Mobile Portable Terminal

Quick Start Guide



V1.0.0

Foreword

General

This manual introduces the structure, installation and basic operations of the Mobile Portable Terminal (hereinafter referred to as "the Device").

Safety Instructions

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

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

Revision History

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

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related jurisdictions. For detailed information, refer to the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.

- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurring when using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

The section introduces the proper way of using the Device, and danger and property damage preventions. Before using the Device, read this manual carefully. Follow the instructions and keep this manual properly.

Operating Requirements

- Do not use high volume for a long time to avoid possible hearing damage.
- Only use the matching charging adapter.
- Do not dissemble the Device randomly.
- Transport, use and store the Device under the allowed humidity and temperature range. When the ambient temperature is too high or too low, it might result in device failure.
- Do not burn, strike or puncture the Device; otherwise it might result in fire, explosion, or inflammation.
- Use the power adapter and USB cable provided with the Device; otherwise you will be responsible for the possible people injury and device damage.

Safety Precautions for Lithium-ion Batteries

- The Device and battery must be used within the specified temperature and humidity range; otherwise the device and battery might be damaged.
- Charge with the provided power adapter or acquisition device. Mixed use might cause damage to the battery.
- If any abnormality is found in use, such as serious heat, bulge, deformation and strange smell, stop using the battery immediately.
- Do not store the battery with other metals to avoid metal objects touching the battery anode and cathode, thus resulting in short circuit.
- Do not dissemble the Device randomly, and do not decompose the battery in any way.
- Do not charge the battery continuously for more than 24 hours. When charging is complete or no charging is needed, disconnect the charger from the Device, and unplug the charger from the power socket.

Lithium Battery Maintenance Instructions

- 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℃.
- Charge the battery once every four months during storage.
- The battery is a consumable accessory. It is recommended to replace it after one year of use.



- You can scan the QR code in the packing box to get the user’s manual.

- You can upgrade the software of the Device. There might be security risk if you select version downgrading, which might introduce the original security vulnerabilities and other defects. Please operate cautiously.
- During the upgrade process, make sure that the battery level of the Device is not less than 20% to avoid abnormal upgrade caused by powering off.

Table of Contents

Foreword ..... **I**
Important Safeguards and Warnings ..... **III**
1 Product Overview **1**
1.1 Introduction 1
1.2 Packing List 1
1.3 Structure 1
2 Installation **5**
2.1 Installing the Device 5
2.2 Removing the Battery 6
3 Basic Operations **8**
Appendix 1 Cybersecurity Recommendations **9**

1 Product Overview

1.1 Introduction

The Device integrates high-performance mobile phone chip solution, ergonomic design, industry application, and AI video technology. It is ideal for public security, energy, corporation, transportation, justice, electricity, insurance and other industries. With functions such as video communication, teleconference, audio and video acquisition, group talk, and voice call, the Device is suitable for the following application scenarios: Law enforcement and evidence obtaining, security and patrol, process control, and remote supervision. Therefore, it can meet the customers' needs for mobile business application.

1.2 Packing List

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

Table 1-1 Packing list

Name	Quantity
Main device	1
Power adapter	1
4600mAh battery	1
Quick Start Guide	1
USB cable	1

1.3 Structure

For the structure, see Figure 1-1. For the detailed description, see Table 1-2.

Figure 1-1 Structure (1)

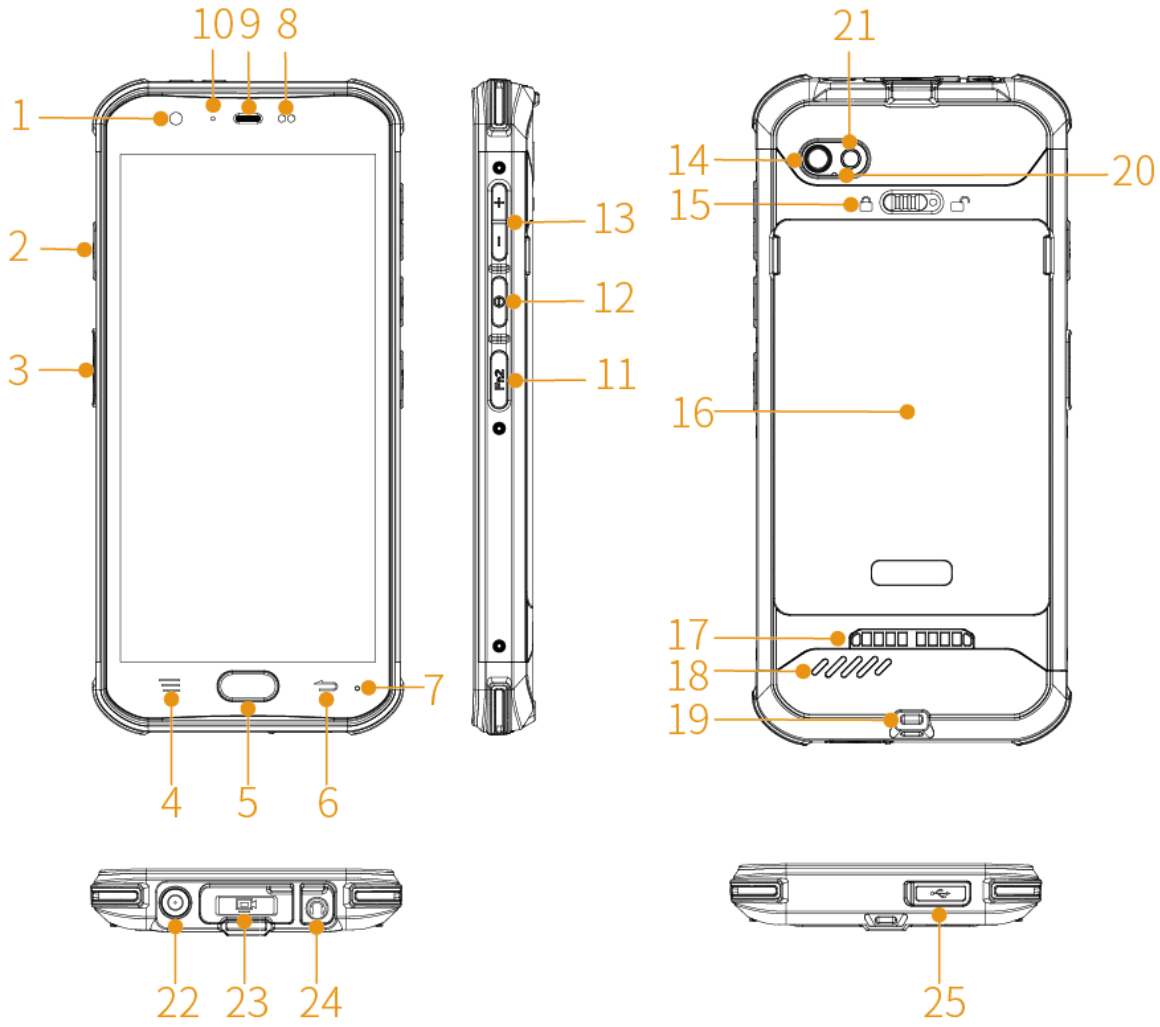


Table 1-2 Structure description (1)

No.	Description	No.	Description
1	Front-facing camera.	2	Fn1 button and customizable. Select **Settings > Device > Customized Button** to set it as recording or capture shortcut button.
3	PTT (Push to Talk) button. Press and hold it to start talk if the Device is in a POC group.	4	Menu button. After unlocking the Device, tap the button on any interface to see the tasks running in the background.
5	Fingerprint sensor. ● After adding the fingerprint, press the button to unlock the Device with fingerprint. ● When the Device is powered on, it can serve as the Home button.	6	Back button. Tap it to go back to the previous interface.
7	Main microphone.	8	Photosensitive proximity sensor.

No.	Description	No.	Description
9	Sound pickup	10	Indicator light. ● Alarm: Red light flashes quickly. ● Low battery: Red light flashes slowly. ● Charging: Red when the battery level is lower than 90%; green when the battery level is 90% or higher. ● Acquiring stream: Green light flashes slowly. ● Video recording: Blue light flashes quickly. ● Audio recording: Blue light flashes slowly.
11	Fn2 button and customizable. Select **Settings > Device > Customized Button** to set it as recording or capture shortcut button.	12	Power button. ● Press and hold the button to power on or off the Device, restart the Device, or take screenshots. ● Short press the button to hibernate or wake up the Device.
13	Volume button. Adjust the volume, including volume + and volume –.	14	Rear-facing camera.
15	Battery cover lock. Slide to the left or right to lock or unlock the battery cover.	16	Battery cover.
17	Pogpin port used to connect to the base and back clip.	18	Speaker
19	Lanyard hole.	20	Back microphone.
21	Flash light	22	SOS button. Press the button to ask for help in an emergency.  Use this function with the corresponding platform software.
23	Port used to connect the external camera.	24	Earphone jack.
25	USB charging port.	—	—

See Figure 1-2 for the internal structure after opening the battery cover.

Figure 1-2 Structure (2)

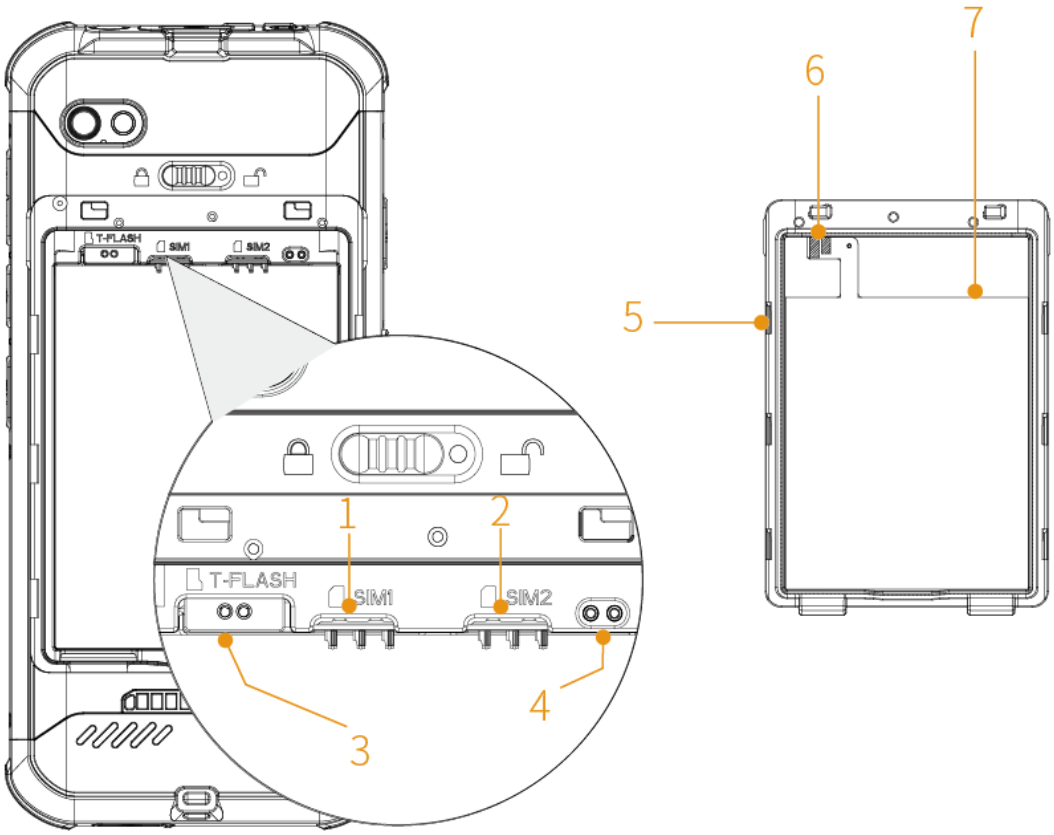


Table 1-3 Structure description (2)

No.	Description
1	SIM card slot 1
2	SIM card slot 2
3	Micro SD card slot
4	NFC contact
5	Battery cover buckle
6	NFC antenna contact
7	NFC antenna

2 Installation

2.1 Installing the Device

After unpacking the box, first install the SIM card, Micro SD card (optional) and battery. For details, see Figure 2-1.

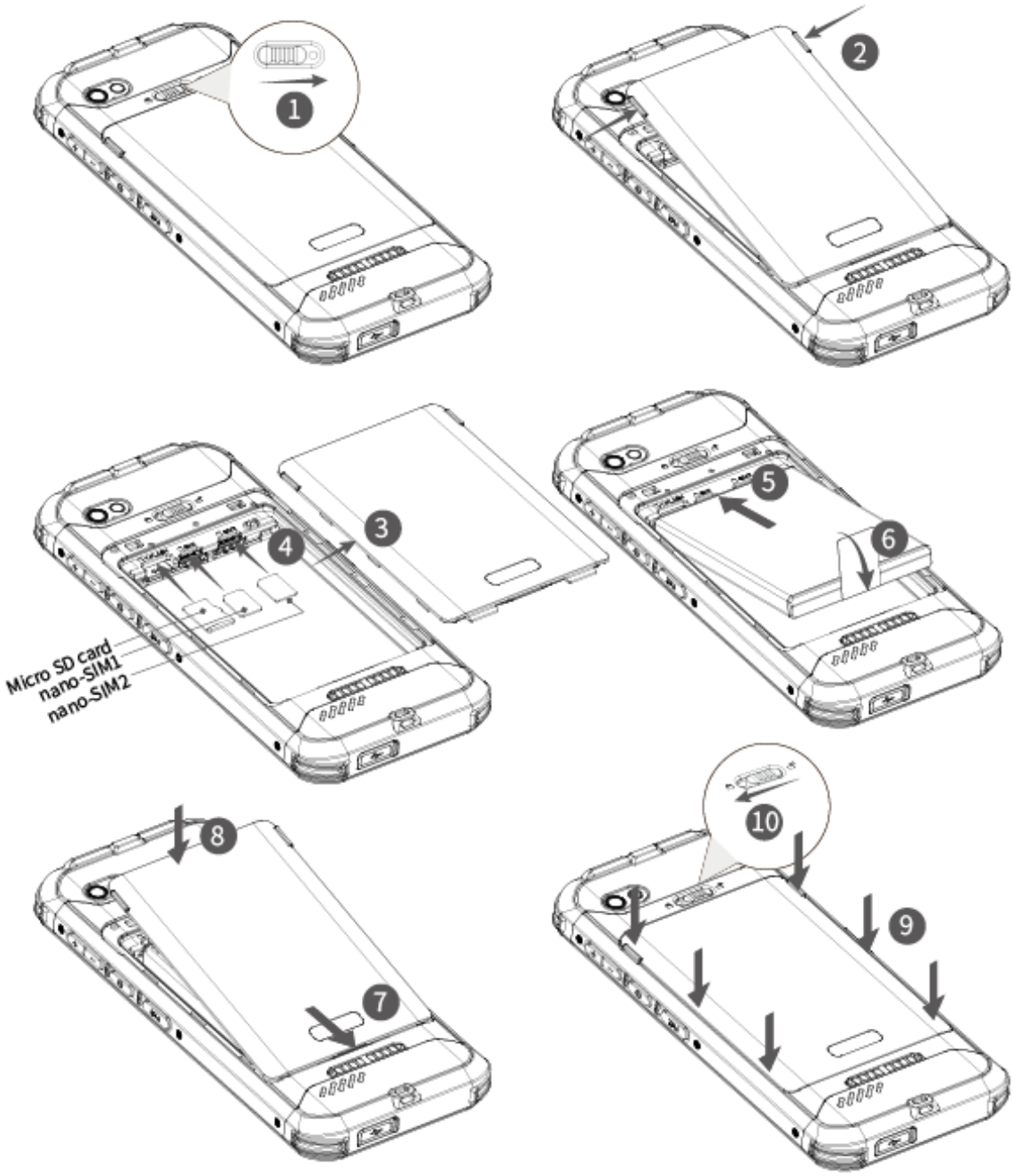
Follow the instructions below.

- Before opening the battery cover, slide the battery cover lock to unlock the battery cover; before closing the battery cover, insert the battery cover from the bottom (do not press the battery handle), press 6 buckles on both sides to make the battery cover flat, and then slide the battery cover lock to the left to lock the battery cover.
- When installing the SIM card and Micro SD card, insert them into the card slots with the metal side facing downwards. After inserting the card, you will hear a "click" sound.
- Use the standard nano-SIM card (small card); inserting a non-standard card may cause the Device to fail to recognize it. If the SIM card you use does not match the Device, contact the carrier.
- To ensure good reading and writing speed, it is recommended to use a Micro SD card that conforms to UHS-I U1 specification.
- Both SIM card 1 and SIM card 2 support 2G/3G/4G, but you need to confirm whether the local band is supported by the Device. For details, see Table 2-1.

Table 2-1 Supported band

Network	Band
2G	GSM B2/B3/B5/B8 CDMA BC0
3G	WCDMA B1/B2/B4/B5/B8 TD-SCDMA B34/B39
4G	FDD-LTE B1/B2/B3/B4/B5/B7/B8/B12/B17/B19/B20/B28 TDD-LTE B34/B38/B39/B40/B41

Figure 2-1 Installing the SIM card, Micro SD card and battery

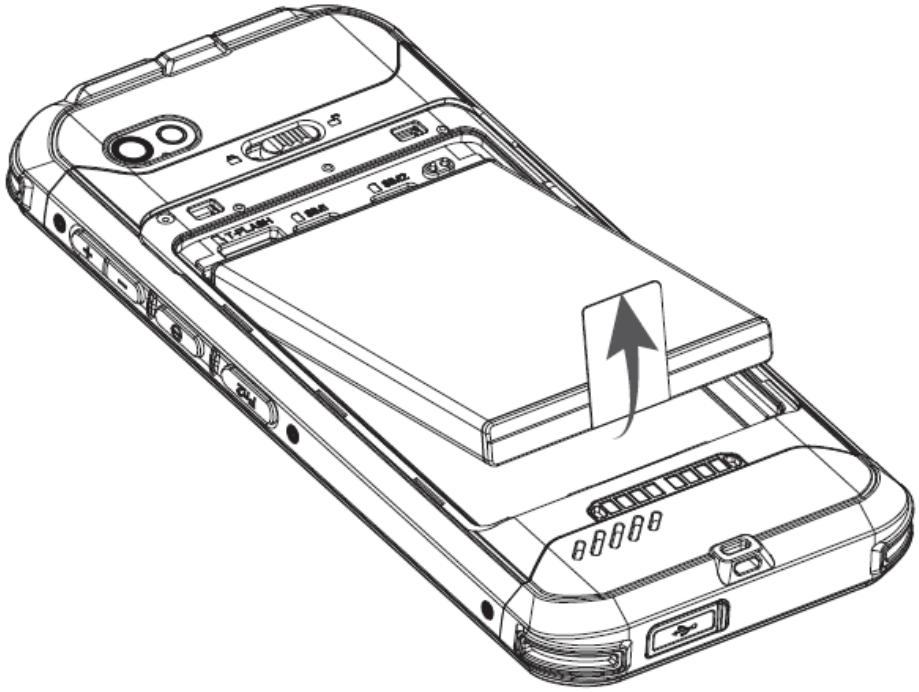


2.2 Removing the Battery

Before removing the battery, power off the Device, slide the battery cover lock to unlock the cover, open the battery cover, and then take out of the battery. See Figure 2-2.

Do not change the battery when the Device is in powered-on status; otherwise the data (videos, audios and snapshots) that needs to be written into ROM might be lost, and there might be other exceptions.

Figure 2-2 Removing the battery



3 Basic Operations

Press the Power button on the right panel to power on or off, restart or hibernate the Device.

- When the Device has been powered off, press and hold the Power button to start it.
- When the Device has been powered on, press and hold the Power button, tap ; **Shutting down...** is displayed, and the Device will be powered off.
- When the Device has been powered on, press and hold the Power button, tap ; **Restarting...** is displayed, and the Device will be restarted.
- When the Device has been powered on, short press the Power button, and the Device will be hibernated; short press the Power button again to wake up the Device.

When the Device has been powered on, press and hold the Power button, tap , and you can take a screenshot of the current screen. You can also press the Power button and Volume – at the same time to take screenshots.

Appendix 1 Cybersecurity Recommendations

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

Mandatory actions to be taken for basic equipment network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

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

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

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

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

1. **Physical Protection**

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

2. **Change Passwords Regularly**

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

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

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

4. **Enable Account Lock**

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

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

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

6. **Enable HTTPS**

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

7. **Enable Whitelist**

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

8. **MAC Address Binding**

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

9. **Assign Accounts and Privileges Reasonably**

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

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

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

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

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

11. **Audio and Video Encrypted Transmission**

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

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

12. **Secure Auditing**

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

13. **Network Log**

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

14. **Construct a Safe Network Environment**

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

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

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

- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- It is recommended that you enable your device's firewall or blacklist and whitelist feature to reduce the risk that your device might be attacked.