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
	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
	Provides methods to help you solve a problem or save time.
	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First Release.	December 2022

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

 WARNING

- 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.



- 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 power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the Device label.
- 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.

Operation Requirements



- Check whether the power supply is correct before use.
- 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.
- This equipment is not suitable for use in locations where children are likely to be present.

Table of Contents

Foreword I

Important Safeguards and Warnings III

1 Product Overview 1

2 Dimensions 2

3 Wiring 3

4 Installation 4

4.1 Installation (Model GL) 4

4.2 Installation (Model E and Model E-S) 5

5 Local Operations 7

5.1 Keypad Introduction 7

5.2 Powering On 10

5.3 Creating Administrator Account 10

5.4 Logging In 10

6 SmartPSS Lite Operations 12

6.1 Installation 12

6.2 Initialization 12

6.3 Logging In 13

Appendix 1 Important Points of Fingerprint Registration Instructions 15

Appendix 2 Input Method 17

Appendix 3 FAQ 18

Appendix 4 Cybersecurity Recommendations 19

1 Product Overview

The Device can be used to track attendance of people. People can clock in/out through fingerprint, password, and card. Card swiping is only available on select models.

2 Dimensions

Figure 2-1 Dimensions (Model GL) (mm[inch])

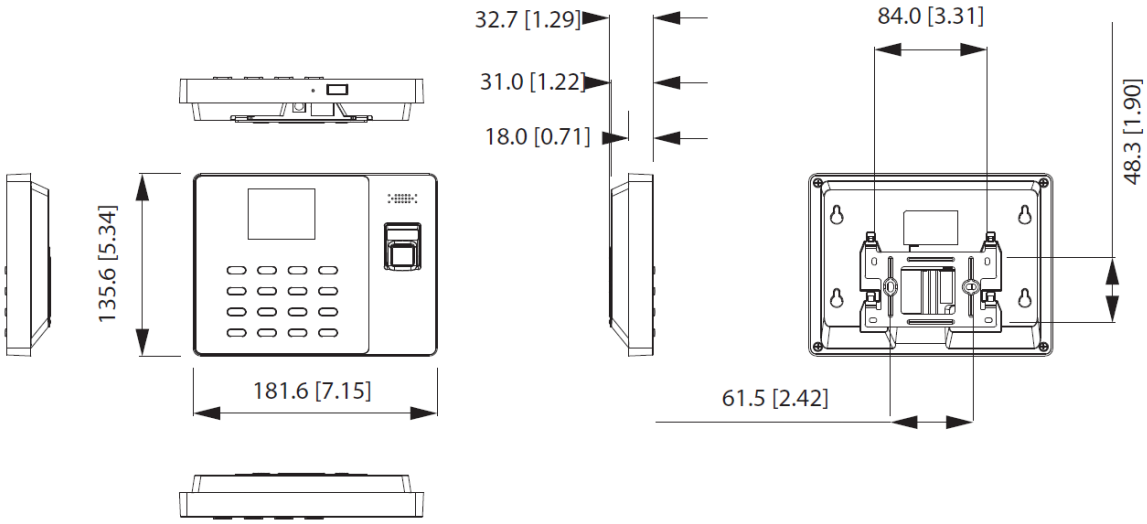
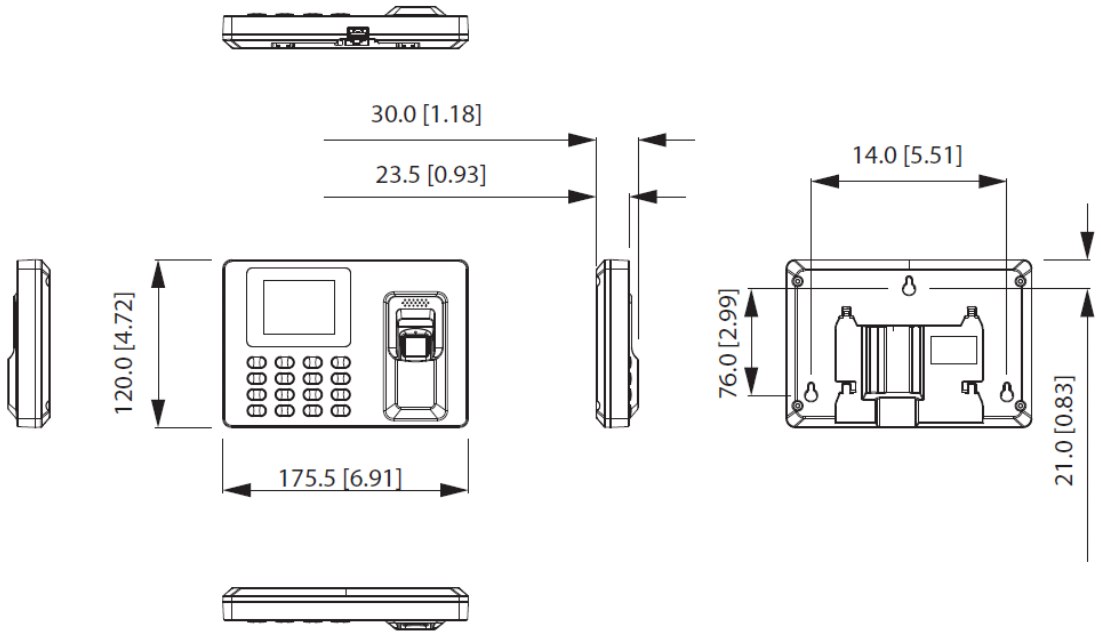
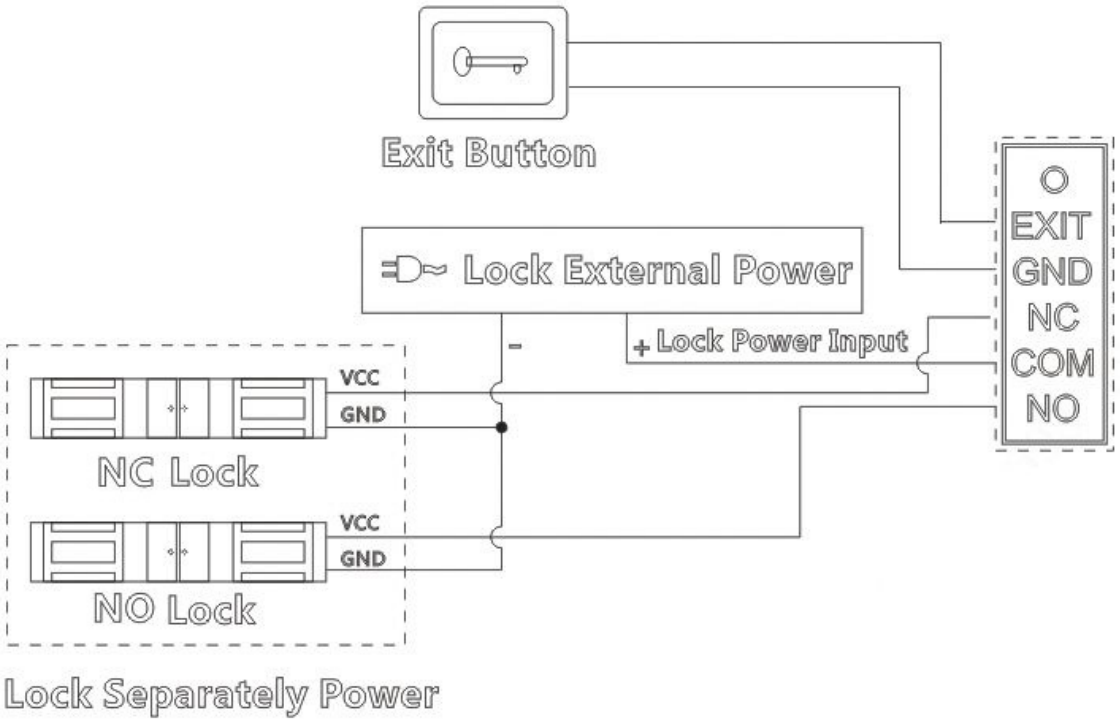


Figure 2-2 Dimensions (Model E and model E-S) (mm[inch])



3 Wiring

Figure 3-1 Wall mount (GL model) (mm[inch])



4 Installation

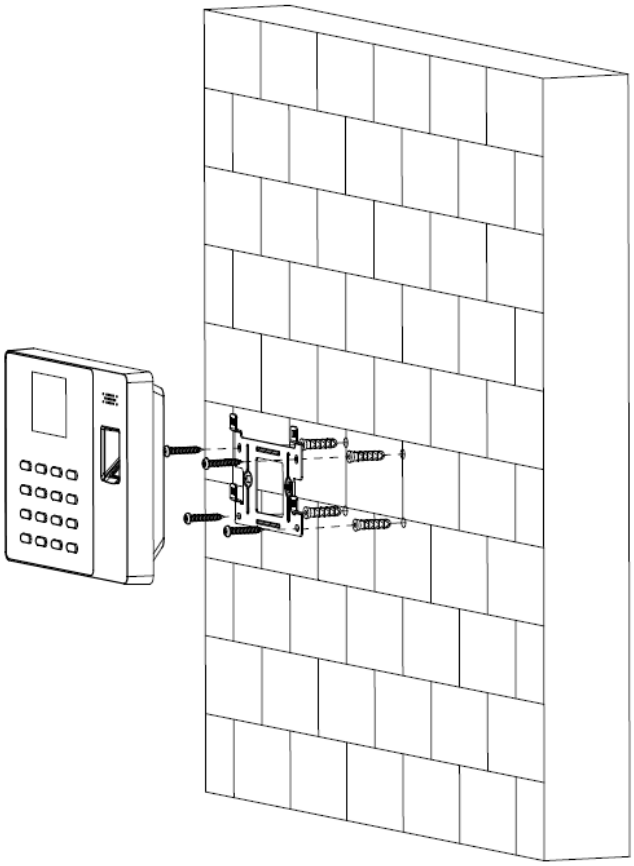
4.1 Installation (Model GL)

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 Access Controller. For details, see "3 Wiring".
4. Attach the Access Controller on the bracket.

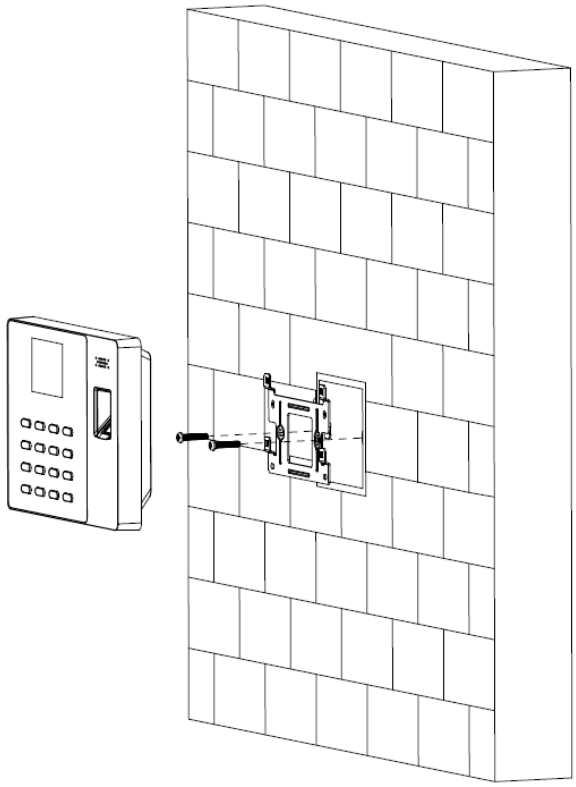
Figure 4-1 Wall mount (GL model) (mm[inch])



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 Access Controller. For details, see "3 Wiring".
4. Attach the Access Controller to the bracket.

Figure 4-2 86 box mount (GL model) (mm[inch])



4.2 Installation (Model E and Model E-S)

Procedure

Step 1 Place the mounting paper on the wall. Drill 3 holes into the wall according to the position of the holes on the paper

The cable outlet is required for in-wall mounting.

Step 2 Hammer in expansion bolts into the holes.

Step 3 Screw 3 screws into the expansion bolts.

Step 4 Wire the Access Controller.

Step 5 Attach the Access Controller to the bracket.

Figure 4-3 Surface-mounted wiring

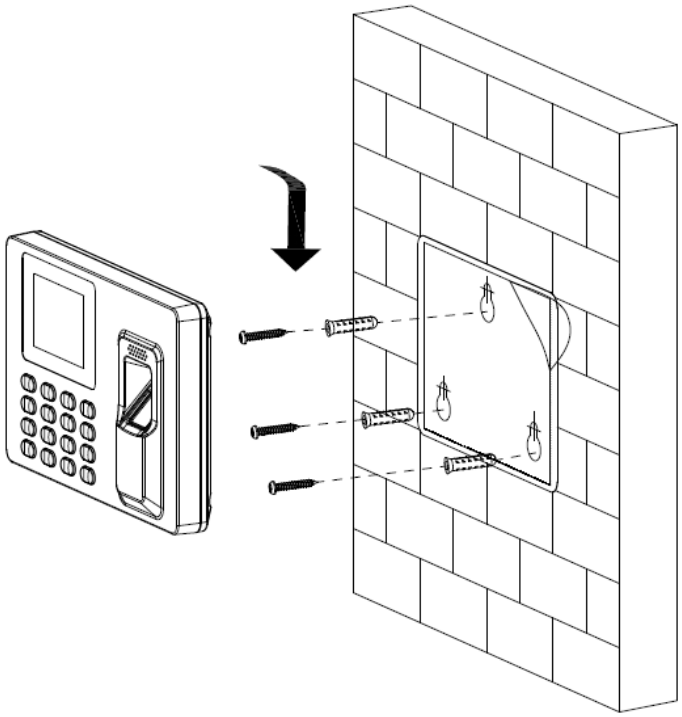
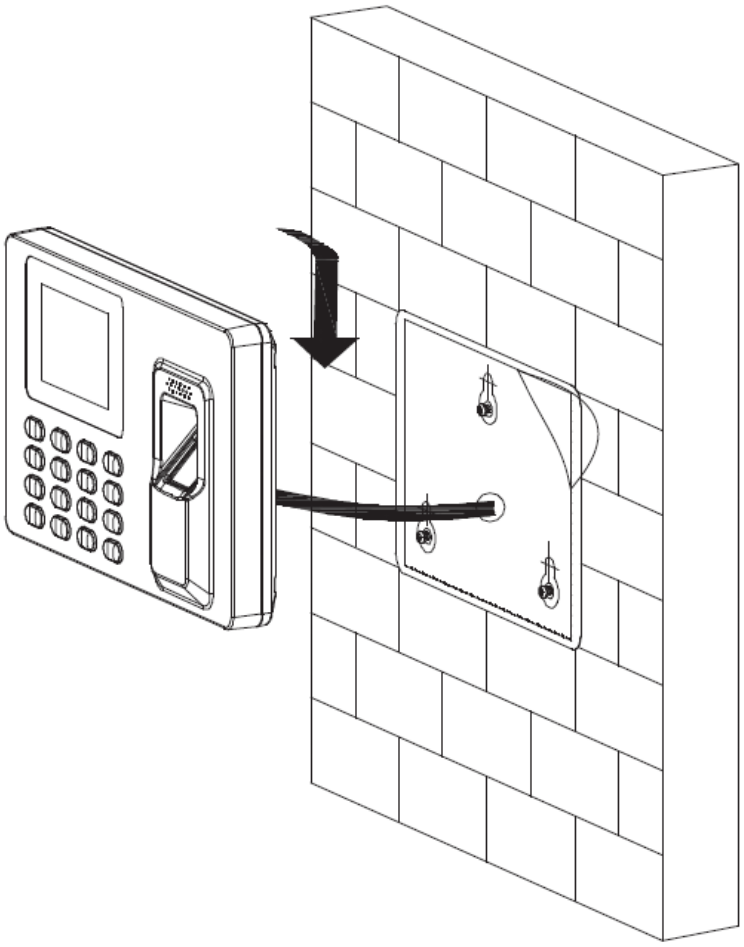


Figure 4-4 In-wall wiring



5 Local Operations

The keypad is slightly different depending on the models of the Device. This section uses the GL model as an example.

5.1 Keypad Introduction

Figure 5-1 Appearance (GL)



Table 5-1 Parameters description

Parameter	Description
0–9	Number keys to input numbers and letters.
ESC/F1	● Exit or go to the previous screen. ● Tap it on the standby screen to clock in.
∧/F2	● Tap it on the standby screen, BREAK OUT will be displayed on the screen. ● Tap to go up the options.
∨/F3	● Tap it on the standby screen, and BREAK IN will be displayed on the screen. ● Tap it to go down through the options.
OK/F4	● Confirm your settings. ● On the standby screen, tap it to clock out.
#	● Delete. ● Shortcut for reviewing records.

Parameter	Description
	● Press and hold it for over 3 seconds to turn the Device off/on. ● On the standby screen, tap it to enter the main menu by fingerprints, passwords or cards. Only administrators can enter the main menu. ● Tap it to change the input types (numbers, letters and symbols).

Figure 5-2 Appearance (Model E)



Figure 5-3 Appearance (Model E-S)



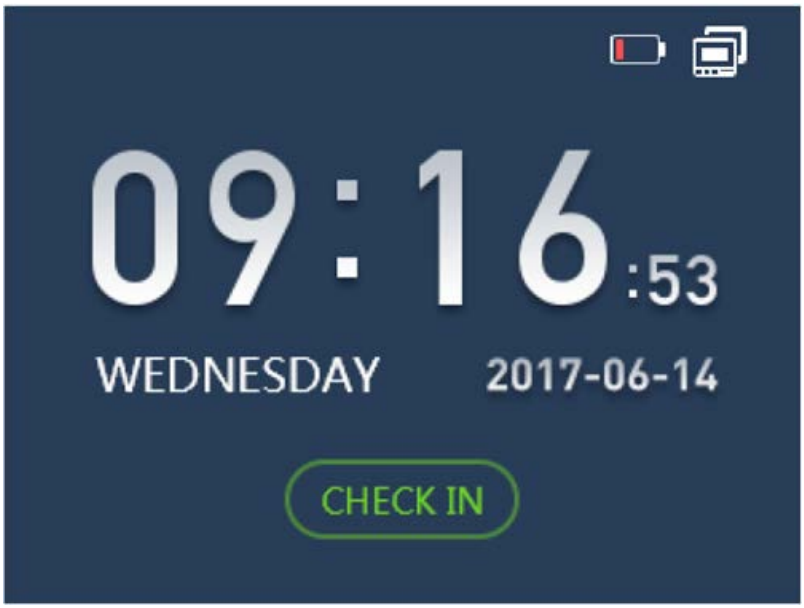
Table 5-2 Parameters description

Parameter	Description
0～9	Number key to input numbers and letters.
ESC	Go back or exit.
∧	Tap it to go up the options.
∨	Tap it to go down through the options.
OK	Enter or confirm
#	Backspace
	Enter the main menu or switch input method.

5.2 Powering On

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

Figure 5-4 Standby screen



- indicates that the network is disconnected.
- indicates that the network is connected.
- indicates the battery status. When the Device starts for the first time, the battery level is 25% (can last for about 1 hour).

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 Tap to enter the main menu screen.

Step 2 Select **1 User** > **Add New User**

Step 3 Enter the user information.

Step 4 Select **Administrator** from **User Level**.

1. Select **User Level**, and then tap **OK/F4**.
2. Select∧**/F2** or∨**/F3** to select **Administrator**.
3. Tap **OK/F4**.

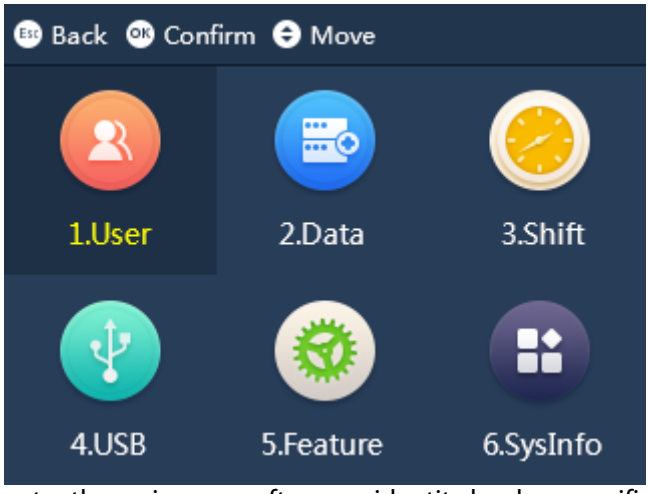
5.4 Logging In

After the admin account is created, you can enter the main menu after you have verified your

identifications through fingerprint, password or card.

The card swiping function is only available on select models.

Figure 5-5 Main Menu



Tap , and then enter the main menu after your identity has been verified.

- Place your finger on the fingerprint sensor.
- Enter the administrator's ID and password.
- Swipe the card on the card reader.

6 SmartPSS Lite Operations

Only certain models support configurations on SmartPSS Lite. For details, see the user's manual of SmartPSS Lite.

6.1 Installation

Contact technical support or download ToolBox to get SmartPSS Lite.

- If you get the software package of SmartPSS Lite, install and run the software according to page instructions.
- If you get the software by the ToolBox, run SmartPSS Lite according to the instructions on the page.

6.2 Initialization

Initialize SmartPSS Lite when you log in for the first time. You will need to set a password for login and your security questions for resetting the password.

Procedure

Step 1 Double-click SmartPSSLite.exe, or click **Open** next to the software icon in the ToolBox.

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

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

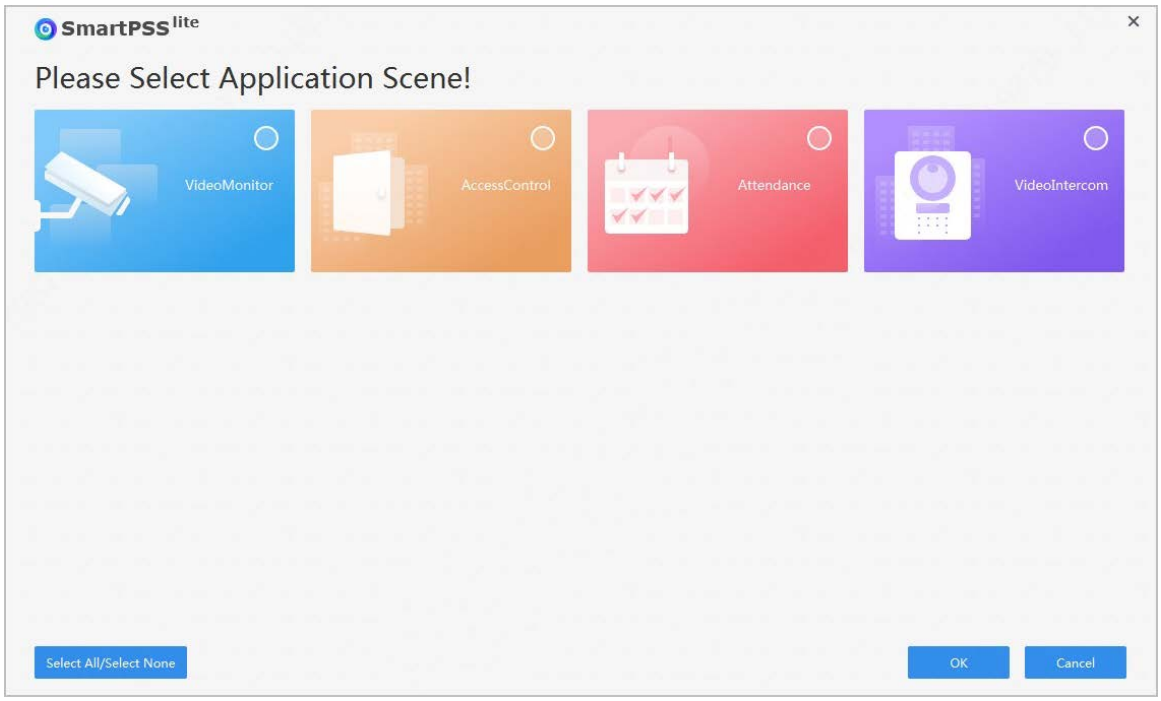
Step 4 Click **Finish** to complete the installation.



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

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

Figure 6-1 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**.

Table 6-1 Initialization parameters

Parameter	Description
Password	The password must consist of 8 to 32 non-blank characters and contain at least 2 types of characters including uppercase letters, lowercase letters, numbers and special characters
Password Strength	Displays the strength of a password against being guessed and brute-force attacks. Green means the password is strong, and red means it is too weak. Set a high security password using the password strength prompt to assist you.
Confirm Password	Enter the password again to confirm the password.
Auto Login after Registration	Enable **Auto Login after Registration** so that SmartPSS Lite will log in automatically after initialization; otherwise the login page is displayed.

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

6.3 Logging In

Procedure

Step 1 Double-click SmartPSSLite.exe, or click **Open** next to the software icon in the ToolBox.

Step 2 Enter the username and password, and then click **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 you log in next time.

Parameter	Description
Auto Login	Enable **Auto Login** so that the SmartPSS Lite will log in automatically the next time when you use the same account.
Forgot password?	Click **Forgot password?** to reset the password when you forget the password.

Appendix 1 Important Points of Fingerprint Registration Instructions

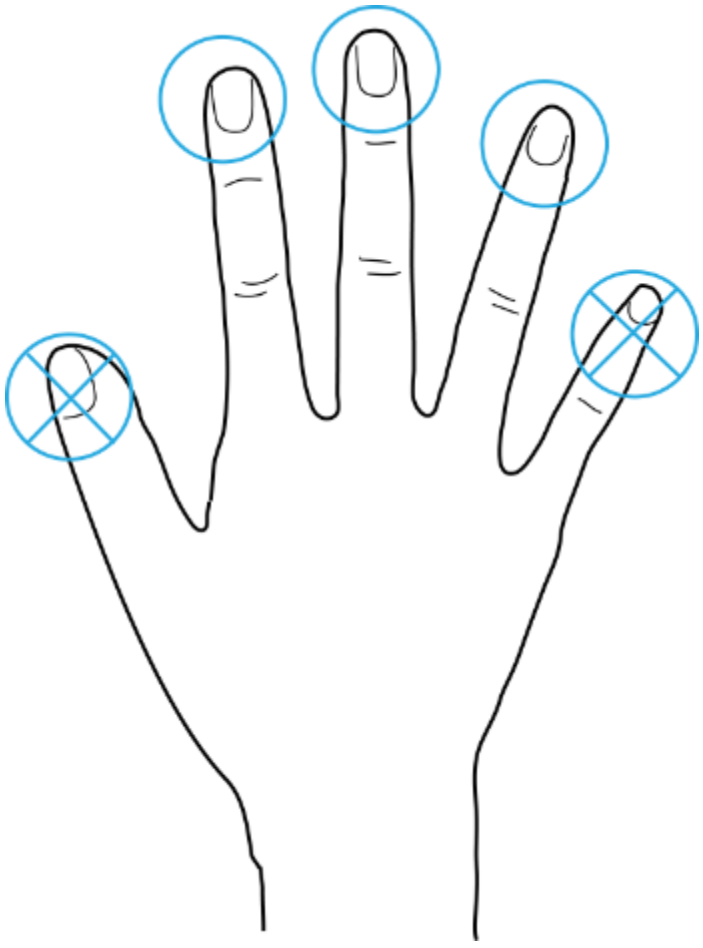
When you register the fingerprint, pay attention to the following points:

- 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

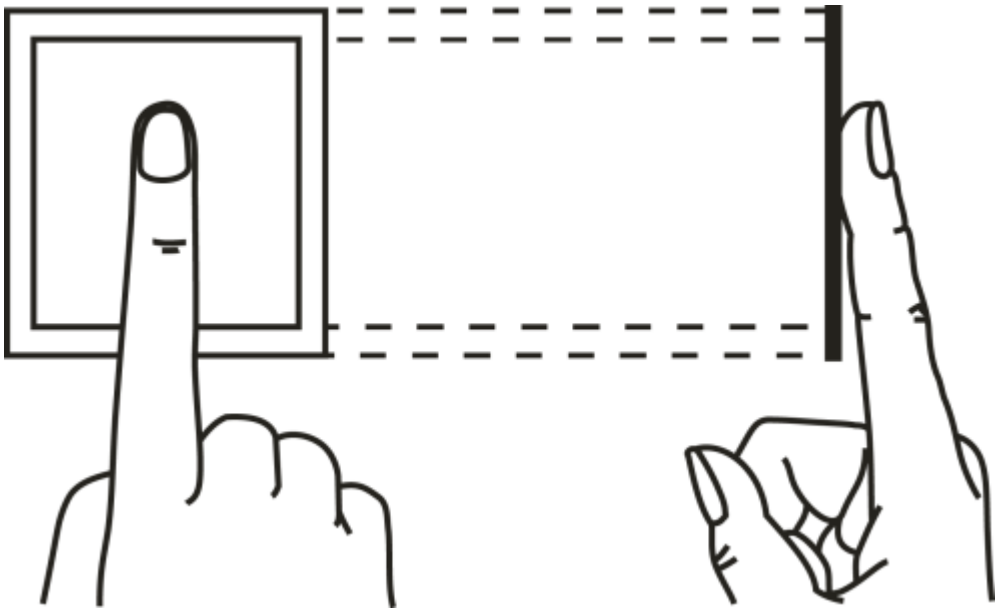
Forefingers, middle fingers, and ring fingers are recommended. Thumbs and little fingers cannot be put at the recording center easily.

Appendix Figure 1-1 Recommended fingers

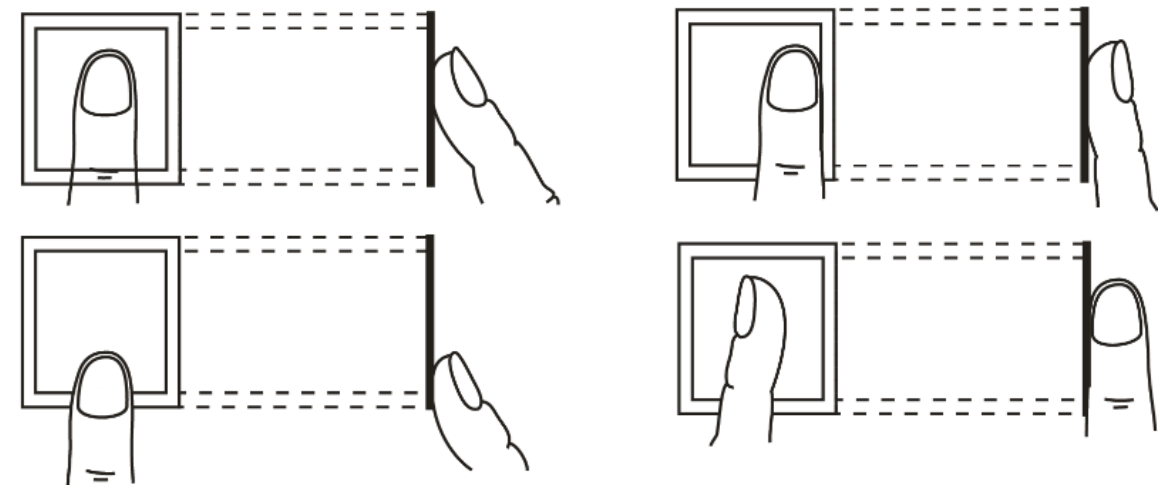


How to Press Your Fingerprint on the Scanner

Appendix Figure 1-2 Correct placement



Appendix Figure 1-3 Wrong placement



Appendix 2 Input Method

You can type English letters, numbers and symbols.

Numbers

1. Tap  to switch input methods until **123** is displayed on the screen.
2. Enter numbers.
3. Tap **OK/F4** to confirm.

Letters

1. Tap  to switch input methods until **ABC** is displayed on the screen.
2. Enter letters.
3. Tap **OK/F4** to confirm.

Symbols

1. Tap  to switch input methods until **:-)** is displayed on the screen.
2. Tap∧**/F2** or∨**/F3** to select symbols.
3. Tap **OK/F4** to confirm.

Appendix 3 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 4 Cybersecurity Recommendations

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 device 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. **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.

8. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a

minimum set of permissions to them.

9. **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.

10. **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.

11. **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.

12. **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.

13. **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.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.