Access Standalone

Quick Start Guide



V1.0.2

Foreword

General

This manual introduces the installation and basic operations of the Access 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
V1.0.2	Updated the wiring diagram.	April 2025
V1.0.1	Added initialization description.	December 2024
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, 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.

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 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 Structure 1
2 Wiring and Installation 2
2.1 Installation Requirements 2
2.2 Wiring 3
2.3 Installation Procedure 7
3 Local Configurations 9
3.1 Initialization 9
3.2 Main Menu 10
3.3 Adding Users 11
4 SmartPSS Lite Operations 12
4.1 Installation 12
4.2 Initialization 12
4.3 Login 15
Appendix 1 Security Recommendation 17

1 Structure

The diagram is for reference only. The structure and dimensions might differ according to the actual models.

Figure 1-1 Dimensions (unit: mm [inch])

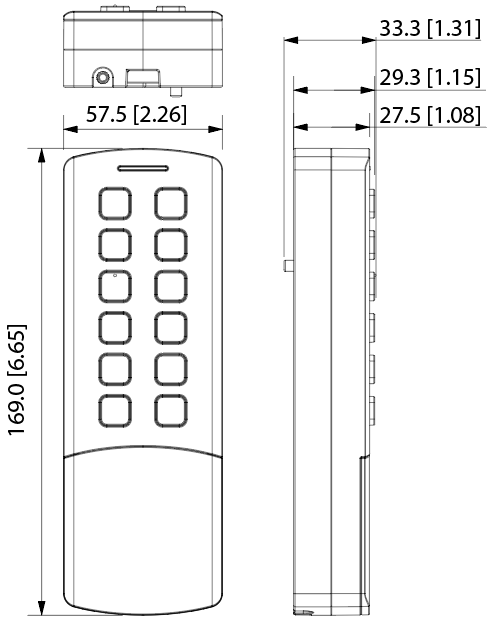
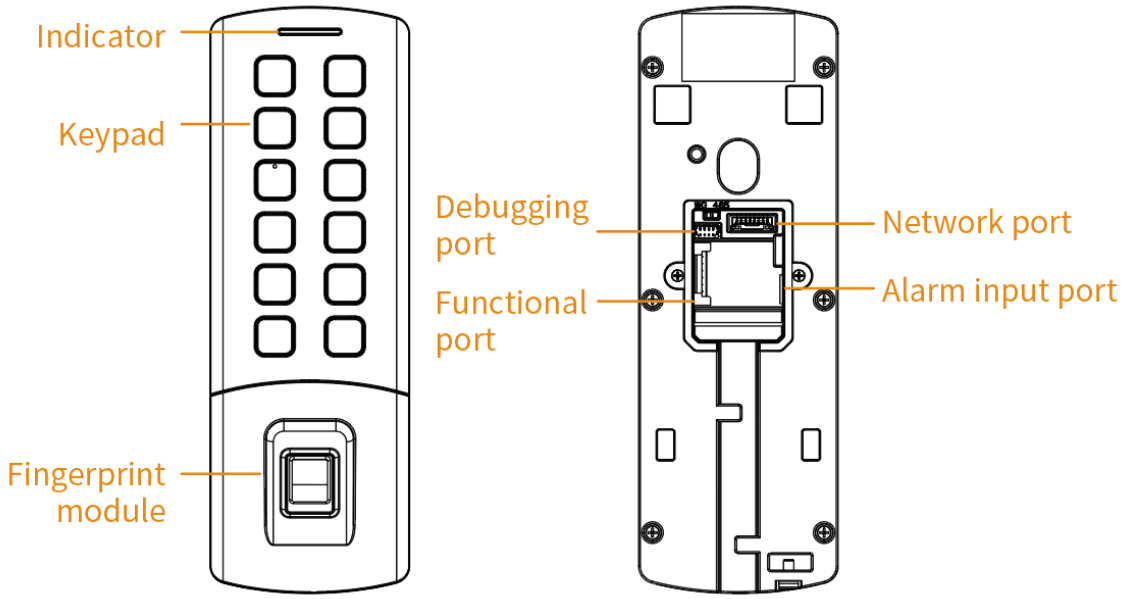


Figure 1-2 Structure



The fingerprint function is available on select models.

2 Wiring and Installation

2.1 Installation Requirements

- The recommended installation height (from the indicator to ground) is 1.4 m.
- The light at the 0.5 meters away from the device should be no less than 100 Lux.
- We recommend you install the device indoors, at least 3 meters away from windows and doors, and 2 meters away from the light source.
- Avoid backlight, direct sunlight, close light, and oblique light.

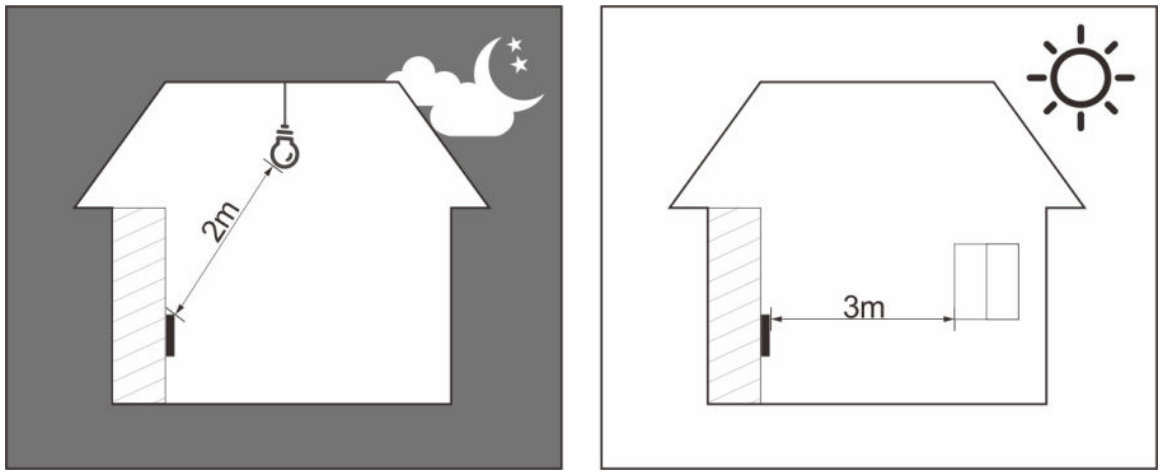
Ambient Illumination Requirements

Figure 2-1 Ambient illumination requirements



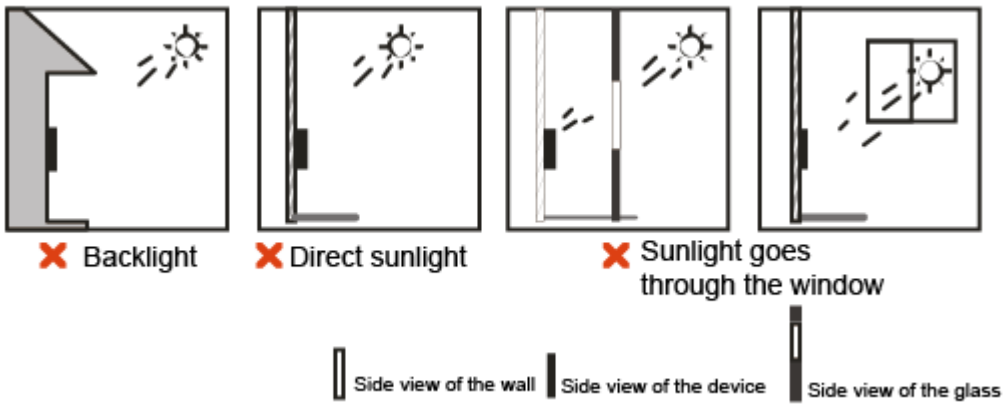
Recommended Installation Location

Figure 2-2 Recommended installation location



Installation Location Not Recommended

Figure 2-3 Installation location not recommended



2.2 Wiring

Ports might differ depending on models of the product.

- RS485A and WG_D0 share the same cable. RS485B and WG_D1 share the same cable.
- When the DIP switch is set to WG, the shared cable can be connected to Wiegand device. When the DIP switch is set to 485, the shared cable can be connected to RS-485 device.
- If you select **Door Control Module** through **Communication Settings** > **RS-485 Config**, a door control security module needs to be purchased separately. The security module needs a separate power supply.
- When the security module function is turned on, the exit button, lock control and alarm linkage become not effective.

Figure 2-4 Wiring

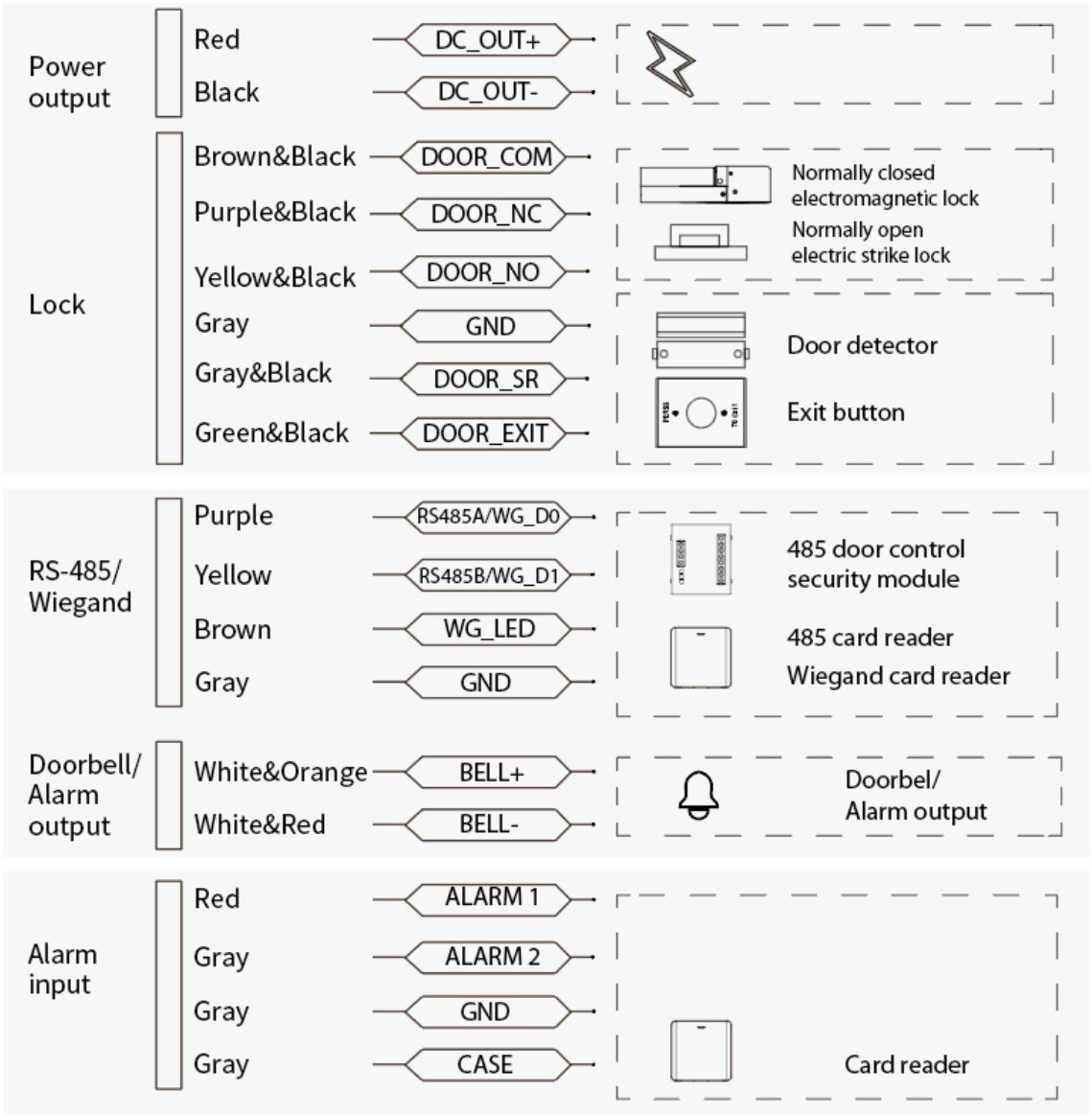


Figure 2-5 Wiring for the regular device

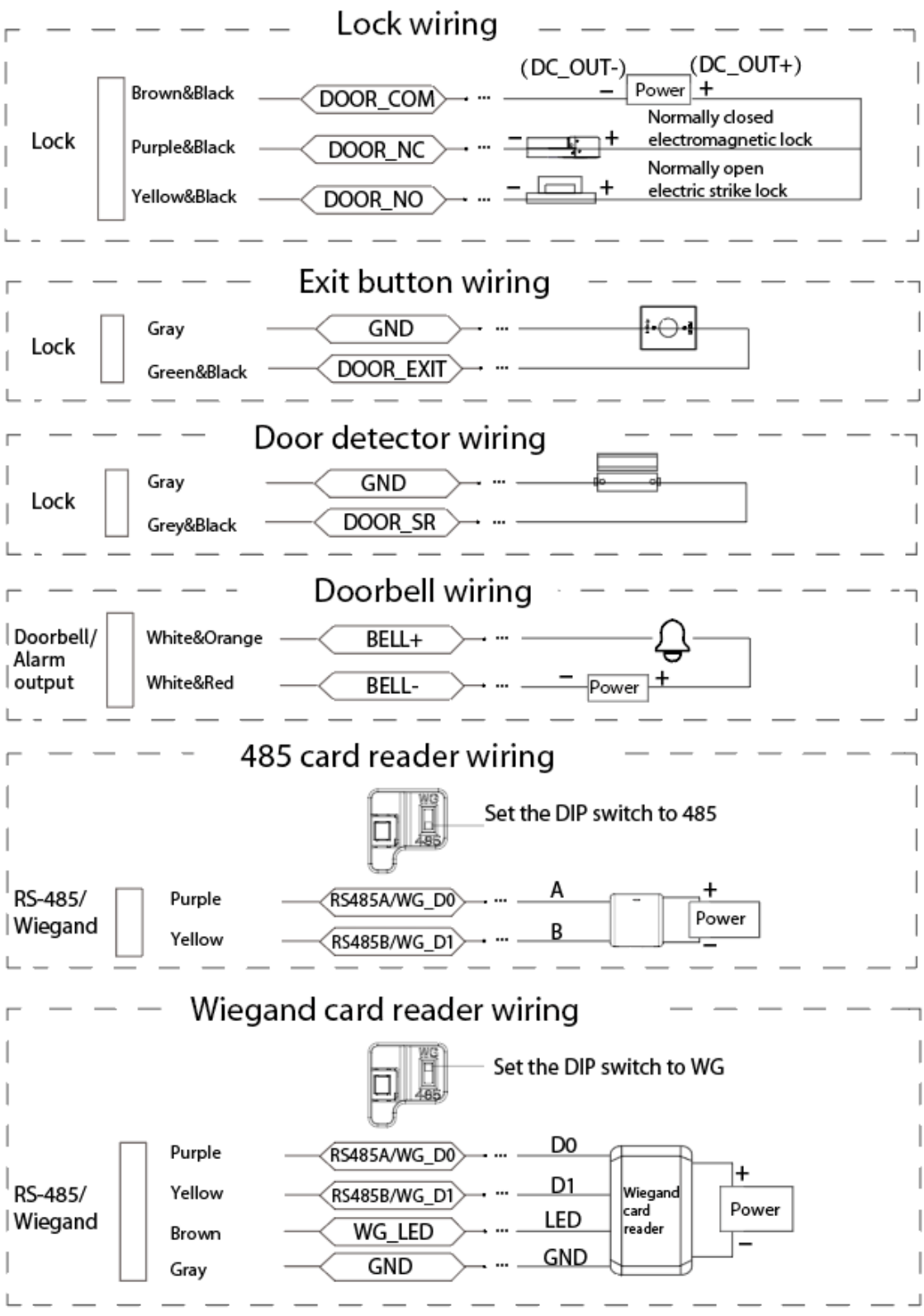


Figure 2-6 Wiring for the door control security module

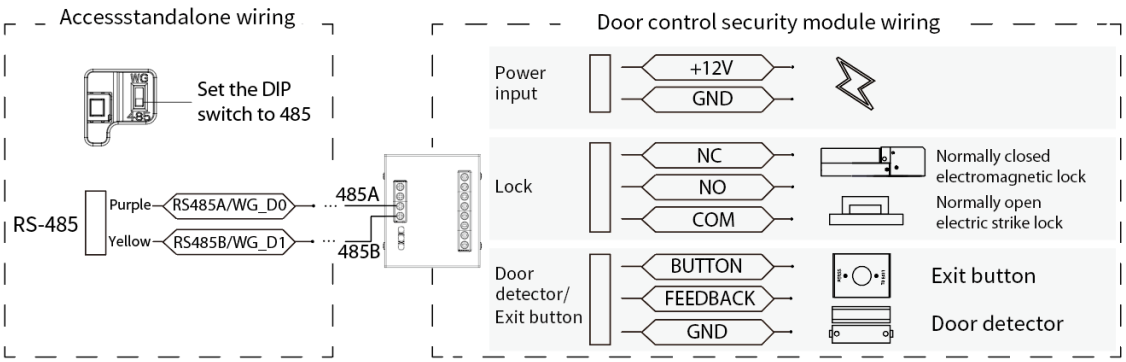


Figure 2-7 Power wiring

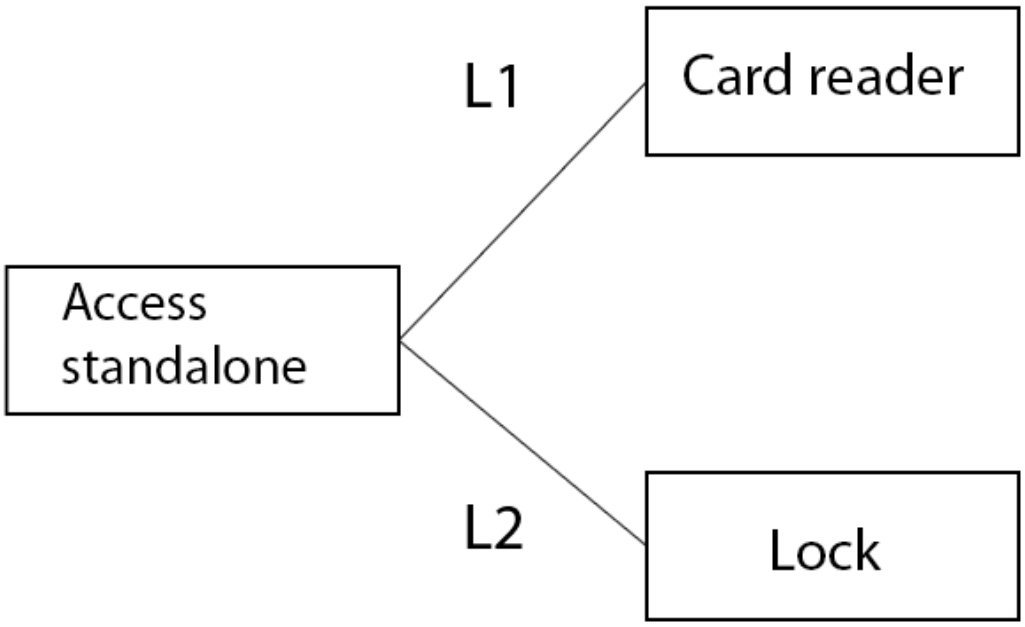


Table 2-1 Cable specification description

No.	Name	Recommended Model and Specification	Recommended Max Power Supply Distance and Communication Distance
L1	Card Reader Cable	• RVV0.5 (DC resistance of a single conductor ≤ 39.0 Ω/km) • RVV1.0 (DC resistance of a single conductor ≤ 19.5 Ω/km) • RVV1.5 (DC resistance of a single conductor ≤ 13.3 Ω/km) • CAT5E (impedance within 100 m ≤ 9 Ω)	• RVV0.5 ◇ RS_485 card reader: ≤ 200 m ◇ Wiegand card reader: ≤ 120 m • CAT5E (one-core) ◇ RS_485 card reader: ≤ 120 m ◇ Wiegand card reader: ≤ 50 m

No.	Name	Recommended Model and Specification	Recommended Max Power Supply Distance and Communication Distance
L2	Lock Cable		• RVV0.5 280 kg one-door electromagnetic lock: ≤ 60 m • RVV1.0 280 kg one-door electromagnetic lock: ≤ 100 m • RVV1.5 280 kg one-door electromagnetic lock: ≤ 140 m

- If the card reader is powered by the access standalone, we recommend you select a card reader with a maximum current not exceeding 200 mA. The selected card reader should support wide voltage operation, with the lowest operating voltage not exceeding 9 V.
- If the lock is powered by the access standalone, we recommend you select a lock with a maximum current not exceeding 500 mA. The selected lock should support wide voltage operation, with the lowest operating voltage not exceeding 10 V.
- The wiring distance of L1 and L2 is affected by the voltage of the power supply and the power supply cable specification. During actual construction, the power supply voltage should be ensured not to be lower than the lowest operating voltage of the access standalone, card reader, and lock. Additionally, L1 and L2 should not share the same wire.
- When using CAT5E (impedance within 100 m ≤ 9 Ω) for the power supply of locks or card readers, we recommend you allocate the extra wires, apart from the necessary signal wires, evenly for the power supply of locks or card readers in order to minimize power supply loss.
- The data might differ according to the actual situation.

2.3 Installation Procedure

The device supports wall mount and there are 2 wiring methods of surface-mounted wiring and in-wall wiring.

Procedure

Step 1 According the holes' positions of the installation bracket, drill 6 holes and 1 wiring slot in the wall.

The wiring slot in the wall is not required for surface-mounted wiring.

Step 2 Insert the expansion screws into the holes, and then screw in the bracket to the wall.

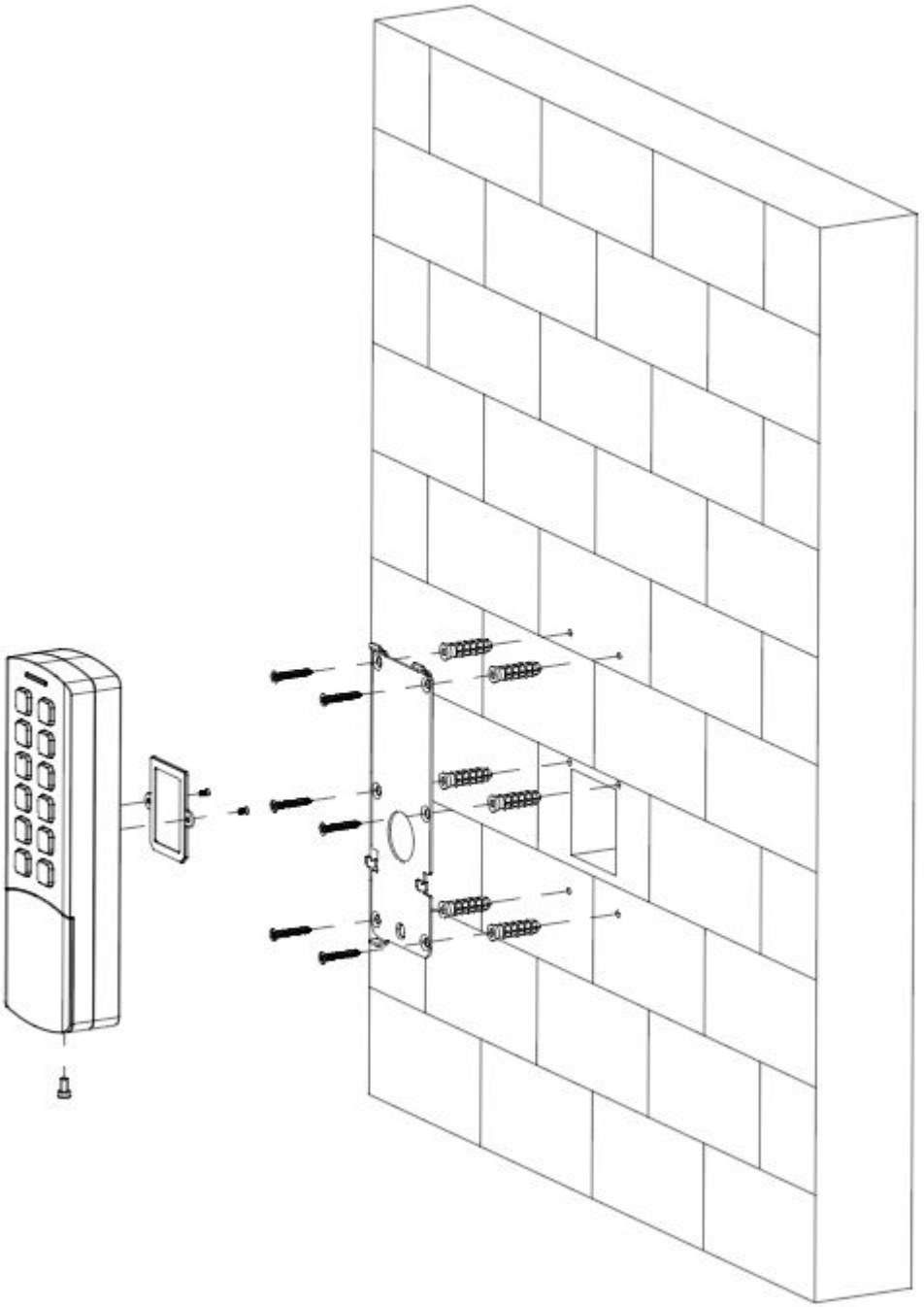
Step 3 Wire the device. For details, see "2.2 Wiring".

- Wire the cable through the installation rear panel and the wiring slot on the wall for in-wall wiring.
- The cable is not required to be wired through the installation rear panel for surface-mounted wiring.

Step 4 Attach the device to the rear panel bracket.

Step 5 Screw in a screw at the bottom of the device.

Figure 2-8 Installation



3 Local Configurations

Local operations might differ depending on different models of Access Controller.

3.1 Initialization

After the Device is powered on for the first time, you need to set the administrator password. The administrator password is used to enter the main menu of the Device.

Procedure

Step 1 Power on the Device, and the indicator light will flash red slowly.

Step 2 Press **#** , enter the administrator password, and then press **#**.

The password must be 1 to 8 characters in length.

If the indicator light is solid blue, it means the Device is initialized.

After initialization, you can only use the functions on the Device. If you want to login to the webpage of the Device, initialize the Device on its webpage or through the ConfigTool.

Related Operations

- You can only set numbers as the admin account password when you initialize it through the Device.
- You can set numbers, letters and other characters as the admin account password when you initialize it through the platform of the ConfigTool.

After you complete the initialization on the Device, you can only perform operations on the Device itself. If you need to connect the Device to the network, use ConfigTool or the platform to initialize the Device.

When you use ConfigTool or the platform to initialize the Device, after configuring the network account and password, the device will automatically complete initialization and enter the standby status. The local admin password is converted from the network password. If the password exceeds 8 characters, only the first 8 characters are kept. The letters are converted into digits according to the E.161 standard. The password conversion is case-insensitive, and all other symbols are converted to 0.

- After the initialization, if you modify the network password, the local admin password will not be affected.
- If you initialize through the Device first, then initialize through the ConfigTool or the platform, the local admin password will not be affected.

Figure 3-1 E.161 (T9 keypad)

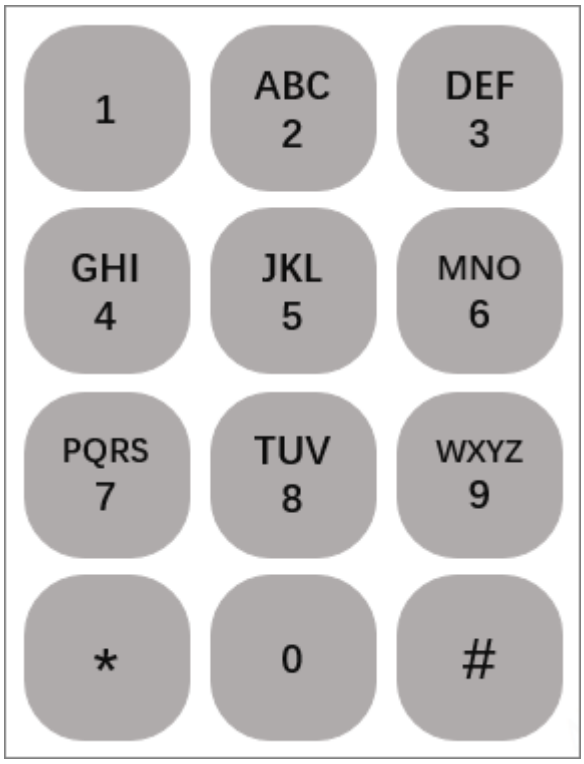


Table 3-1 Conversion example

Network Password	Local Admin Password
ABC12345	22212345
admin123	23646123
admin12!	23646120
admin123456	23646123

3.2 Main Menu

Entering Main Menu

Press **#** , enter the administrator password, and then press **#**.

- The indicator flashes blue, and it means you have entered the main menu.
- The indicator flashes red once, the buzzer beeps 3 times, and then the indicator turns solid blue, which means the password is wrong.

Related Prompts

- The indicator flashes green once, and the buzzer beeps once, which means that the operation or access control verification is successful.
- The indicator flashes red once, and the buzzer beeps 3 times, which means that the operation or access control verification failed.
- If the indicator flashes red slowly, it means the Device is not uninitialized.

- If the indicator is solid blue, it means the Device is in the standby status.
- The indicator flashes blue, it means the Device enters the main menu.
- The keypad is white when you operate the device. If there is no operation within 10 seconds, the light turns off and the Device exits the current screen.

3.3 Adding Users



- You can add only one card, one password or one fingerprint for one user. At least one method of card, password, and fingerprint must be added.
- Fingerprint function is available on select models.

Procedure

Step 1 Press **#** , enter the administrator password, and then press **#**.

Enter the main menu, and the indicator flashes blue.

Step 2 Press **1** and **#** to add users.

Step 3 Enter the user ID, and then press **#**.

- If the indicator does not light up and the Device beeps, the user ID is added successfully.
- If the indicator flashes red and the Device beeps, you fail to add the user ID. The possible reason is the ID already exists. Please try the other ID.



You can only enter numbers for the ID on the Device.

Step 4 After swiping the card, press **#** to add the card.

If you do not need to add the card, press **#** to skip it.

Step 5 Enter the user password, and then press **#**.

If you do not need to set the user password, press **#** to skip it.



The password can be 1 to 8 characters in length.

Step 6 Add the fingerprint, and then press **#**.

If you do not need to set the fingerprint, press **#** to skip it.



This function is available on select models.

Step 7 Repeat Step 2 to Step 6 to add more users.

After adding the user, press * to return to the main menu, and then press * to return to the standby status.

4 SmartPSS Lite Operations

4.1 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.

4.2 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.

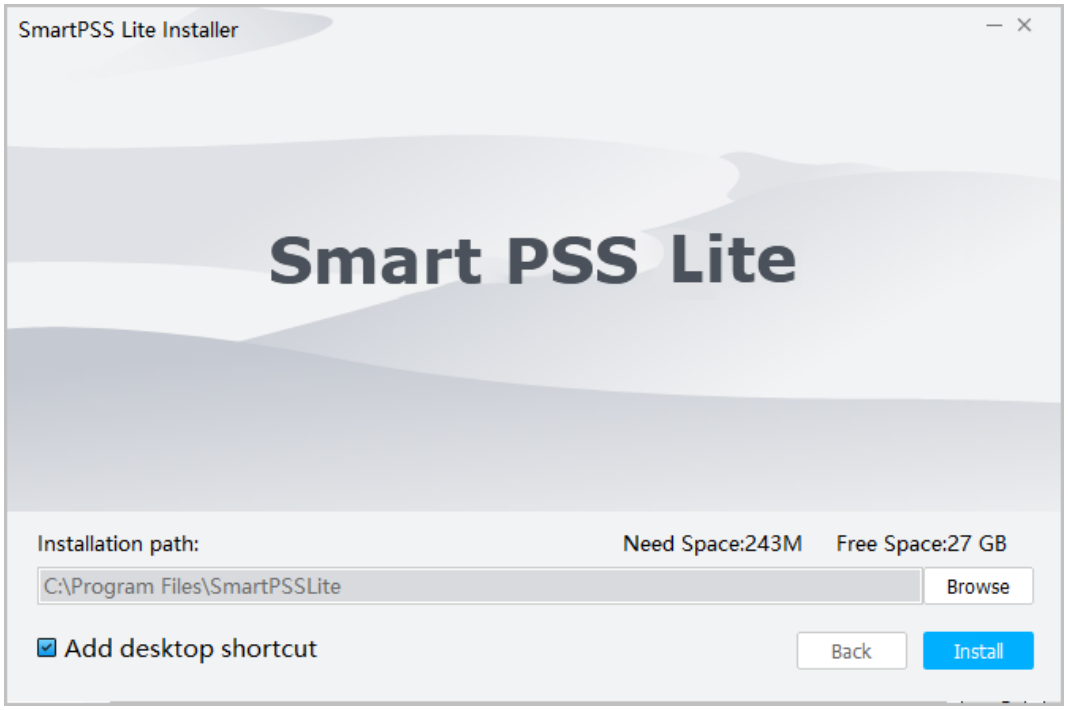
Step 2 Select the language from the drop-down list, select **I have read and agree the software agreement** , and then click **Next**.

Figure 4-1 Select language



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

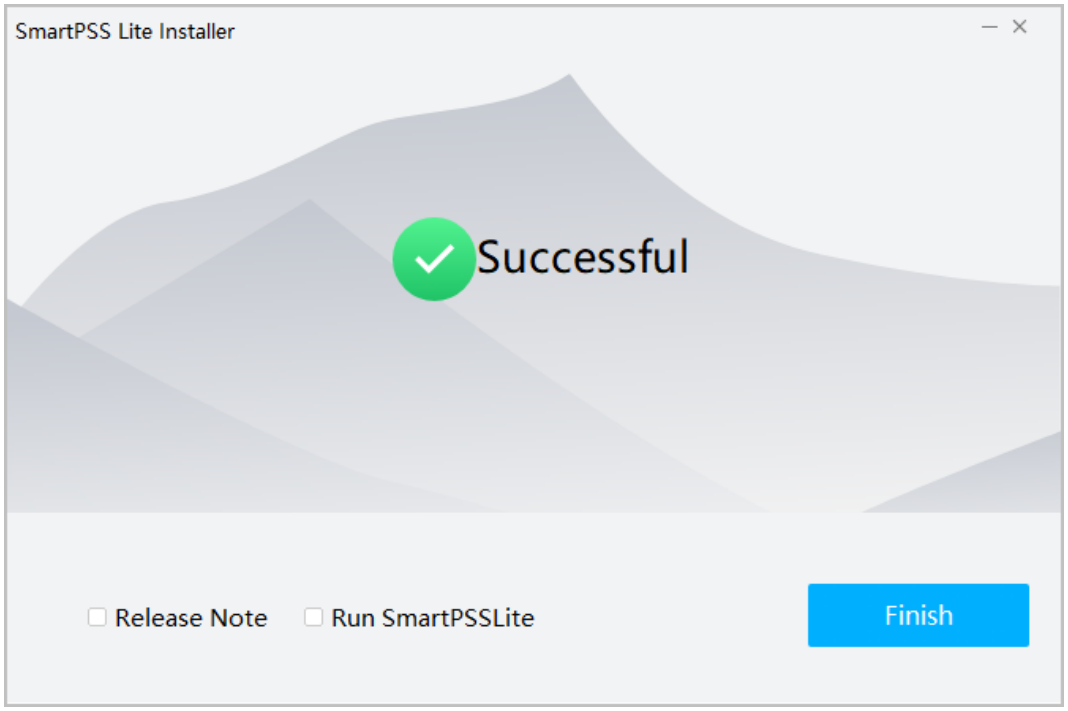
Figure 4-2 Select installation path



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

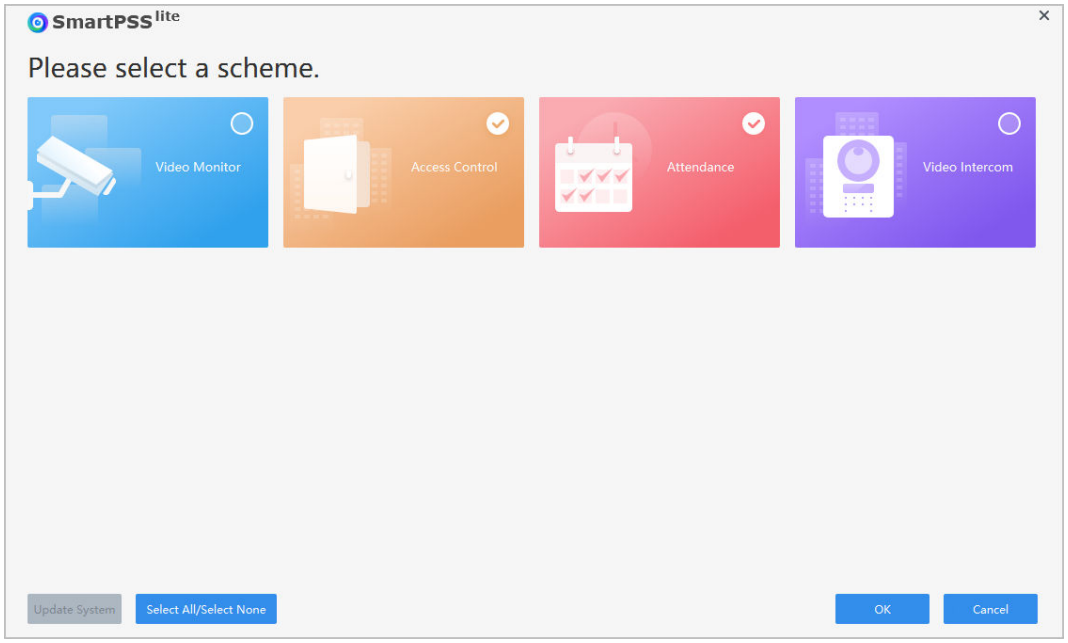
Select **Run SmartPSSLite** to start SmartPSS Lite.

Figure 4-3 Install complete



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

Figure 4-4 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 4-5 Set password

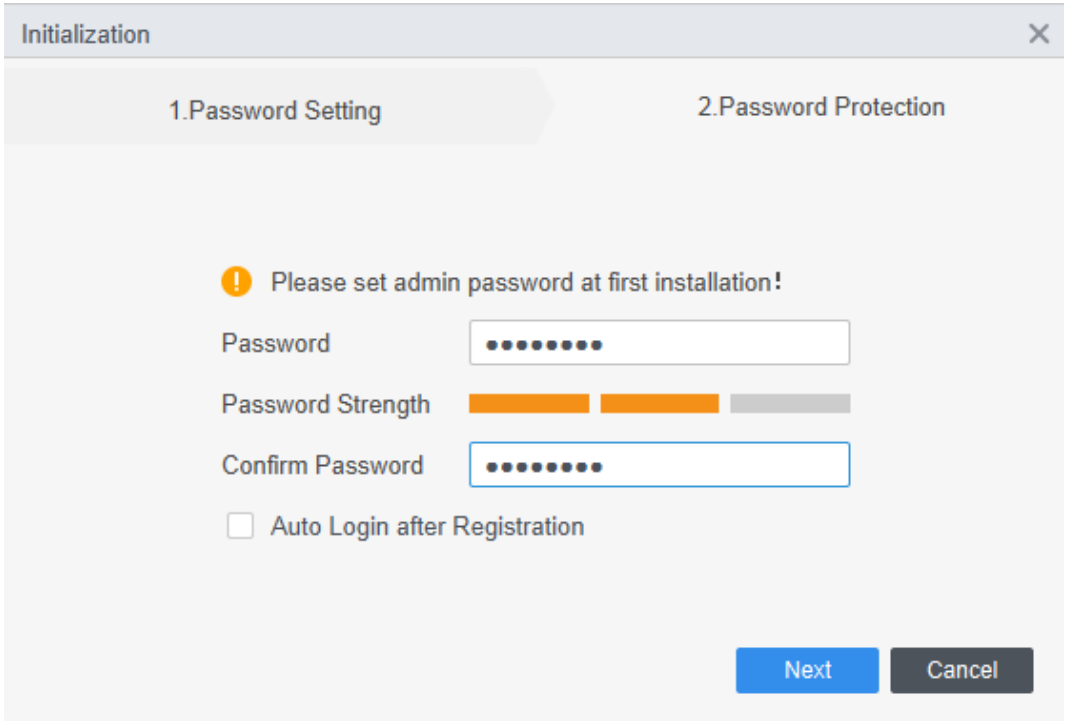
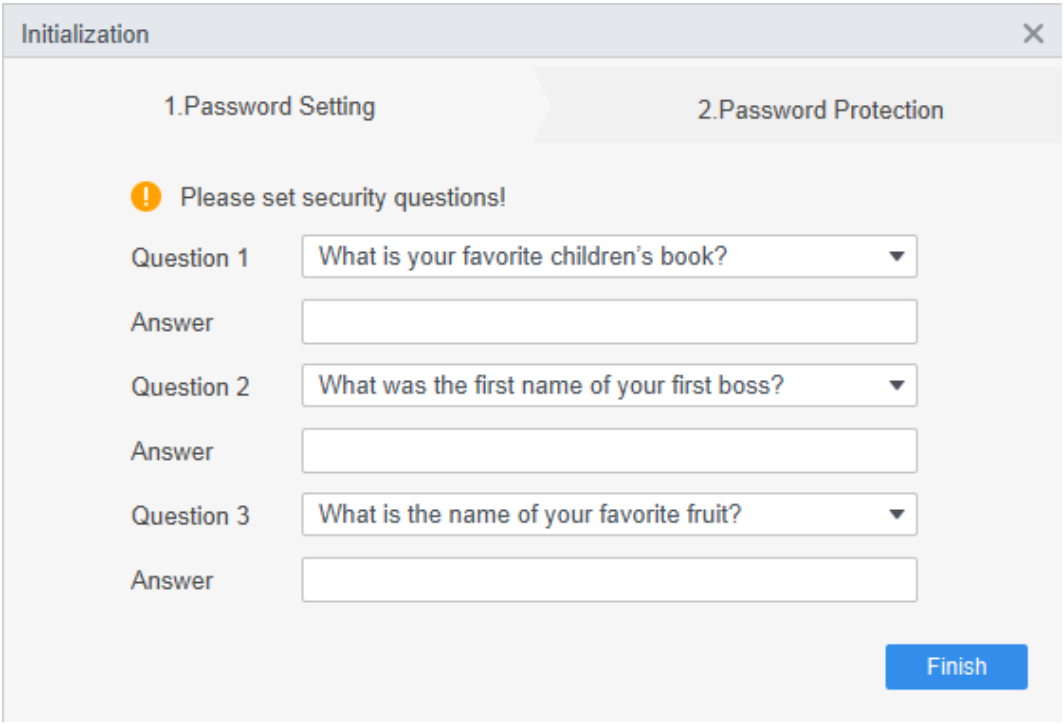


Table 4-1 Initialization parameters

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 4-6 Set security questions



4.3 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 4-7 Login

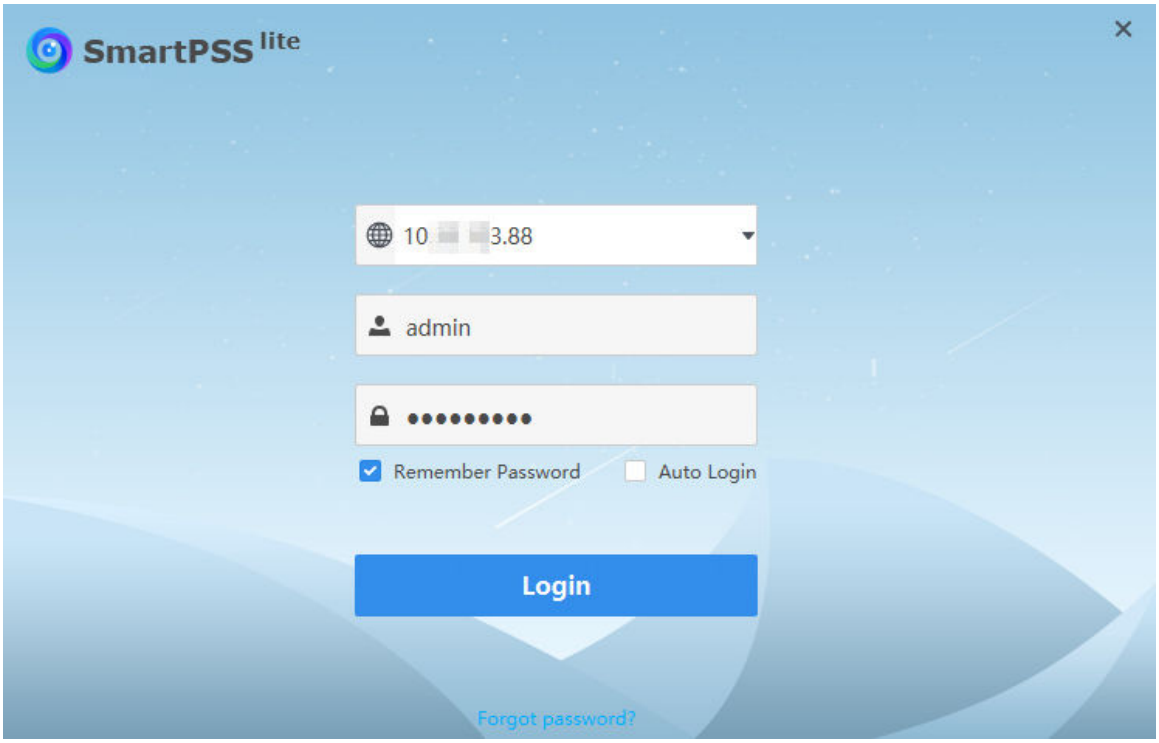


Table 4-2 Parameters of login

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 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 Allowlist**

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