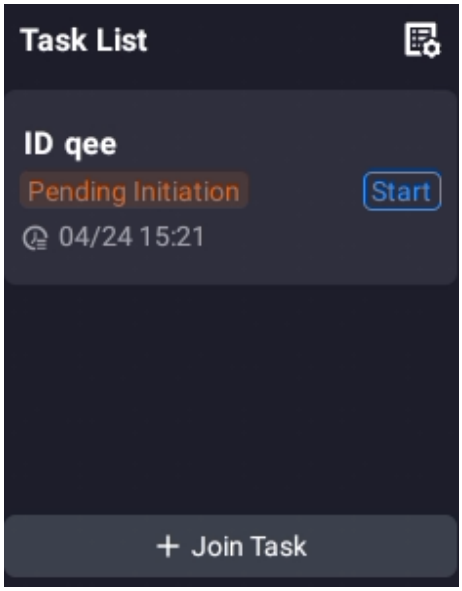
Figure 3-60 Task details



Tap to view the QR code generated by the task ID.

Step 4 Re-enter the task screen and the tasks are displayed in the list.

Figure 3-61 Task list

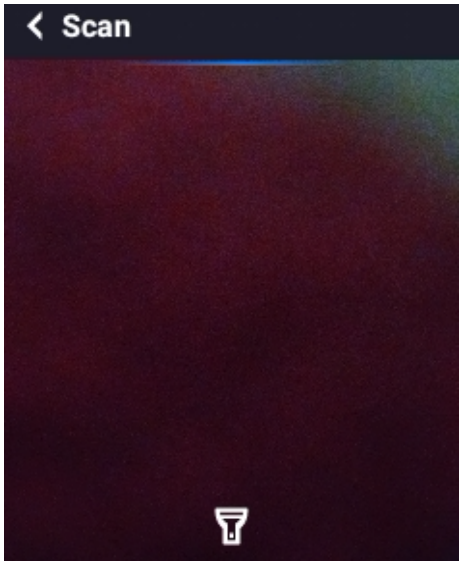


- Tap **Start** , **Continue** and **Done** to configure the status of each task. Even if a task is completed, it can be continued again.
- The details of the generated video, audio, and image files will have task IDs.
- Swipe down on the home screen, and the tasks in progress are displayed.

3.16 Scanning the QR Code

Tap to enter the scanning screen. You can scan the QR code to copy it, and if you have any platform software installed, you can paste it and send it.

Figure 3-62 Scan the QR code



Click to enable the white light for supplementing light.

4 System Update

You can update the system on MPT Manager or on the local device.

4.1 Updating on MPT Manager

Procedure

Step 1 Install MPT Manager.

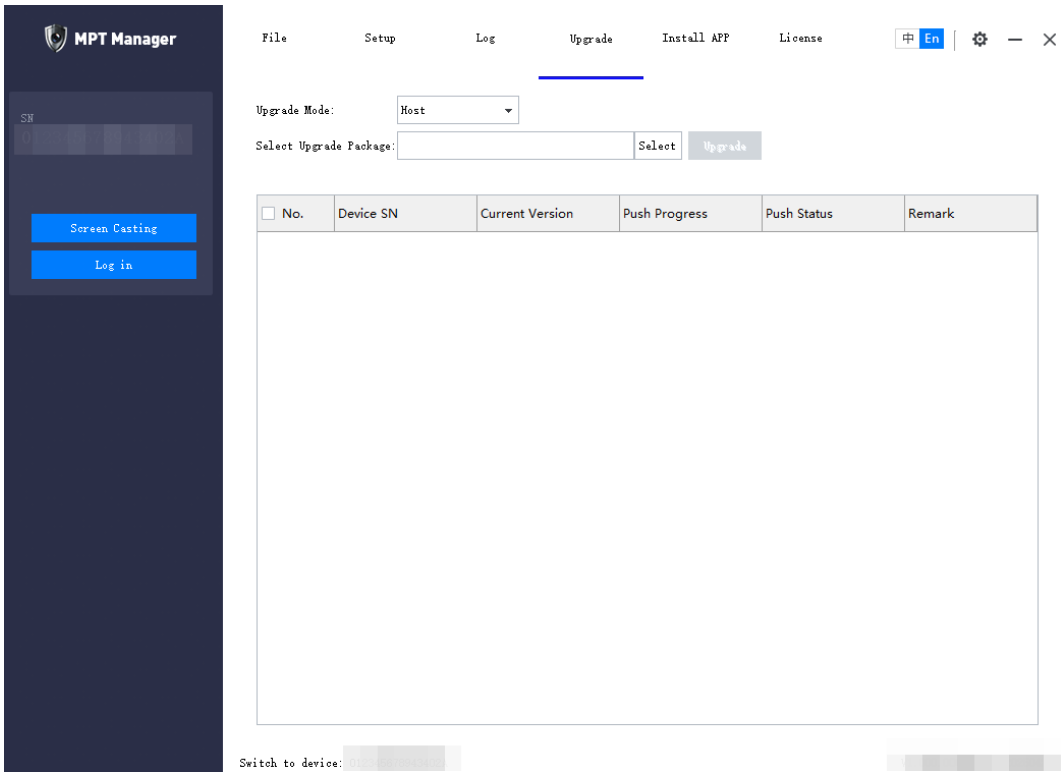
Follow the system prompts and click **Next** until the installation is complete. After that, a shortcut icon for MPT Manager will be displayed on your computer desktop.

Step 2 Start the Device, and then connect it to your computer through USB cable.

Step 3 Double-click on the desktop, click **Log in** to enter device password, and then click **OK**.

Step 4 Click **Upgrade** to enter the upgrade page and select the update mode from the drop-down list.

Figure 4-1 Upgrade



Step 5 Click **Select** to select the upgrade package and click **Upgrade**.

The MPT Manager page might be updated; please refer to the actual page.

Step 6 Select the device and click **Upgrade**.

The push progress becomes 100% when the update package is successfully pushed to the Device.

4.2 Updating on Local Device

You can update the system in the local device in the following ways.

- Online Update: For details, see "3.6.1 Online Update".
- Local System Upgrade: For details, see "3.6.3 Local System Upgrade".
- Scan to Update: For details, see "3.6.4 Scan to Update".

5 Platform Operations

After connecting the Device to the platform, users with corresponding permissions can access and manage the Device on the platform.

5.1 Adding the Device to the Platform

Add the Device to the platform for remote management. For details on platform operations, see the corresponding user's manual of the platform.

Prerequisites

- The Device and the platform are on the same network segment.
- If you want to add the device to the platform through registration, make sure to configure the registration settings on the Device. For details on registration settings, see "3.5.1.1.1 Auto Registration".

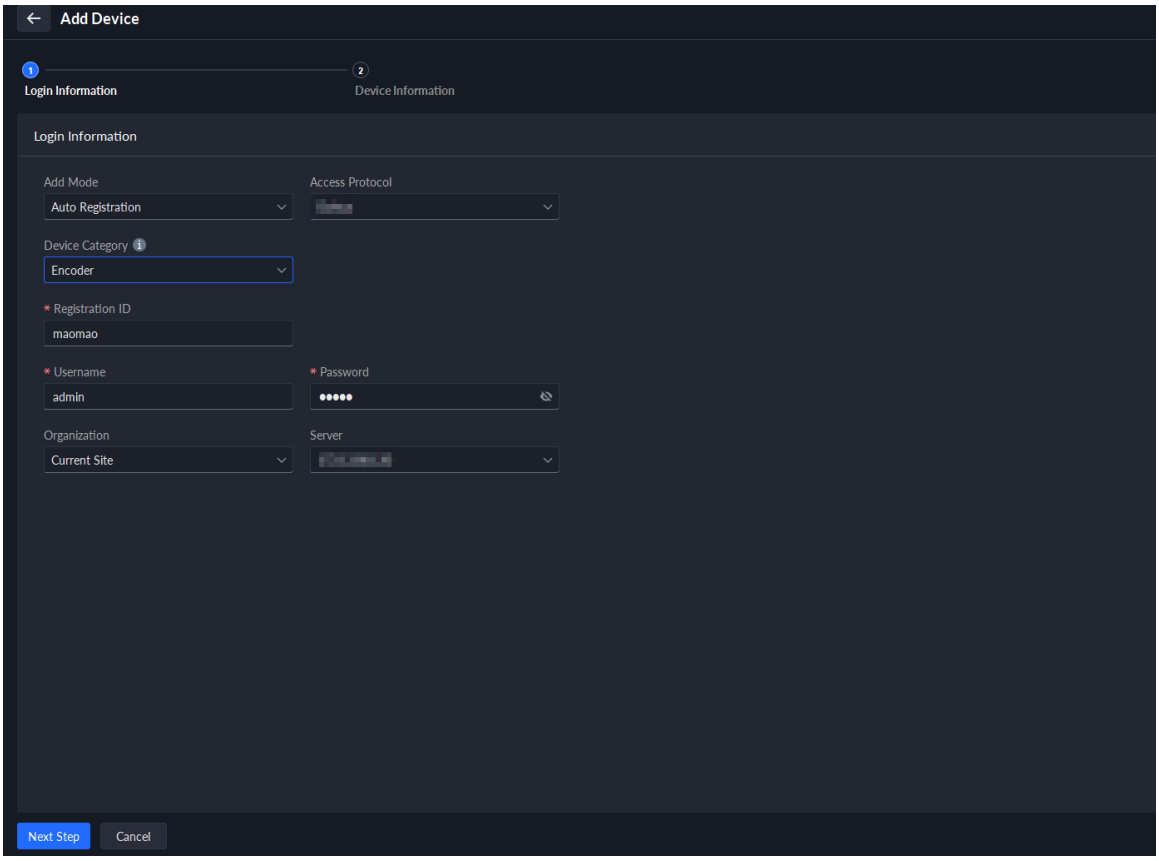
Procedure

Step 1 Log in to the DSS Client.

Step 2 On the home page, click , and then select **Basic Config** > **Device**.

Step 3 On the **Device** page, click **Add**.

Figure 5-1 Add MPT (1)



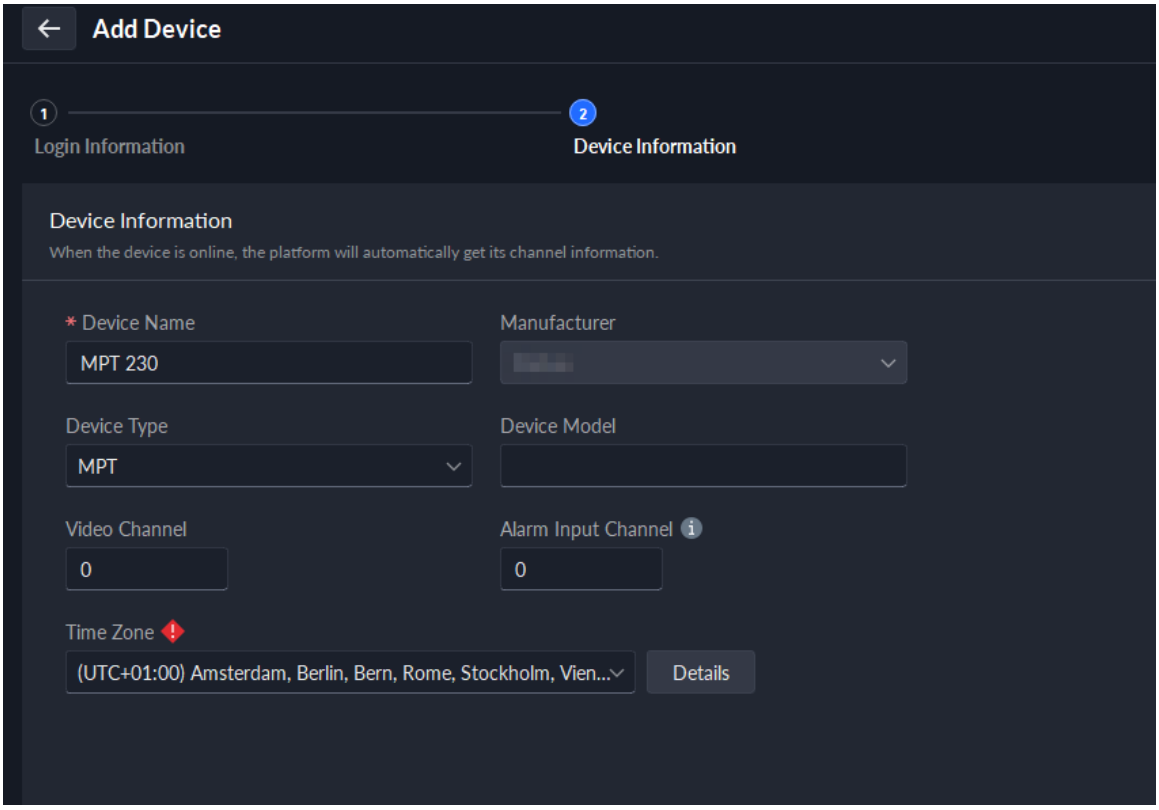
Step 4 Configure the parameters.

Table 5-1 Parameters of adding the device

Parameter	Description
Add Mode	• **Auto Register** : Register the Device using the registration ID. It is the most common method. • **IP Address** : Register the Device using its IP address.
Device Category	Select **Encoder**.
Registration ID	If you select **Auto Register** as **Add Type**, enter the registration ID of the Device. The registration ID must be the same as the one entered on the MPT device when registering the platform.
IP Address	If you select **IP Address** as **Add Type**, enter the IP address and port number of the Device. The port is 37777 by default.
Device Port	
User	Enter the username and password of the Device.
Password	
Organization	Select the organization that the Device belongs to. The default organization code is **Current Site**.

Step 5 Click **Next Step**.

Figure 5-2 Add MPT (2)



Step 6 Configure the device information.

Table 5-2 Parameters of device information

Parameter	Description
Device Name	Customize the device name.
Type	Select **MPT**.
Video Channel	The default value is 0. When the device channels cannot be displayed on certain platforms, it is recommended to enter 2.
Alarm Input Channel	The default value is 0.
Time Zone	Select the time zone.

Step 7 Click **OK**.

Step 8 Click of the added device, select **Basic Info**, and then get device SN information. Otherwise, you might fail to add the device.

5.2 Connecting to the Platform

Register the Device to the platform. For details, see "3.5.1.1.1 Auto Registration".

6 Battery Maintenance

- The device supports5 V/2 A DC power supply. Please charge the device promptly when the battery level is low.
- When the main battery is installed, the interface will show the remaining charge percentage of the main battery.
- If the main battery is removed while the backup battery has charge, the device will switch to backup battery power. When the backup battery is depleted, the device will automatically shut down.
- In the default configuration (with battery removal alarm enabled), removing the main battery will trigger a battery disconnection alarm.

To ensure battery safety and service life, the device incorporates an intelligent battery protection management system that continuously monitors battery temperature and status. When excessive battery temperature is detected, protective measures will be automatically triggered. The system will:

1. Suspend the charging process and might temporarily disable high-power functions such as lighting and network connectivity to reduce load and heat generation.
2. All functions will automatically resume normal operation once the battery temperature and status return to safe levels.

- Fully charge the device before first use after prolonged storage.
- A low battery alarm will activate when battery level drops to ≤5%.
- The device will automatically power off when battery is depleted.
- If the device will remain unused for an extended period (one week or more), charge the battery to 60%, remove it from the device, and store it in a clean, dry, well-ventilated area at an ambient temperature of 20±5 ℃.
- We recommend you charge the battery at least every three months during storage.
- The battery is a consumable component and should be replaced after one year of use.

7 SIM Card and Battery Installation

The product supports 5 VDC/2 A power recharge. When the battery power is low, recharge it in time.

- When the Device has the main battery, the interface displays main battery percentage.
- If you remove the main battery and the small battery has power, it will supply energy; if the small battery is also depleted, the device will shut down.
- After installing the main battery, start the Device manually.
- In the default configuration (with battery removal alert enabled), removing the main battery will trigger the battery removal alert.

- Recharge the battery if the Device is not in use for a long time.
- The system triggers low battery alarm when the battery level is lower than 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 at least once every three months during storage.
- The battery is a consumable accessory. You are recommended to replace it after one year of use.

7.1 Installing the SIM Card

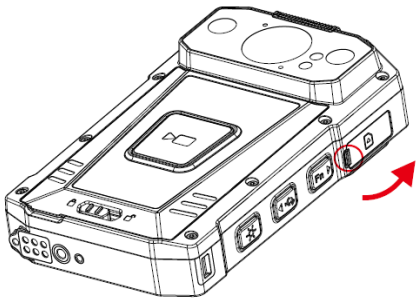
Background Information

- SIM card and the peripheral accessories do not support hot swapping. The card becomes activated after the Device restarts.
- Shut down the Device before installing the SIM card; otherwise the Device might be damaged.

Procedure

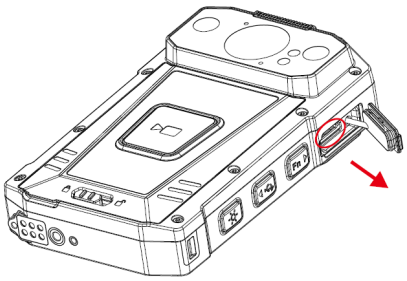
Step 1 Pull out the SIM card tray.

Figure 7-1 Pull out the SIM card tray



Step 2 Use tweezers or your fingernail to take out the SIM card slot.

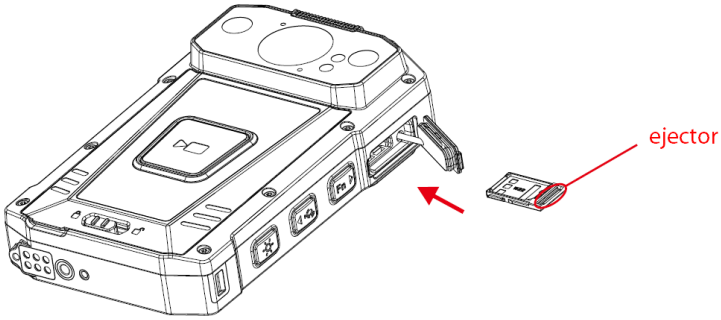
Figure 7-2 Take out the SIM card slot



Step 3 Place the SIM card onto the slot (it can be positioned on either side), ensuring the ejector is facing up, and then insert the tray back into the device.

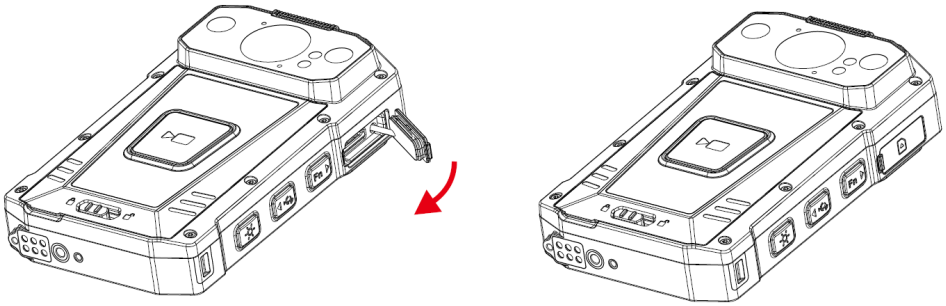
The SIM card tray supports inserting dual cards.

Figure 7-3 Install SIM card



Step 4 Rotate the SIM card tray to close it.

Figure 7-4 Close the SIM card tray

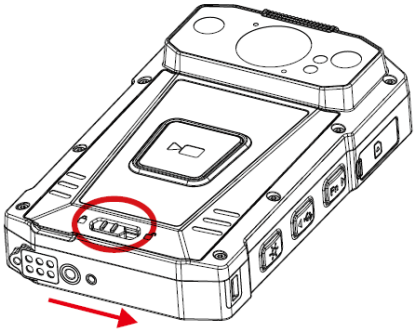


7.2 Installing the Battery

Procedure

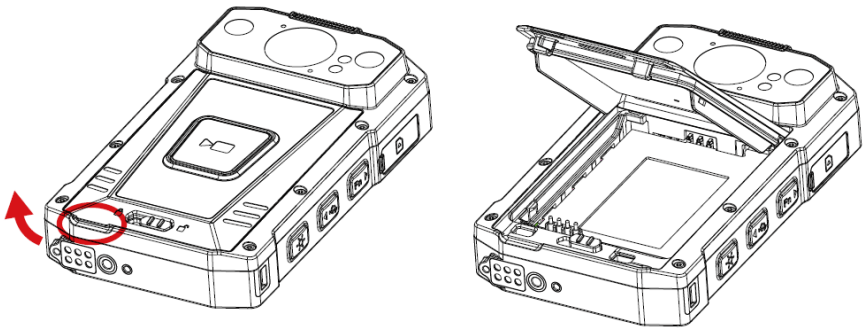
Step 1 Toggle the slider to the right.

Figure 7-5 Toggle the slider



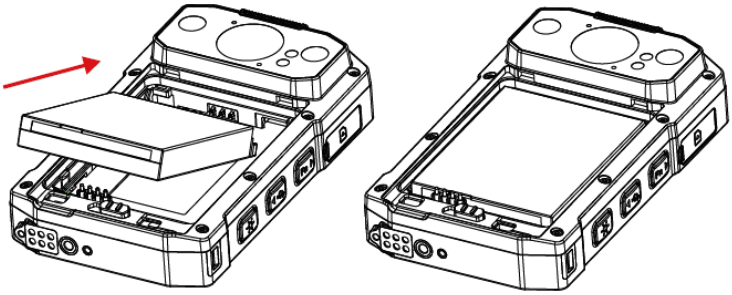
Step 2 Use your thumb to remove the battery cover.

Figure 7-6 Remove the battery cover



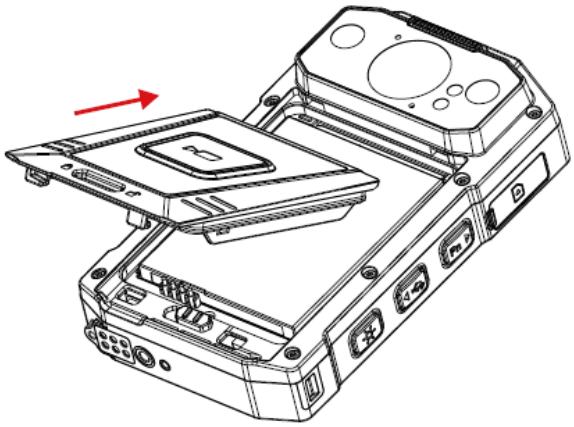
Step 3 Insert the battery at an angle into the battery compartment.

Figure 7-7 Install the battery



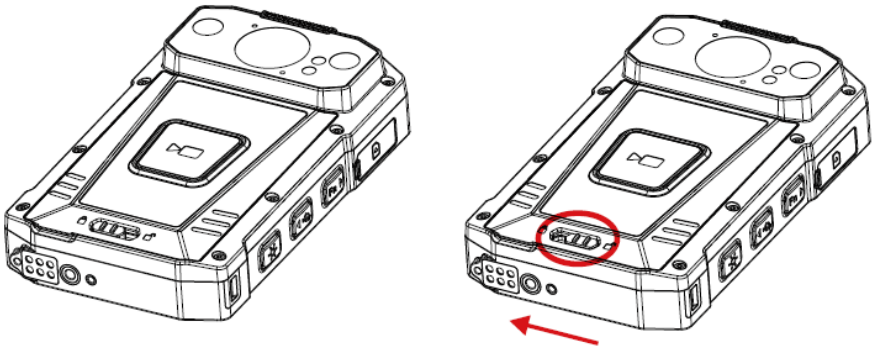
Step 4 Insert the battery cover at an angle into the device.

Figure 7-8 Install the battery cover



Step 5 Toggle the slider to the locked position.

Figure 7-9 Toggle the slider



8 FAQ

1. **How can I add, delete user or change password?**
   - The operations might vary with the version and model. For details, see the corresponding user manual.
   - Only the admin account has the permission to add user.
   - To change the password, go to > **admin** > **Change password**.
   - Only the admin account has the permission to view and change the information of other users. Other users can only view the information and change the password of their own account.
2. **How can I restore the Device to factory settings or clear the password?**

   Restoring default settings will clear all data stored on your device, including system, app data and settings and face and ANPR files. The Device still retains the serial number. You can select whether to clear video, audio and image data in the internal storage and micro SD card. Proceed with caution. Only the admin account can reset the Device.
3. **Where can I configure VPN?**

   Go to > **Network** > **Mobile Data** > **VPN**.
4. **Where can I configure APN?**

   Select > **Network** > **Mobile Data** > **Mobile Network** > **Advanced**, and then tap **Access Point Names**.

Appendix 1 Security Commitment and Recommendation

Dahua Vision Technology Co., Ltd. (hereinafter referred to as "Dahua") places great emphasis on cybersecurity and privacy protection. We continuously allocate special funds to enhance employees' awareness and capabilities in security, and ensure sufficient security protection for our products. Dahua has established a professional security team to provide comprehensive security empowerment and control throughout the entire product lifecycle, including design, development, testing, production, delivery, and maintenance. Dahua products adhere to the principle of minimum necessary data collection, service minimization, strict prohibition of backdoors, and the disabling of unnecessary and insecure services (such as Telnet). We continuously introduce innovative security technologies to bolster the security capabilities of our products. Additionally, we go above and beyond by providing global users with security alarm and 24/7 security emergency response services. This approach ensures that we are better safeguarding their security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report potential risks or vulnerabilities to the Dahua PSIRT. They can do so by visiting the cybersecurity section on the Dahua website.

The security of software platforms not only relies on the continuous attention and efforts from manufacturers throughout R & D, production, and delivery, but also requires active participation from users. Users should remain attentive to the environment and methods to ensure its secure operation. To this end, we suggest users to safely use the software platform, including but not limited to:

Account Management

1. **Use Strong 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. **Change Password Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.
3. **Assign Accounts and Permissions Reasonably**

   According to business and management needs, reasonably add new users, and reasonably allocate a minimum set of permissions for them.
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. **Set and Update Passwords Reset Information Timely**

   The platform supports password reset function. To reduce the risk of being attacked, please set up related information for password reset in time. 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.
6. **Enable Account Binding IP/MAC**

It is recommended to enable the account binding IP/MAC mechanism to further improve access security.

Network Configuration

1. **Enable Firewall Allowlist**

   We suggest you to enable allowlist 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 allowlist.
2. **Network Isolation**

   The network should be isolated by partitioning the video monitoring network and the office network on the switch and router to different VLANs. This prevents attackers from using the office network to launch Pivoting attacks on the video monitoring network.

Security Auditing

1. **Check Online Users**

   It is recommended to check online users irregularly to identify whether there are illegal users logging in.
2. **View the Platform Log**

   By viewing the log, you can get the IP information of the attempt to log in to the platform and the key operation information of the logged-in user.

Physical Protection

We suggest that you perform physical protection to the device that has installed the platform. For example, place the device 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.

Perimeter Security

We suggest that you deploy perimeter security products and take necessary measures such as authorized access, access control, and intrusion prevention to protect the software platform security.

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188