


Access Controller

LXKW302-40

Quick Start Guide



V1.0.0






Foreword

General

This manual introduces the wiring, installation and basic operations of 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 Time
V1.0.0	First release.	December 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 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



- 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.
- Please follow the electrical requirements to power the Access Controller.
 - ◇ 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 Access Controller.
 - ◇ When selecting the power adapter, the power supply requirements (such as rated voltage) are subject to the Access Controller 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 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 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.
- Ground the device to protective ground before you power it on.
- 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.
- The Access Controller is not suitable for use in locations where children are likely to be present.

Table of Contents

Foreword	I
Important Safeguards and Warnings	III
1 Dimensions and Appearance	1
2 Ports Overview	3
3 Wiring of Locks	10
3.1 Wiring of Magnetic Locks	10
3.1.1 Wiring of Dual Magnetic Locks with PoE (12 V and Relay)	10
3.1.2 Wiring of Dual Magnetic Locks with 12 V External Power Supply (12 V and Relay)	11
3.1.3 Wiring of Dual Magnetic Locks with 12 V External Power Supply (Relay)	12
3.1.4 Wiring of 2-in-1 Magnetic Lock with 12 V External Power Supply (Relay)	14
3.2 Wiring of Electric Strike Lock	15
3.2.1 Wiring of Dual Electric Strikes with PoE	15
3.2.2 Wiring of Dual Electric Strikes with 12 V External Power Supply	16
4 Installation	18
4.1 Wall Mount	18
4.2 DIN Rail Mount	20
5 Access Control Configurations	23
5.1 Networking Diagram	23
5.2 Configurations of Main Controller	23
5.2.1 Configuration Flowchart	23
5.2.2 Initialization	24
5.2.3 Logging In	25
5.2.4 Adding Devices	30
5.2.4.1 Adding Devices One by One	31
5.2.4.2 Adding Devices in Batches	32
5.2.5 Adding Users	33
5.2.5.1 Adding Group	33
5.2.5.2 Adding Roles	34
5.2.5.3 Configuring Basic User Information	34
5.2.5.4 Adding Authentication Methods	37
5.2.5.4.1 Adding Passwords	37
5.2.5.4.2 Adding Cards	38
5.2.5.4.3 Adding Fingerprints	40
5.2.5.4.4 Adding Bluetooth Cards	41

5.2.6 Adding Weekly Plans.....	46
5.2.7 Adding Zone.....	47
5.2.8 Adding Permission Rules	48
5.2.9 Configuring Global Alarm linkages (Optional)	50
5.2.10 Viewing Data Synchronization Progress.....	53
5.2.11 Configuring Cloud Service	53
5.3 Configurations of Sub Controller	54
5.3.1 Initialization.....	54
5.3.2 Logging In	54
Appendix 1 Security Recommendation	55

1 Dimensions and Appearance

Figure 1-1 Dimensions (mm [inch])

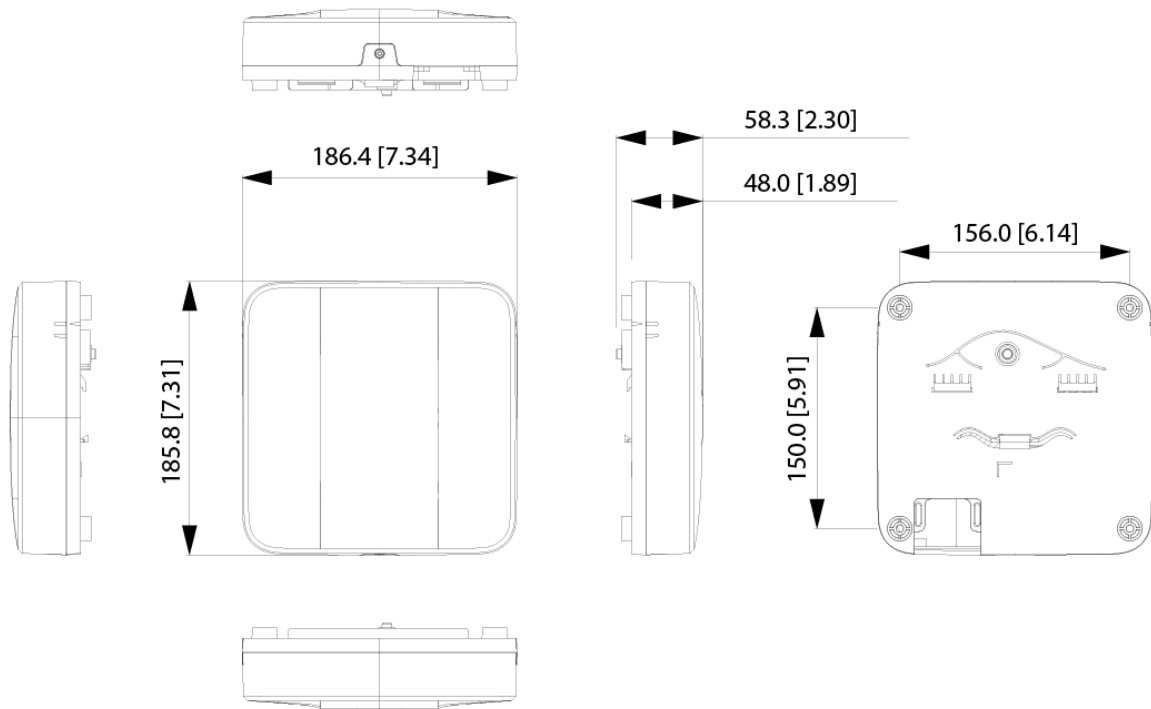


Figure 1-2 Front view

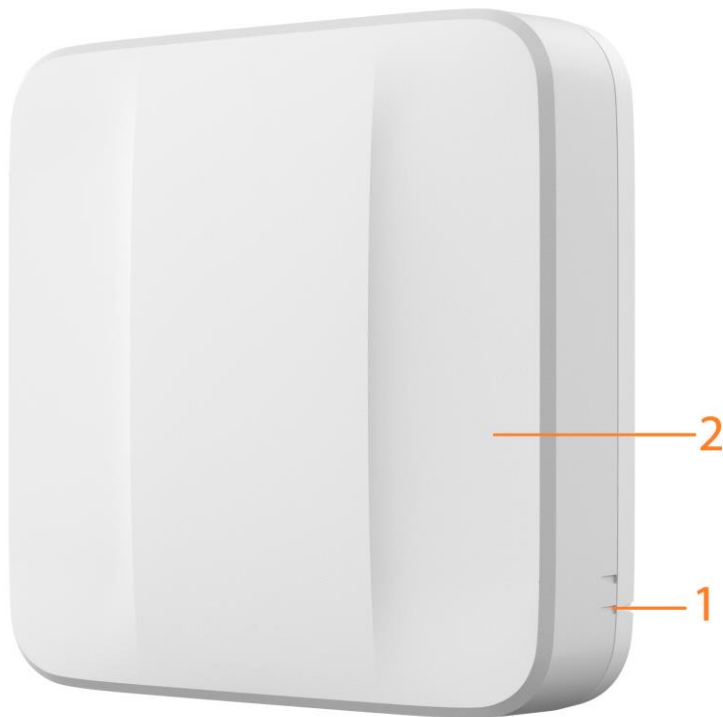


Table 1-1 Components description

No.	Description
1	Guiding mark

No.	Description
2	Front panel

Figure 1-3 Back cover

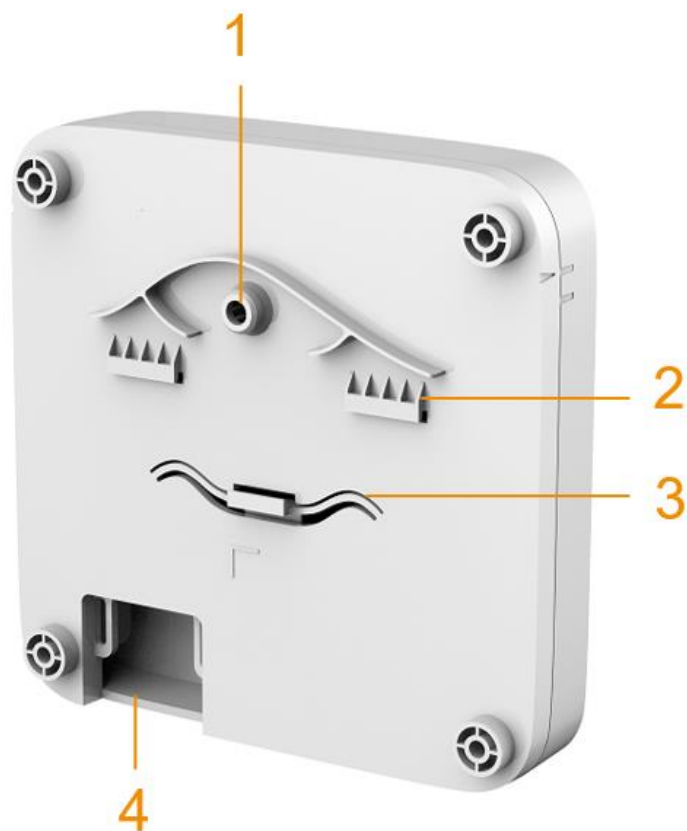


Table 1-2 Back cover description

No.	Description
1	Tamper alarm switch
2	Upper DIN clip
3	Lower DIN clip
4	Wiring outlet

2 Ports Overview

Figure 2-1 Ports

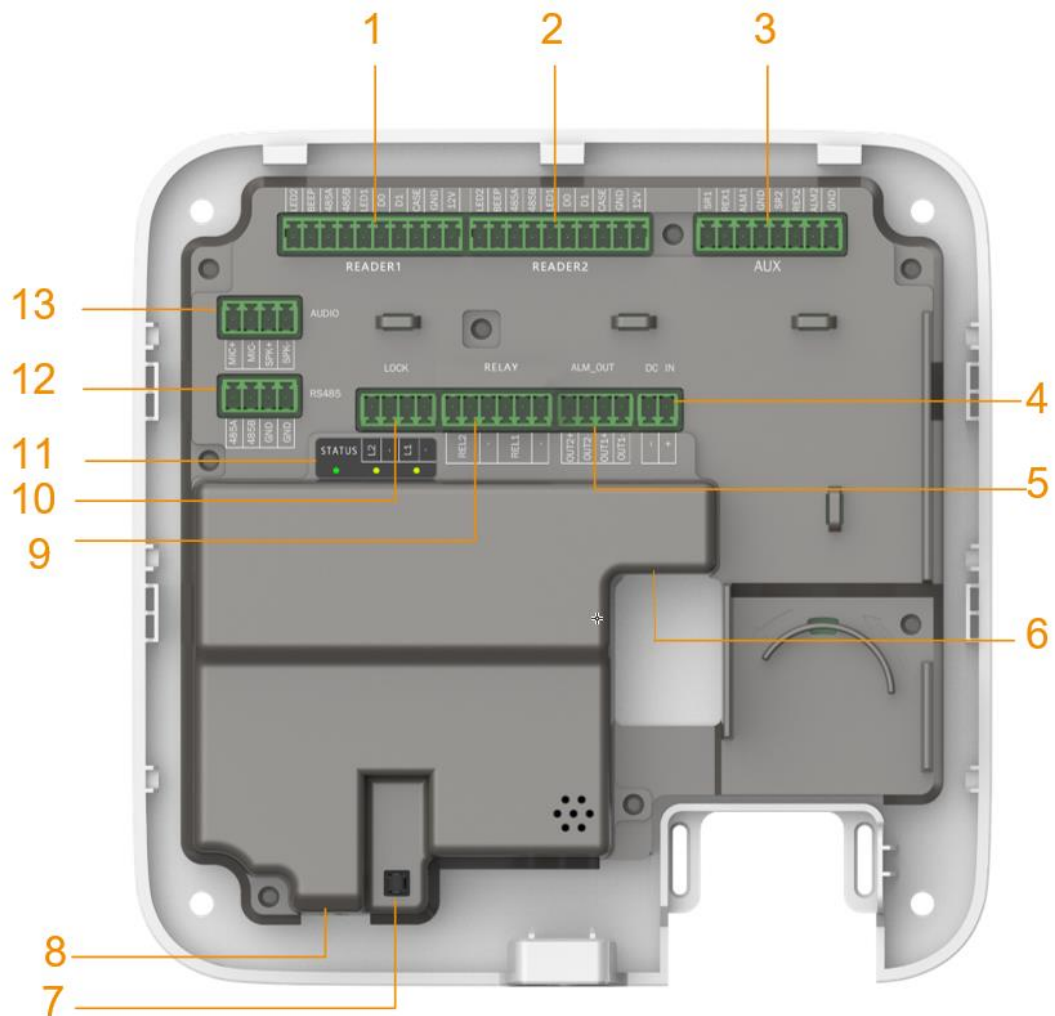


Table 2-1 Ports description

No.	Name	Description
1	READER1	Reader connector
2	READER2	Reader connector
3	AUX	Auxiliary connector (including door detector, door exit button, and alarm input)
4	DC IN	Power connector
5	ALM_OUT	Alarm output connector
6	RJ45	Network connector (PoE)
7	—	Tampering alarm switch
8	—	Reset button
9	RELAY	Relay connector
10	LOCK	Power lock connector

No.	Name	Description
11	STATUS	LED indicator
12	RS485	RS485 connector (not used)
13	AUDIO	Audio connector (not used)

Figure 2-2 Reader connector

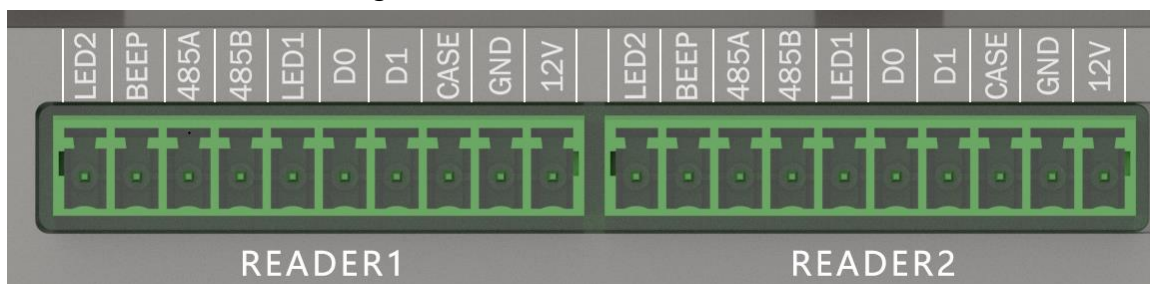


Table 2-2 Reader connector description

Port	Description
12 V	Supplies 12 VDC power for the reader.
GND	Connects the grounding wire.
CASE	Connects the reader tampering alarm.
D1	Connects a Wiegand reader.
D0	
LED1	Signal response. Connects to the signal wire of the Wiegand reader.
RS485B	Connects a RS-485 reader.
RS485A	
BEEP	Reserved port
LED2	Reserved port

Figure 2-3 LED indicator



Table 2-3 Description of LED indicator ports

Port	Port Name	Indicator color	Status
STATUS	Power indicator	Solid green	Working normally.
		Solid red	The system starts .
		Blue light flashes	System is updating.
L2	Lock 2 indicator	Solid yellow and green	Lock open
		Solid red	Lock closed

Port	Port Name	Indicator color	Status
L1	Lock 1 indicator	Solid yellow and green	Lock open

Figure 2-4 Auxiliary I/O ports

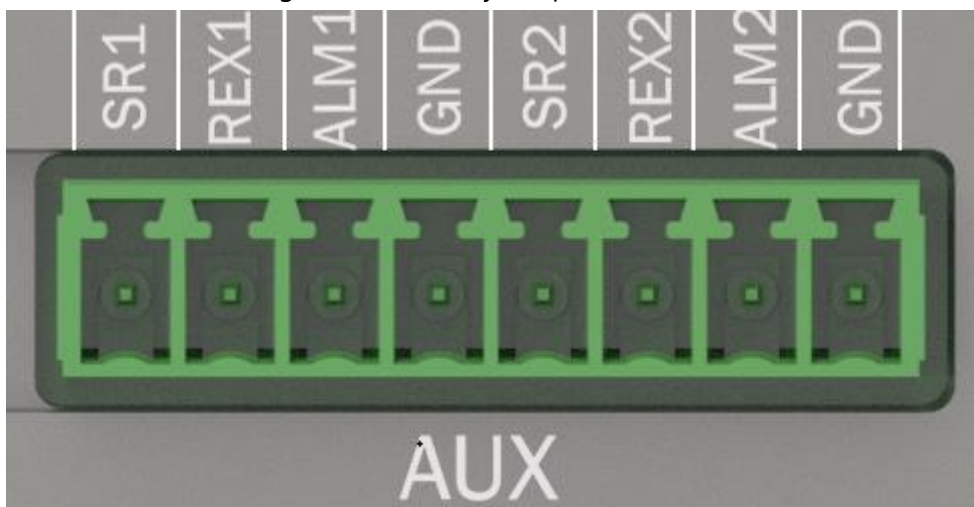


Table 2-4 Description of auxiliary I/O ports

Ports	Description
SR1	Door detector for door 1
REX1	Exit button for door 1
ALM1	Alarm input 1
GND	Grounding wire
SR2	Door detector for door 2
REX2	Exit button for door 2
ALM2	Alarm input 2
GND	Grounding wire

Figure 2-5 Power ports

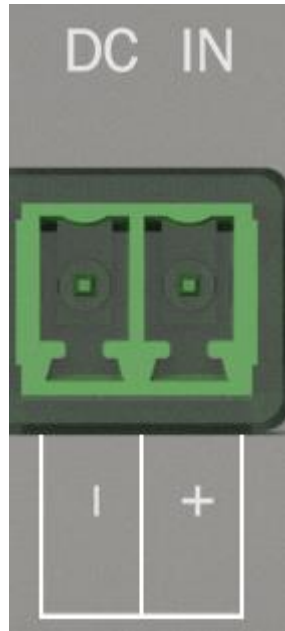


Table 2-5 Description of power ports

Ports	Description
–	Grounding wire
+	12 VDC. For powering the Access Controller when not using Power over Ethernet.

Figure 2-6 Alarm output ports

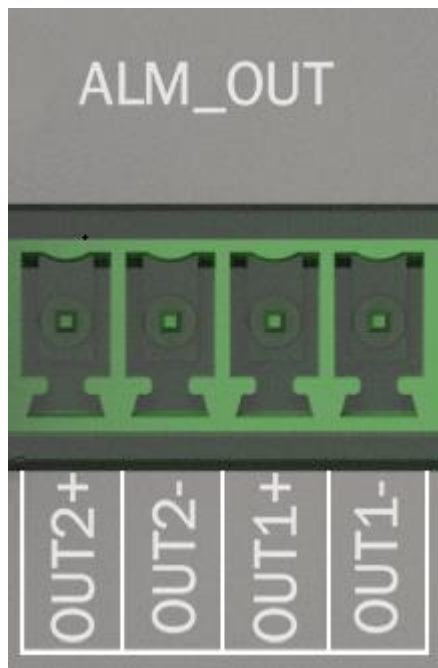


Table 2-6 Description of alarm output ports

Ports	Description
OUT2+	Alarm output 2
OUT2-	

Ports	Description
OUT1+	Alarm output 1
OUT1-	

Figure 2-7 Relay ports

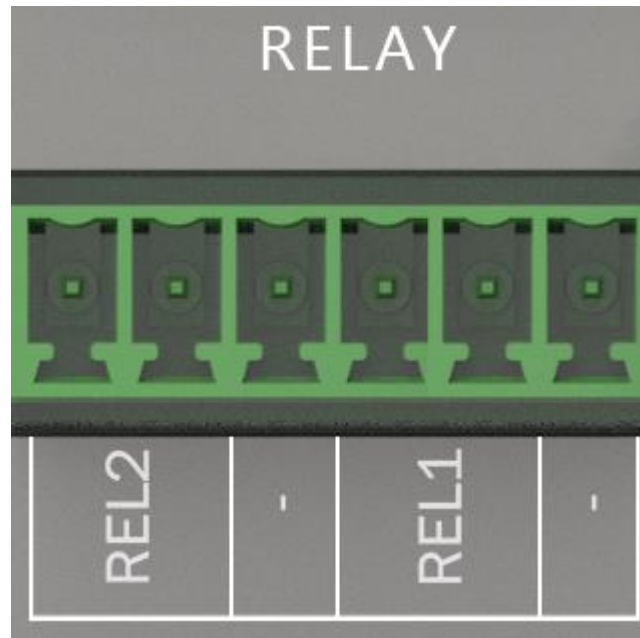


Table 2-7 Description of relay ports


Ports	Description
REL1	<p>Connects to relay devices. Max voltage = +12 VDC; Max load = 500 mA</p> <p> Connect locks to the pins according to the wiring diagram generated through the hardware configuration. For details, see "3 Wiring of Locks".</p>
REL2	
—	Grounding wire.

Figure 2-8 Lock ports



Table 2-8 Description of lock


Ports	Description
L1/L2	Power one or two locks (DC output). The lock connector can also be used to power external devices.
REL2	<p>Connects to lock (12 VDC and Max total load = 1000 mA).</p> <p></p> <ul style="list-style-type: none"> Controls up to 12 V lock. Connects locks and loads to the pins according to the wiring diagram generated through the hardware configuration. For details, see "3 Wiring of Locks".
–	Grounding wire.

Figure 2-9 RS-485 ports

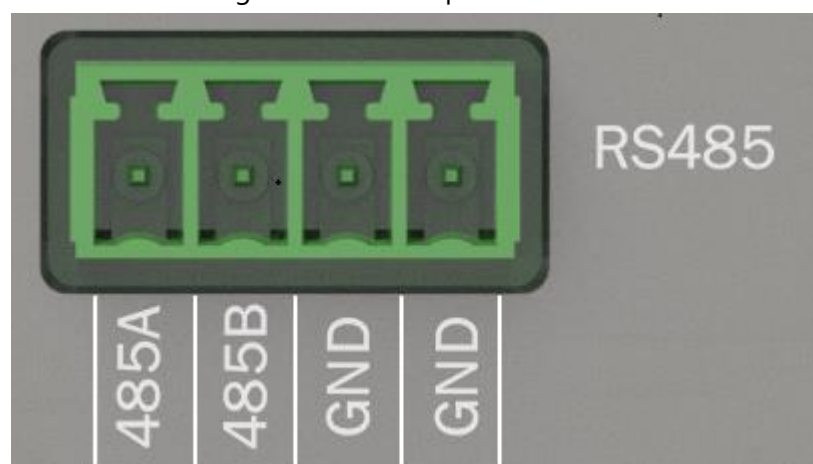


Table 2-9 Description of RS-485

Ports	Description
485A/485B	Reserved port. Not used.
GND	Grounding wire.

Figure 2-10 Audio ports

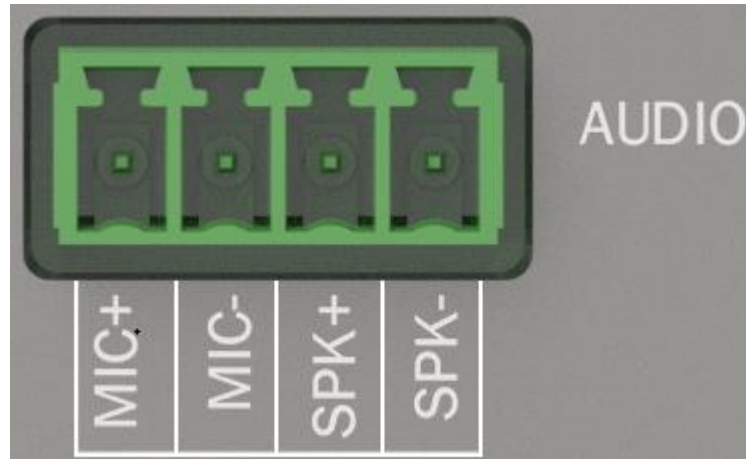


Table 2-10 Description of audio ports

Ports	Description
MIC+	Reserved port. Not used.
MIC-	Grounding wire.
SPK+	Reserved port. Not used.
SPK-	Grounding wire.

3 Wiring of Locks

This section uses lock wiring of two-door solution as an example. The wiring of lock might differ depending on the lock type that you configured.

- Configure lock for **Relay**.
 - ◇ Relay Open = Unlocked: Set the lock to unlock when the relay is open.
 - ◇ Relay Open = Locked: Set the lock to remain locked when the relay is open.
- Configure lock for **12V**.
 - ◇ Fail Secure: Sets the lock to remain locked during power outages.
 - ◇ Fail Safe: Sets the lock to unlock during power outages.

3.1 Wiring of Magnetic Locks

3.1.1 Wiring of Dual Magnetic Locks with PoE (12 V and Relay)

Supplies power for the Access Controller over the same Ethernet cable. One door uses the external power supply, and the other uses the Access Controller to supply power.

1. Select **Relay Open = Unlocked** from the **Relay** list for lock 1 (door 1).

Figure 3-1 Lock 1 (door 1)

Power Supply of Locks

☐ 12V Fail Secure v ?

☒ Relay Relay Open = Unlock... v ?

2. Select **Fail Safe** from the **12V** list for lock 2 (door 2).

Figure 3-2 Lock 2 (door 2)

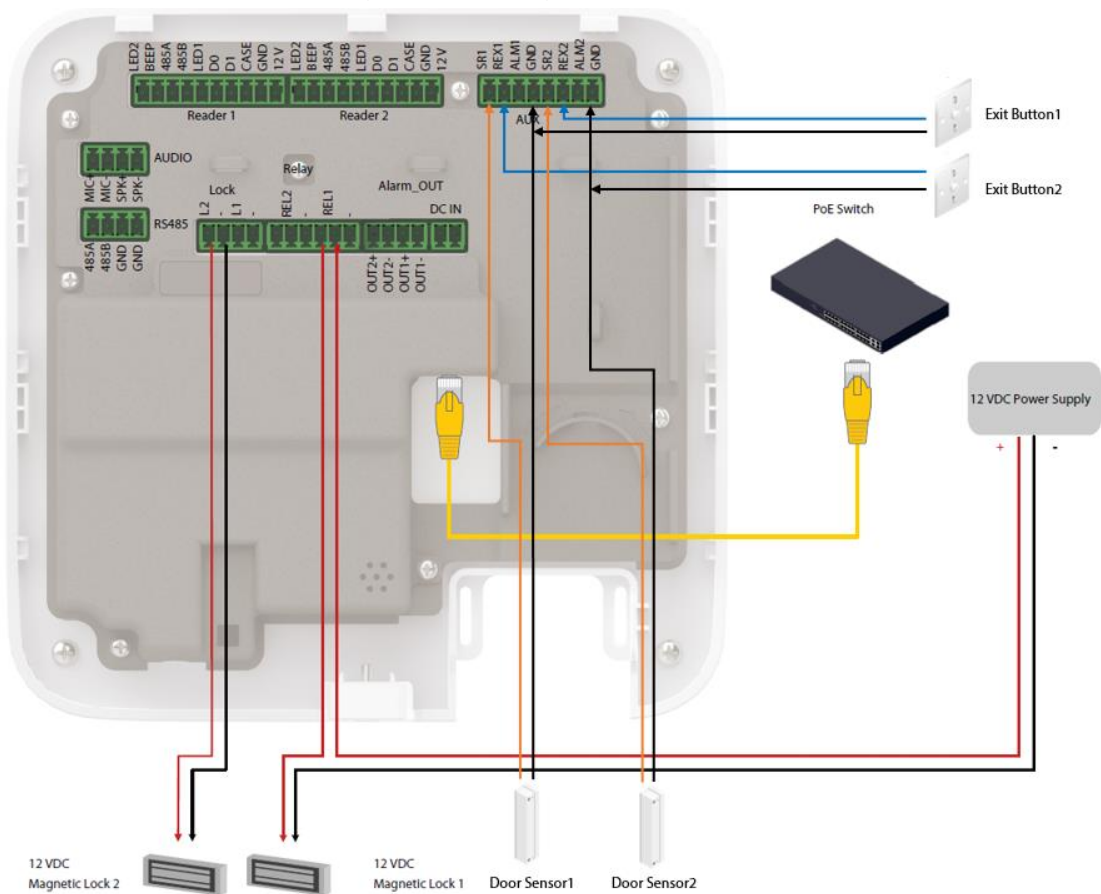
Power Supply of Locks

☒ 12V Fail Safe v ?

☐ Relay Relay Open = Locked v ?

3. Wire the locks according to the diagram below.

Figure 3-3 Wiring of locks



3.1.2 Wiring of Dual Magnetic Locks with 12 V External Power Supply (12 V and Relay)

Supply power for the Access Controller through 12 V external power supply. One door uses the external power supply, and the other uses the Access Controller to supply power.

1. Select **Relay Open = Unlocked** from the **Relay** list for lock 1 (door 1).

Figure 3-4 Lock 1 (door 1)

Power Supply of Locks

☐ 12V

Fail Secure

v
?

☒ Relay

Relay Open = Unlock...

v
?

2. Select **Fail Safe** from the **12V** list for door 2.

Figure 3-5 Lock 2 (door 2)

Power Supply of Locks

☒ 12V

Fail Safe

▼ ?

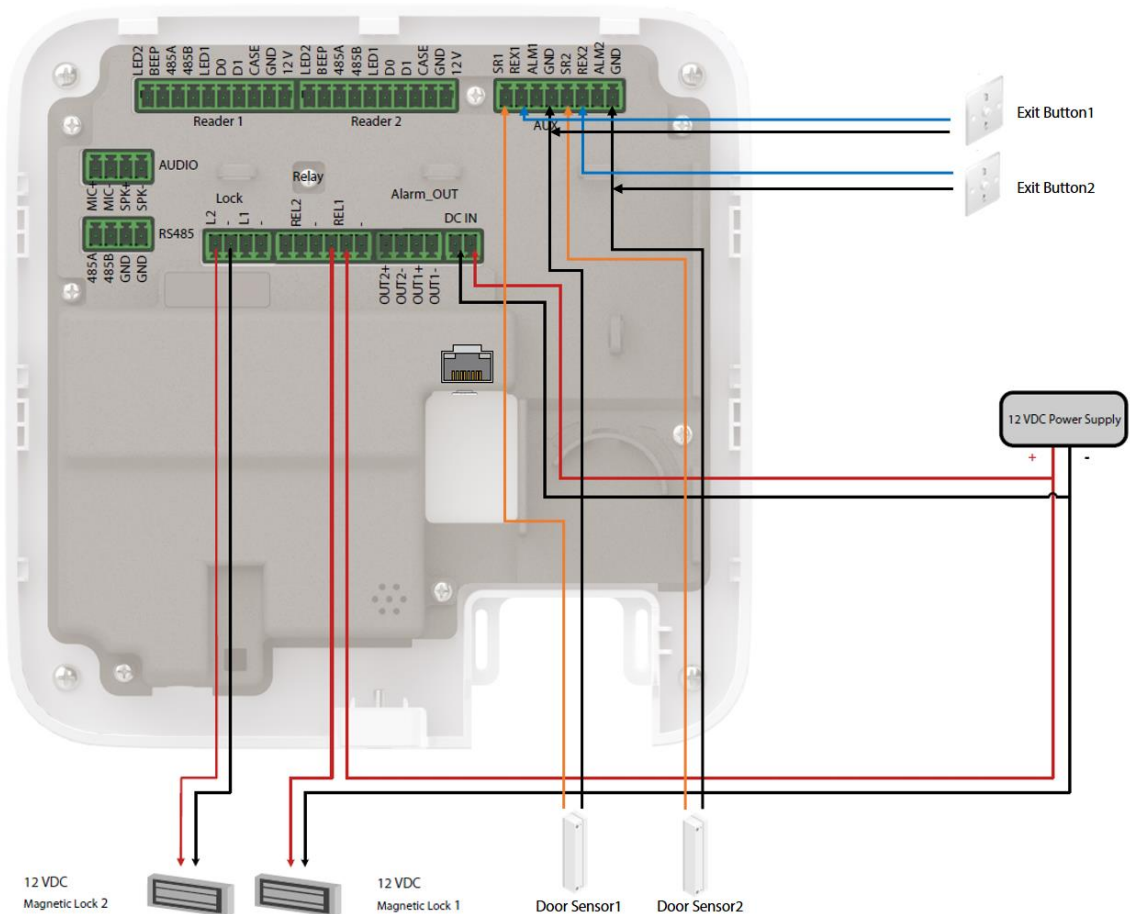
☐ Relay

Relay Open = Locked

▼ ?

3. Wire the locks according to the diagram below.

Figure 3-6 Wiring of locks



3.1.3 Wiring of Dual Magnetic Locks with 12 V External Power Supply (Relay)

Supply power for the Access Controller through 12 V external power supply. Both doors use the external power supply.

1. Select **Relay Open = Unlocked** from the **Relay** for lock 1 (door 1).

Figure 3-7 Lock 1 (door 1)

Power Supply of Locks

☐ 12V

Fail Secure

?

☒ Relay

Relay Open = Unlock...

?

2. Select **Relay Open = Unlocked** from the **Relay** list for lock 2 (door 2).

Figure 3-8 Lock 2 (door 2)

Power Supply of Locks

☐ 12V

Fail Secure

?

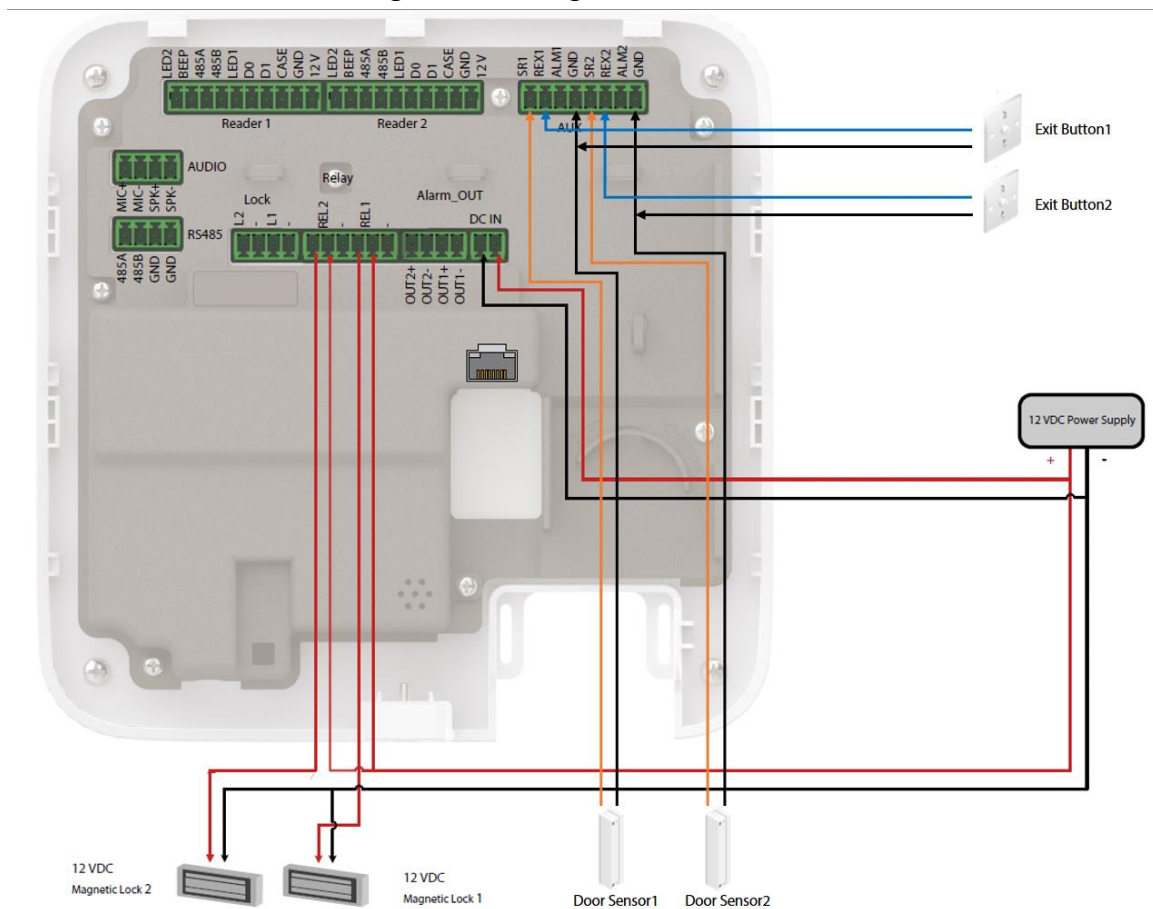
☒ Relay

Relay Open = Unlock...

?

3. Wire the locks according to the diagram below.

Figure 3-9 Wiring of locks



3.1.4 Wiring of 2-in-1 Magnetic Lock with 12 V External Power Supply (Relay)

Supply power for the Access Controller through 12 V external power supply. Both doors use the external power supply.

1. Select **Relay Open = Unlocked** from the **Relay** for lock 1 (door 1).

Figure 3-10 Lock 1 (door 1)

Power Supply of Locks

☐ 12V Fail Secure ?

☒ Relay Relay Open = Unlock... ?

2. Select **Relay Open = Unlocked** from the **Relay** list for lock 2 (door 2).

Figure 3-11 Lock 2 (door 2)

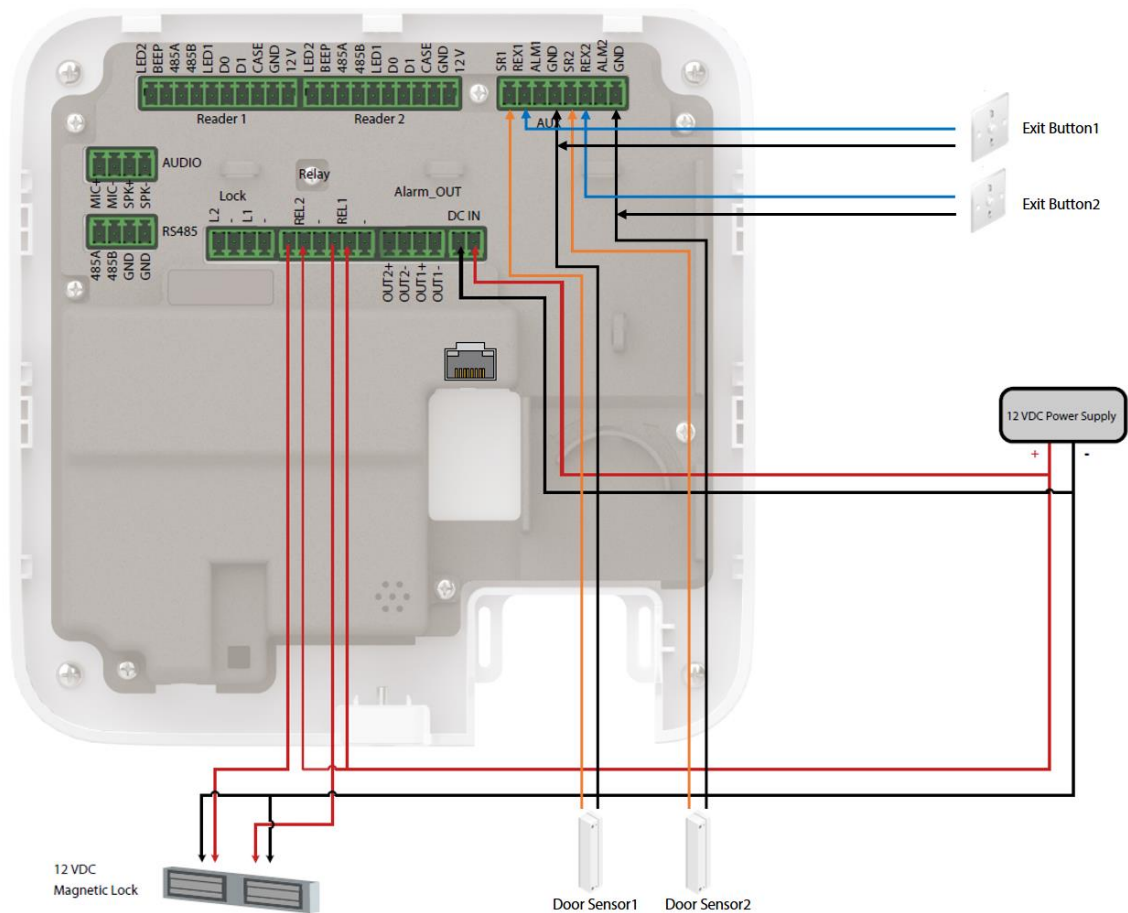
Power Supply of Locks

☐ 12V Fail Secure ?

☒ Relay Relay Open = Unlock... ?

3. Wire the locks according to the diagram below.

Figure 3-12 Wiring of locks



3.2 Wiring of Electric Strike Lock

3.2.1 Wiring of Dual Electric Strikes with PoE

Supplies power for the Access Controller over the same Ethernet cable. and the Access Controller supplies power for both locks.

1. Select **Fail Secure** from the **12V** list for lock 1 (door 1).

Figure 3-13 Lock 1 (door 1)

Power Supply of Locks

☒ 12V

Fail Safe
 ▼
?

☐ Relay

Relay Open = Locked
 ▼
?

2. Select **Fail Secure** from the **12V** list for lock 2 (door 2).

Figure 3-14 Lock 2 (door 2)

Power Supply of Locks

☒ 12V

Fail Safe

▼

?

☐ Relay

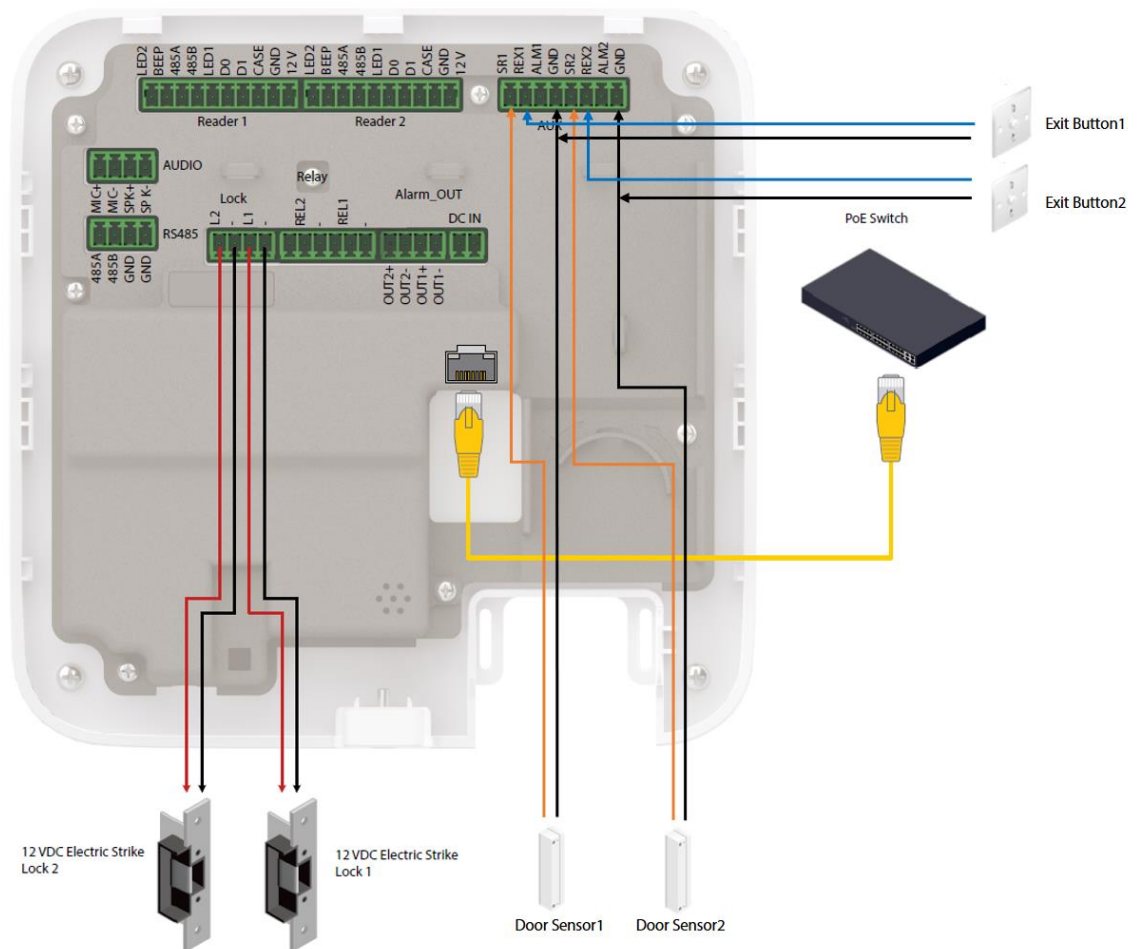
Relay Open = Locked

▼

?

3. Wire the locks according to the diagram below.

Figure 3-15 Wiring of locks



3.2.2 Wiring of Dual Electric Strikes with 12 V External Power Supply

Supply power for the Access Controller through 12 V external power supply, and the Access Controller supplies power for the both locks.

1. Select **Fail Secure** from the **12V** list for lock 1 (door 1).

Figure 3-16 Lock 1 (door 1)

Power Supply of Locks

☒ 12V

Fail Secure

▼

?

☐ Relay

Relay Open = Locked

▼

?

2. Select **Fail Secure** from the **12V** list for door 2.

Figure 3-17 Lock 2 (door 2)

Power Supply of Locks

☒ 12V

Fail Secure

▼

?

☐ Relay

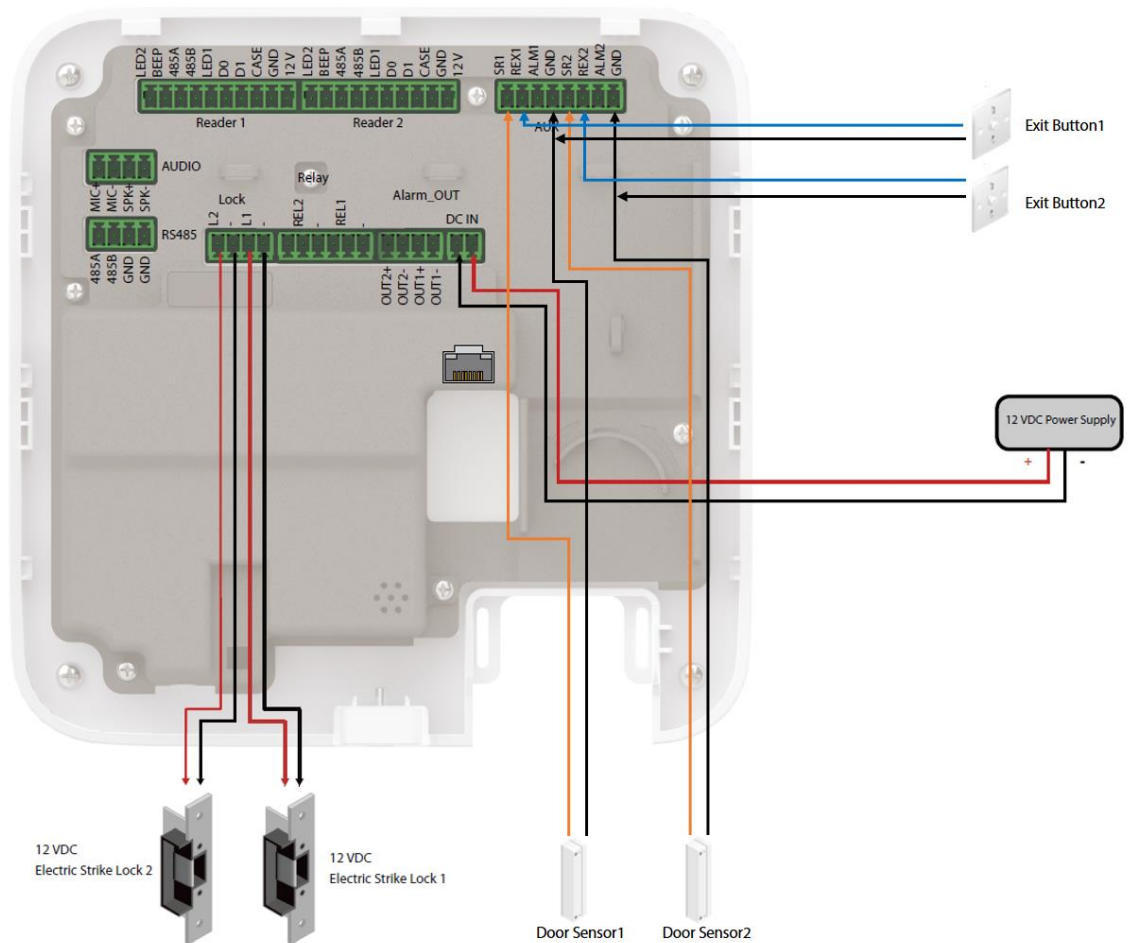
Relay Open = Locked

▼

?

3. Wire the locks according to the diagram below.

Figure 3-18 Wiring of locks



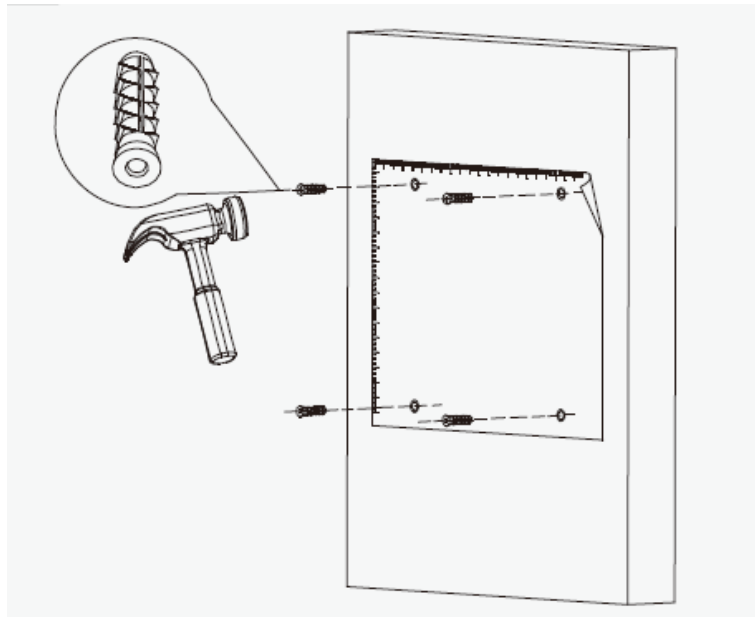
4 Installation

4.1 Wall Mount

Procedure

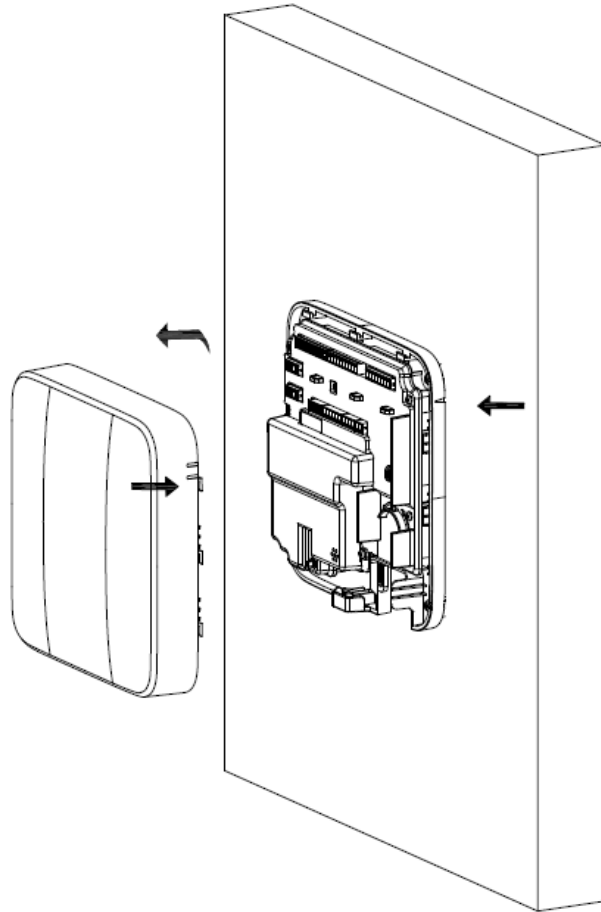
- Step 1 Paste the positioning map to the wall at an appropriate position.
- Step 2 Drill holes through the marks on the map.
- Step 3 Hammer in the expansion tubes, and then remove the map.

Figure 4-1 Hammer in the expansion tubes



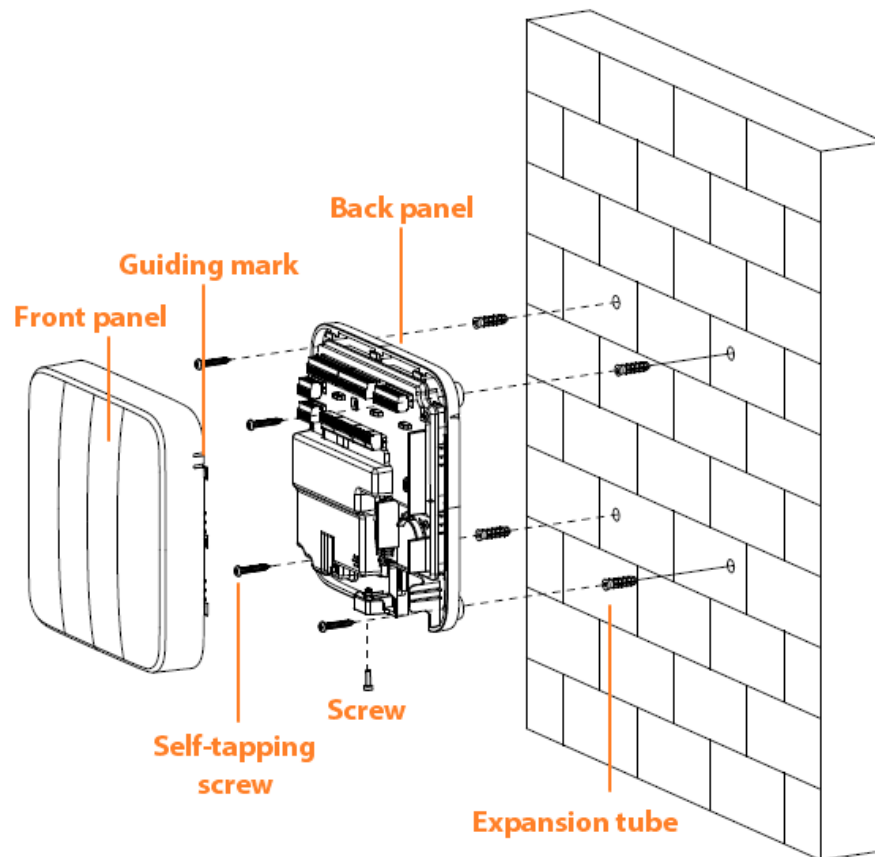
- Step 4 Slide up the front panel of the Access Controller and remove the panel.

Figure 4-2 Remove the front panel



- Step 5 Attach the back panel of the Access Controller to the wall with self-tapping screws.
- Step 6 Wire the Access Controller, bind the wires with nylon cable ties, and then cut off the excess part of the ties.
- Step 7 Align the marks on the front panel with the marks on the back panel, and then slide down the front panel to cover the Access Controller.
- Step 8 Screw a screw into the bottom of the Access Controller to secure it.

Figure 4-3 Mount the Access Controller to the wall



Step 9 Remove the protection film.

4.2 DIN Rail Mount

Procedure

Step 1 Attach the DIN rail to the wall with screws.



The DIN rail does not come with the Access Controller.

Step 2 Hook the lower DIN clip of the back panel onto the bottom of the DIN rail, slightly push upwards the back panel, and then push the back panel backwards to hook the upper DIN clip onto the top of the DIN rail.

Make sure the clips "grip" the rail on both the top and bottom of the rail.



If you want to remove the Access Controller from the rail, simply push upwards on the DIN clip, remove the upper clip off the rail, and then lower the back panel to remove the lower clip off the rail. No screwdrivers or special tools are required.

Figure 4-4 DIN clips

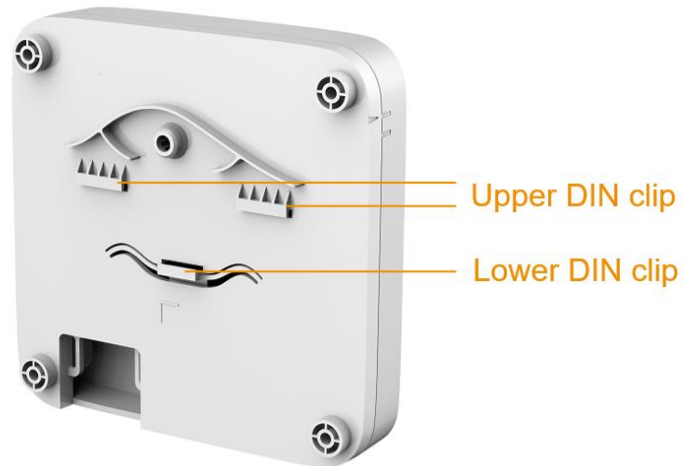
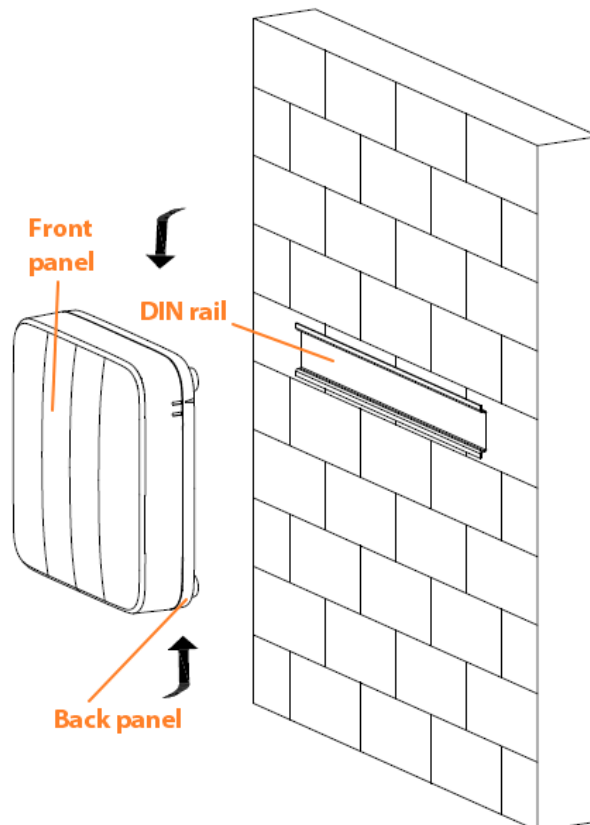


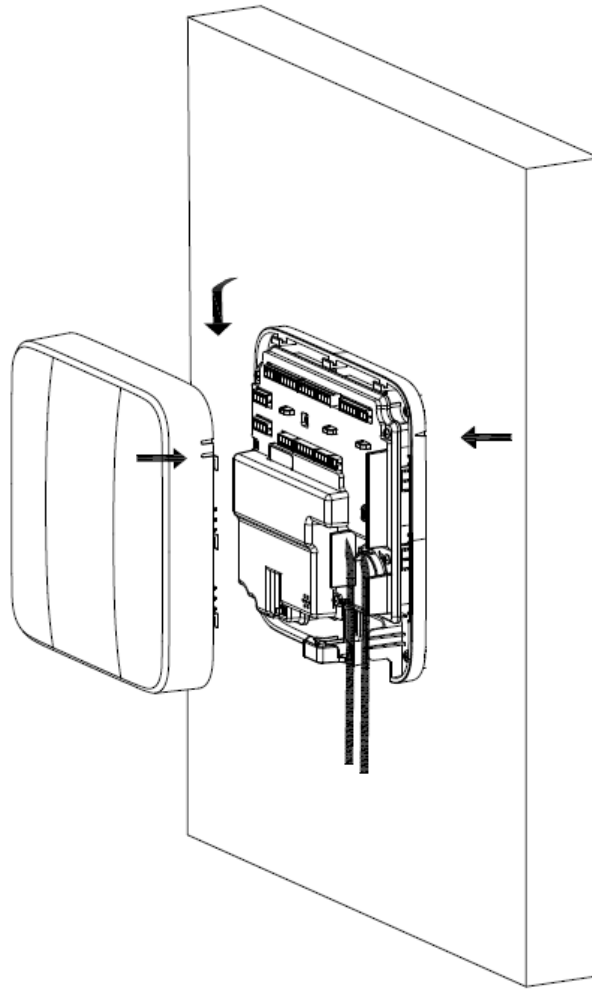
Figure 4-5 Hook DIN clips to the rail



- Step 3 Slide up the front panel of the Access Controller to remove the cover.
- Step 4 Wire the Access Controller, bind the wires with nylon cable ties, and then cut off the excessive part of the ties.
- Step 5 Align the marks on the front panel with the marks on the back panel, and then slide

down the front cover to attach it.

Figure 4-6 Slide down the front cover



Step 6 Screw a screw into the bottom of the Access Controller to secure it.

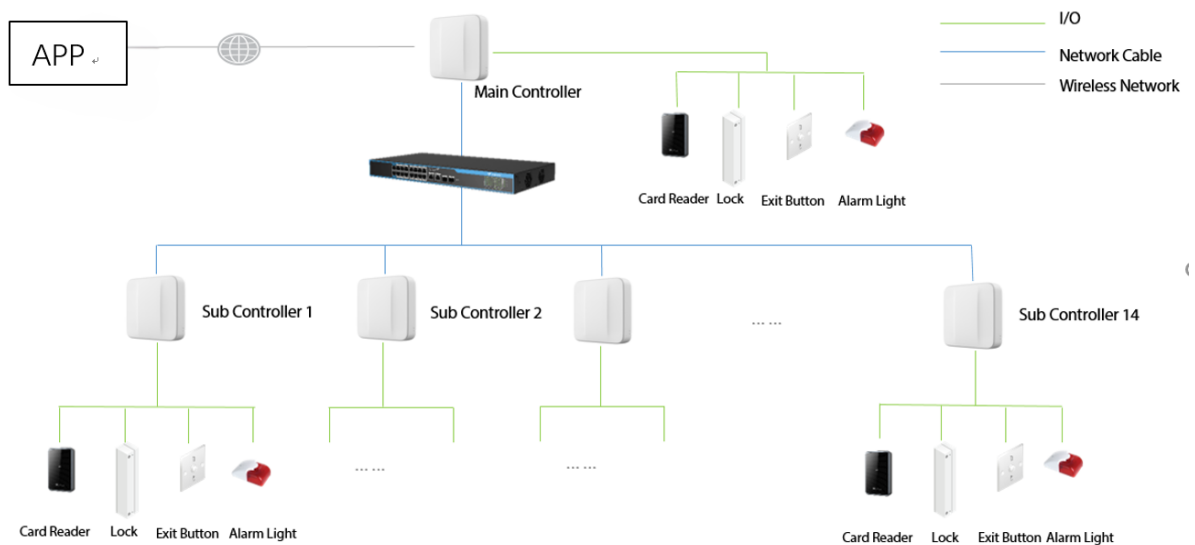
Step 7 Remove the protection film.

5 Access Control Configurations

5.1 Networking Diagram

The main controller comes with a management platform (herein referred as the "platform"). Sub controller needs to be added to the platform of the main controller. The main controller can manage up to 14 sub controllers.

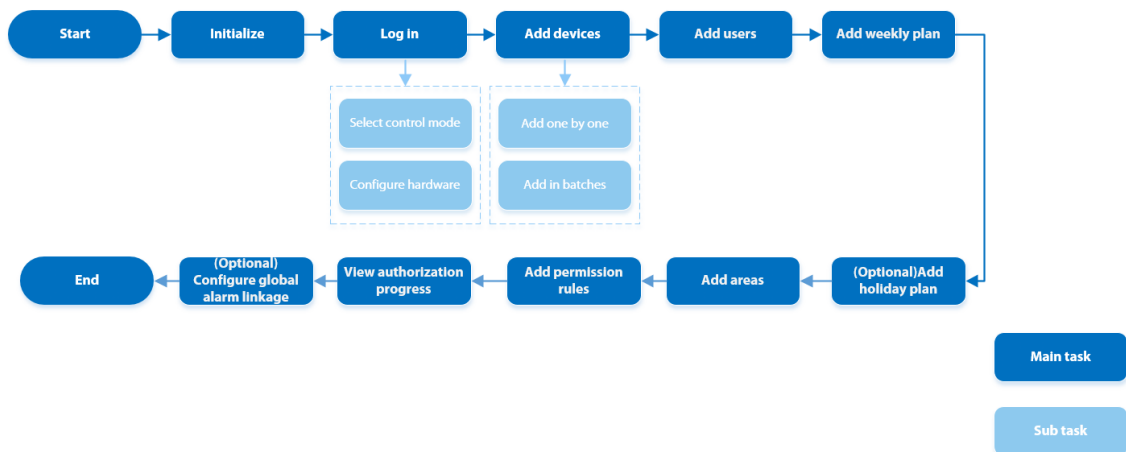
Figure 5-1 Networking diagram



5.2 Configurations of Main Controller

5.2.1 Configuration Flowchart

Figure 5-2 Configuration flowchart



5.2.2 Initialization

Initialize the main controller when you log in to the webpage for the first time or after it is restored to its factory defaults.

Prerequisites


Make sure that the computer used to log in to the webpage is on the same LAN as the main controller.

Procedure

Step 1 Open a browser, go to the IP address (the IP address is 192.168.1.101 by default) of the main controller.



We recommend you use the latest version of Chrome or Firefox.

Step 2 Set the password and email address, and then click .



- The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters: upper case and lower case letters, numbers, and special characters (excluding ' " ; : &). Set a high-security password by following the password strength prompt.
- Keep the password safe after initialization and change the password regularly to improve security.

Figure 5-3 Password settings


Step 3 Configure the system time, and then click .

Figure 5-4 Time zone setting

The screenshot shows a web interface with three tabs: "Password Settings", "Time Zone Setting" (which is active), and "Auto Check for Updates". Below the tabs, there are three settings:

Date Format	Month_Day_Year	▼
Time Zone	(UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi	▼
System Time	12/26/2024 02:01:16 AM	Synchronize PC

Step 4 (Optional) Select **Auto Check for Updates**.

The system automatically check is there any higher version available, and inform the user to update the system. The system automatically checks for new updates, and informs you when a new update is available.

Figure 5-5 Auto check for updates

The screenshot shows a web interface with three tabs: "Password Settings", "Time Zone Setting", and "Auto Check for Updates" (which is active). Below the tabs, there is a checkbox labeled "Auto Check for Updates". Below the checkbox, there is a text box with the label "Notify when a version update is detected". Below the text box, there is a paragraph of text:

To keep you up-to-date on firmware updates, we will collect information on your device such as the name, IP address and serial number of the device, and its firmware version. All collected information will only be used to verify the legitimacy of the device, and to send notifications of updates.

Step 5 Click . Login to the system, then it goes to the **Setup Wizard** page.

5.2.3 Logging In

For first-time login during initialization, you need to follow the login wizard to configure the type of main controller and its hardware.

Procedure

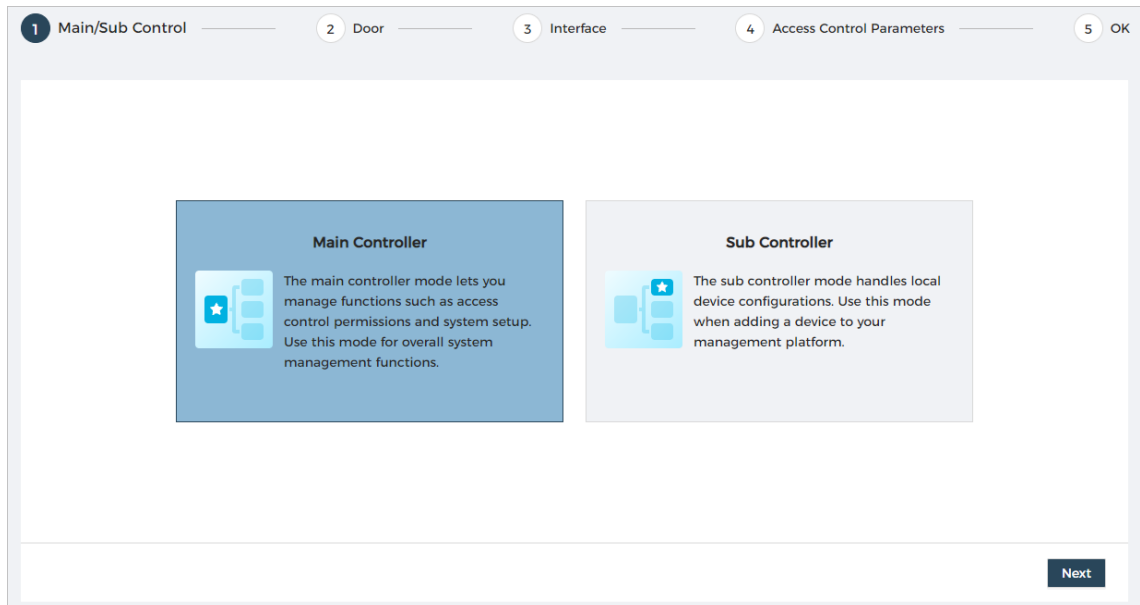
Step 1 On the login page, enter the username and password.



- The default administrator name is admin, and the password is the one you set during initialization. We recommend you change the administrator password regularly to increase the security of the platform.
- If you forget the administrator login password, you can click **Forgot password?**.

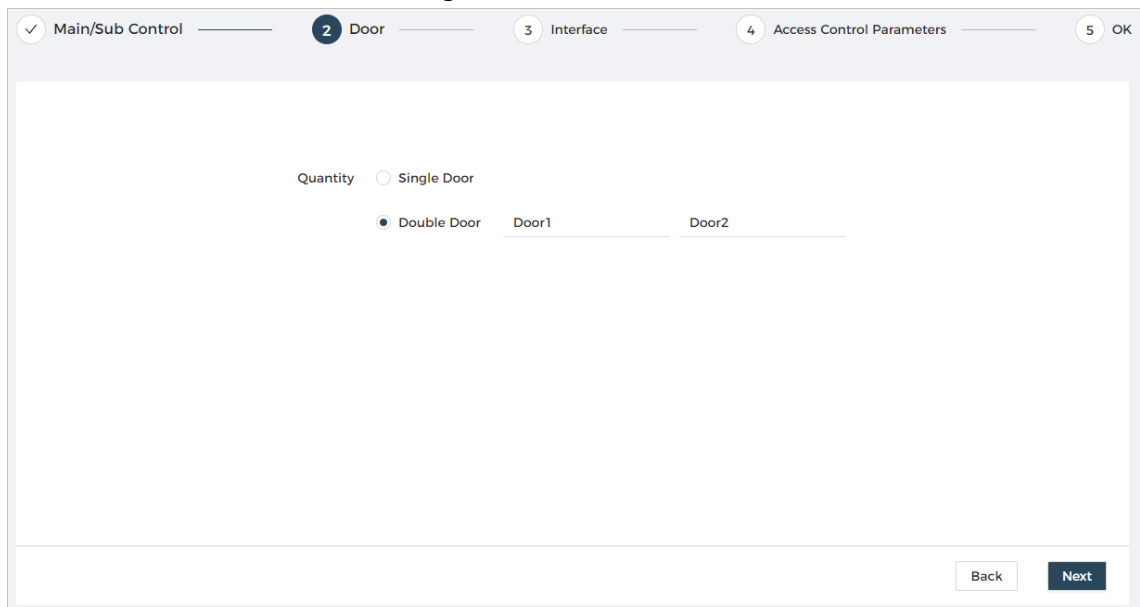
Step 2 Select **Main Control**, and then click **Next**.

Figure 5-6 Main/Sub control



Step 3 Select the number of doors, enter the name of the door, and then click **Next**.

Figure 5-7 Door





Step 4 Configure the parameters of the doors, and then click **Next**.

Figure 5-8 Configure door parameters

The screenshot shows a configuration window titled 'Configure door parameters' with a progress bar at the top indicating steps: Main/Sub Control, Door, Interface (current), Access Control Parameters, and OK. The interface is divided into two sections, 'Door1' and 'Door2'. Each section contains a 'Card Reader' configuration area and a 'Power Supply of Locks' area. In the 'Card Reader' area, there are checkboxes for 'Entry Card Reader', 'Exit Button', and 'Door Sensor'. Below these, the 'Card Reader Proto...' is set to 'Single' (with a dropdown arrow) and 'LED' is selected. The 'Power Supply of Locks' area has radio buttons for '12V' (selected) and 'Relay'. The 'Fail Secure' dropdown is set to 'Fail Secure' and the 'Relay Open = Locked' dropdown is set to 'Relay Open = Locked'. At the bottom right, there are 'Back' and 'Next' buttons.

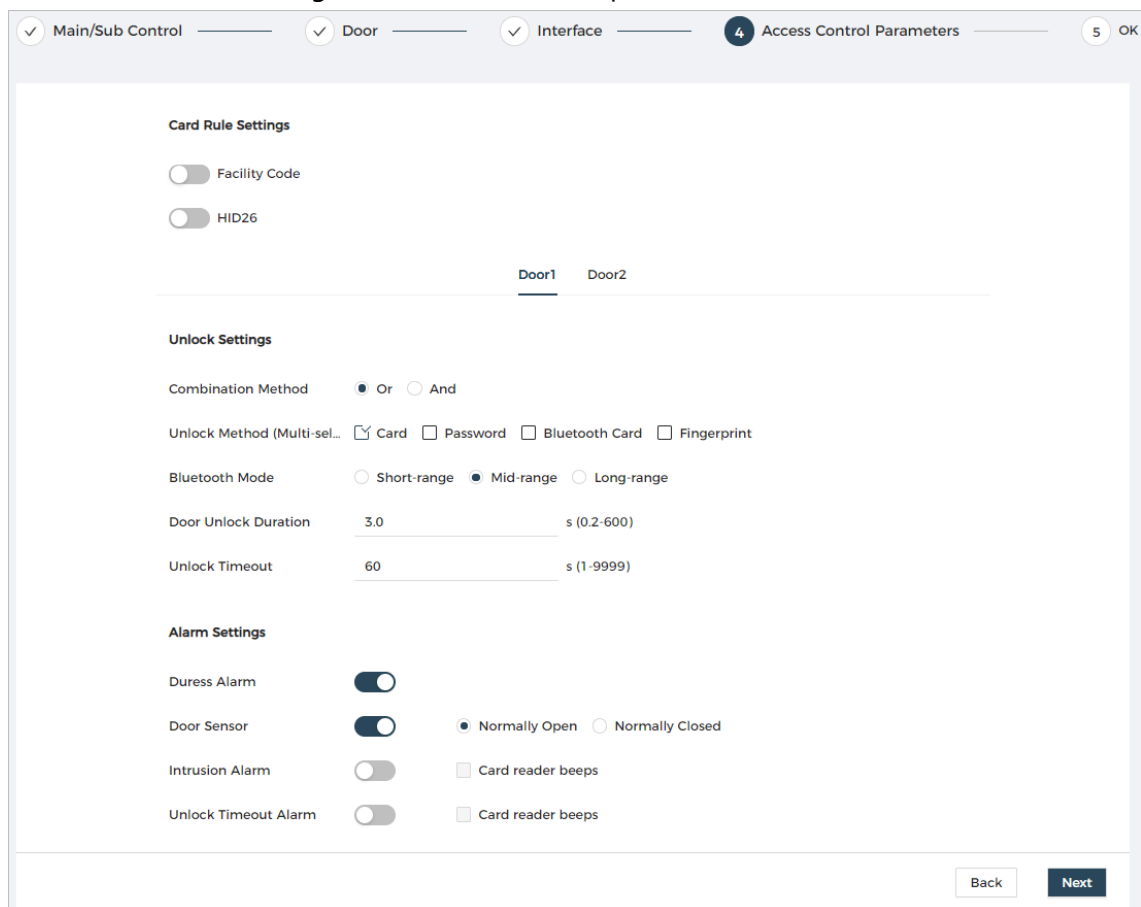
Table 5-1 Parameter description

Parameter	Description
Entry Card Reader	Select the card reader protocol.
Exit Card Reader	<ul style="list-style-type: none"> Wiegand: Connects to a Wiegand reader. You can connect the LED wire to the LED port of the controller, and the reader will beep and flash when the door unlocks. OSDP: Connects to an OSDP reader. RS-485: Connects to a RS-485 reader.
Exit Button	<p>Connects to an exit button.</p> <p> Exit button is not available when Single Door is selected in the previous step.</p>
Door Sensor	Connects to a door detector.

Parameter	Description
Power Supply of Locks	<ul style="list-style-type: none"> • 12 V: The controller provides power to the lock. <ul style="list-style-type: none"> ◇ Fail secure: When the power is interrupted or fails, the door stays locked. ◇ Fail safe: When the power is interrupted or fails, the door automatically unlocks to let people leave. • Relay: The relay supplies power for the lock. <ul style="list-style-type: none"> ◇ Relay open = locked: Sets the lock to remain locked when the relay is open. ◇ Relay open = unlocked: Sets the lock to unlock when the relay is open. <p> The electromagnetic lock unlocks in an instant and locks again immediately when the access controller is in the soft reboot.</p>

Step 5 Configure access control parameters.

Figure 5-9 Access control parameters



Step 6 In **Unlock Settings**, select **Or** or **And** from **Combination Method**.


- Or: Use one of the selected unlock methods to authorize opening the door.
- And: Use all of the selected unlock methods to authorize opening the door.



Bluetooth card cannot be selected when you set the combination method to **And**.

Step 7 Select the unlock methods, and then configure the other parameters.

Table 5-2 Unlock settings description

Parameter	Description
Unlock Method (Multi-select)	Supports unlocking through card, fingerprint, password or Bluetooth card. The Bluetooth card function is turned off by default.
Bluetooth Mode	<p>The Bluetooth card must be a certain distance away from the access control device to exchange data and unlock the door. Following are the ranges that are most suitable for it.</p> <ul style="list-style-type: none">• Short-range: The Bluetooth unlock range is less than 0.66 ft (0.2 m).• Mid-range: The Bluetooth unlock range is less than 6.56 ft (2 m).• Long-range: The Bluetooth unlock range is less than 32.81 ft (10 m). <p> The Bluetooth unlock range might differ depending on models of your phone and the environment.</p>
Door Unlock Duration	After a person is granted access, the door will remain unlocked for a defined time for them to pass through. It ranges from 0.2 seconds to 600 seconds.
Unlock Timeout	A timeout alarm is triggered when the door remains unlocked for longer than the defined value.

Step 8 In **Alarm Settings**, configure the alarm parameters.

Table 5-3 Description of alarm parameters

Parameter	Description
Duress Alarm	An alarm will be triggered when a duress card, duress password or duress fingerprint is used to unlock the door.
Door Sensor	Select the type of door detector.
Intrusion Alarm	<ul style="list-style-type: none">• When the door detector is enabled, an intrusion alarm will be triggered if the door is opened abnormally.• A timeout alarm will be triggered when the door remains unlocked for longer than the defined unlock time.• When Card reader beeps is enabled, the card reader beeps when the intrusion alarm or timeout alarm is triggered.
Unlock Timeout Alarm	

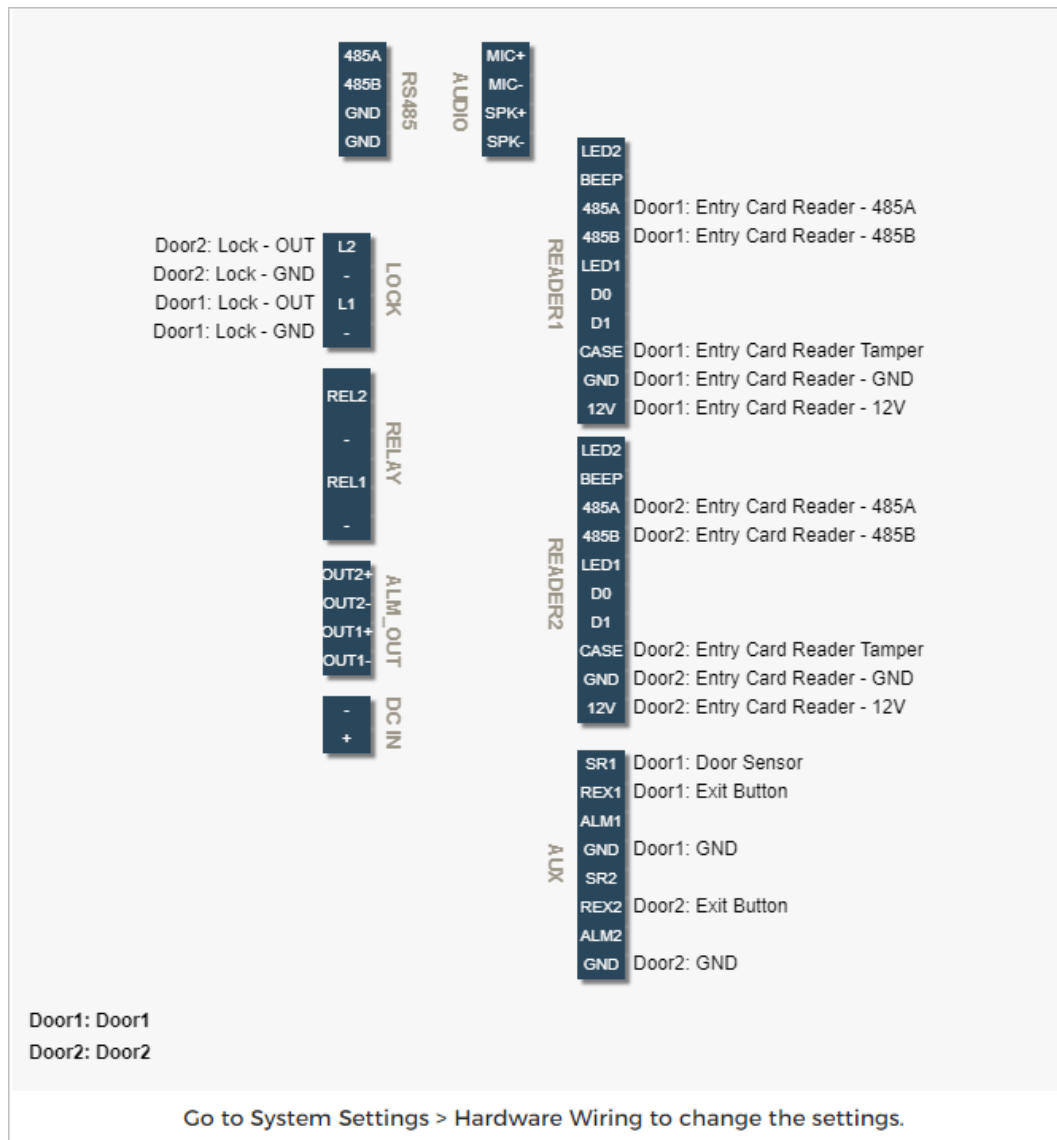
Step 9 Click **Next**.

A wiring diagram is generated based on your configurations. You can wire the device according to the diagram.



The image below is for reference only.

Figure 5-10 Wiring diagram



Step 10 Click **Apply**.

- You can go to **System Settings > Hardware Wiring** to change the settings after you successfully log in to the platform.
- Click **Download Image** to download the diagram to your computer.

Related Operations

If you want to change the settings of the hardware, go to **System Settings > Hardware Wiring**.

5.2.4 Adding Devices

You can add devices to the management platform of the main controller in batches or one by one. If the controller was set to the main controller while you were going through the login wizard, you can add and manage sub controllers through the Platform.



Only the main controller comes with a management platform.

5.2.4.1 Adding Devices One by One

You can add sub controllers to the main controller one by one.

Procedure

Step 1 Click **Device Management**, and then click **Add**.

Step 2 Enter the device information.

Figure 5-11 Device information

The 'Add' dialog box contains the following fields:

- * Device Name
- Add Mode
- IP
- IP Address: 0 . 0 . 0 . 0
- * Port: 80
- * Username
- * Password

Table 5-4 Device parameters Description

Parameter	Description
Device Name	Enter the name of the access controller. We recommend you name it after its installation area.
Add Mode	Select IP to add the access controller by entering its IP address.
IP Address	Enter the IP address of the controller.
Port	The port number is 80 by default.
Username	Enter the username and password of the access controller.
Password	

Step 3 Click **OK**.

The added controllers are displayed on the **Device Management** page.

Figure 5-12 Successfully added devices

Device Management Page Summary:

- Buttons: Add, Device Search, Modify IP, Sync Time, Delete
- Counts: Total Devices 1, Online Devices 1
- Table Headers: No., Device Name, IP Address, Device Type, Model Name, SN, Port, Connection Status, Settings
- Table Data:

1	AC001TEST01MSS	192.168.1.1	Access Controller	GTP-EST-1		80	Online	
---	----------------	-------------	-------------------	-----------	--	----	--------	--



If the controller was set as the main controller while you were going through the login wizard, the controller will be added to the management platform automatically and function as both the main controller and sub controller.

Related Operations

- ✎ : Edit the information on the device.



Only sub controllers support the below operations.

- ➔ : Go to the webpage of the sub controller.
- 🚪 : Log out of the device.
- 🗑 : Delete the device.

5.2.4.2 Adding Devices in Batches

We recommend you use the auto-search function when you add sub controllers in batches. Make sure the sub controllers you want to add are on the same network segment.

Procedure

Step 1 Click **Device Management**, and then click **Search Device**.

Figure 5-13 Device search

No.	Device Type	Initialization Status	IP Address	Port	MAC Address
1	ASI6213S-PW	Initialized		80	
2	C-2PA	Initialized		80	
3	AC02B3-KA	Initialized		80	

- Click **Start Search** to search for devices on the same LAN.
- Enter a range for the IP segment, and then click **Search**.

All devices that were searched for will be displayed.



You can select devices from the list, and click **Device Initialization** to initialize them in batches.

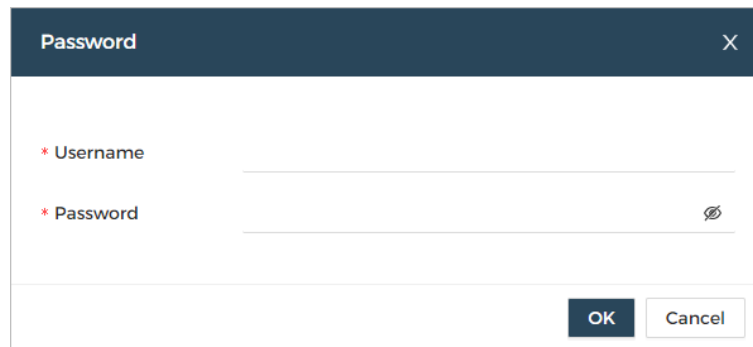


To ensure the security of devices, initialization is not supported for devices on different segments.

Step 2 Select the access controllers that you want to add to the platform, and then click **Add**.

- Step 3 Enter the username and password of the sub controller, and then click **OK**. The added sub controllers are displayed on the **Device Management** page.

Figure 5-14 Password



Related Operations

- Modify IP: Select added devices, and then click **Modify IP** to change their IP addresses.
- Sync Time: Select added devices, and then click **Sync Time** to sync the time of the devices with the NTP server.
- Delete: Select the devices, and then click **Delete** to delete them.

5.2.5 Adding Users

Add users to groups. Enter basic information for users and set verification methods to verify their identities.

Related Operations

- Export all the users to Excel: On the **User Management** page, click **Export** to export all users. You can also import the exported user information to other controllers.



To prevent data loss caused by force majeure damage to the equipment, it is recommended to regularly export user data for backup purposes.

- Import users: On the **User Management** page, click **Import** > **Download Template**, enter user information in the template, and then click **Import** > **Import** to import all users.
- Extract all the users: On the **User Management** page, click **More** > **Extract Person Info**, and select a device to extract all the users from the sub controller and send them to them the Platform of the main controller.

5.2.5.1 Adding Group

- Step 1 Select **User Management**.
- Step 2 Click **+**.
- Step 3 Enter the name of the group, and then click **Add**.



The default group cannot be deleted.

Figure 5-15 Add group

The screenshot shows a modal dialog titled 'Add'. It contains two input fields: 'Organization' and 'Default Group' (which has a dropdown arrow). Below these is a 'Group Name' input field. At the bottom right, there are two buttons: 'Add' and 'Cancel'.

5.2.5.2 Adding Roles

Procedure

Step 1 On the home page, select **User Management**.

Step 2 Create roles.



- The following roles already exist and cannot be modified or deleted: Default, Manager, Administrator, Visitor and Employee.
- The only general user type with manager role has the highest authority and it is not limited by advanced access rules, such as first card unlock, multi-person unlock, anti-passback, always closed door and unlock methods.

1. Click +.
2. Enter the name of the role, and then click **Add**.

5.2.5.3 Configuring Basic User Information

Procedure

Step 1 Select **User Management**.

Step 2 Add users.

- Add users one by one.
 1. Select user group from the left, click **Add**, and then enter the basic information for the user.

Figure 5-16 Basic information on the user

The screenshot shows a modal window titled 'Add' with a close button (X) in the top right corner. It has two tabs: 'General' (selected) and 'Authentication'. The 'General' tab contains the following fields:

- * User ID**: A text input field with an information icon.
- * User Name**: A text input field.
- * Group**: A dropdown menu showing 'Default Group\Group 1'.
- * User Type**: A dropdown menu showing 'General'.
- Valid from**: A date and time picker showing '12-25-2024 12:00:00 AM'.
- Valid to**: A date and time picker showing '12-31-2037 11:59:59 PM'.
- Email**: A text input field.
- * Use limit**: A dropdown menu showing 'Unlimited'.

At the bottom right, there are three buttons: 'Add' (highlighted in dark blue), 'Add More' (light blue), and 'Cancel' (white with a grey border).

Table 5-5 Parameter description

Parameter	Description
User ID	The ID of the user.
User Name	The name of the user.
Group	The group that the user belongs to.
User Type	<p>The type of user.</p> <ul style="list-style-type: none"> • General: General users can unlock the door. • VIP: When the VIP unlocks the door, service personnel will receive a notice. • Guest: Guests can unlock the door within a defined period or for a defined number of times. After the defined period expires or the number of times for unlocking runs out, they cannot unlock the door. • Staff: Staff users will have their permissions recognized, but they have no permission to unlock the door. • Blocklist: When users in the blocklist unlock the door, service personnel will receive a notification. • Manager: Manager users enjoys the highest permissions, which will not be affected by unlocking mode or door status. • Other: When they unlock the door, the door will stay unlocked for 5 more seconds.
Valid from	Set the period that the access permissions of the person are effective.
Valid to	
Email	The email address must be the same as the one that was used to sign up for PRO-X.
Use limit	The number of times that a guest user can unlock the door.

2. Click **Add**.

You can click **Add More** to add more users.

- Add users through importing the template.
 1. Click **Import** > **Download Template** to download the user template.
 2. Enter user information in the template, and then save it.
 3. Click **Import** > **Import**, and upload the template to the platform.
The users are added to the platform automatically.
- Use **Batch Add** to easily add users.
 1. Click **Batch Add**.
 2. Enter the start number of the user ID, and the number of total users.
The platform will generate a sequence of numbers starting from the defined user ID. For example, if the **User ID** is 001, and the **Total Users** is 5, the system will generate a sequence of numbers from 001 to 005.

Figure 5-17 Batch add

Batch Add

* User ID

001

* Total Users

5

Group

Default Group\Group 1

Effective Time

12-25-2024 12:00:00 AM → 12-31-2037 11:59:59 PM

User ID	Card Number
001	
002	
003	
004	
005	

Issue Card Config

Card Reader

Enrollment Reader

Modify

Card Number

Press the Enter key to enter.

Start Issuing Cards

Add

Cancel

3. Select the group, and set the effective time.
4. Issue cards to the users in batches.
You can manually enter the card number, or use the enrollment reader or card

reader to read the card number.

5.2.5.4 Adding Authentication Methods

Add password, cards, fingerprint or Bluetooth cards to users, so that users can unlock the door through authentication. Each user can have up to 1 password, 5 IC/ID cards, 3 fingerprints, and 5 Bluetooth cards.

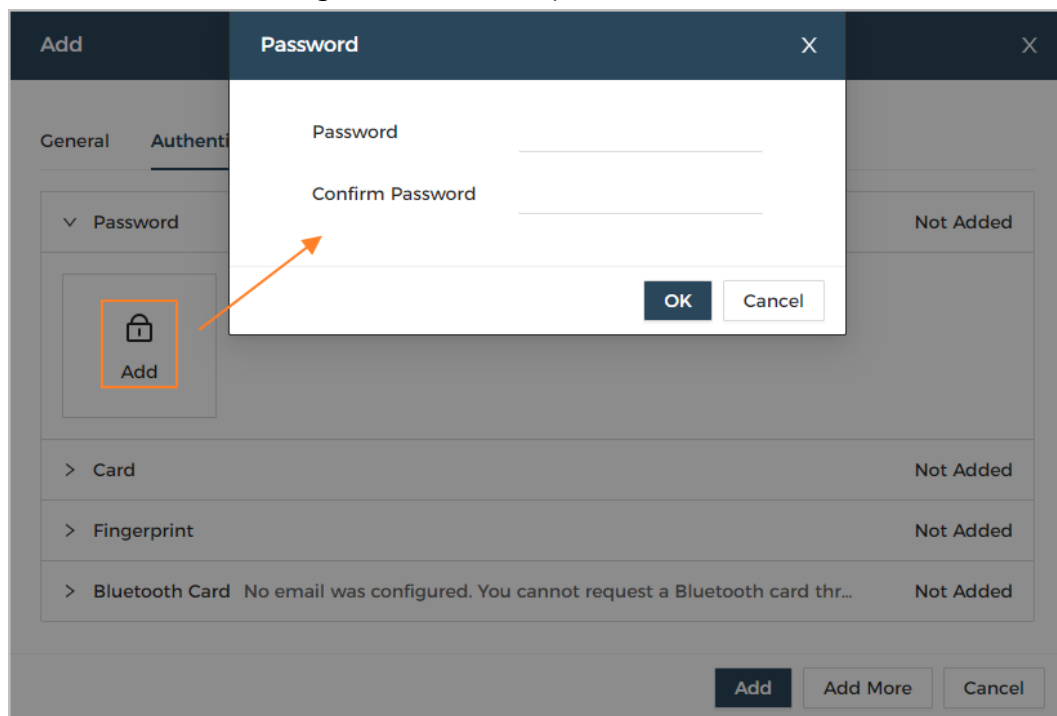
5.2.5.4.1 Adding Passwords

Add passwords to users for them to gain access by entering their password.

Procedure

- Step 1 When adding a user, click the **Authentication** tab.
- Step 2 Click **Add**, and then enter and confirm the password.
- Step 3 Click **OK**.

Figure 5-18 Add the password





- If Pin code authentication is not enabled, you can unlock the door by entering the unlock password in the format of **user ID#password#**. For example, if the user ID is 123, and the password you set is 12345, and then you must enter **123#12345#** to unlock the door.
- If Pin code authentication is enabled, you can unlock the door by entering the unlock password in the format of **password#**. For example, if the user ID is 123, and the password you set is 12345, and then you must enter **12345#** to unlock the door.

5.2.5.4.2 Adding Cards

Add IC cards or ID cards to users for them to gain access by swiping their cards.

Procedure

Step 1 (optional) Before you assign cards to users, set the card type and the type of card number.

1. On the **User Management** page, select **More > Card Type**.
2. If you plan to issue cards through using enrollment reader, select a card type, and then click **OK**.



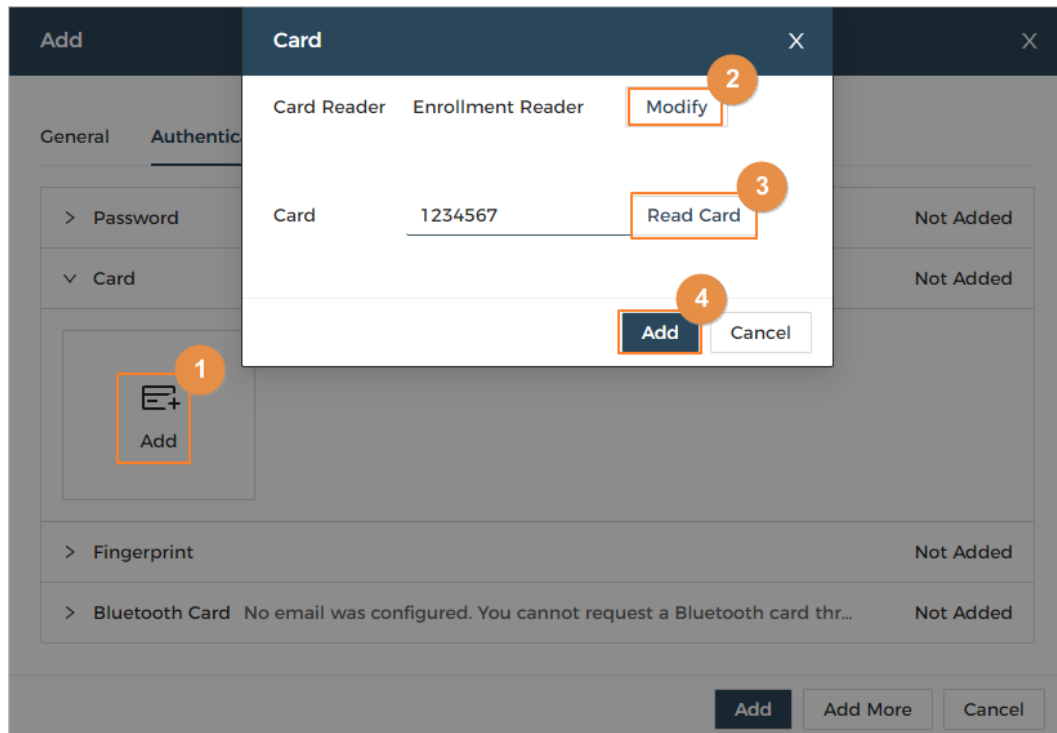
Make sure that the card type is the same as the card type that will be issued when you plan on issuing cards through using enrollment reader.

3. Select **More > Card No. System**.
4. Select decimal format or hexadecimal format for the card number.

Step 2 When adding a user, click the **Authentication** tab, and then click **Card** to add cards. 4 methods are available to add cards.

- Enter the card number manually.
 1. Click **Add**.
 2. Enter the card number, and then click **Add**.
- Use the enrollment reader to read the card number.

Figure 5-19 Use the enrollment reader to read the card number



1. Click **Add**.
2. Click **Modify**, and then select **Enrollment Reader**.
Make sure that the card enrollment reader is connected to your computer.
3. Follow the on-screen instructions to download and install the plug-in.
4. Click **Read Card**, and then swipe the cards on the enrollment reader.
A 60-second countdown is displayed to remind you to swipe the card, and the system will read the card number automatically. If the 60-second countdown expires, click **Read Card** again to start a new countdown.
5. Click **Add**.
- Use the card reader to read the card number.
 1. Click **Add**.
 2. Click **Modify**, and then select a card reader.
Make sure that the card reader is connected to the access controller.
 3. Click **Read Card**, and then swipe the cards on the card reader.
A 60-second countdown is displayed to remind you to swipe the card, and the system will read the card number automatically. If the 60-second countdown expires, click **Read Card** again to start a new countdown.
 4. Click **Add**.
- Add cards in batches: Issue cards to users in batches.
 1. On the **User Management** page, click **Batch Issue Cards**, and then select **Issue Cards to Selected Users** or **Issue Cards to All Users**.
 2. You can manually enter the card number, or click **Modify** to issue cards through the enrollment reader or card reader.

Figure 5-20 Issue cards through the enrollment reader or card reader

Batch Issue Cards

Card

Bluetooth Card

Issue Cards

User ID	User Name	Card Number	Hide User
123	123		⊖
124	124		⊖

User ID

124

User Name

124

User Type

General

Email

Group

Group 1

Effective Time

2024-12-25 00:00:00-2037-12-31 23:59:59

Issue Card Config

Card Reader

Enrollment Reader

Modify

Card Number

Press the Enter key to enter.

Start Issuing Cards

OK

Cancel

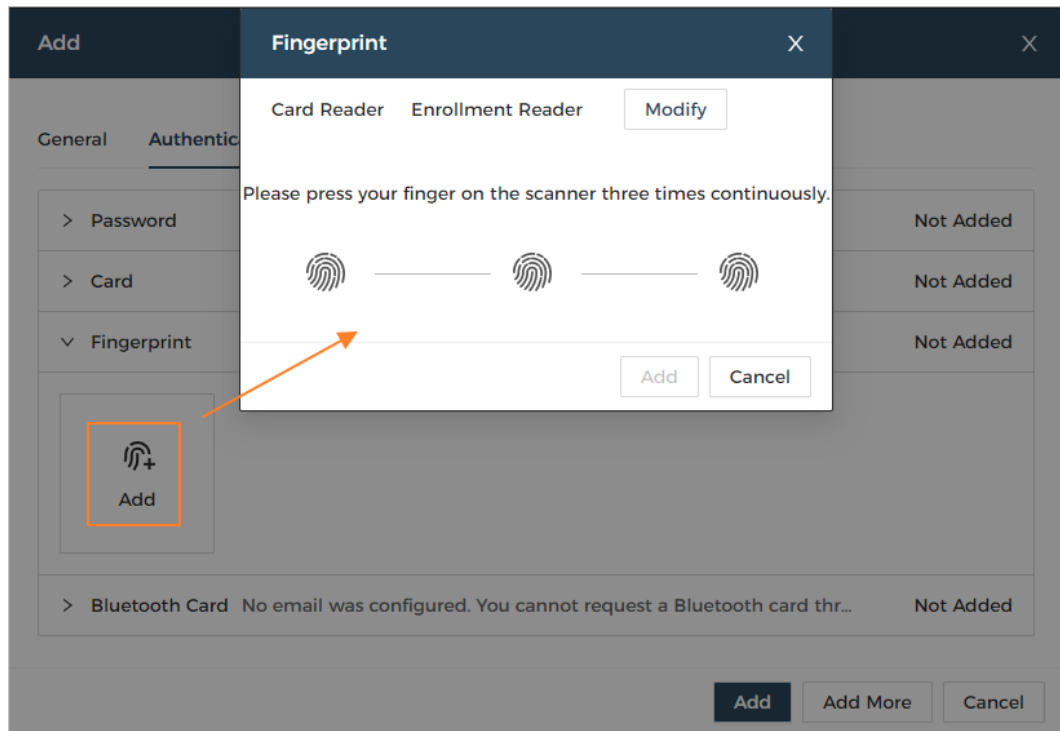
5.2.5.4.3 Adding Fingerprints

Add fingerprints to users for them to use their fingerprints to unlock doors.

Procedure

Step 1 When adding a user, click the **Authentication** tab, and then click **Fingerprint**.

Figure 5-21 Fingerprint



Step 2 Connect a fingerprint scanner to the computer, and follow the on-screen instructions to register the fingerprint.

Step 3 Click **Add**.

5.2.5.4.4 Adding Bluetooth Cards

Add Bluetooth cards to users for them to gain access through Bluetooth cards.

Prerequisites

- The Bluetooth unlock function has been turned on.
- The main controller has been added to PRO-X.
- Users have been added to the platform of the access controller.
- General users, such as company employees, have installed and signed up for PRO-X with their email.

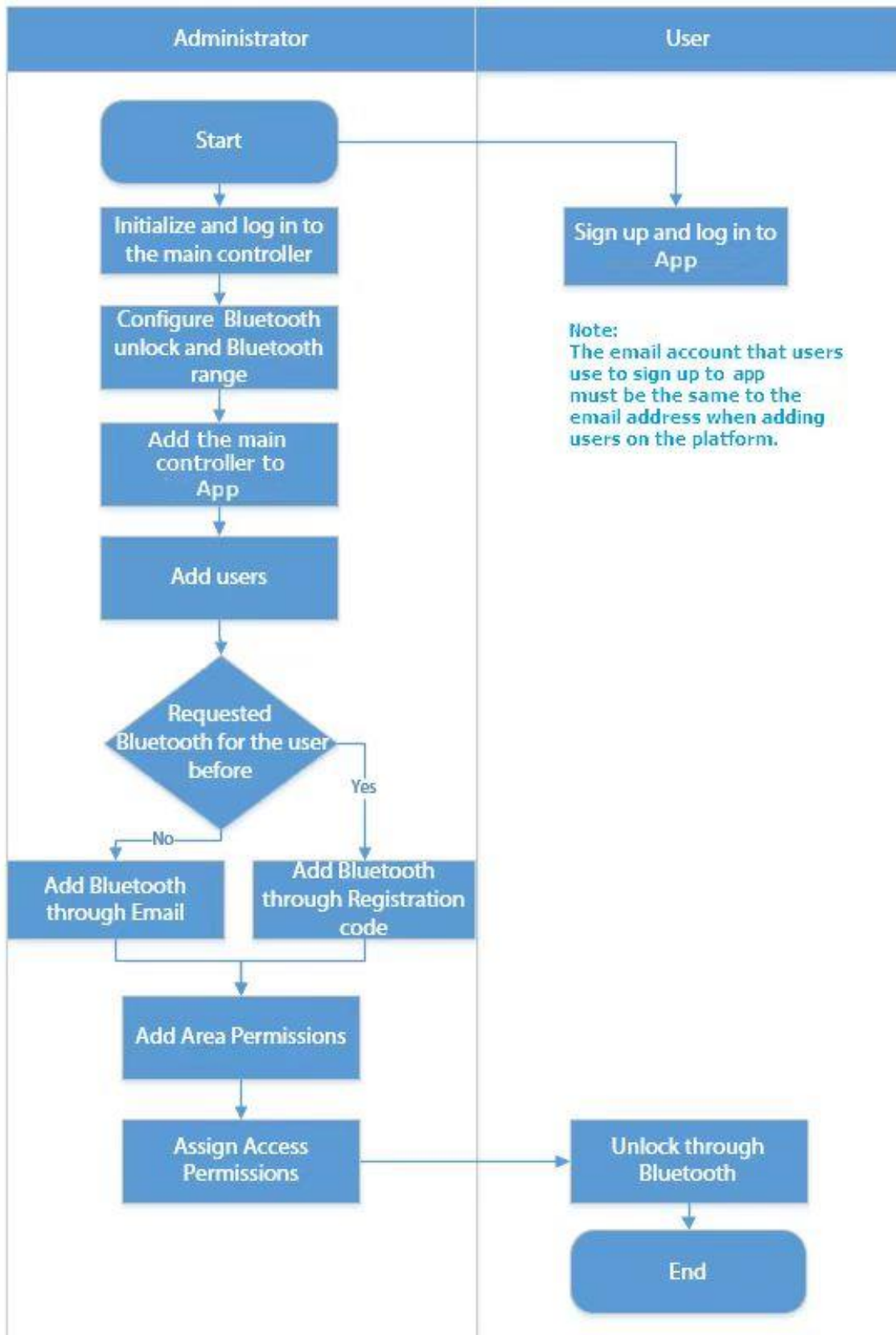


The email that users use to sign up for PRO-X must be the same as the one you used to add them to the access controller.

Background Information

Refer to the flowchart for configuring Bluetooth unlock. Administrator and general users need to perform different operations to complete the process. General users, like company employees, only need to sign up and log in to PRO-X with their email to unlock doors using Bluetooth cards that were issued to them.

Figure 5-22 Flowchart for configuring Bluetooth unlock



Procedure

- Step 1 On the **Authentication** tab, click **Bluetooth Card**.
 3 methods are available to add Bluetooth cards.
- Request through email one by one: Click **Request through Email**.

A Bluetooth card is generated automatically. You can generate up to 5 cards for each user.

- Request through email in batches.

1. On the **User Management** page, click **Batch Issue Cards**.



Batch issue cards only supports requesting through Email.

- ◇ Issue Bluetooth cards to all the users on the list: Click **Issue Cards to All Users**.
 - ◇ Issue Bluetooth cards to selected users: Select users, and then click **Issue Cards to Selected Users**.
2. Click **Bluetooth Card**.
 3. Click **Request through Email**.



- ◇ Users who do not have an email or already have 5 Bluetooth cards will be displayed on the non-requestable list.
- ◇ Export users that lack emails: Click **Export Users that Lack Emails**, enter the emails in the correct format, and then click **Import**. They will be moved to the requestable list.

Figure 5-23 Batch issue cards

Batch Issue Cards

X

CardBluetooth Card

Bluetooth cards can only be generated in batches through emails.

Issue Cards

Requestable (2)

Non-Requestable (0)

Export Users that Lack Emails

Import

User ID	User Name	Email	Bluetooth Card No.	Status	Settings
123	123		0		
124	124		0		

User ID123

User Name123

User TypeGeneral

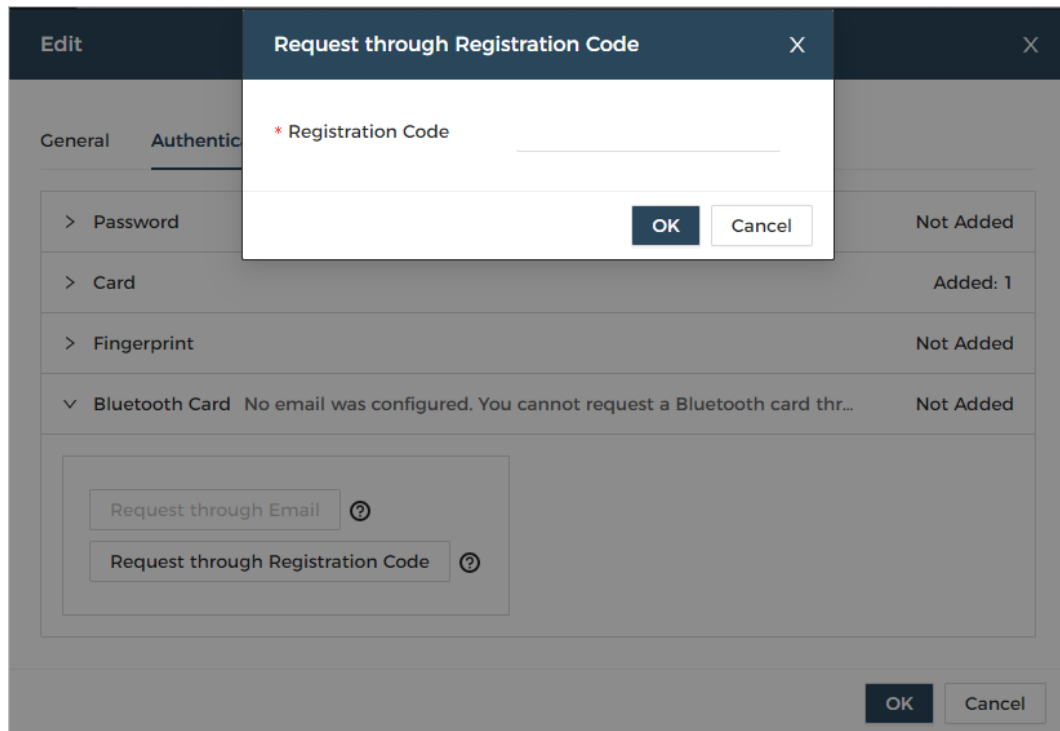
GroupGroup 1

Effective Time2024-12-25 00:00:00-2037-12-31 23:59:59

Request through Email

- If you have requested Bluetooth cards for the user before, you can add the Bluetooth cards through registration code.
 1. On PRO-X, tap **Registration Code** of a Bluetooth card.
The registration code is automatically generated by PRO-X.
 2. Copy the registration code.
 3. On the **Bluetooth Card** tab, click **Request through Registration Code**, paste the registration code, and then click **OK**.

Figure 5-24 Request through registration code



4. Click **OK**.

The Bluetooth card is added.

Step 2 Click **OK**.

Result

After users sign up and log in to PRO-X with the Email address, they can open PRO-X to unlock the door through Bluetooth cards. For details, see the user's manual of PRO-X.

- Auto unlock: The door automatically unlocks when you are in the defined Bluetooth range, which allows the Bluetooth card to transmit signals to the card reader.



In auto unlock mode, the Bluetooth card might continuously unlock the door when you are within the Bluetooth range for a long time until a failure occurs. Please turn off Bluetooth on the phone and then turn it on again.

- Shake to unlock: The door unlocks when you shake your phone to allow the Bluetooth card to transmit signals to the card reader.

Related Operations

- Users can manage Bluetooth cards on PRO-X.
 - ◇ Move to the Top: If multiple Bluetooth cards have been added, you can move cards to the top that are currently in use.
 - ◇ Rename: Rename the Bluetooth card.
 - ◇ Delete: Delete the Bluetooth card.
- Export users that lack emails: Click **Export**, enter the emails in the correct format and then click Import. They will be moved to the requestable list.

- View the request records: On the **User Management** page, select **More > Bluetooth Card Records** to view the request status.
 - ◇ **View Details:** View the details of the request, including user information, reasons for failed requests and more. You can also request again for failed users.
 - ◇ **Request Again:** Request again for failed users.

5.2.6 Adding Weekly Plans


The weekly plan is used to set the unlock schedule for the week. The platform offers a default template with a full daytime schedule. You can also create your own templates.

Procedure

Step 1 Select **Access Rules > Weekly Plan**, and then click **Add**.



- The default full-day time template cannot be modified.
- You can create up to 128 weekly plans.

Step 2 Click  to edit the time template.

- 1) Define the name of the weekly plan.
- 2) Click on the date that you want to set (for example, **Mon**), and then drag the slider to adjust the time period for each day.

You can also click **Copy** to apply the configured time period to other days.



You can only configure up to 4 periods for each day.

- 3) Click **Apply**.

Figure 5-25 Add the weekly plan

The screenshot shows the 'Weekly Plan' edit interface. On the left sidebar, there is a list of plans with an 'Add' button (1). The main form has a 'Name' field (2) containing 'Weekly Plan 1' and a 'Description' field. Below is the 'Time Plan' section (3) which includes a 24-hour timeline and a table for each day of the week (Sun-Sat) with blue bars and 'Copy' buttons. At the bottom are 'Apply' (4) and 'Cancel' buttons.

5.2.7 Adding Zone

A zone is a collection of door access permissions. Create a zone, and then link users to the zone so that they can gain access permissions set for the zone.

Procedure

- Step 1 Select **Access Rules > Zone Settings**.
- Step 2 Click **Add** to add zones.
You can add up to 40 zone permissions.

Figure 5-27 Add zones

Add [X]

* Zone Name

Door List

Search [Q]

- ☐ A [redacted] DMSS
- ☐ 1 [redacted]

[OK] [Cancel]

Step 3 Enter the name of the zone.

Step 4 Select doors.

Step 5 Click **OK**.

5.2.8 Adding Permission Rules

By creating permissions rules, you can assign access permissions to users by linking them to the zones. This will allow authorized personnel to gain access to secure zones.

Procedure

Step 1 Select **Access Rules > Permission Settings**.

Step 2 Click **Add** to add a permission rule.

Figure 5-28 Assign permissions in batches

The screenshot shows a web interface for adding a permission rule. The window is titled 'Add'. It contains several input fields and buttons. A red box with a '1' highlights the 'Name' field containing 'Permission1'. Another red box with a '2' highlights the 'Weekly Plan' and 'Holiday Plan' dropdown menus. The 'Weekly Plan' is set to 'Full-day Time Template' and the 'Holiday Plan' is set to 'No Holiday'. Below these is a 'Remarks' text area. The bottom half of the window is divided into two sections: 'User Info' and 'Zone Info'. Each section has a large empty box with 'No data' and an 'Add' button. Red boxes with '3' and '4' highlight these 'Add' buttons. At the bottom, there are 'Apply' and 'Cancel' buttons. A red box with a '5' highlights the 'Apply' button.

Step 3 Enter the name of the permission rule.

Step 4 Select the weekly plan and the holiday plan.

Step 5 In the **User Info** section, click **Add** to select user, and then click **OK**.

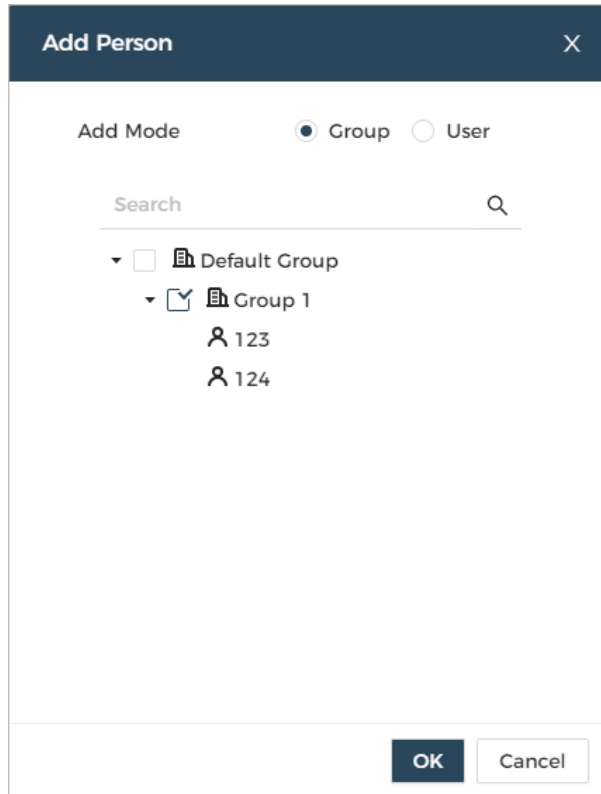
You can select users by group or by user.

- Group: All users in the group 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 an existing group, they will be automatically assigned access permissions defined for the group.

Figure 5-29 Add person

The image shows a 'Add Person' dialog box with a dark blue header bar containing the title 'Add Person' and a close button 'X'. Below the header, there is a section labeled 'Add Mode' with two radio buttons: 'Group' (which is selected) and 'User'. Underneath, there is a search bar with the placeholder text 'Search' and a magnifying glass icon. Below the search bar, there is a list of groups. The first group is 'Default Group' with a dropdown arrow and an unchecked checkbox. The second group is 'Group 1' with a dropdown arrow and a checked checkbox. Under 'Group 1', there are two user entries, each represented by a person icon and the number '123' and '124' respectively. At the bottom right of the dialog, there are two buttons: 'OK' and 'Cancel'.

Step 6 In the **Zone Info** section, click **Add** to select a zone, and then click **OK**.

Step 7 Click **Apply**.

5.2.9 Configuring Global Alarm linkages (Optional)

You can configure global alarm linkages across different access controllers.

Procedure

Step 1 Go to **Access Rules > Global Alarm Linkage**.



- When you have configured both global alarm linkages and local alarm linkages, and if the global alarm linkages conflict with the local alarm linkages, the last alarm linkages you have configured will take effective.
- When you have configured alarm linkages for sub controllers through the main controller, if the main controller has been restored to the factory defaults, we recommended you restore the sub controller to factory defaults at the same time.

Step 2 Configure the alarm output.

1. Select an alarm input from the alarm input channel list, and then click **Link Alarm Output**.
2. Click **Add**, select an alarm output channel, and then click **OK**.

Add

Alarm Output Channel List

Search

Alarm Output 1

Alarm Output 2

2 Selected

No.	Alarm Output Channel	Device	Settings
1	1	ACC0003TEST04MS	X
2	2	ACC0003TEST04MS	X

<

1

>

OK

Cancel

- ### Step 3 Configure the door linkage.

- 51

Add

Door List

Search

▼

Door1

Door2

1 2 3 4 5

2 Selected

No.	Door Channel	Door Status	Settings
1	Door1	Always Unlocked ▾	✕
2	Door2	Always Locked ▾	✕

<

1

>

OK

Cancel

4. Click **Enable** to turn on the door linkage function.

Link Alarm Output

Link Door Channel





Enable

☐

Link Fire Safety Contr...

☐

Add

No.	Door Channel	Door Status	Device	Settings
1	Door1	Always Unlocked ▼	 S	
2	Door2	Always Locked ▼	 S	

2 record(s)

<

1

>

Apply

Copy to



If you turn on link fire safety control, all door linkages will automatically change to the **Always Unlocked** status, and all the doors will open when the fire alarm is triggered.

5. Click **Apply**.

You can click **Copy to** to apply the defined alarm linkages to other alarm input channels.

5.2.10 Viewing Data Synchronization Progress

After you assign access permissions to users, you can view the data synchronization process.

Procedure

Step 1 Go to **Access Rules > Data Sync**.

Step 2 View the data synchronization progress.

Figure 5-33 Data synchronization progress

Time	Zone Permission	Device Name	Details	Results	Settings
12:25:2024 04:29:06 PM		A-SS	Sync Person Info to Main Controller	✓: 2, ✗: 0	
12:25:2024 04:22:28 PM		A-SS	Sync Person Info to Main Controller	✓: 2, ✗: 0	
12:25:2024 04:05:05 PM		A-SS	Sync Person Info to Main Controller	✓: 1, ✗: 0	
12:25:2024 04:04:45 PM		A-SS	Sync Person Info to Main Controller	✓: 1, ✗: 0	
12:25:2024 04:02:14 PM		A-SS	Sync Person Info to Main Controller	✓: 1, ✗: 0	
12:25:2024 04:02:04 PM		A-SS	Sync Person Info to Main Controller	✓: 1, ✗: 0	

5.2.11 Configuring Cloud Service

Add the main controller to PRO-X before you request Bluetooth cards for users. For details on using quickies, see the user's manual of Quickies.



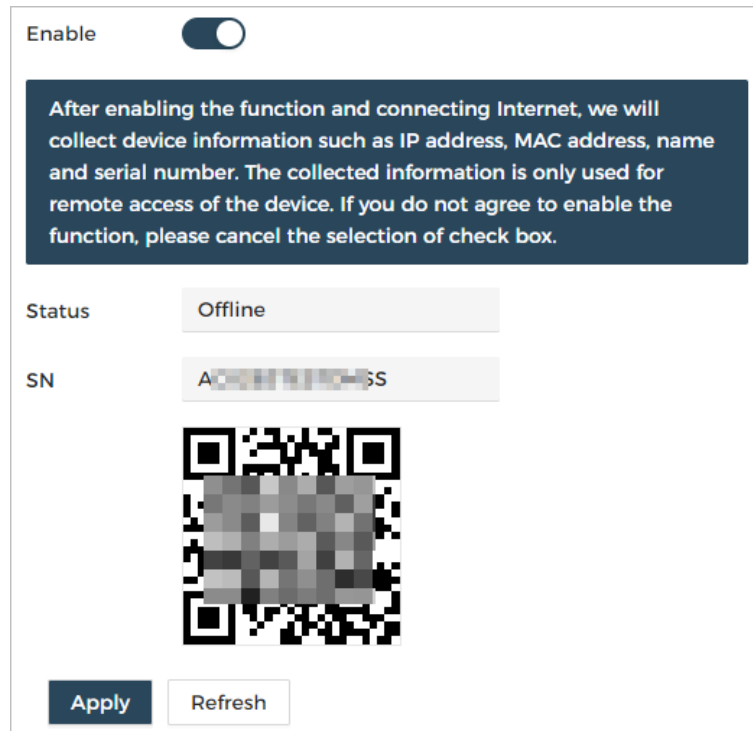
If you have changed the password of the main controller, or restored it to factory defaults, you need to delete the controller on PRO-X and add it to PRO-X again.

Procedure

Step 1 Go to **System Settings > Network Setting > Cloud Service**.

Step 2 Turn on the cloud service function.

Figure 5-34 Cloud service



Step 3 Click **Apply**.

Step 4 Download PRO-X and sign up with Email, scan the QR code with PRO-X to add the access controller to it.

5.3 Configurations of Sub Controller

You can log in to the webpage of the sub controller to configure it locally.

5.3.1 Initialization

Initialize the sub controller when you log in to the webpage for the first time or after the sub controller is restored to its factory default settings. For details on how to initialize the sub controller, see "5.2.2 Initialization".



After initializing the sub controller, change its network mode to **Static**. **DHCP** is only used for initialization.

5.3.2 Logging In

Set the access controller to sub controller while going through the login wizard. For details, see "5.2.3 Logging In".

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 Allow list**

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

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

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

 - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
 - According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
 - Establish 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).