Access Standalone

User Manual

V1.0.2

Foreword

General

This manual introduces the functions and 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.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.2	Updated the wiring diagram.	April 2025
V1.0.1	Added initialization description.	December 2024
V1.0.0	First release.	September 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'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.
- 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.

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.

Table of Contents

1 Product Overview

1.1 Overview

The Device is intended for access management in a controlled area. With a neat appearance and IPX6 waterproof grade, it can be used outdoors.

It has the following main features:

- Supports touch keyboard and TCP/IP protocol.
- Supports 30,000 valid cards and can store up to 60,000 records.
- Supports unlocking the door through the following modes:
  - Card
  - User ID + Password
  - Card + Password
  - Card or (User ID + Password)
- Supports overtime alarm, intrusion alarm, duress alarm, and tamper alarm.
- Supports guest card, duress card, blocklist/allowlist card, and patrol card.
- Support 128 groups of time schedules, 128 groups of period, and 128 groups of holiday period.

1.2 Structure

Figure 1-1 Structure

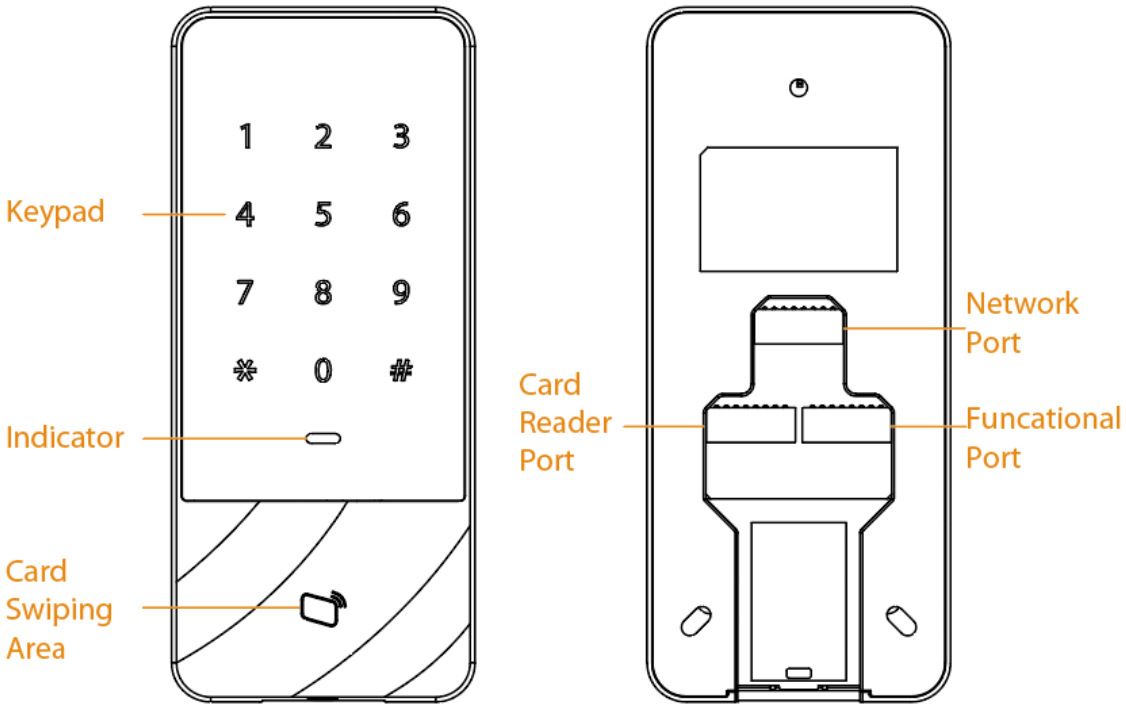


Table 1-1 Description of components and ports

Component/Port	Description
Keypad	• 0-9: Number buttons. • *: Return to previous step or exit. • #: Enter or confirm.
Indicator	• If the indicator flashes green and the Device beeps, it means the operations succeed or the identifications are successfully verified. • If the indicator flashes red and the Device beeps, it means the operations fail or the identifications fail to be verified.
Card Swiping Area	Swipe the authorized cards to open the door.
Card Reader Port	Includes RS-485 port, Wiegand port and power output port.
Functional Port	Includes door detector, exit button, lock port and power input port.
Network Port	Connects to the network cable.

2 Wiring and Installation

2.1 Installation Requirements

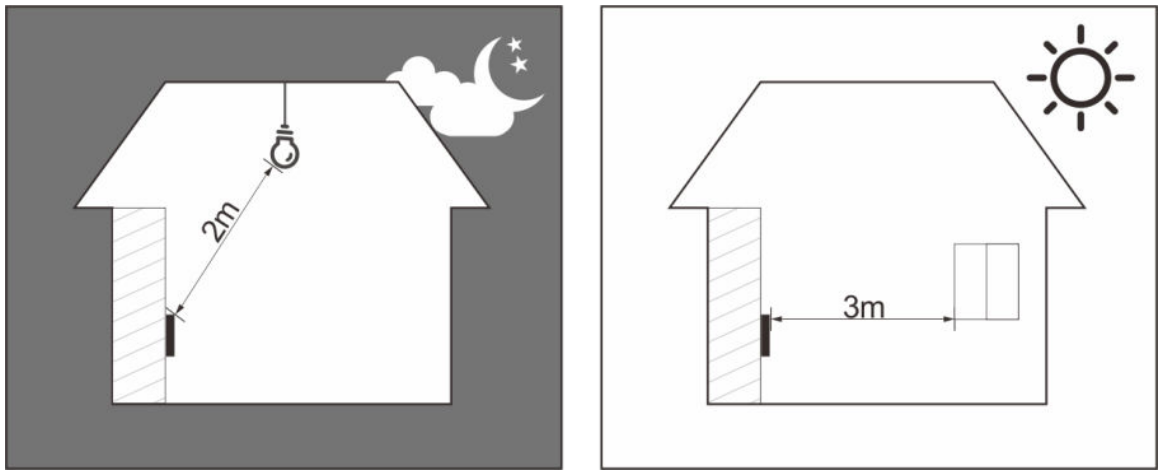
- The installation height is recommended to be from 1.2 m to 1.6 m(from the lens to the ground).
- The light at the 0.5 meters away from the Device should be no less than 100 lux.
- We recommend you install the indoors, at least 3 meters away from windows and doors, and 2 meters away from the light source.
- Avoid backlight, direct sunlight, close light, and oblique light.

Ambient Illumination Requirements

Figure 2-1 Ambient illumination requirements

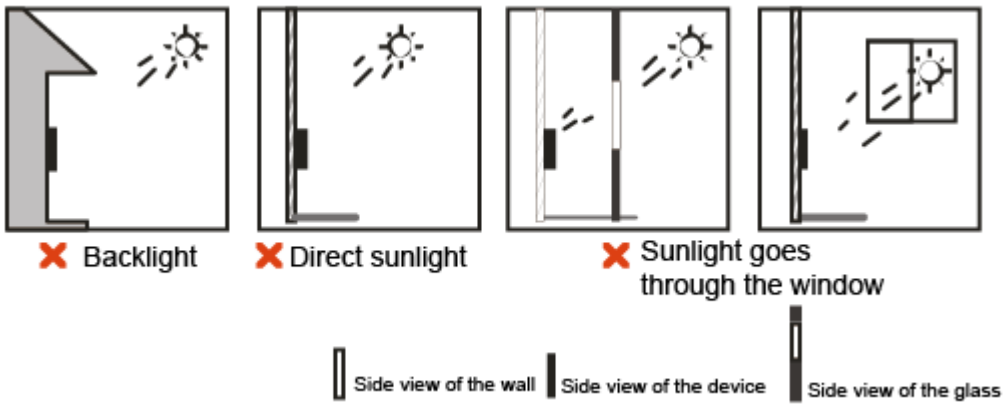
Recommended Installation Location

Figure 2-2 Recommended installation location



Installation Location Not Recommended

Figure 2-3 Installation location not recommended



2.2 Wiring

Connect the cables to the corresponding ports.

Figure 2-4 Cables

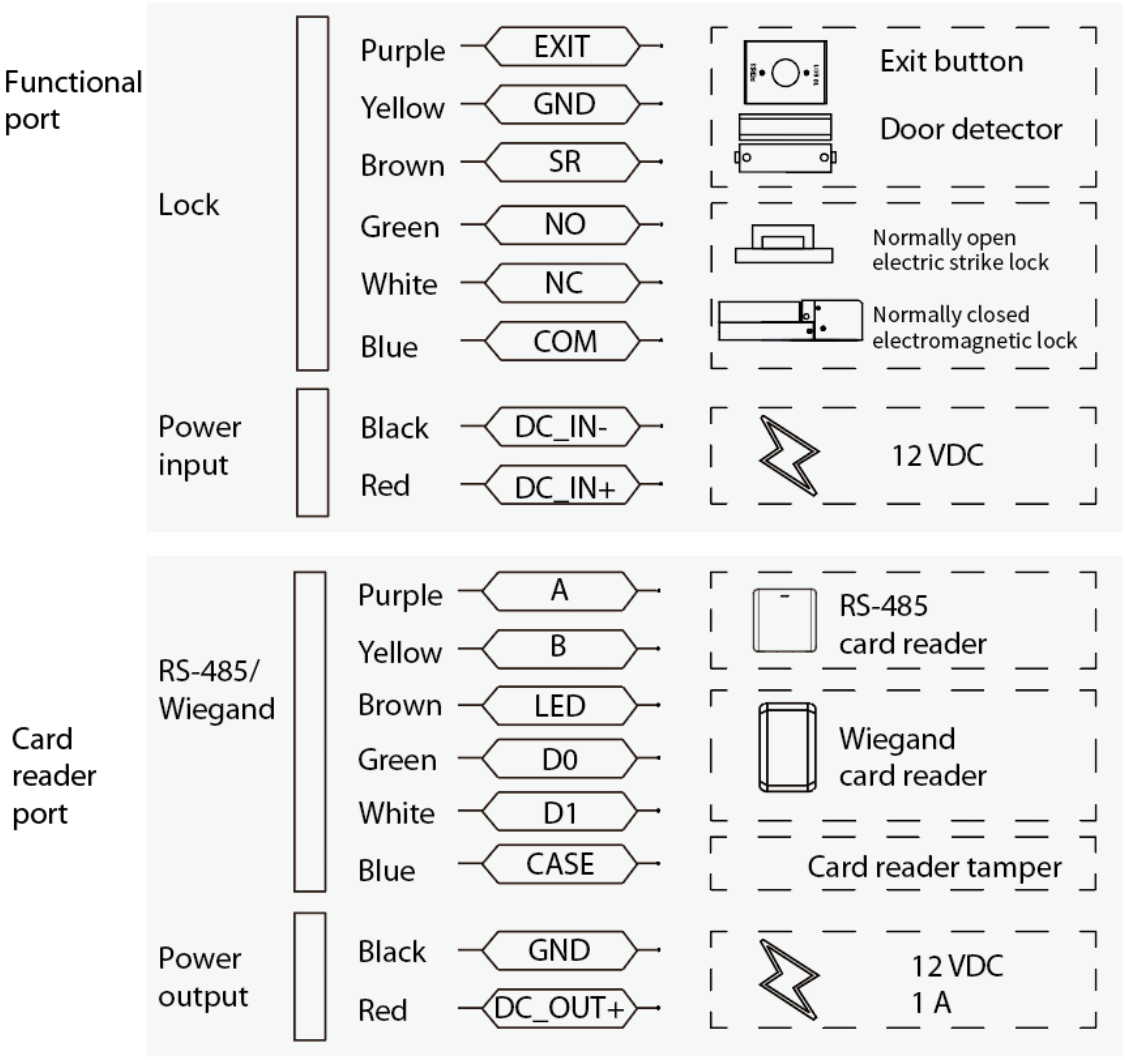
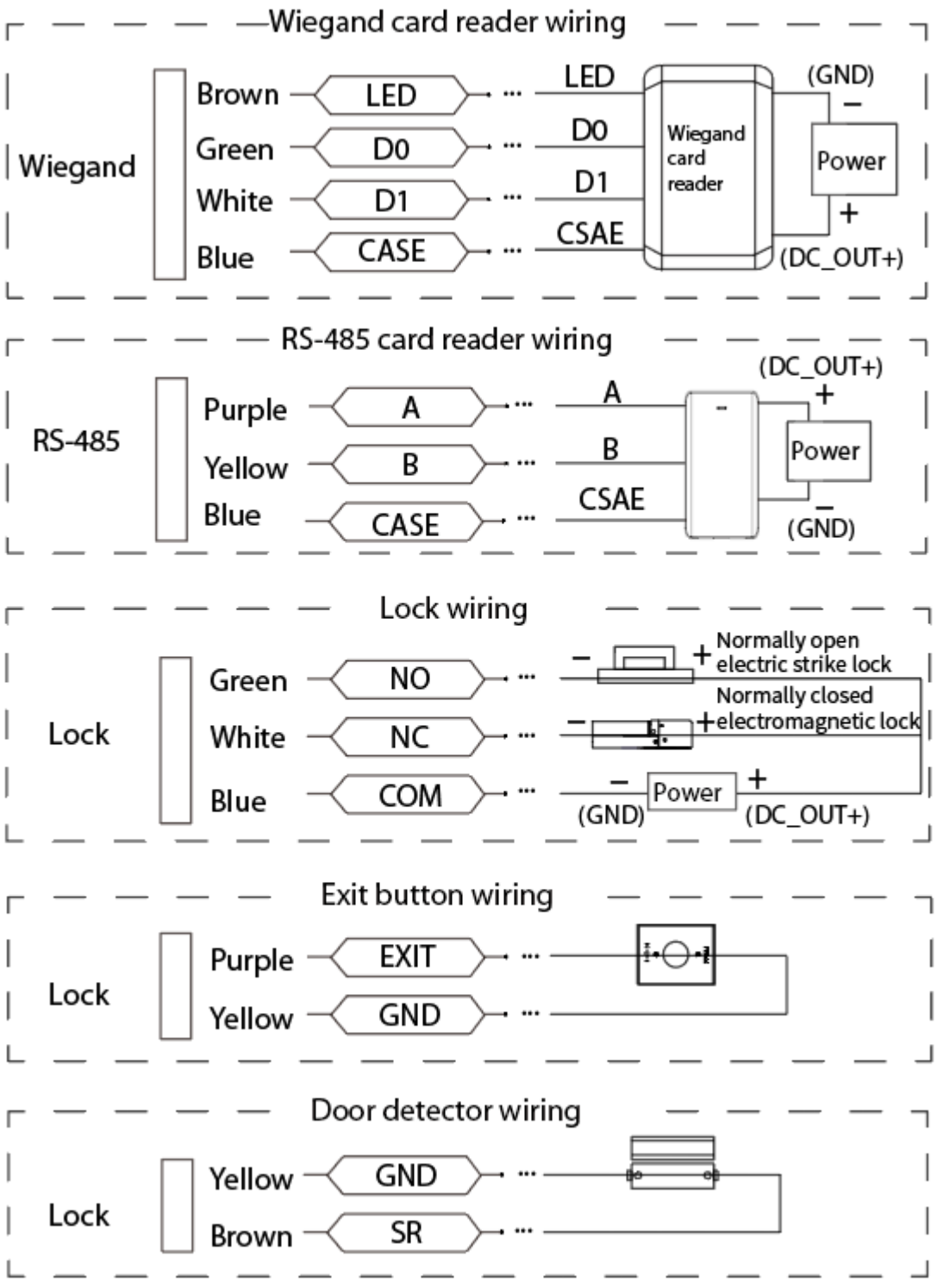


Figure 2-5 Wiring



The lock can be powered by the access standalone (through DC_OUT+ and GND) or the independent power supply. If the power supply distance exceeds 30 m, we recommend you use the independent power supply.

Figure 2-6 Power wiring

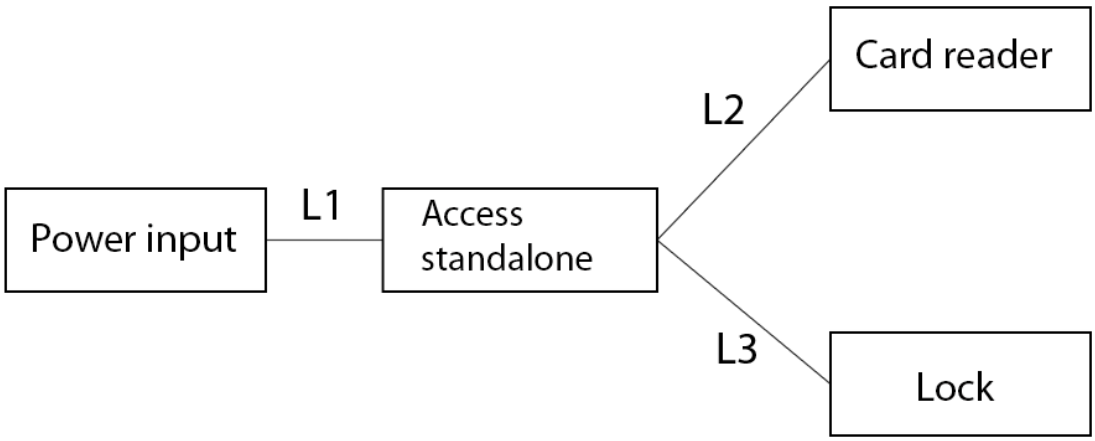


Table 2-1 Cable specification description

No.	Name	Recommended Model and Specification	Recommended Max Power Supply Distance (Use RVV ×1.0 cable, and the impedance within 100 meters ≤ 2 Ω
L1	Power Cord	RVV2 × 1.0	• Access standalone: The distance of L1 should be less than 100 m. • Access standalone and card reader: The distance of L1 and L2 should be less than 50 m. • Access standalone and lock: The distance of L1 and L3 should be less than 30 m. • Access standalone and lock and card reader: The distance of L1 and L2 should be less than 25 m. The distance of L1 and L3 should be less than 25 m.
L2	Card Reader Cable	RVV2 × 1.0, RVV4 × 1.0 or CAT5E network cable	
L3	Lock Cable		

- 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 1000 mA. The selected lock should support wide voltage operation, with the lowest operating voltage not exceeding 10 V.
- The wiring distance of L1, L2, and L3 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, L2 and L3 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.

2.3 Installation

Procedure

Step 1 Loosen the screw at the bottom of the Device, and then remove the installation rear panel.

Step 2 According the holes' positions of the installation rear panel, drill 3 holes in the wall.

The wiring slot in the wall is required for in-wall wiring.

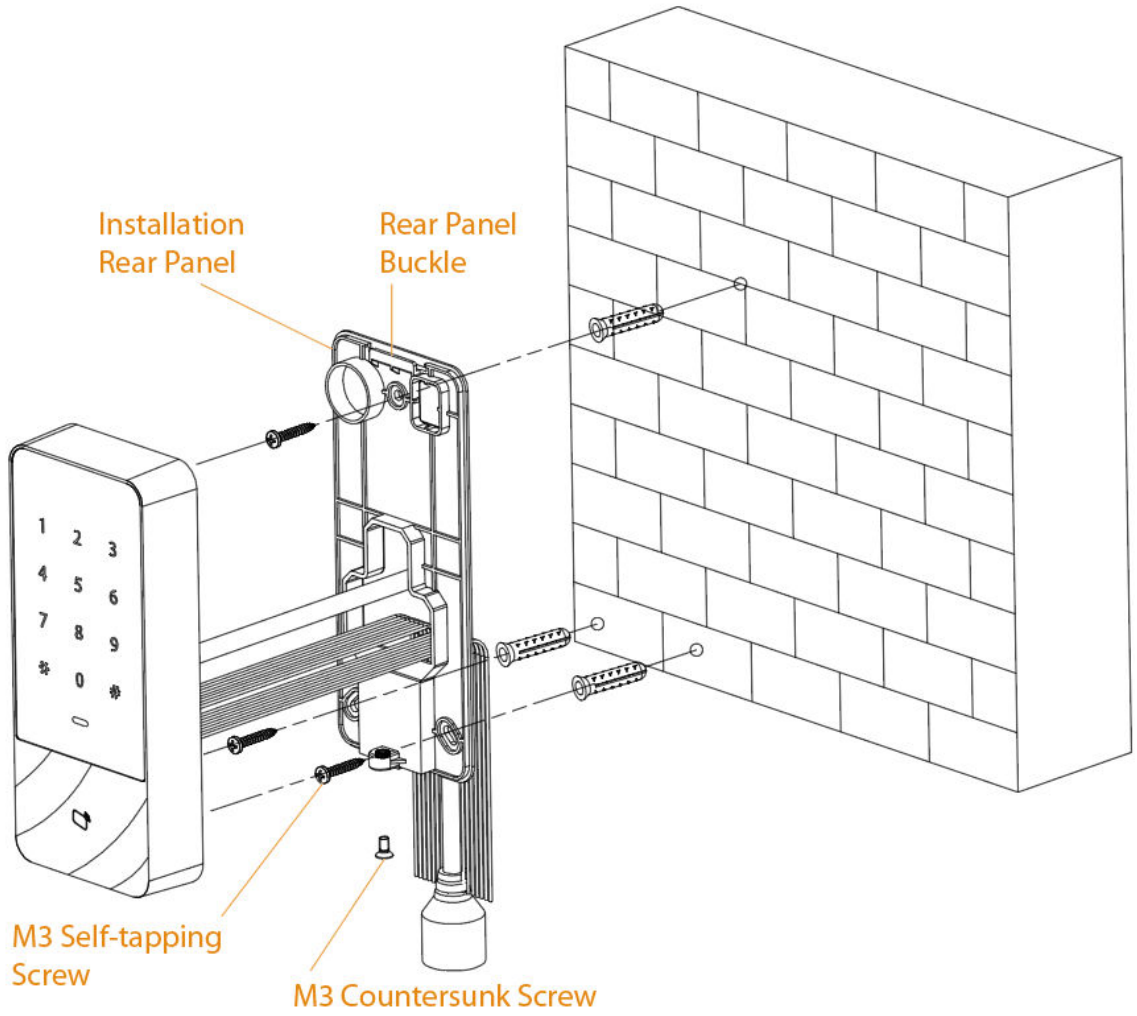
Step 3 Insert the cables to the ports on the Device, and then thread the cables through the installation rear panel. For details on wiring, see "2.2 Wiring".

Step 4 Attach the installation rear panel to the wall using 3 M3 self-tapping screws.

Step 5 Attach the Device to the installation rear panel.

Step 6 Insert 1 screw at the bottom of the Device, and then tighten the screw to finish the installation.

Figure 2-7 Installation



3 Local Operations

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 Wake up the Device, 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.

Related Operations

After you complete the initialization on the Device, you can use it. 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)

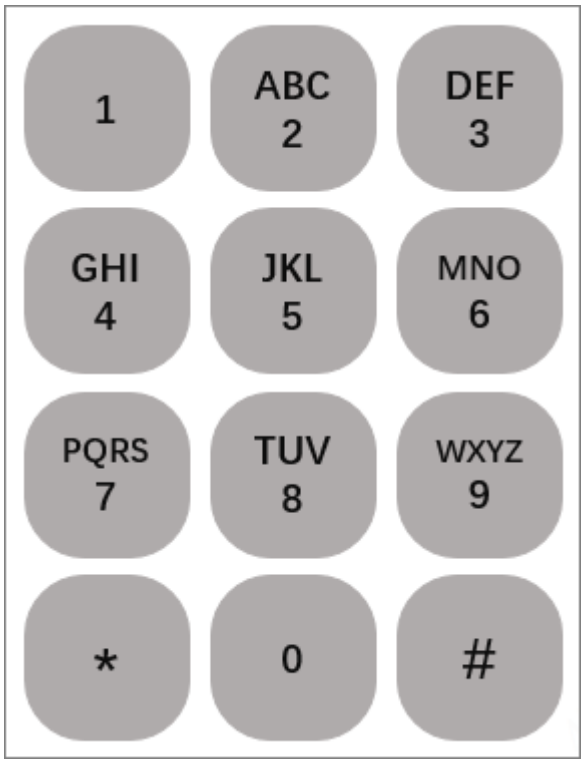


Table 3-1 Conversion example

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

3.2 Main Menu

Entering Main Menu

Wake up the Device, 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.
- After you press the keypad to wake up the Device, the keypad light is blue.
- The keypad light turns off after no operation within 30 seconds.
- When the Device is in the standby mode, if you swipe the card, the keypad light will not turn on.

3.3 User Management

3.3.1 Adding User

Procedure

Step 1 Wake up the Device, 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 **#**.

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

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

- You can press **#** to skip the step if you do not need to add the card.
- You cannot add the existed card.

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

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

The duress password is the password +1. For example, if the user password is 12345, the duress password will be 12346. A duress alarm will be triggered when a duress password is used to unlock the door.

- The password can be 1 to 8 characters in length.
- If you skip the step of adding card, the password is required. Otherwise, you cannot add the user successfully.

Step 6 Repeat Step 3 to Step 5 to add more users.

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

3.3.2 Deleting User

Procedure

Step 1 Wake up the Device, press **#** , enter the administrator password, and then press **#**.

Enter the main menu, and the indicator flashes blue.

Step 2 Press **2** and **#**.

Step 3 Delete a user.

- Swipe the card, and then press **#**.

  If you swipe a card that has not been added, the deletion fails.
- Enter the user ID, and then press **#**.

  If you enter the ID that has not been added, the deletion fails.
- Enter 0000, and then press **#** to delete all users.

After deletion, press * to return to the main menu, and then press * to exit the main menu.

3.4 Configuring Door Unlock Mode

Procedure

Step 1 Wake up the Device, press **#** , enter the administrator password, and then press **#**.

Enter the main menu and the indicator flashes blue.

Step 2 Press **3** and **#**.

Step 3 Select the unlock mode.

- Press **0** and **#** to set unlocking by card.
- Press **1** and **#** to set unlocking by card and user password.

  Swipe the card first. After the Device beeps, enter the password, and then press **#** to open the door.
- Press **2** and **#** to set unlocking by user ID and password.

  Enter the user ID, and then press **#** . After the Device beeps, enter the password, and then press **#** to open the door.
- Press **3** and **#** to set unlocking by card or user ID and password.

  Swipe the card to open the door, or enter the user ID, press **#** , enter the password, and then press **#** to open the door.

Step 4 Press * to exit the main menu.

3.5 Configuring Unlock Duration

The door remains open after a defined time after it unlocks, which allows people to pass through.

Procedure

Step 1 Wake up the Device, press **#** , enter the administrator password, and then press **#**.

Enter the main menu and the indicator flashes blue.

Step 2 Press **4** and **#**.

Step 3 Enter the time, and then press **#**.

The value ranges from 1 second to 600 seconds. The default value is 3 seconds.

Step 4 Press * to exit the main menu.

3.6 Configuring Door Sensor

After the door sensor is enabled, the door timeout alarm is enabled at the same time by default. If the door stays open after the set door timeout period, the buzzer of the Device generates alarms.

Procedure

Step 1 Wake up the Device, press **#** , enter the administrator password, and then press **#**.

Enter the main menu and the indicator flashes blue.

Step 2 Press **5** and **#**.

Step 3 Turn on or turn off the door sensor.

The door sensor is turned off by default.

- Press **0** and **#** to turn off the door sensor.
- Press **1** and **#** to turn on the door sensor.

Step 4 Press * to exit the main menu.

3.7 Password Management

3.7.1 Changing the Administrator Password

To ensure device security, we recommend that you change the administrator password from time to time.

Procedure

Step 1 Wake up the Device, press **#** , enter the administrator password, and then press **#**.

Enter the main menu and the indicator flashes blue.

Step 2 Press **0** and **#**.

Step 3 Enter the new password, and then press **#**.

Step 4 Enter the new password again, and then press **#**.

Step 5 Press * to exit the main menu.

3.7.2 Adding Public Password

Procedure

Step 1 Wake up the Device, press **#** , enter the administrator password, and then press **#**.

Enter the main menu and the indicator flashes blue.

Step 2 Press **6** and **#**.

Step 3 Enter the public password, and then press **#**.

The password can be 1 to 8 characters in length.

You can add up to 500 public passwords. The public password must be unique.

Step 4 Press * to exit the main menu.

3.7.3 Deleting Public Password

Procedure

Step 1 Wake up the Device, press **#** , enter the administrator password, and then press **#**.

Enter the main menu and the indicator flashes blue.

Step 2 Press **7** and **#**.

Step 3 Enter the public password and press **#**.

Repeat this step to delete other public passwords.

Step 4 Press ***** to exit the main menu.

3.8 Main Card Management

3.8.1 Adding Main Card

After adding the main card, you can quickly add and delete other user cards through the main card.

Background Information

The main card cannot be used to unlock the door.

Procedure

Step 1 Wake up the Device, press **#** , enter the administrator password, and then press **#**.

Enter the main menu and the indicator flashes blue.

Step 2 Press **8** and **#**.

Step 3 Swipe the card, and then press **#**.

- If the indicator flashes green, and the Device beeps, it means the card is added as the main card.
- If the indicator flashes red, and the Device beeps, it means you fail to add the card as the main card.

- User cards that have been added can also be set as main card.
- If a user card is set to main card, it will not be able to unlock the door.
- Only supports one main card. If a new main card is added, the old main card will be overwritten.

Step 4 Press ***** to exit the main menu.

3.8.2 Deleting Main Card

Procedure

Step 1 Wake up the Device, press **#** , enter the administrator password, and then press **#**.

Enter the main menu, and the indicator flashes blue.

Step 2 Press **9** and **#**.

Step 3 Swipe the card, and the press **#**.

Step 4 Press ***** to exit the main menu.

3.8.3 Managing User Cards through Main Card

If no operation is performed in 3 seconds after you swipe the main card, the Device enters the main card mode, and the Device will determine the corresponding function according to the swipe times of the main card. In the main card mode, the indicator flashes red and blue alternately, and if there is no operation for 10 seconds or you swipe the main card again for one time, it returns to the standby status.

- Add user card: Swipe the main card once, and then swipe the user card to add it. User cards can be added continuously.
- Delete the user card: Swipe the main card twice, and then swipe the user card to delete it. User cards can be deleted continuously.
- Clear all user cards: Swipe the main card 5 times in a row.

3.9 Configuring Door Timeout Period

After the door sensor is enabled, if the door stays open after the set time, the buzzer of the Device will give an alarm.

Procedure

Step 1 Wake up the Device, press **#** , enter the administrator password, and then press **#**.

Enter the main menu and the indicator flashes blue.

Step 2 Press **10** and **#**.

Step 3 Enter the door timeout period, and then press **#**.

The value range is from 1 second to 9999 seconds. The default value is 60 seconds.

Step 4 Press ***** to exit the main menu.

3.10 Restoring to Factory Settings

Procedure

Step 1 Wake up the Device, press **#** , enter the administrator password, and then press **#**.

Enter the main menu, and the indicator flashes blue.

Step 2 Press **11** and **#**.

Step 3 Restore the Device to factory settings.

- Press **00** and **#** to restore factory settings (retain user information).

  Restore the configurations to the factory settings except for user information, logs, public passwords and IP address.
- Press **000** and **#** to restore factory settings (restore all information).

  Restore the configurations to the factory settings except for IP address.

3.11 Configuring Working Modes

Configure the working mode for the Device according to its actual function. The Device has 2 working modes. If the Device is connected to other recognition devices, it works as the access

controller, and the working mode is **Access Controller** . If the Device works as the recognition device, and connects to other controllers, configure the working mode as **Card Reader**.

Procedure

Step 1 Wake up the Device, press **#** , enter the administrator password, and then press **#**.

Enter the main menu and the indicator flashes blue.

Step 2 Press **12** and **#**.

Step 3 Select the working mode.

- Access controller mode: Press **0** and **#**.
- Card reader: Press **1** and **#**.

◇ The cables connection when the Device is in the card reader mode should be the same as the connection of the card reader.

◇ As the tamper alarm output, the COM and NC cables of the lock port connect to CASE and GND cables of the access controller respectively.

Step 4 Press * to exit the main menu.

3.12 Configuring Block NFC Cards

After the function is enabled, people cannot use the copied NFC cards to open the door.

Background Information

- This function is available on select models of devices.
- This function is available on select models of mobile phones.

Procedure

Step 1 Wake up the Device, press **#** , enter the administrator password, and then press **#**.

Enter the main menu and the indicator flashes blue.

Step 2 Press **13** and **#**.

Step 3 Turn on or turn off the function.

If is turned off by default.

- Turn off: Press **0** and **#**.
- Turn on: Press **1** and **#**.

Step 4 Press * to exit the main menu.

3.13 Initializing Admin Password

If you forget the admin password, you can restore the Device to the factory settings using 2 methods.

After restoring, configure the administrator password again.

- Restore to factory settings (except for user information): Power on the Device. After it beeps once, within 30 seconds, press * + **0** + *.

  Restore the configurations to the factory settings except for user information, logs, public passwords and IP address.

- Restore to factory settings: Power on the Device. After it beeps once, within 30 seconds, press * + **0** + **0** + **0** + **0** + * to restore all the configurations, including IP address to factory settings.

3.14 Unlocking the Door

3.14.1 Unlocking by Card

Swipe the user card to unlock the door.

If a user card is set to main card, it will not be able to unlock the door.

3.14.2 Unlocking by Card and Password

If you set the unlock mode to **Card + Password** , swipe the user card and enter the user password, and then press **#** to unlock the door.

3.14.3 Unlocking by User ID and Password

If you set the unlock mode to **User ID + Password** , enter the user ID, press **#**, enter the user password, and then press **#** to unlock the door.

3.14.4 Unlocking by Card or User ID and Password

If you set the unlock mode to **Card or User ID and Password** , swipe the user card to unlock the door, or enter the user ID, press **#**, enter the user password, and then press **#** to unlock the door.

3.14.5 Unlocking through Public Password

Enter the public password, and then press **#** to open the door. For details on how to set public passwords, see "3.7.2 Adding Public Password".

Public password can be used to unlock the door in any unlock modes.

4 Smart PSS Lite Configuration

This section introduces how to manage and configure the device through Smart PSS Lite. For details, see the user's manual of Smart PSS Lite.

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

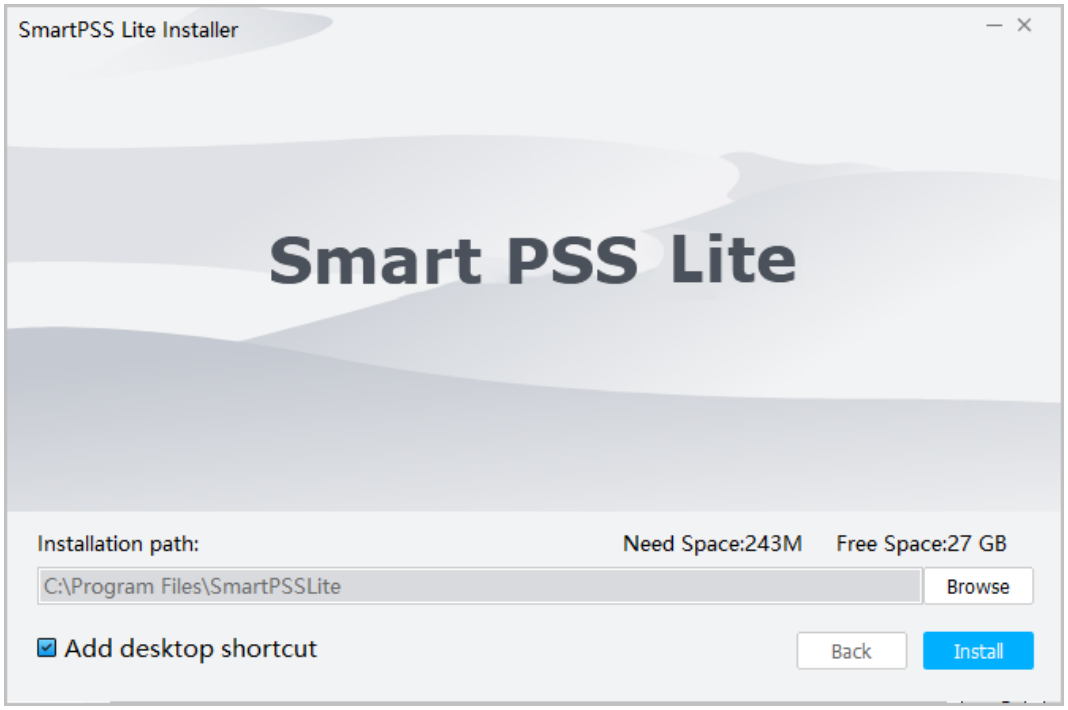
Step 1 Double-click SmartPSSLite.exe.

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**.

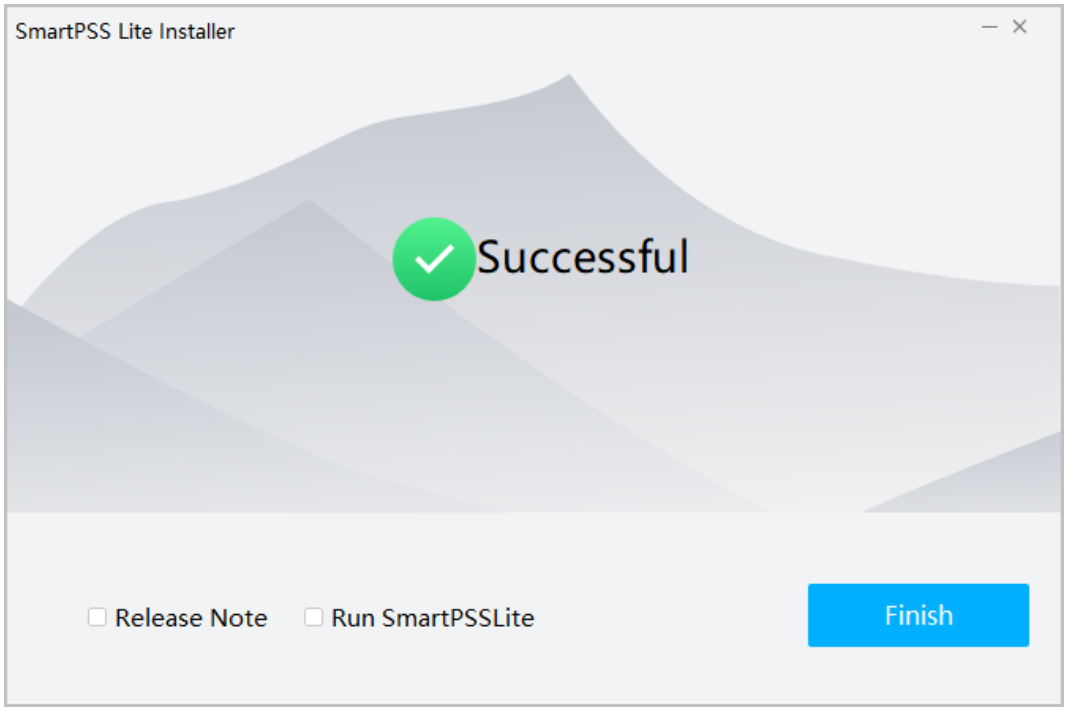
Figure 4-2 Select installation path



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

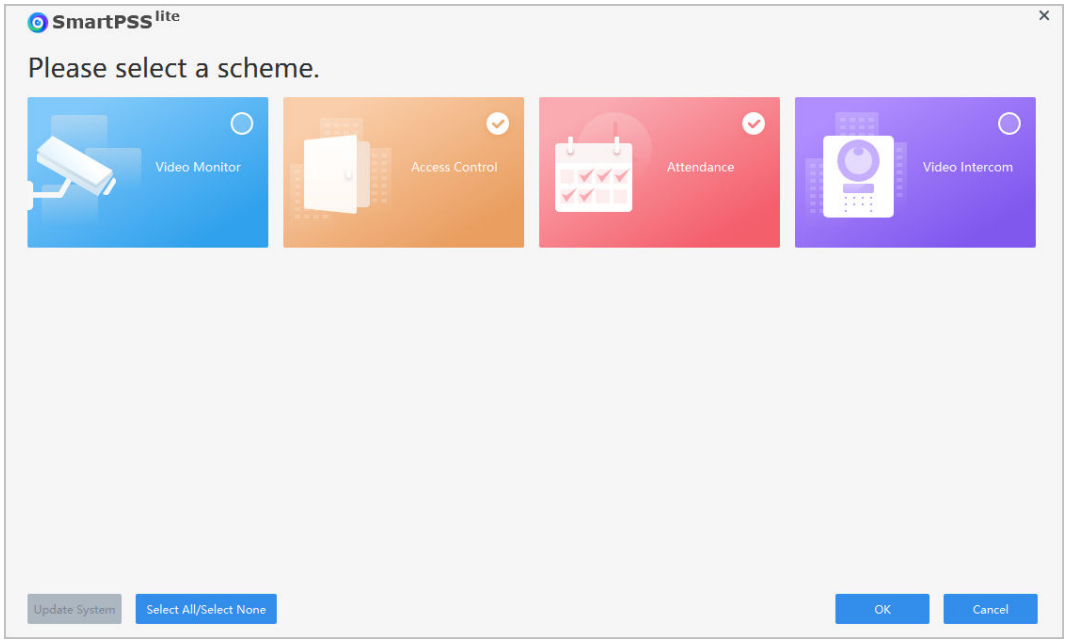
Select **Run SmartPSSLite** to start SmartPSS Lite.

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

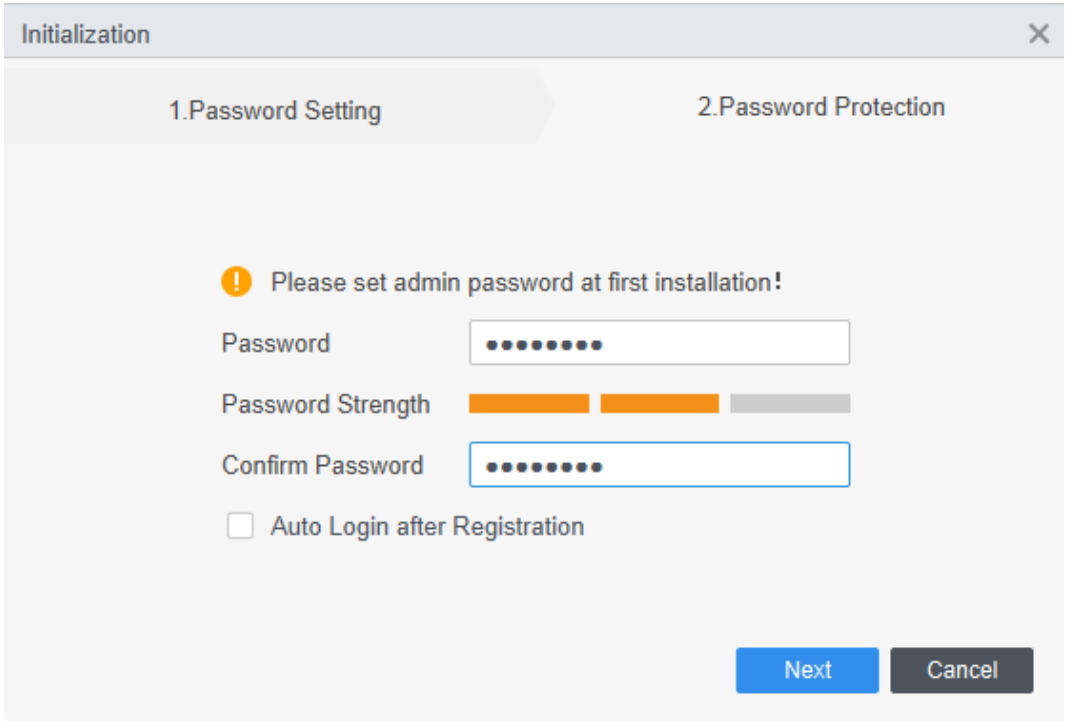
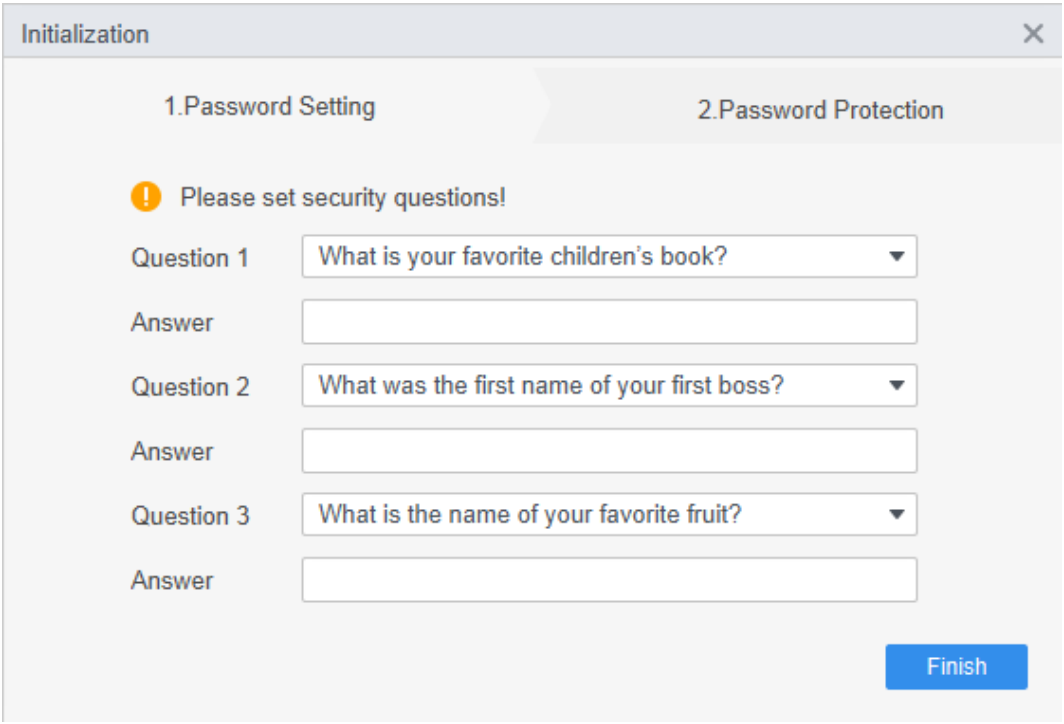


Table 4-1 Initialization parameters

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 Adding Devices

There are several methods available to add devices.

- Automatically search
- Manually adding
- Import in batches

4.3.1 Adding Device by Searching

You can add multiple devices by searching for them on the current network segment or other network segments.

Background Information

We recommend you add devices through searching when want to add multiple devices that are on the same network segment, or when you want to add devices with a known network segment but you do not know the exact IP address of the devices.

Procedure

Step 1 On the home page, click **Devices**.

Step 2 Select a search method.

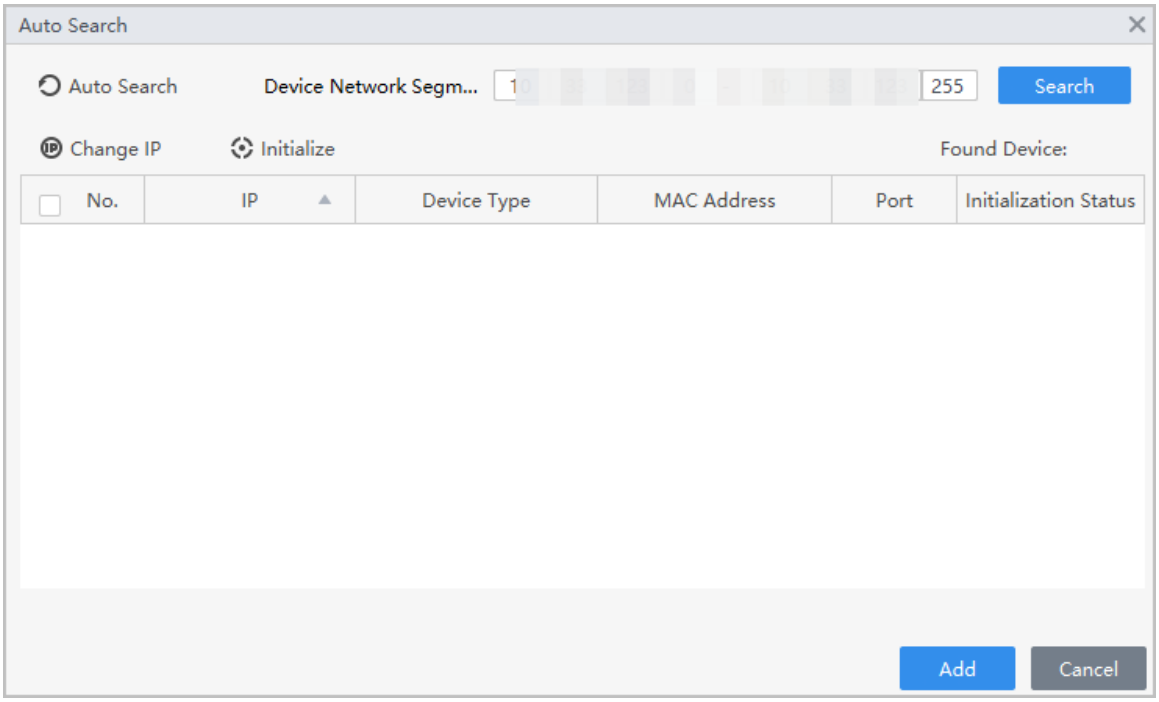
- Auto Search: Enter the username and the password of the device. The system will automatically search for devices that are on the same network to your computer.
- Device Network Segment: Enter the username and the password of the device, and then define the start IP and the end IP. The system will automatically search for devices in this IP range.

Step 3 Click **Auto Search**.

Step 4 Enter a IP range, and then click **Search**.

The system automatically searches for devices in this IP range. You can also click **Auto Search** to automatically search for devices on the same network your computer is connected to.

Figure 4-7 Search for devices



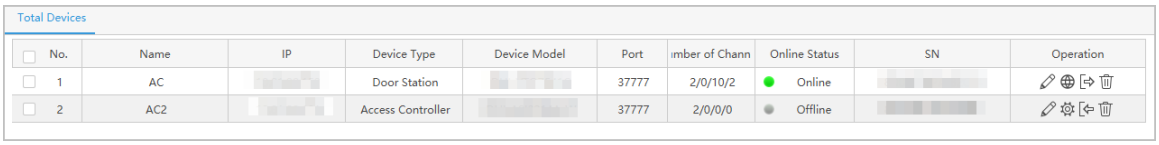
Step 5 Select devices, and then click **Add**.

Step 6 Enter the login username and password of the selected devices, and then click **OK**.

Step 7 Enter the login user name and password, and then click **OK**.

The devices will be added to the platform.

Figure 4-8 Added devices



- : Change the information of the device.
- : Goes to the **Device Config** module in the platform.
- : Goes to the webpage of the device.
- : Log out of the device, and the status of the device will become **Offline**.
- : Log in to the device, and the status of the device will become **Online**.
- : Delete the device.

Related Operations

- Change IP one by one: Select a device, and then click **Change IP** to change the IP of the device.
- Change IP in batches: Select multiple devices, and then click **Change** to change their IP.

  Enter the start IP, and the system will automatically assign IP to devices through increasing the IP by one based on the start IP. For example, if the start IP is 10.XX.XXX.52, and the following IP of devices will be 10.XX.XXX.53, 10.XX.XXX.54, and more.
- Initialize devices: Click **Initialize** to initialize devices.

  Only support activating devices which are on the same network segment to your computer.

  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 4-9 E.161 (T9 keypad)

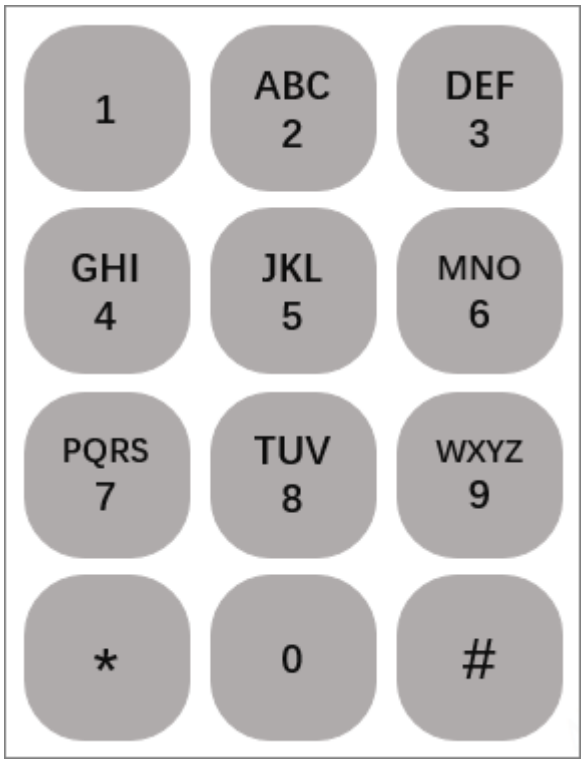


Table 4-2 Conversion example

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

4.3.2 Adding Device One by One

If you already know the IP address of a device, you can manually add it to the platform.

Procedure

Step 1 On the home page, click **Devices**.

Step 2 Click **Add**, and then enter the device information.

Figure 4-10 Add devices

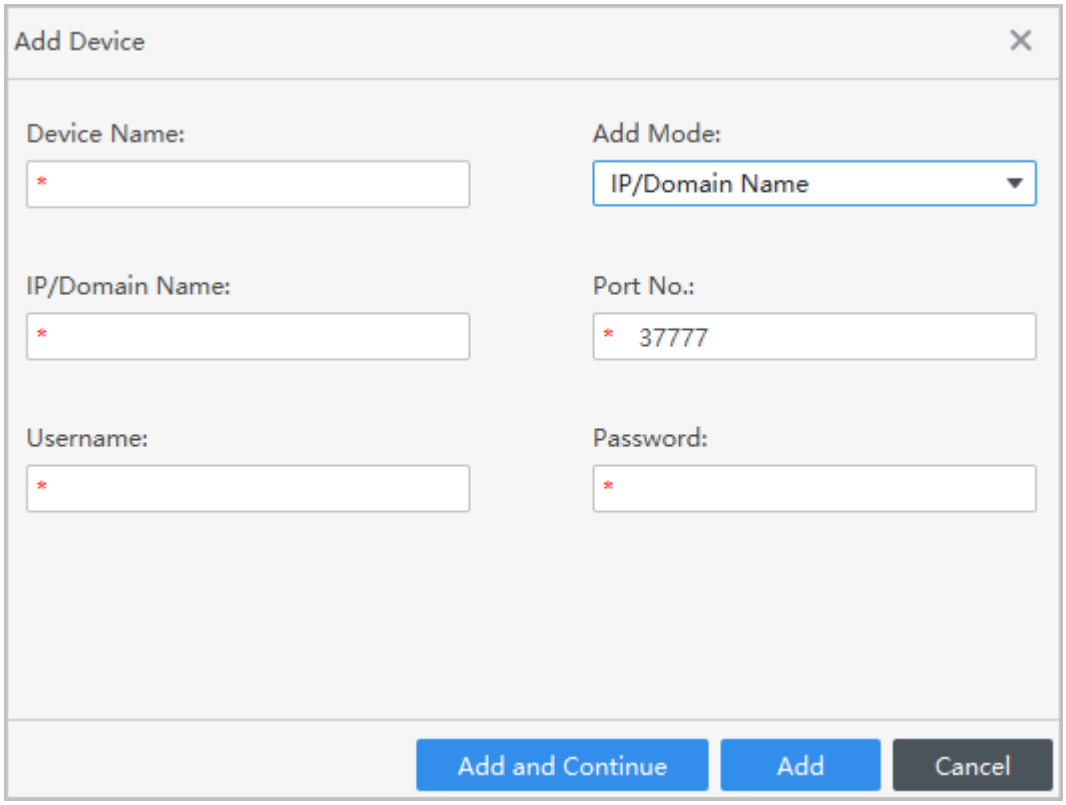


Table 4-3 Parameters of IP adding

Parameter	Description
Device Name	The name of the device.
Add Mode	• IP/Domain Name: Add devices through IP Address. • SN (Available on devices that support P2P): Add devices through their serial number.
IP/Domain Name	Enter the IP address or domain name of the device.
Port No.	Enter the port number (80 by default).
Username	Enter the username and the password of the device.
Password	

Step 3 Click **Add**.

You can also click **Add and Continue** to add more devices.

4.3.3 Importing Device in Batches

You can export the device information, and then import it to another platform to add them in batches. We recommend you add devices by importing them when the devices are not on the same network segment.

Prerequisites

A .xml file of device information was exported. For details, see the corresponding user's manual.

Procedure

Step 1 On the home page, click **Devices**.

Step 2 Click **Import** to import the file the platform.

Devices will be logged in automatically after adding.

4.4 User Management

Add users, assign cards to them, and configure their access permissions.

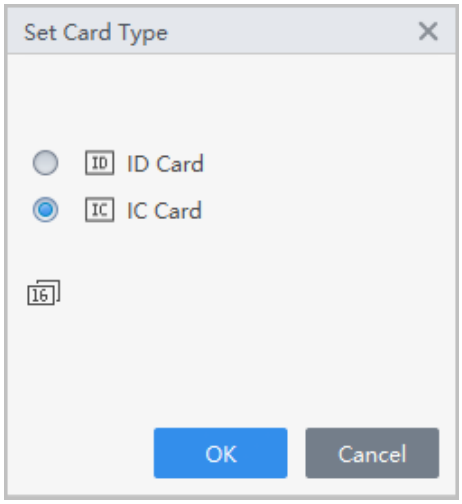
4.4.1 Setting Card Type

Select **Person** > **Person Management**, and then **Card Type**.

Before issuing card, set card type first. For example, if the issued card is ID card, select type as ID card.

The system uses hexadecimal card number by default. Click to change it to decimal card number.

Figure 4-11 Set card type



4.4.2 Configuring Card Type

Set the card type before you assign cards to users. For example, if the assigned card is an ID card, set card type to ID card.

Procedure

Step 1 Log in to Smart PSS Lite.

Step 2 Click **Access Solution** > **Personnel Manager** > **User**.

Step 3 On the **Card Issuing Type** and then select a card type.

Make sure that the card type is same to the actually assigned card; otherwise, the card number cannot be read.

Step 4 Click **OK**.

4.4.3 Adding Users

4.4.3.1 Adding Personnel One by One

Procedure

Step 1 Select **Person** > **Person Management**, and then click **Add**.

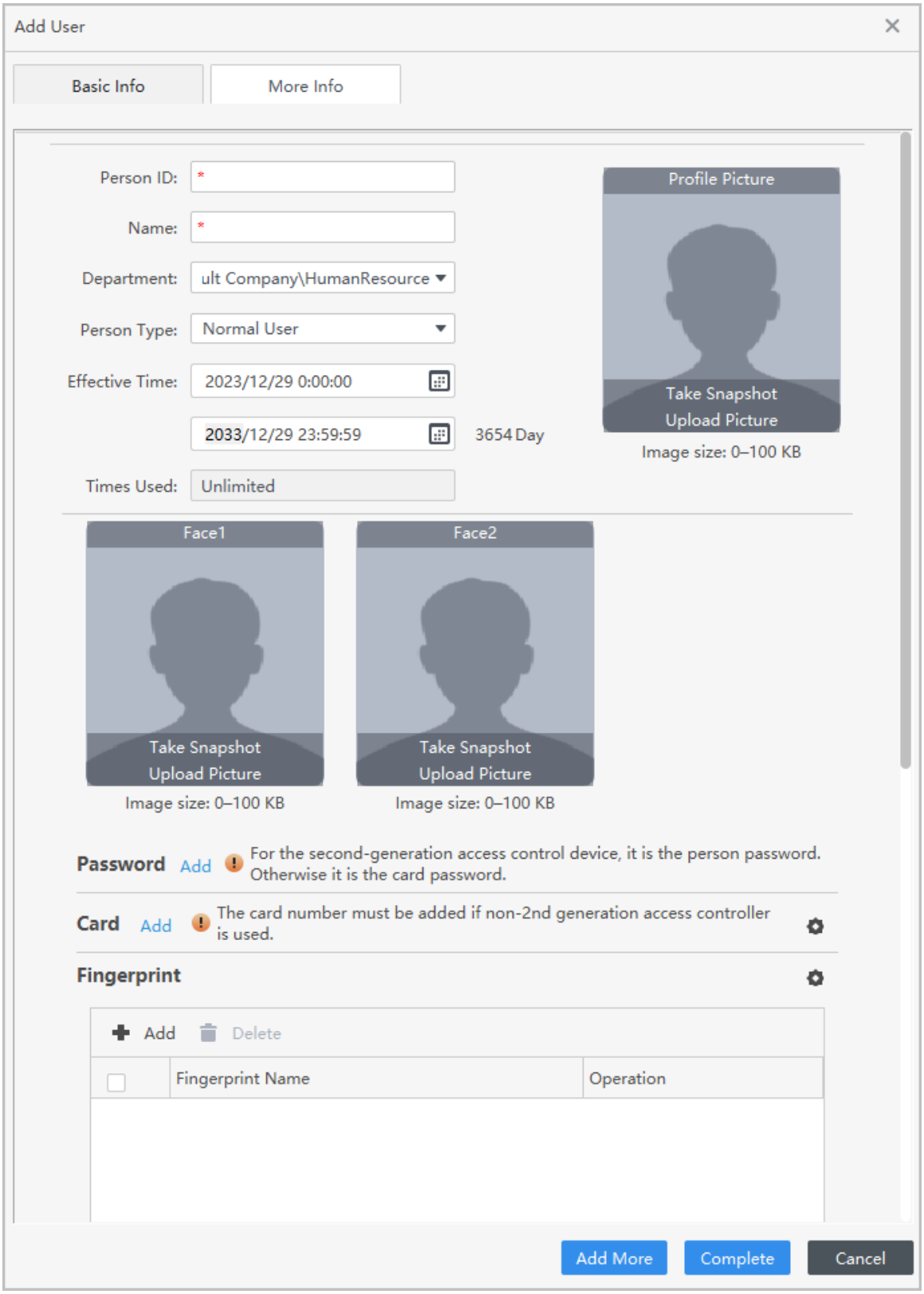
Step 2 Enter basic information of person.

1. Select **Basic Info**.
2. Add basic information of personnel.
3. Take snapshot or upload picture, and then click **Finish**.
4. Configure identity verification methods.
   - Set password

     Click **Add** to add the password. For second-generation access controllers, set person passwords; for other devices, set card passwords. New passwords must consist of 6-8 digits.
   - Configure card
     a. Click to select **Device** or **Card issuer** as card reader.
     b. Add card.
     c. After adding, you can select the card as main card or duress card, or replace the card with a new one, or delete the card.
     d. Click to display the QR code of the card.

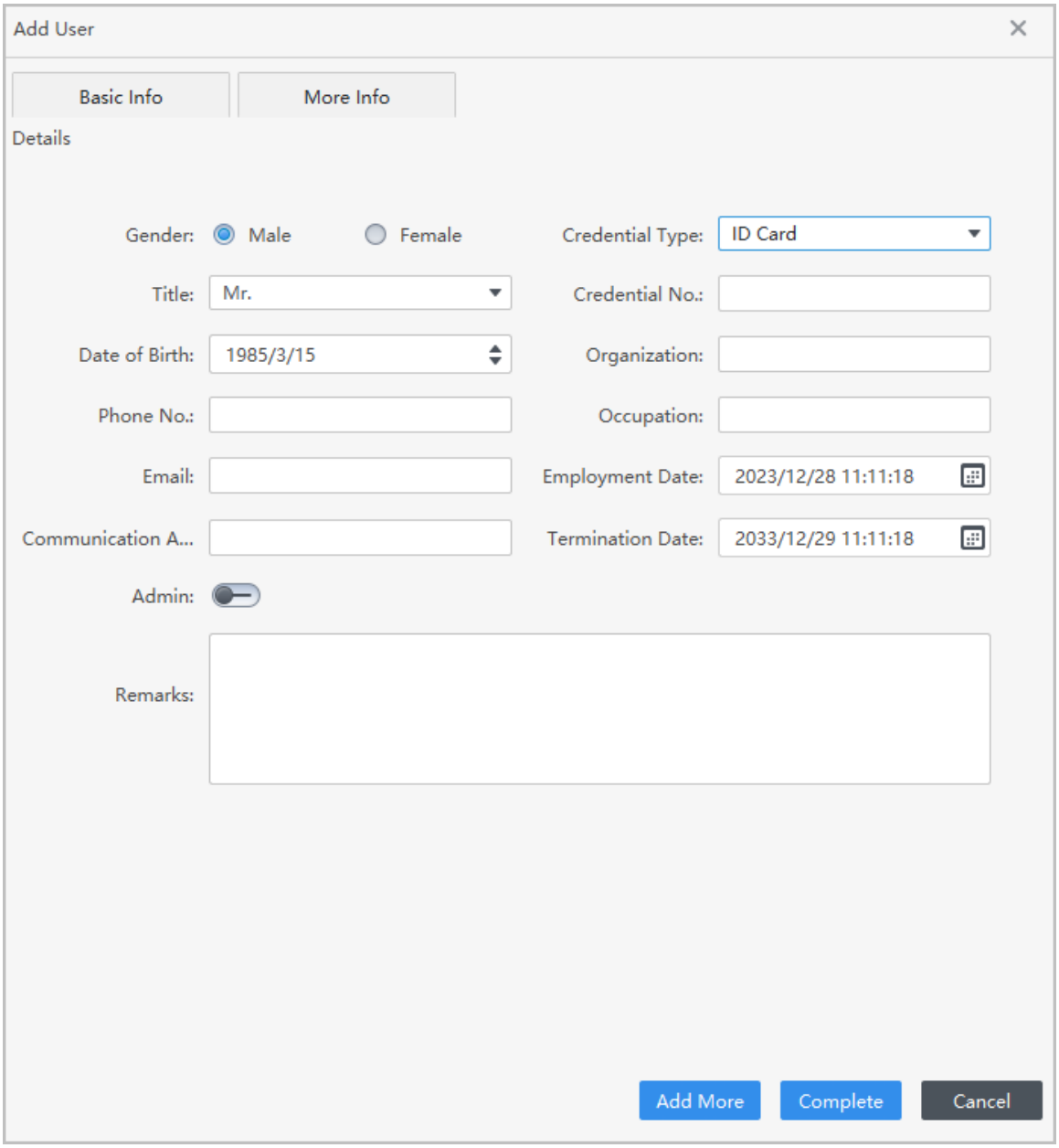
     Only 8-digit card number in hexadecimal mode can display the QR code of the card.
   - Configure fingerprint
     a. Click to select **Device** or **Fingerprint Scanner** as the fingerprint collector.
     b. Add fingerprint. Select **Add** > **Add Fingerprint**, and then press finger on the scanner for three times continuously.
   - Configure feature codes
     a. Click , and then select a device.
     b. Click **Extract**, and then the device will extract the features of the face.

Figure 4-12 Add basic information



Step 3 Click **More Info** tab to add extended information of the staff, and then click **Complete**.

Figure 4-13 Add more information



Step 4 Click **Complete**.

After completing adding, you can click to modify information or add details in the list of person.

Related Operations

- Click to modify information or add details in the list of staff.
- Click to delete all information of the person.
- Click to freeze the card, and then the card cannot be used normally.

4.4.3.2 Adding Personnel in Batches

Procedure

Step 1 Select **Person** > **Person Management**, and then click **Batch Add**.

Step 2 Select the device type, set the start number, number of card.

Step 3 Set the department, and the effective time and expiration time of card.

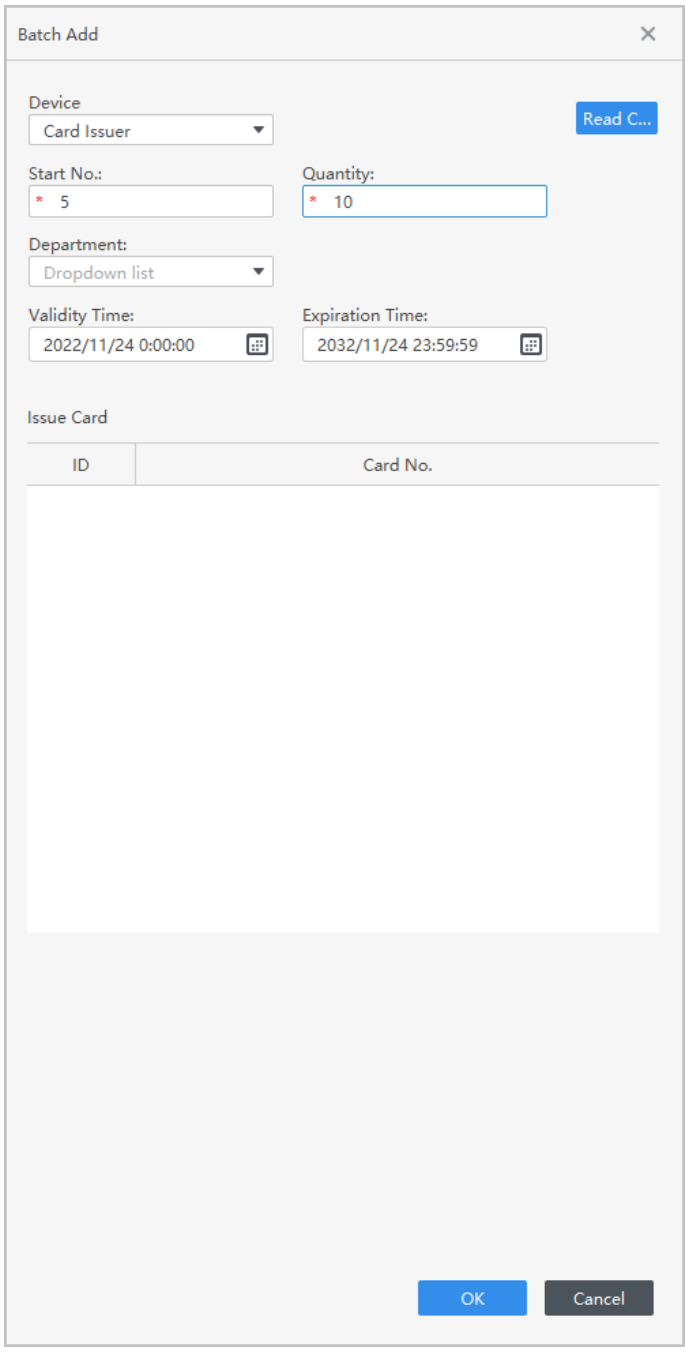
Step 4 Click **Read Card No.**.

Step 5 Place cards on the card issuer or the card reader.

The card number will be read automatically or filled in automatically.

Step 6 Click **OK**.

Figure 4-14 Add personnel in batches



4.4.4 Assigning Access Permissions

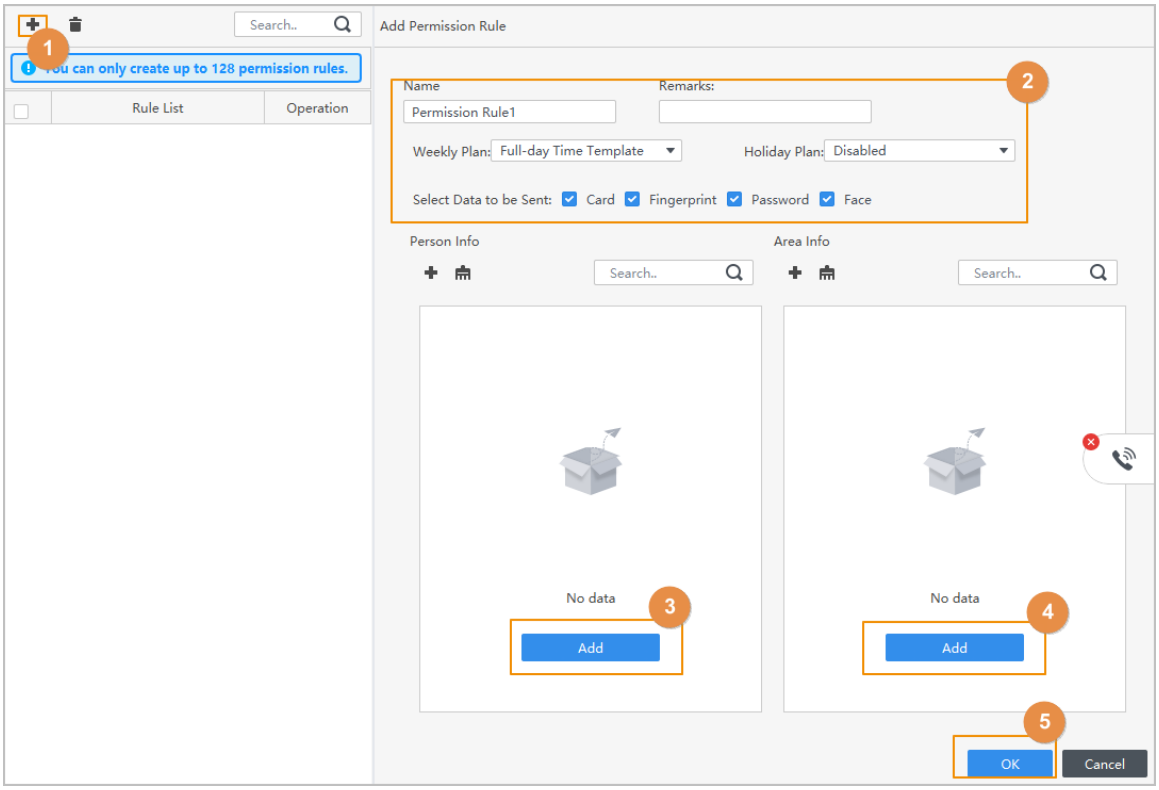
The method to configure permission for department and for personnel is similar, and here uses department as an example.

Procedure

Step 1 Select **Access Control Config** > **Permission Settings**.

Step 2 Click ➕ to add a permission rule.

Figure 4-15 Assign permissions rules



Step 3 Enter the name of the permission rule, select the time plan and unlock methods.

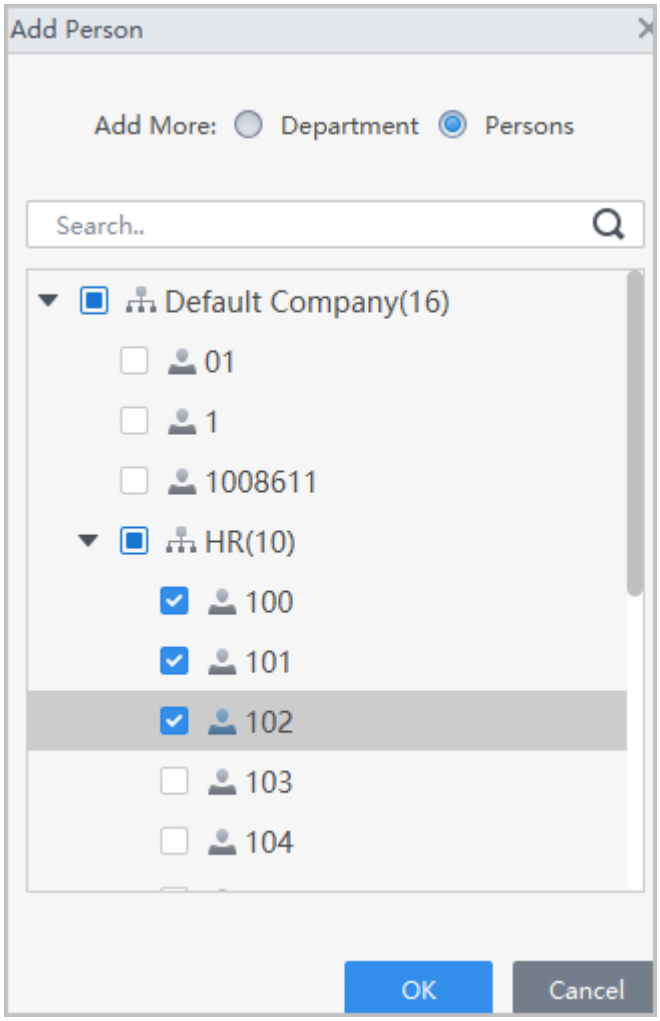
Step 4 In the **Person Info** area, click **Add** to select personnel, and then click **OK**.

You can select personnel on the department or individual users.

- Dept: All personnel in the department will be assigned with access permissions.
- User: Only selected users will be assigned with access permissions.

When you want to assign permission to a new person or change access permissions for an existing person, you can simply add the user in a existing department or link them with a existing role, they will be automatically assigned access permissions set for the department or role.

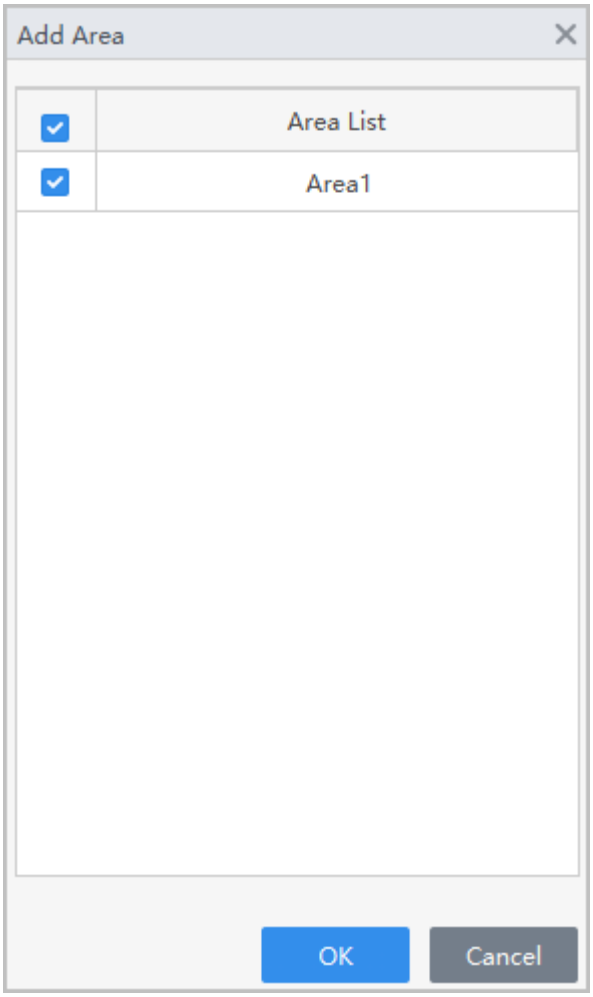
Figure 4-16 Add users



You can click + to create new permission areas. For details on creating permission areas, see the corresponding user's manual.

Step 5 In the **Area Info** , click **Add** to select an area, and then click **OK**.

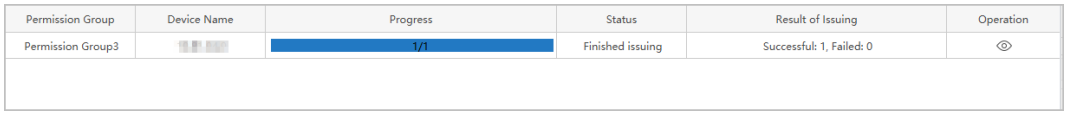
Figure 4-17 Add area



Step 6 Click **OK**.

Step 7 If authorization failed, click in the list to view the possible reason.

Figure 4-18 Authorization progress



4.4.5 Assigning Attendance Permissions

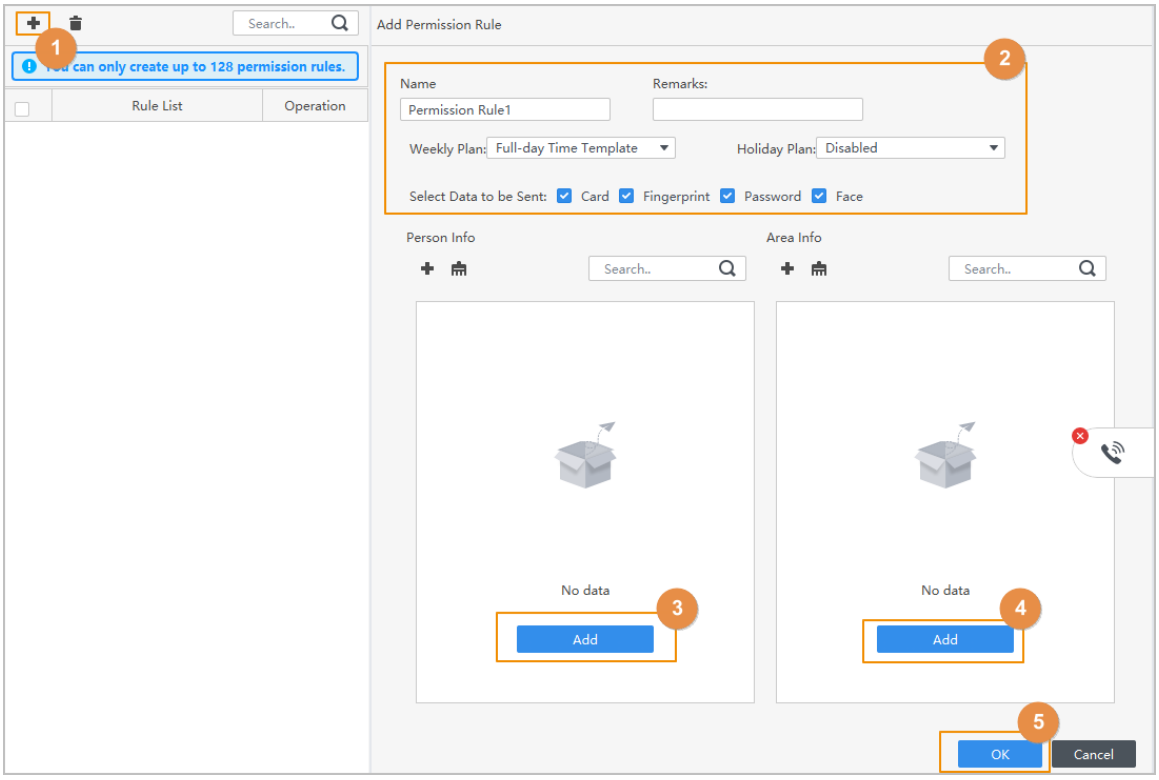
The method to configure permission for department and for personnel is similar, and here uses department as an example.

Procedure

Step 1 Select **Access Control Config** > **Permission Settings**.

Step 2 Click to add a permission rule.

Figure 4-19 Assign permissions rules



Step 3 Enter the name of the permission rule, select the time plan and unlock methods.

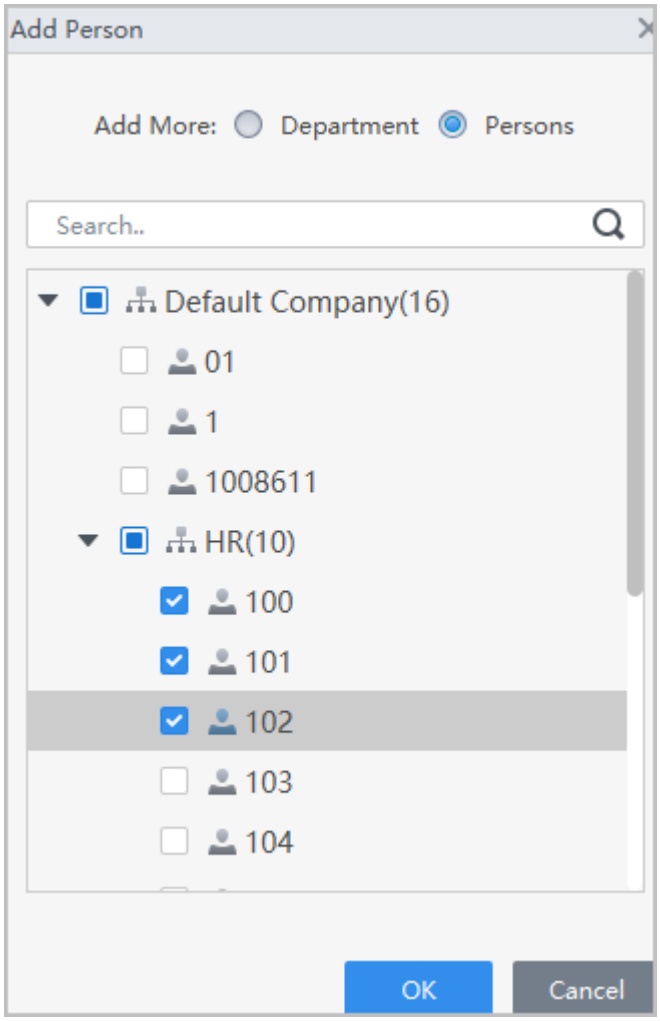
Step 4 In the **Person Info** area, click **Add** to select personnel, and then click **OK**.

You can select personnel on the department or individual users.

- Dept: All personnel in the department will be assigned with access permissions.
- User: Only selected users will be assigned with access permissions.

When you want to assign permission to a new person or change access permissions for an existing person, you can simply add the user in a existing department or link them with a existing role, they will be automatically assigned access permissions set for the department or role.

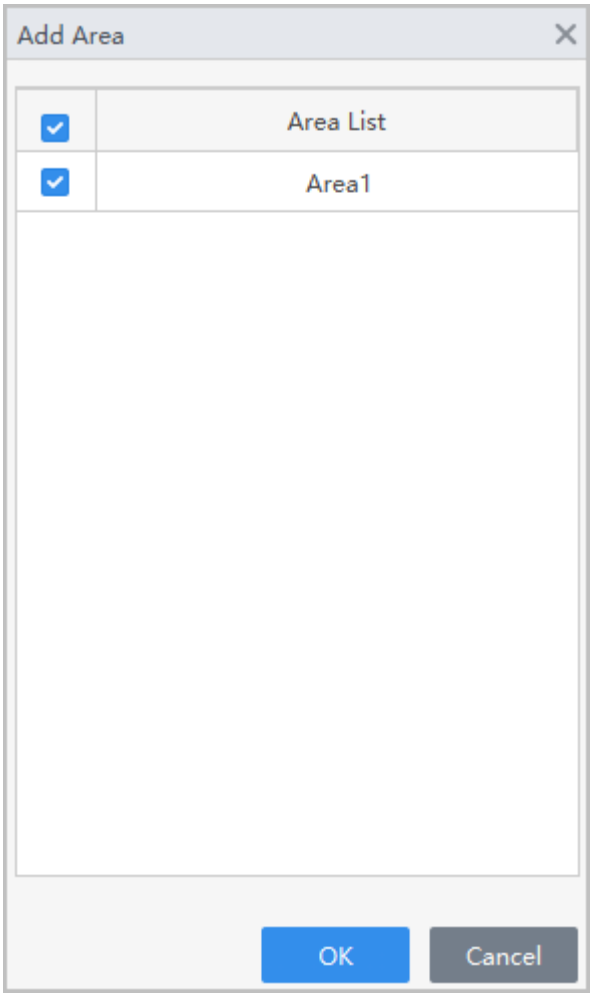
Figure 4-20 Add users



You can click + to create new permission areas. For details on creating permission areas, see the corresponding user's manual.

Step 5 In the **Area Info** , click **Add** to select an area, and then click **OK**.

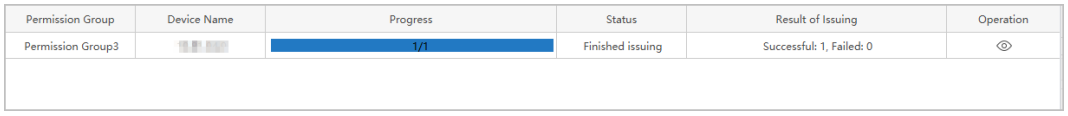
Figure 4-21 Add area



Step 6 Click **OK**.

Step 7 If authorization failed, click in the list to view the possible reason.

Figure 4-22 Authorization progress



4.5 Access Control Monitoring

Procedure

Step 1 Click **Access Control Monitoring** on the home page.

Step 2 Manage the door.

Figure 4-23 Monitor the door

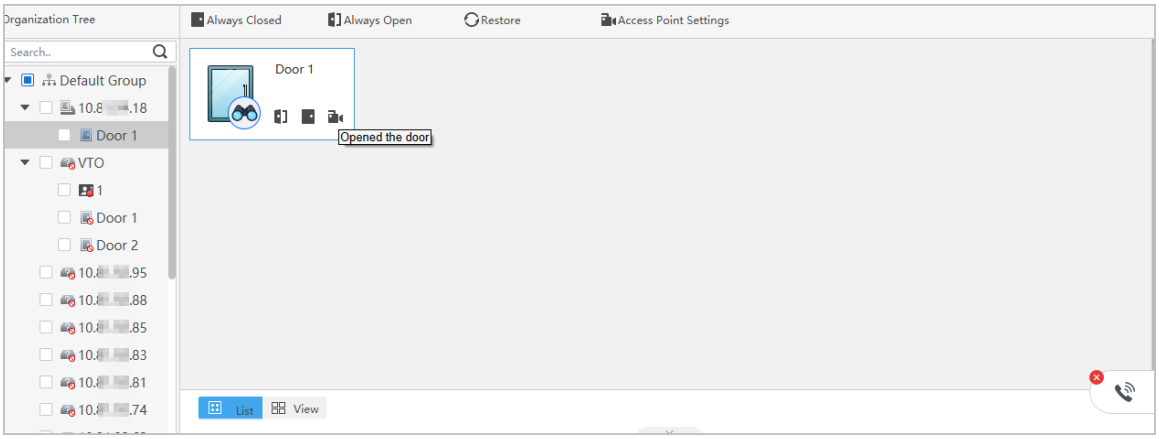


Table 4-4 Parameters description

Function	Description
Remotely control the door	Remotely control the door. ● Method 1: Right-click a door, and then select **Open** or **Close**. ● Method 2: Click or to open or close the door.
	View the video captured by the camera of the access controller or the linked external camera. If you cannot view real-time video, it means that the access control device has no camera and is not connected to an external camera. Please configure an external camera for access controller. For details, see the corresponding user's manual.. If you want to view multiple live videos at the same time, click View, and then drag the access control device in the organization tree to windows, or double-click the access control device in the organization tree.
Always Open	After setting always open or always closed, the door is open or closed all the time and cannot be controlled manually. If you want to manually control the door again, click **Normal** to reset the door status.
Always Closed	
Restore	
Access Point Settings	Set devices (NVR, IPC, IVSS and more) that support target recognition as the access control point. After setting, the door unlock records will be uploaded to the platform.

Step 3 Right-click a access control device to manage the device.

Figure 4-24 Manage the device

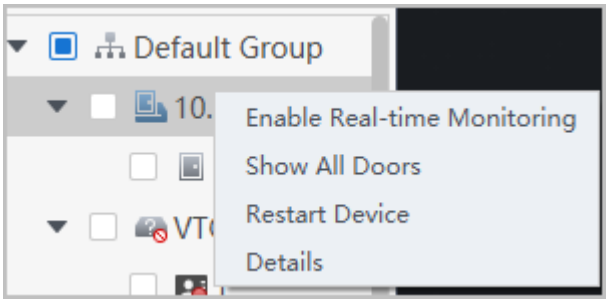


Table 4-5 Parameters description

Parameter	Description
Enable Real-time Monitoring	Start real-time event monitoring.
Show all Doors	Show all doors connected to the access control device.
Restart Device	Restart the access control device.
Details	View the device information, such as version, and more.

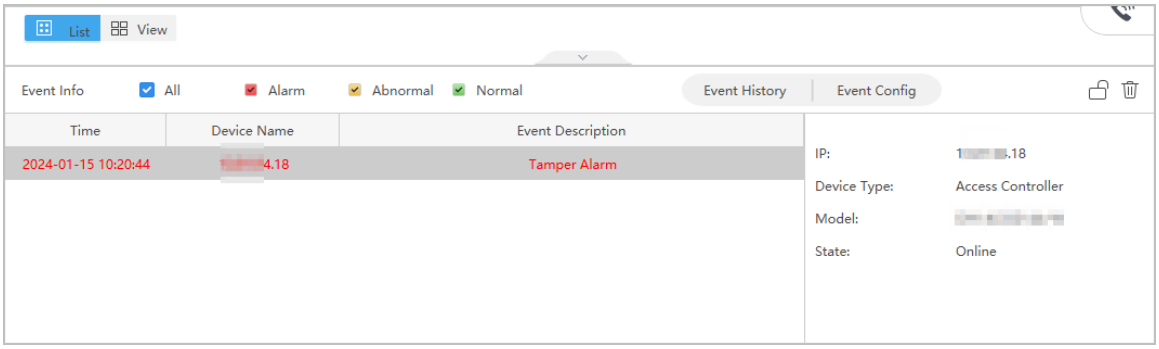
Step 4 View door status on **Event Info** list. For details, see the corresponding user's manual.

Related Operations

Click to open the **Event Info** list.

- View access control information: You can view real-time access information in the **Event Info** list. The information will be cleared after the platform restarts.
- Filter events: Select the event type in the **Event Info** , and the event list displays events of the selected types. For example, select **Alarm**, and the event list only displays alarm events.
- Lock or unlock the event list: Click on the right side of **Event Info** to lock or unlock the event list, and then the real-time events cannot be viewed.
- Delete events: Click on the right side of **Event Info** to clear all events in the event list.
- Click **Event History** to jump to the **Access Control Record** page, and click **Event Config** to jump to the **Event Config** page.

Figure 4-25 Event information



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).