Attendance Standalone

Quick Start Guide



V1.0.0

Foreword

General

This manual introduces the installation and basic operations of the Attendance Standalone (hereinafter referred to as the "Device"). Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

The following signal words 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, reductions in performance, or unpredictable results.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	August 2024

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, 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.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.

- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. 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 company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

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 Requirement



Transport, use and store the Device under allowed humidity and temperature conditions.

Storage Requirement



Store the Device under allowed humidity and temperature conditions.

Installation Requirements



- Do not connect the power adapter to the Device while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the Device.
- Do not connect the Device to two or more kinds of power supplies, to avoid damage to the Device.
- Improper use of the battery might result in a fire or explosion.
- Please follow the electrical requirements to power the device.
  - Following are the requirements for selecting a power adapter.
    - The power supply must conform to the requirements of IEC 60950-1 and IEC 62368-1 standards.
    - The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
    - When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.
  - We recommend using the power adapter provided with the device.
  - When selecting the power adapter, the power supply requirements (such as rated voltage) are subject to the device label.



- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the Device in a place exposed to sunlight or near heat sources.
- Keep the Device away from dampness, dust, and soot.
- Install the Device on a stable surface to prevent it from falling.
- Install the Device in a well-ventilated place, and do not block its ventilation.

- Use an adapter or cabinet power supply provided by the manufacturer.
- Use the power cords that are recommended for the region and conform to the rated power specifications.
- The Device is a class I electrical appliance. Make sure that the power supply of the Device is connected to a power socket with protective earthing.
- The device must be installed at a height of 2 meters or below.
- If the product has a metal case, we recommend you install it in an environment with a temperature lower than 40℃ (104°F) to avoid overheating and affecting your experience.

Operation Requirements



- Check whether the power supply is correct before use.
- Ground the device to protective ground before you power it on.
- Do not unplug the power cord on the side of the Device while the adapter is powered on.
- Operate the Device within the rated range of power input and output.
- Use the Device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the Device, and make sure that there is no object filled with liquid on the Device to prevent liquid from flowing into it.
- Do not disassemble the Device without professional instruction.
- This product is professional equipment.
- The Device is not suitable for use in locations where children are likely to be present.
- If the product supports PoE power supplies and can supply power to electromagnetic locks, which are in the normally open state while they are powered off, the connected door lock will automatically open if there are issues with the network cable or it becomes disconnected. We recommend you regularly check the wiring to minimize the risk of malfunctions. In locations with high safety requirements, we recommend you use an electromagnetic lock that is in the normally closed state when it is powered off, or install an uninterruptible power supply (UPS) to prevent potential accidents.

Table of Contents

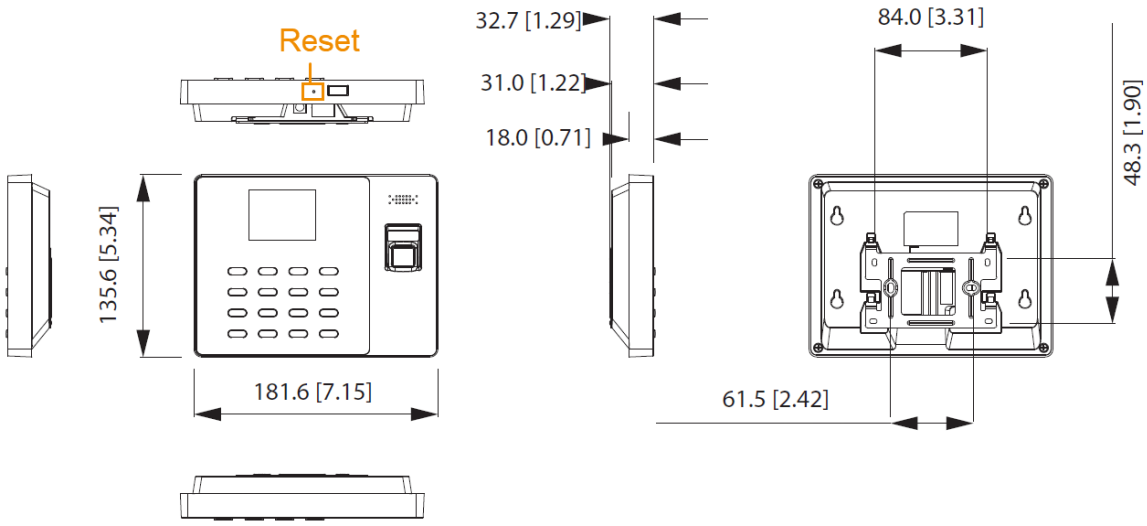
Foreword I
Important Safeguards and Warnings III
1 Product Overview 1
2 Dimensions 2
3 Wiring 3
4 Installation 4
5 Local Operations 7
5.1 Keypad Introduction 7
5.2 Powering On 8
5.3 Creating Administrator Account 9
5.4 Logging In 9
6 SmartPSS Lite Operations 10
6.1 Installation 10
6.2 Initialization 10
6.3 Login 13
Appendix 1 Important Points of Fingerprint Registration Instructions 15
Appendix 2 FAQ 17
Appendix 3 Security Recommendation 18

1 Product Overview

The Device can be used to track attendance of people and control the door status. People can clock in/out through fingerprint, password, and card.

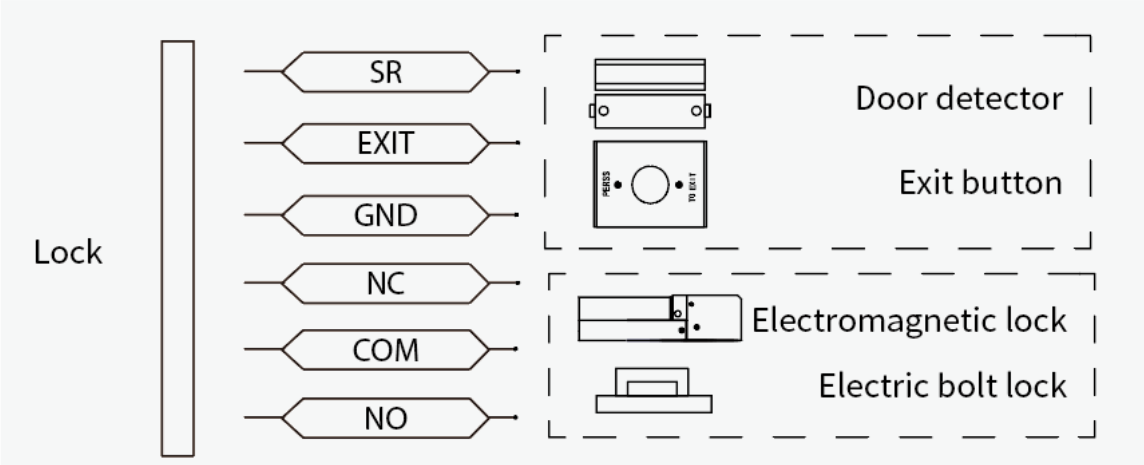
2 Dimensions

Figure 2-1 Dimensions (mm [inch])



3 Wiring

Figure 3-1 Wiring



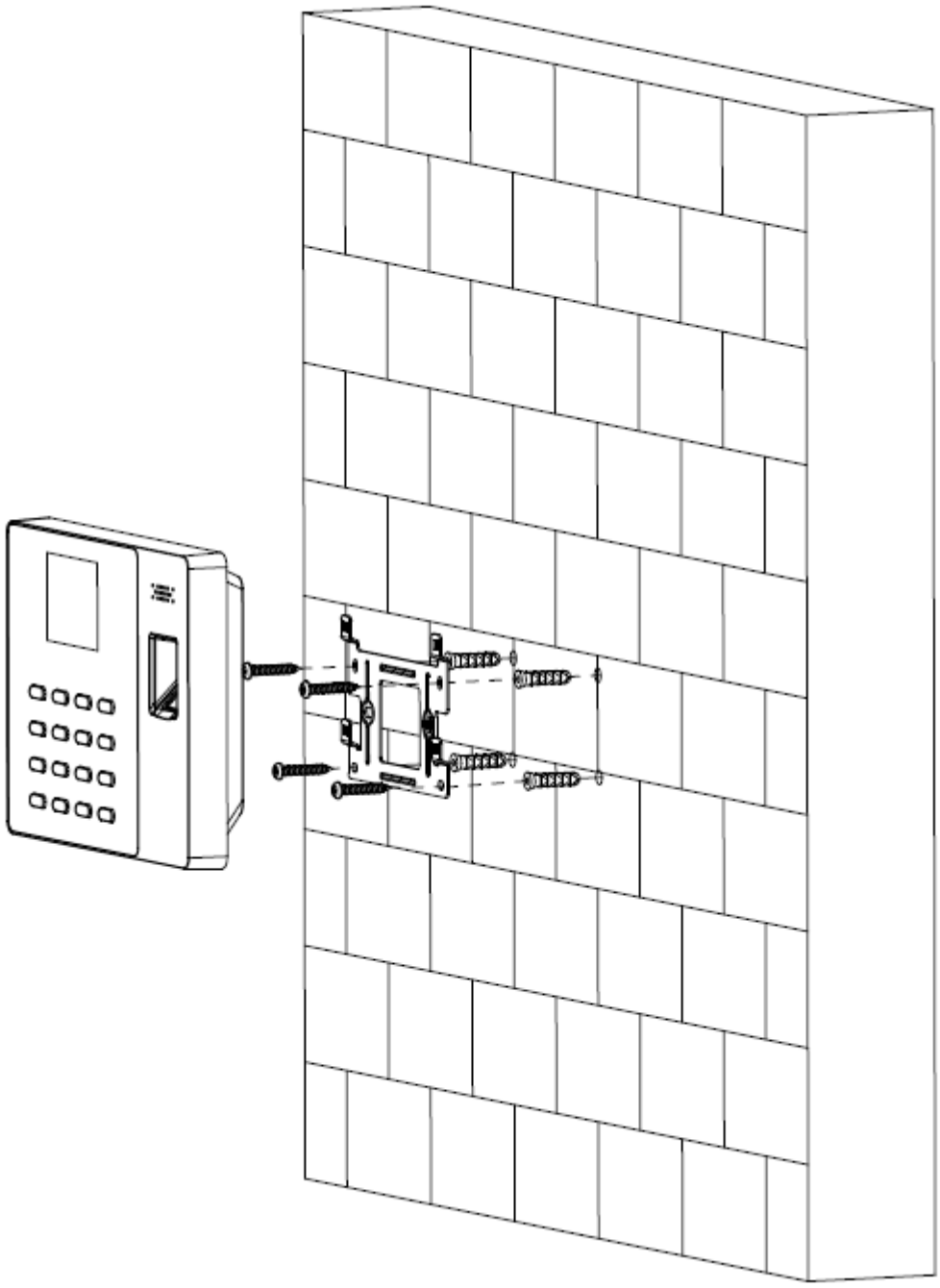
4 Installation

Wall Mount

1. According to the holes' position of the bracket, drill 4 holes and 1 cable outlet in the wall. Hammer in expansion bolts into the holes.

   The cable outlet is not required for surface-mounted wiring.
2. Use the 4 screws to attach the bracket to the wall.
3. Wire the Device. For details, see "3 Wiring".
4. Attach the Device on the bracket.

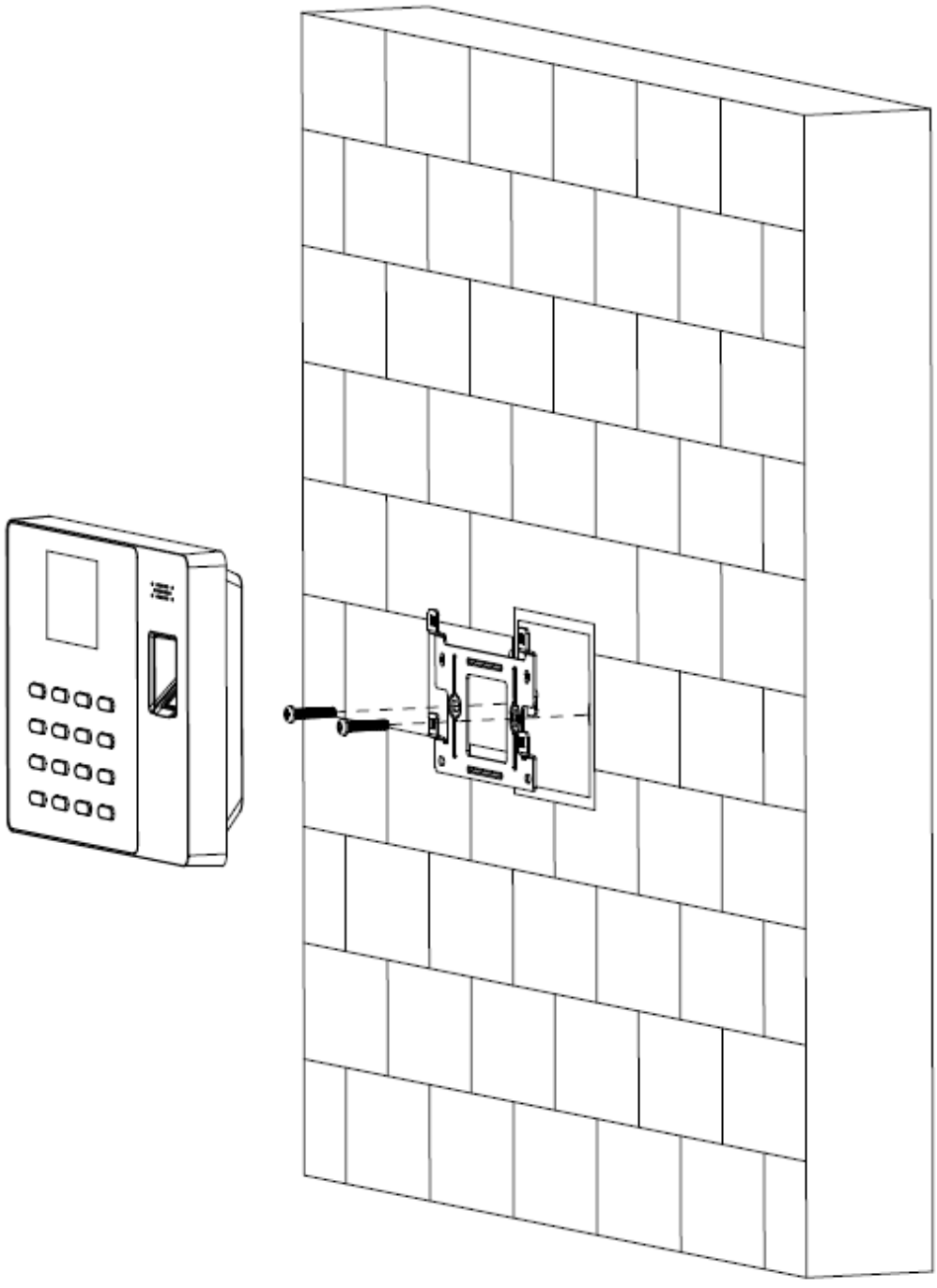
Figure 4-1 Wall mount



Box Mount

1. Put an 86 box in the wall at an appropriate height.
2. Fasten the bracket to the 86 box with 2 screws.
3. Wire the Device. For details, see "3 Wiring".
4. Attach the Device to the bracket.

Figure 4-2 86 box mount



5 Local Operations

5.1 Keypad Introduction

Figure 5-1 Appearance



The functions of F1, F2, F3 and F4 may differ according to the actual attendance mode. This section introduces the functions of the buttons when the mode is default **Auto/Manual Mode**. For details on other functions on other modes, see the user's manual.

Table 5-1 Button description

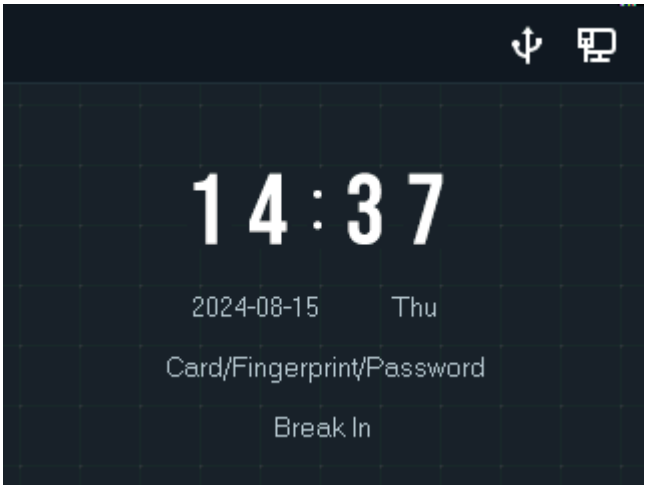
Button	Description
0–9	• Press to input numbers and letters in the input box. • Press to verify the identity through the user ID and password on the standby screen. • Press 0 for 3 seconds, and use the administrator password to open the door. The attendance function in this situation is invalid.
ESC/F1	• Exit or go to the previous screen. • Press it on the standby screen to configure the check in mode.

Button	Description
∧/F2	• Press it on the standby screen to configure the break out mode. • Press to go up the options.
∨/F3	• Press it on the standby screen to configure the break in mode. • Press it to go down through the options.
OK/F4	• Confirm your settings. • Press it on the standby screen to configure the check out mode.
#	• Delete. • Shortcut for reviewing records. Press the button, use your card or fingerprint to verify the identity, and the attendance records of the verified user are displayed.
	• If the device is in the standby mode and the screen is light up, press button for over 3 seconds to turn the Device off. • Press the button for 10 seconds in any screen to turn the Device off. • On the standby screen, press it to enter the main menu by fingerprints, passwords or cards. Only administrators can enter the main menu. • Press it to change the input types (numbers, letters and symbols).

5.2 Powering On

After the Device is powered on, the standby screen is displayed.

Figure 5-2 Standby screen



-  means the network is connected.
-  means the USB is inserted.
-  means the power is lower than 10%.

5.3 Creating Administrator Account

When the Device is started for the first time, anyone can enter the main menu and configure the Device. For the account security, we recommend you create the administrator account first, and then only administrators can enter the main menu.

Procedure

Step 1 Press  to enter the main menu screen.

Step 2 Select **Users** > **Create User**

Step 3 Enter the user information.

Step 4 Press OK to select **Admin** as **User Permission**.

Step 5 Configure other parameters, press Esc, and then press OK to save the configurations.

5.4 Logging In

After the admin account is created, you can enter the main menu after you have verified your identifications through fingerprint, password or card.

On the standby screen, press , and then enter the main menu after your identity has been verified.

- Swipe the card on the card reader area.
- Place your finger on the fingerprint sensor.
- Enter the user ID and password.

  The user type must be **admin**.
- Enter the administrator's ID and password.

6 SmartPSS Lite Operations

6.1 Installation

Contact technical support or go to the official website to get the SmartPSS Lite. If you get the software package of the SmartPSS Lite, install and run the software according to page instructions.

6.2 Initialization

Initialize SmartPSS Lite when you log in for the first time, including setting a password for login and security questions for resetting password.

Procedure

Step 1 Double-click SmartPSSLite.exe.

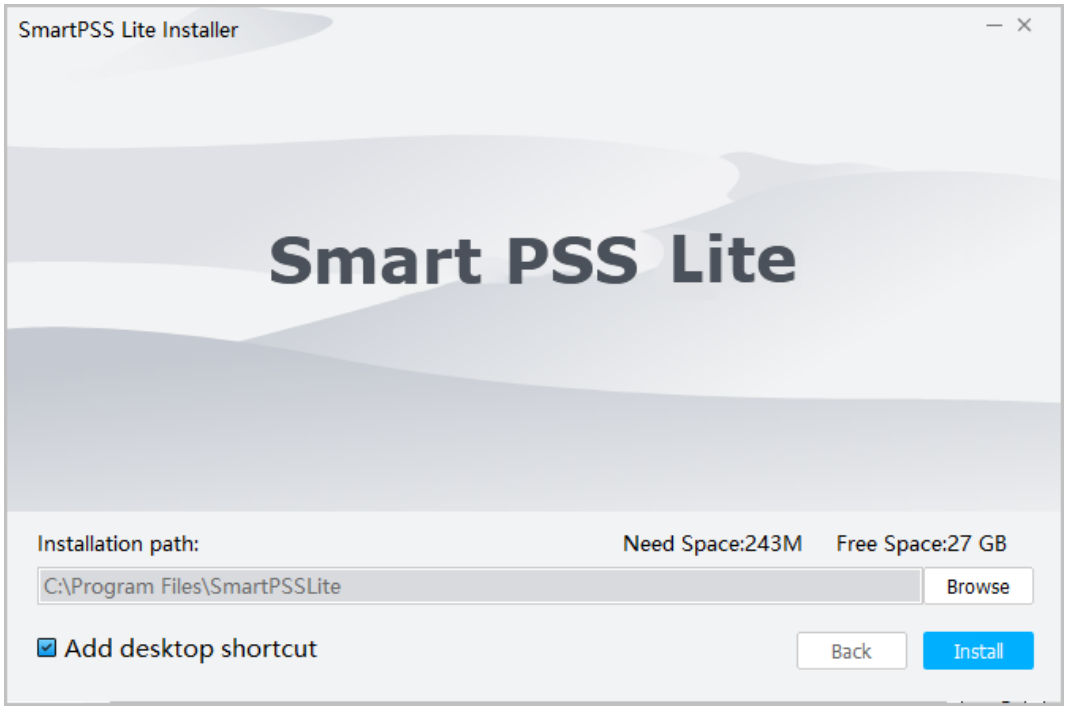
Step 2 Select the language from the drop-down list, select **I have read and agree the software agreement** , and then click **Next**.

Figure 6-1 Select language



Step 3 Click **Browse** to select installation path, and then click **Install**.

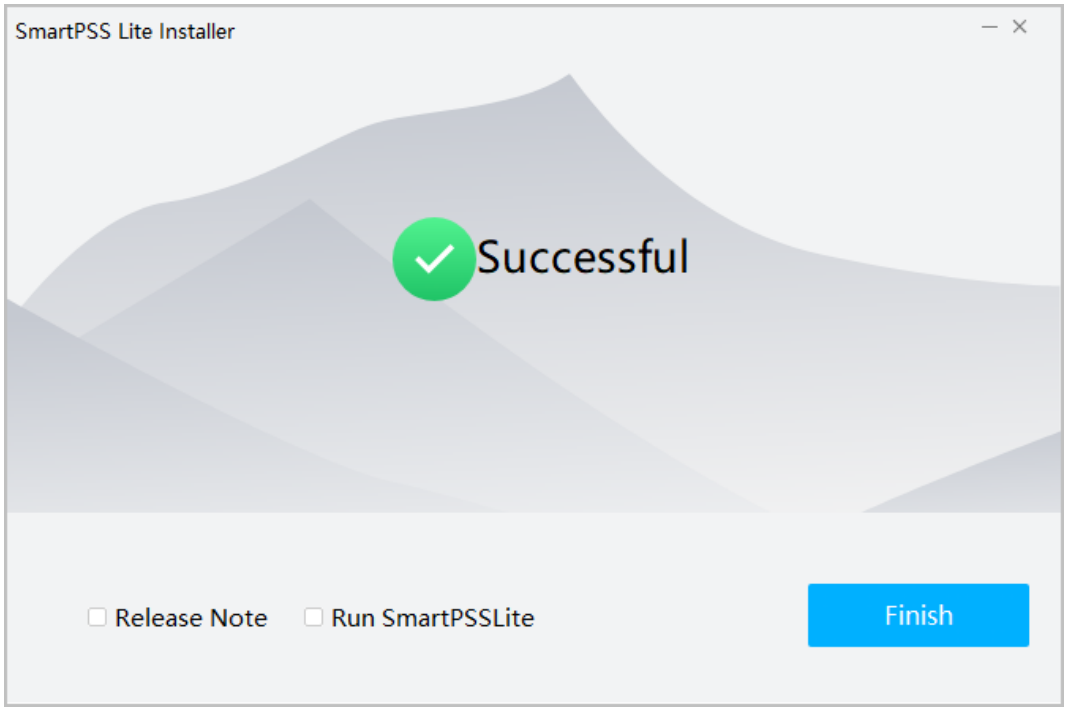
Figure 6-2 Select installation path



Step 4 Click **Finish** to complete the installation.

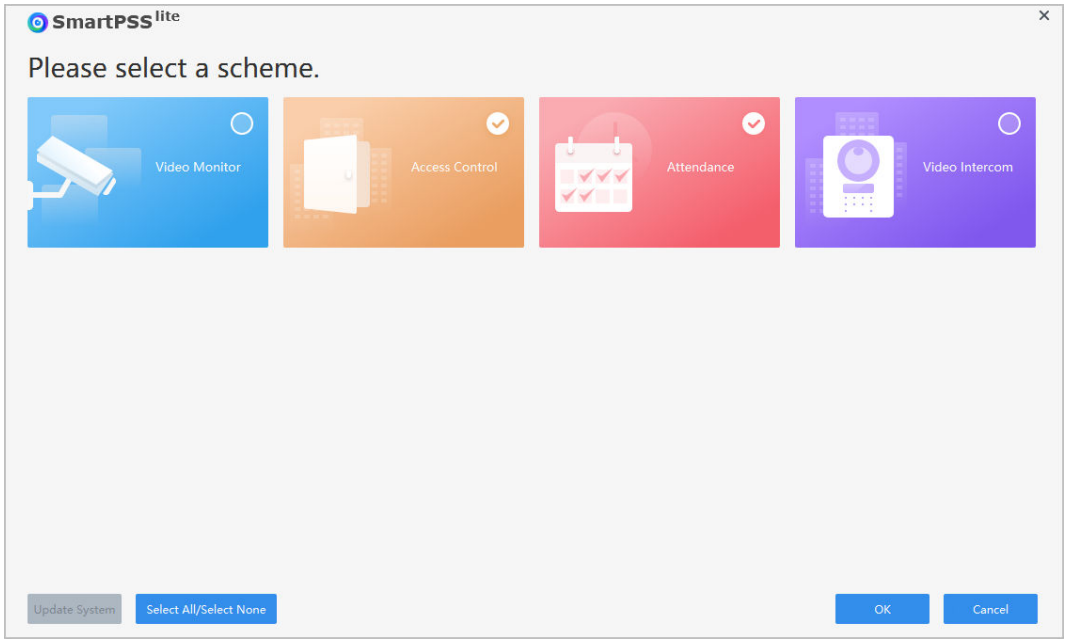
Select **Run SmartPSSLite** to start SmartPSS Lite.

Figure 6-3 Install complete



Step 5 Select the application scenes you want to add, and then click **OK**.

Figure 6-4 Select application scenes



Step 6 Click **Agree and Continue** to agree **Software License Agreement** and **Product Privacy Policy**.

Step 7 Set password on the **Initialization** page, and then click **Next**.

Figure 6-5 Set password

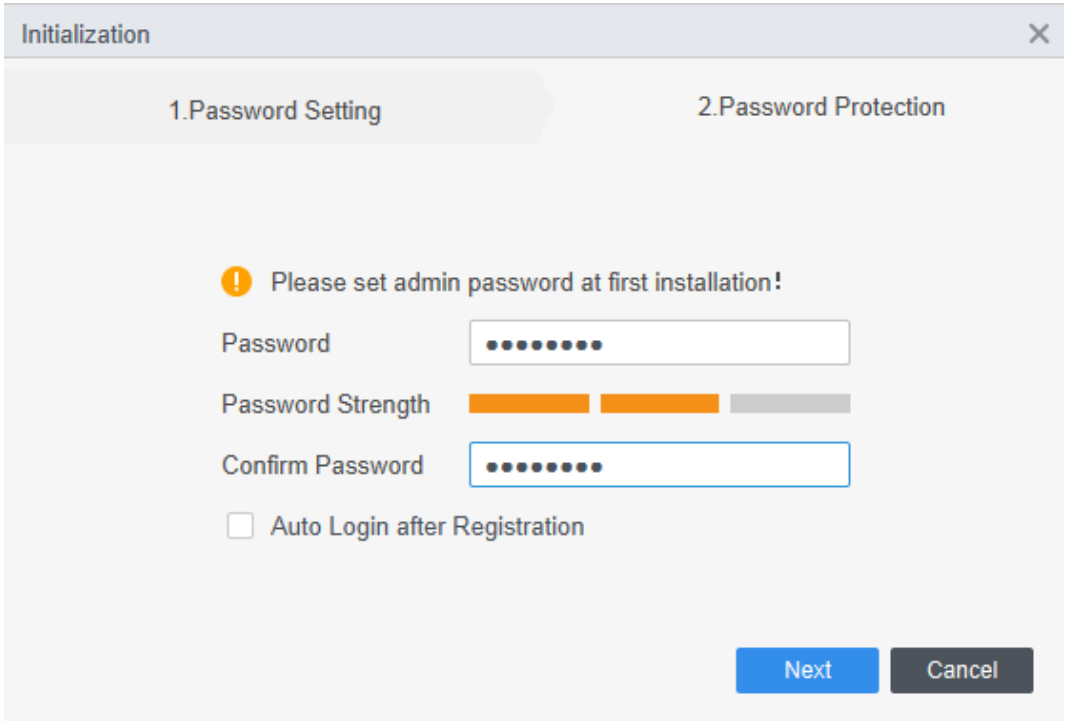
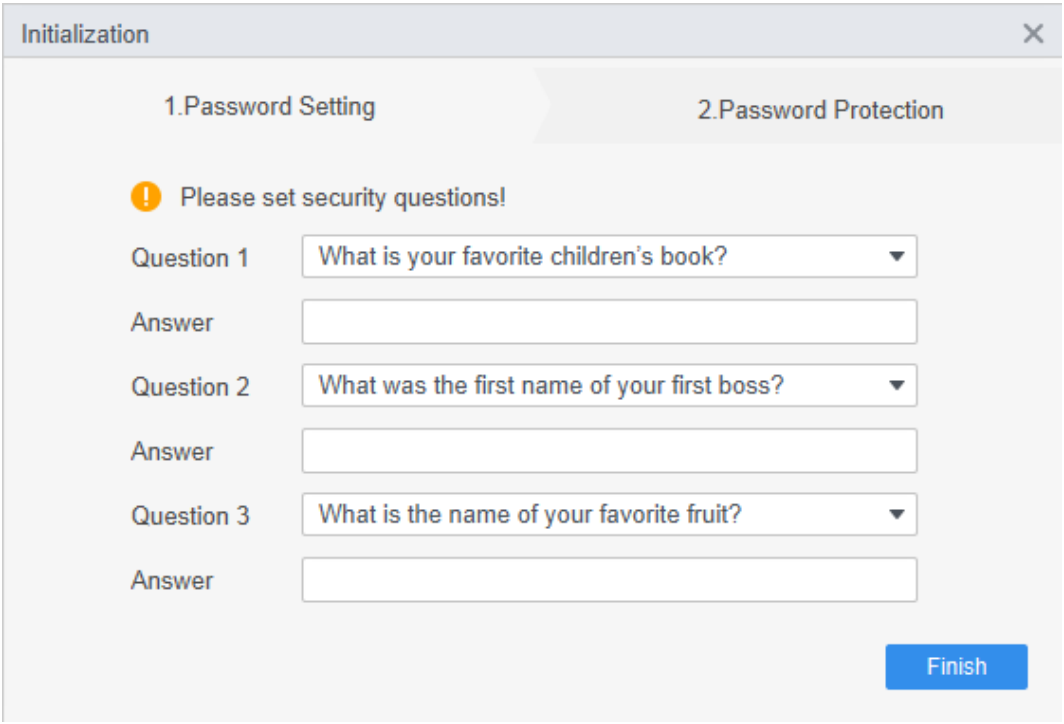


Table 6-1 Initialization parameters

Parameter	Description
Password	The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among uppercase, lowercase, number, and special character (excluding ' " ; : &).
Password Strength	Displays the effectiveness of a password against guessing or brute-force attacks. Green means the password is strong enough, and red means less strong. Set a password of high security level according to the password strength prompt.
Confirm Password	Enter the password again to confirm the password.
Auto Login after Registration	Enable **Auto Login after Registration** so that the SmartPSS Lite will log in automatically after initialization; otherwise the login page is displayed.

Step 8 Set security questions, and then click **Finish**.

Figure 6-6 Set security questions



6.3 Login

Procedure

Step 1 Double-click SmartPSSLite.exe.

Step 2 Enter username and password, and then click **Login**.

If multiple networks are available on your computer, you can select one from them.

Figure 6-7 Login

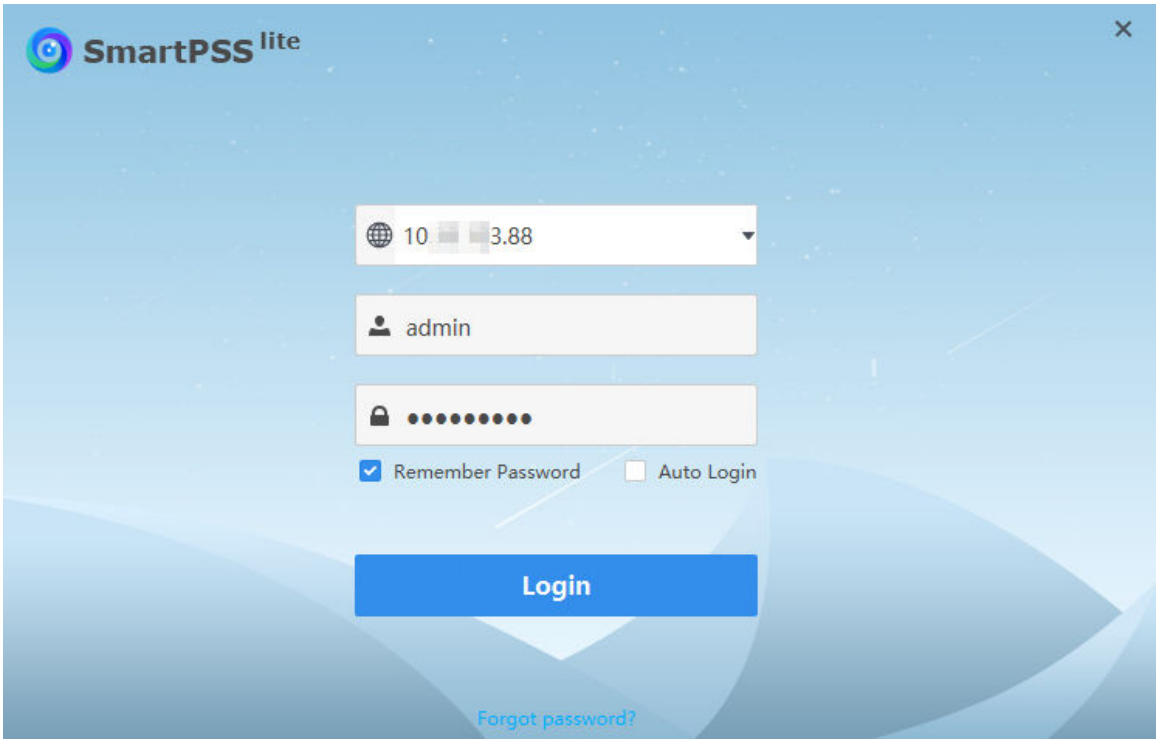


Table 6-2 Parameters of login

Parameter	Description
Remember Password	Enable **Remember Password** so that you do not need to enter the password again when logging in next time.
Auto Login	Enable **Auto Login** so that the SmartPSS Lite will log in automatically the next time when you use the same user account.
Forgot password?	Click **Forgot password?** to reset password through security questions when you forget the password.

Appendix 1 Important Points of Fingerprint Registration Instructions

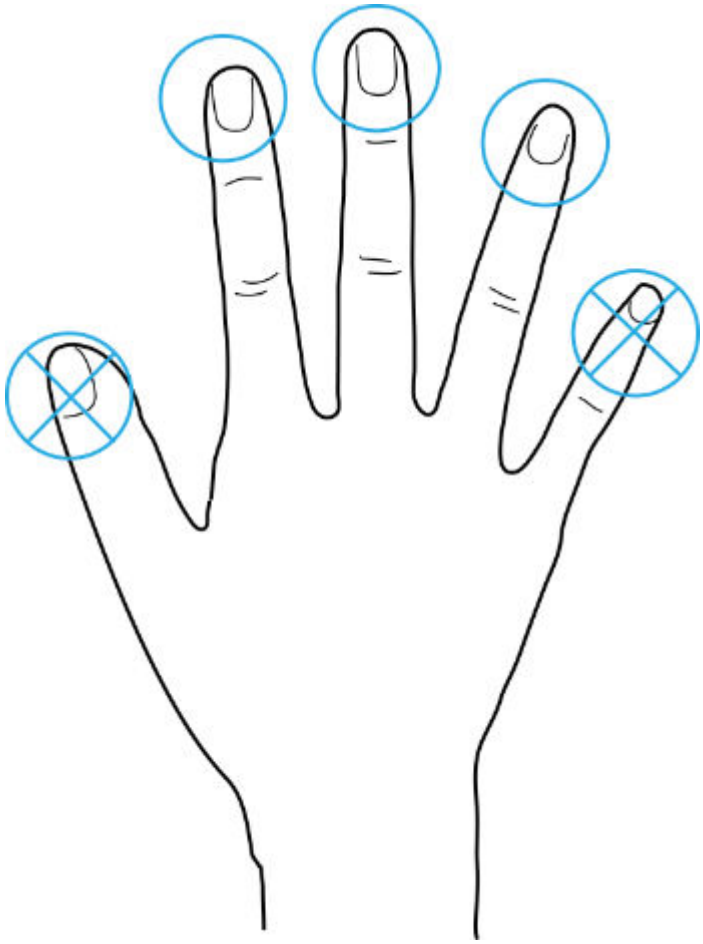
When you register the fingerprint, pay attention to the following points:

- Make sure that your fingers and the scanner surface are clean and dry.
- Press your finger on the center of the fingerprint scanner.
- Do not put the fingerprint sensor in a place with intense light, high temperature, and high humidity.
- If your fingerprints are unclear, use other unlocking methods.

Fingers Recommended

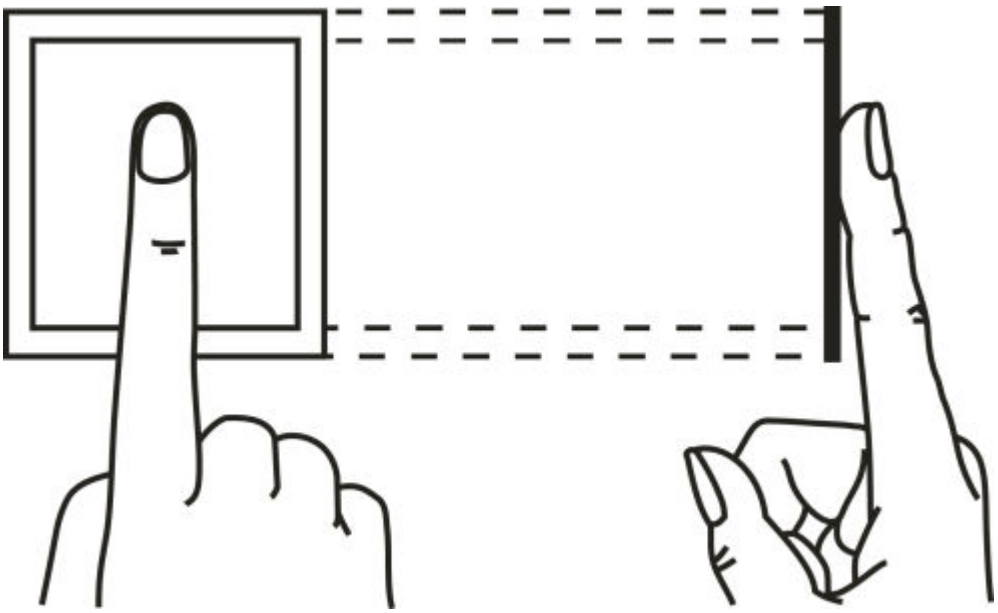
Forefingers, middle fingers, and ring fingers are recommended. Thumbs and little fingers cannot be put at the recording center easily.

Appendix Figure 1-1 Recommended fingers

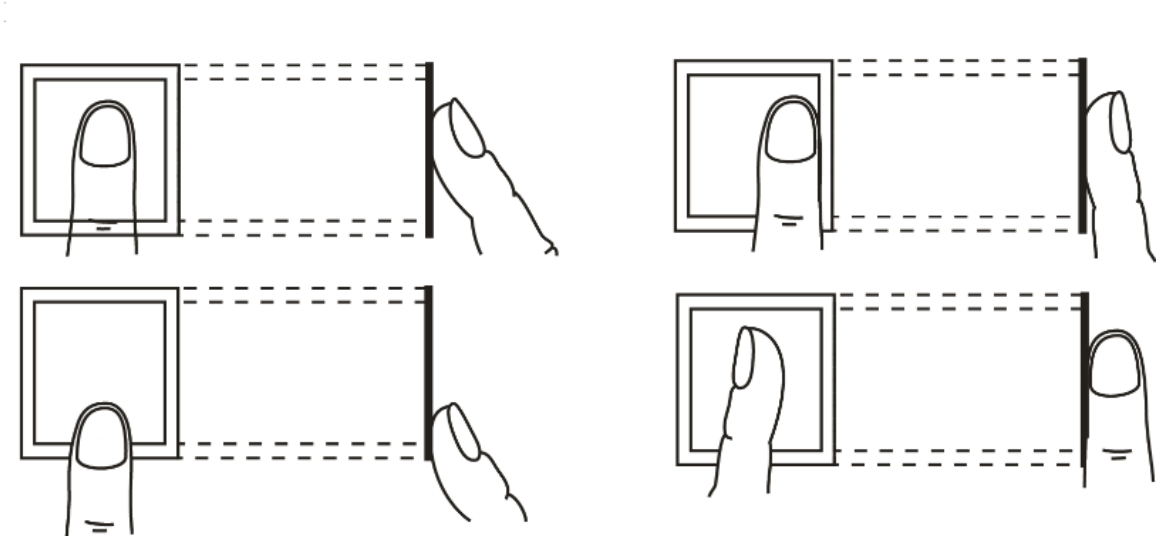


How to Press Your Fingerprint on the Scanner

Appendix Figure 1-2 Correct placement



Appendix Figure 1-3 Wrong placement



Appendix 2 FAQ

- Q: The Device prompts me to do it again after I have placed my finger on the sensor.

  A: Check if your fingerprints have been registered.
- Q: The bell does not ring.

  A: Check if bell ring is set successfully and the broadcast volume switch is on.
- Q: I cannot update the Device through the USB.

  A: Check if the Device is successfully recognized by the Device, and check the update file name.
- Q: Failed to export by USB flash drive.

  A: Use USB in FAT32 format.
- Q: I forget administrator password.

  A: Contact the manufacturer.
- Q: How to search for user attendance record?

  A: On the standby screen, tap **#**, and then place your finger on the fingerprint sensor, or enter the user ID and password, or swipe the card.

Appendix 3 Security Recommendation

Account Management

1. **Use complex 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: 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 repeating characters, such as 111, aaa, etc.

2. **Change passwords periodically**

   It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

3. **Allocate accounts and permissions appropriately**

   Appropriately add users based on service and management requirements and assign minimum permission sets to users.

4. **Enable account lockout function**

   The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

5. **Set and update password reset information in a timely manner**

   The device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. **Enable HTTPS**

   It is recommended that you enable HTTPS to access web services through secure channels.

2. **Encrypted transmission of audio and video**

   If your audio and video data contents are very important or sensitive, it is recommended to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.

3. **Turn off non-essential services and use safe mode**

   If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

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

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

4. **Change HTTP and other default service ports**

   It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allow list**

   It is recommended that you turn on the allow list function, and only allow IP in the allow list to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allow list.
2. **MAC address binding**

   It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.
3. **Build a secure network environment**

   In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

   - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
   - According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
   - Stablish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

   It is recommended to check online users regularly to identify illegal users.
2. **Check device log**

   By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.
3. **Configure network log**

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

Software Security

1. **Update firmware in time**

   According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.
2. **Update client software in time**

   It is recommended to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control

and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).