Access Controller

Quick Start Guide

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

V1.0.2

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
V1.0.2	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

1 Dimensions and Appearance

Figure 1-1 Dimensions (mm [inch])

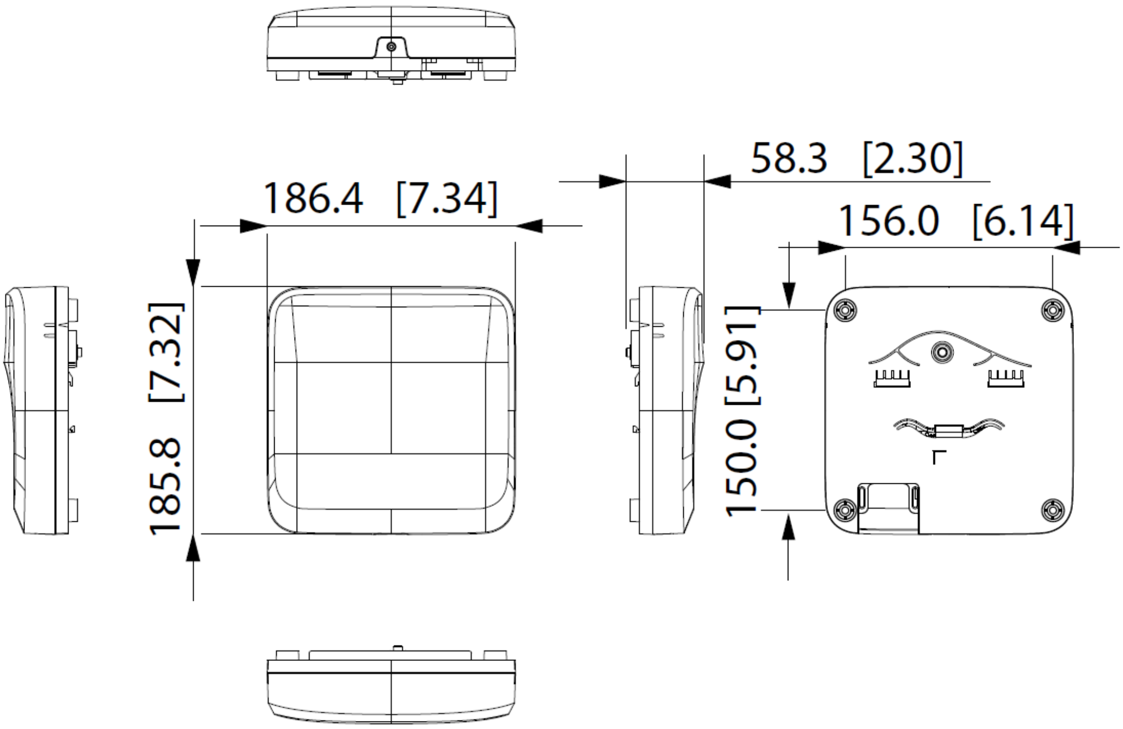


Figure 1-2 Front view

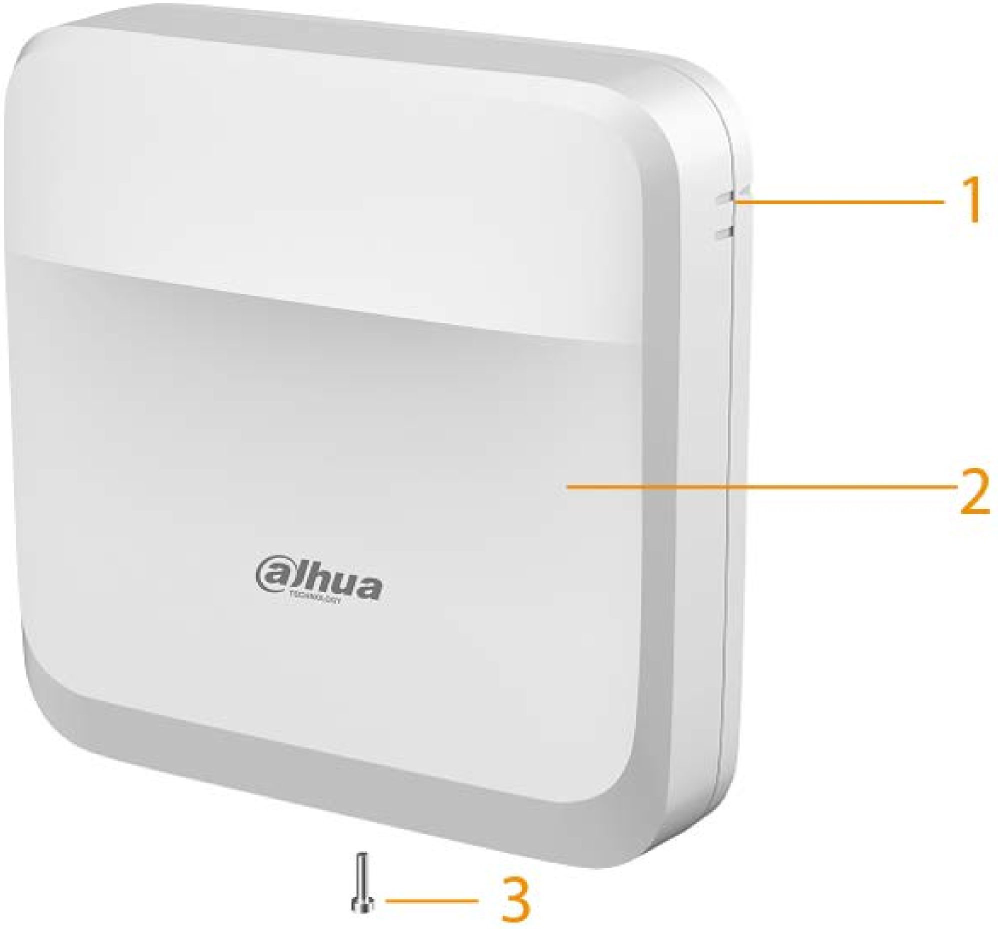


Table 1-1 Components description

No.	Description
1	Guiding mark
2	Front panel
3	Screw

Figure 1-3 Back cover

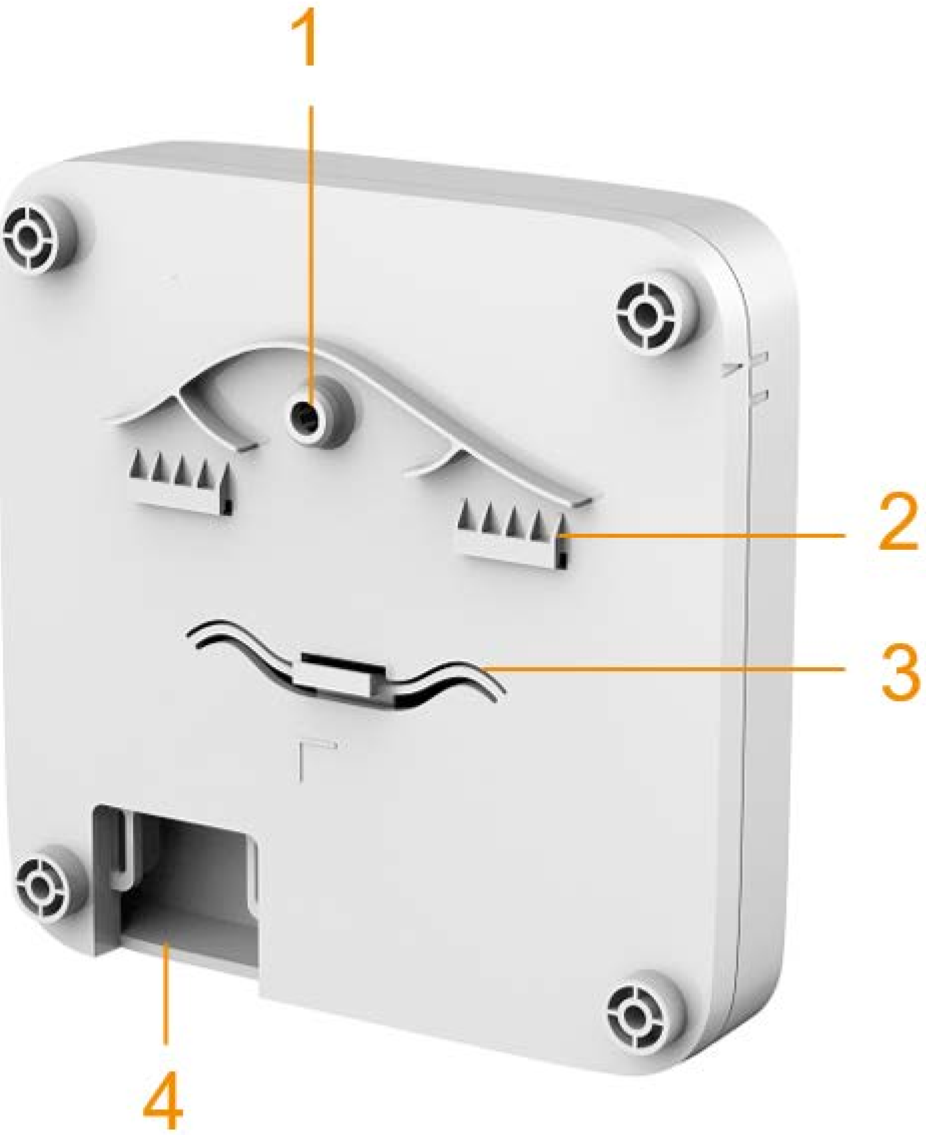


Table 1-2 Back cover description

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

2 Ports Overview

Figure 2-1 Ports

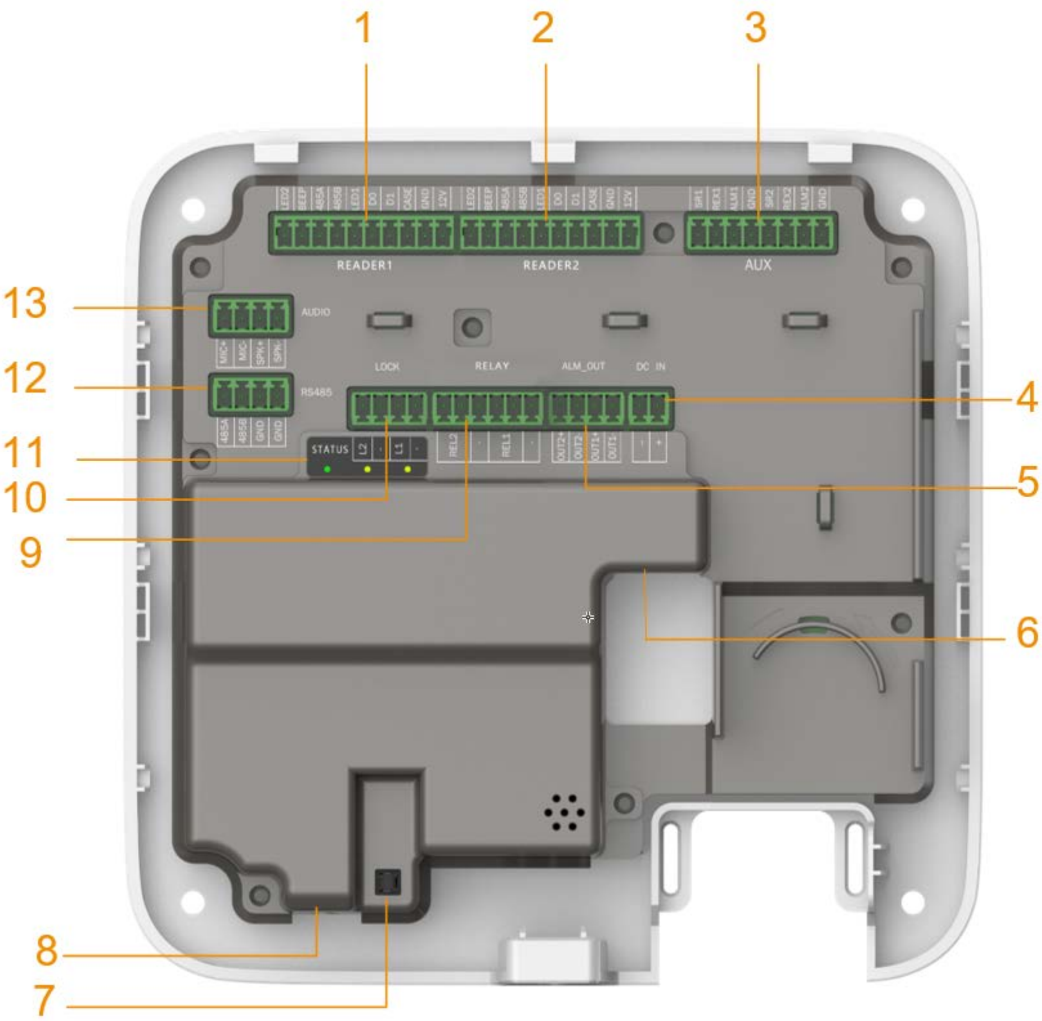


Table 2-1 Ports description

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
10	LOCK	Power lock connector
11	STATUS	LED indicator

No	Name	Description
12	RS485	RS485 connector (not used)
13	AUDIO	Audio connector (not used)

Figure 2-2 Reader connector

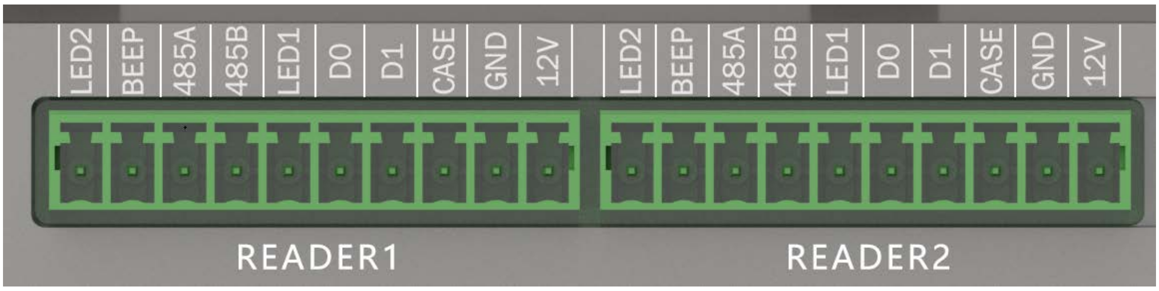


Table 2-2 Reader connector description

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

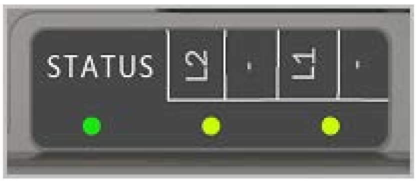


Table 2-3 Description of LED indicator ports

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
L1	Lock 1 indicator	Solid yellow and green	Lock open

Figure 2-4 Auxiliary I/O ports

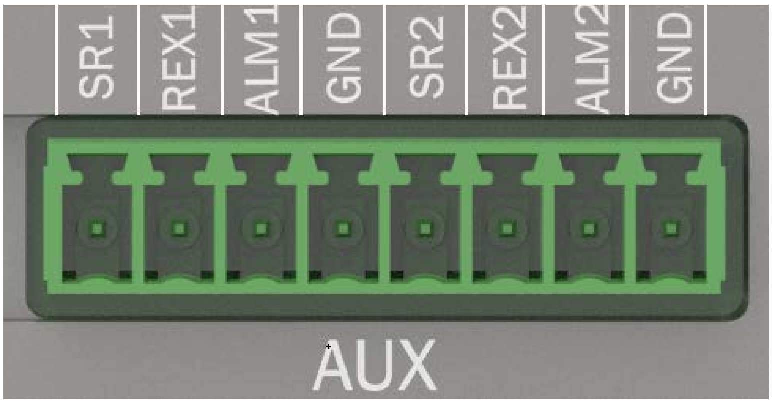


Table 2-4 Description of auxiliary I/O ports

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

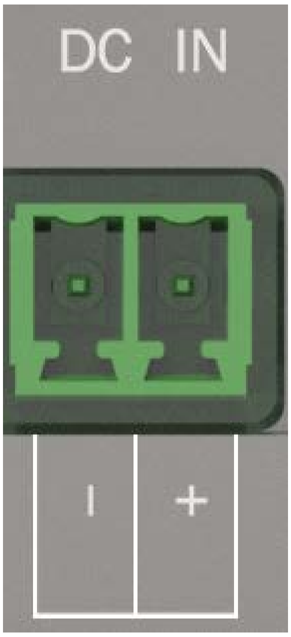


Table 2-5 Description of power ports

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

Figure 2-6 Alarm output ports

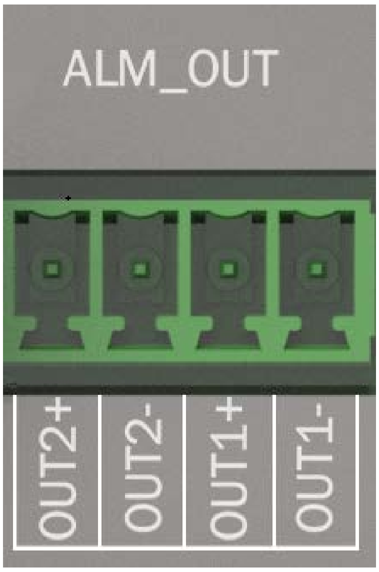


Table 2-6 Description of alarm output ports

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

Figure 2-7 Relay ports

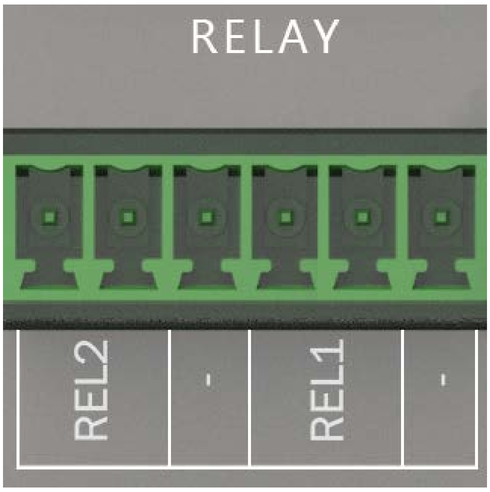


Table 2-7 Description of relay ports

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

Figure 2-8 Lock ports

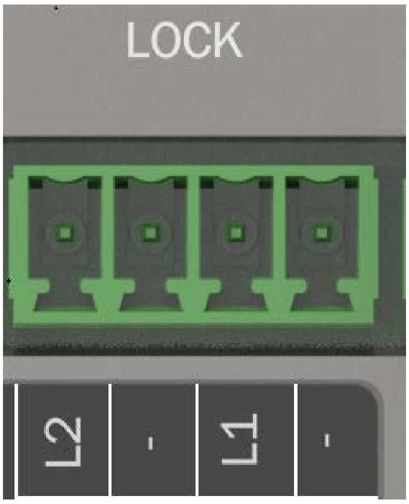


Table 2-8 Description of lock

Ports	Description
L1/L2	Power one or two locks (DC output). The lock connector can also be used to power external devices. Connects to lock. 12 VDC Max total load = 1000 mA 📖 ● 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".
REL2	
–	Grounding wire.

Figure 2-9 RS-485 ports

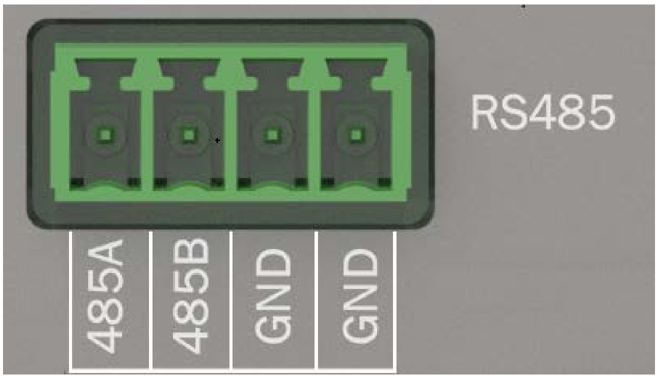


Table 2-9 Description of RS-485

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

Figure 2-10 Audio ports

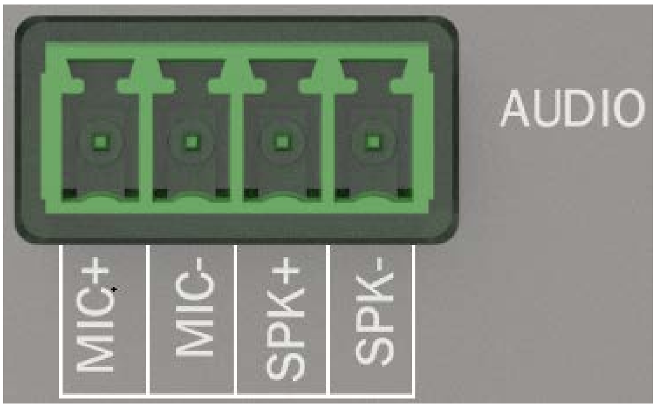


Table 2-10 Description of audio ports

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

3 Wring 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.

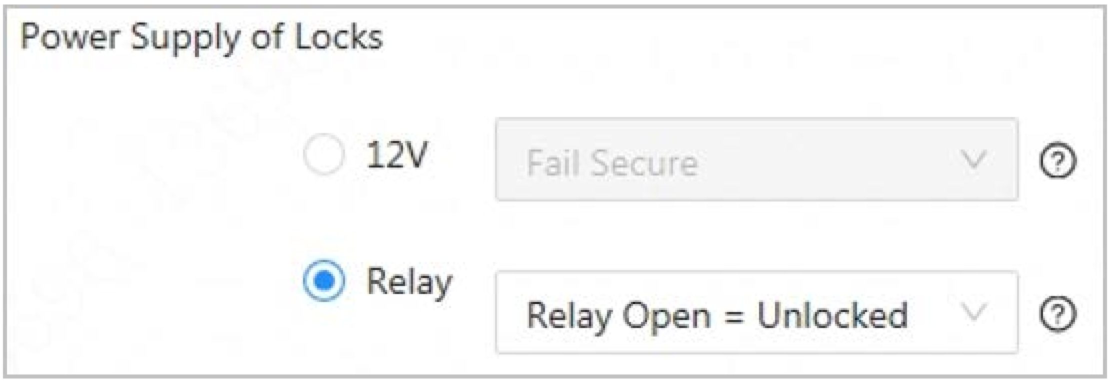
3.1 Wiring of Magnetic Locks

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)



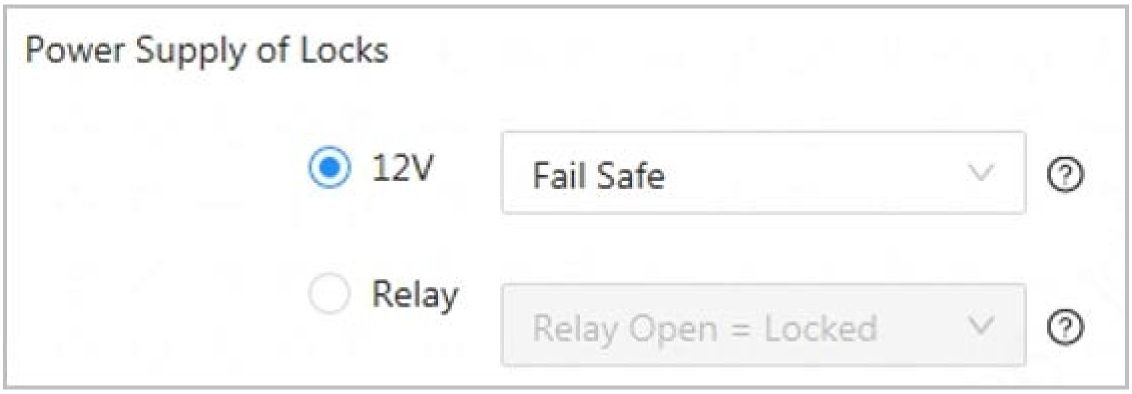
Power Supply of Locks

○ 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)



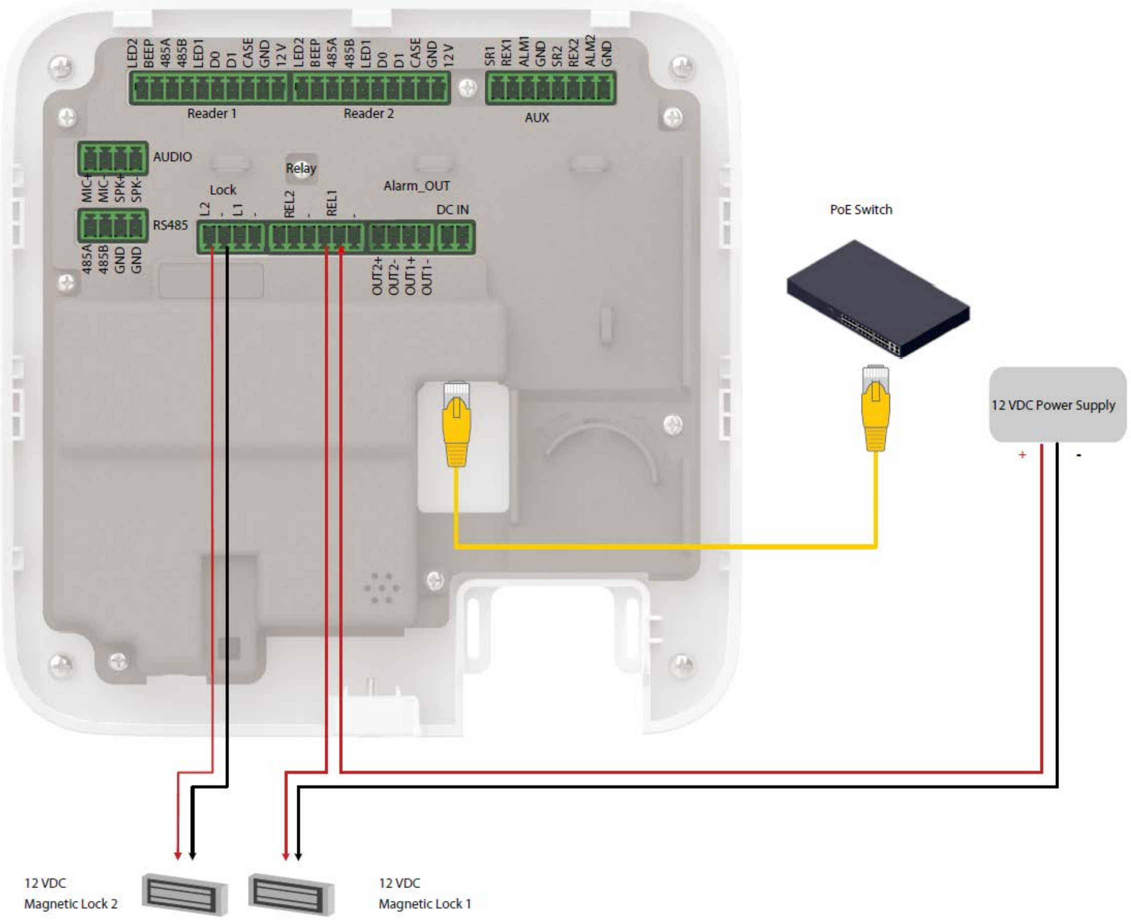
Power Supply of Locks

● 12V Fail Safe

○ Relay Relay Open = Locked

3. Wiring the locks according to the diagram below.

Figure 3-3 Wiring of locks

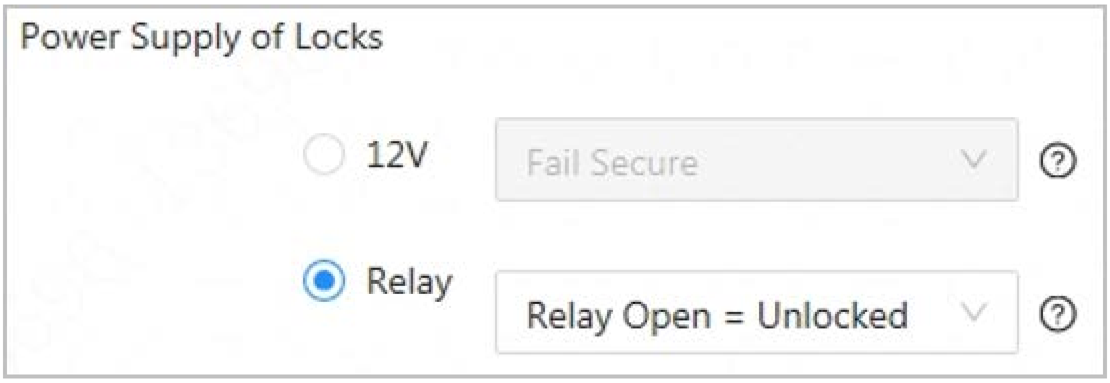


3.1.2 Wring of Dual Magnetic Locks with 12 V External Power Supply (12 V and Relay)

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)

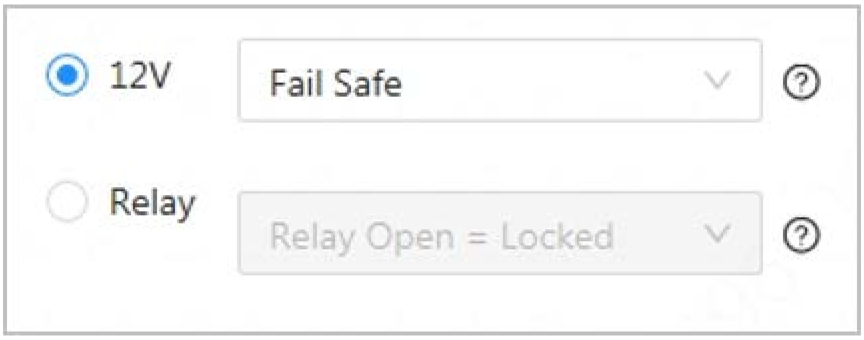

Power Supply of Locks

○ 12V | Fail Secure

● Relay | Relay Open = Unlocked

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

Figure 3-5 Lock 2 (door 2)

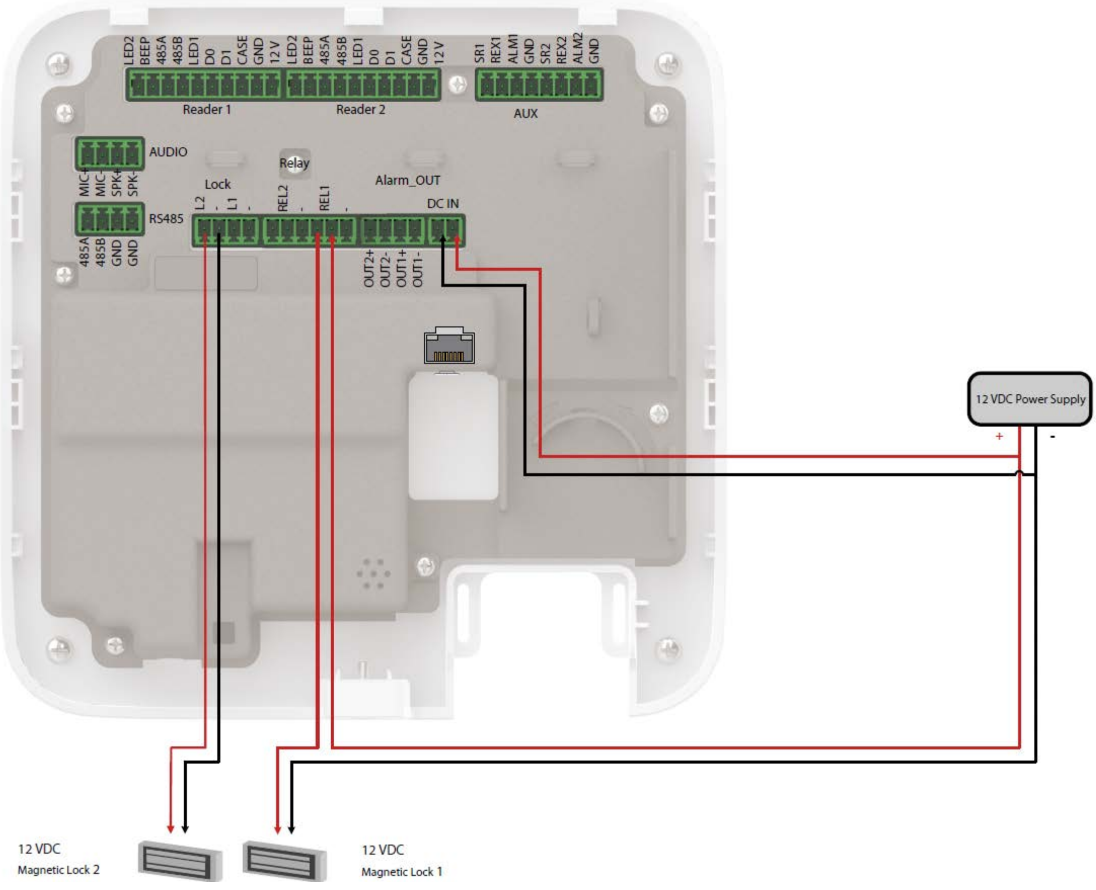


● 12V — Fail Safe

○ Relay — Relay Open = Locked

3. Wiring the locks according to the diagram below.

Figure 3-6 Wiring of locks

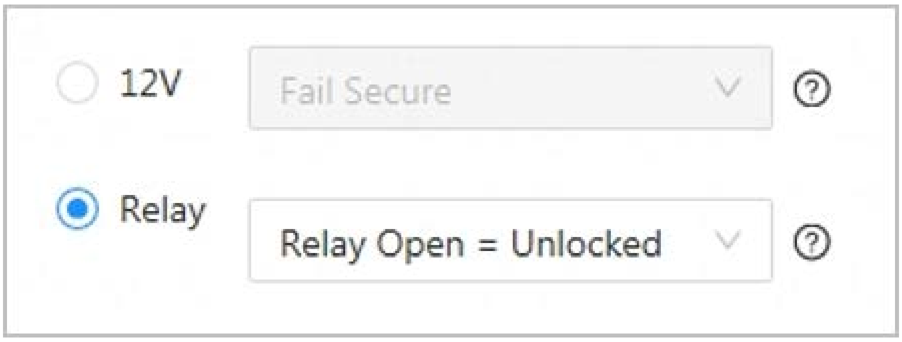


3.1.3 Wring of Dual Magnetic Locks with 12 V External Power Supply (Relay)

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)

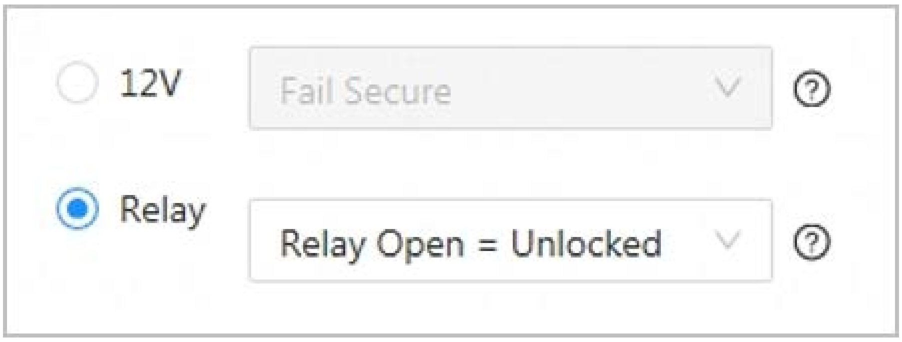


○ 12V Fail Secure

● Relay Relay Open = Unlocked

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

Figure 3-8 Lock 2 (door 2)

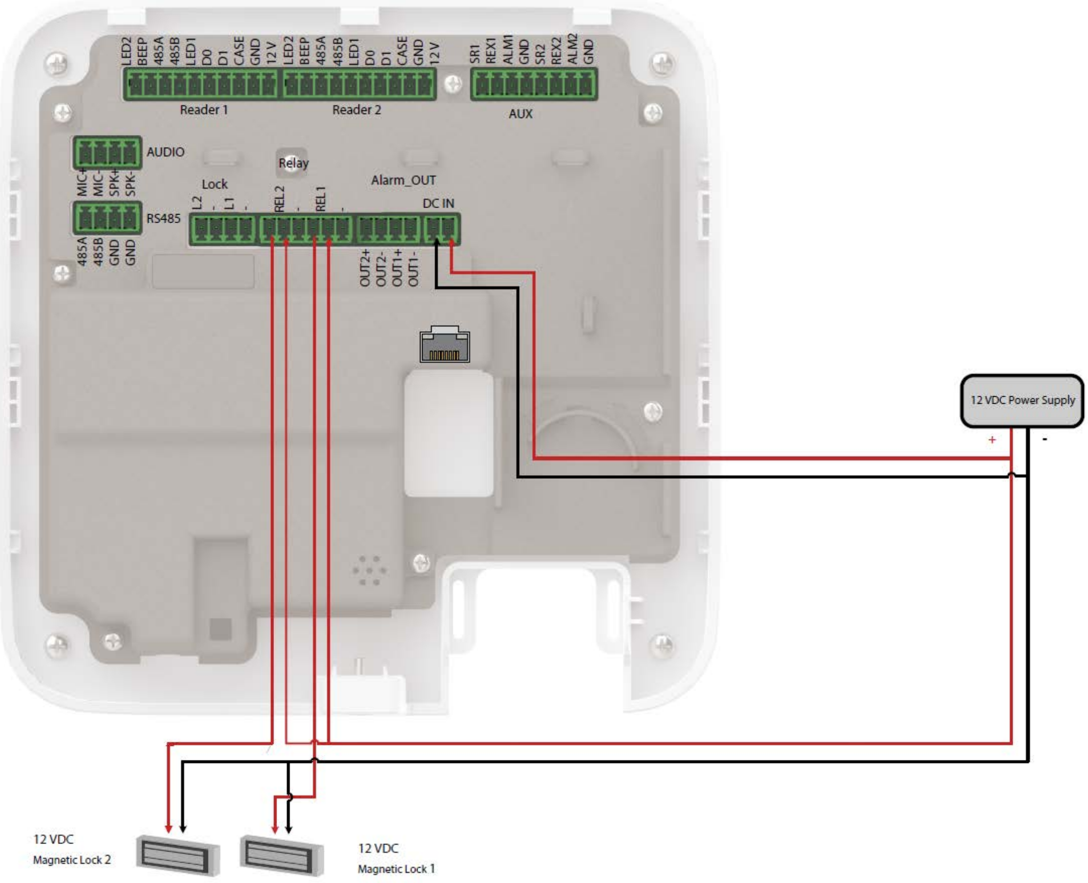


○ 12V Fail Secure

● Relay Relay Open = Unlocked

3. Wiring the locks according to the diagram below.

Figure 3-9 Wiring of locks



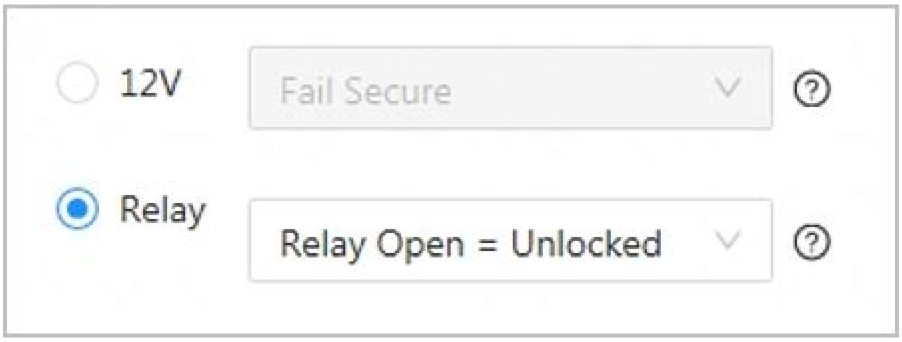
3.1.4 Wring of 2-in-1 Magnetic Lock with 12 V External Power

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)

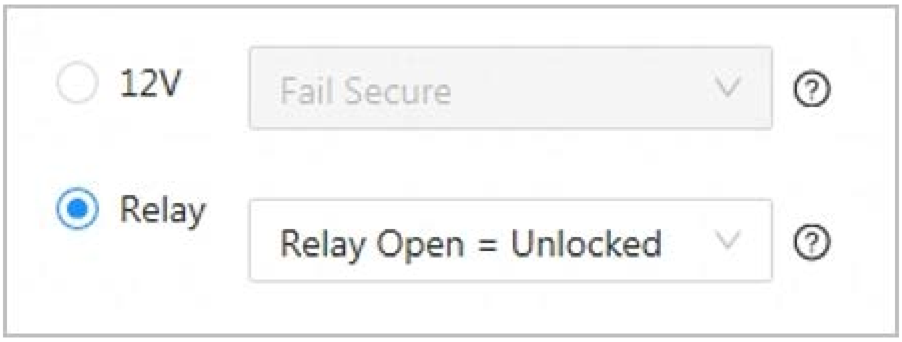


○ 12V Fail Secure

● Relay Relay Open = Unlocked

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

Figure 3-11 Lock 2 (door 2)

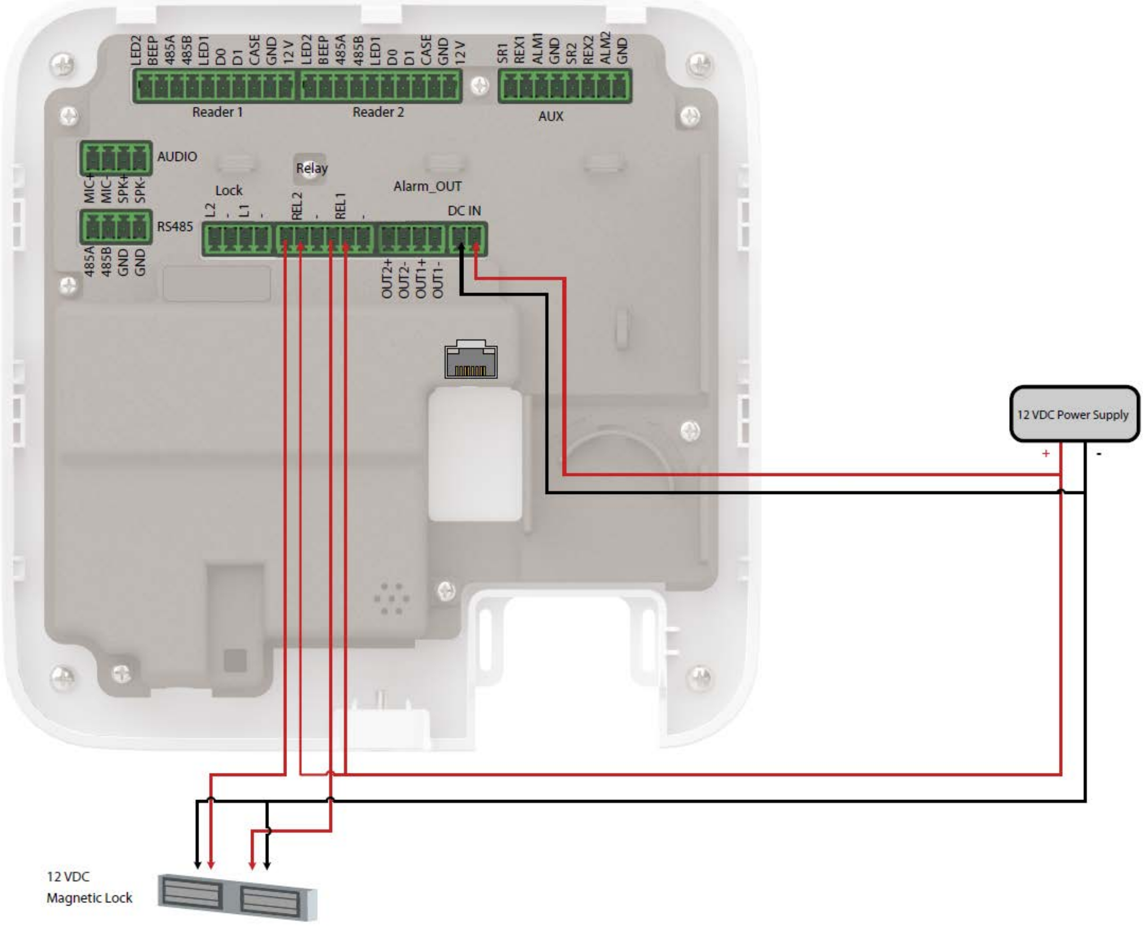


○ 12V Fail Secure

● Relay Relay Open = Unlocked

3. Wiring the locks according to the diagram below.

Figure 3-12 Wiring of locks



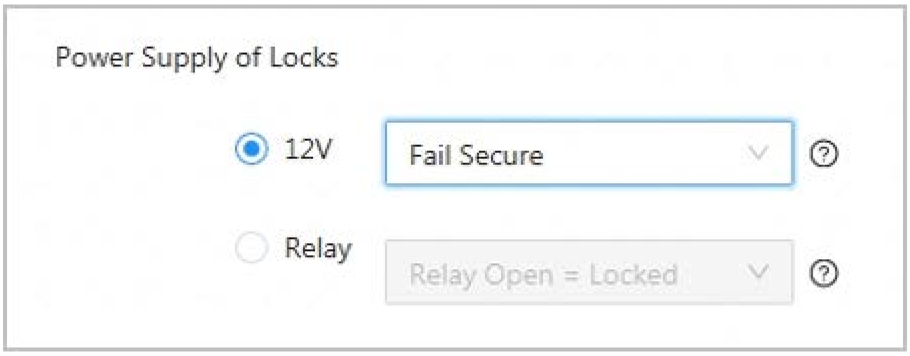
3.2 Wiring of Electric Strike Lock

3.2.1 Wring 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)



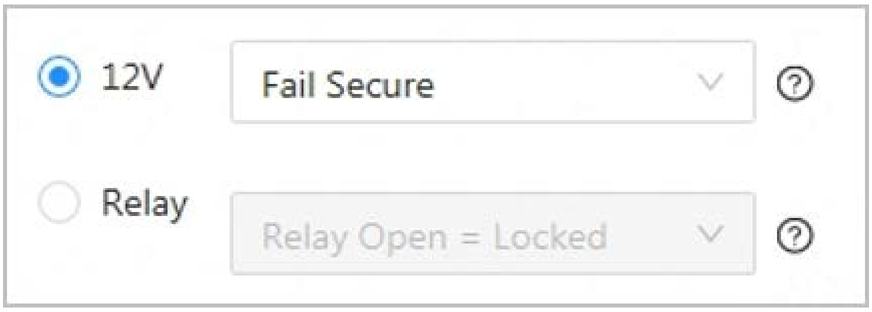
Power Supply of Locks

● 12V Fail Secure

○ Relay Relay Open = Locked

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

Figure 3-14 Lock 2 (door 2)

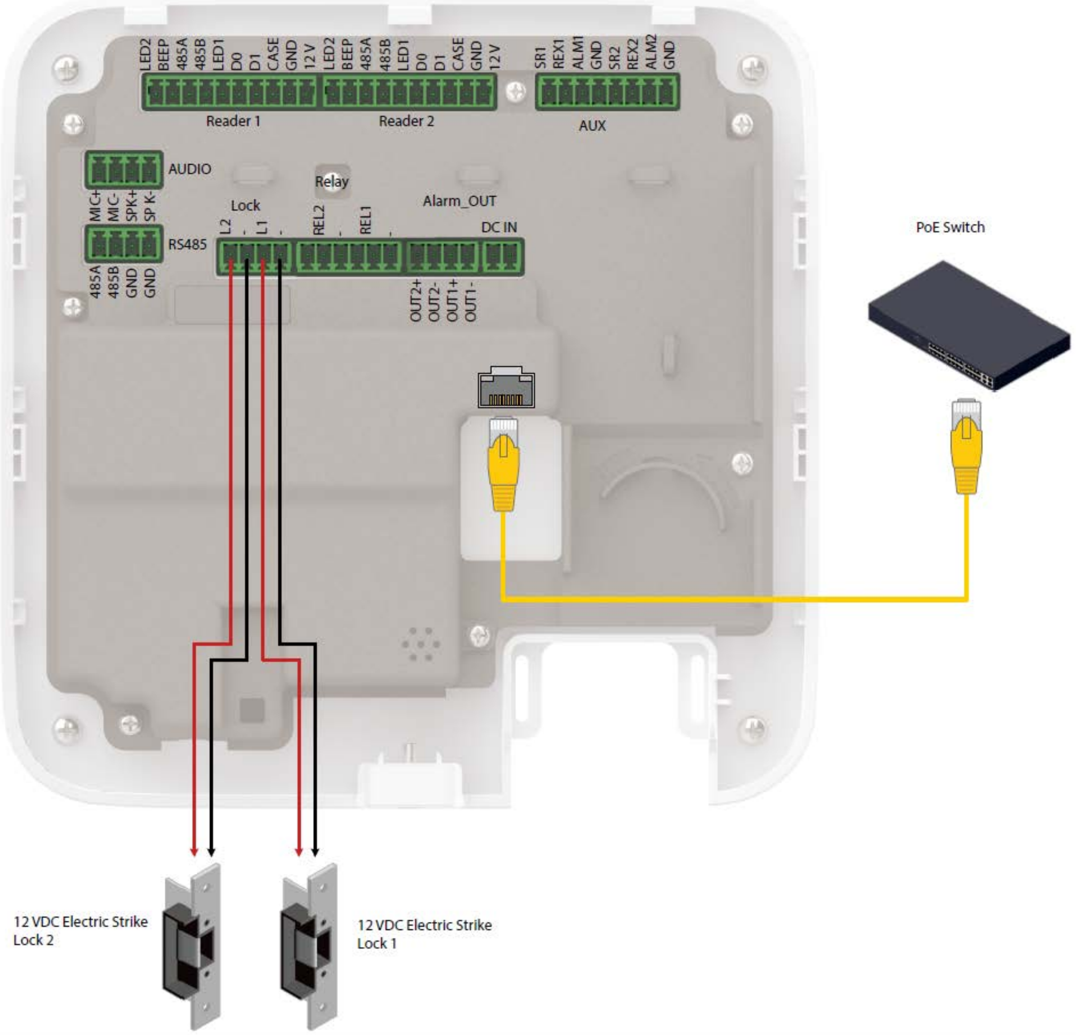


● 12V Fail Secure

○ Relay Relay Open = Locked

3. Wiring the locks according to the diagram below.

Figure 3-15 Wiring of locks

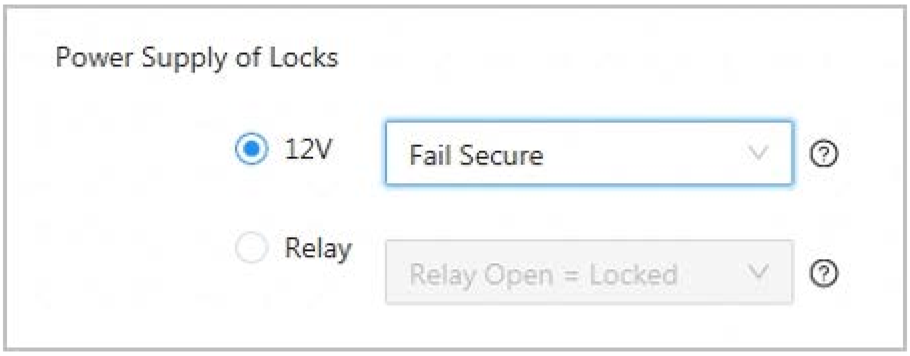


3.2.2 Wring of Dual Electric Strikes with 12 V External Power Supply

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)



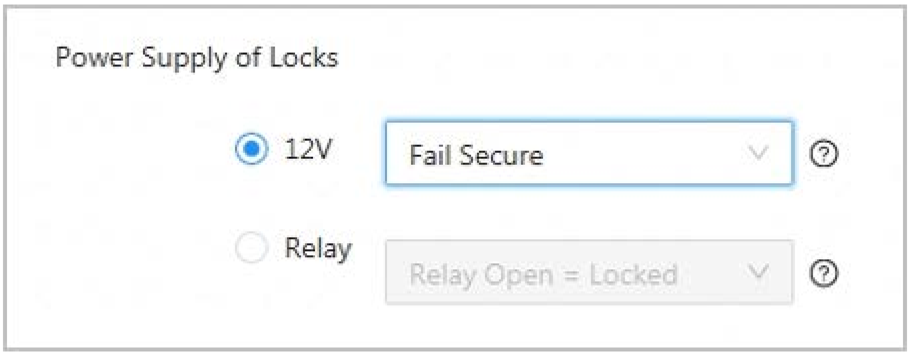
Power Supply of Locks

● 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)



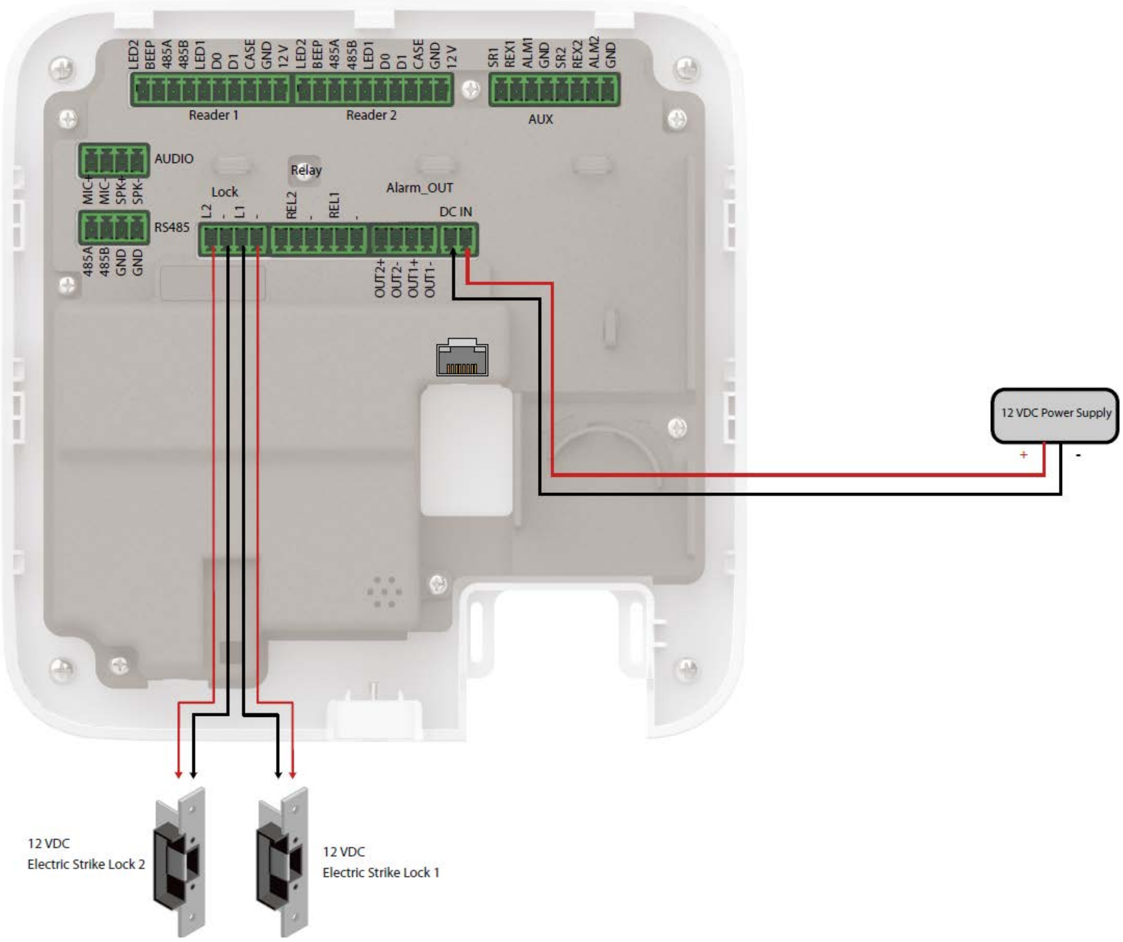
Power Supply of Locks

● 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

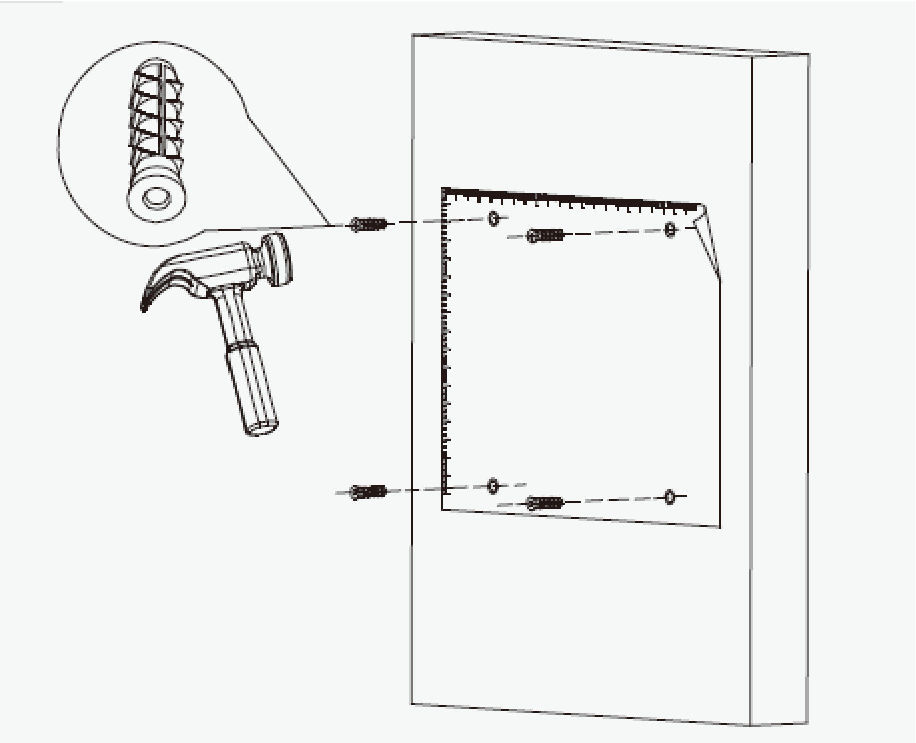
Procedure

Step 1 Paste the positioning map to the wall at an appropriate position.

Step 2 Drill holes through the marks on the map.

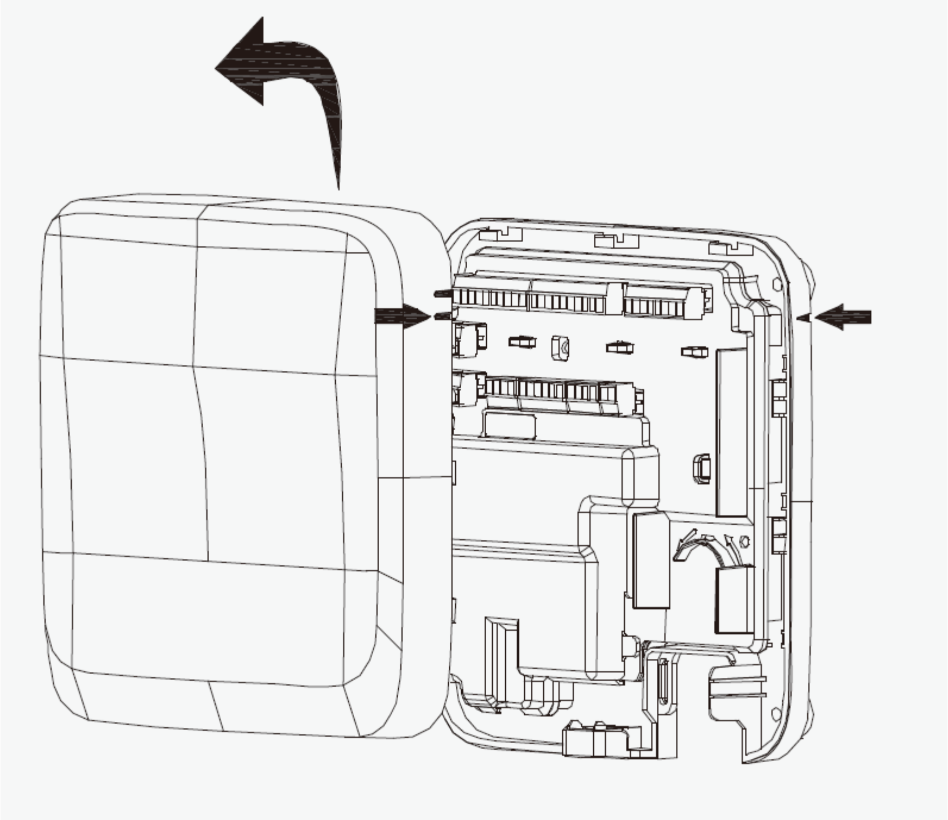
Step 3 Hammer in the expansion tubes, and then remove the map.

Figure 4-1 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



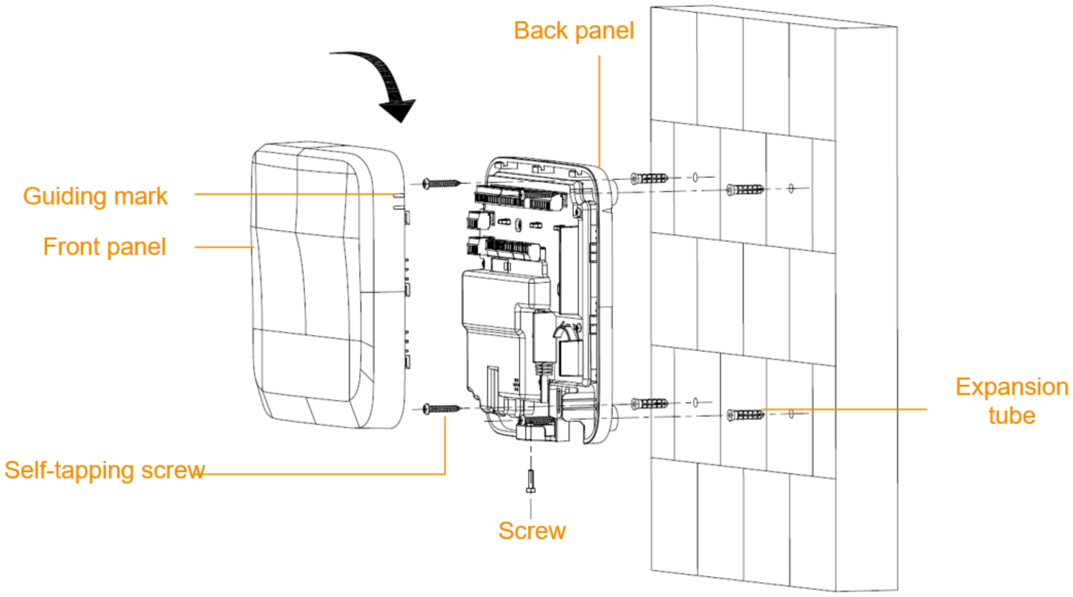
Step 5 Attach the back panel of the Access Controller to the wall with self-tapping screws.

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

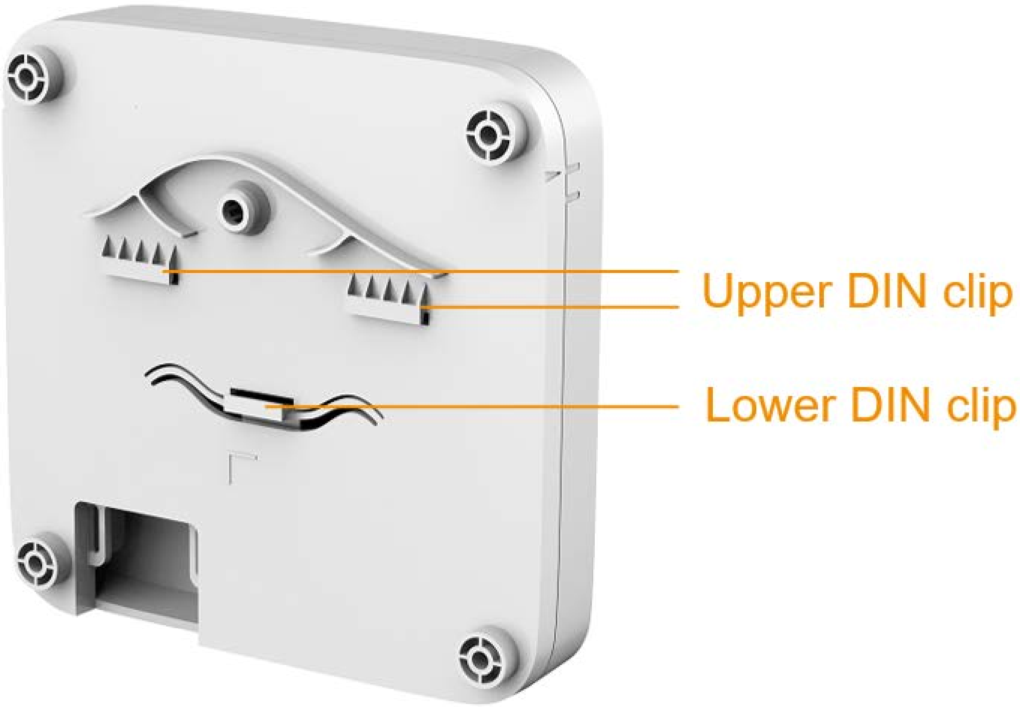
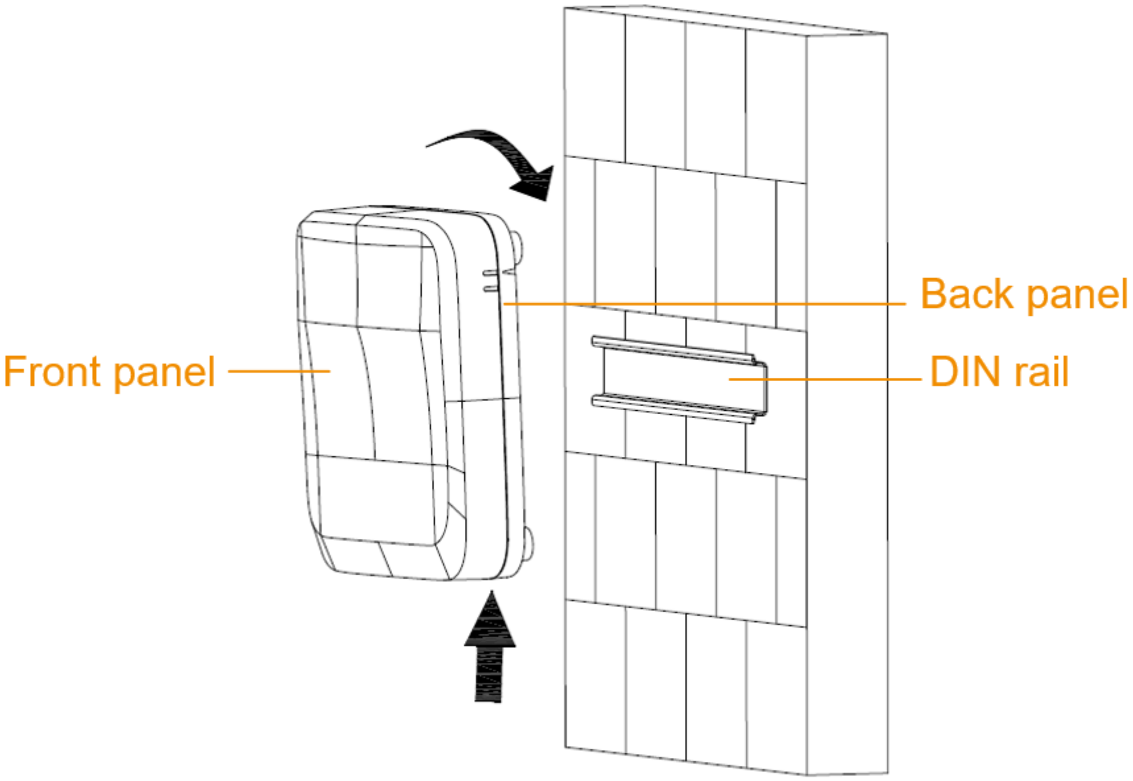


Figure 4-5 Hook DIN clips to the rail

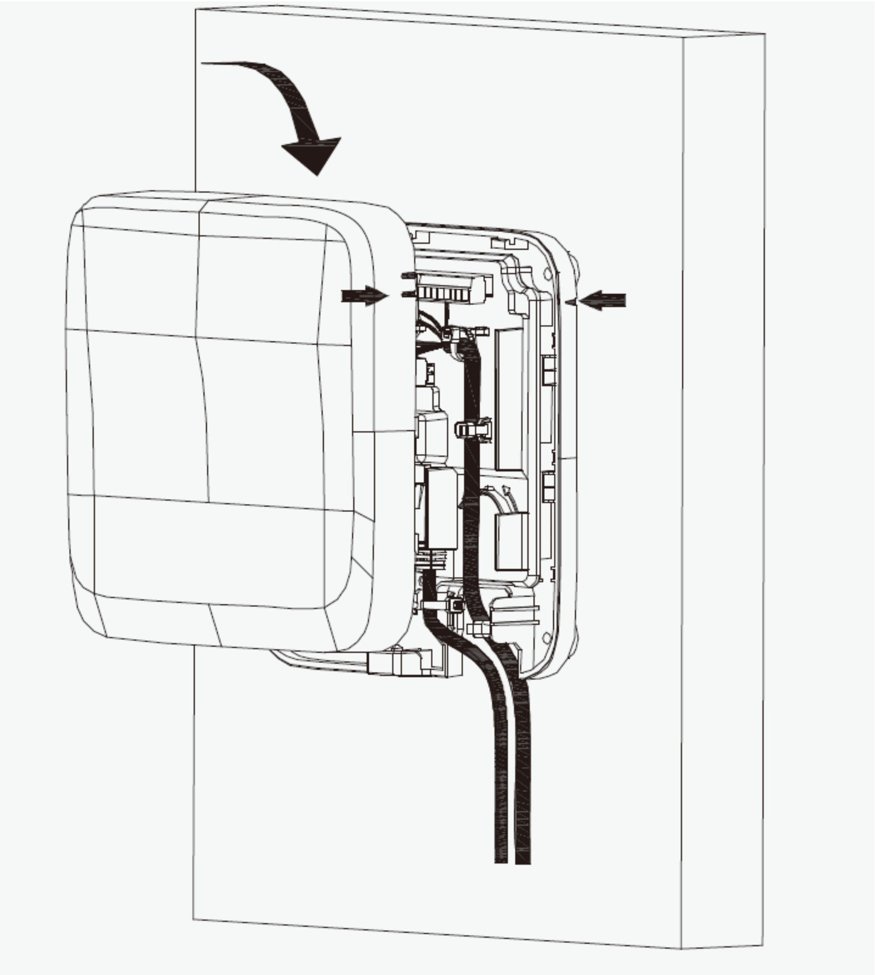


Step 3 Slide up the front panel of the Access Controller to remove the cover.

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.

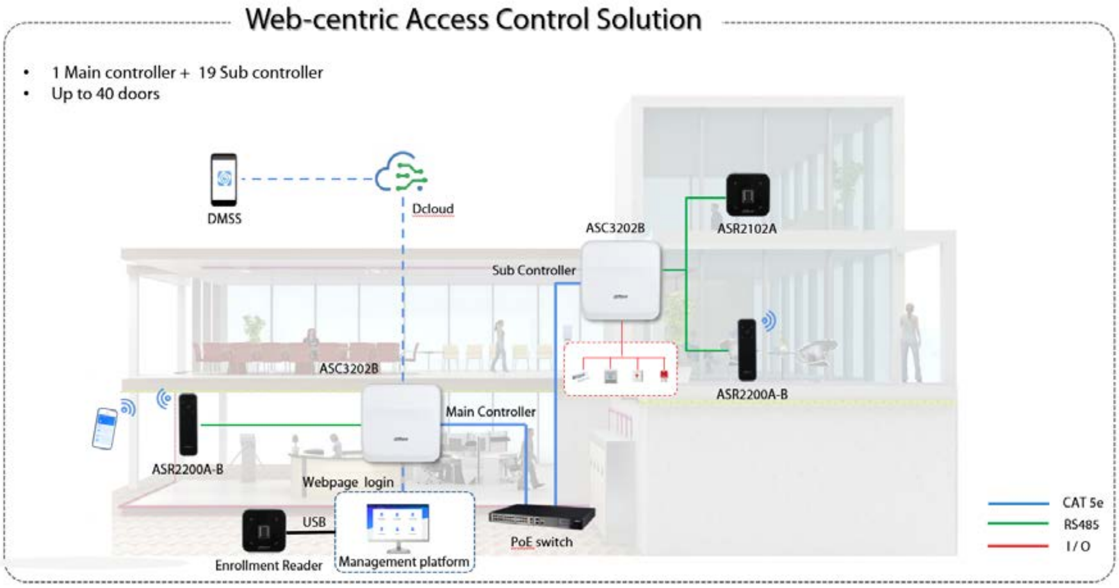
Step 7 Remove the protection film.

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 management platform of the main controller. The main controller can manage up to 19 sub controllers.

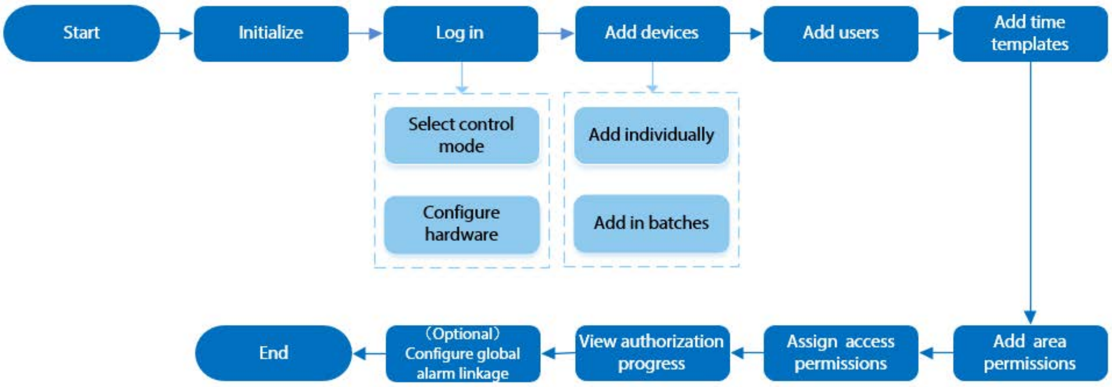
Figure 5-1 Networking diagram



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 192.168.1.108 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**.

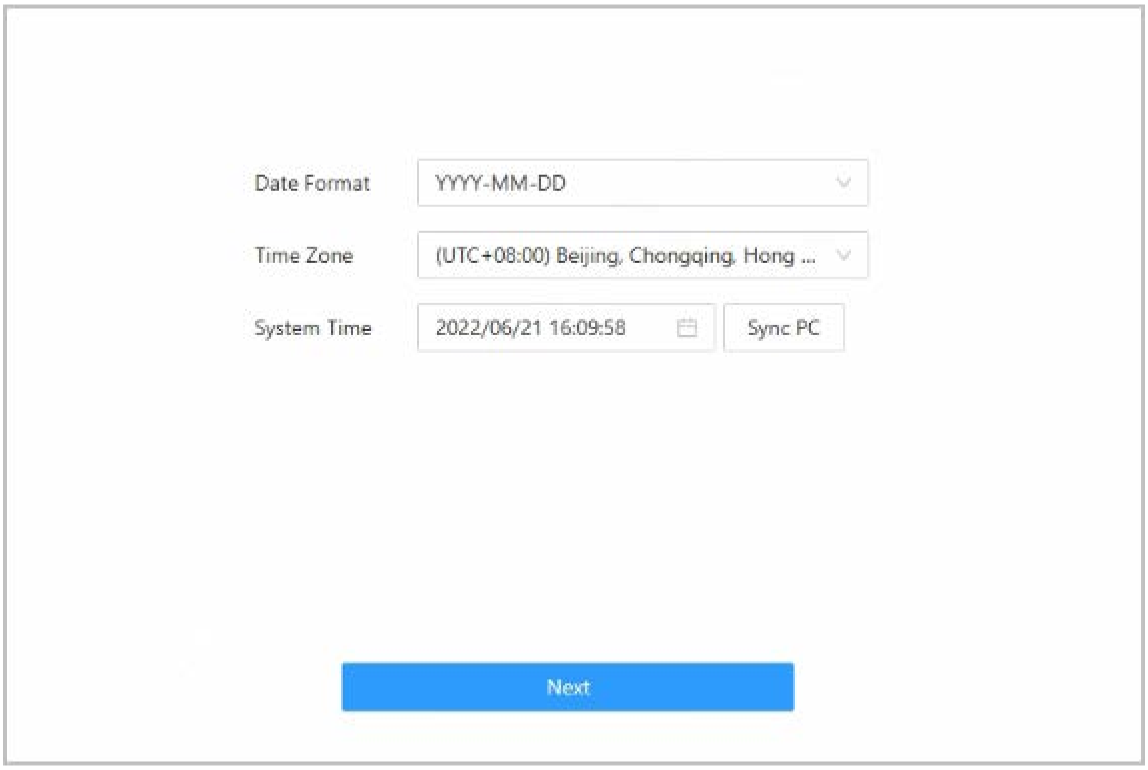
Step 4 Set the password and email address.

📖

- 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 5-3 Configure the time



Date Format: YYYY-MM-DD

Time Zone: (UTC+08:00) Beijing, Chongqing, Hong ...

System Time: 2022/06/21 16:09:58

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.

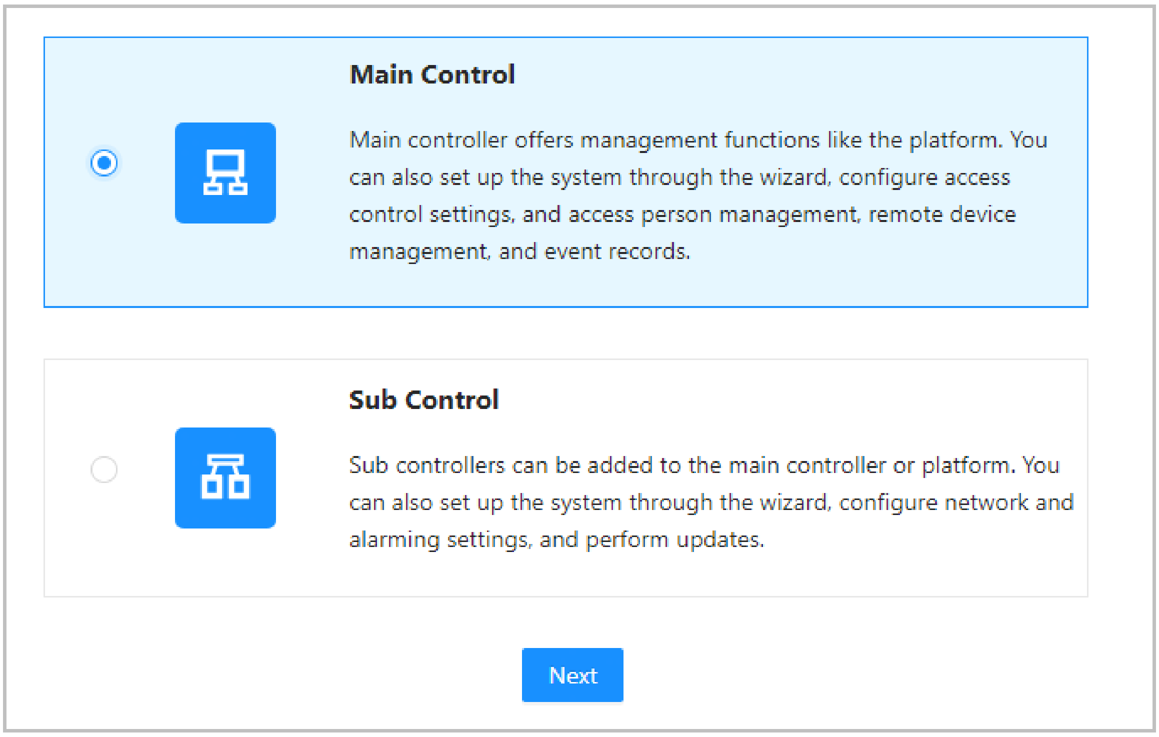
Procedure

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 5-4 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**

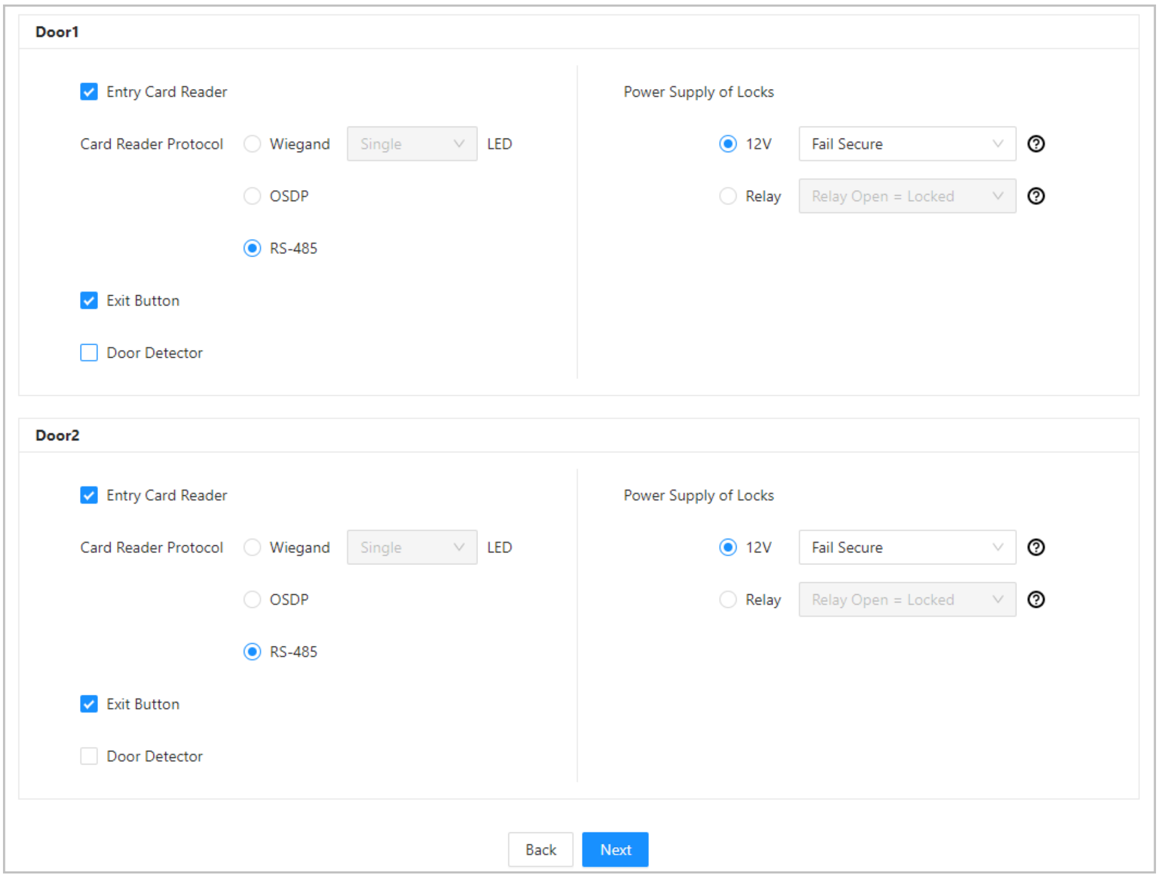
Sub controllers can be added to the main controller or platform. You can also set up the system through the wizard, configure network and alarming settings, and perform updates.

- 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 5-5 Configure door parameters



Door1

☑ Entry Card Reader

Card Reader Protocol ○ Wiegand Single LED

○ OSDP

● RS-485

☑ Exit Button

☐ Door Detector

Power Supply of Locks

● 12V Fail Secure

○ Relay Relay Open = Locked

Door2

☑ Entry Card Reader

Card Reader Protocol ○ Wiegand Single LED

○ OSDP

● RS-485

☑ Exit Button

☐ Door Detector

Power Supply of Locks

● 12V Fail Secure

○ Relay Relay Open = Locked

Table 5-1 Parameter description

Parameter	Description
Entry Card Reader	Select the card reader protocol. ● 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	● 12 V: The controller provides power to the lock. ◇ 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. ◇ 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.

Step 5 Configure access control parameters.

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

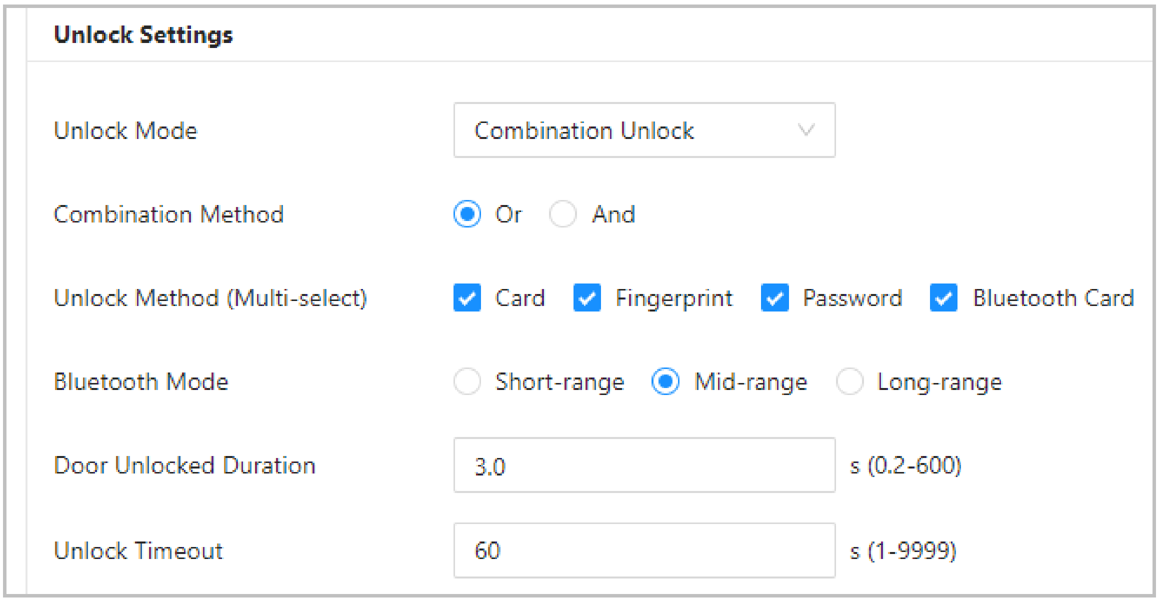
- Or: Use one of the selected unlock methods to authorize opening the door.

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

The Controller supports unlocking through card, fingerprint, password and Bluetooth card.

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

Figure 5-6 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: 3.0 s (0.2-600)

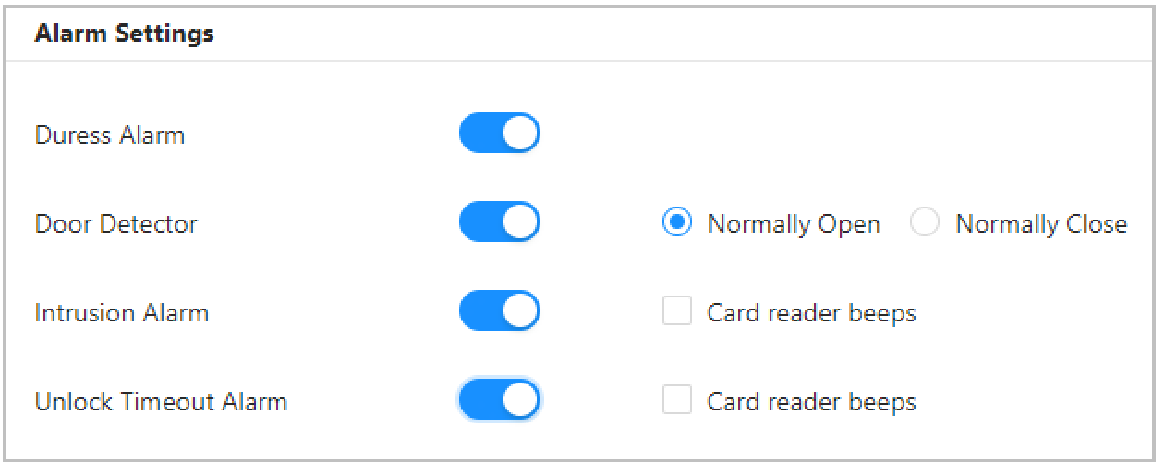
Unlock Timeout: 60 s (1-9999)

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	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. ● 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. ⚠ The Bluetooth unlock range might differ depending on models of your phone and the enviroment.
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 5-7 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

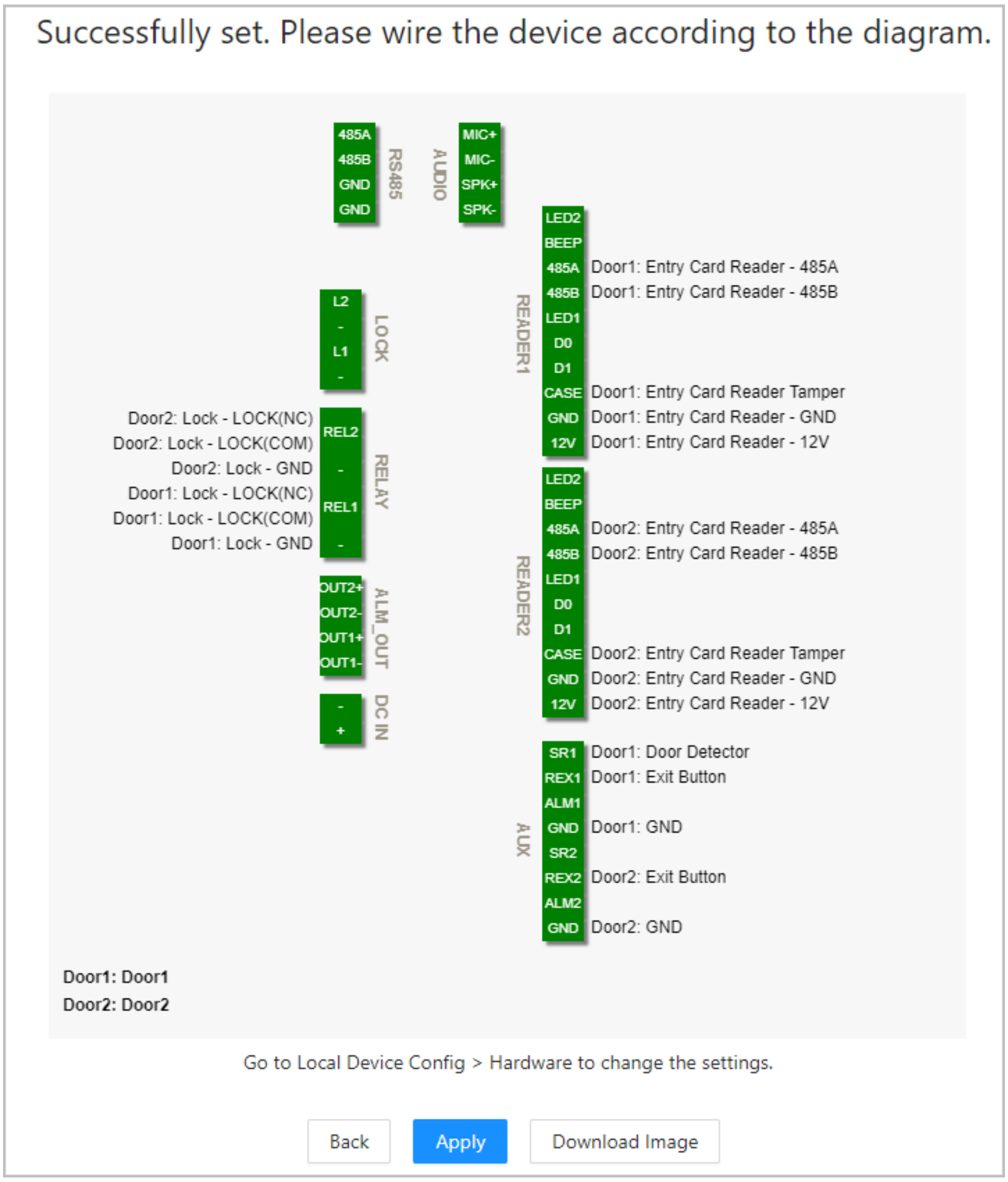
Parameter	Description
Duress Alarm	An alarm will be triggered when a duress card, duress password or duress fingerprint is used to unlock the door.
Door Detector	Select the type of door detector.
Intrusion Alarm	● When the door detector is enabled, an intrusion alarm will be triggered if the door is 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 5-8 Wiring diagram



Successfully set. Please wire the device according to the diagram.

485A
485B
GND
GND
RS485
AUDIO
MIC+
MIC-
SPK+
SPK-
READER1
LED2
BEEP
485A Door1: Entry Card Reader - 485A
485B Door1: Entry Card Reader - 485B
LED1
D0
D1
CASE Door1: Entry Card Reader Tamper
GND Door1: Entry Card Reader - GND
12V Door1: Entry Card Reader - 12V
LOCK
L2
-
L1
-
RELAY
Door2: Lock - LOCK(NC) REL2
Door2: Lock - LOCK(COM)
Door2: Lock - GND -
Door1: Lock - LOCK(NC) REL1
Door1: Lock - LOCK(COM)
Door1: Lock - GND -
READER2
LED2
BEEP
485A Door2: Entry Card Reader - 485A
485B Door2: Entry Card Reader - 485B
LED1
D0
D1
CASE Door2: Entry Card Reader Tamper
GND Door2: Entry Card Reader - GND
12V Door2: Entry Card Reader - 12V
ALM_OUT
OUT2+
OUT2-
OUT1+
OUT1-
DC IN
-
+
AUX
SR1 Door1: Door Detector
REX1 Door1: Exit Button
ALM1
GND Door1: GND
SR2
REX2 Door2: Exit Button
ALM2
GND Door2: GND
Door1: Door1
Door2: Door2

Go to Local Device Config > Hardware to change the settings.

Back
Apply
Download Image

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

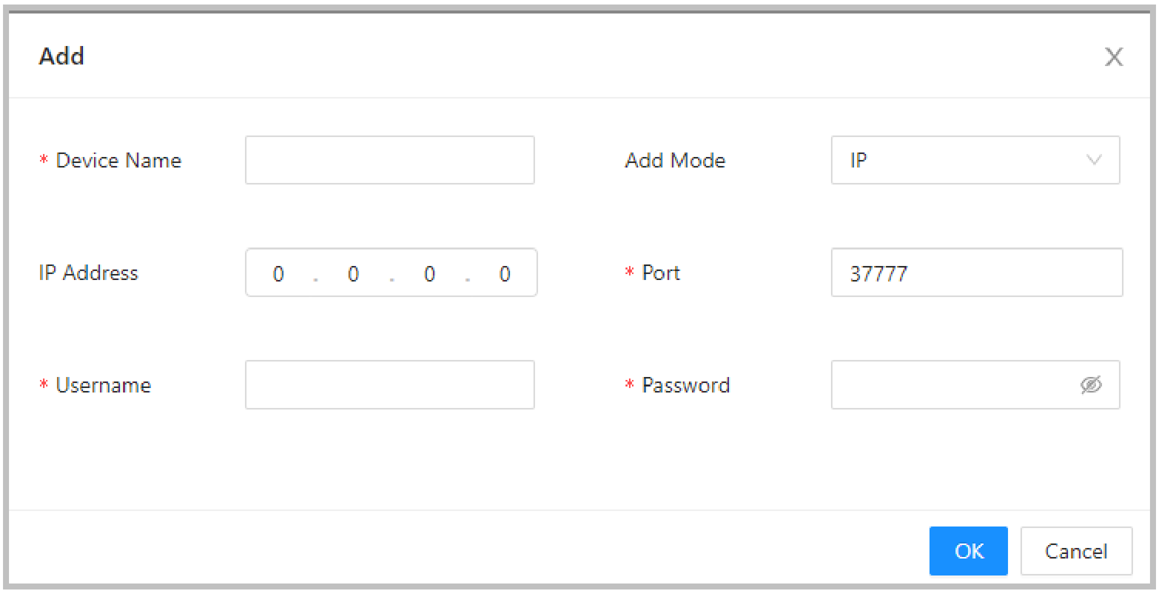
You can add sub controllers to the main controller one by one.

Procedure

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

Step 2 Enter the device information.

Figure 5-9 Device information



Add

* Device Name		Add Mode	IP
IP Address	0 . 0 . 0 . 0	* Port	37777
* Username		* Password	

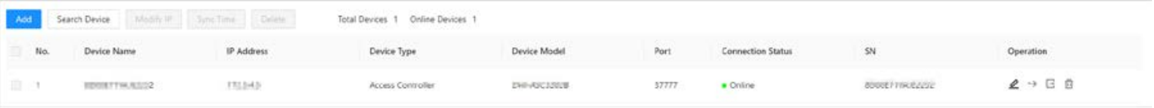
Table 5-4 Device parameters Description

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 5-10 Successfully add devices



Total Devices 1 Online Devices 1

No.	Device Name	IP Address	Device Type	Device Model	Port	Connection Status	SN	Operation
1	[illegible]	[illegible]	Access Controller	[illegible]	37777	● Online	[illegible]	

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

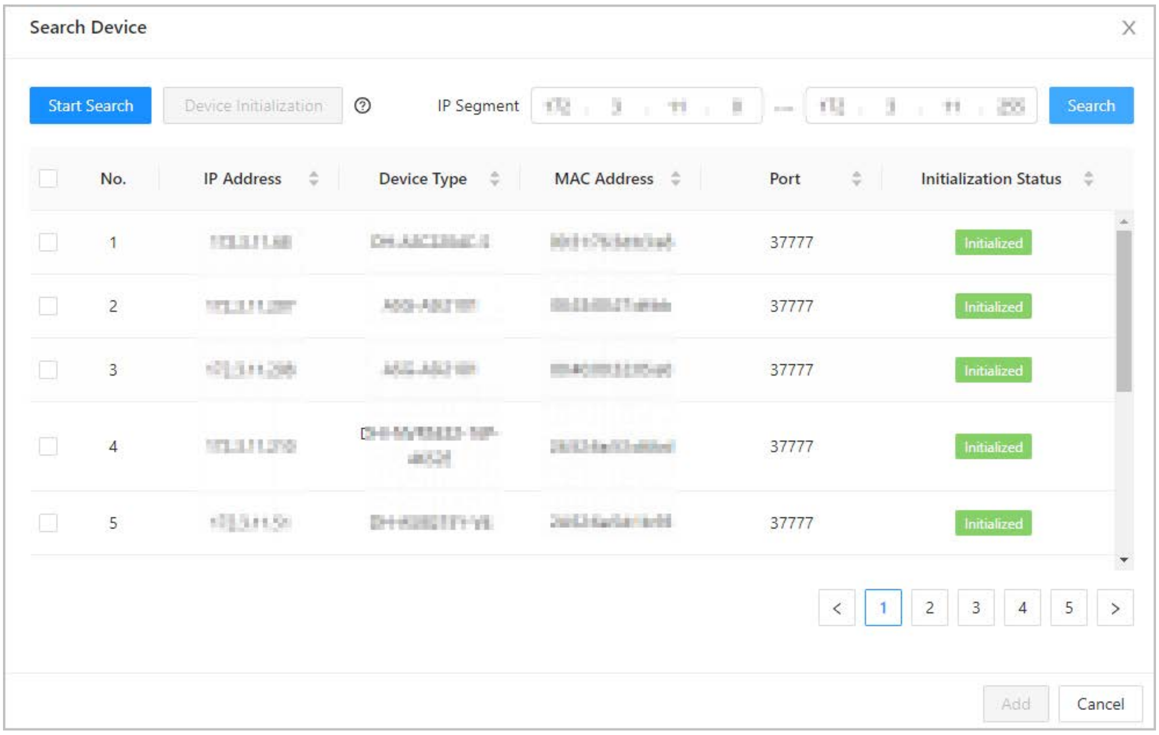
We recommend you use the auto-search function when you add sub controllers in batches. Make sure the sub controllers you want to add are on the same network segment.

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 5-11 Auto search



Search Device

Start Search | Device Initialization | IP Segment [redacted] — [redacted] | Search

□	No.	IP Address	Device Type	MAC Address	Port	Initialization Status
□	1	[redacted]	[redacted]	[redacted]	37777	Initialized
□	2	[redacted]	[redacted]	[redacted]	37777	Initialized
□	3	[redacted]	[redacted]	[redacted]	37777	Initialized
□	4	[redacted]	[redacted]	[redacted]	37777	Initialized
□	5	[redacted]	[redacted]	[redacted]	37777	Initialized

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 Access Controller, 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**, 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 Configuring Basic User Information

Procedure

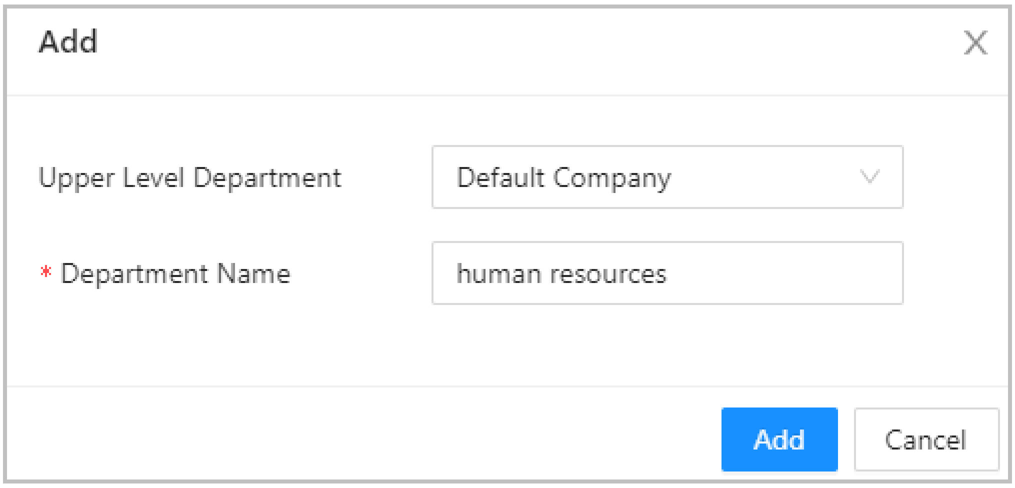
Step 1 On the home page, select **Person Management**.

Step 2 Create a department.

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

The default company cannot be deleted.

Figure 5-12 Add department



Add

Upper Level Department: Default Company

* Department Name: human resources

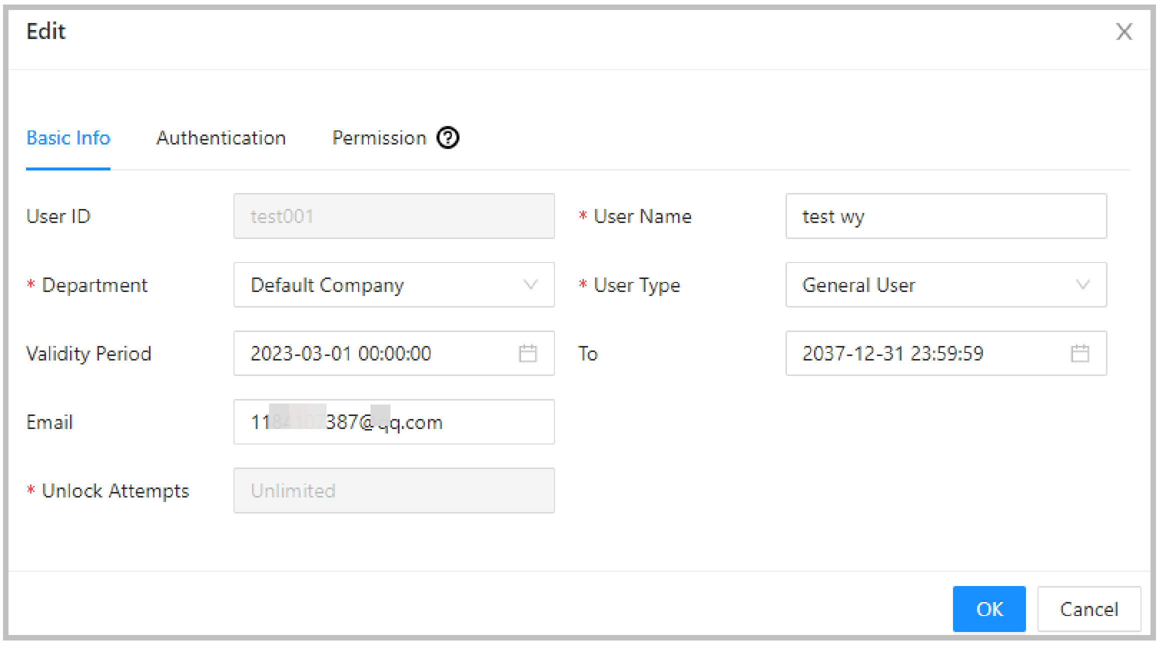
Step 3 Add users.

- Add users one by one.

  When you want to assign access permissions to one person, you can add users one by one. For details on how to assign access permissions, see "5.2.7 Adding Area Permissions".

  1. Click **Add**, and then enter the basic information for the user.

Figure 5-13 Basic information on the user



Edit

User ID: test001

* User Name: test wy

* Department: Default Company

* User Type: General User

Validity Period: 2023-03-01 00:00:00 To 2037-12-31 23:59:59

Email: 11[redacted]387@[redacted]q.com

* Unlock Attempts: Unlimited

Table 5-5 parameters description

Parameter	Description
User ID	The ID of the user.
Department	The department that the user belongs to.

Parameter	Description
Validity Period	Set a date on which the access permissions of the person will become effective.
Email	The Email address must be same to the Email account that is used to sign up to DMSS.
To	Set a date on which the access permissions of the person will expire.
User Name	The name of the user.
User Type	The type of the user. ● **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 set number of times. After the defined period expires or the unlocking times runs out, they cannot unlock the door. ● **Patrol User**: Patrol users will have their attendance tracked, but they have no unlocking permissions. ● **Blocklist User**: When users in the blocklist unlock the door, service personnel will receive a notification. ● **Other User**: When they unlock the door, the door will stay unlocked for 5 more seconds.
Unlock Attempts	The times of unlock attempts for guest users.

2. Click **Add**.

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

- Add users in batches.
  1. Click **Import** > **Download Template** to download the user template.
  2. Enter user information in the template, and then save it.
  3. Click **Import**, and upload the template to the Platform.

     The users are added to the Platform automatically.

Step 4 Click **OK**.

5.2.5.2 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 1 password, 5 IC/ID cards, 3 fingerprints, and 5 Bluetooth cards.

5.2.5.2.1 Adding Password

Add password to users, and then they can gain access by entering the password.

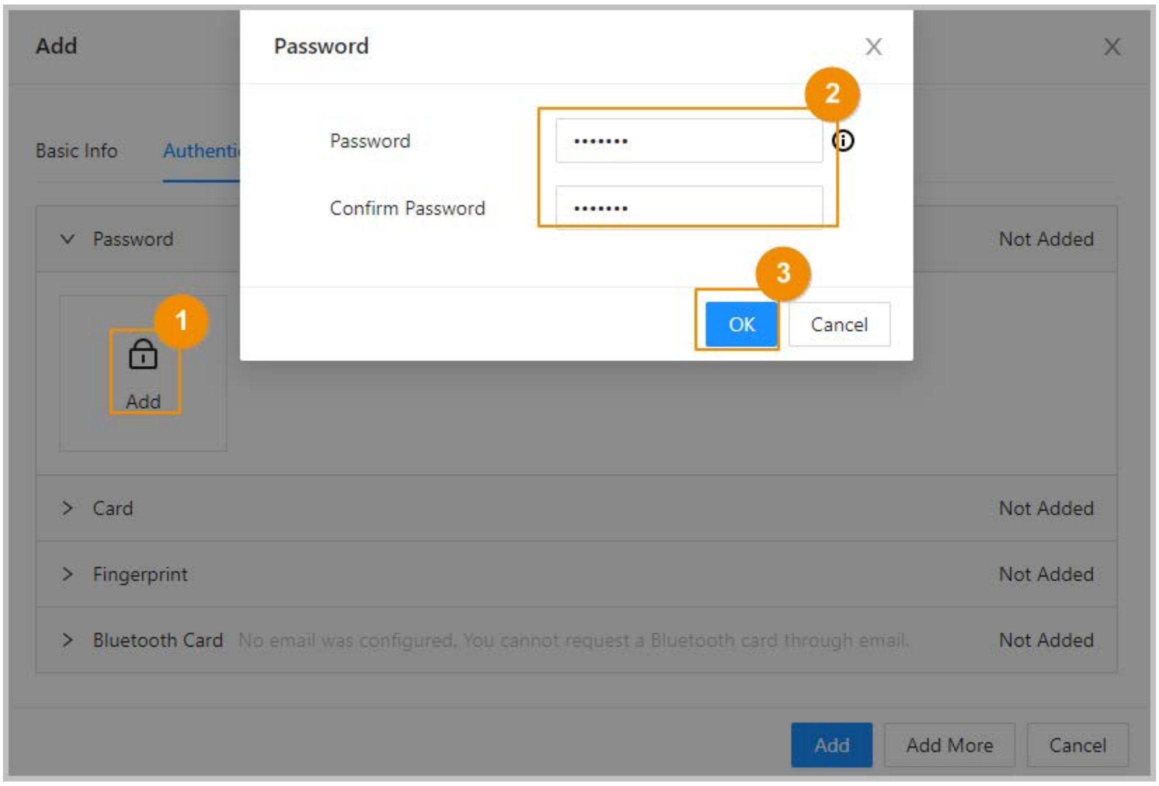
Procedure

Step 1 On the **Authentication** tab, click **Add**

Step 2 Enter and confirm password.

Step 3 Click **OK**.

Figure 5-14 Add password



5.2.5.2.2 Adding Cards

Add IC cards or ID cards to users, and then they can gain access by swiping cards.

Procedure

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

1. On the **Person Management** page, select **More** > **Card Type**.
2. Select ID or IC Card, and then click **OK**.

   Make sure that the card type is same as the card type that will be issued; otherwise, the card number cannot be read. For example, if the issued card is an ID card, set card type to ID card.
3. Select **More** > **Card No. System**.
4. Select decimal format or hexadecimal format for the card number.

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

3 methods are available to add cards.

- Enter the card number manually.
  1. Click **Add**.
  2. Enter the card number, and then click **Add**.
- Read the number automatically through a card enrollment reader.
  1. Click **Modify**, and then select **Enrollment Reader**.
     Make sure that the card enrollment reader is connected to your computer.
  2. Follow the on-screen instructions to download and install the plug-in.
  3. Click **Read Card**, and then swipe cards on the enrollment reader.
     A 60-second countdown is displayed to remind you to swipe cards, 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**.

- Read the number automatically through a card reader.
  1. Click **Modify**, and then select a card reader.
     Make sure that the card reader is connected to your computer.
  2. Click **Read Card**, and then swipe cards on the card reader.
     A 60-second countdown is displayed to remind you to swipe cards, and the system will read the card number automatically. If the 60-second countdown expires, click **Read Card** again to start a new countdown.
  3. Click **Add**.

Step 3 Click **Add**.
The cards are added to the user.

Related Operations

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

5.2.5.2.3 Adding Fingerprint

Add fingerprint to users, and then they can unlock through fingerprint.

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**.

5.2.5.2.4 Adding Bluetooth Cards

Add Bluetooth cards to users, so they can gain access through Bluetooth cards.

Prerequisites

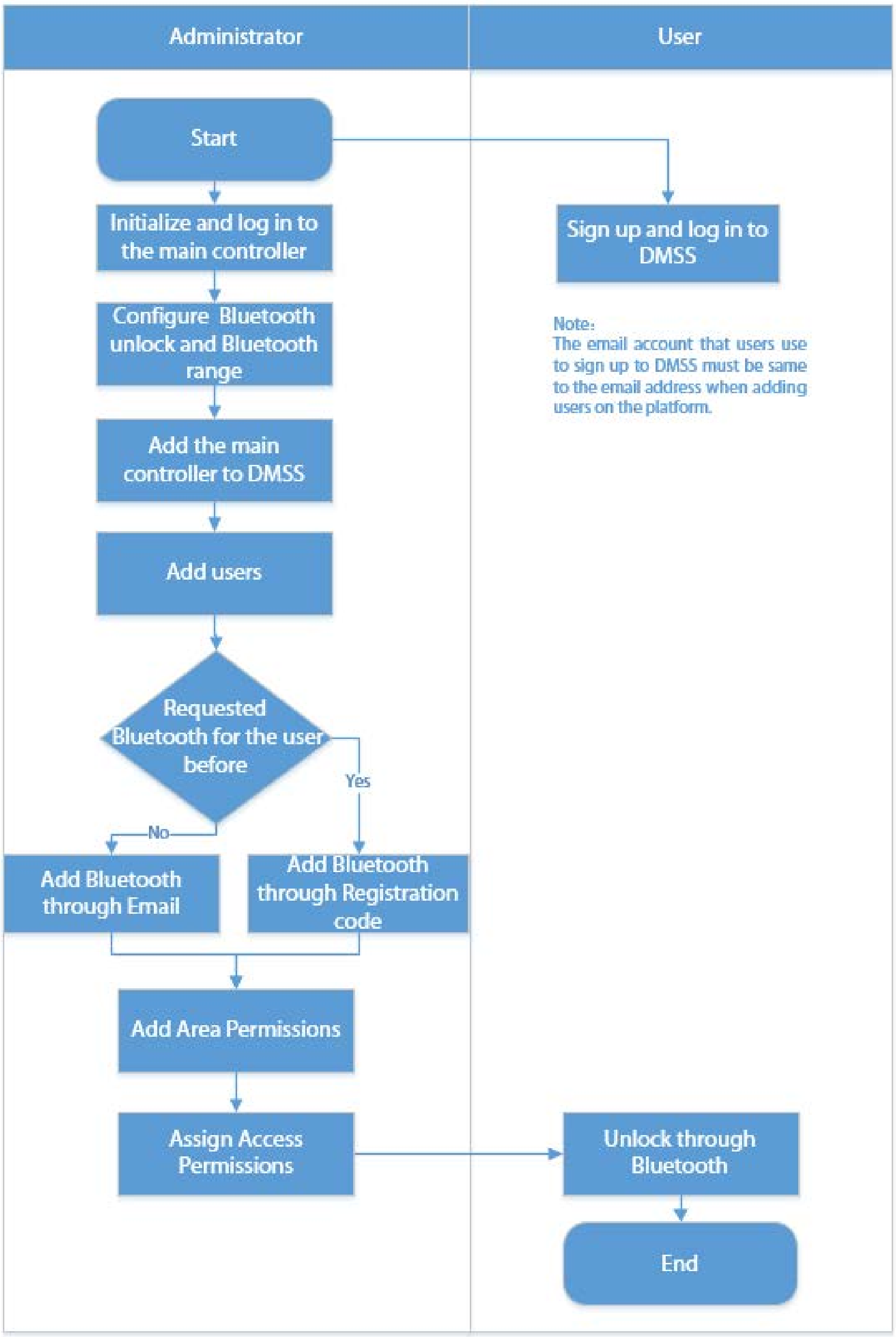
- Bluetooth unlock function has been turned on.
- The main controller has been added to DMSS. For details, see "5.2.11 Configuring Cloud Service".
- Users have been added to the Platform of the Access Controller. For details, see "5.2.5.1 Configuring Basic User Information".
- General users such as company employees have installed and signed up to DMSS with their Email.

  The Email account that users use to sign up to DMSS must be same to the email address you entered when adding users to the access controller.

Background Information

Refer to the flowchart of configuring Bluetooth unlock. Administrator and general users need to do different operations as below. General users like company employees only need to sign up and log in to DMSS with their Email, and then they can unlock through Bluetooth cards that are issued to them.

Figure 5-15 Flowchart of configuring Bluetooth unlock


Administrator
User
Start
Initialize and log in to the main controller
Configure Bluetooth unlock and Bluetooth range
Add the main controller to DMSS
Add users
Requested Bluetooth for the user before
Yes
No
Add Bluetooth through Email
Add Bluetooth through Registration code
Add Area Permissions
Assign Access Permissions
Sign up and log in to DMSS
Note:
The email account that users use to sign up to DMSS must be same to the email address when adding users on the platform.
Unlock through Bluetooth
End

Procedure

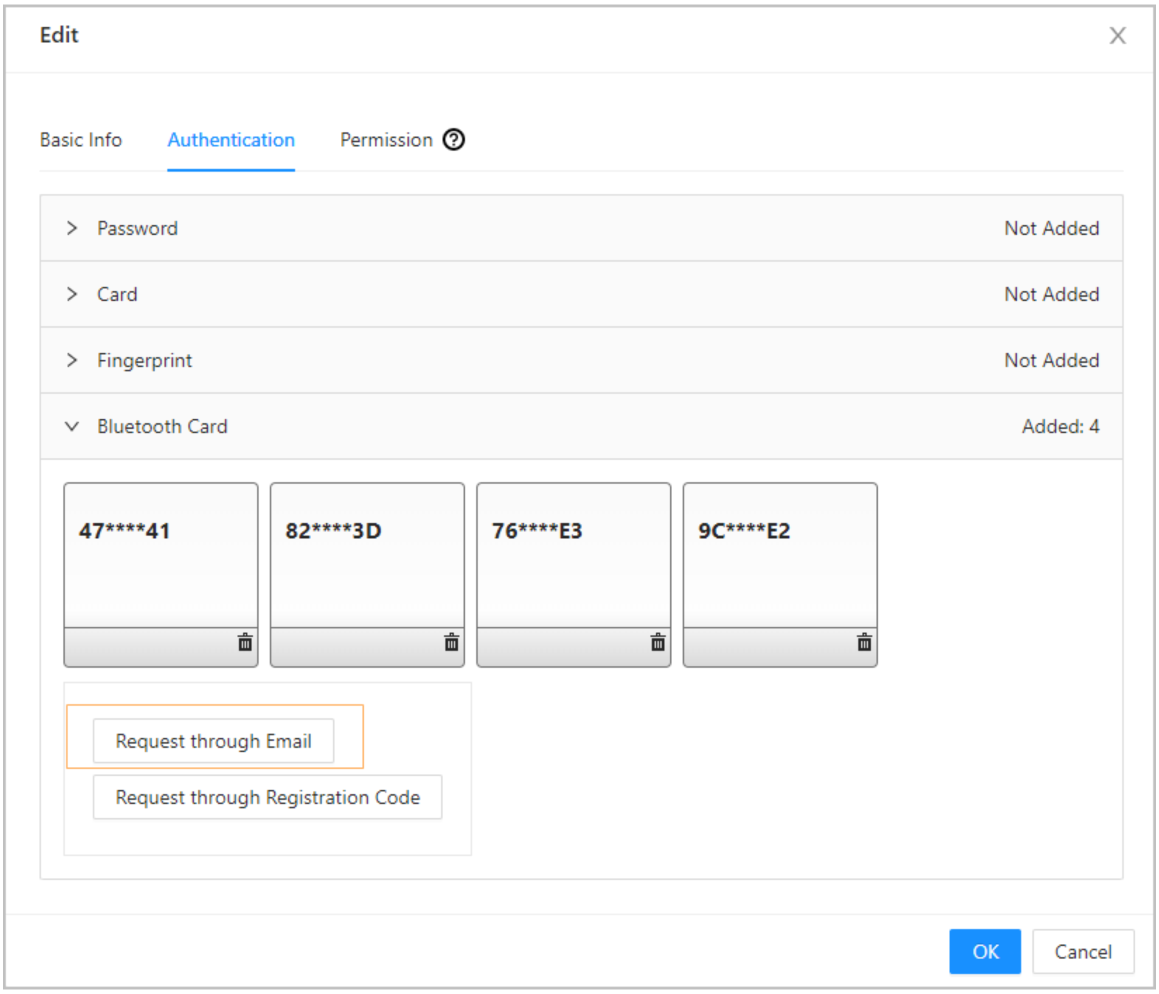
Step 1 On the tab, click **Bluetooth Card**.

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 5-16 Request through Email



- Request through Email in batches.

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

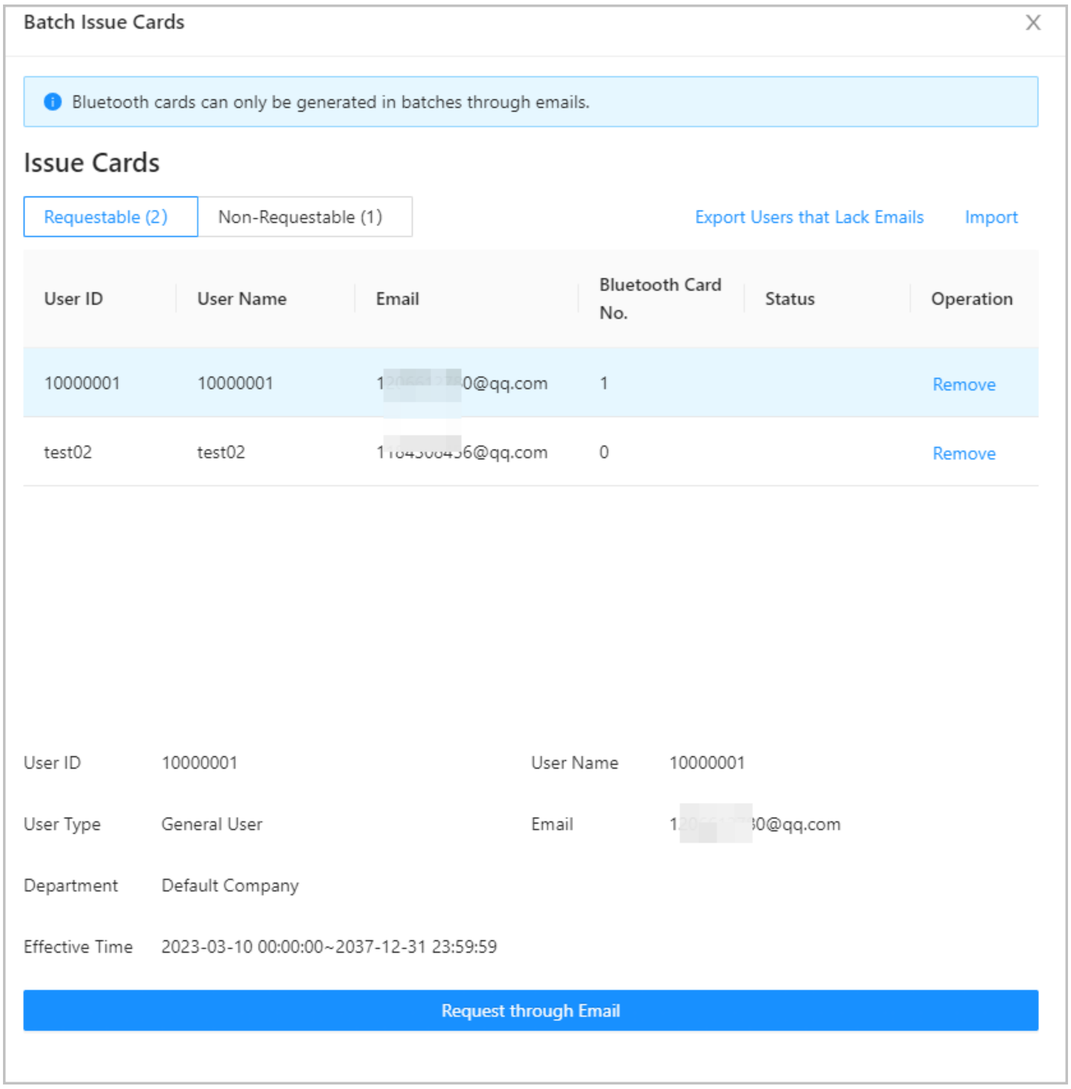
   Batch issue cards only supports requesting through Email.

   - ◇ Issue Bluetooth cards to all users in 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 **Request through Email**.

- ◇ For users that do not have Email or already have 5 Bluetooth cards, they will be displayed in the non-requestable list.
- ◇ Export users that lack Emails: Click **Export**, enter their Emails in the format, and then click **Import**. They will be moved into the requestable list.

Figure 5-17 Batch issue cards



Batch Issue Cards

Bluetooth cards can only be generated in batches through emails.

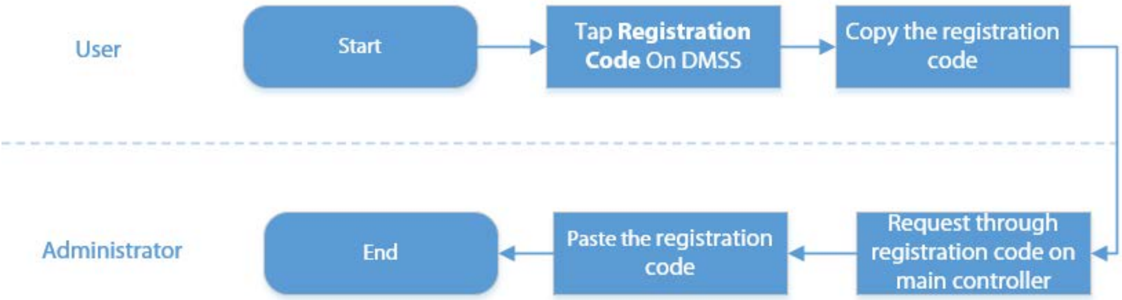
Issue Cards

User ID	User Name	Email	Bluetooth Card No.	Status	Operation
10000001	10000001	1[redacted]0@qq.com	1		Remove
test02	test02	1[redacted]6@qq.com	0		Remove

User ID	10000001	User Name	10000001
User Type	General User	Email	1[redacted]0@qq.com
Department	Default Company		
Effective Time	2023-03-10 00:00:00~2037-12-31 23:59:59		

- If you have requested Bluetooth cards for the user before, you can add the Bluetooth cards through registration code.

Figure 5-18 The flowchart of requesting through registration code



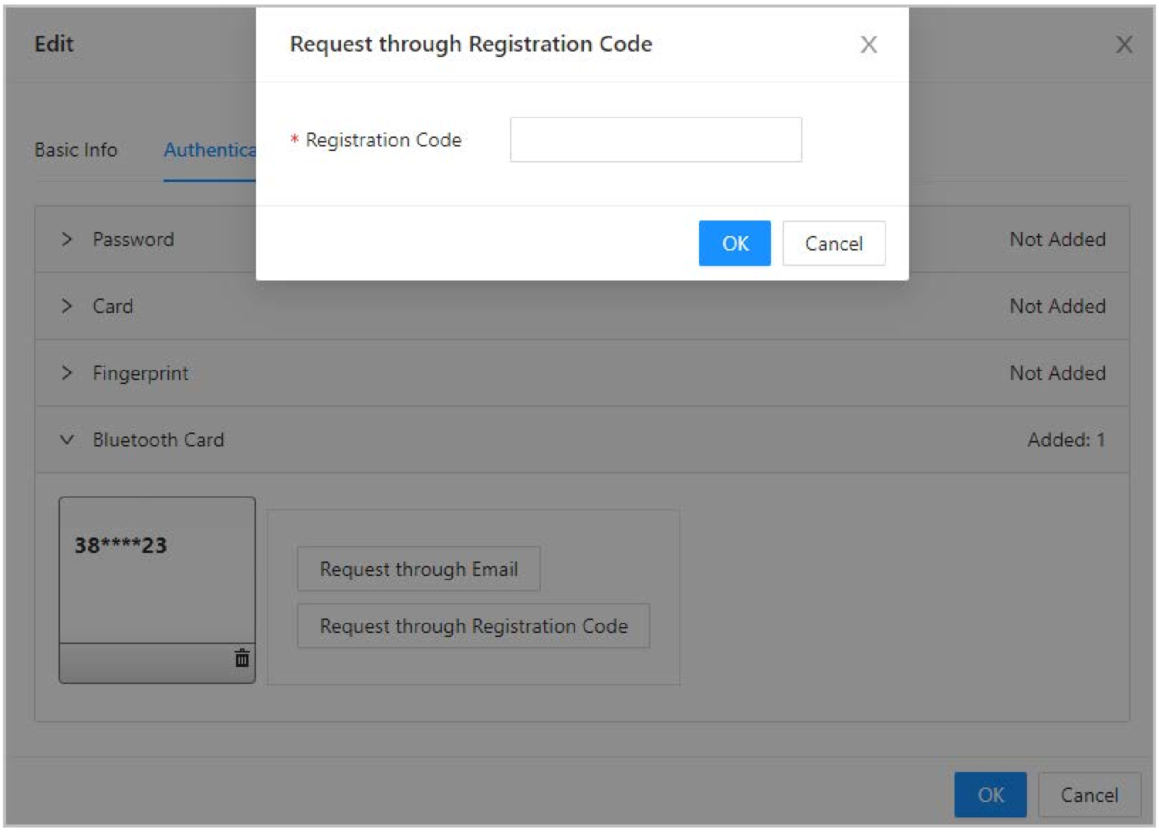
User
Start
Tap Registration Code On DMSS
Copy the registration code
Administrator
Request through registration code on main controller
Paste the registration code
End

1. On DMSS, tap **Registration Code** of a Bluetooth card.

The registration code is automatically generated by DMSS.

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 5-19 Request through registration code



4. Click **OK**.

   The Bluetooth card is added.

Step 2 Click **OK**.

Result

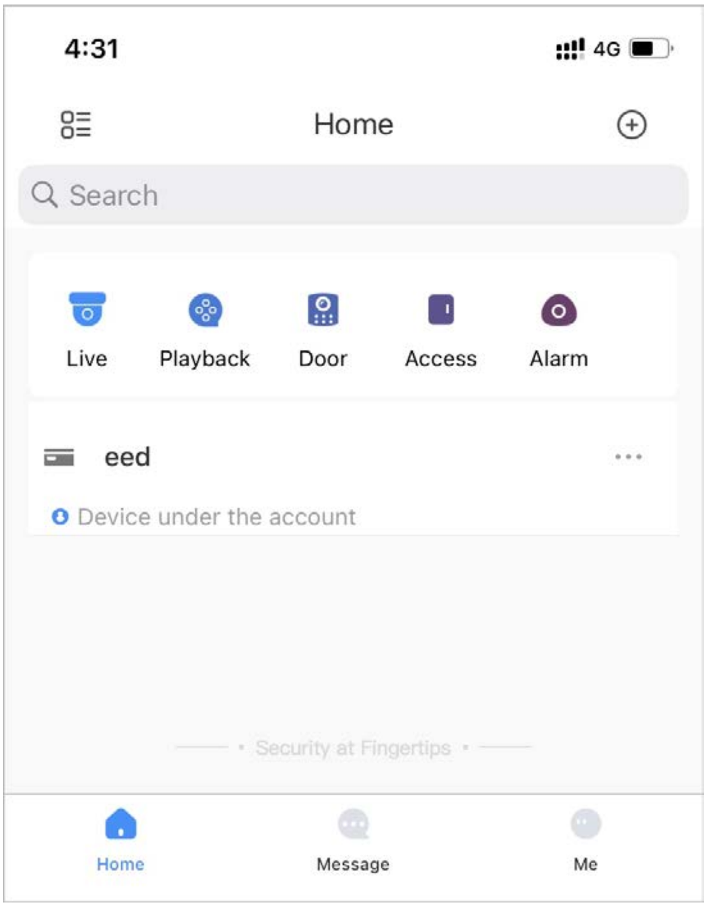
After users sign up and log in to DMSS with the Email address, they can open DMSS to unlock the door through Bluetooth cards. For details, see the user's manual of DMSS.

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

  ⚠

  In the auto unlock mode, the Buletooth card will frequently unlock the door if you are still in the Bluetooth range, and finally a failure might occur. Please turn off Bluetooth on the phone and turn it on again.
- Shake to Unlock: The door unlocks when you shake your phone to allow the Bluethooth card transmits signals to the card reader.

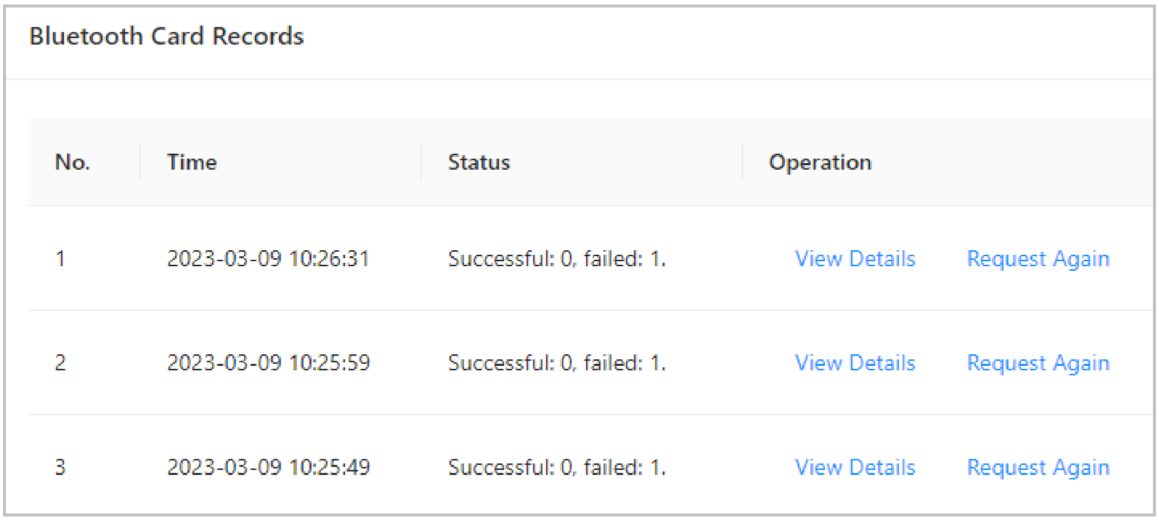
Figure 5-20 Unlock the door through Bluetooth cards



Related Operations

- Users can manage Bluetooth cards on DMSS.
  - Move to the Top: If multiple Bluetooth cards have been added, you can top up a card as the card in use.
  - Rename: Rename the Bluetooth card.
  - Delete: Delete the Bluetooth card.
- Export users that lack Emails: Click **Export**, enter their Emails in the format, and then click **Import**. They will be moved into the requestable list.
- View the request records: On the **Person Management** page, click **More** > **Bluetooth Card Records** to view the request status.

Figure 5-21 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 Time Templates (Optional)

Time template defines the unlock schedules of the Controller. The platform offers 4 time templates by default. The template is also customizable.

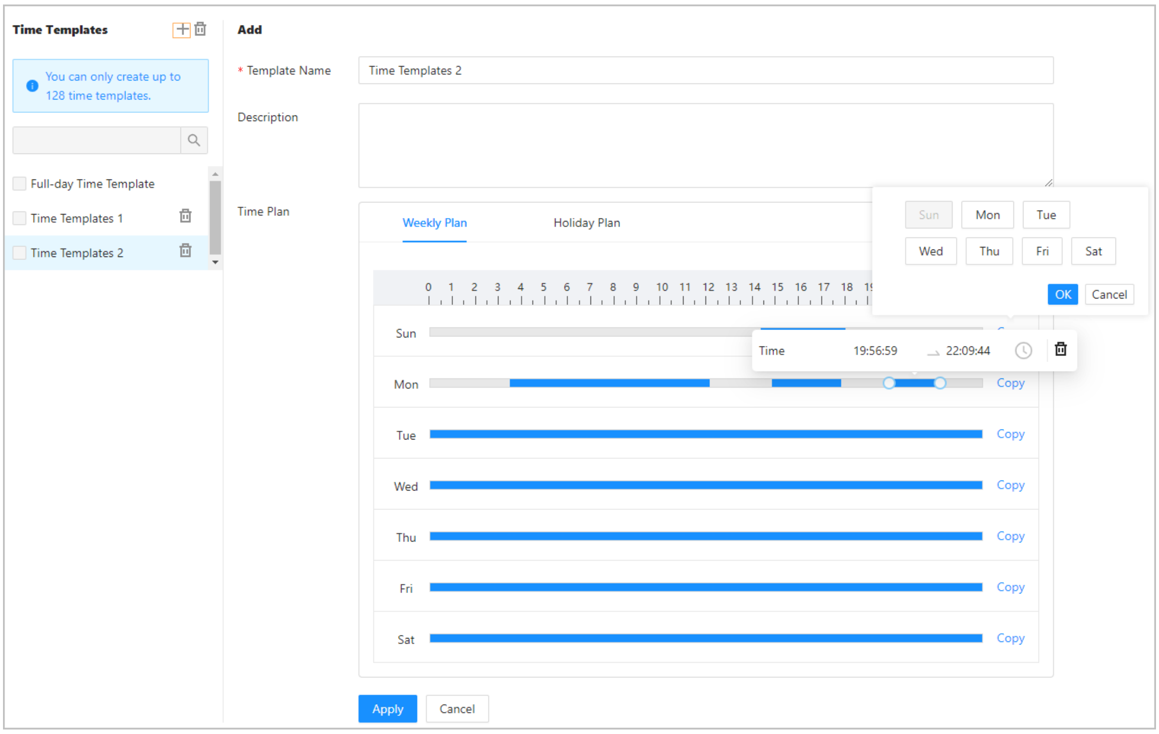
Procedure

Step 1 On the home page, select **Access Control Config** > **Time Template**, and then click +.

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

Step 2 Enter the name of the time template.

Figure 5-22 Create time templates



* Template Name: Time Templates 2

Description:

Time Plan: Weekly Plan

Time 19:56:59 → 22:09:44

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**.

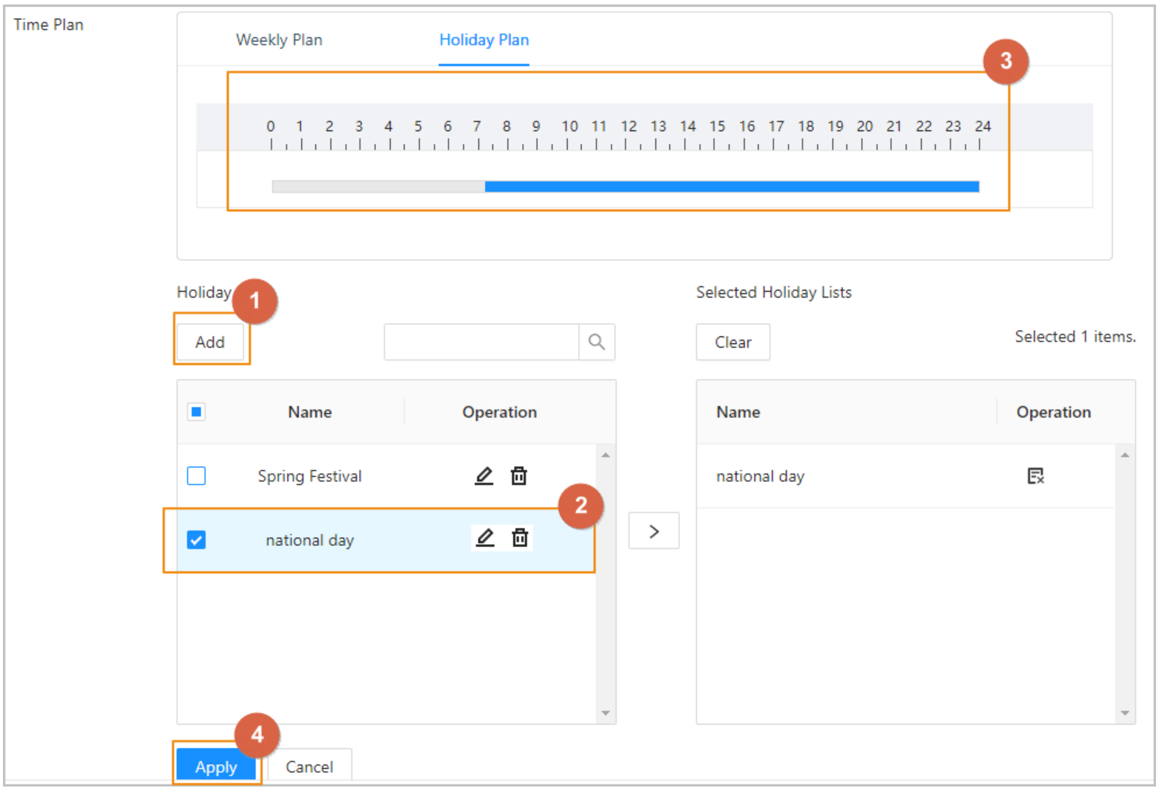
Step 5 Configure holiday plans.

1. Click the **Holiday Plan** tab, and then click **Add** to add holidays.

   You can add up to 64 holidays.

2. Select a holiday.
3. Drag the slider to adjust the time period for the holiday.
4. Click **Apply**.

Figure 5-23 Create holiday plan



5.2.7 Adding Area Permissions

An area permission group is a collection of door access permissions in a defined time. Create a permission group, and then associate users with the group so that users will be assigned with access permissions defined for the group.

Procedure

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

Step 2 Click + .

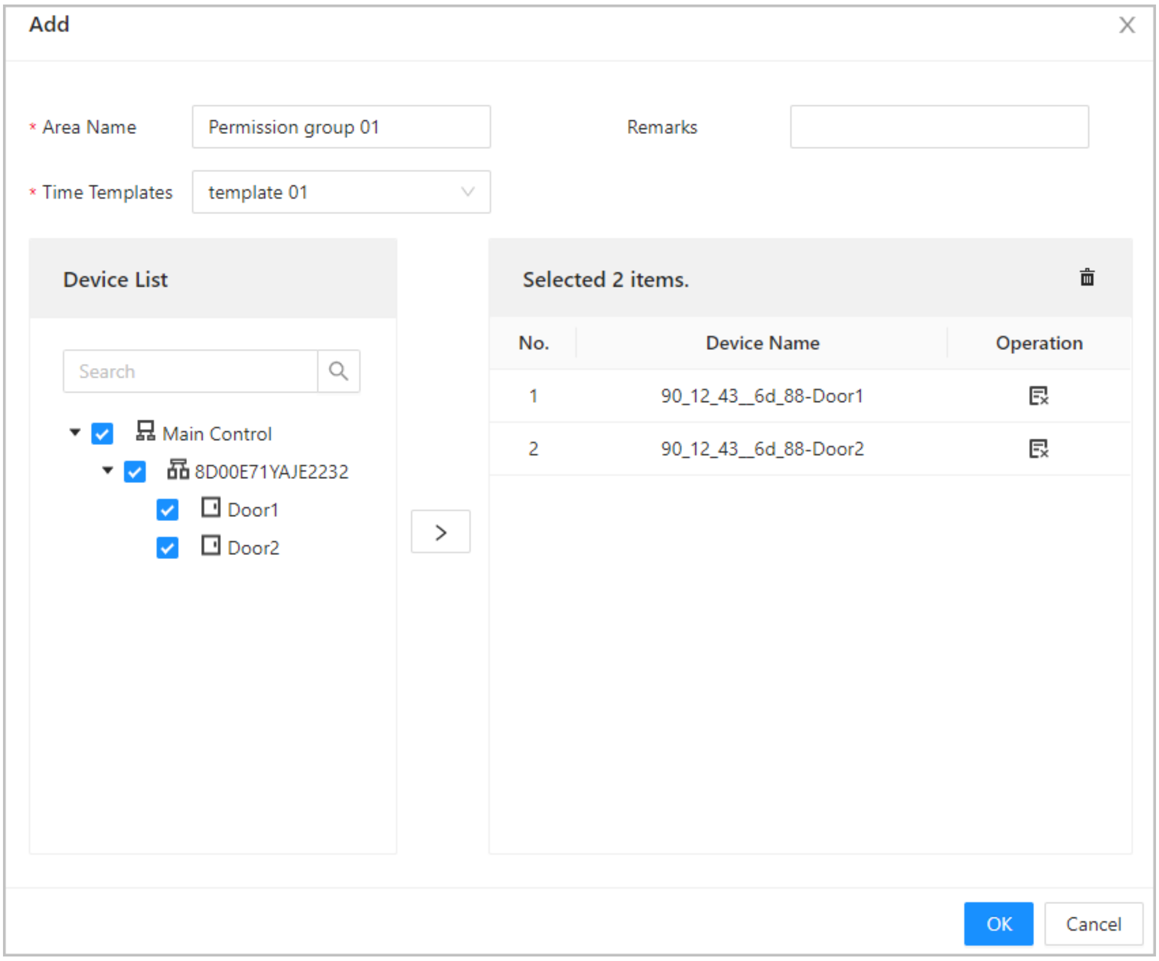
You can add up to 128 area permissions.

Step 3 Enter the name of the area permission group, remarks (optional), and select a time template.

Step 4 Select doors.

Step 5 Click **OK**.

Figure 5-24 Create area permission groups



Add

* Area Name: Permission group 01

Remarks:

* Time Templates: template 01

Device List

Search

- ☑ Main Control
  - ☑ 8D00E71YAJE2232
    - ☑ Door1
    - ☑ Door2

Selected 2 items.

No.	Device Name	Operation
1	90_12_43__6d_88-Door1	
2	90_12_43__6d_88-Door2	

5.2.8 Assigning Access Permissions

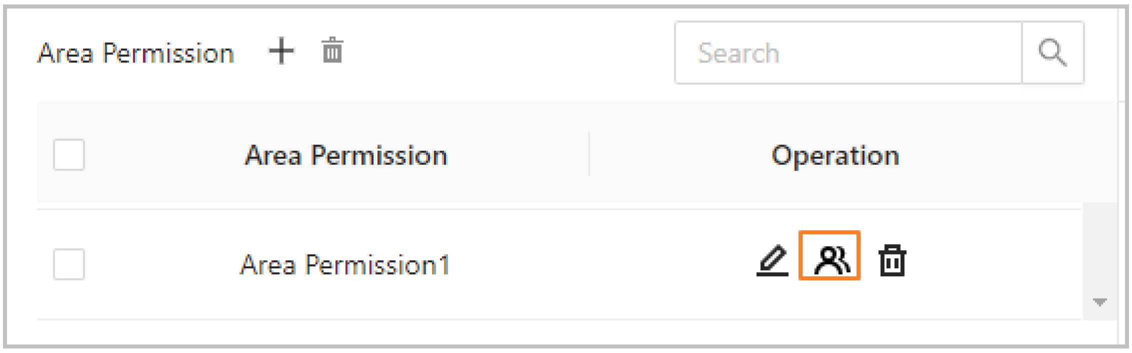
Assign access permissions to users by linking them to the area permission group. This will allow the users to gain access to secure areas.

Procedure

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

Step 2 Click for an existing permission group, and then select users from the department.

Figure 5-25 Select users



Area Permission

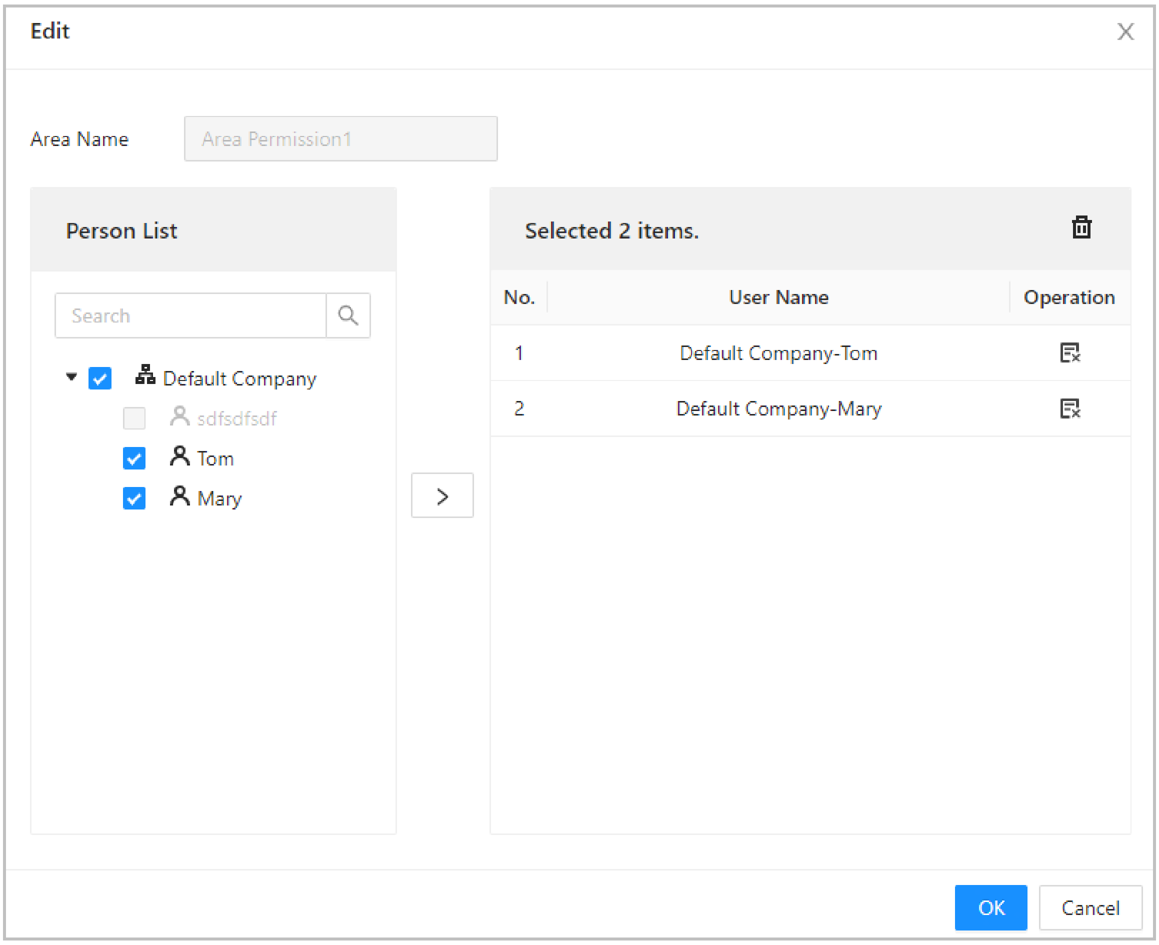
Search

□	Area Permission	Operation
□	Area Permission1	

You can select a whole department.

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

Figure 5-26 Assign permissions in batches



No.	User Name	Operation
1	Default Company-Tom	
2	Default Company-Mary	

Step 3 Click **OK**.

Related Operations

When you want to assign permission to a new person or change access permissions for an existing person, you can assign access permission to them one by one.

1. On the home page, select **Person Management**.
2. Select the department, and then select an existing user.

   If the user was not added before, click **Add** to add the user. For details on creating users, see "5.2.5 Adding Users".

3. Click ✎ corresponding to the user.
4. On the **Permission** tab, select existing permission groups.

   - You can click **Add** to create new area permissions. For details on creating area permissions, see "5.2.7 Adding Area Permissions".
   - You can link multiple area permissions to a user.

5. Click **OK**.

5.2.9 Viewing Authorization Progress

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

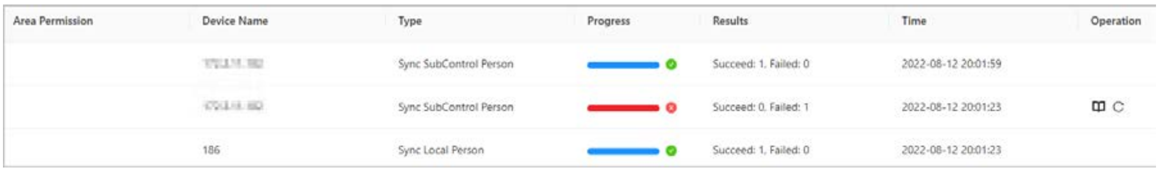
Procedure

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 5-27 Authorization progress



Area Permission	Device Name	Type	Progress	Results	Time	Operation
	[redacted]	Sync SubControl Person	✓	Succeed: 1, Failed: 0	2022-08-12 20:01:59	
	[redacted]	Sync SubControl Person	✗	Succeed: 0, Failed: 1	2022-08-12 20:01:23	🕮 ↻
	186	Sync Local Person	✓	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

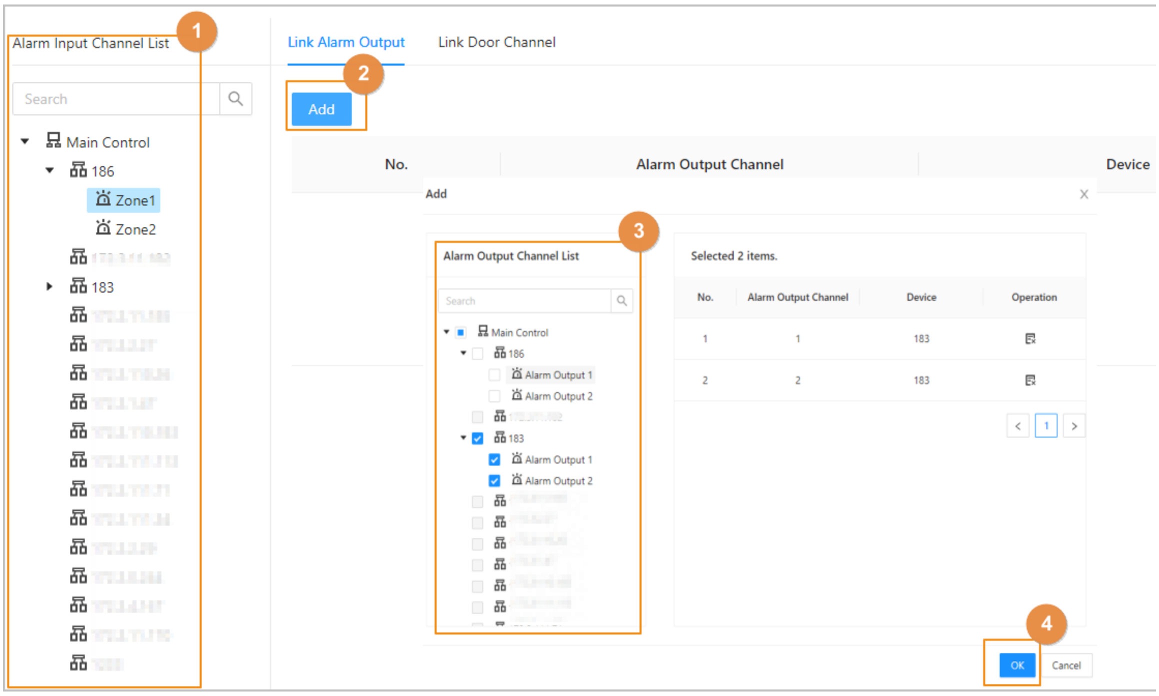
Step 1 Select **Access Control Config** > **Global Alarm Linkage**.

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.

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**.

Figure 5-28 Alarm output



Selected 2 items.

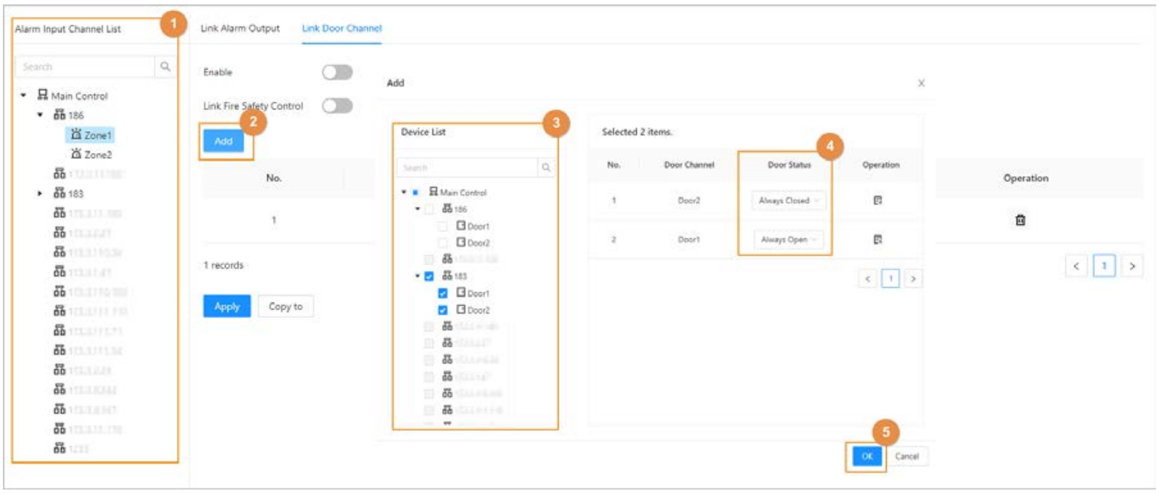
No.	Alarm Output Channel	Device	Operation
1	1	183	
2	2	183	

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

Step 3 Configure the door linkage.

1. Select an alarm input from the channel list, and then click **Add**.
2. 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 5-29 Door linkage



Selected 2 items.

No.	Door Channel	Door Status	Operation
1	Door2	Always Closed	
2	Door1	Always Open	

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

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

4. 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.

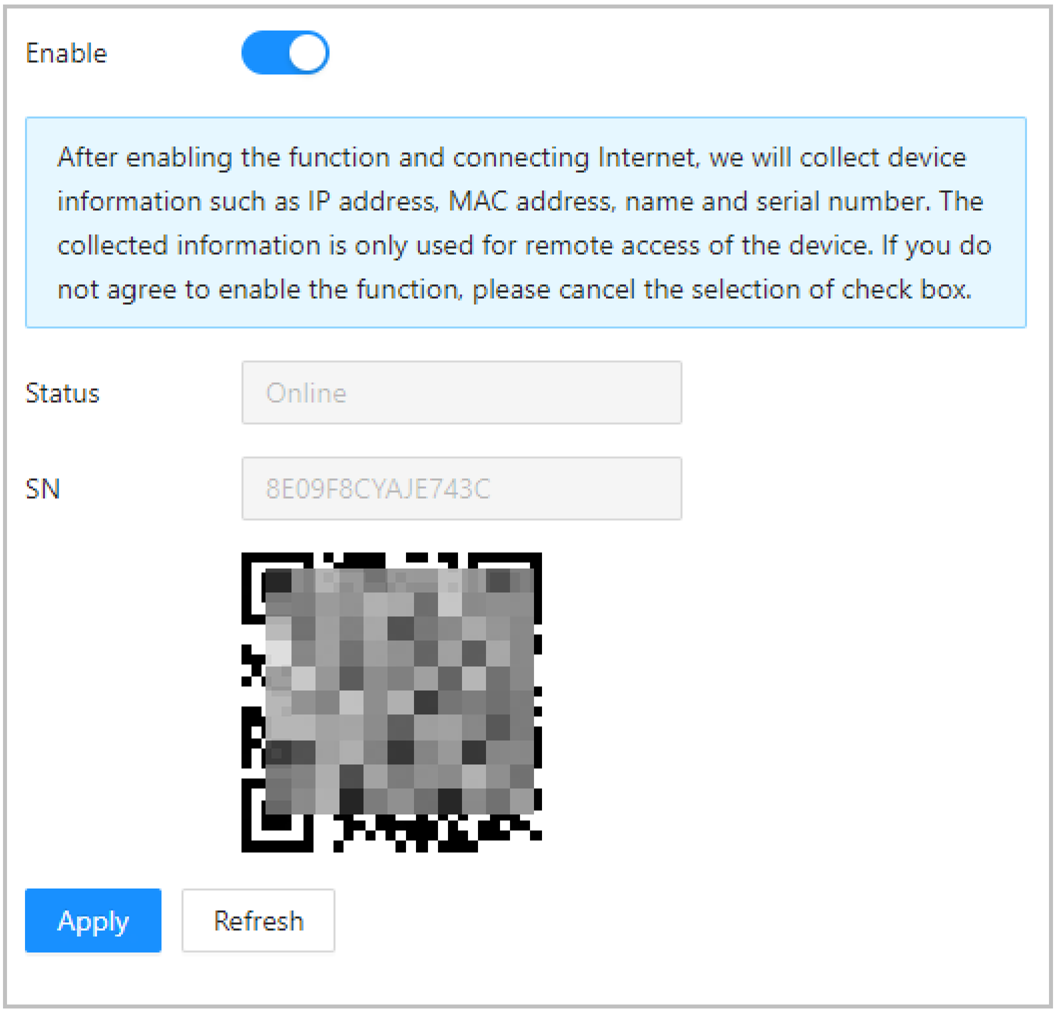
Procedure

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 5-30 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: Online

SN: 8E09F8CYAJE743C

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 from Dahua 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.

More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188