Fingerprint Access Controller

User's Manual

V1.0.2

Foreword

General

This manual introduces the functions and operations of the Face Recognition Access Controller (hereinafter referred to as the "Access Controller"). 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 Date
V1.0.2	Updated the manual.	February 2023
V1.0.1	Updated the wiring.	June 2022
V1.0.0	First release	August 2019

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 Access Controller, hazard prevention, and prevention of property damage. Read carefully before using the Access Controller, and comply with the guidelines when using it.

Transportation Requirement

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

Storage Requirement

Store the Access Controller under allowed humidity and temperature conditions.

Installation Requirements

 WARNING

- Do not connect the power adapter to the Access Controller 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 Access Controller.
- Do not connect the Access Controller to two or more kinds of power supplies, to avoid damage to the Access Controller.
- 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 Access Controller in a place exposed to sunlight or near heat sources.
- Keep the Access Controller away from dampness, dust, and soot.
- Install the Access Controller on a stable surface to prevent it from falling.
- Install the Access Controller 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 Access Controller label.
- The Access Controller is a class I electrical appliance. Make sure that the power supply of the Access Controller 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 Access Controller while the adapter is powered on.
- Operate the Access Controller within the rated range of power input and output.
- Use the Access Controller under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the Access Controller, and make sure that there is no object filled with liquid on the Access Controller to prevent liquid from flowing into it.
- Do not disassemble the Access Controller without professional instruction.
- This product is professional equipment.

Table of Contents

1 General

The metal fingerprint access controller is an access control device that supports card unlock and fingerprint unlock.

1.1 Features

- Zinc alloy front panel.
- 32-bit CPU.
- Support W26\W34 (be compatible with the third party products).
- Support RS-485 and Wiegand protocol.
- Card reading frequency: 13.56MHZ; card reading distance: 1 cm–3 cm; response time less than 0.1 s.
- Contactless card reading, can read Mifare card, read card number of public transportation IC card, bank IC card, and Mifare card.
- Support "watchdog" (a device that protects a system from software or hardware failures).
- Support online upgrade; if online upgrade failed, you can upgrade again
- Support card unlock, fingerprint unlock, and card & fingerprint unlock.
- Buzzer and indicator lights.
- Support tamper alarm.
- Anti-thunder, anti-static, and short-circuit protection function.
- All ports with overcurrent protection and overvoltage protection function.
- Protection: IP65 and IK10.
- Working temperature: -30°C to +50°C.
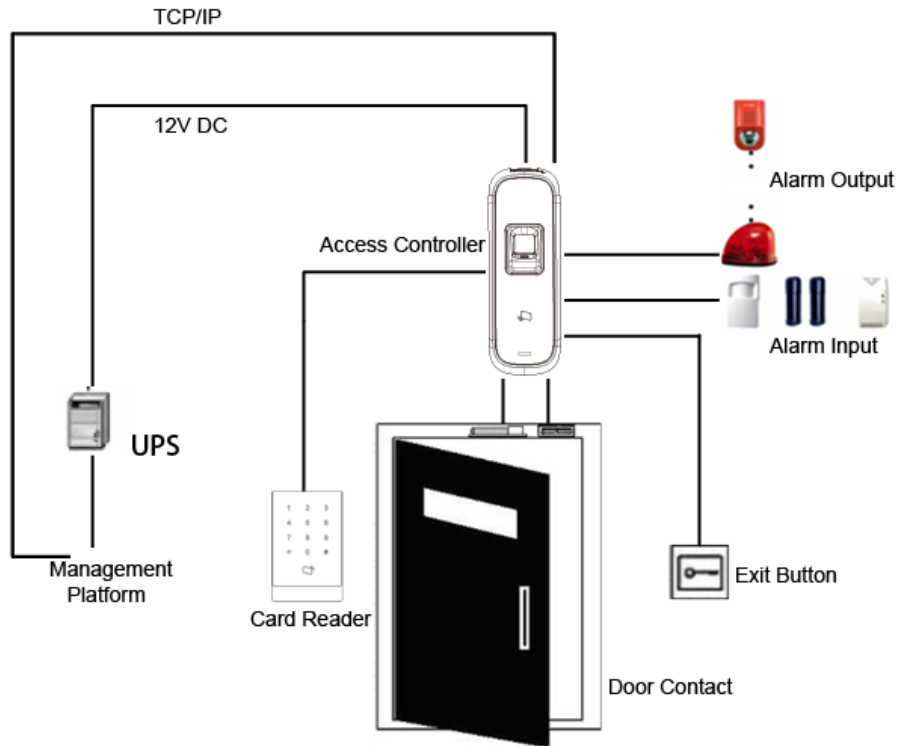- Working humidity: ≤95%.

1.2 Dimensions

Figure 1-1 Dimensions (mm [inch])
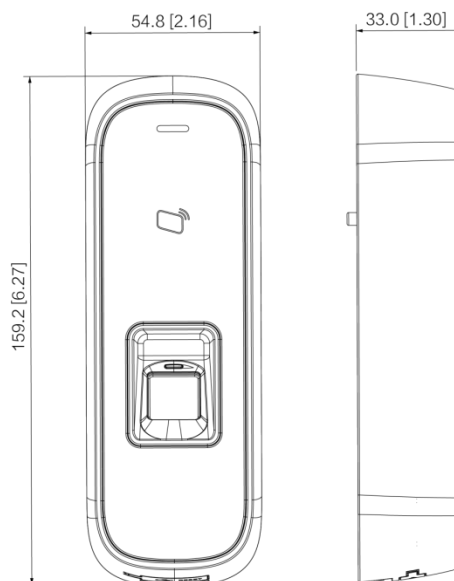
2 Installation

2.1 Application Diagram

Figure 2-1 Application diagram
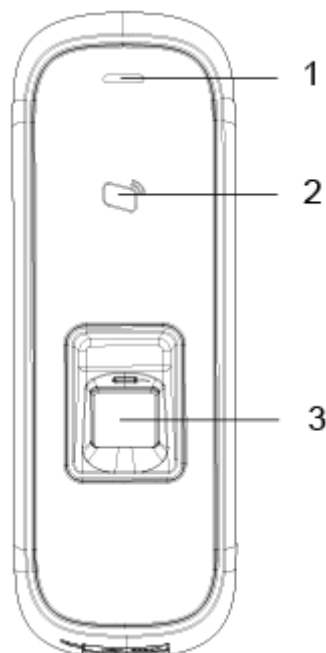

2.2 Component

Figure 2-2 Front panel
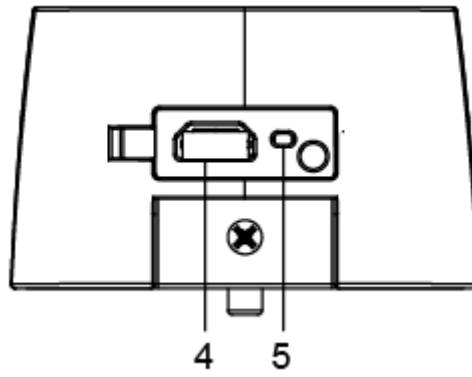
Figure 2-3 Ports at the bottom

Table 2-1 Component description (1)

No.	Name	No.	Name
1	Indicator light	4	USB port
2	Card swiping area	5	Restart
3	Fingerprint sensor	–	–

2.3 Installation

Figure 2-4 Installation
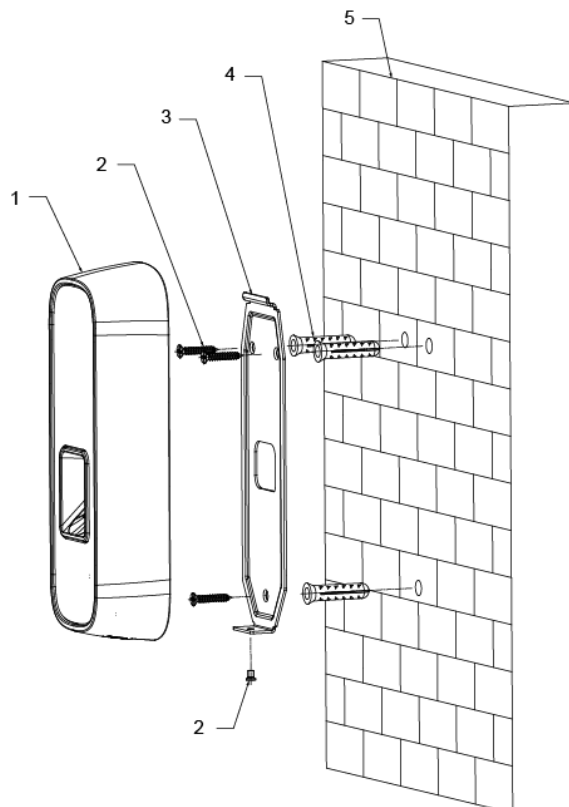
Table 2-2 Component description (2)

No.	Name	No.	Name
1	Access controller	4	Anchor bolt
2	ST3×18 screw	5	Wall
3	Bracket	–	–

Procedure

Step 1 Drill 3 holes at appropriate height on the wall according to hole positions on the bracket.

Step 2 Hammer the anchor bolts in the wall.

Step 3 Fix the bracket on the wall through the three ST3×18 screws.

Step 4 Attach the access controller to the bracket through the bracket fastener.

Step 5 Check whether the access controller is firmly mounted to the wall.
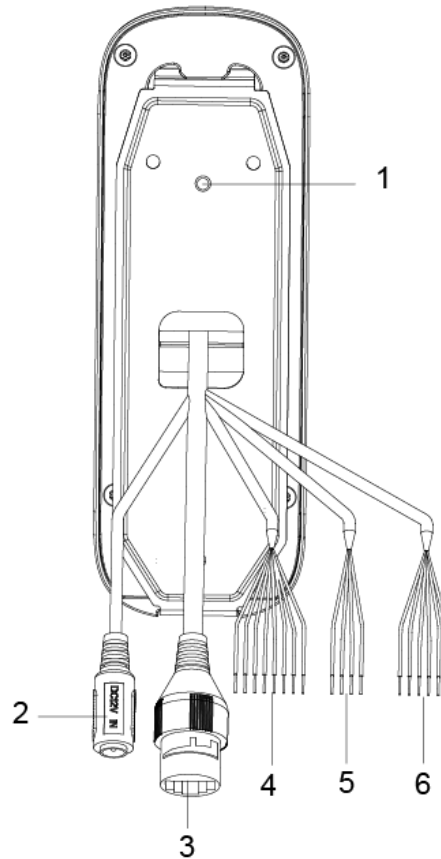
2.4 Cable Connection

Figure 2-5 Cable connection

Table 2-3 Component description (3)

No.	Name	No.	Name
1	Tamper switch	4	CON4
2	Power port	5	CON5
3	Ethernet port	6	CON6

2.4.1 Wiegand/RS-485

Table 2-4 Wiegand/RS-485 cable connection

Parameter	Cable Color	Cable Name	Description
CON4 (Wiegand/RS-485)	Blue	CASE	Connected to CASE signal cable of peripheral devices; used to detect tamper.

Parameter	Cable Color	Cable Name	Description
	White	D1	Wiegand D1 input (connected to peripheral card readers)/output (connected to access controllers).
	Green	D0	Wiegand D0 input (connected to peripheral card readers)/out (connected to access controllers).
	Brown	LED	Connected to peripheral LED signal cables to confirm validity of Wiegand D0 and D1 data transmission.
	Yellow	RS–485_B	RS-485 negative input (connected to peripheral card readers)/output (connected to access controllers).
	Purple	RS–485_A	RS-485 positive input (connected to peripheral card readers)/output (connected to access controllers).
	Red	12V_OUT	Power positive output.
	Black	GND	GND of power port.

Table 2-5 Cable specification and length

Parameter	Cable Connection Description	Length
RS-485 Input/ Output	CAT5e cable, RS-485 connection	100 m
Wiegand Input/ Output	CAT5e cable, Wiegand connection	50 m

2.4.2 Lock/Door Contact/Exit Button

Table 2-6 Lock/door contact/exit button cable connection

Parameter	Cable Color	Cable Name	Description
CON6	Black and green	DOOR_BUTTON	Exit button
	Black and blue	GND	Lock signal GND
	Black and grey	DOOR_SR	Door contact input
	Black and brown	DOOR_COM	Common port of lock
	Black and yellow	DOOR_NO	Normally open port of lock
	Black and purple	DOOR_NC	normally closed port of lock

Cable connection methods might vary according to lock types. See Figure 2-6, Figure 2-7, Figure 2-8, and Figure 2-9.

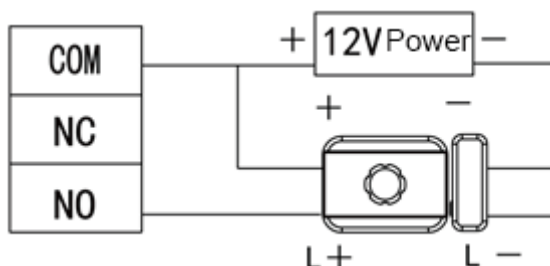Figure 2-6 Motor lock cable connection
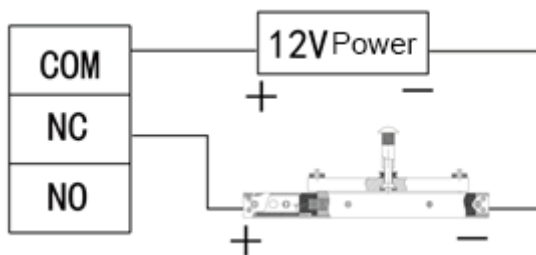
Figure 2-7 Magnetic lock cable connection

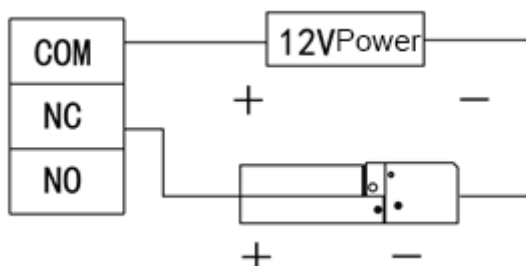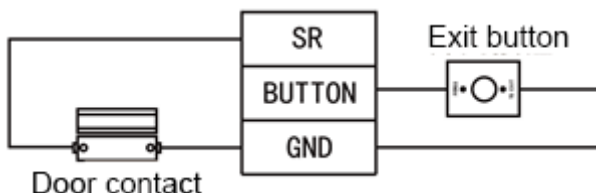Figure 2-8 Electric lock cable connection

Figure 2-9 Door contact and exit button cable connection

2.4.3 Alarm Input/Output

Table 2-7 Alarm Input/output cable connection

Parameter	Cable Color	Cable Name	Description
CON5 (Peripheral alarm input and output)	White and red	ALM_NO	One alarm output port, used to connect the access controller to sound and light alarm devices. Once alarms like door contact timeout (internal alarm input) and intrusion (external alarm output) occur, alarm output device will give out sound and light alarms for 15 seconds.
	White and orange	ALM_COM	
	White and brown	ALM_IN	One alarm input port, used to connect the access controller to peripheral alarm input devices like infrared detectors and smoke detectors.
	White and green	GND	Alarm input signal GND.

- There are two methods to connect peripheral alarm output devices. You need to select as needed.
  ◇ When you use IP camera, you can select peripheral output device cable connection method in Figure 2-10.
  ◇ When you use sound and light siren, you can select cable connection method in Figure 2-11.

Figure 2-10 Peripheral alarm output device cable connection (1)
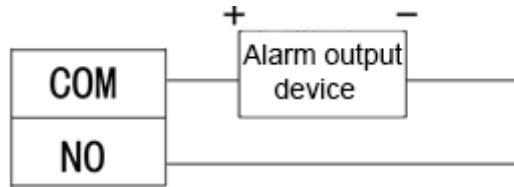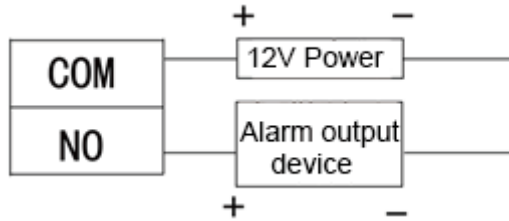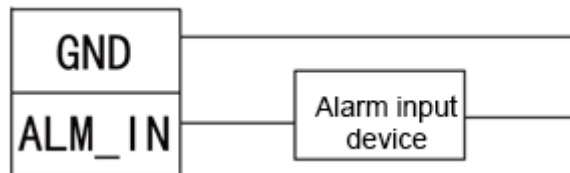

Figure 2-11 Peripheral alarm output device cable connection (2)

- For peripheral alarm input device cable connection, see Figure 2-12.

Figure 2-12 Peripheral alarm input device cable connection

2.4.4 Other Cables

Table 2-8 Other cable connection descriptions

Parameter	Description
Tamper switch	When the access controller is detached from the wall forcibly, alarms will be triggered.
Power port	Connected to 12 VDC power supply.
Ethernet port	Connected to network cable.

3 Operations

After the access controller is powered on for the first time, the first card that is swiped is the administrator card. Three modes are available for the access controller: Standby verification, local user management, and USB flash drive management. You can add, delete, and clear users; export data to and import data from USB flash drive, and update the access controller with the USB flash drive.

- The access controller can work as an all-in-one or a card reader. This section only introduces the operations of the device as an all-in-one.
- You can open the back cover of the access controller, and press the restart button on the motherboard to restart the device.

3.1 Standby Verification

Power on the access controller, and then swipe the administrator card, the yellow light glows, which means the device as an all-in-one is in standby verification mode.

If the yellow light does not glow, continuously swipe the administrator card 7 times in 15 seconds to put the device as an all-in-one in standby verification mode.

3.2 User Management

You can add, delete, and clear users on the access controller.

- Make sure that the access controller as an all-in-one is in standby verification mode, and no USB flash drive is inserted.
- The interval of continuously swiping the administrator card cannot be greater than 5 seconds.
- If there is no operation within 15 seconds, the system will exit from user management mode.

3.2.1 Adding User

You can add a user by adding a card or a fingerprint.

Step 1 Swipe the administrator card once.
        The yellow light is on.
Step 2 Swipe the administrator card again, and then you can start to add user.
        Wait for 5 seconds, the cyan light is on, and the fingerprint module light also flashes.
Step 3 Swipe the card, or press the fingerprint that you want to add.
Step 4 Swipe the administrator card once to save the user.

- When adding a user, swipe the card only once. One fingerprint needs to be collected three times, and up to three fingerprints can be collected.
- You can only add one user at a time. A user must be linked to at least 1 card or 1 fingerprint, or at most 1 card and 3 fingerprints.

3.2.2 Deleting Users

You can delete a user by deleting the user's card or fingerprint.

Step 1 Swipe the administrator card once.

The yellow light is on.

Step 2 Swipe the administrator card 3 times, and then you can start to delete user.

Wait for 5 seconds, the cyan light is on.

Step 3 Swipe the card, or press the fingerprint that has been added to the access controller.

You can delete up to 10 users at a time.

Step 4 Swipe the administrator card once to delete the user.

3.2.3 Clearing Users

You can clear users by swiping the administrator card.

Step 1 Swipe the administrator card once.

The yellow light is on.

Step 2 Swipe the administrator card 5 times.

Wait for 5 seconds, the cyan light is on.

Step 3 Swipe the administrator card once to clear users.

3.2.4 Switching Work Mode

The access controller can work as an all-in-one or a card reader.

Step 1 Swipe the administrator card once.

The yellow light is on.

Step 2 Swipe the administrator card 7 times.

Wait for 5 seconds, the cyan light is on.

Step 3 Swipe the administrator card once, and the access controller switch to a card reader.

When the access controller works as a card reader, continuously swipe the administrator card 7 times in 15 seconds to switch the device to an all-in-one in standby verification mode.

3.3 USB Flash Drive Management

You can export user data to or import such data from USB flash drive, export card swiping records and alarm records to the flash drive, or update the access controller with the flash drive.

- Make sure that the access controller as an all-in-one is in standby verification mode, and USB flash drive is inserted.
- Do not remove the USB flash drive or perform other operations during import, export or update. Otherwise, the import, export, or update might fail.
- The interval of continuously swiping the administrator card cannot be greater than 5 seconds.

3.3.1 Exporting Data

Export data on the access controller to the USB flash drive.

Step 1   Swipe the administrator card once.

        The yellow light is on.

Step 2   Swipe the administrator card 2 times.

Step 3   After 5 seconds, swipe the administrator card once, and the data is exported to the USB flash drive.

        During exporting, the purple light is on.

3.3.2 Importing Data

After exporting user data from an access controller using USB flash drive, you can import such data to another access controller.

Step 1   Insert the USB flash drive with user data to the target access controller. Swipe the administrator card once.

        The yellow light is on.

Step 2   Swipe the administrator card 4 times.

Step 3   After 5 seconds, swipe the administrator card, and the data is imported to the target access controller.

        During importing, the purple light is on.

3.3.3 Updating Access Controller

You can update your access controller with USB flash drive.

Step 1   Name the update file on PC as "update.bin", and save the update file in the root directory of the USB flash drive.

Step 2   Swipe the administrator card once.

        The yellow light is on.

Step 3   Swipe the administrator card 6 times.

Step 4   After 5 seconds, swipe the administrator card once, and the update starts.

        The access controller will restart after the update finishes.

        During updating, the purple light is on.

4 Configuring DSS Pro

You can manage personnel and their fingerprints, and configure door groups and rules of opening doors to realize access control on the DSS Pro client.

This section introduces the quick configuration of the access controller on the DSS Pro platform. For details, see the DSS Pro operation manual.

- The interfaces of different DSS Pro client version might vary, and the actual interface shall prevail.
- The IP address is 192.168.1.108 by default, and the default username and password are both admin.

4.1 Logging in to DSS Pro Web Page

4.2 Adding Device

If users want to use the newly added device, enter **User** interface, edit user to make him have permission to use the device, otherwise, the device cannot be used.

You can add the access controller to the DSS client, after that you can manage and configure device remotely on client. For details about adding devices, refer to the user's manual of DSS Pro.

4.3 Logging in to the DSS Pro Client

After installing DSS Pro client, double-click on the desktop to run the client. Initialize the client according to on-screen instructions, and then log in to it.

4.4 Personnel Management

Personnel refer to the people responsible for access control management. They have the authorization to unlock doors with password, fingerprint, card, or face recognition.

4.4.1 Adding Department

Adding department is to group or classify personnel, so the personnel in the same department can be conveniently managed.

Step 1 Click . On the **Homepage** interface, select **Personnel Management**.

The **Personnel Management** interface is displayed.

Step 2 Select a node from the department list on the left side, and click **Add**.

Step 3 The **New Department** interface is displayed. See Figure 4-1. The new department is directly under the selected node.

Figure 4-1 New department
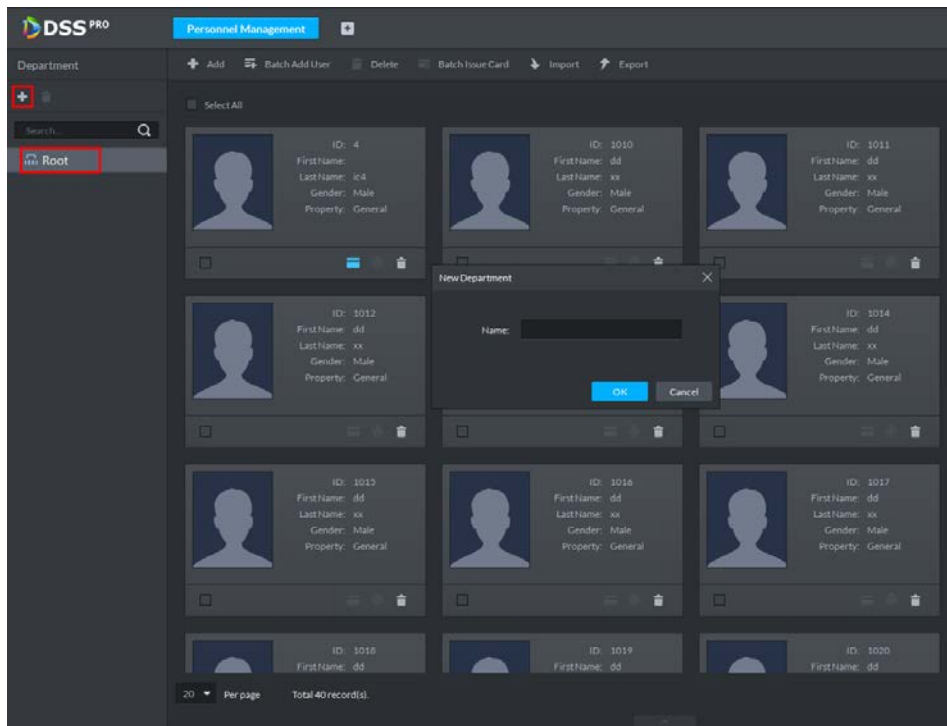
Step 4 Enter the department name and click **OK**.

Step 5 The newly added department is displayed. See Figure 4-2.

Figure 4-2 Newly added departments
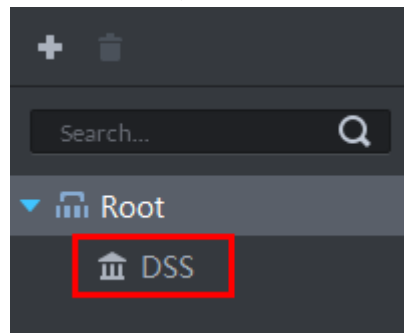
- You can delete or rename a newly added department.

- Select a department, click ☐ to delete it, and follow the on-screen instructions. You cannot delete a department with personnel.

- To rename a department, right-click it and select **Rename** to modify the name.

4.4.2 Adding Personnel

Add personnel and authorize them to unlock doors. When adding personnel, system uploads the collected personnel information to the server for proper protection.

- Person ID shall be the same on the platform and access control devices; otherwise person data
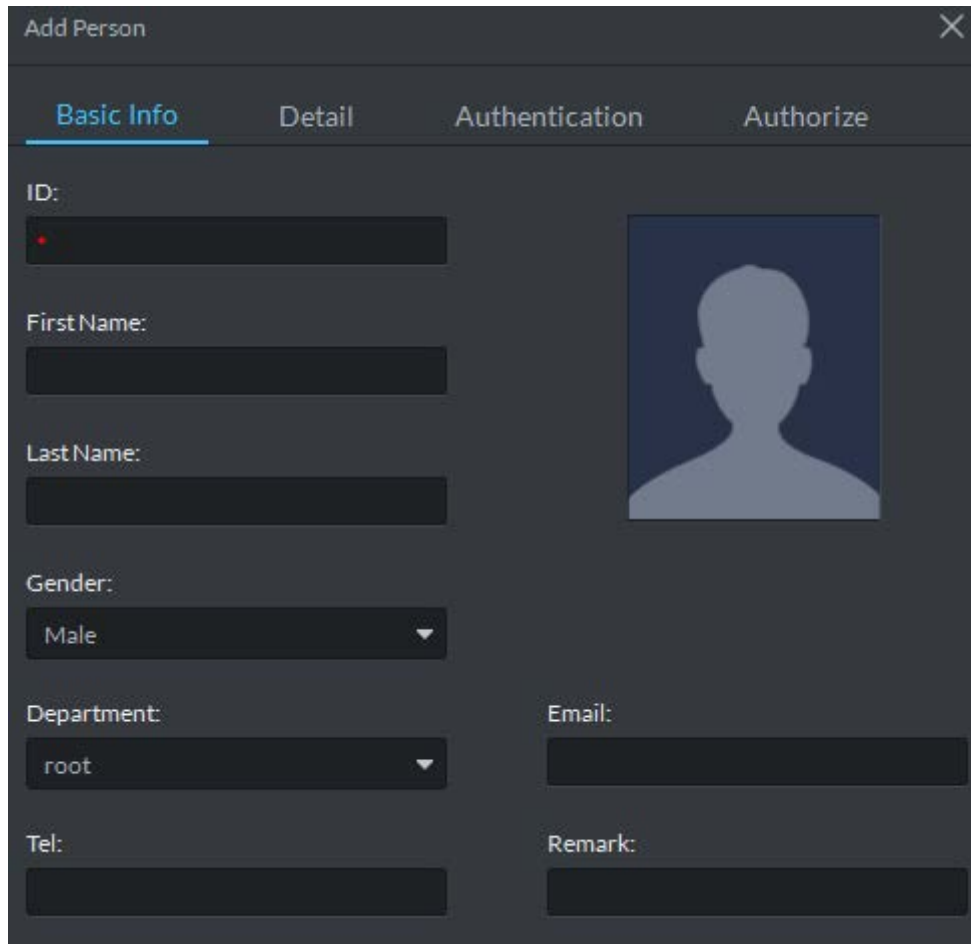
could be wrong.
- To collect fingerprints or card No., connect a fingerprint collector or card reader first.
- IR face feature code is obtained from the access control device when editing person information.

4.4.2.1 Adding One Person

Step 1 On the **Personnel Management** interface, click **Add**.
        The **Add Person** interface is displayed. See Figure 4-3.

Figure 4-3 Add a person

Step 2 Click the **Basic Info** tab to configure person information.

        ID is required, and others are optional.
Step 3 Click the **Detail** tab, and then set person details as required.
Step 4 Click the **Authentication** tab, and then set access control information. See Figure 4-4. For details, see Table 4-1.

Figure 4-4 Authentication
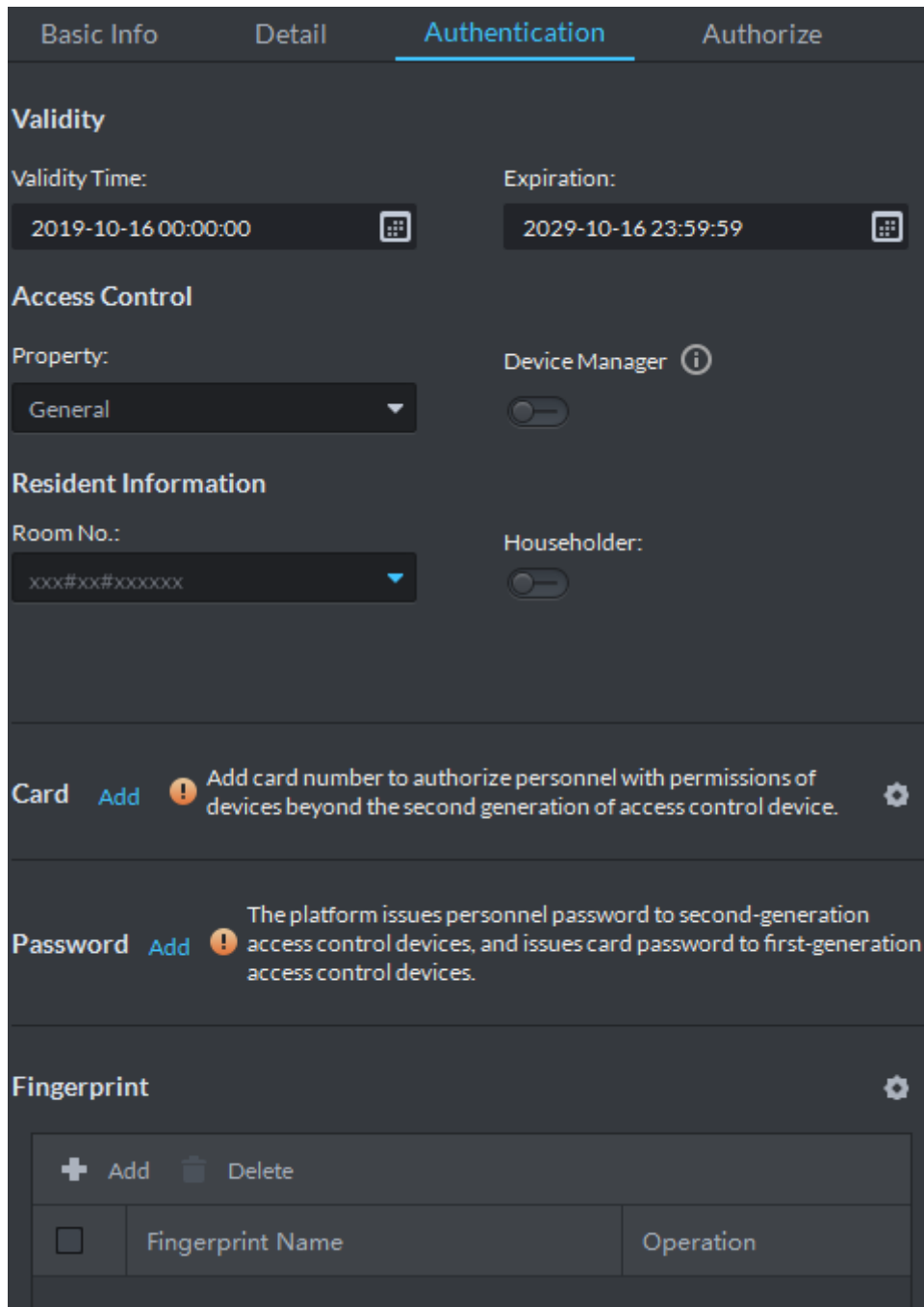
Table 4-1 Authentication parameters

Parameter		Description
Term of Validity	Validity Time	Effective time of the access control permission.
	Expiration	Expiration time of the access control permission.
Access Control	Property	Set person types. 📖 If the person has the permission of First Card Unlock, you need to select **General** in the **Property** dropdown list.
	Device Manager	Personnel include common people and system managers. A device manager has the device operation permission. This function is only effective when the person information is applied to the second-generation devices.

Parameter		Description
Resident Information	Room No.	Room No. is the number of the apartment in which this person lives. The room No. is displayed in the access records and video intercom operation records. Access permission of the corresponding VTO is also included when authorizing access control permission to this person.
	Householder	When several people live in one apartment, you can set one of them as the householder. The householder will be taken as the only contact of video intercom.

Step 5   Issue cards to personnel.

One person can have up to 5 cards. There are two ways to issue cards: by entering card No. and by card reader. Card No. can contain 8 or 16 numbers. 16-digit card No. is only available with the second-generation access control devices. When a card No. is less than 8 or 16 numbers, the system will automatically add zeros prior to the No. to make it 8 or 16 digits. For example, if the provided No. is 8004, it will become 00008004; if the provided No. is 1000056821, it will become 0000001000056821.

● By entering card No.

1) Click **Add** next to **Card**.

The **Issue Card** dialog box is displayed. See Figure 4-5.

Figure 4-5 Issue card by entering card No.
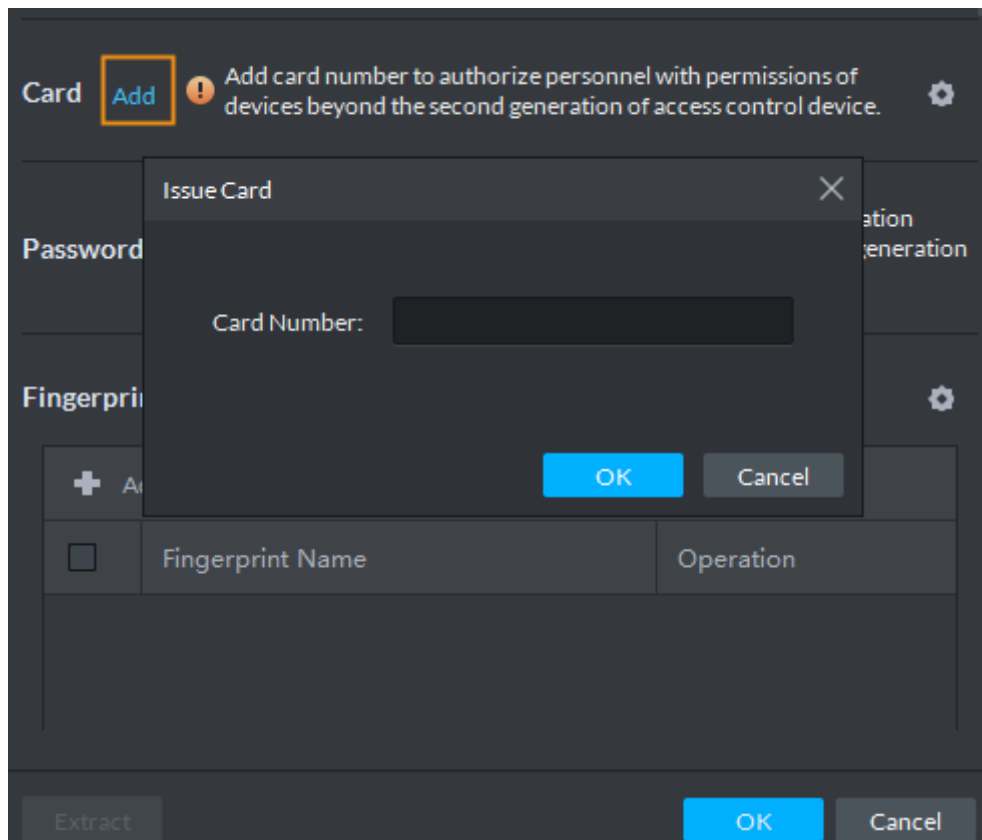
2) Enter card number and click **OK**.

The card is added. See Figure 4-6. For operations of added card, see Table 4-2.

Figure 4-6 Added card
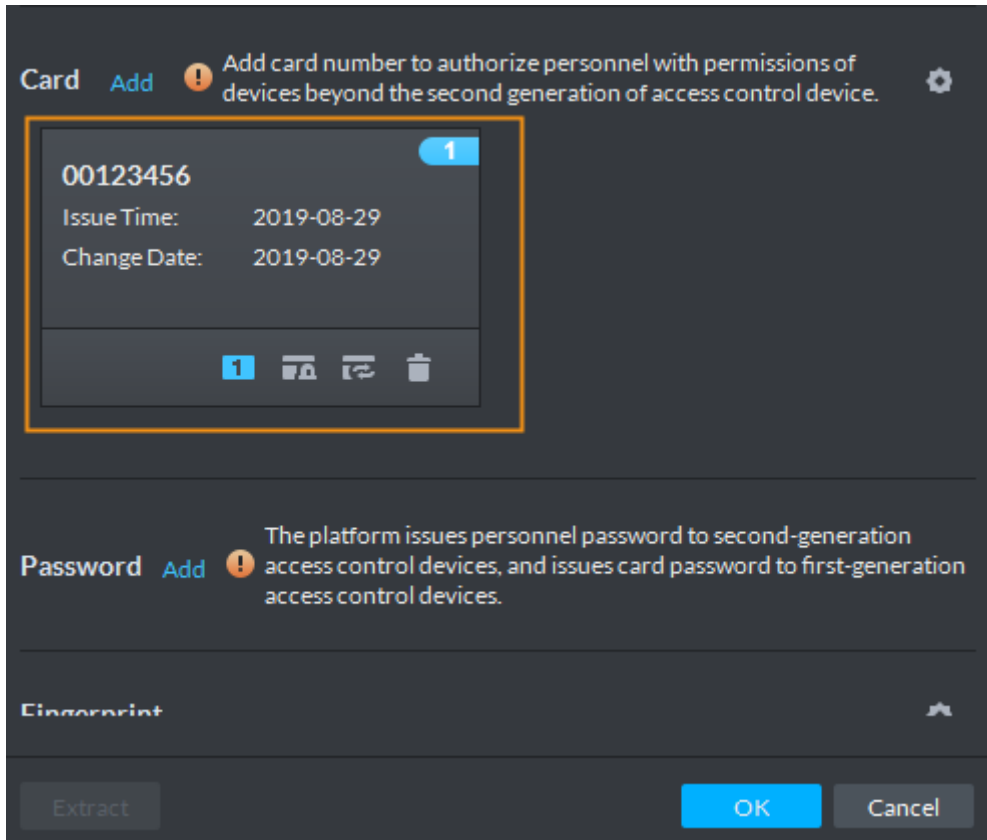
Table 4-2 Card operations

Icon	Description
![1]	If a person has more than one card, only the main card can be issued to the first-generation cards. The first card of a person is the main card by default. Click ![1] on an added card, the icon turn into ![1], which indicates that the card is a main card. Click ![1] to cancel the main card setting.
![duress]	Set a card as duress card. When opening door with a duress card, there will be a duress alarm. Click this icon, it turns into ![duress], and a ![alarm] icon is displayed at upper right, which indicates that the card is set as a duress card. To cancel the duress setting, click ![duress].
![change]	Change card for the person when the current card does not work.
![delete]	Remove the card, and then it has no access permission.

●   By card reader

1)   Click ![gear].

Figure 4-7 Issue card by card reader
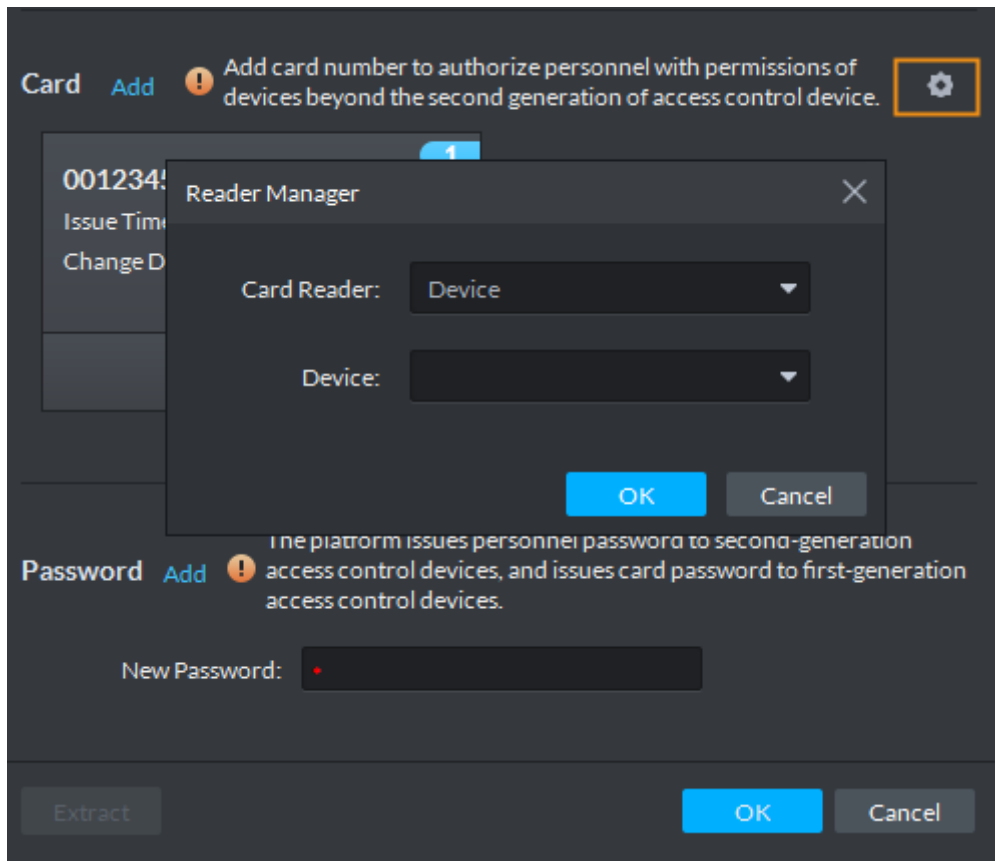
2) Select from **Card Reader** or **Device**, and then click **OK**.
3) Swipe card on the card reader or device.

The card is added. See Figure 4-6. For card operations, see Table 4-2.

Step 6 Set access password.

To open door with password, you need to set passwords for personnel, and then one can open door by entering person ID and password.

1) Click **Add** next to **Password**.

Figure 4-8 Set a password
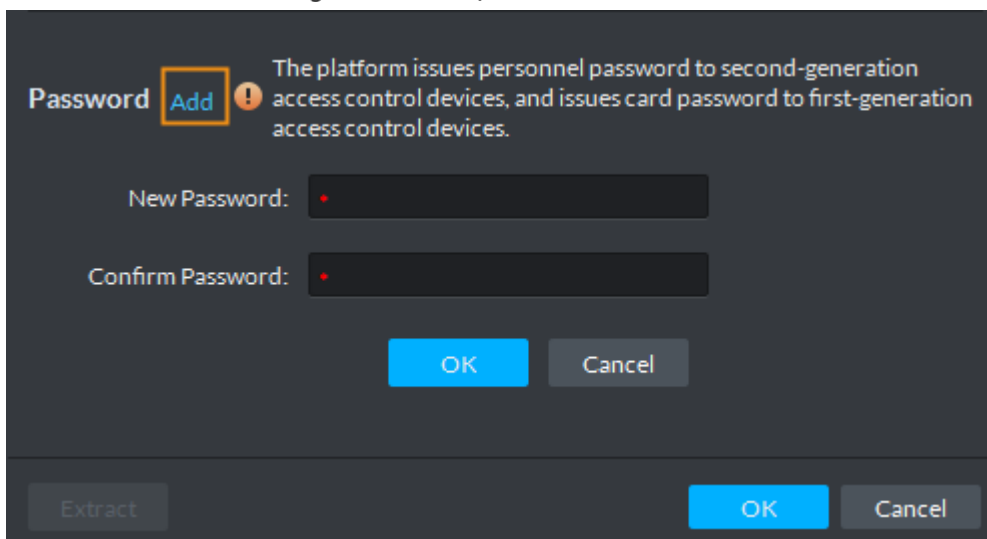
2) Enter the password, and then click **OK**.

Step 7 Collect fingerprint.

To open door with fingerprint, you need to collect personnel fingerprints. A person can have up to 10 fingerprints.
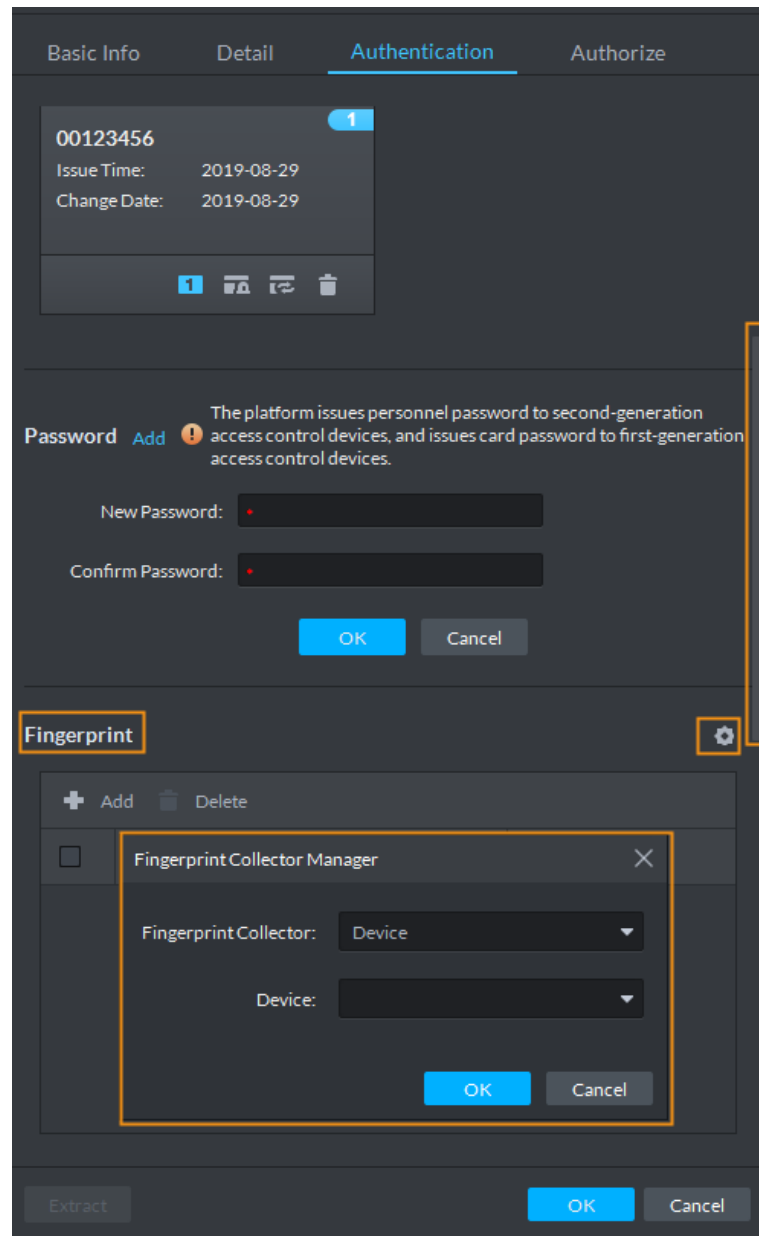
1) Scroll down the **Authentication** page, and then in the Fingerprint section, click ⚙.

Figure 4-9 Fingerprint collector manager

2) Select a fingerprint collector, and then click **OK**.
3) Click **Add**.

Figure 4-10 Collect fingerprint
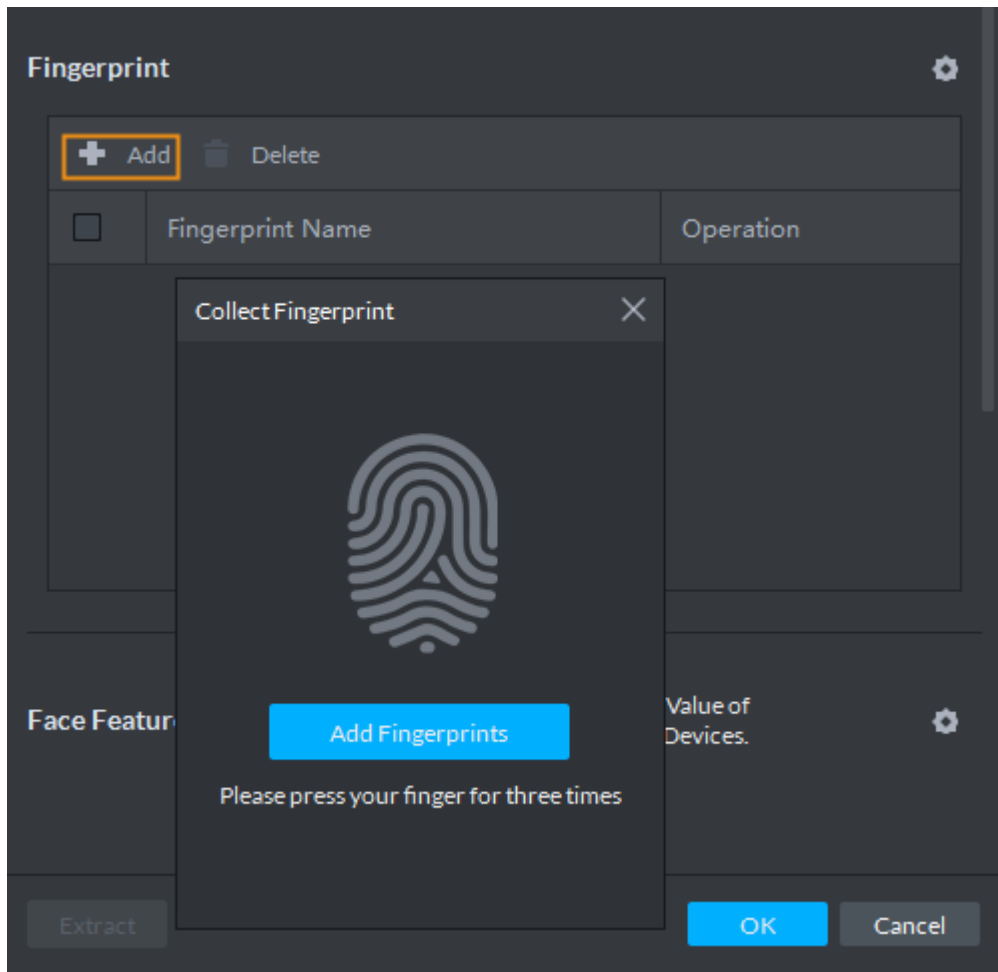
4) Click Add Fingerprints.

Figure 4-11 Collect fingerprint

5) Record fingerprint on the reader by raising and then pressing the finger after hearing the beep sound. Repeat this for three times to finish fingerprint collection. See Figure 4-12. For more fingerprint operations, see Table 4-3.

Figure 4-12 A collected fingerprint
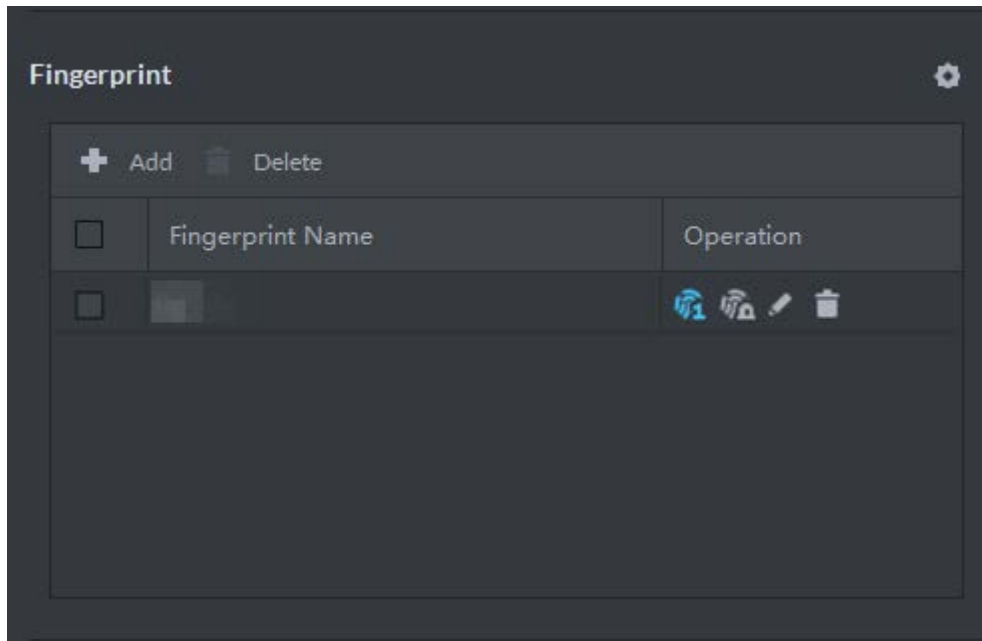
Table 4-3 Fingerprint operations

| Icon	Description
	When more than 3 fingerporints are collected, only the main fingerprints can be issued to devices. The first 3 fingperprints are main ones by default. One person can have up to 3 main fingerprints. Click this icon, and then it turns into , which indicates that this fingerprint has been set as a main one. To cancel the main fingerprint setting, click .
	Set a fingerprint as duress fingerprint. When opening door with a duress, there will be a duress alarm. Click this icon, it turns into , which indicates that the fingerprint has been set as a duress fingerprint. To cancel the duress setting, click .
	Modify fingerprint name.
	Remove the fingerprint, and then it has no access permission.

Step 8   Click the **Authorize** tab.

Select the target door groups, entrance & exit channels and video intercom channels. See Figure 4-13.

A door group contains a group of doors which can be authorized in batches. To add a door group, click **Add Door Group**.
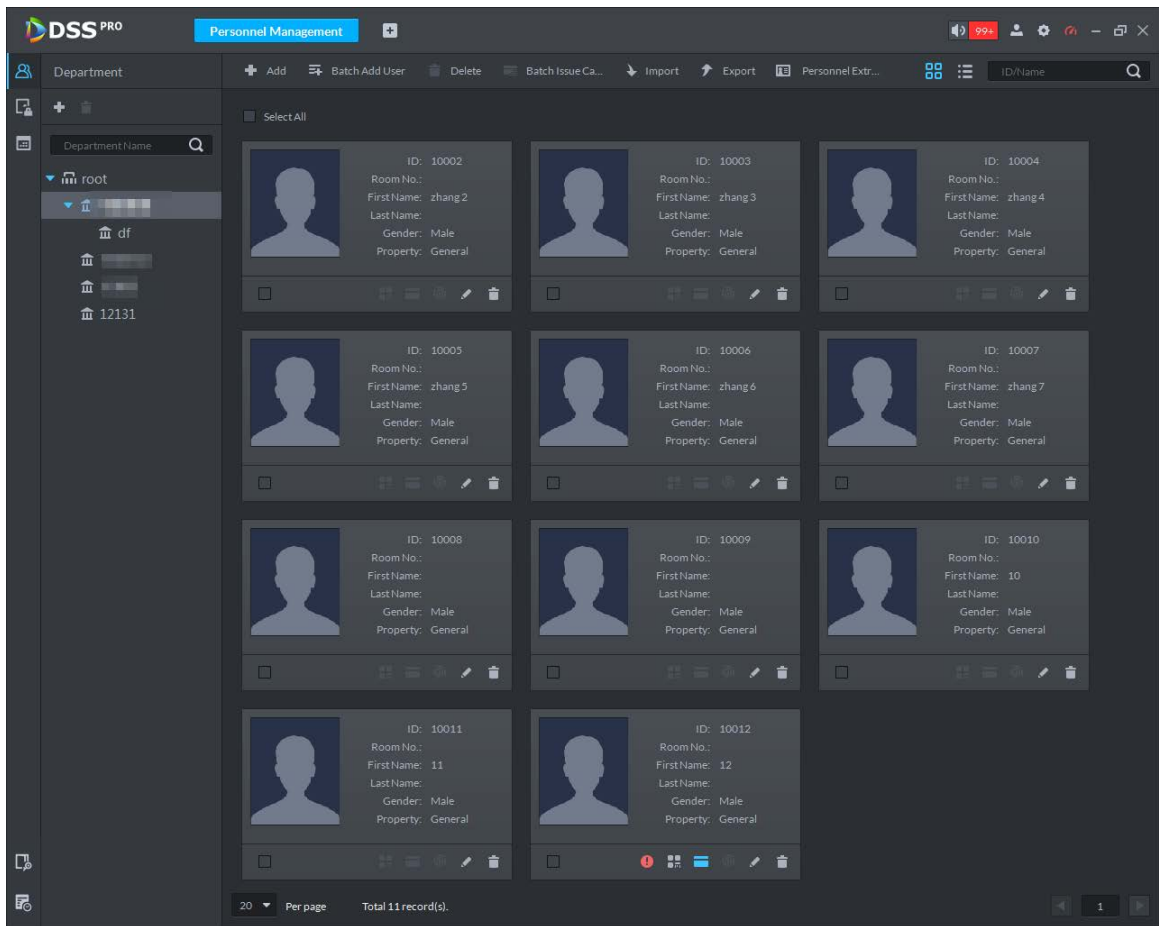
Figure 4-13 Authorize
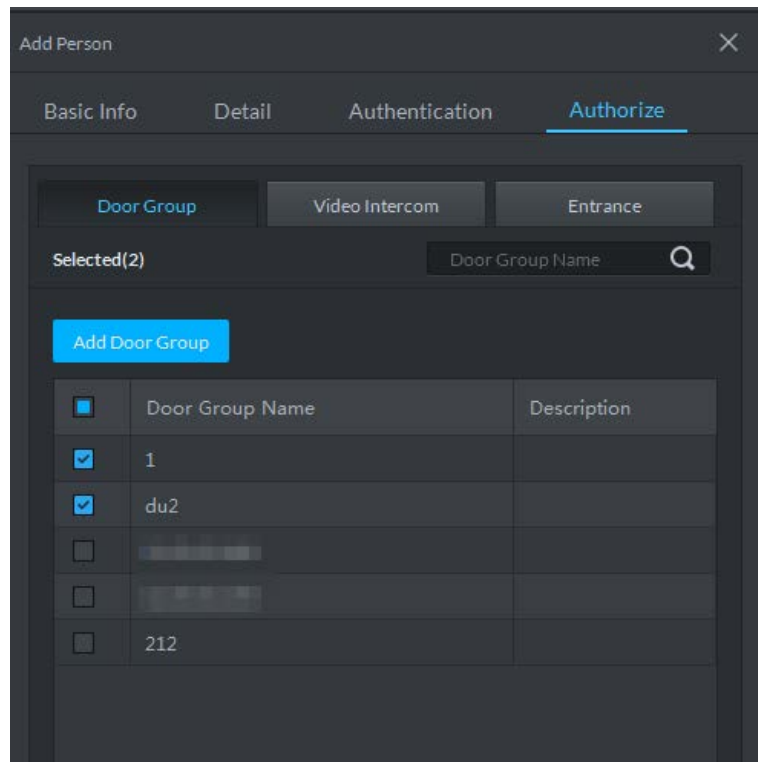
Step 9   Click **OK**.

- To edit person information such as basic details, passwords, fingerprints, IR face feature codes and face pictures, see the user's manual *of DSS Pro*.

- To delete a person, you can select the person, and then click ⬛; to delete all people on this page, select the **Select All** check box, and then click **Delete**.

Figure 4-14 Added people

4.4.2.2 Adding Personnel in Batches

If multiple people are added at one time, you can issue cards to them. When you need to issue passwords and fingerprints to them, you can edit personnel authorization separately.

Step 1   On the **Personnel Management** interface, click **Batch Add User**.

Figure 4-15 Add personnel in batch (1)

Step 2   Enter the starting ID number in the **ID** box, enter the number of people you need in the **Quantity** box, select a department, and then set the term of validity.

Figure 4-16 Add personnel in batch (2)

Step 3   Issue cards.

You can issue cards by entering card numbers or by using a card reader.

- By entering card numbers
1)   Double-click the **Card No.** cells, and then enter a card numbers one by one.
2)   Click **OK**.

Figure 4-17 Newly added people
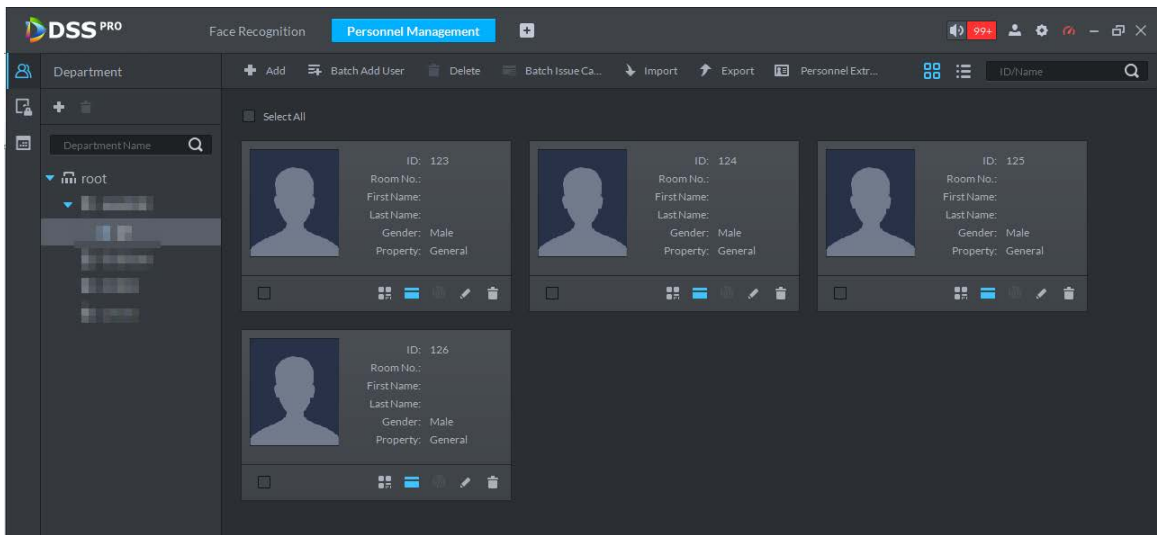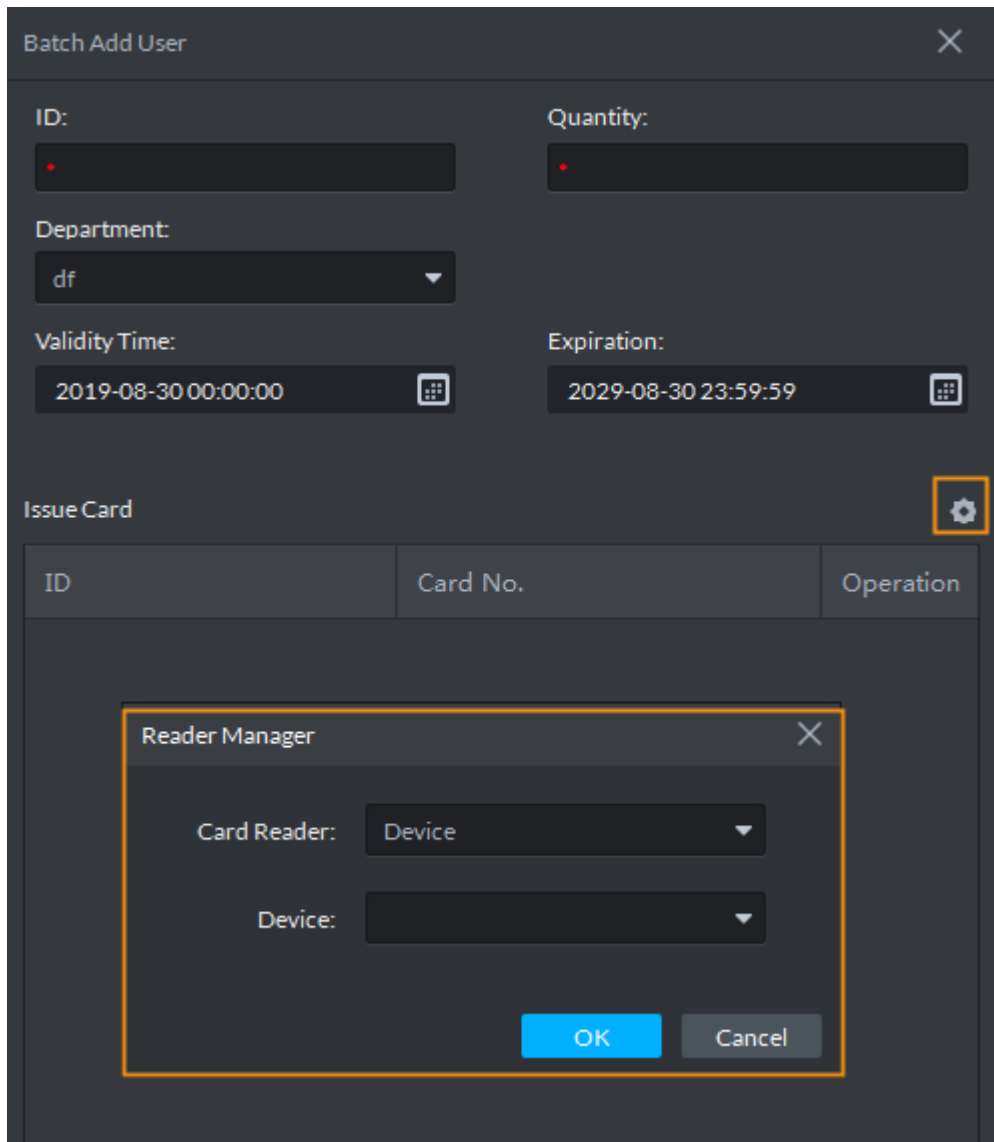

- By using card reader.

1) On the **Batch Add User** interface, click ⚙.

Figure 4-18 Reader manager

2) Select a card reader or a device, and then click **OK.**
3) Select people, and then swipe cards on the card reader or device.

4) Click **OK**.

The added personnel list is displayed. See Figure 4-17.

To edit personnel information such as password and fingerprint, see the *DSS Pro_User's Manual-V1.0.3*.

4.5 Configuring Door Groups

Configure door groups so that you can quickly assign permissions by door groups.

Step 1 On the **Personnel Management** interface, click ![icon].

Figure 4-19 Access control permission interface
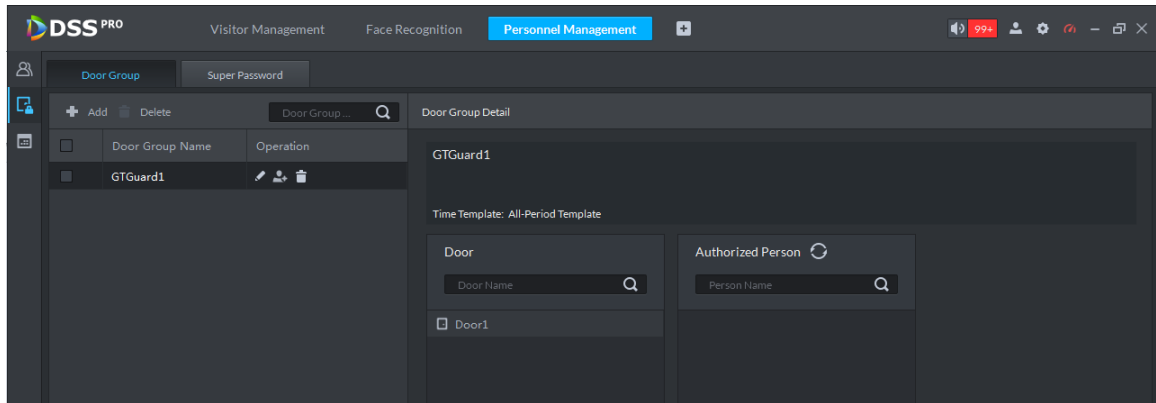
Step 2 Create a door group.

1) Click the **Door Group** tab.

The **Door Group** interface is displayed.

2) Click **Add**.

Figure 4-20 Add a door group

3) Enter the group name, select a time template and a holiday schedule, select a device channel, and then click **OK**.

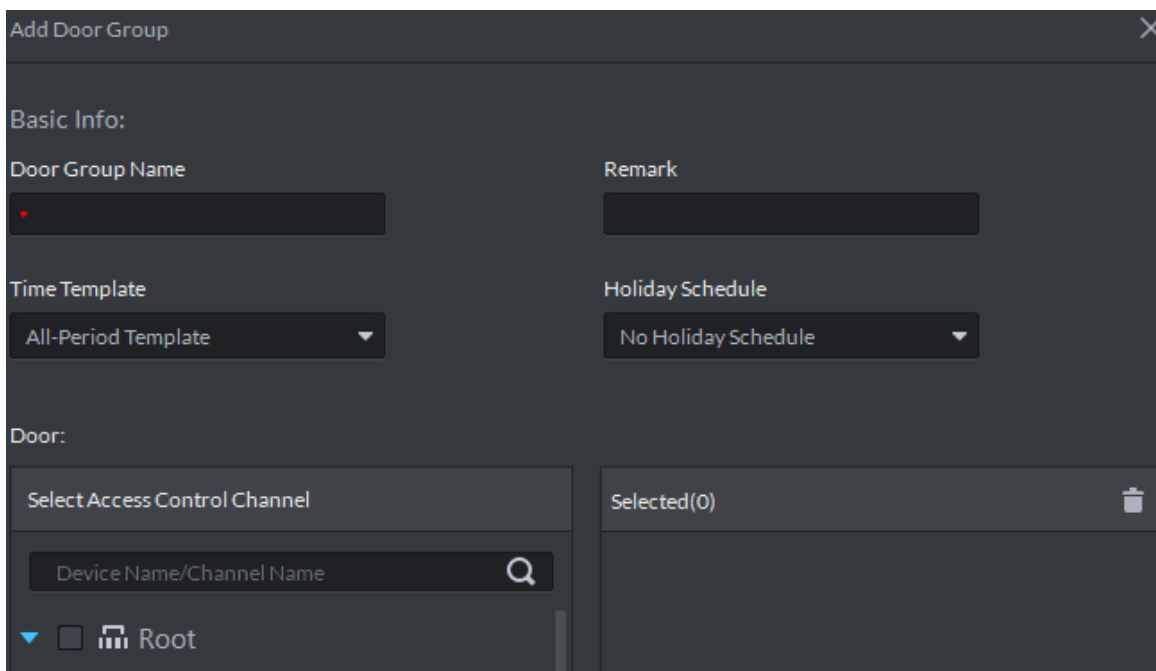After the time template and device channel is selected, when assigning permissions to personnel, it is valid only to select a time period within the template and select a channel as selected here.

📖
- To create a new time template, select **Manage time template** in the **Time Template** dropdown list. For details, see the user's manual of DSS Pro.
- To create a new holiday schedule, select **Add Holiday Schedule** in **the Holiday Schedule** dropdown list. For details, see user's manual of DSS Pro.

Step 3   Authorize.
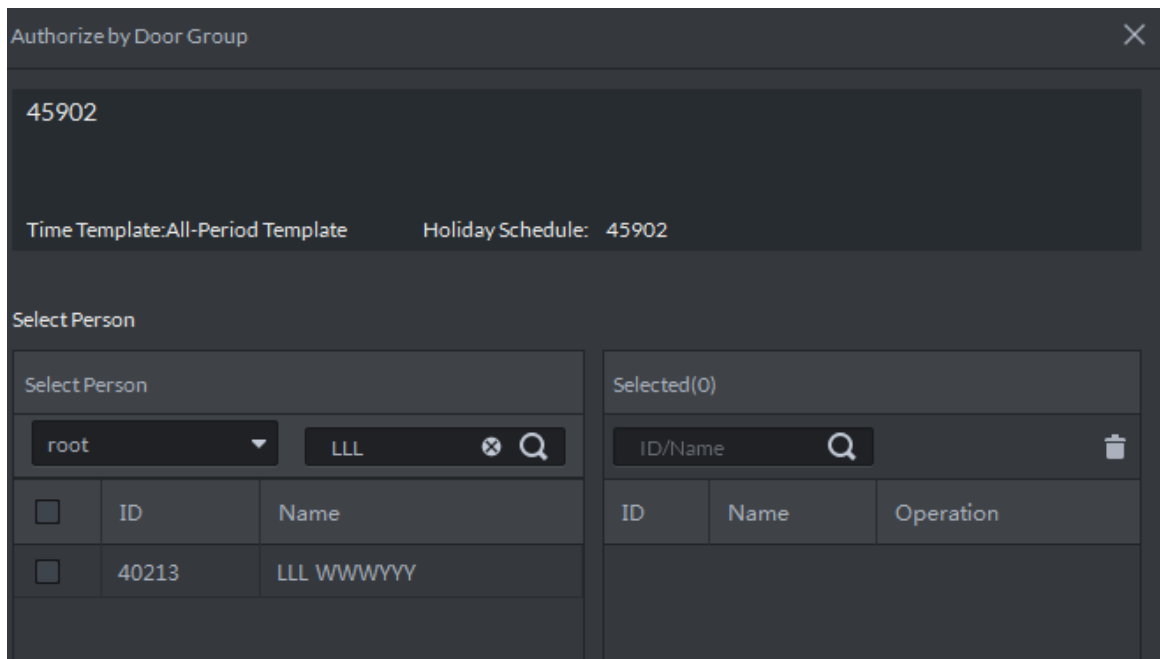
1)   On the **Door Group** interface, select a door group, and then click the corresponding ![icon] icon.

Figure 4-21 Authorize by door group

2)   Select personnel, and then click **OK**.

📖

Click ![icon] to update authorized personnel.

Appendix 1 Fingerprint Record Instruction

Notice

- Make sure that your fingers are clean and dry before recording your fingerprints.
- Press your finger to the fingerprint recording area, and make your fingerprint is centered on the recording area.
- Do not put the fingerprint sensor at places with intense light, high temperature, and high humidity.
- For the ones whose fingerprints are worn or are unclear, try other unlock methods.

Recommended Fingers

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
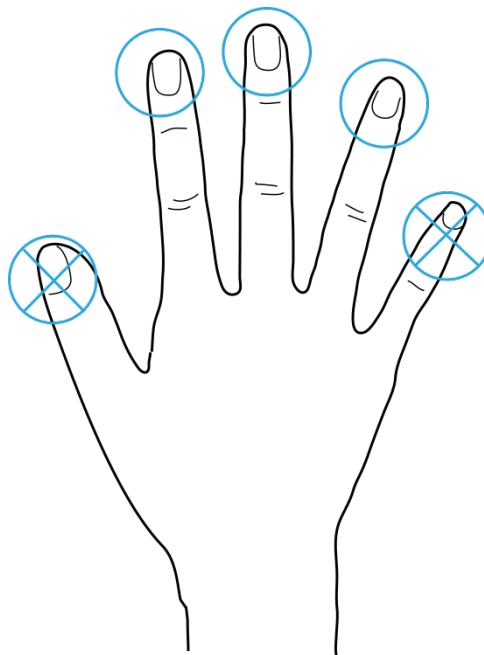
Finger Pressing Method

- Correct method

Appendix Figure 1-2 Correct finger pressing
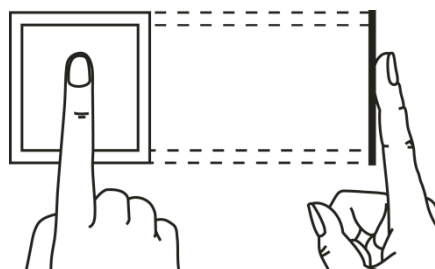
● Incorrect method

Appendix Figure 1-3 Wrong finger pressing

Fingertip perpendicular to the record area
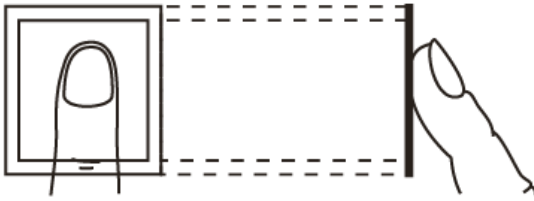
Fingertip not at the center of the record area
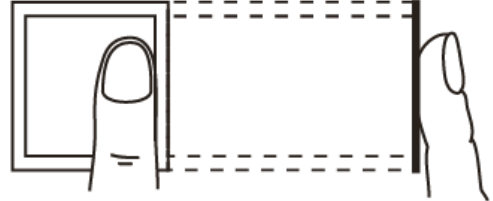
Fingertip not at the center of the record area
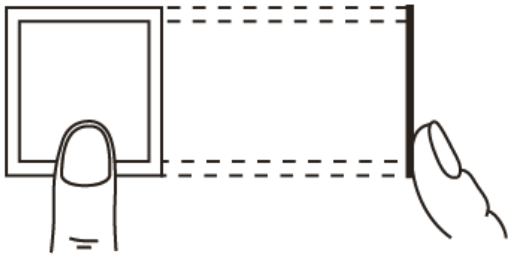
Fingertip inclination
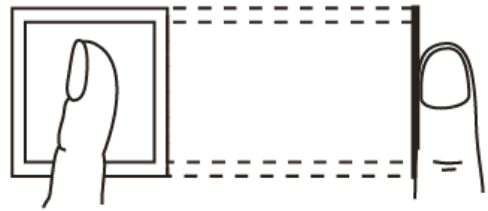
Appendix 2 Packing List

After unpacking the package, check whether the items are complete against the packing list and keep this guide properly for future reference.

Appendix Table 2-1 Packing list

Name	Quantity
Access controller	1
Quick start guide	1
Screw bag	1
USB patch cable	1

Appendix 3 Cybersecurity Recommendations

Mandatory actions to be taken for basic device 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 device (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 device 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 device network security:

1. **Physical Protection**

    We suggest that you perform physical protection to device, especially storage devices. For example, place the device 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 device (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 device, 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 device 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 device, 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 device 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.