






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
V1.0.3	Updated adding users and configuring permissions.	June 2023
V1.0.2	Updated the description on adding users.	April 2023
V1.0.1	Updated the wiring and the unlock methods.	March 2023
V1.0.0	First release.	September 2022

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the 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.

Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Dimensions and Appearance	1
2 Ports Overview	4
3 Wring of Locks	11
3.1 Wiring of Magnetic Locks	11
3.1.1 Wring of Dual Magnetic Locks with PoE (12V and Relay).....	11
3.1.2 Wring of Dual Magnetic Locks with 12 V External Power Supply (12 V and Relay).....	12
3.1.3 Wring of Dual Magnetic Locks with 12 V External Power Supply (Relay).....	13
3.1.4 Wring of 2-in-1 Magnetic Lock with 12 V External Power Supply (Relay).....	15
3.2 Wiring of Electric Strike Lock.....	16
3.2.1 Wring of Dual Electric Strikes with PoE.....	16
3.2.2 Wring of Dual Electric Strikes with 12 V External Power Supply.....	17
4 Installation.....	20
4.1 Wall Mount.....	20
4.2 DIN Rail Mount	22
5 Access Control Configurations	25
5.1 Networking Diagram.....	25
5.2 Configurations of Main Controller.....	25
5.2.1 Configuration Flowchart.....	25
5.2.2 Initialization	26
5.2.3 Logging In	27
5.2.4 Adding Devices.....	32
5.2.5 Adding Users	34
5.2.6 Adding Weekly Plans.....	50
5.2.7 Adding Areas.....	51
5.2.8 Adding Permission Rules	52
5.2.9 Viewing Authorization Progress.....	54
5.2.10 Configuring Global Alarm linkages (Optional).....	55
5.2.11 Configuring Cloud Service	56
5.3 Configurations of Sub Controller.....	58
5.3.1 Initialization	58
5.3.2 Logging In.....	58
Appendix 1 Cybersecurity Recommendations.....	59

1 Dimensions and Appearance

Figure 1-1 Dimensions (mm [inch])

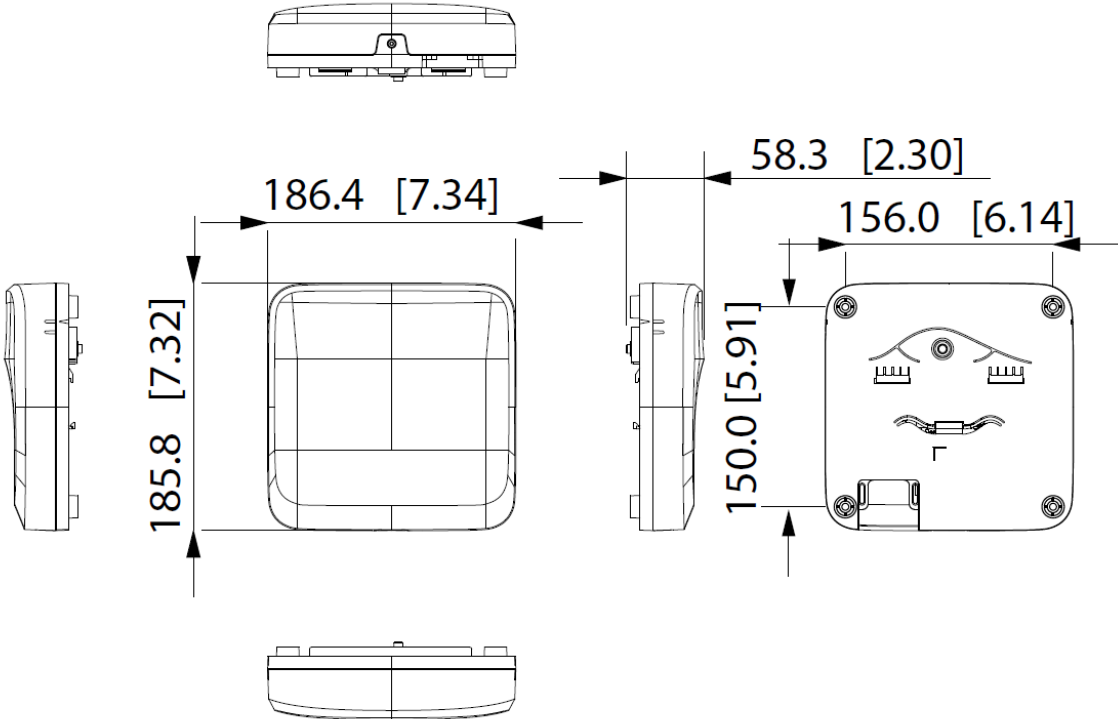


Figure 1-2 Front view

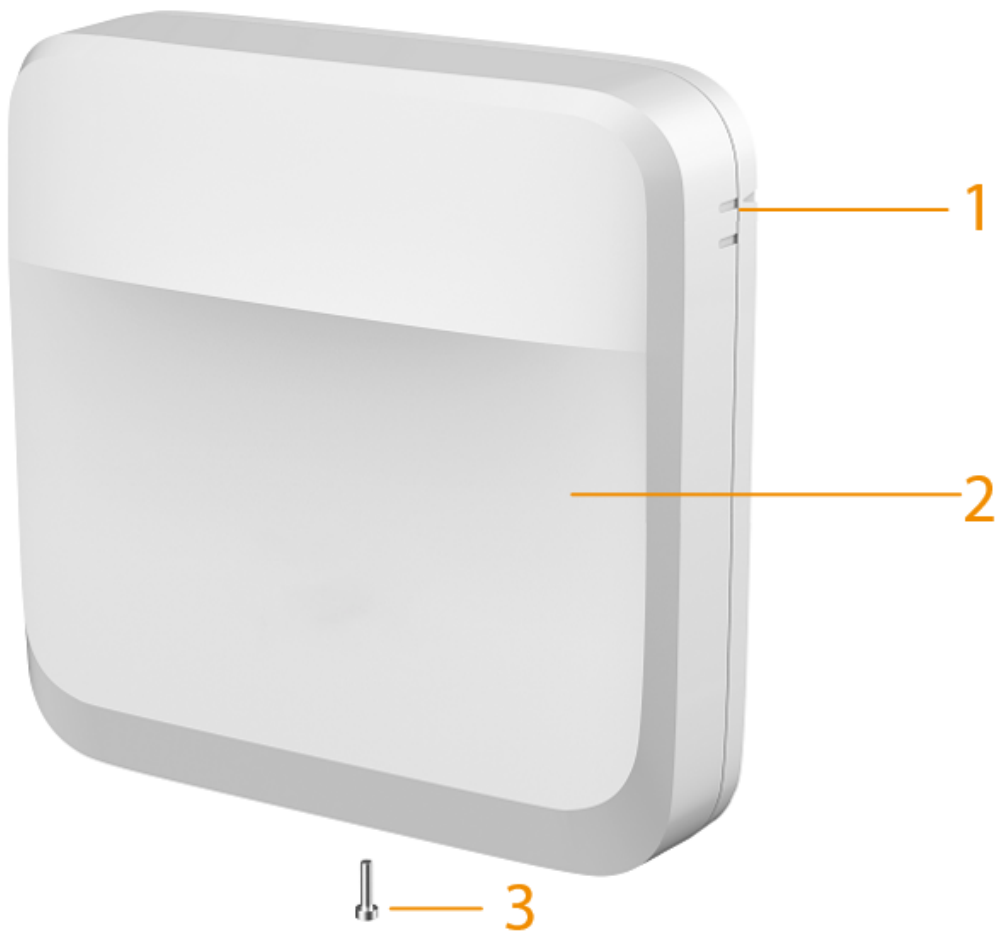


Table 1-1 Components description

No.	Description
1	Guiding mark
2	Front panel
3	Screw

Figure 1-3 Back cover

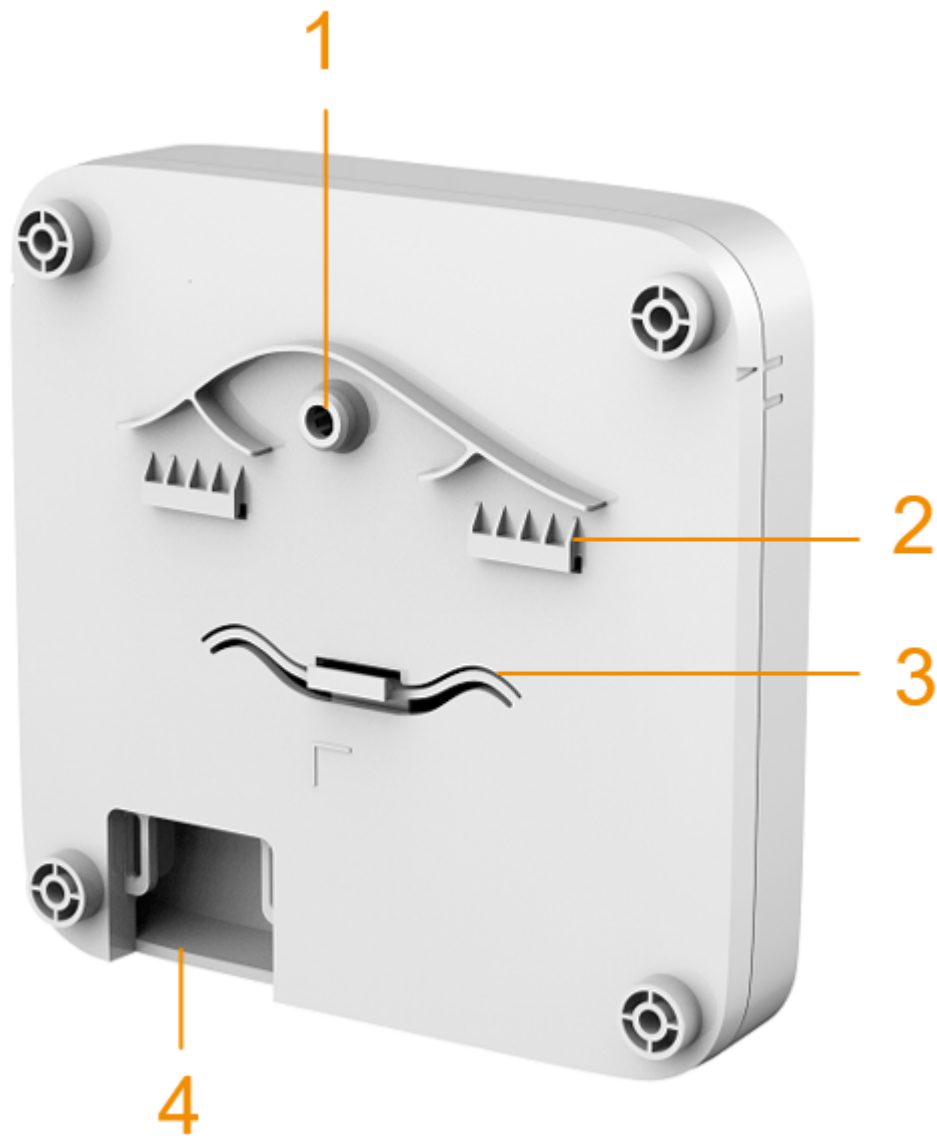


Table 1-2 Back cover description

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

2 Ports Overview

Figure 2-1 Ports

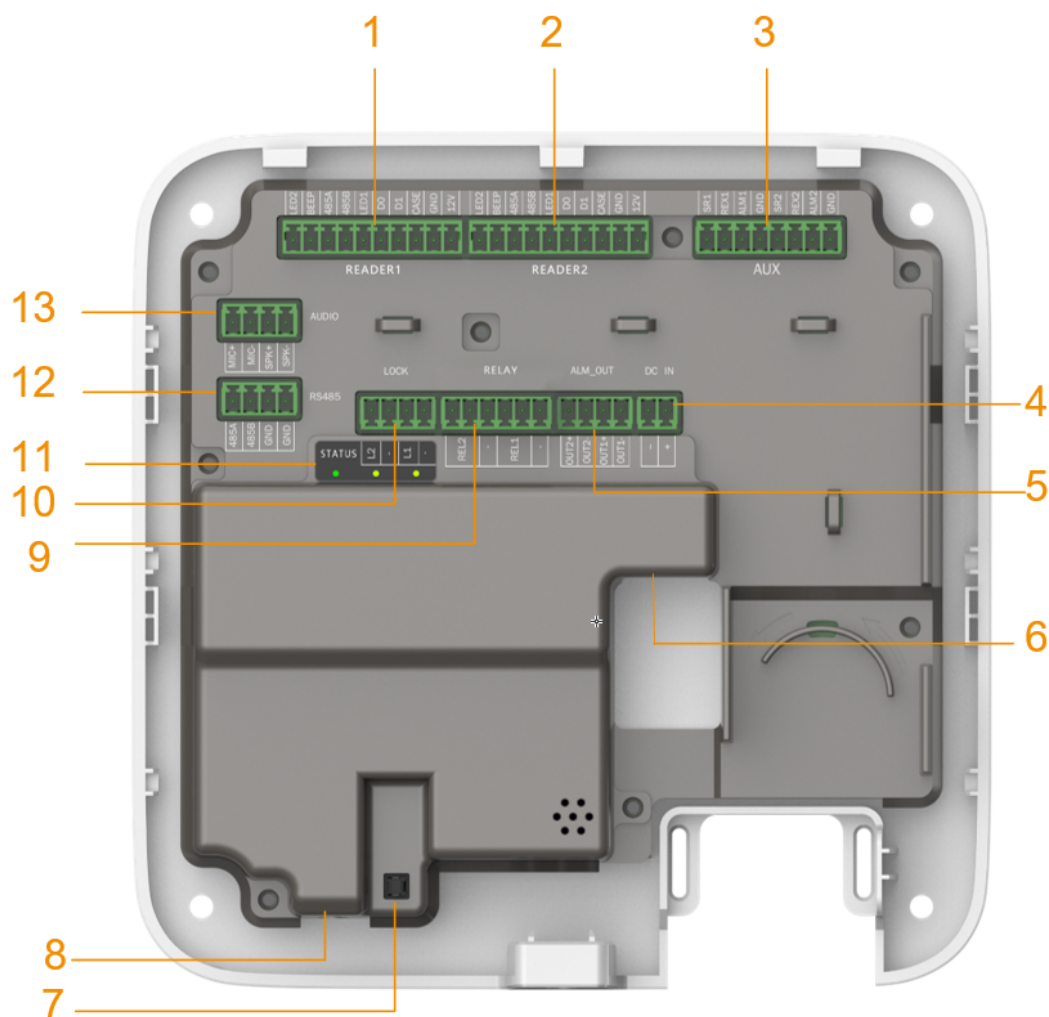


Table 2-1 Ports description

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

No	Name	Description
10	LOCK	Power lock connector
11	STATUS	LED indicator
12	RS485	RS485 connector (not used)
13	AUDIO	Audio connector (not used)

Figure 2-2 Reader connector

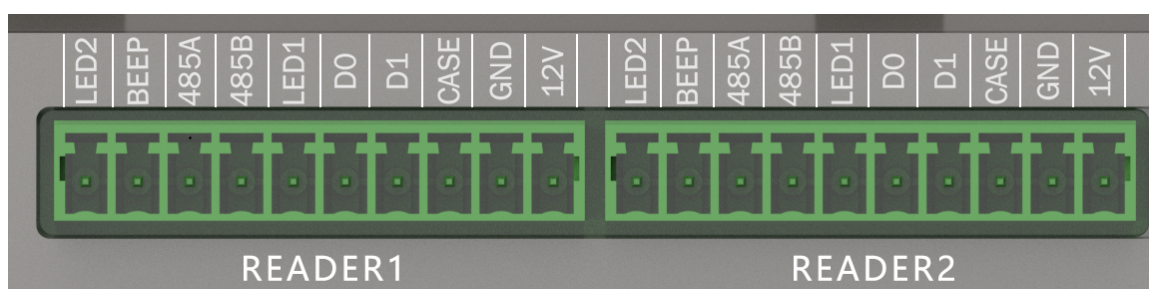


Table 2-2 Reader connector description

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.

Port	Port Name	Indicator color	Status
L2	Lock 2 indicator	Solid yellow and green	Lock open
		Solid red	Lock closed
L1	Lock 1 indicator	Solid yellow and green	Lock open

Figure 2-4 Auxiliary I/O ports

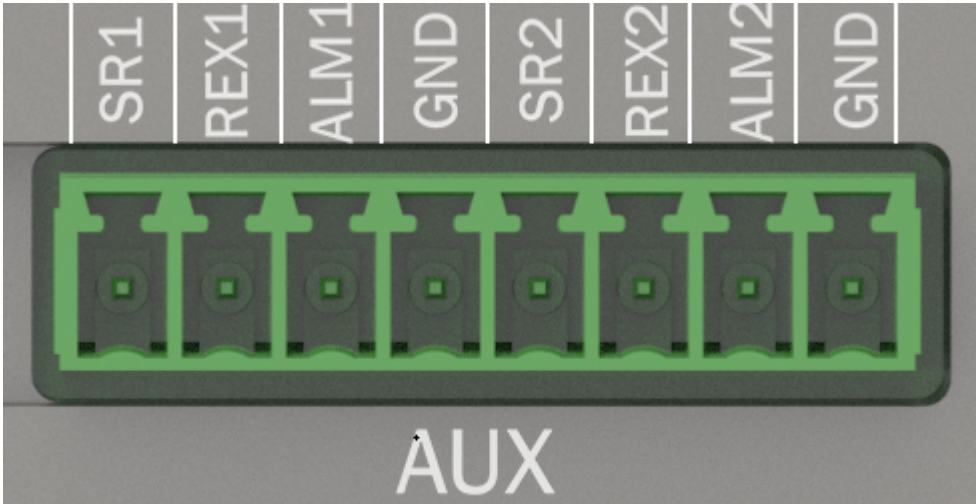


Table 2-4 Description of auxiliary I/O ports

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

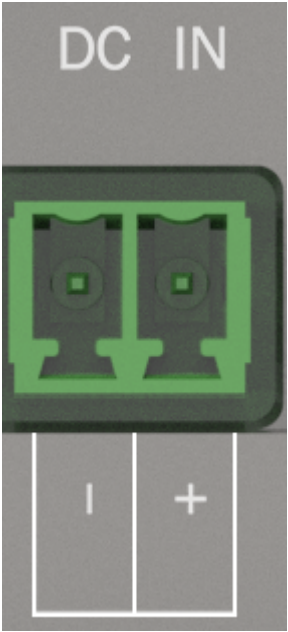


Table 2-5 Description of power ports

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

Figure 2-6 Alarm output ports

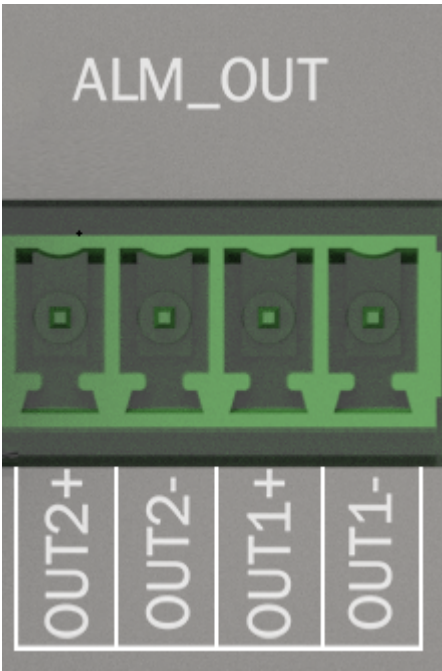


Table 2-6 Description of alarm output ports

Ports	Description
OUT2+	Alarm output 2
OUT2-	
OUT1+	Alarm output 1
OUT1-	

Figure 2-7 Relay ports

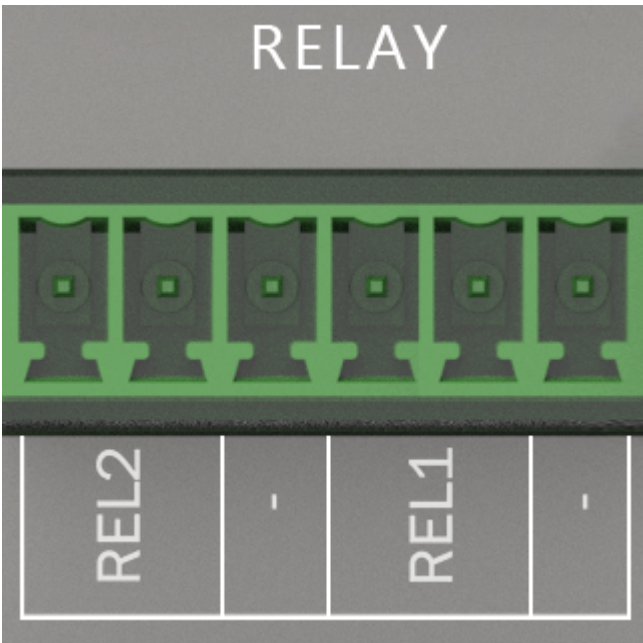


Table 2-7 Description of relay ports


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

Figure 2-8 Lock ports

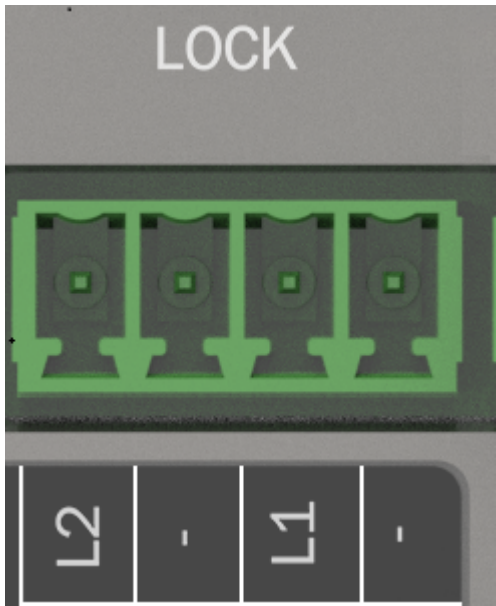


Table 2-8 Description of lock


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

Figure 2-9 RS-485 ports

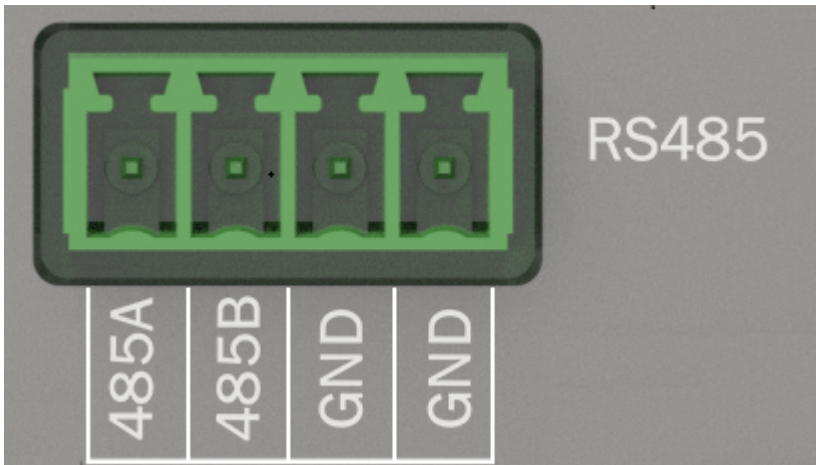


Table 2-9 Description of RS-485

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

Figure 2-10 Audio ports

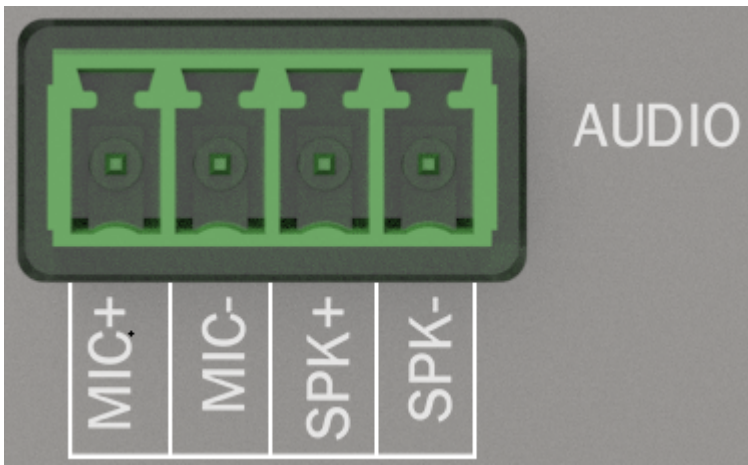


Table 2-10 Description of audio ports

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

3 Wiring of Locks

This section use 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 Wring of Dual Magnetic Locks with PoE (12V 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

☒ Relay
 Relay Open = Unlocked

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

Figure 3-2 Lock 2 (door 2)

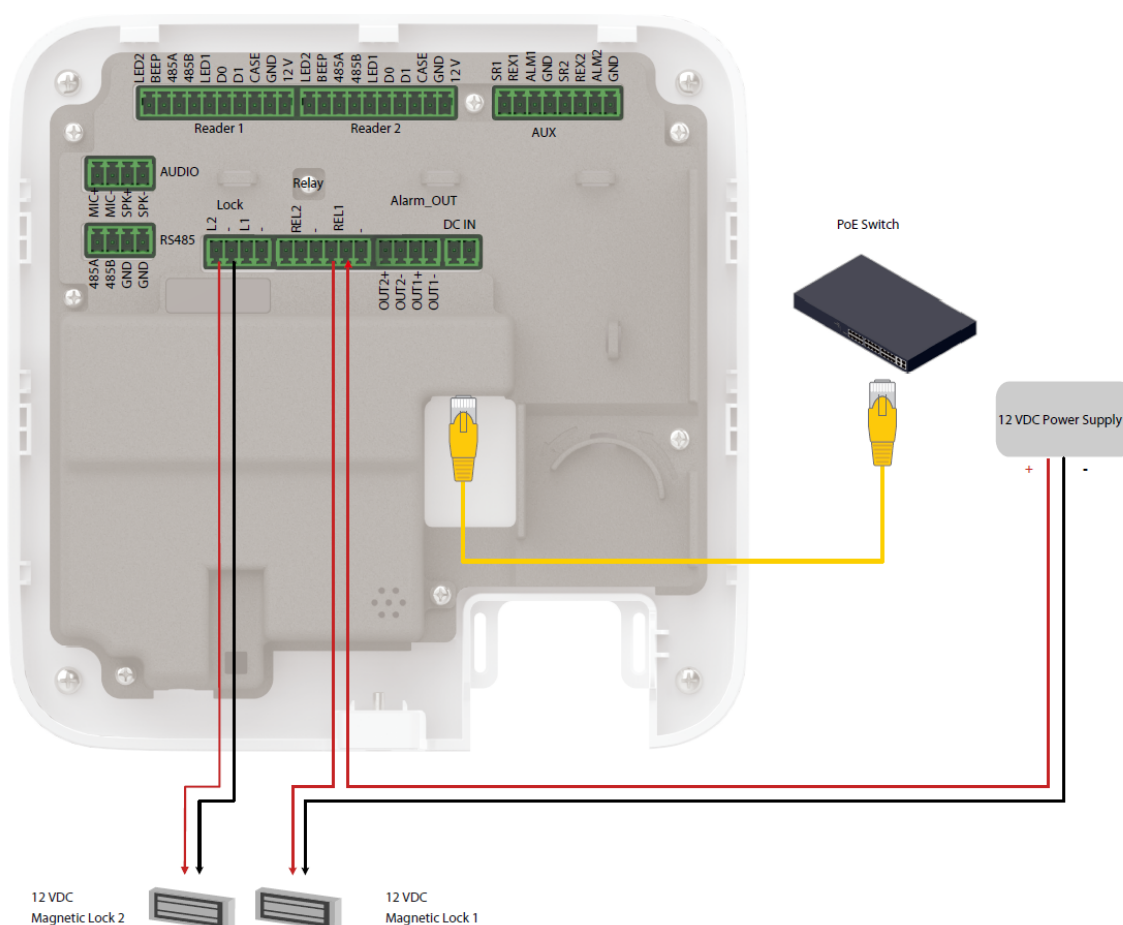
Power Supply of Locks

☒ 12V
 Fail Safe

☐ Relay
 Relay Open = Locked

3. Wiring the locks according to the diagram below.

Figure 3-3 Wiring of locks

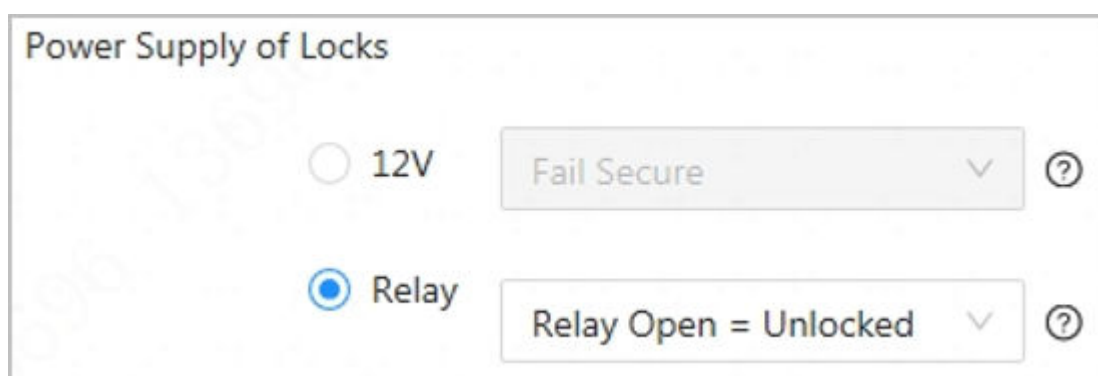


3.1.2 Wring of Dual Magnetic Locks with 12 V External Power Supply (12 V and Relay)

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.

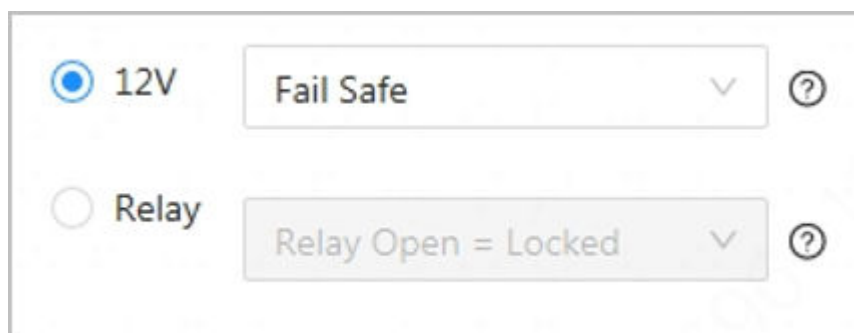
1. Select **Relay Open = Unlocked** from the **Relay** list for lock 1 (door 1).

Figure 3-4 Lock 1 (door 1)



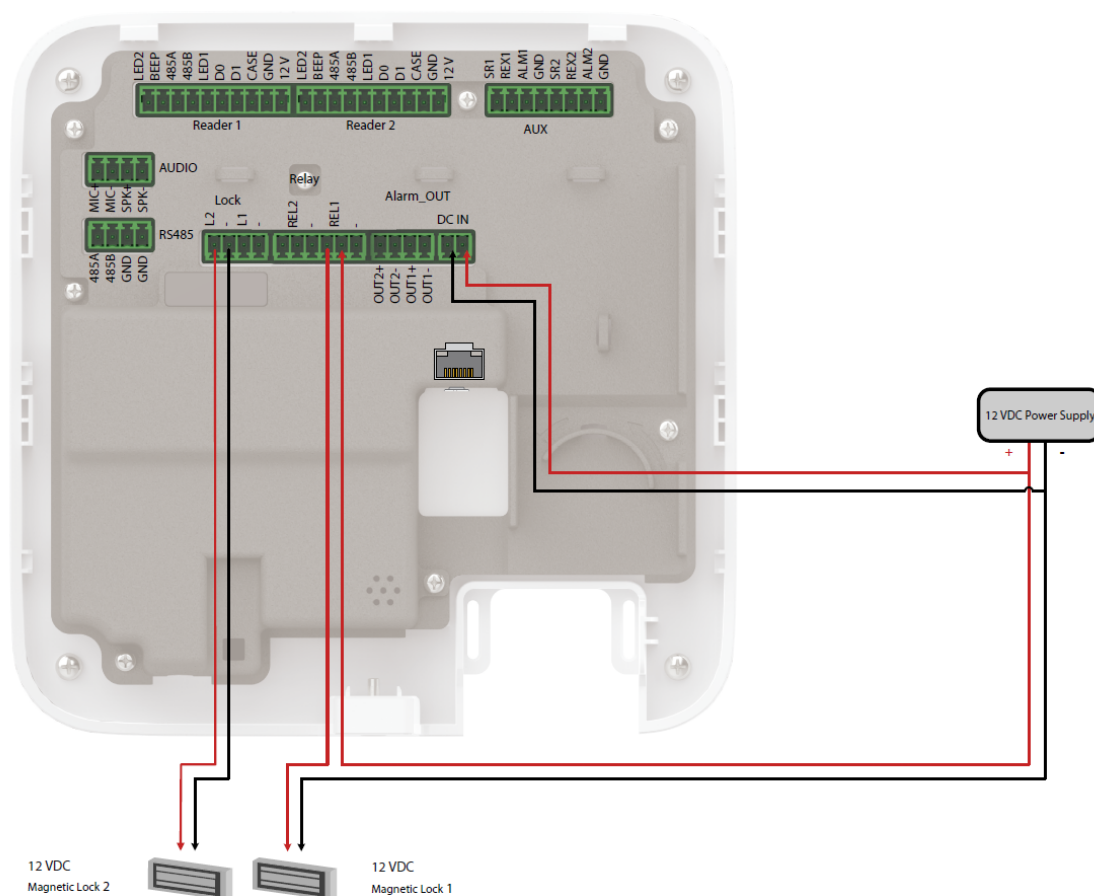
2. Select **Fail Safe** from the **12V** list for door 2.

Figure 3-5 Lock 2 (door 2)



3. Wiring the locks according to the diagram below.

Figure 3-6 Wiring of locks



3.1.3 Wring 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)



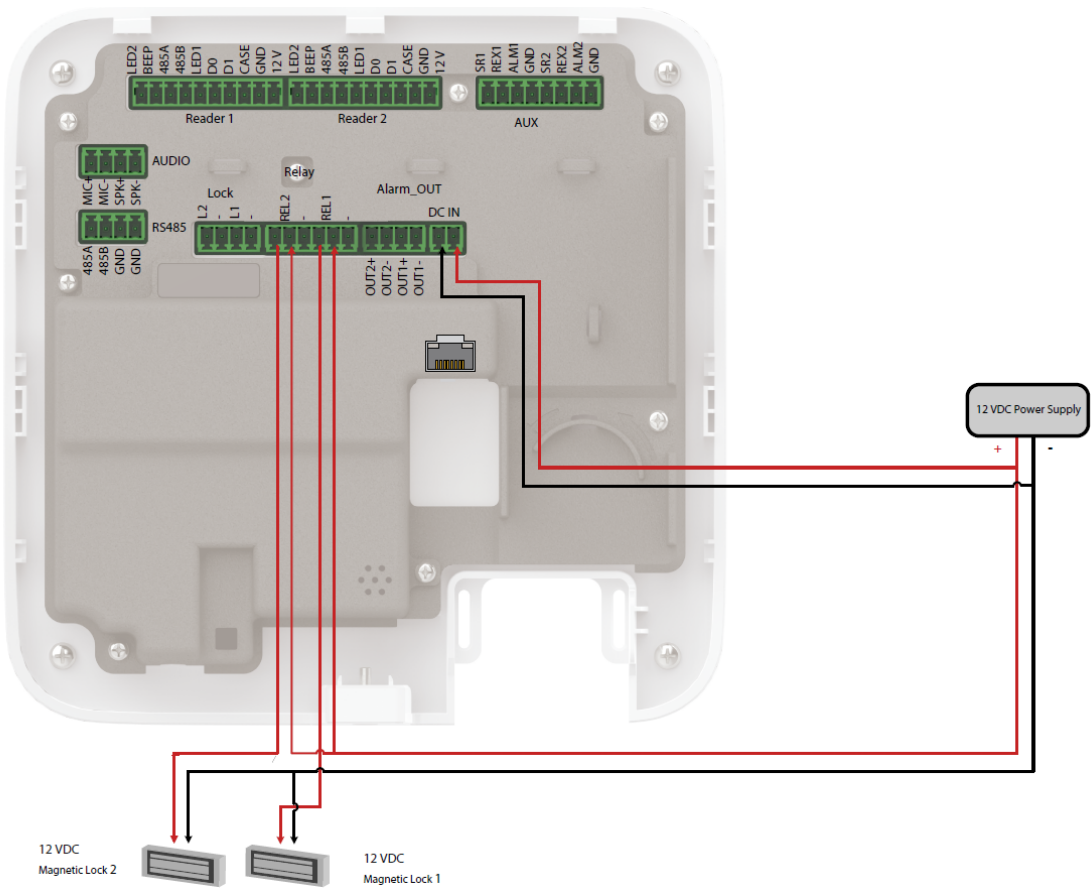
2. Select **Relay Open = Unlocked** from the **Relay** list for lock 2 (door 2).

Figure 3-8 Lock 2 (door 2)



3. Wiring the locks according to the diagram below.

Figure 3-9 Wiring of locks



3.1.4 Wring 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)



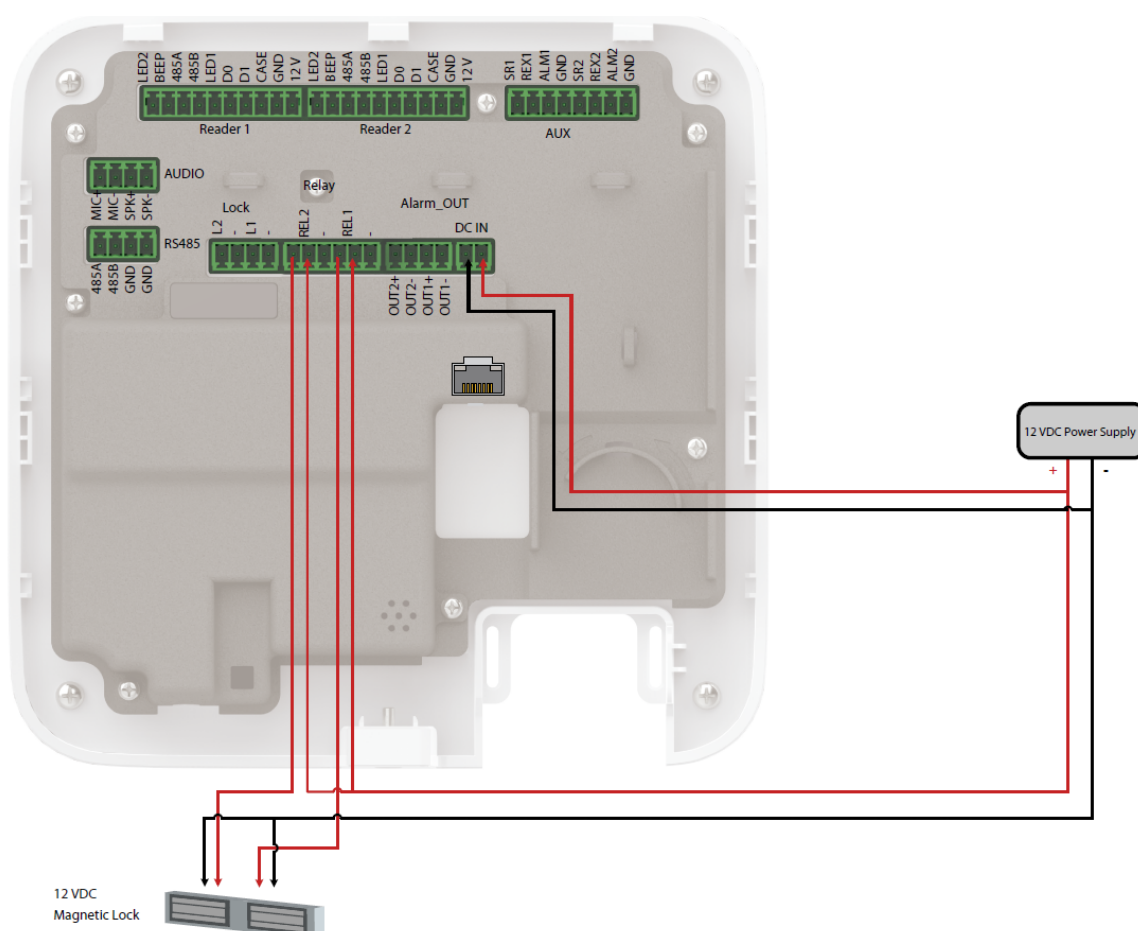
2. Select **Relay Open = Unlocked** from the **Relay** list for lock 2 (door 2).

Figure 3-11 Lock 2 (door 2)



3. Wiring the locks according to the diagram below.

Figure 3-12 Wiring of locks



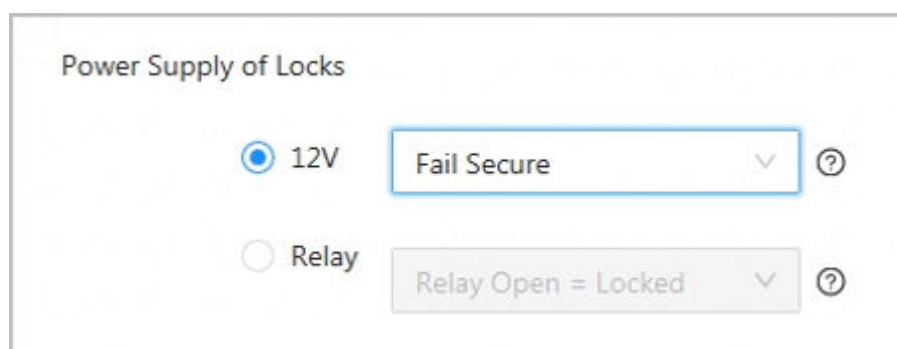
3.2 Wiring of Electric Strike Lock

3.2.1 Wiring of Dual Electric Strikes with PoE

Supplies power for the Access Controller over the same Ethernet cable. Both doors use the external power supply.

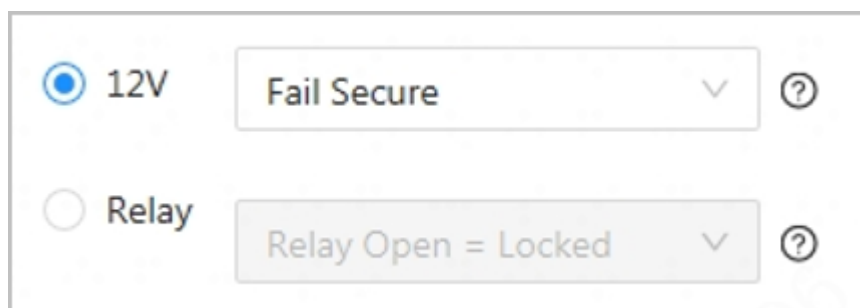
1. Select **Fail Secure** from the **12V** list for lock 1 (door 1).

Figure 3-13 Lock 1 (door 1)



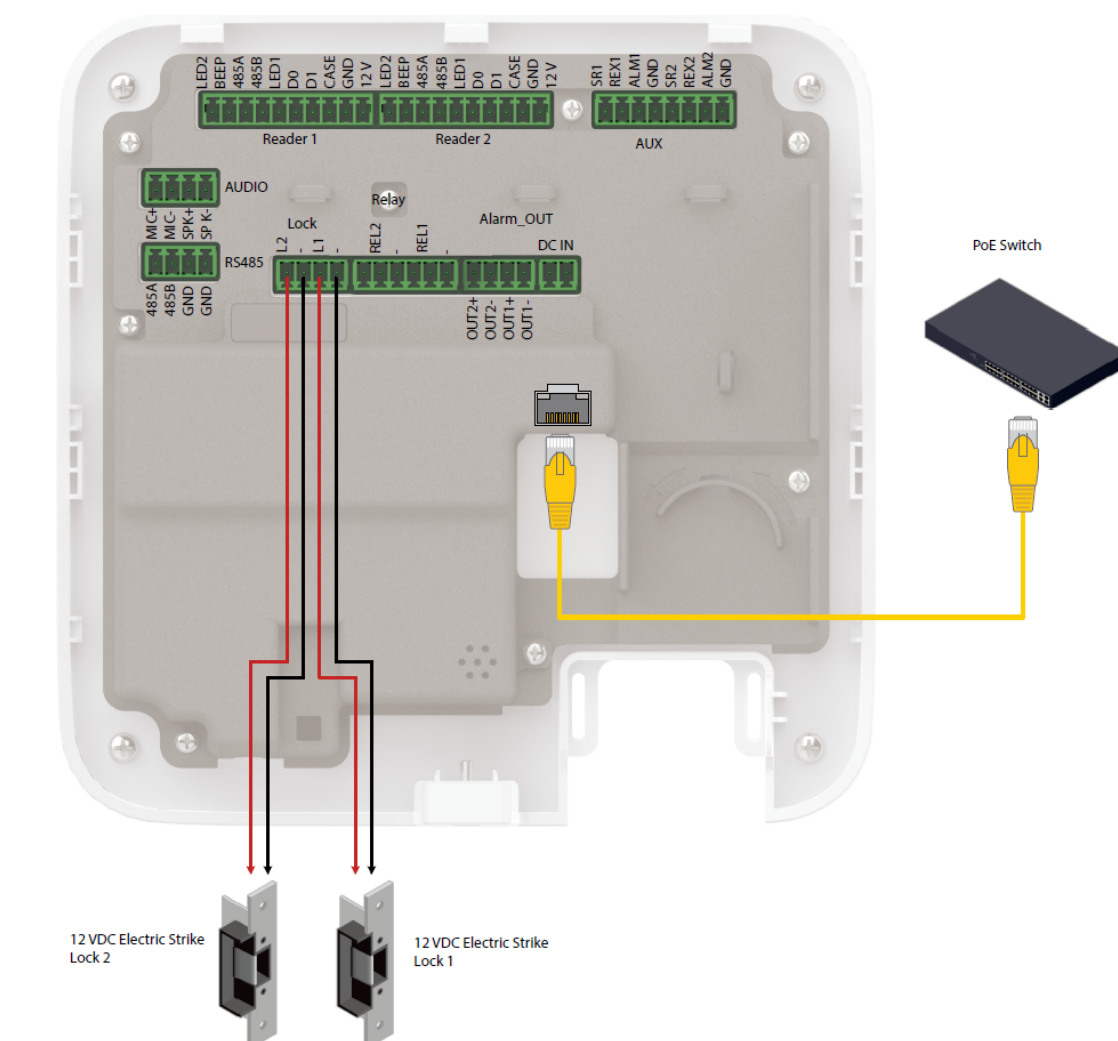
2. Select **Fail Secure** from the **12V** list for lock 2 (door 2).

Figure 3-14 Lock 2 (door 2)



3. Wiring the locks according to the diagram below.

Figure 3-15 Wiring of locks



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

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

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)

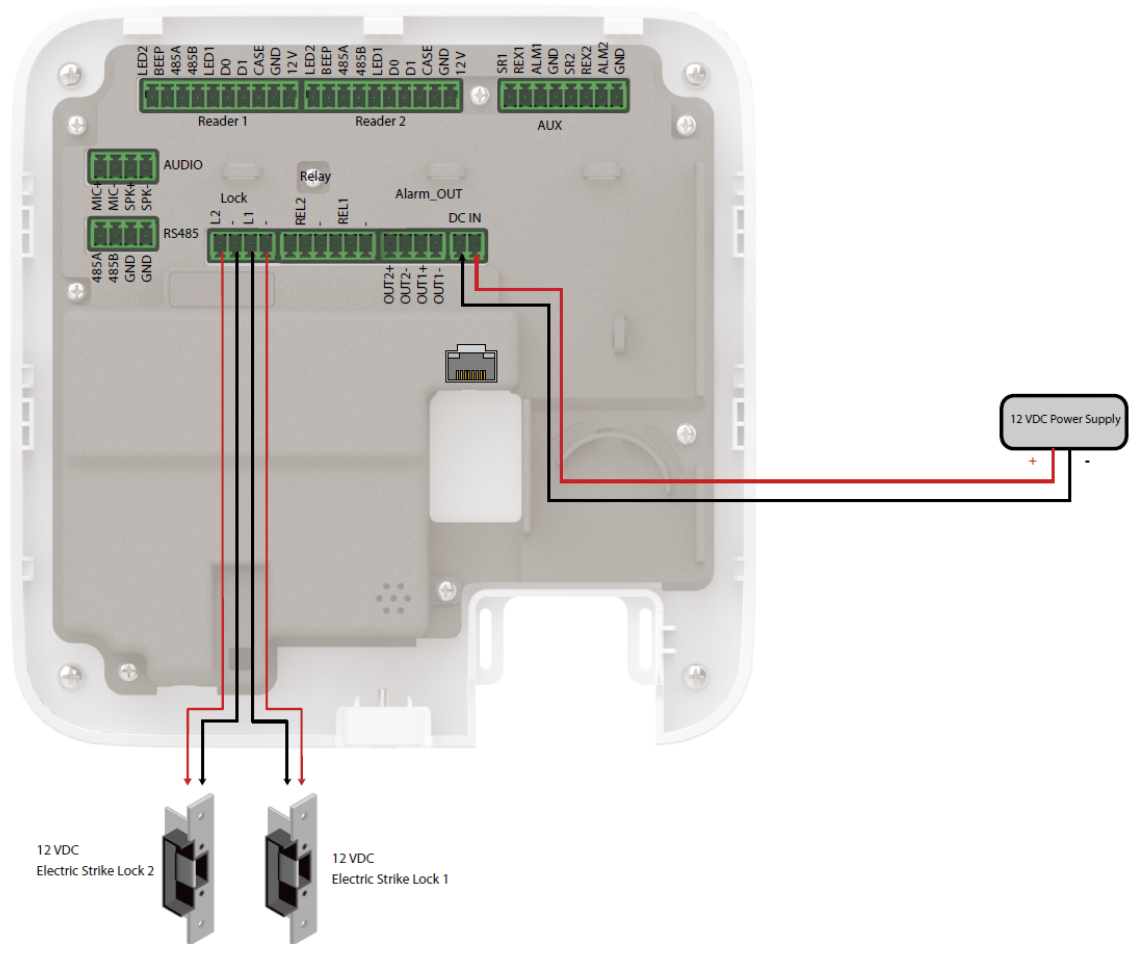
Power Supply of Locks

☒ 12V Fail Secure ?

☐ Relay Relay Open = Locked ?

3. Wiring the locks according to the diagram below.

Figure 3-18 Wiring of locks



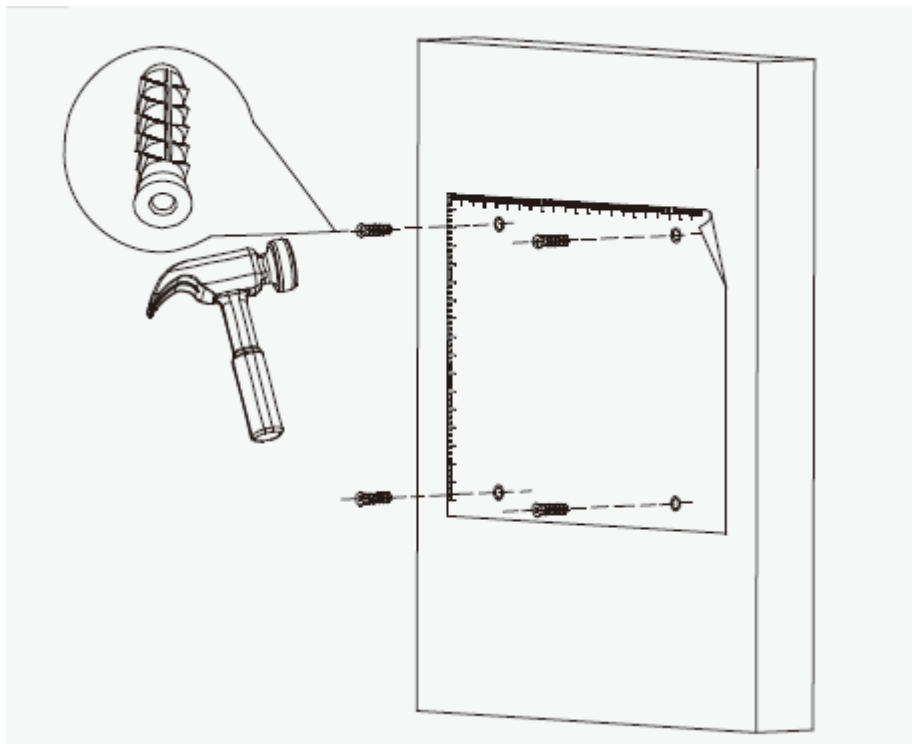
4 Installation

4.1 Wall Mount

Procedure

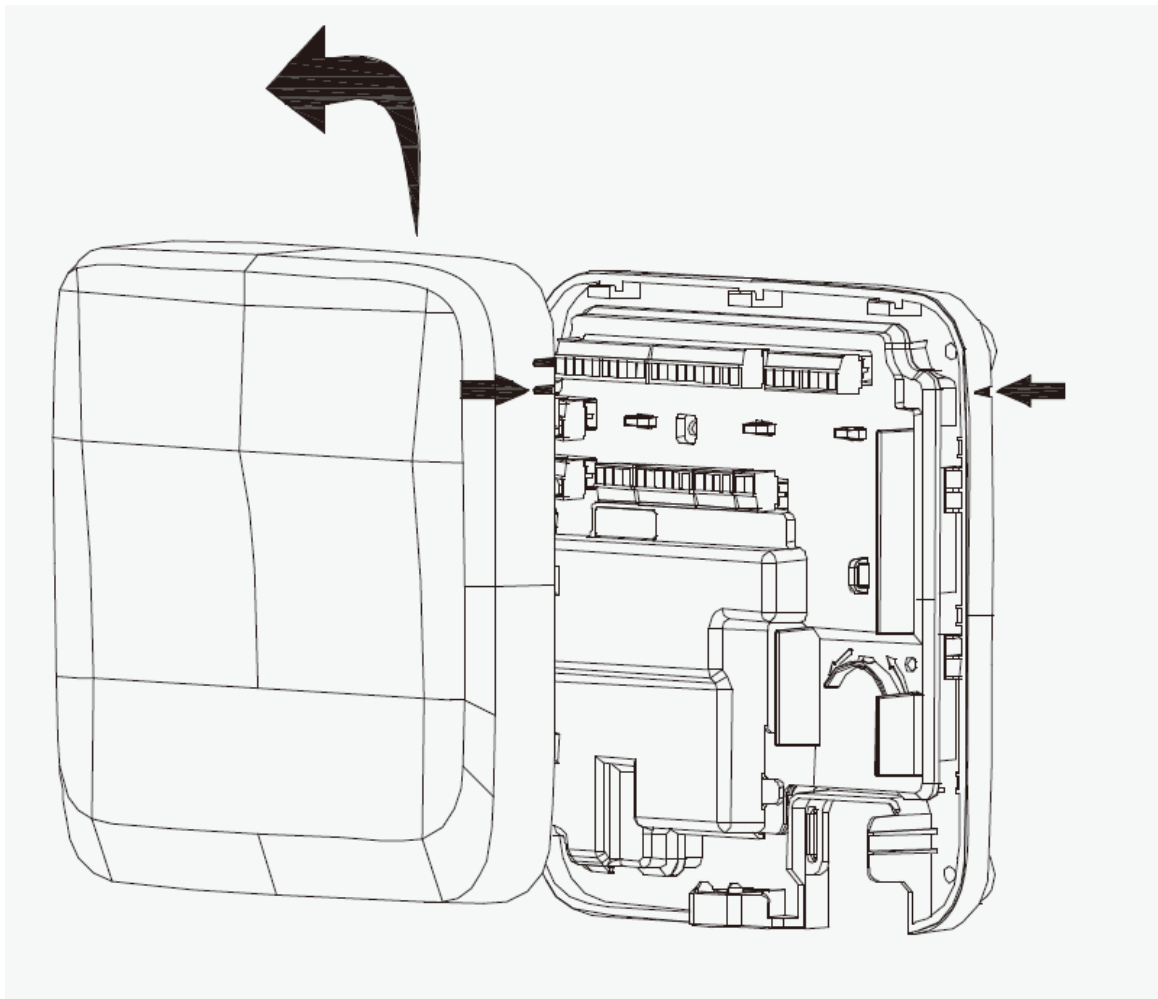
- Step 1 Paste the positioning map to the wall at an appropriate position.
- Step 2 Drill holes through the marks on the map.
- Step 3 Hammer in the expansion tubes, and then remove the map.

Figure 4-0 Hammer in the expansion tubes



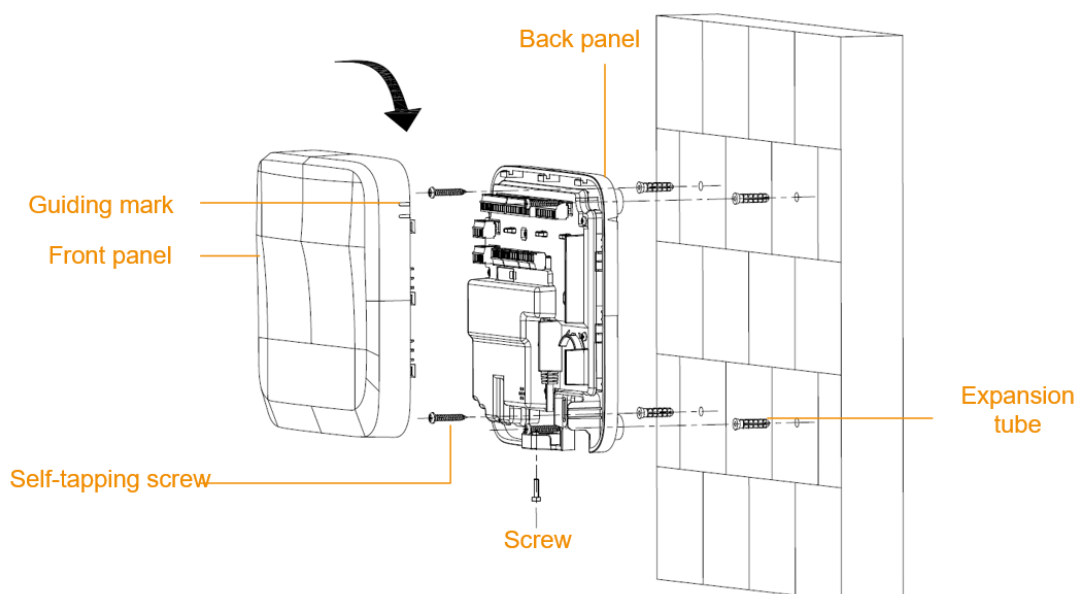
- Step 4 Slide up the front panel of the Access Controller and remove the panel.

Figure 4-1 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 4-2 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 4-3 DIN clips

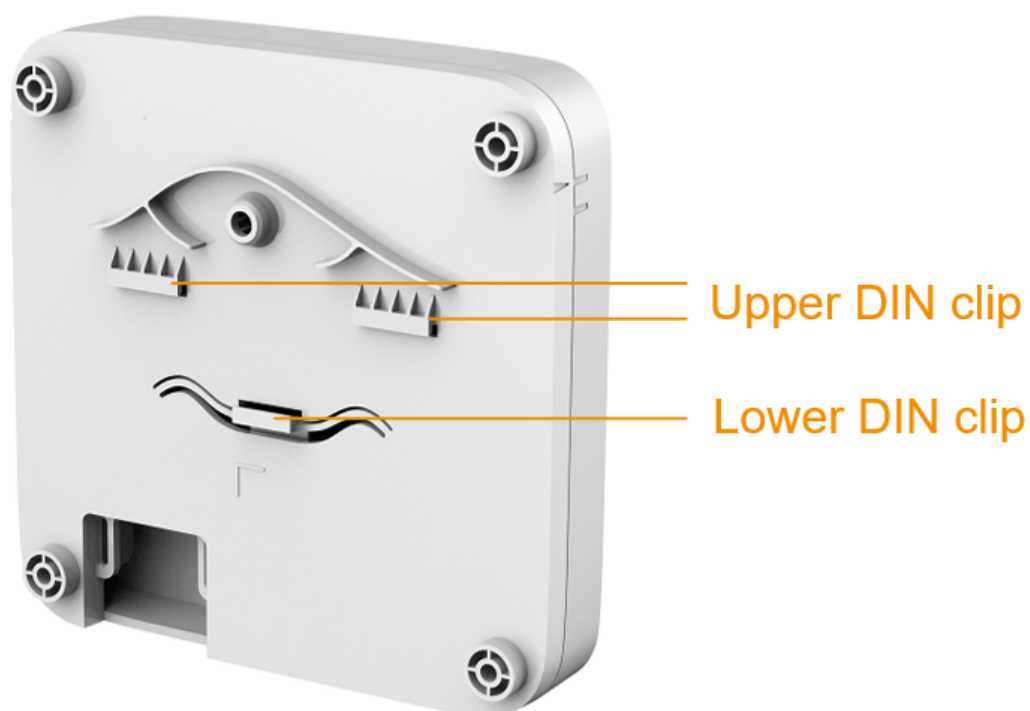
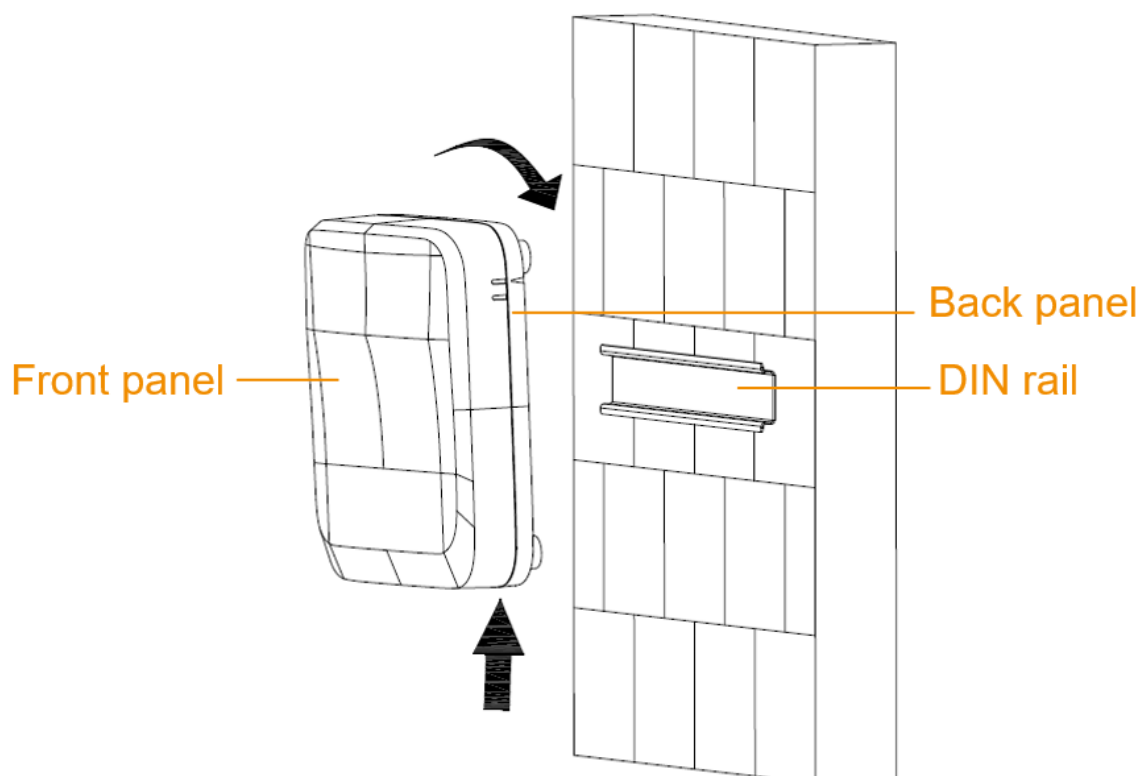


Figure 4-4 Hook DIN clips to the rail

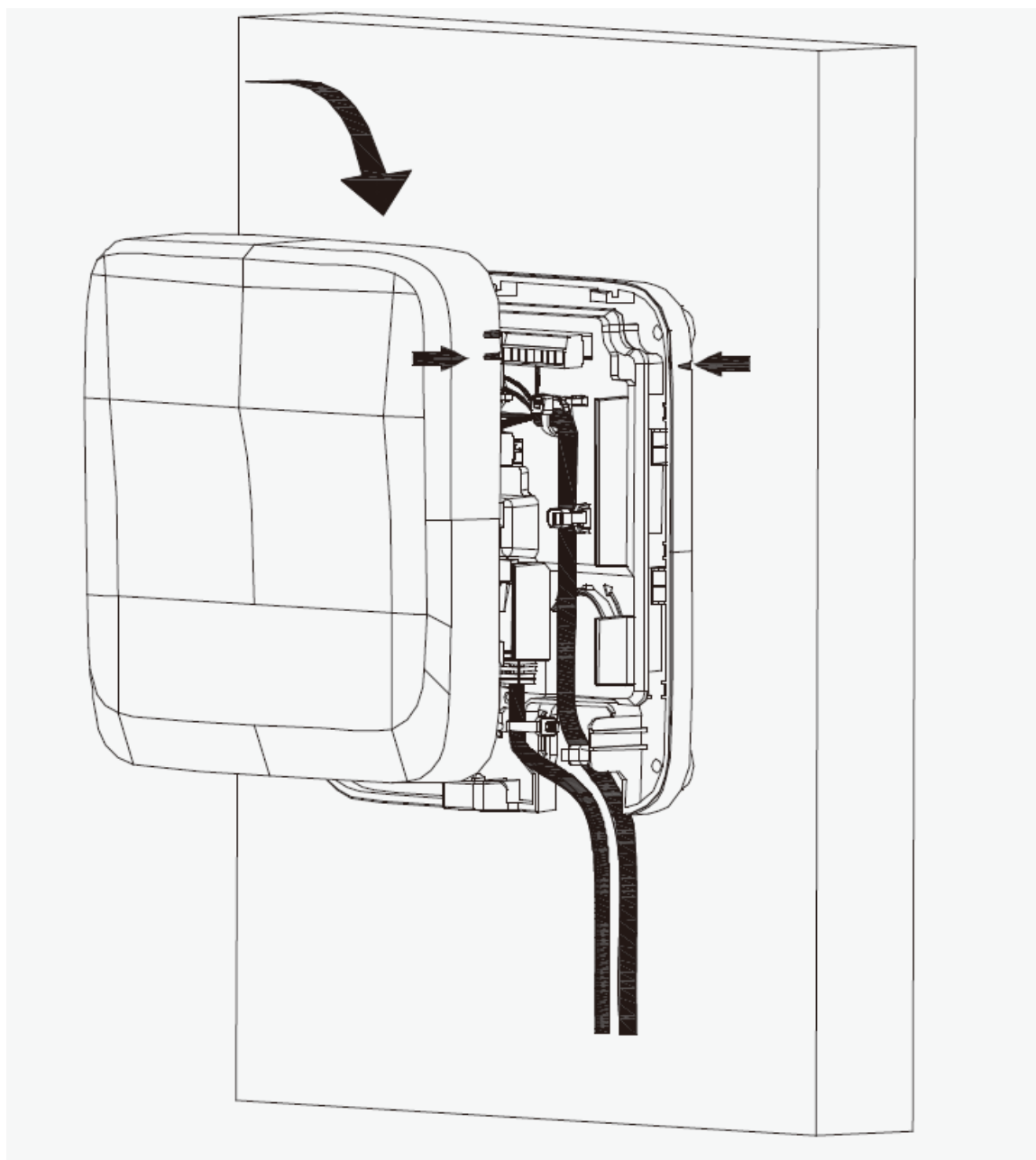


Step 3 Slide up the front panel of the Access Controller to remove the cover.

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 4-5 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.

5.1 Networking Diagram

Figure 5-0 Networking diagram

Web-centric Access Control Solution

- 1 Main controller + 19 Sub controller
- Up to 40 doors

The diagram illustrates a multi-story building with a complex access control system. A central 'Main Controller' is connected to a 'Sub Controller' and a 'PoE switch'. The 'Main Controller' is also connected to an 'Enrollment Reader' via a 'USB' cable. A 'Management platform' is shown with a 'Webpage login' interface. The 'Sub Controller' is connected to two 'ASR2200A-B' readers and an 'ASR2102A' reader. The 'PoE switch' is connected to the 'Sub Controller' and a 'PoE switch' (labeled 'PoE switch' in the diagram). A 'DMSS' (Mobile Device Management System) is connected to a 'Dcloud' cloud service. A 'Mobile phone' is shown with a signal icon. A 'Legend' in the bottom right corner indicates: Blue line for CAT 5e, Green line for RS485, and Red line for I/O.

5.2 Configurations of Main Controller

5.2.1 Configuration Flowchart

```
graph LR; Start([Start]) --> Initialize[Initialize]; Initialize --> LogIn[Log In]; LogIn --> AddDevices[Add devices]; AddDevices --> AddUsers[Add users]; AddUsers --> AddWeeklyPlan[Add weekly plan]; AddWeeklyPlan --> AddHolidayPlan["(Optional) Add holiday plan"]; AddHolidayPlan --> AddAreas[Add areas]; AddAreas --> AddPermissionRules[Add permission rules]; AddPermissionRules --> ViewAuthProgress[View authorization progress]; ViewAuthProgress --> ConfigAlarmLinkage["(Optional) Configure global alarm linkage"]; ConfigAlarmLinkage --> End([End]); AddDevices -.-> SelectControlMode[Select control mode]; AddDevices -.-> ConfigureHardware[Configure hardware]; AddDevices -.-> AddOneByOne[Add one by one]; AddDevices -.-> AddInBatches[Add in batches];
```

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 192.168.1.108 by default) of the main controller.



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

Step 2 Select a language, and then click **Next**.

Step 3 Read the software license agreement and privacy policy carefully, select **I have read and agree to the terms of the Software License Agreement and Privacy Policy.**, and then click **Next**.

Step 4 Set the password and email address.



- 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.

Step 5 Configure the system time, and then click **Next**.

Figure 5-2 Configure the time

The screenshot shows a web interface for configuring system time. It features three main sections: 'Date Format' with a dropdown menu set to 'YYYY-MM-DD', 'Time Zone' with a dropdown menu set to '(UTC+08:00) Beijing, Chongqing, Hong ...', and 'System Time' with a text field showing '2022/06/21 16:09:58' and a 'Sync PC' button. A large blue 'Next' button is positioned at the bottom center of the form.

Step 6 (Optional) Select **Auto Check for Updates** , and then click **Completed**.

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.

Step 7 Click **Completed**.

The system automatically goes to the login page after initialization is successful.

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 5-3 Type of access controller

Main Control

Main controller offers management functions like the platform. You can also set up the system through the wizard, configure access control settings, and access person management, remote device management, and event records.

Sub Control

Sub controllers can be added to the main controller or platform. You can also set up the system through the wizard, configure network and alarming settings, and perform updates.

Next

- **Main Control:** The main controller comes with a management platform. You can manage all sub-controllers, configure access control, access personal management on the platform, and more.
- **Sub Control:** Sub controllers needs to be added to the management platform of the main controller or other management platforms such as DSS Pro or SmartPSS Lite. You can perform the configurations on the webpage of the sub-controller.

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


Step 4 Configure the parameters of the doors.

Figure 5-4 Configure door parameters

The screenshot displays a configuration window for two doors, Door1 and Door2. Each door's settings are organized into two main sections. The left section contains three checkboxes: 'Entry Card Reader' (checked), 'Exit Button' (checked), and 'Door Detector' (unchecked). Below these is the 'Card Reader Protocol' section, which includes radio buttons for 'Wiegand', 'OSDP', and 'RS-485' (selected). A 'Single' dropdown menu and an 'LED' label are also present. The right section, titled 'Power Supply of Locks', offers two radio button options: '12V' (selected) and 'Relay'. The '12V' option has a 'Fail Secure' dropdown menu, while the 'Relay' option has a 'Relay Open = Locked' dropdown menu. Both dropdowns include a help icon. At the bottom of the window are 'Back' and 'Next' buttons.

Table 5-1 Parameter description

Parameter	Description
Entry Card Reader	<p>Select the card reader protocol.</p> <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	Connects to an exit button.
Door Detector	Connects to a door detector.
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.

Parameter	Description
	<p>◇ Relay open = unlocked: Sets the lock to unlock when the relay is open.</p> <p></p> <p>The electromagnetic lock unlocks in a instant and locks again immediately when the Access Controller is in the soft reboot.</p>

Step 5 Configure 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 can not be selected when you set the combination method to **And**.

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

Figure 5-5 Unlock settings

Unlock Settings

Unlock Mode

Combination Unlock

Combination Method

☒ Or
 ☐ And

Unlock Method (Multi-select)

☒ Card
 ☒ Fingerprint
 ☒ Password
 ☒ Bluetooth Card

Bluetooth Mode

☐ Short-range
 ☒ Mid-range
 ☐ Long-range

Door Unlocked Duration


s (0.2-600)

Unlock Timeout

s (1-9999)

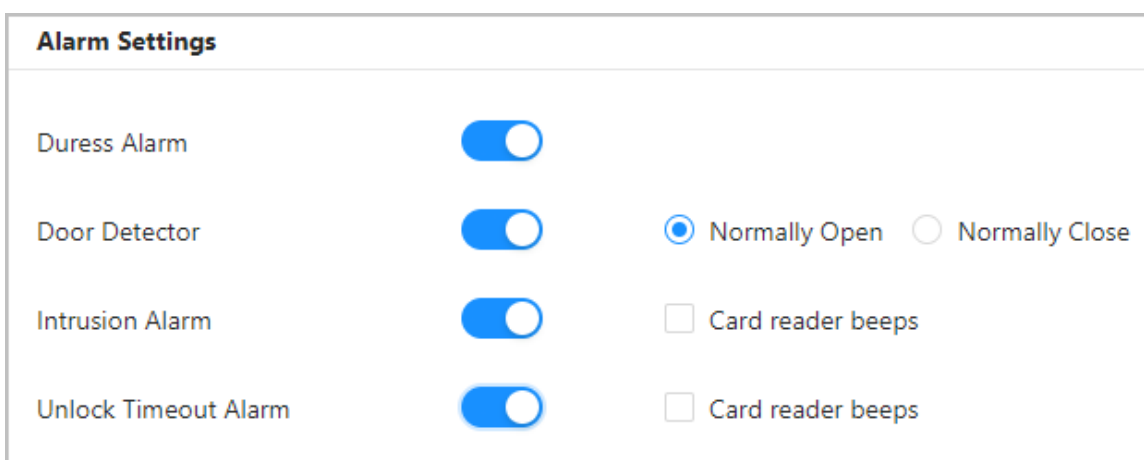
Table 5-2 Unlock settings description

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 0.2 m. • Mid-range: The Bluetooth unlock range is less than 2 m. • Long-range: The Bluetooth unlock range is less than 10 m.

Parameter	Description
	 The Bluetooth unlock range might differ depending on models of your phone and the environment.
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 s to 600 s.
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.

Figure 5-6 Alarm



Alarm Settings

Duress Alarm ☒

Door Detector ☒ ☒ Normally Open ☐ Normally Close

Intrusion Alarm ☒ ☐ Card reader beeps

Unlock Timeout Alarm ☒ ☐ Card reader beeps

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 Detector	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	

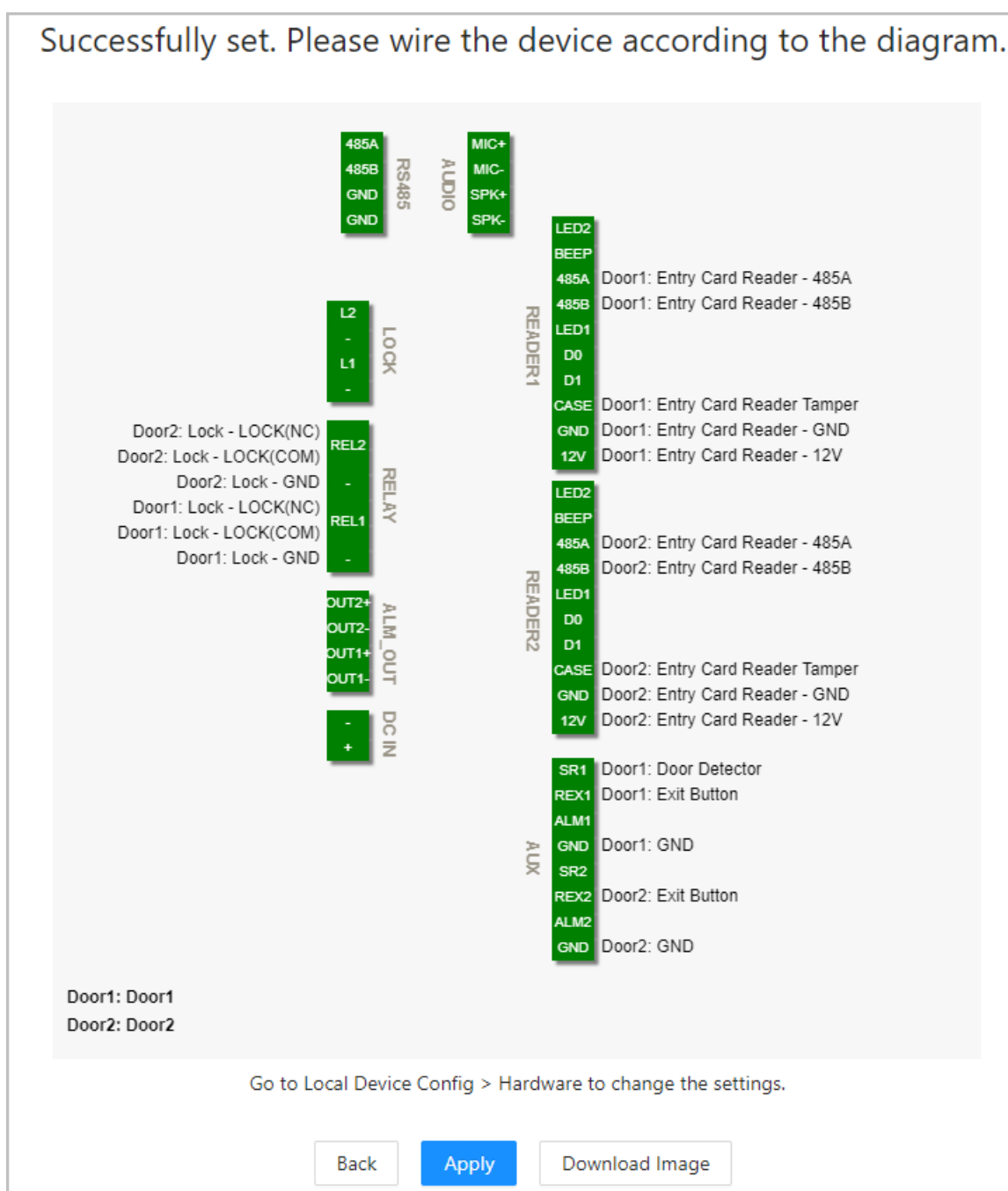
Step 9 Click **Next**.

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 5-7 Wiring diagram



Step 10 Click **Apply**.

- You can go to **Local Device Config** > **Hardware** 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 **Local Device Config** > **Hardware**.

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 Device One by One

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

Procedure

Step 1 On the home page, click **Device Management**, and then click **Add**.

Step 2 Enter the device information.

Figure 5-8 Device information

Table 5-4 Device parameters Description

Parameter	Description
Device Name	Enter the name of the 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 37777 by default.
Username/Password	Enter the username and password of the Controller.

Step 3 Click **OK**.

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

Figure 5-9 Successfully add devices

Add		Search Device	Modify IP	Sync Time	Delete	Total Devices 1 Online Devices 1			
<input type="checkbox"/>	No.	Device Name	IP Address	Device Type	Device Model	Port	Connection Status	SN	Operation
<input type="checkbox"/>	1	192.168.1.2	192.168.1.2	Access Controller	ETH-AC3200	37777	Online	8000E7F9A0C0E	



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 On the home page, Click **Device Management**, and then click **Search Device**.

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

Figure 5-10 Auto search

Search Device

Start Search

Device Initialization

IP Segment

192.168.1.0/24

Search

<input type="checkbox"/>	No.	IP Address	Device Type	MAC Address	Port	Initialization Status
<input type="checkbox"/>	1	192.168.1.2	ETH-AC3200	8000E7F9A0C0E	37777	Initialized
<input type="checkbox"/>	2	192.168.1.3	ETH-AC3200	8000E7F9A0C0E	37777	Initialized
<input type="checkbox"/>	3	192.168.1.4	ETH-AC3200	8000E7F9A0C0E	37777	Initialized
<input type="checkbox"/>	4	192.168.1.5	ETH-AC3200	8000E7F9A0C0E	37777	Initialized
<input type="checkbox"/>	5	192.168.1.6	ETH-AC3200	8000E7F9A0C0E	37777	Initialized

<

1

2

3

4

5

>

Add

Cancel

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 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.

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

Related Operations

- **Export all the users to Excel:** On the **Person 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 **Person Management** page, click **Download Template**, enter user information in the template, and then click **Import** to import all users.
- **Extract all the users:** On the **Person 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 Departments

Procedure

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

Step 2 Create a department.

- Click **+**.
- Enter the name of the department, and then click **Add**.



The default department cannot be deleted.

Figure 5-11 Add department

The screenshot shows a modal dialog titled "Add" with a close button (X) in the top right corner. Inside the dialog, there are two input fields. The first field is labeled "Upper Level Department" and has a dropdown menu currently showing "Default Company". The second field is labeled "* Department Name" (with a red asterisk indicating it is required) and contains the text "human resources". At the bottom right of the dialog, there are two buttons: a blue "Add" button and a grey "Cancel" button.

Step 3 Click **OK**.

5.2.5.2 Adding Roles

Procedure

Step 1 On the home page, select **Person 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.

- a. Click **+**.
- b. Enter the name of the role, and then click **Add**.

5.2.5.3 Configuring Basic User Information

Procedure

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

Step 2 Add users.

- Add users one by one.
 - a. Click **Add**, and then enter the basic information for the user.

Figure 5-12 Basic information on the user

The screenshot shows a web form titled 'Add' with a close button (X) in the top right corner. Below the title bar, there are two tabs: 'Basic Info' (selected) and 'Authentication'. The form contains the following fields:

- * User ID**: Text input with value '292309'.
- * User Name**: Text input with value 'TOM'.
- * Department**: Dropdown menu with value 'Default Company'.
- * User Type**: Dropdown menu with value 'General User'.
- Validity Period**: Two date pickers. The first has value '2023-06-13 00:00:00' and the second (labeled 'To') has value '2037-12-31 23:59:59'.
- Role**: Dropdown menu with value 'Manager'. A link 'Add Role' is next to it.
- Email**: Text input with value '11841...@...com'.
- * Unlock Attempts**: Text input with value 'Unlimited'.

At the bottom right, there are three buttons: 'Add' (blue), 'Add More', and 'Cancel'.

Table 5-5 Parameters description

Parameter	Description
User ID	The ID of the user.
Department	The department that the user belongs to. For details on how to create departments, see "5.2.5.1 Adding Departments".
Validity Period	Set a date on which the access permissions of the person will become effective.
Role	Assign an existing role to the user. You can also click Add Role to create a new role.
Email	The email address must be the same as the one that was used to sign up for DMSS.
To	Set a date on which the access permissions of the person will expire.
User Name	The name of the user.
User Type	<p>The type of user.</p> <ul style="list-style-type: none"> ◇ General User : General users can unlock the door. ◇ VIP User : When the VIP unlocks the door, service personnel will receive a notice. ◇ Guest User : Guests can unlock the door within a defined period or for a set number of times. After the defined period expires or the number of times for unlocking runs out, they cannot unlock the door. ◇ Patrol User : Patrol users will have their attendance tracked, but they have no permission to unlock the door. ◇ Blocklist User : When users in the blocklist unlock the door, service personnel will receive a notification.

Parameter	Description
	◇ Other User : When they unlock the door, the door will stay unlocked for 5 more seconds.
Unlock Attempts	The number of times a guest user can unlock the door.

b. Click **Add**.

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

- Add users through importing the template.
 - a. Click **Import** > **Download Template** to download the user template.
 - b. Enter user information in the template, and then save it.
 - c. Click **Import**, and upload the template to the Platform.

The users are added to the Platform automatically.

- Use **Quick Add** to easily add users.
 - a. Click **Quick Add**.
 - b. Enter the start number of the user ID, and the quantity.

The platform will generate a sequence of numbers starting from the defined start number. For example, if the start number is 999, and the quantity is 5, the system will generate a sequence of numbers from 999 to 1003.

Figure 5-13 Quick add

Quick Add

* Start No.

999

* Quantity

5

Department

Default Company\A\B

Role

Default

Effective Time

2023-06-13 00:00:00 → 2037-12-31 23:59:59

User ID	Card Number
999	890
1000	789
1001	
1002	
1003	

Issue Card Config

Card Reader

Enrollment Reader

Modify

Card Number

Press the Enter key to enter.

Start Issuing Cards

Add

Cancel

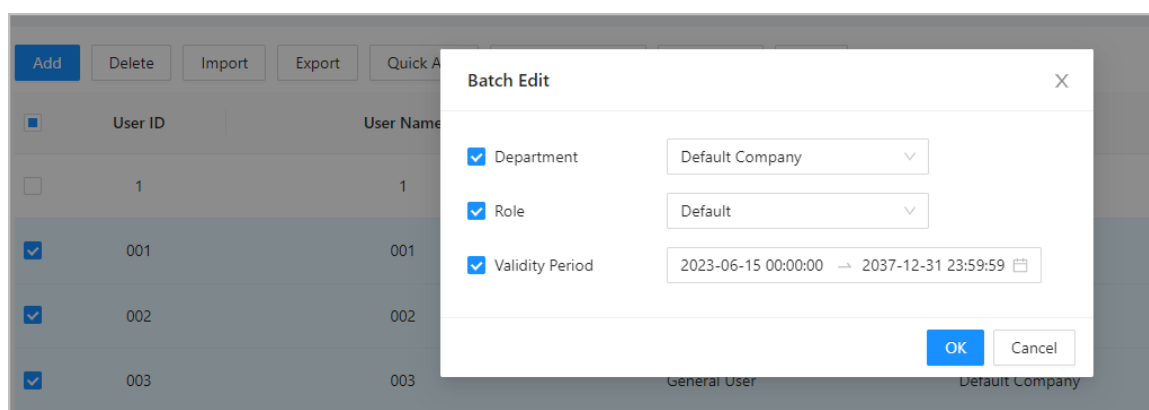
- c. Select the department, role and the effective time.
- d. Issue cards to the users in batches.

You can manually enter the card number, or use the enrollment reader or card reader to read the card number. For details, see "5.2.5.4.2 Adding Cards".

Related Operations

Batch Edit: Edit personal information in batches.

Figure 5-14 Batch edit



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.

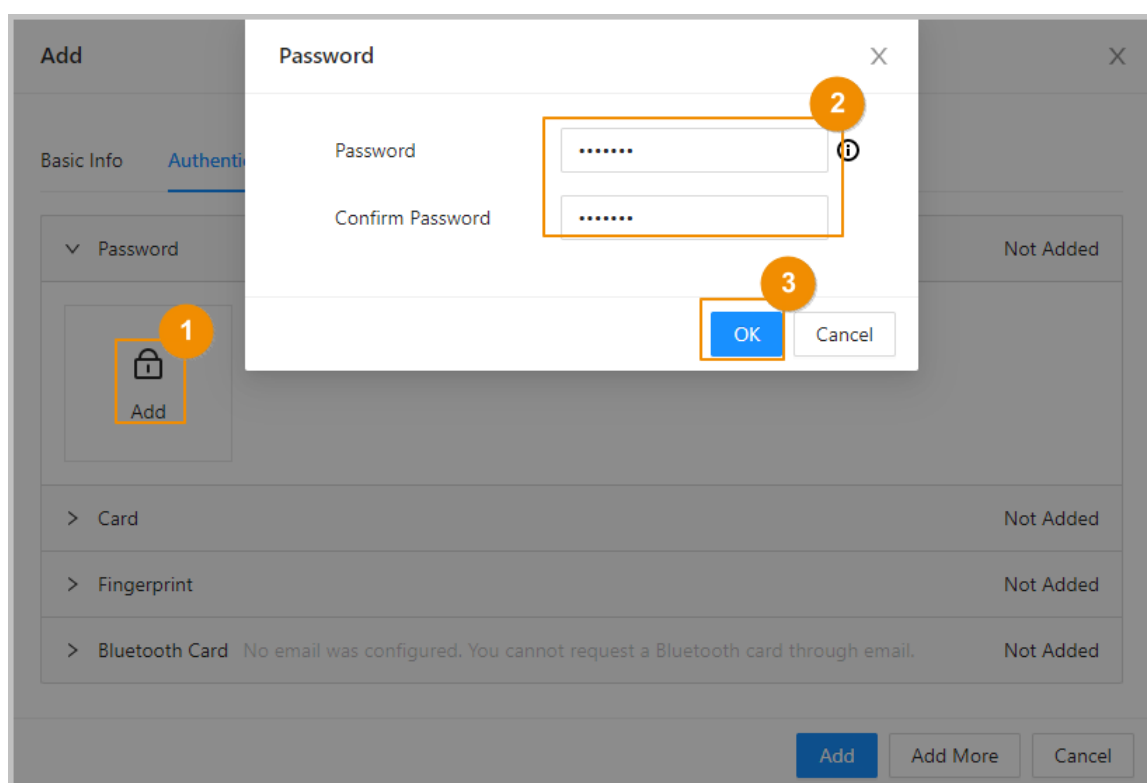
5.2.5.4.1 Adding Passwords

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

Procedure

- Step 1 On the **Authentication** tab, click **Add**
- Step 2 Enter and confirm the password.
- Step 3 Click **OK**.

Figure 5-15 Add the password



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.
- On the **Person Management** page, select **More > Card Type**.
 - If you plan on issuing 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. For details, see Click Add. Click Modify, and then select Enrollment Reader. Make sure that the card enrollment reader is connected to your computer. Follow the on-screen instructions to download and install the plug-in. 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. Click Add. .

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

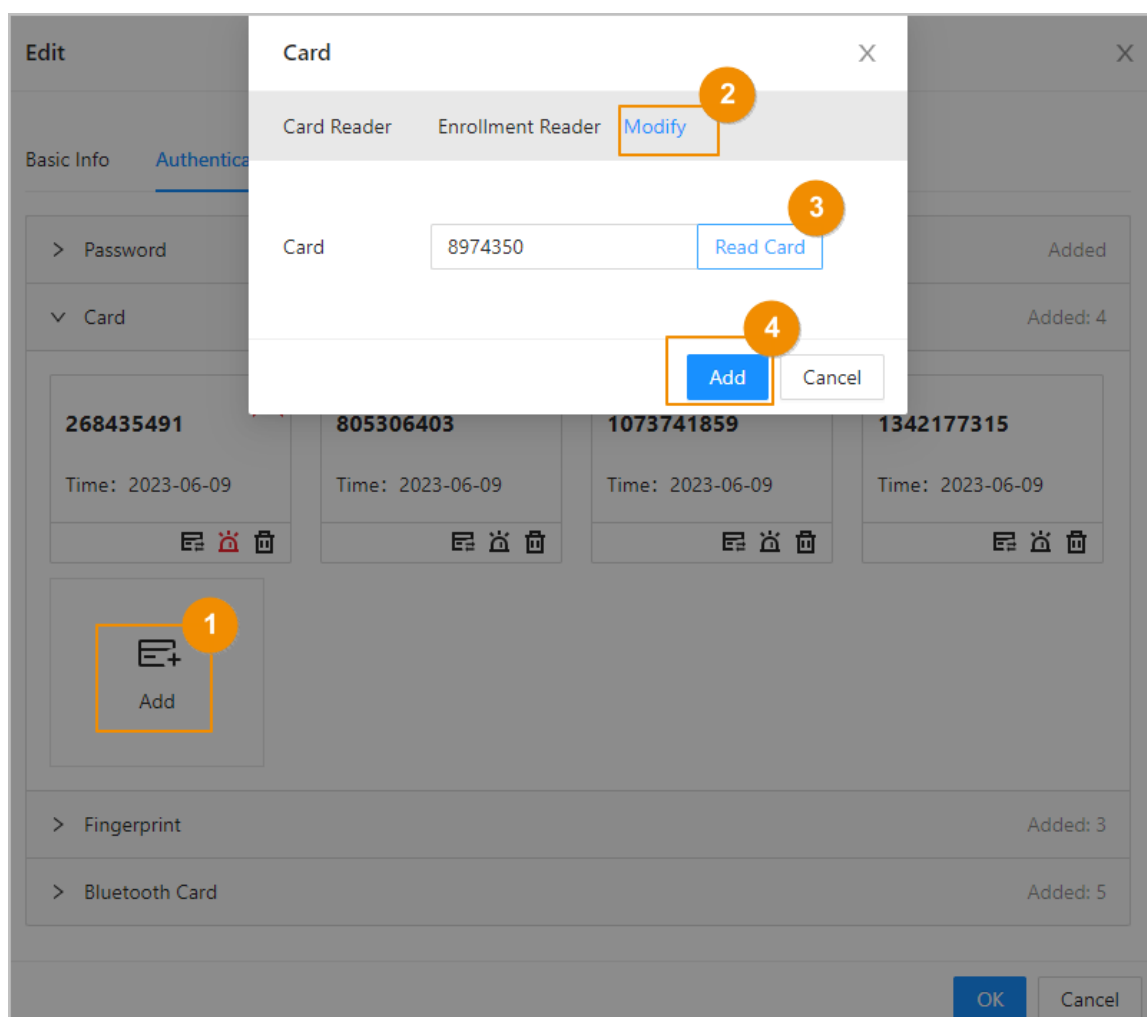
Step 2 On the **Authentication** tab, click **Card** to add cards.

4 methods are available to add cards.

- Enter the card number manually.
 - Click **Add**.

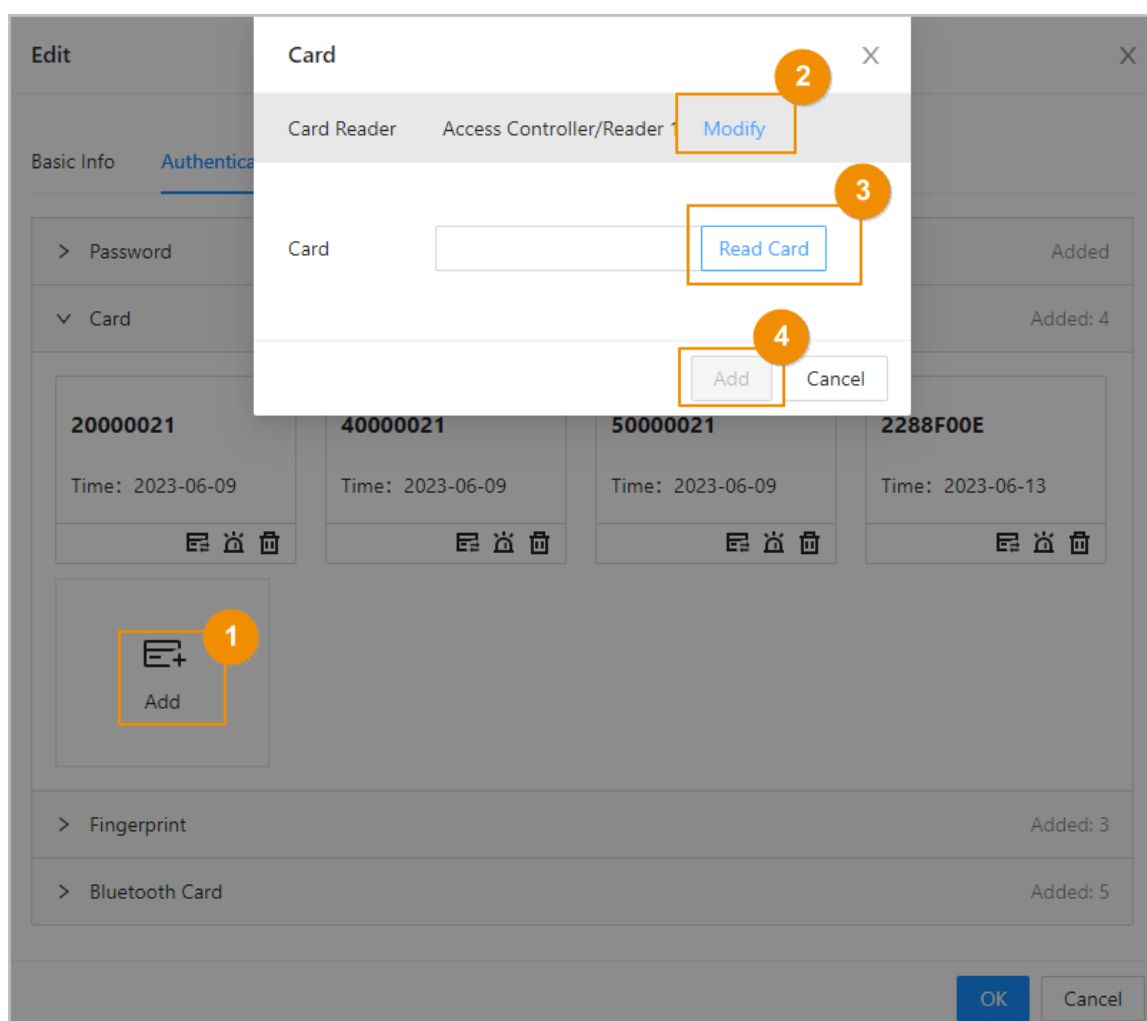
- b. Enter the card number, and then click **Add**.
- Use the enrollment reader to read the card number.

Figure 5-16 Use the enrollment reader to read the card number



- a. Click **Add**.
- b. Click **Modify**, and then select **Enrollment Reader**.
Make sure that the card enrollment reader is connected to your computer.
- c. Follow the on-screen instructions to download and install the plug-in.
- d. 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.
- e. Click **Add**.
- Use the card reader to read the card number.

Figure 5-17 Use the card reader to read the card number



- a. Click **Modify**, and then select a card reader.
Make sure that the card reader is connected to the Access Controller.
 - b. 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.
 - c. Click **Add**.
- Add cards in batches: Issue cards to users in batches.
 - a. Click **Batch Issue Cards**, and then select **Issue Cards to Selected Users** or **Issue Cards to All Users**.
 - b. You can manually enter the card number, or click **Modify** to issue cards through the enrollment reader or card reader.

Figure 5-18 Issue cards through the enrollment reader or card reader

Batch Issue Cards

Card Bluetooth Card

Issue Cards

User ID	User Name	Card Number	Operation
00003	00003		⊖
00004	00004		⊖
10000021	zhangsan21	The number of cards for ...	⊖
10000022	zhangsan22	The number of cards for ...	⊖

User ID: 00003 User Name: 00003
 User Type: VIP User Email:
 Department: Default Company Role: Default
 Effective Time: 2023-06-13 00:00:00~2023-12-31 23:59:59

Issue Card Config

Card Reader: Enrollment Reader Modify **1**

Card Number: Start Issuing Cards **2**

OK Cancel **3**

Related Operations

- : Change the number of the card.
- : Set the card to duress card.
An alarm is triggered when people use the duress card to unlock the door.
- : Delete the card.

5.2.5.4.3 Adding Fingerprints

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

Procedure

Step 1 On the **Authentication** tab, click **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 DMSS. For details, see "5.2.11 Configuring Cloud Service".
- Users have been added to the Platform of the Access Controller. For details, see "5.2.5.3 Configuring Basic User Information".
- General users, such as company employees, have installed and signed up for DMSS with their email.

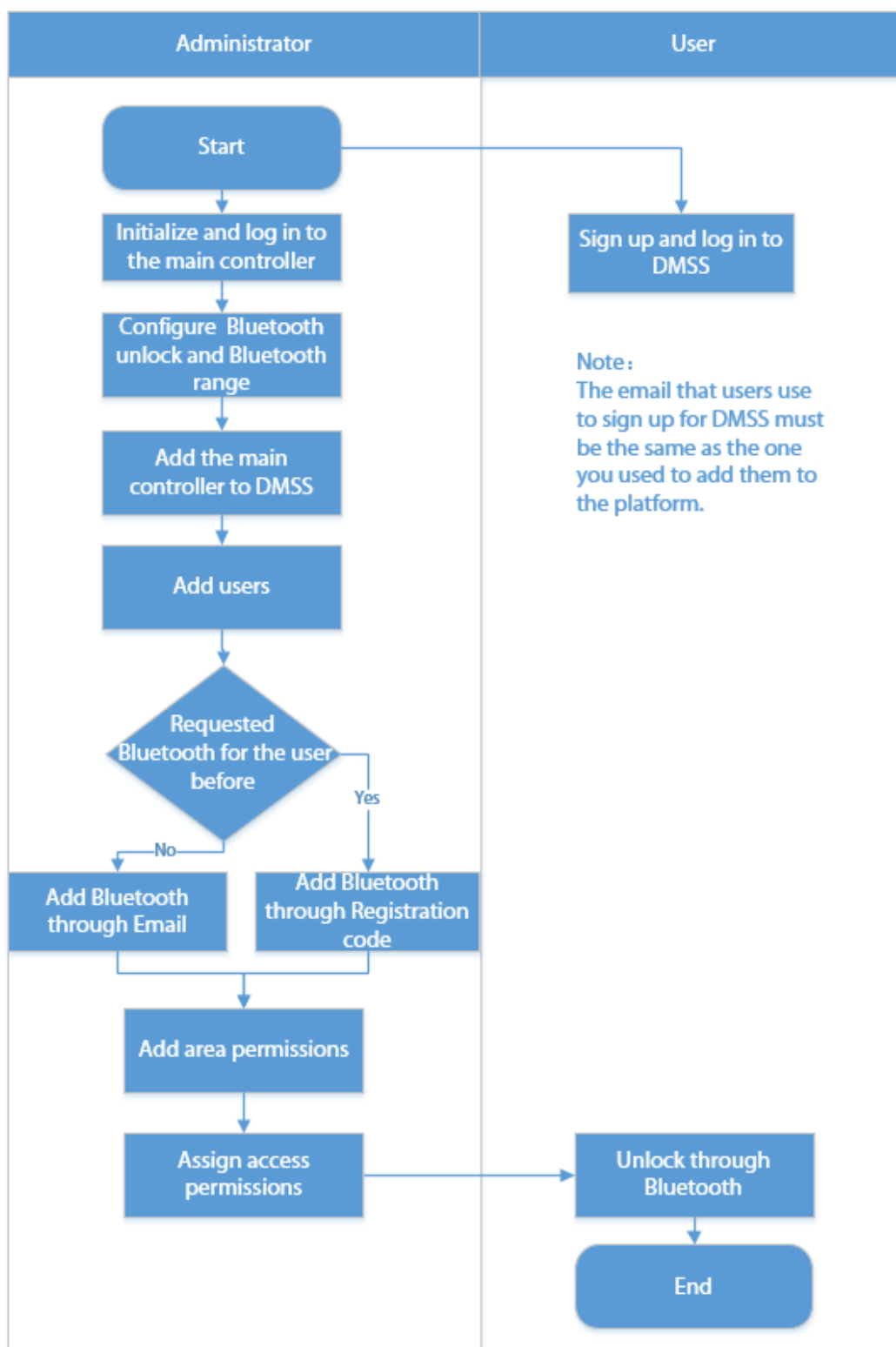


The email that users use to sign up for DMSS must be the same as the one you used to add them to the access controller.

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 DMSS with their email to unlock doors using Bluetooth cards that were issued to them.

Figure 5-19 Flowchart for configuring Bluetooth unlock



Procedure

- Step 1** On the 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.

Figure 5-20 Request through Email

The screenshot shows a user management interface with an 'Edit' window. The 'Authentication' tab is active, displaying a list of authentication methods. The 'Bluetooth Card' method is expanded, showing four generated card numbers. The 'Request through Email' button is highlighted with an orange box, indicating the next step in the process.

- Request through Email in batches.
 - a. On the **Person 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**.

- b. Click **Bluetooth Card**.
- c. 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**, enter the emails in the correct format, and then click **Import**. They will be moved to the requestable list.

Figure 5-21 Batch issue cards

Batch Issue Cards

Card Bluetooth Card

Bluetooth cards can only be generated in batches through emails.

Issue Cards

Requestable (3)

Non-Requestable (1)

Export Users that Lack Emails

Import

User ID	User Name	Email	Bluetooth Card No.	Status	Operation
001	001	118[REDACTED].com	0		⊖
002	002	118[REDACTED].com	0		⊖
003	003	116[REDACTED].com	0		⊖

User ID

001

User Name

001

User Type

General User

Email

118[REDACTED].com

Department

Default Company

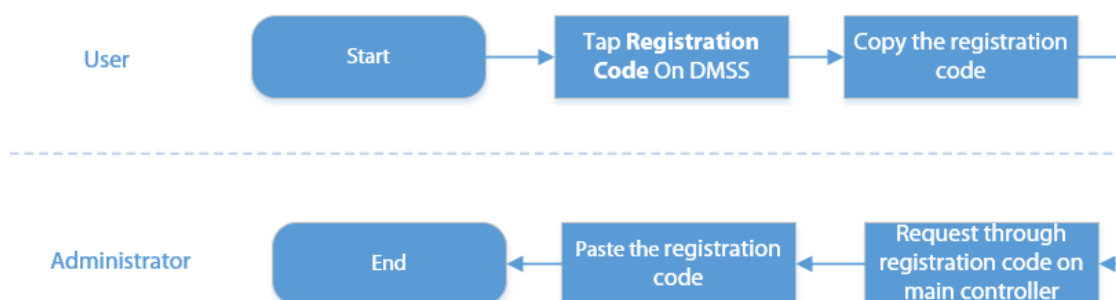
Effective Time

2023-06-15 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. using registration codes.

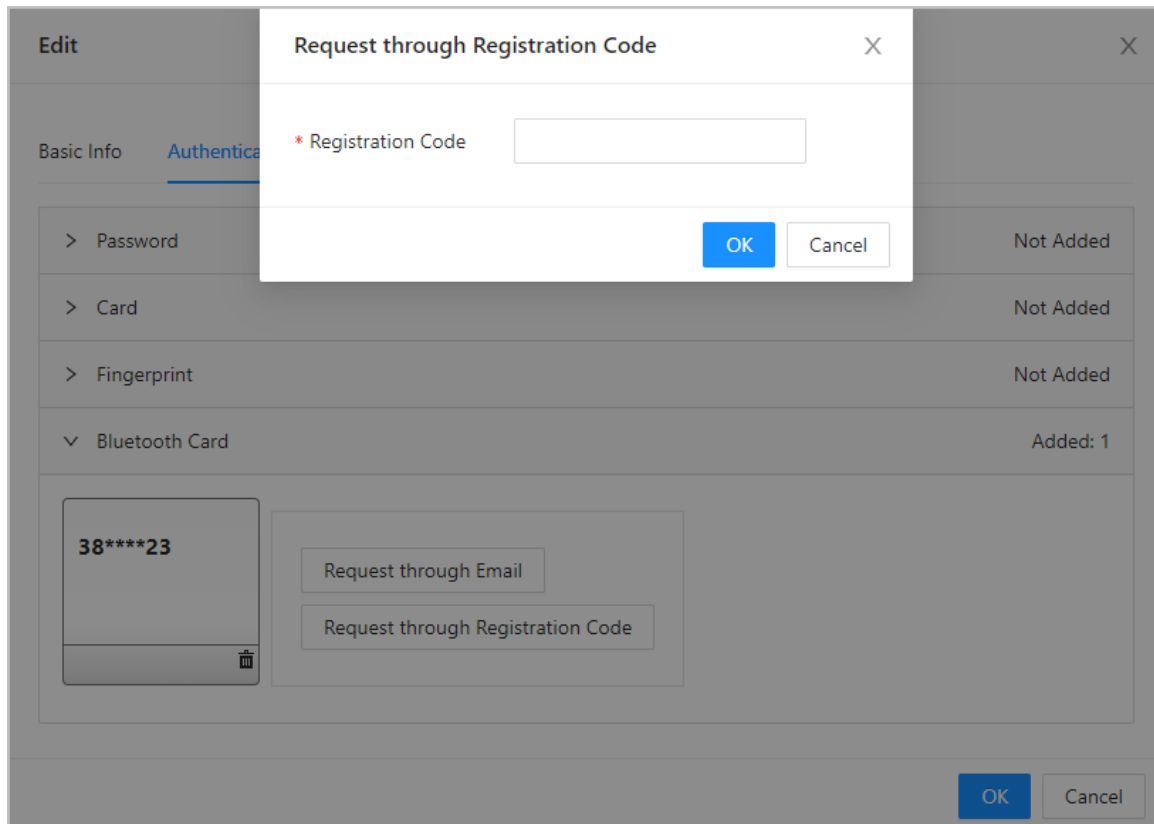
Figure 5-22 The flowchart for requesting through registration code



- On DMSS, tap **Registration Code** of a Bluetooth card.
The registration code is automatically generated by DMSS.
- Copy the registration code.

- c. On the **Bluetooth Card** tab, click **Request through Registration Code**, paste the registration code, and then click **OK**.

Figure 5-23 Request through registration code



- d. Click **OK**.

The Bluetooth card is added.

Step 2 Click **OK**.

Results

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

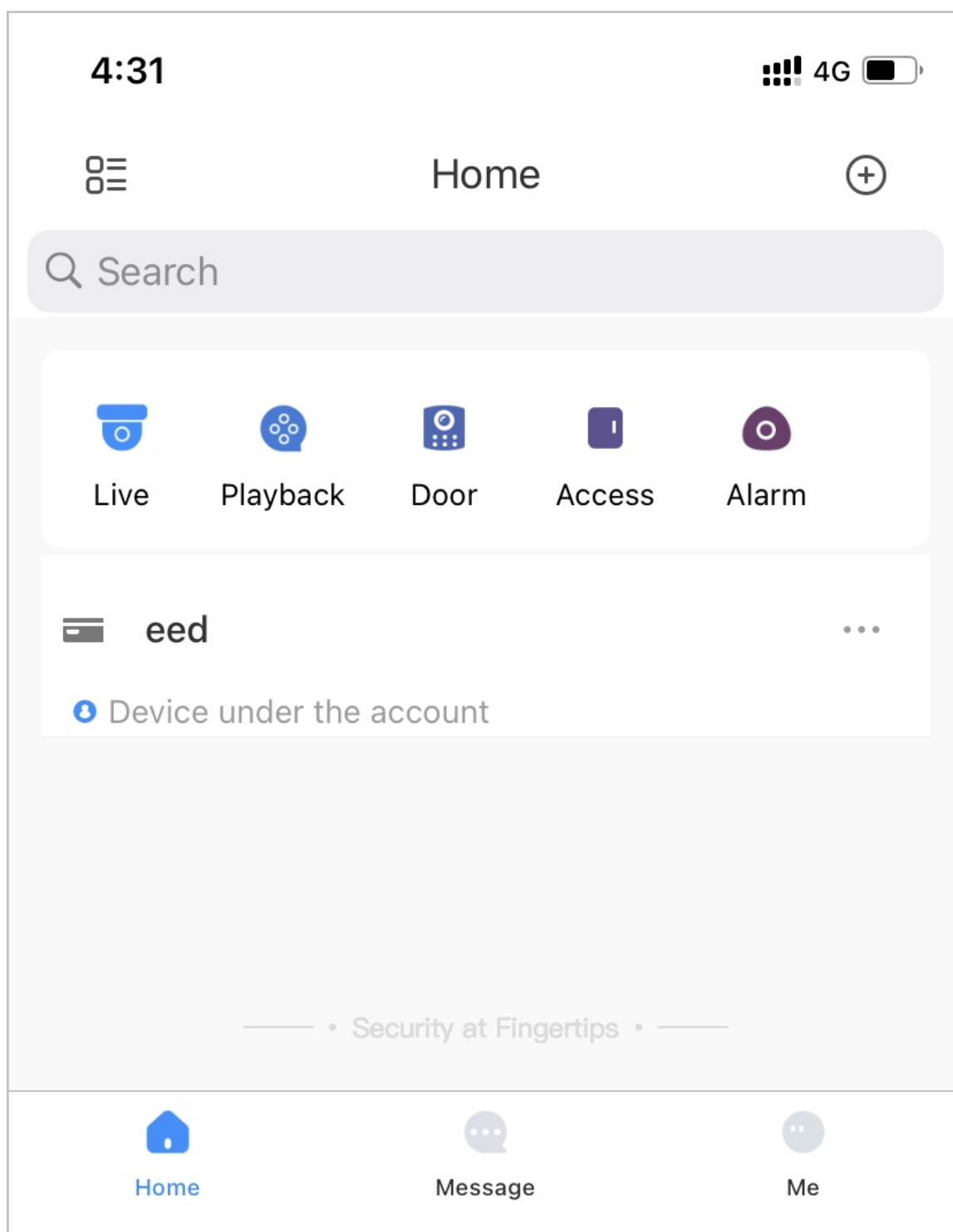
- **Auto Unlock:** The door automatically unlocks when you are in the defined Bluetooth range, which allows the Bluetooth card to transmit signals to the card reader.



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.

Figure 5-24 Unlock the door through Bluetooth cards



Related Operations

- Users can manage Bluetooth cards on DMSS.
 - ◇ 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 **Person Management** page, click **More** > **Bluetooth Card Records** to view the request status.

Figure 5-25 Request status

Bluetooth Card Records				
No.	Time	Status	Operation	
1	2023-03-09 10:26:31	Successful: 0, failed: 1.	View Details	Request Again
2	2023-03-09 10:25:59	Successful: 0, failed: 1.	View Details	Request Again
3	2023-03-09 10:25:49	Successful: 0, failed: 1.	View Details	Request Again

- ◇ 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 On the home page, select **Access Control Config** > **Weekly Plan**, and then click **+**.



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

- Step 2 Enter the name of the time template.

Figure 5-26 Create the weekly plan

Step 3 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 time sections for each day.

Step 4 Click **Apply**.

5.2.7 Adding Areas

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

Procedure

Step 1 Click **Access Control Config > Area Settings**.

Step 2 Click **+** to add areas.

You can add up to 40 area permissions.

Figure 5-27 Add areas

Step 3 Enter the name of the area.

Step 4 Select doors.

Step 5 Click **Apply**.

5.2.8 Adding Permission Rules

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

Procedure

Step 1 On the home page, select **Access Control Config** > **Permission Settings**.

Step 2 Click + to add a permission rule.

Figure 5-28 Assign permissions in batches

Step 3 Enter the name of the permission rule.

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

You can select personnel on the department, role or individual users.

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



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

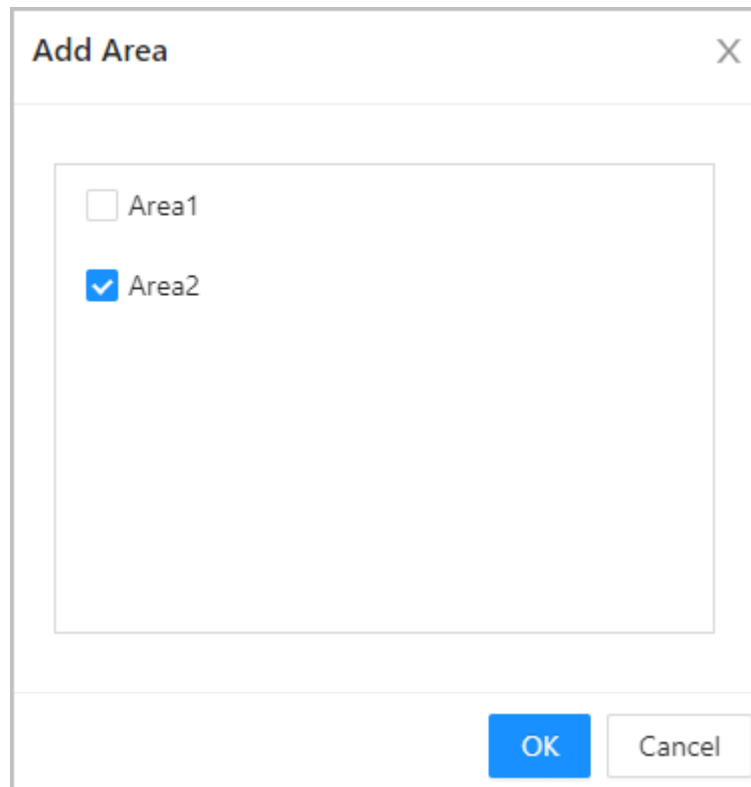
Figure 5-29 Add personnel



You can click **+** to create new permission groups. For details on creating permission groups, see "5.2.7 Adding Areas".

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

Figure 5-30 Add area



The 'Add Area' dialog box contains a list of areas. 'Area1' is unchecked, and 'Area2' is checked with a blue checkmark. At the bottom right, there are 'OK' and 'Cancel' buttons.

Step 6 In the **Time Templates** area, select the weekly plan and the holiday plan.

Step 7 Click **Apply**.

Related Operations

5.2.9 Viewing Authorization Progress

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



Procedure

Step 1 On the home page, select **Access Control Config** > **Authorization Progress**.


Step 2 View the authorization progress.

- Sync SubControl Person: Sync personnel on the main controller to the sub-controller.
- Sync Local Person: Sync personnel on the management platform of the main controller to its server.
- Sync Local Time: Sync the time templates in the area permissions to the sub-controller.

Figure 5-31 Authorization progress

Area Permission	Device Name	Type	Progress	Results	Time	Operation
	186	Sync SubControl Person	<div><div></div></div>	Succeed: 1, Failed: 0	2022-08-12 20:01:59	
	186	Sync SubControl Person	<div><div></div></div>	Succeed: 0, Failed: 1	2022-08-12 20:01:23	 
	186	Sync Local Person	<div><div></div></div>	Succeed: 1, Failed: 0	2022-08-12 20:01:23	

Step 3 (Optional) If authorization failed, click  to try again.

You can click  to view details on the failed authorization task.

5.2.10 Configuring Global Alarm linkages (Optional)

You can configure global alarm linkages across different Access Controllers.

Procedure

Step 1 Select **Access Control Config > Global Alarm Linkage**.

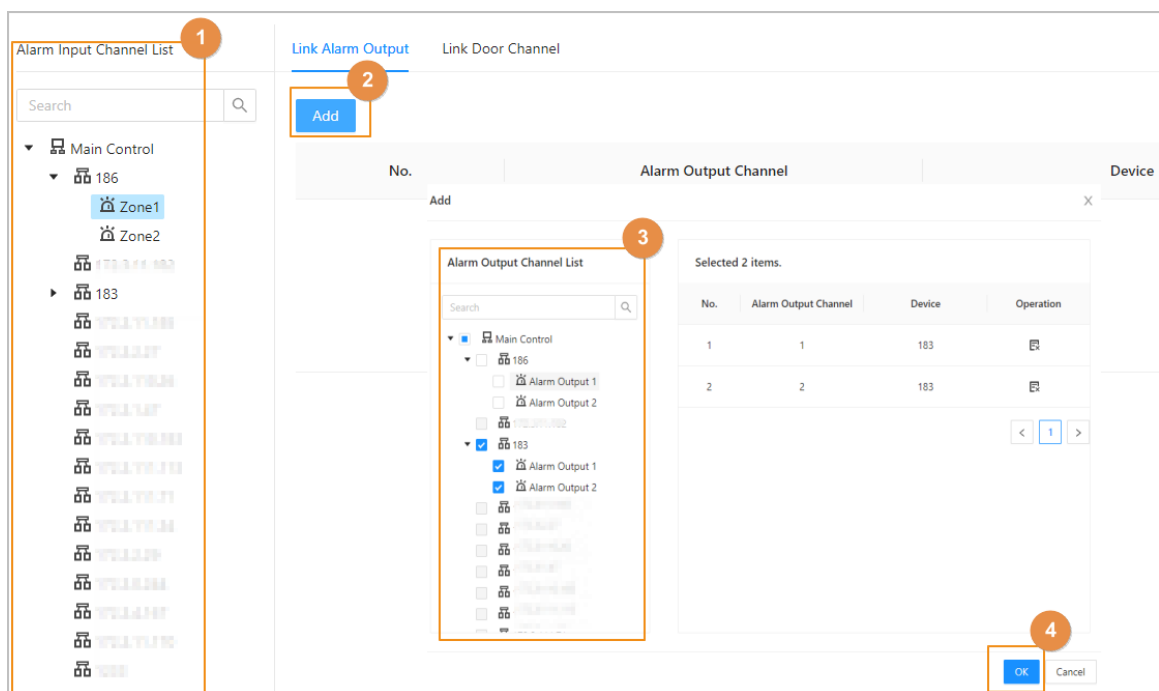


- When you have configured both global alarm linkages and local alarm linkages, and if the global alarm linkages conflict with the local alarm linkages, the last alarm linkages you have configured will take effective.
- When you have configured alarm linkages for sub controllers through the main controller, 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.

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

Figure 5-32 Alarm output

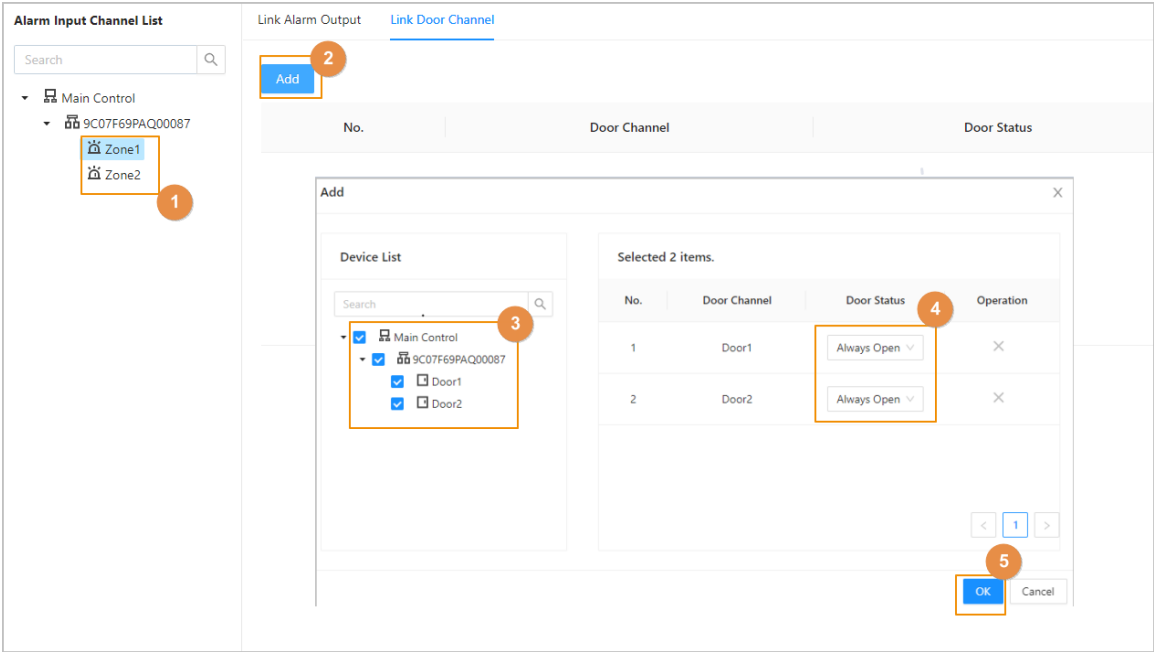


- Turn on the alarm output function and then enter the alarm duration.
- Click **Apply**.

Step 3 Configure the door linkage.

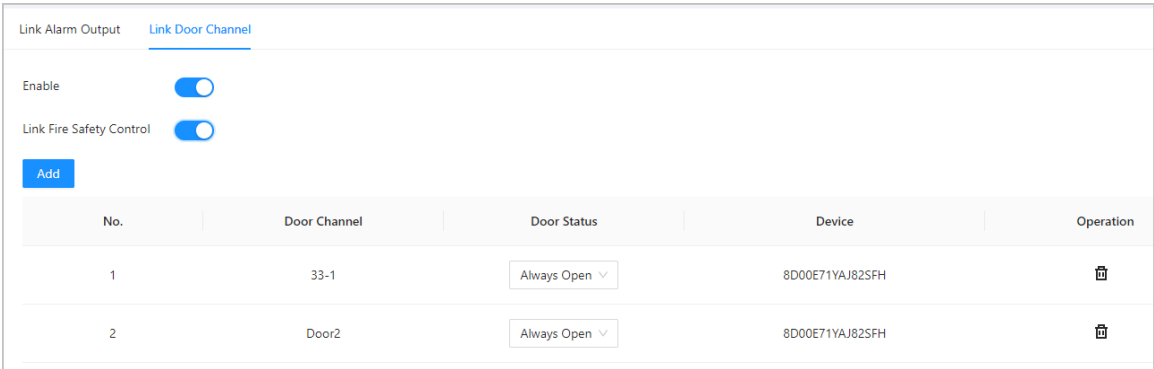
- Select an alarm input from the channel list, and then click **Add**.
- Select the linkage door, select the door status, and then click **OK**.
 - Always Closed: The door automatically locks when an alarm is triggered.
 - Always Open: The door automatically unlocks when an alarm is triggered.

Figure 5-33 Door linkage



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

Figure 5-34 Door linkage



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

d. Click **Apply**.

You can click **Copy to** to apply the pre-configured alarm linkages to other alarm input channels.

5.2.11 Configuring Cloud Service

Add the Main Controller to DMSS before you request Bluetooth cards for users. For details on using DMSS, see the user's manual of DMSS.

Background Information



If you have changed the password of the Main Controller, or restored it to factory defaults, you need to delete the controller on DMSS and add it to DMSS again.

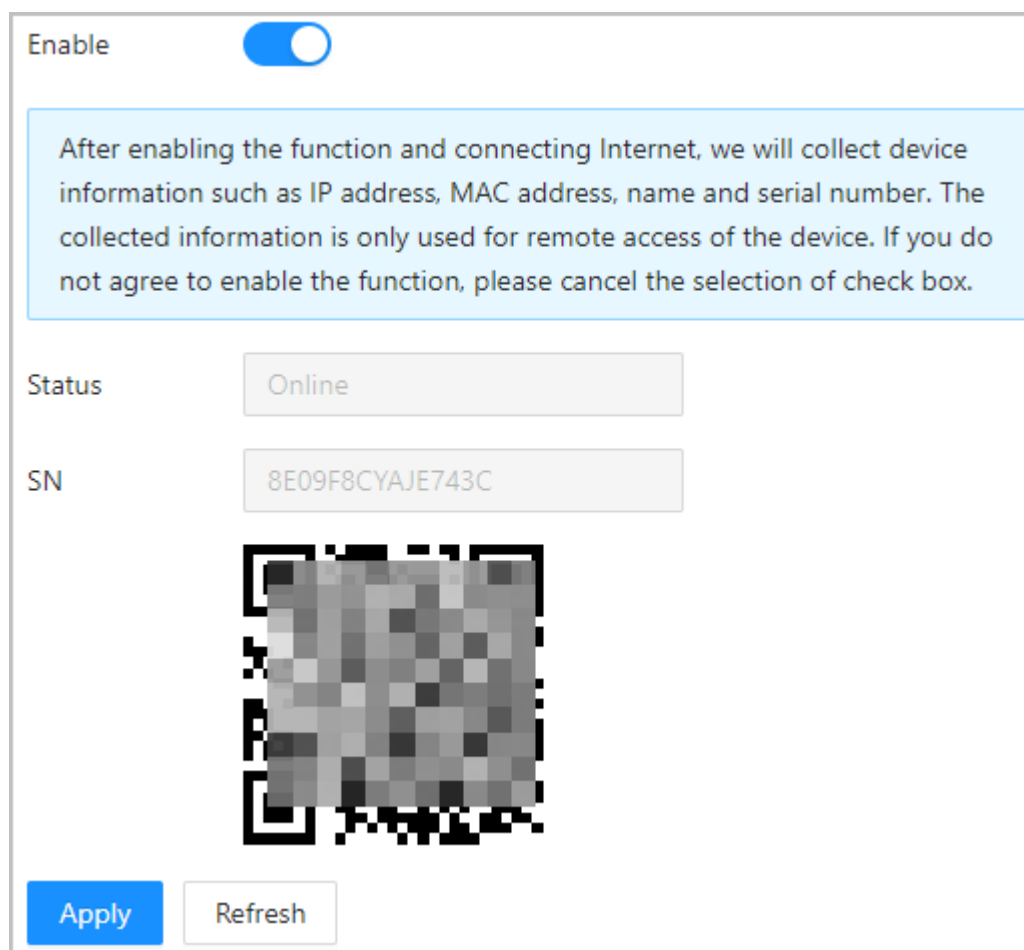
Procedure

Step 1 On the home page, select **Local Device Config** > **Network Setting** > **Cloud Service**.

Step 2 Turn on the cloud service function.

The cloud service function is turned on by default.

Figure 5-35 Cloud service

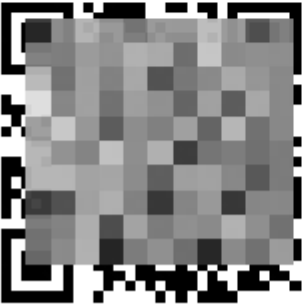


Enable ☒

After enabling the function and connecting Internet, we will collect device information such as IP address, MAC address, name and serial number. The collected information is only used for remote access of the device. If you do not agree to enable the function, please cancel the selection of check box.

Status

SN



Step 3 Click **Apply**.

Step 4 Download DMSS and sign up with Email, scan the QR code with DMSS 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".

5.3.2 Logging In

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

Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

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.