Access Controller

Quick Start Guide

Foreword

General

This manual introduces the installation and 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
V1.0.1	Updated the wiring.	September 2022
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])
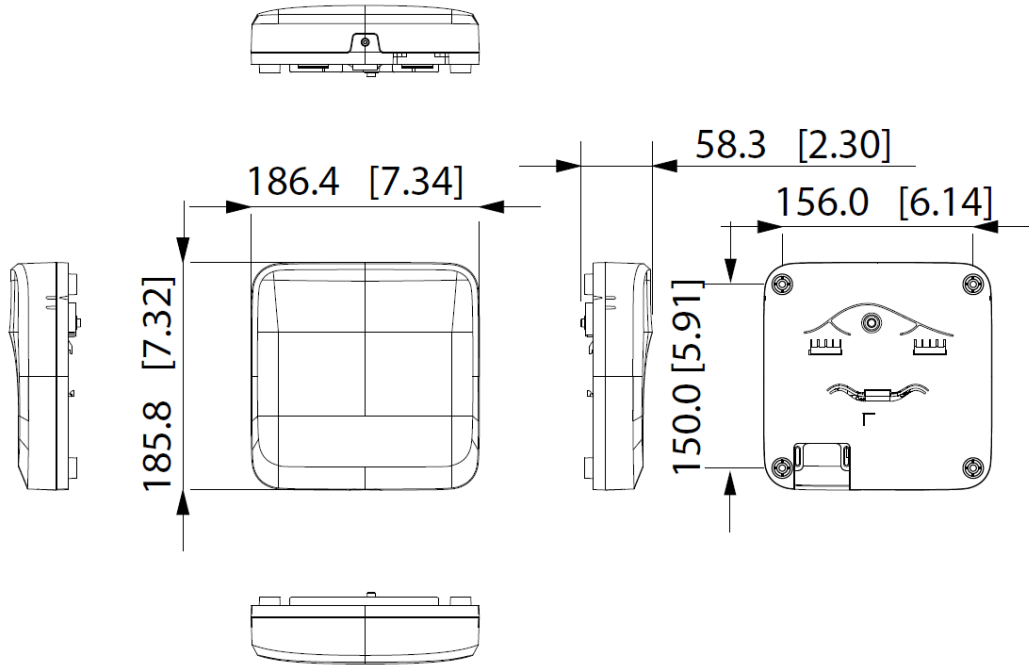
Figure 1-2 Front view

Table 1-1 Components description

No.	Description
1	Guiding mark
2	Front panel
3	Screw

Figure 1-3 Back cover
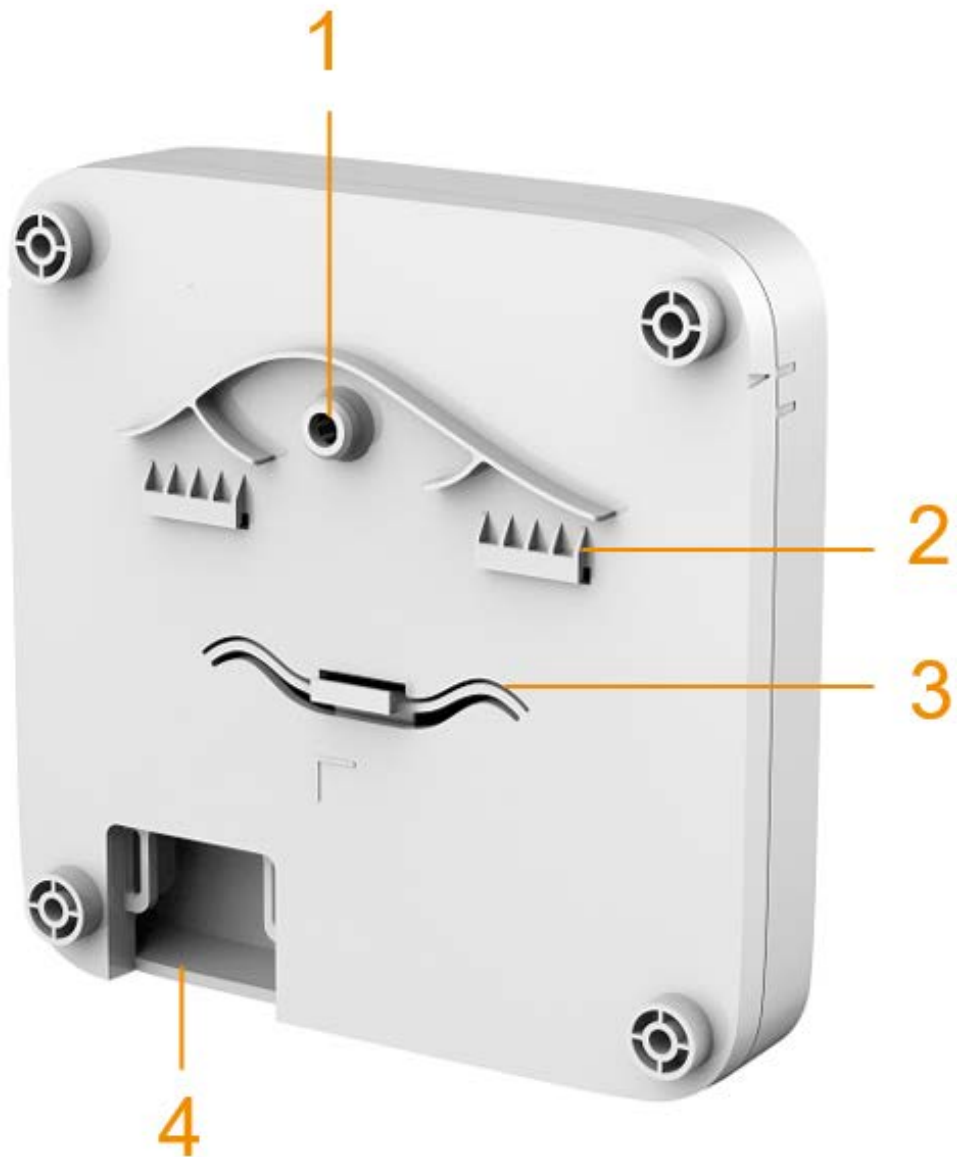
Table 1-2 Back cover description

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

2 Ports Overview

Figure 2-1 Ports
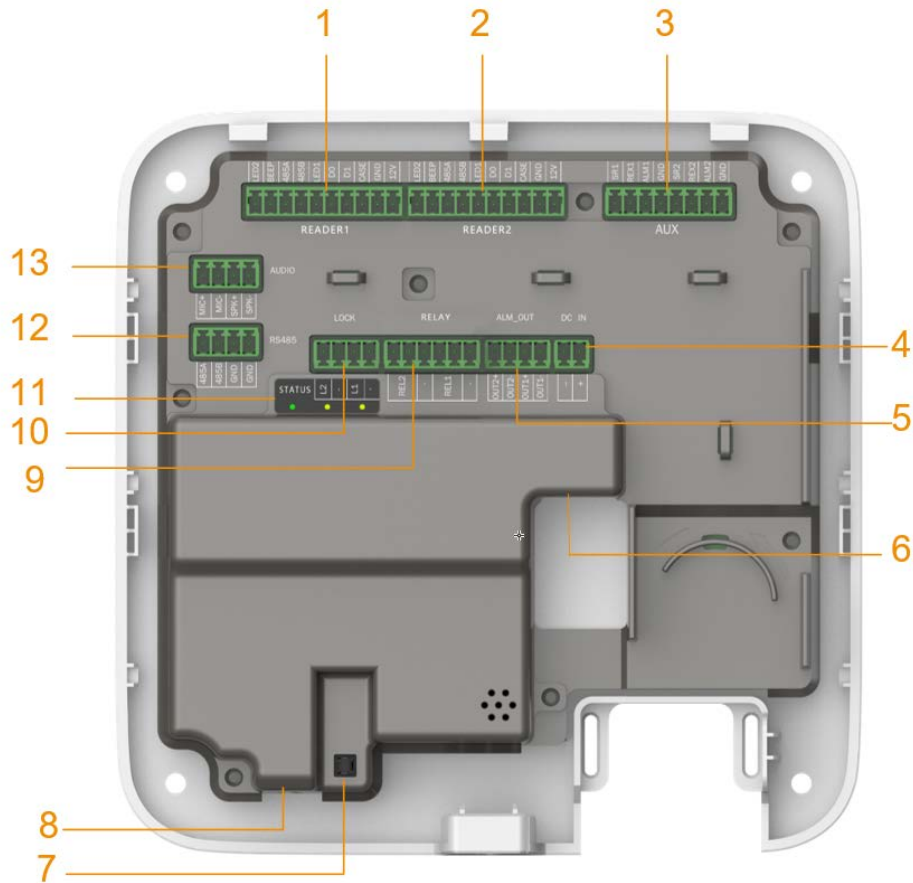
Table 2-1 Ports description

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
12	RS485	RS485 connector (not used)
13	AUDIO	Audio connector (not used)

Figure 2-2 Reader connector
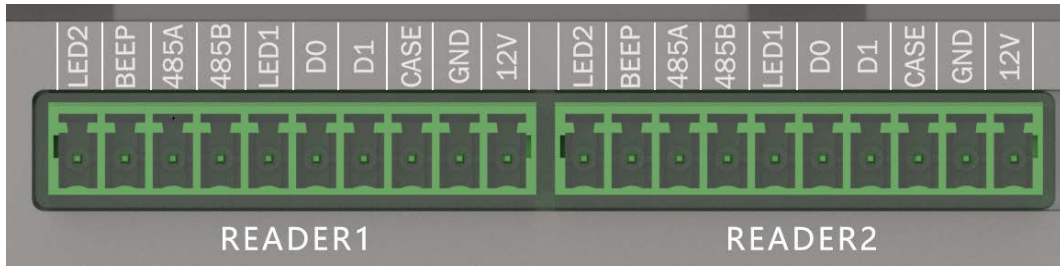
Table 2-2 Reader connector description

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
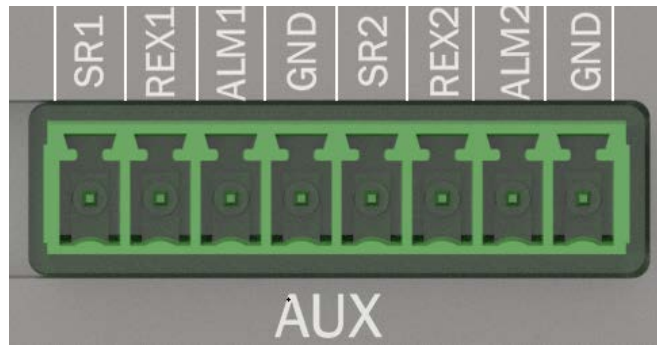
Table 2-4 Description of auxiliary I/O ports

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
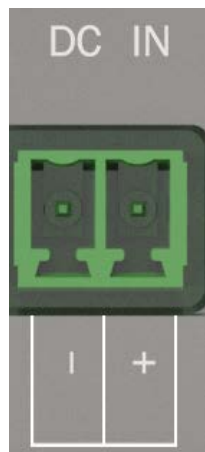
Table 2-5 Description of power ports

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

Figure 2-6 Alarm output ports
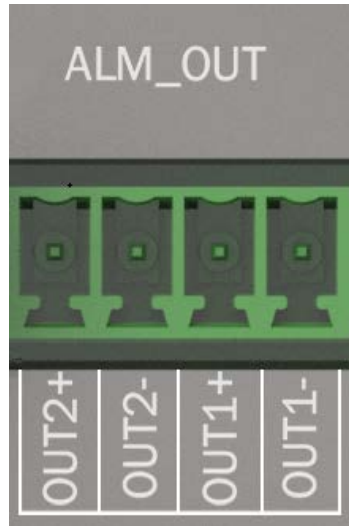
Table 2-6 Description of alarm output ports

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
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
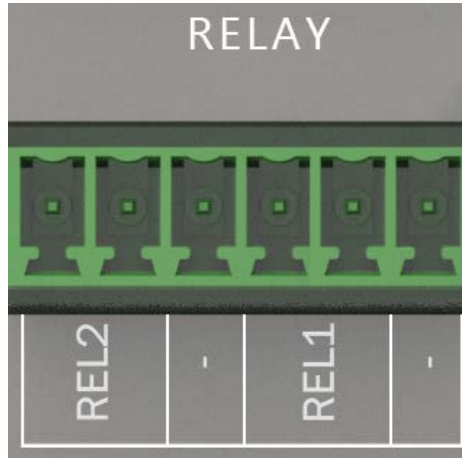

Table 2-8 Description of lock

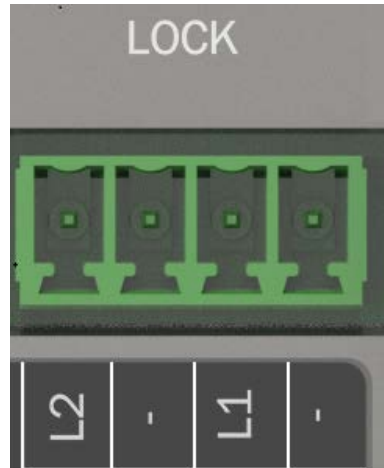| Ports	Description
L1/L2	Power one or two locks (DC output). The lock connector can also be used to power external devices.
REL2	Connects to lock. 12 VDC Max total load = 1000 mA 📖 ● For controlling up to 12 V lock. ● Connect locks and loads to the pins according to the wiring diagram generated through the hardware configuration. For details, see "3 Wring of Locks".
–	Grounding wire.

Figure 2-9 RS-485 ports
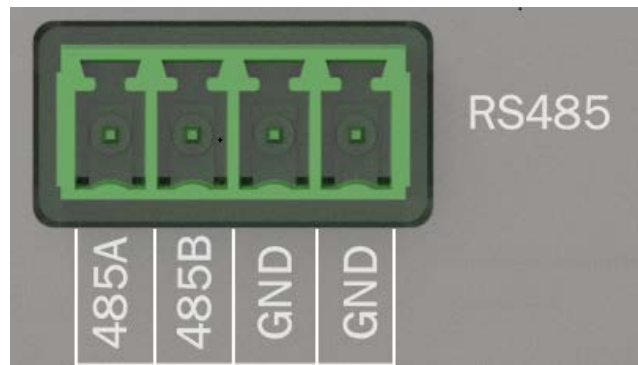
Table 2-9 Description of RS-485

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

Figure 2-10 Audio ports
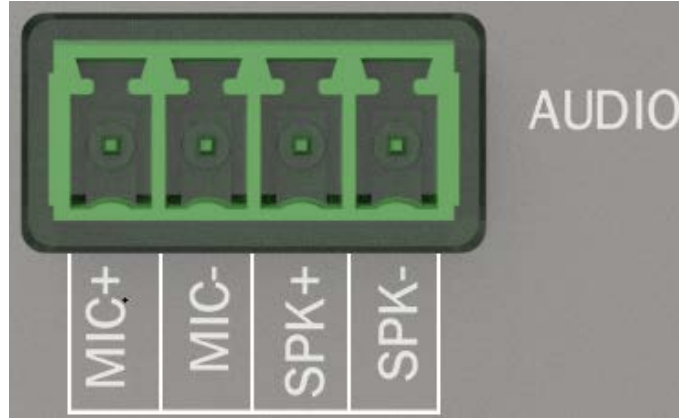
Table 2-10 Description of audio ports

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

3 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)

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

Figure 3-2 Lock 2 (door 2)

3. Wiring the locks according to the diagram below.

Figure 3-3 Wiring of locks
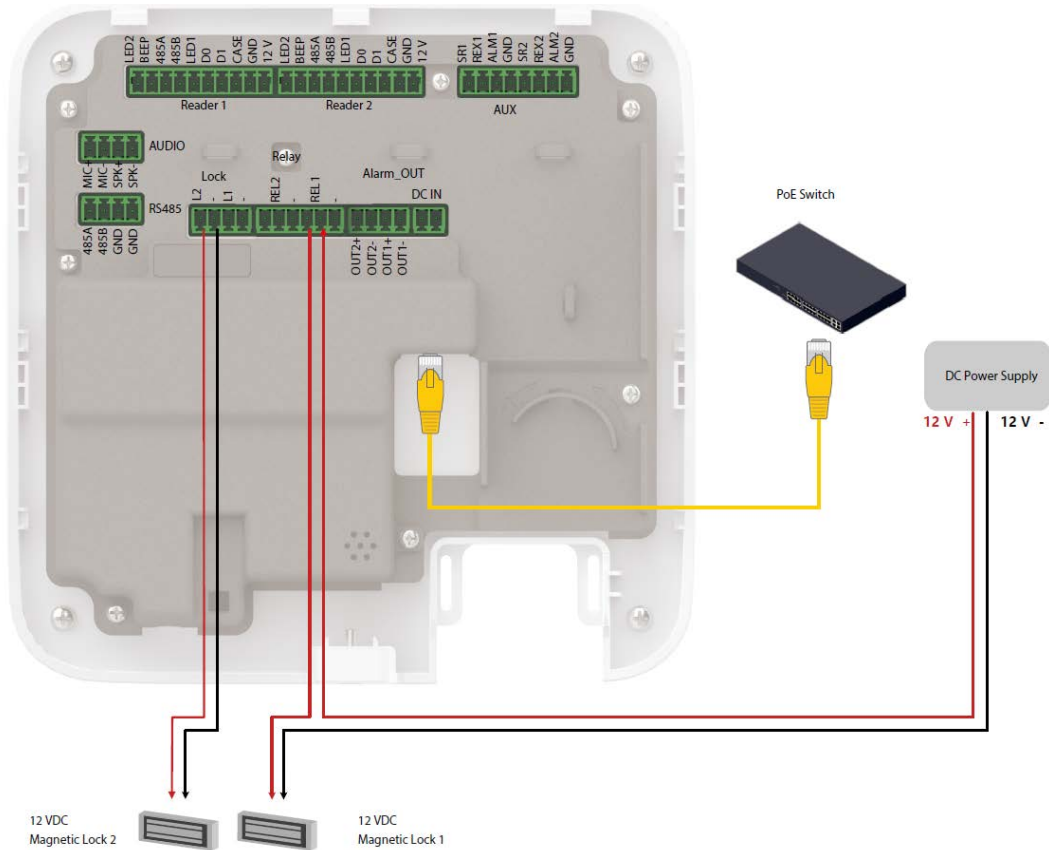
3.1.2 Wring of Dual Magnetic Locks with 12 V External Power Supply (12 V and Relay)

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)

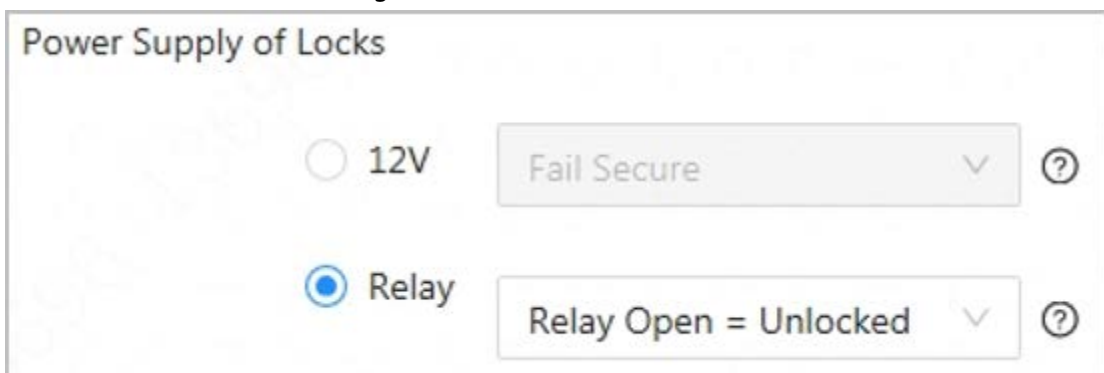3. Wiring the locks according to the diagram below.

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
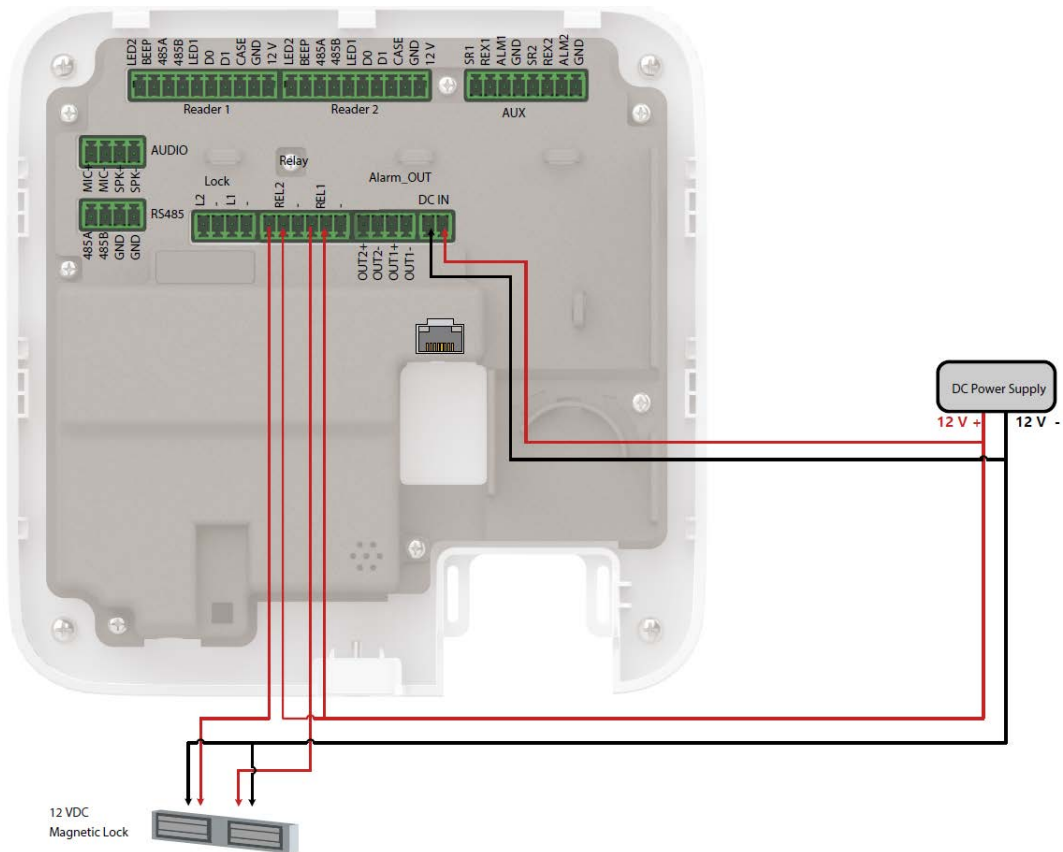
3.2 Wiring of Electric Strike Lock

3.2.1 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).
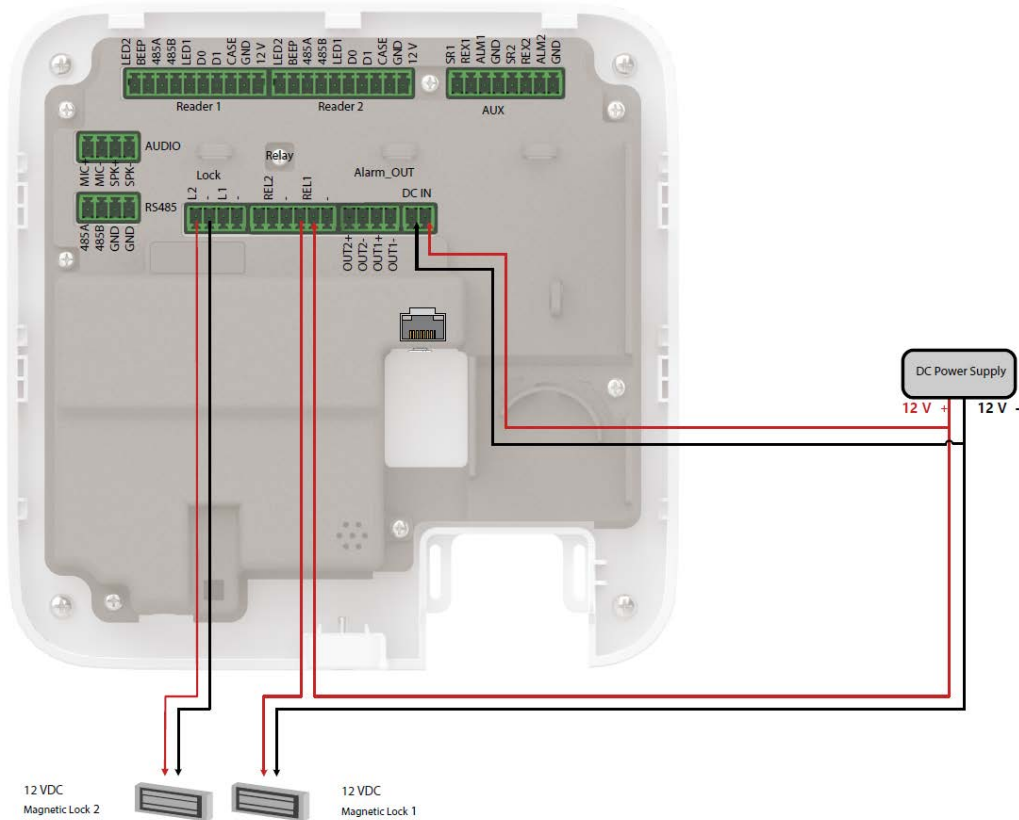
Figure 3-13 Lock 1 (door 1)
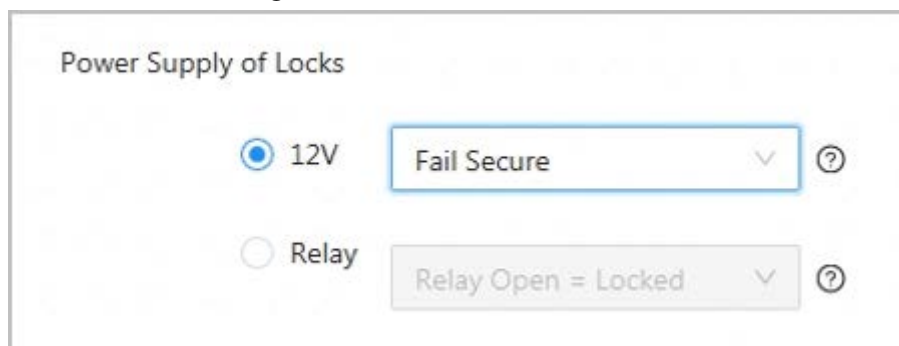
2. Select **Fail Secure** from the **12V** list for lock 2 (door 2).

Figure 3-14 Lock 2 (door 2)
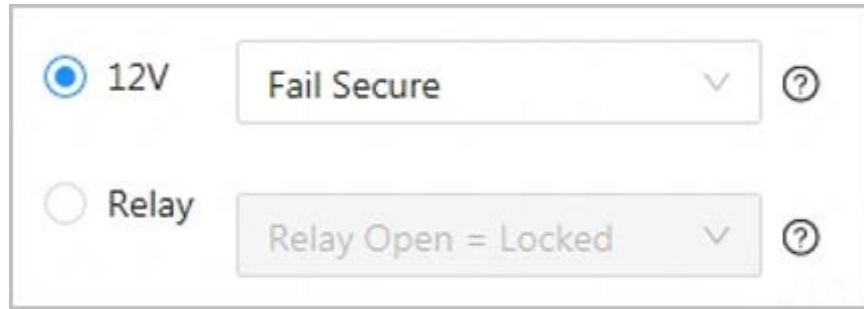
3. Wiring the locks according to the diagram below.

Figure 3-15 Wiring of locks
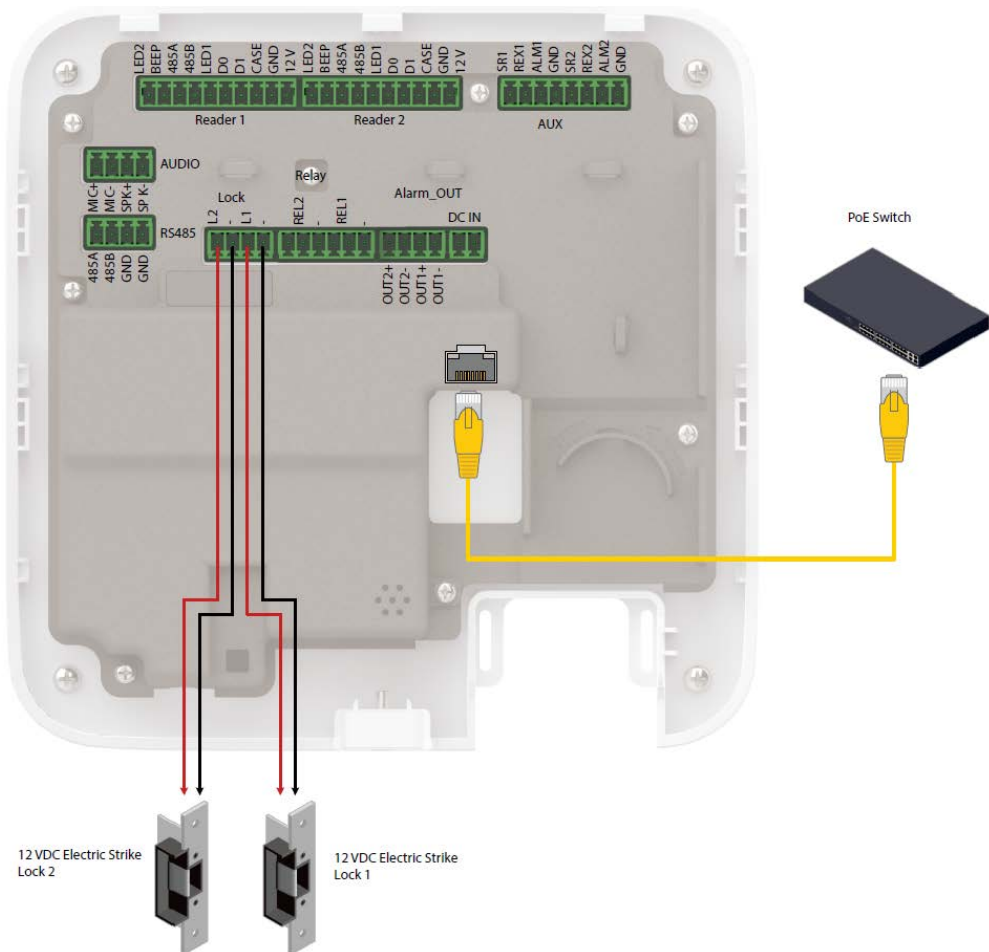
3.2.2 Wring of Dual Electric Strikes with 12 V External Power Supply

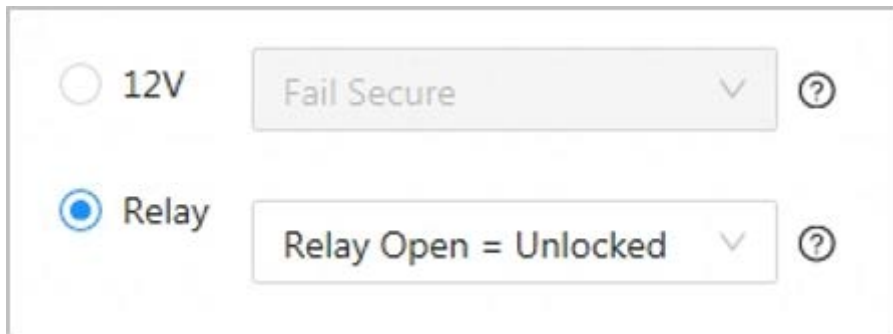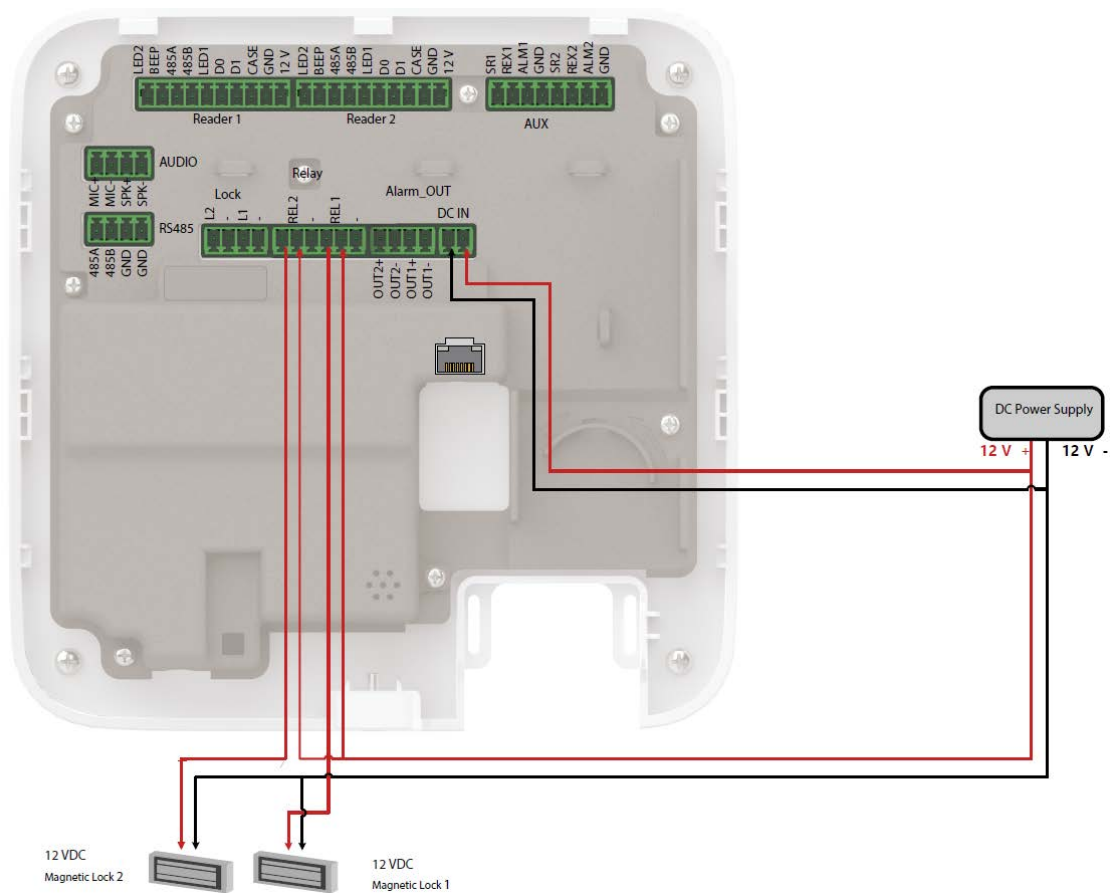Supply power for the Access Controller through 12 V external power supply. Both doors use the external power supply.

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

Figure 3-16 Lock 1 (door 1)
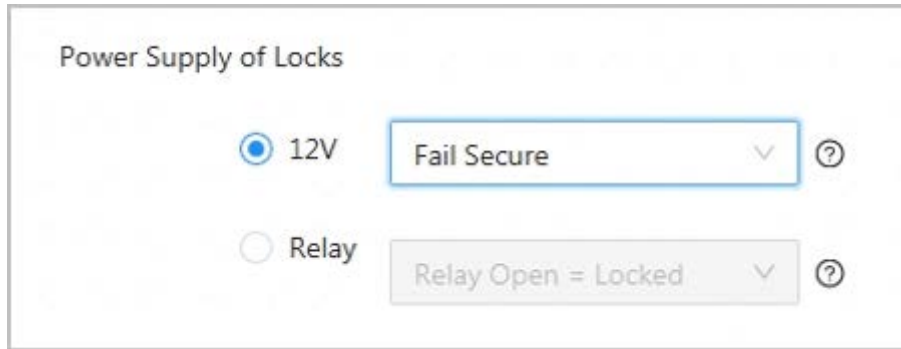
2. Select **Fail Secure** from the **12V** list for door 2.

Figure 3-17 Lock 2 (door 2)
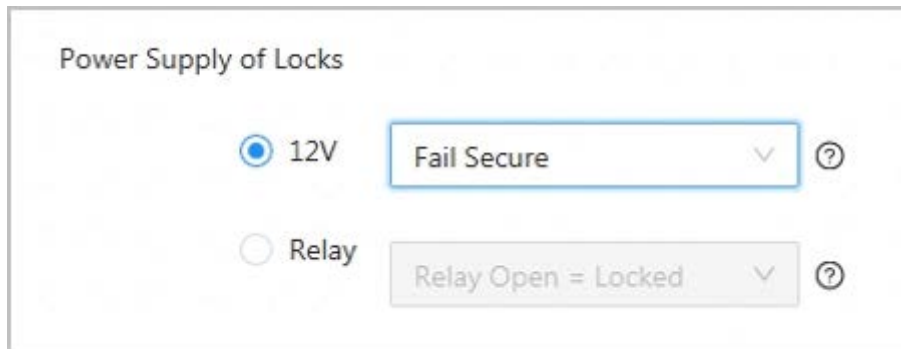
3. Wiring the locks according to the diagram below.

Figure 3-18 Wiring of locks
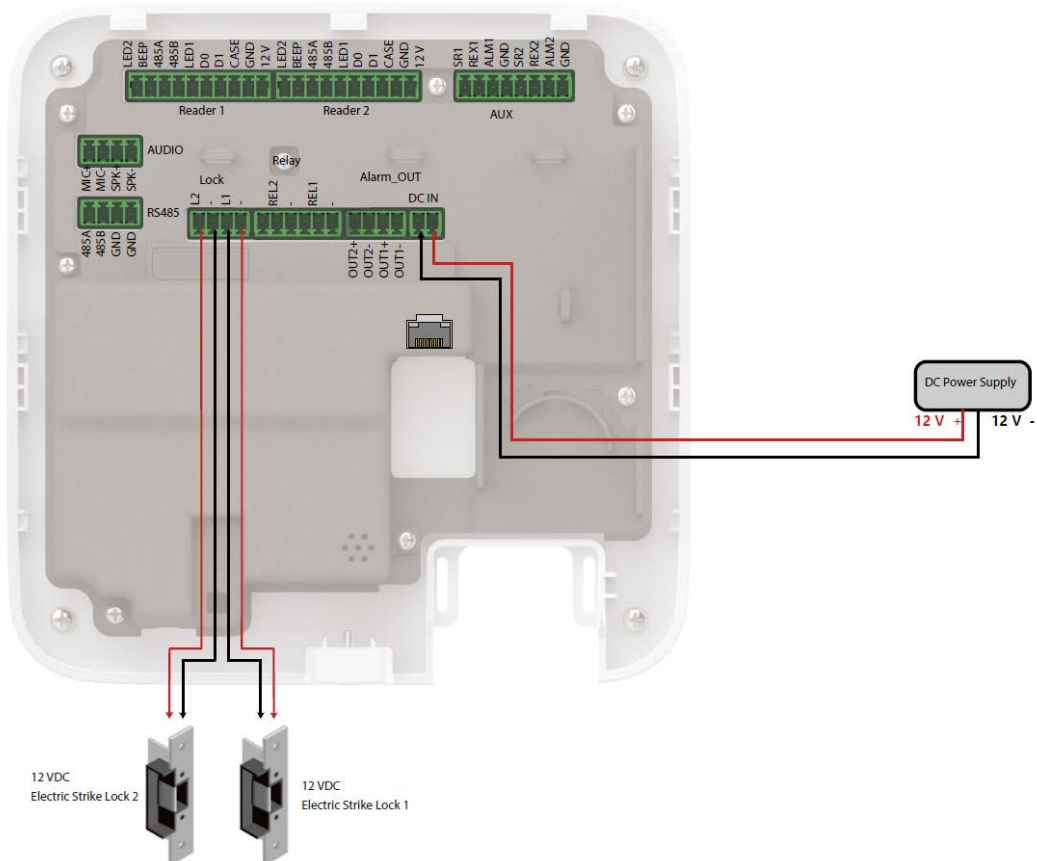
4 Installation

4.1 Wall Mount

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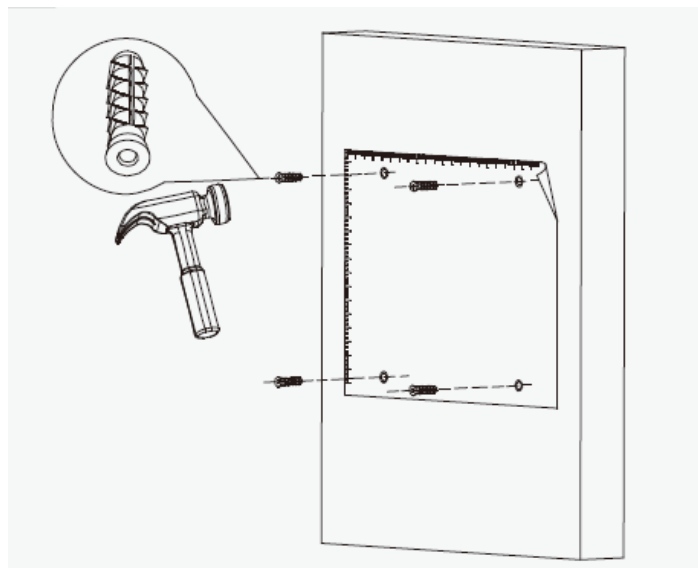
Step 4   Slide up the front panel of the Access Controller and remove the panel.

Figure 4-2 Remove the front panel
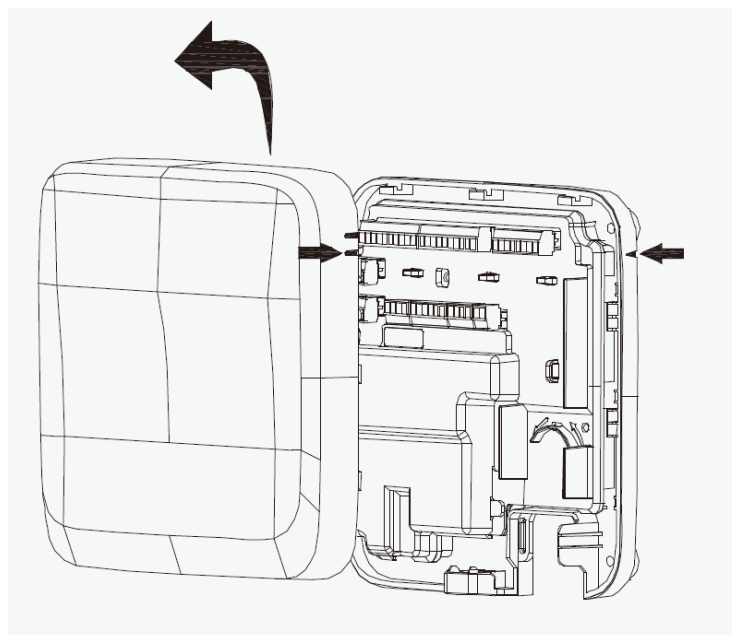
Step 5   Attach the back panel of the Access Controller to the wall with self-tapping screws.

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
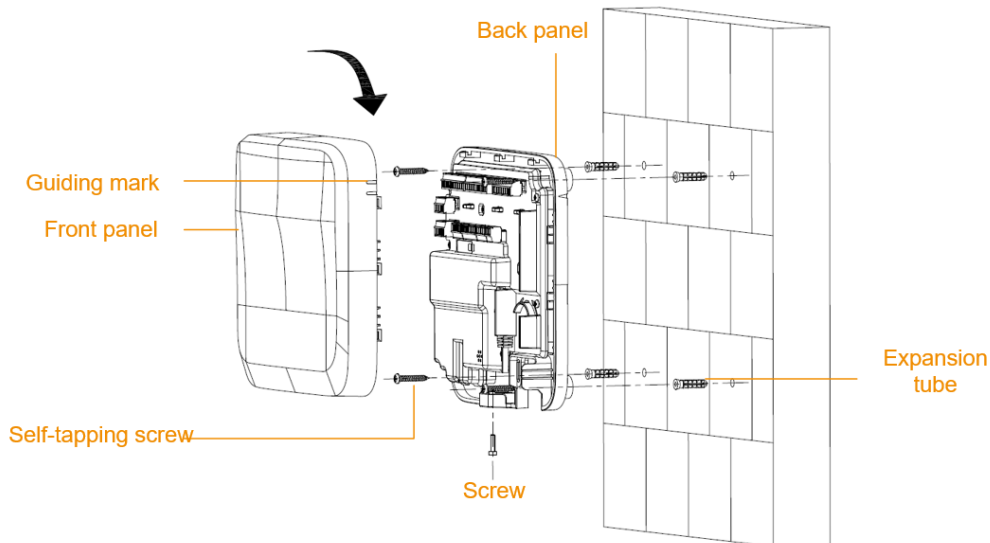
Step 9   Remove the protection film.

4.2 DIN Rail Mount

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
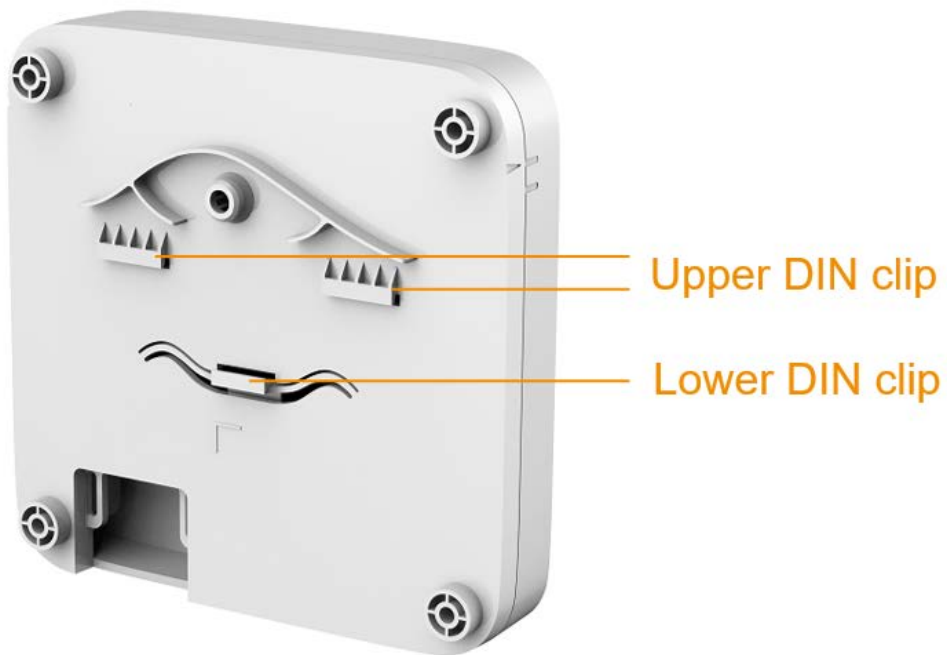
Figure 4-5 Hook DIN clips to the rail
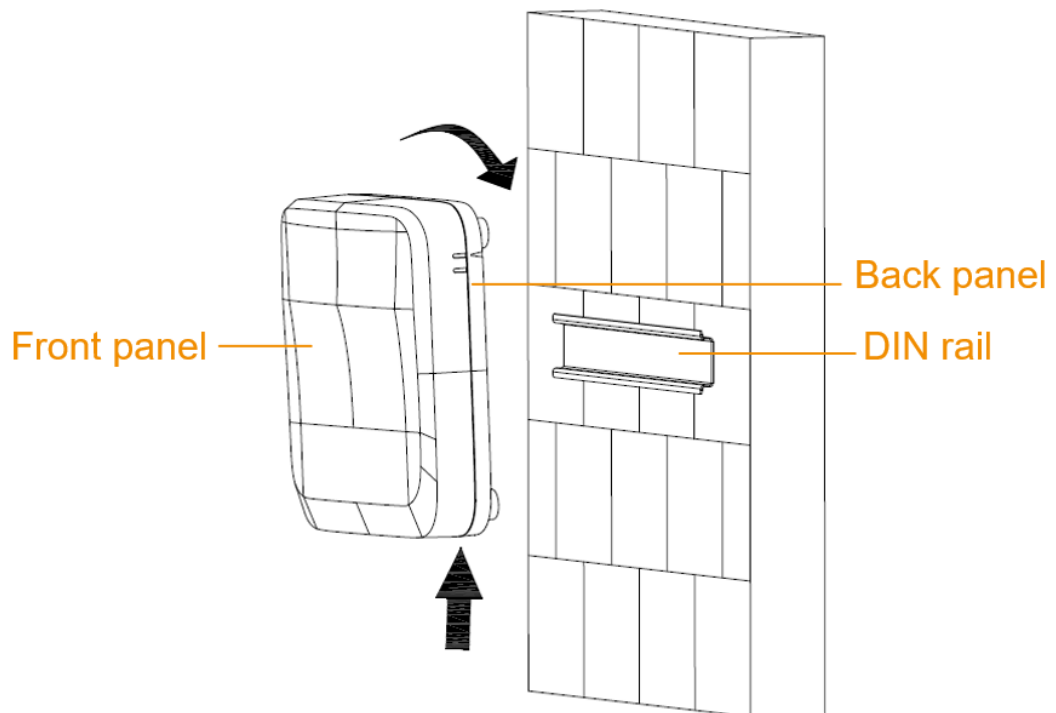
Step 3   Slide up the front panel of the Access Controller to remove the cover.

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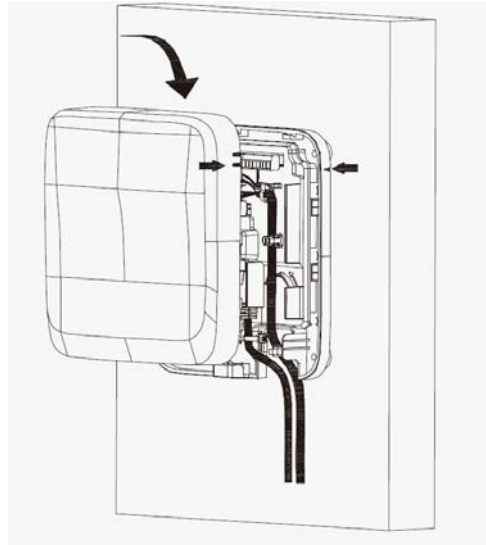
Step 6   Screw a screw into the bottom of the Access Controller to secure it.

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
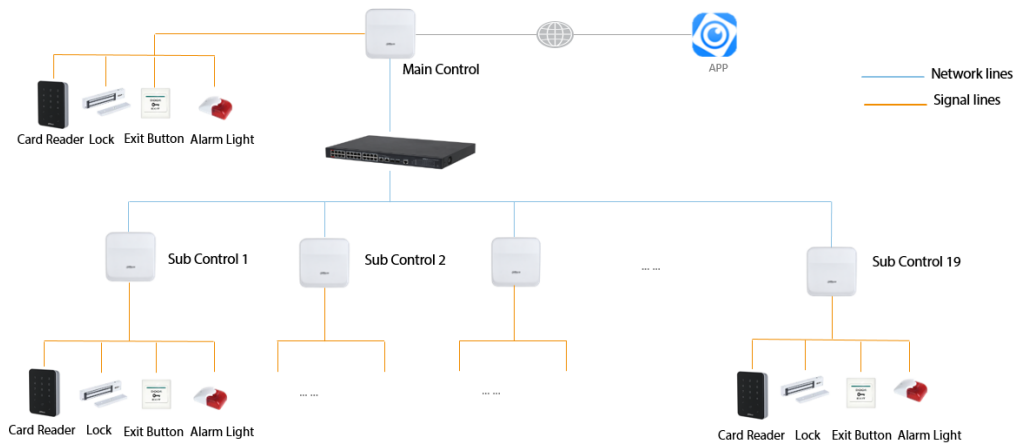
5.2 Configurations of Main Controller

5.2.1 Configuration Flowchart

Figure 5-2 Configuration flowchart
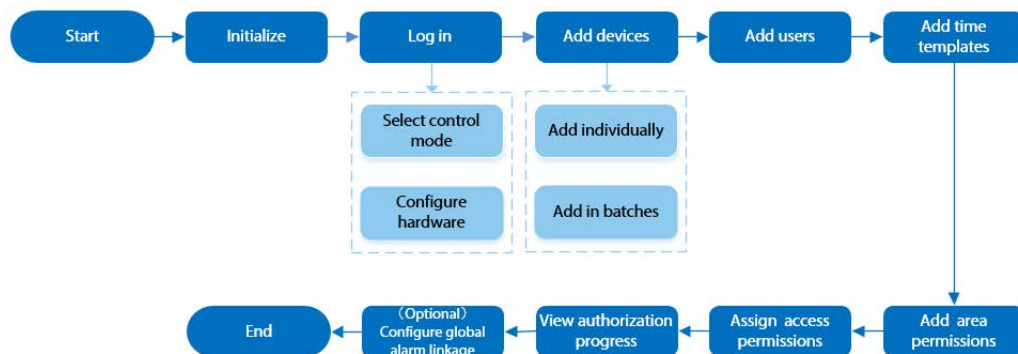
5.2.2 Initialization

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

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 initialization, you need to follow the login wizard to configure the type of the main controller and its hardware.

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 security of the platform.
- If you forget the administrator login password, you can click **Forget password?**.

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

Figure 5-4 Type of access controller
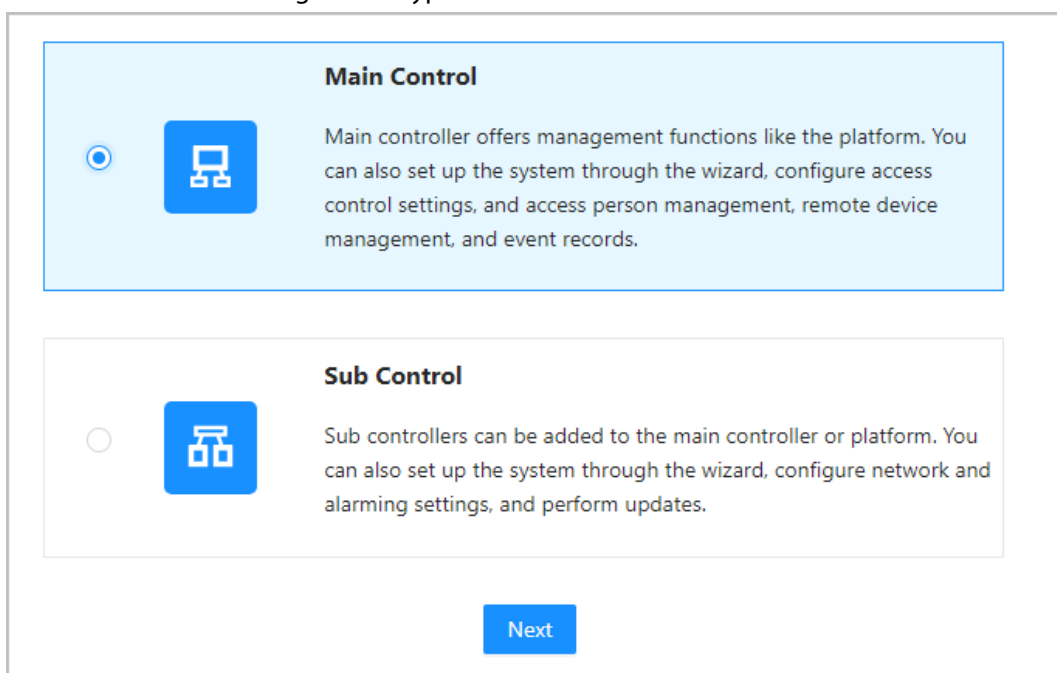
- Main Control: The main controller comes with a management platform. You can manage all sub-controllers, configure access control, access personal management on the platform, and more.
- Sub Control: Sub controllers needs to be added to the management platform of the main controller or other management platforms such as DSS Pro or SmartPSS Lite. You can only perform the local configurations on the webpage of the sub-controller. For details, see "5.3 Configurations of 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

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 an OSDP reader.
Exit Button	Connects to a exit button.
Door Detector	Connects to a door detector.
Power Supply of Locks	● 12 V: The controller provides power for the lock. ◇ Fail secure: When the power is interrupted or fails, the door stays locked. ◇ Fail safe: When the power be 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.

<u>Step 5</u>   Configure access control parameters.

<u>Step 6</u>   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 unlock through card, fingerprint, and password.

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

Figure 5-6 Element (multiple choice)

Unlock Settings

Combination Method	⦿ Or ◯ And
Unlock Method (Multi-select)	☑ Card ☑ Fingerprint ☑ Password
Door Unlocked Duration	3.0 s (0.2-600)
Unlock Timeout	60 s (1-9999)

Table 5-2 Unlock settings description

Parameter	Description
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 seconds.
Unlock Timeout	A timeout alarm is triggered when the door remains unlocked for longer than the defined value.

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

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 door detector is enabled, an intrusion alarm will be triggered if the door is opened abnormally.
Unlock Timeout Alarm	• A timeout alarm is 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.

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
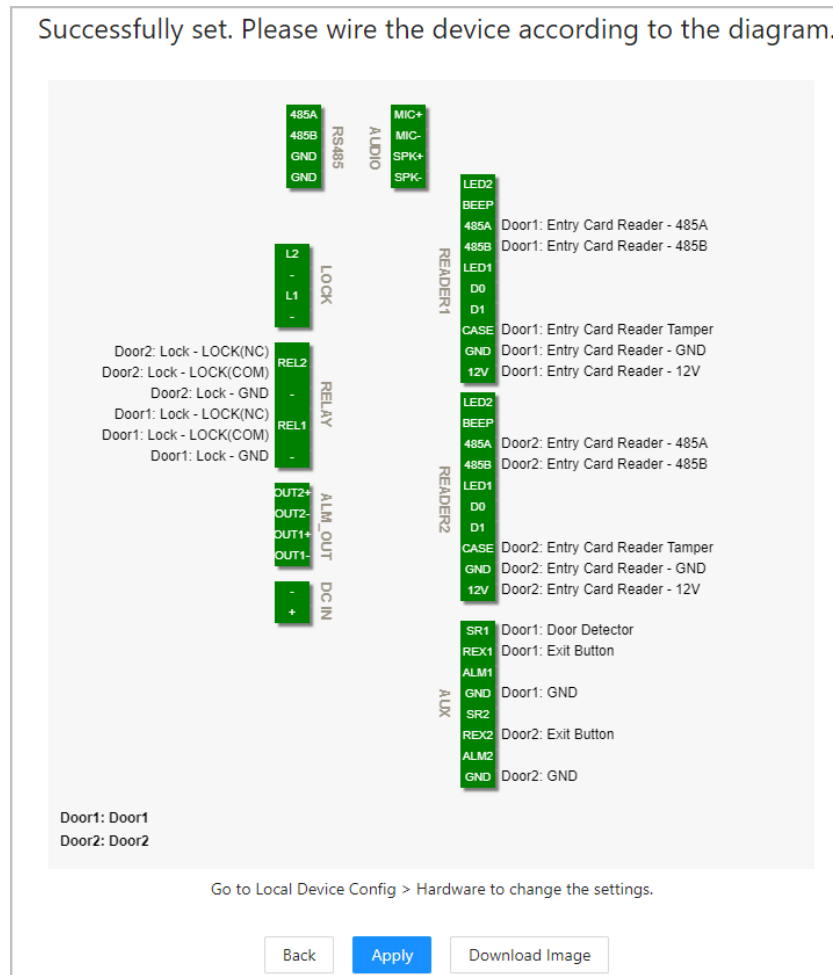
Step 10   Click **Apply**.

● 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.

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 Individually

You can add sub controllers one by one by entering their IP addresses or domain names.

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

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

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
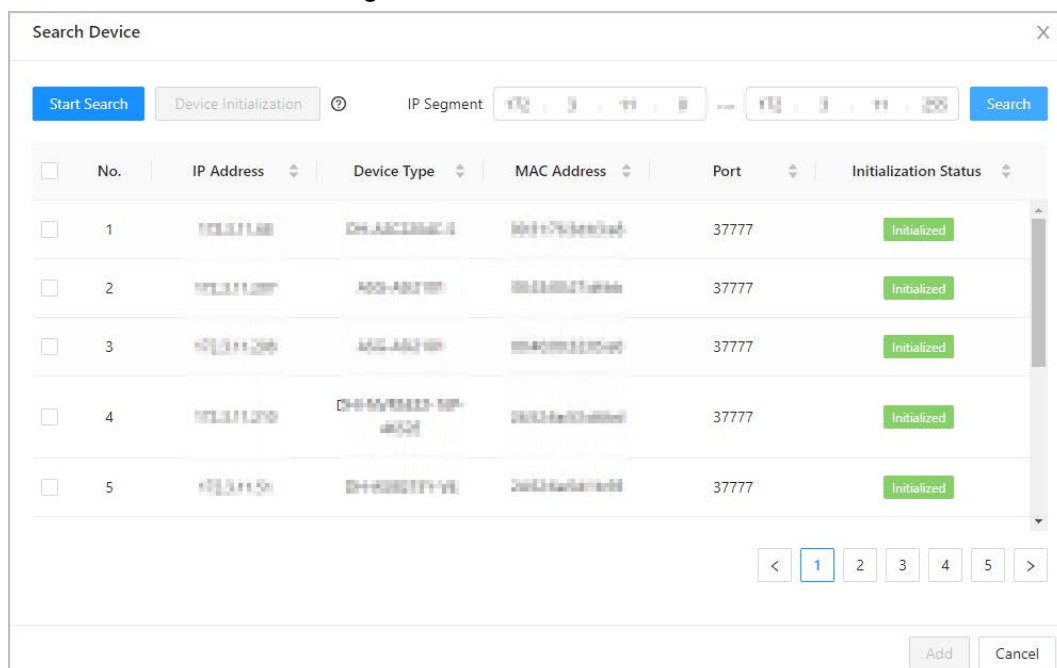
All devices that were searched for will be displayed.

📖

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.

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

Step 3   (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 assigned; otherwise, the card number cannot be read. For example, if the assigned 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 4   Add users.

● Add users one by one.

📖

When you want to assign access permissions to one person, you can add users individually. 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

Table 5-5 parameters description

Parameter	Description
User ID	The ID of the user.
Department	The department that the user belongs to.
Validity Period	Set a date on which the access permissions of the person will become effective.
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 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 5   Click the **Authentication** tab, set the authentication method to verify the identity of people.

Each user can have 1 password, 5 cards, and 3 fingerprints.

Table 5-6 Set authentication methods

Authentication Methods	Description
Password	Enter and confirm the password.
Card	- 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 ⚙. 2. Select **Enrollment Reader**, and click **OK**. Make sure that the card enrollment reader is connected to your computer. 3. Click **Add**, and follow the on-screen instructions to download and install the plug-in. 4. Swipe the card on the enrollment reader. A 20-second countdown is displayed to remind you to swipe the card, and the system will read the card number automatically. If the 20-second countdown expires, click **Read Card** to start a new countdown. 5. Click **Add**. - Read the number automatically through a card reader. 1. Click ⚙. 2. Select **Device**, select the card reader, and click **OK**. Make sure the card reader is connected to the access controller. 3. Swipe the card on the card reader. A 20-second countdown is displayed to remind you to swipe the card, and the system will read the card number automatically. .If the 20-second countdown expires, click **Read Card** to start a new countdown. 4. Click **Add**.
Fingerprint	Connect a fingerprint scanner to the computer, and follow the on-screen instructions to register the fingerprint.

Figure 5-14 Authentication method

Table 5-7 Authentication method

Parameter	Description
Password	Users can gain access by entering the password.
Card	Users can gain access by swiping the card. 📖 ● 🔄 : 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. ● 🗑 : Deletes the card.
Fingerprint	User can gain access through verifying the fingerprint.

Step 6   Click **OK**.

Related Operations

● On the **Person Management** page, click **Export** to export all users in the Excel format.
● On the **Person Management** page, click **More** > **Extract**, and select a device to extract all users from the sub controller to the Platform of the main controller.
● On the **Person Management** page, click **More** > **Card Type**, set the card type before you assign cards to users. For example, if the assigned card is an ID card, set the card type to ID card.
● On the **Person Management** page, click **More** > **Card No. System**, set the card system to the decimal or hexadecimal format.

5.2.6 Adding Time Templates

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

The default templates cannot be changed.

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

Step 2   Enter the name of the time template.

Figure 5-15 Create time templates
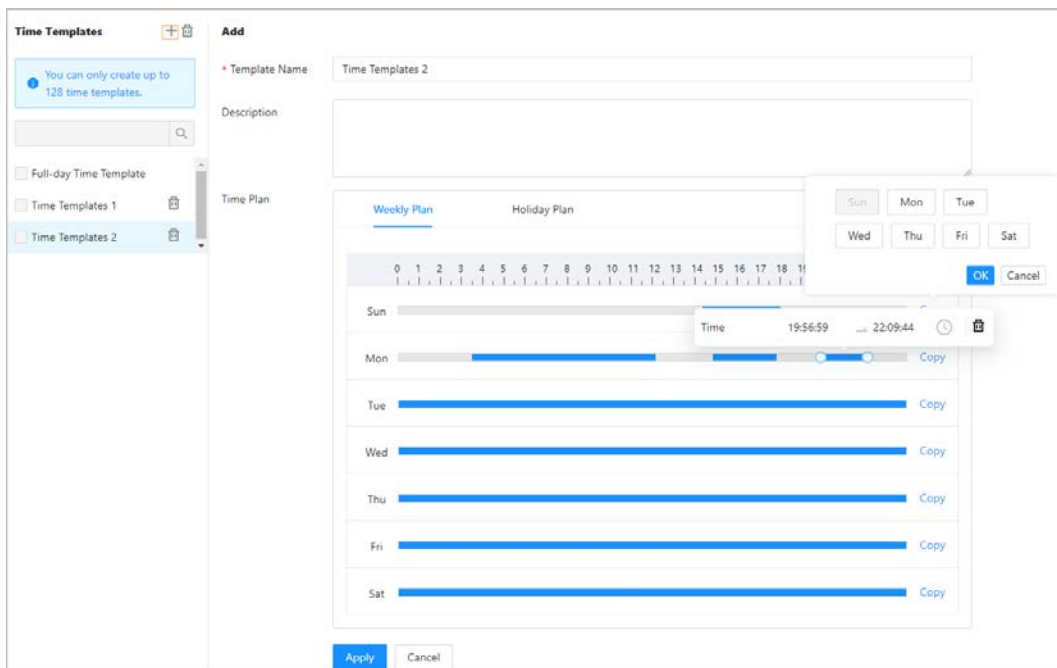
- ● The default full-day time template can be not modified.
- ● You can only create up to 128 time templates.

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 5-16 Create holiday plan
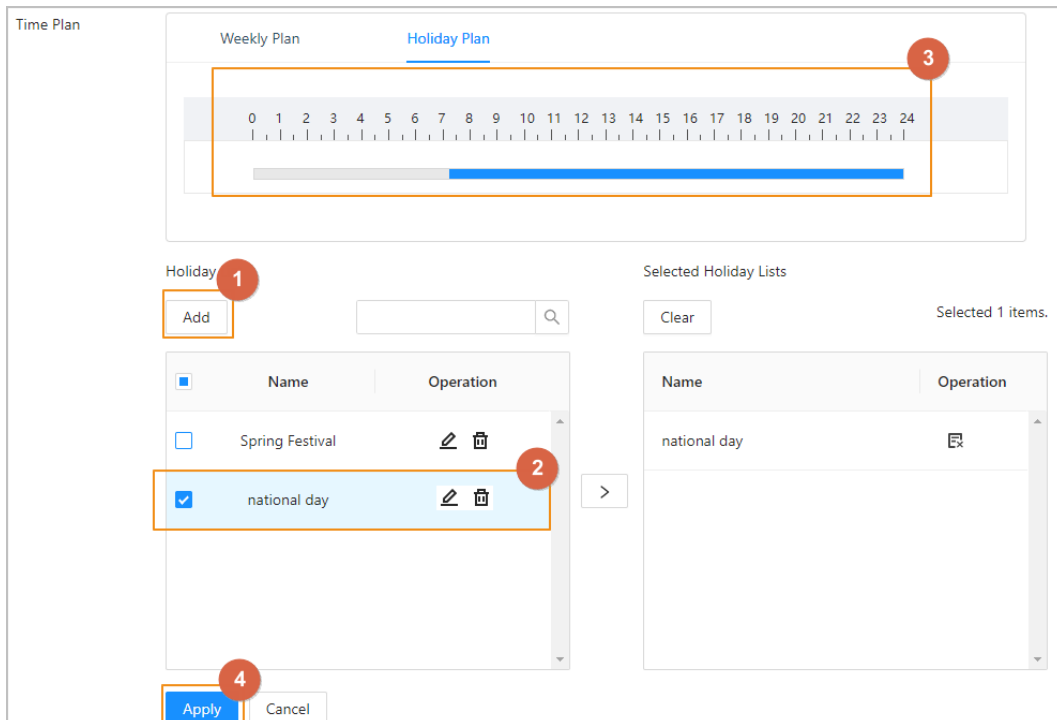
5.2.7 Adding Area Permissions

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.

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 5-17 Create area permission groups
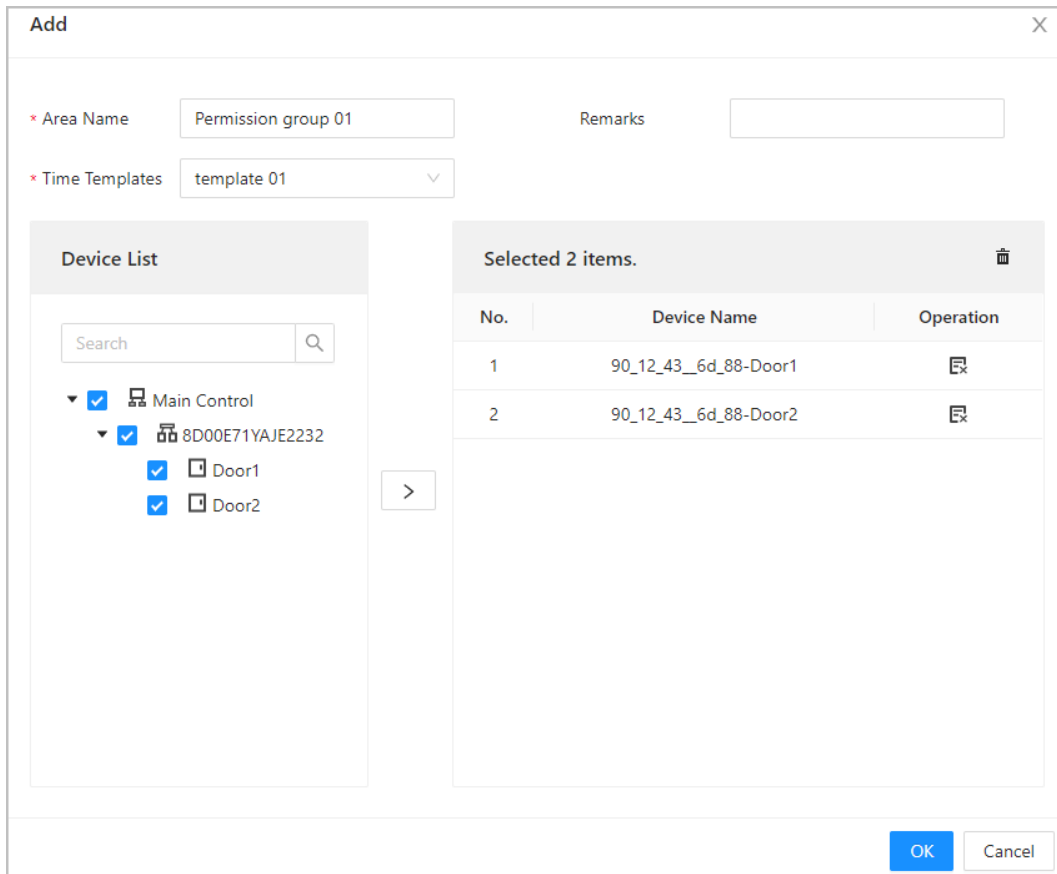
5.2.8 Assigning Access Permissions

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

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. You can select a whole department.

Figure 5-18 Select users

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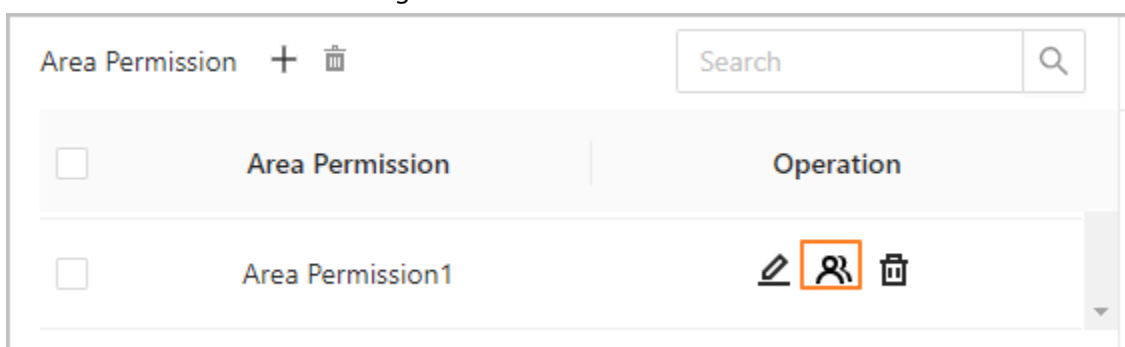
You can click ➕ to create new permission groups. For details on creating permission groups, see "5.2.7 Adding Area Permissions".

Figure 5-19 Assign permissions in batches
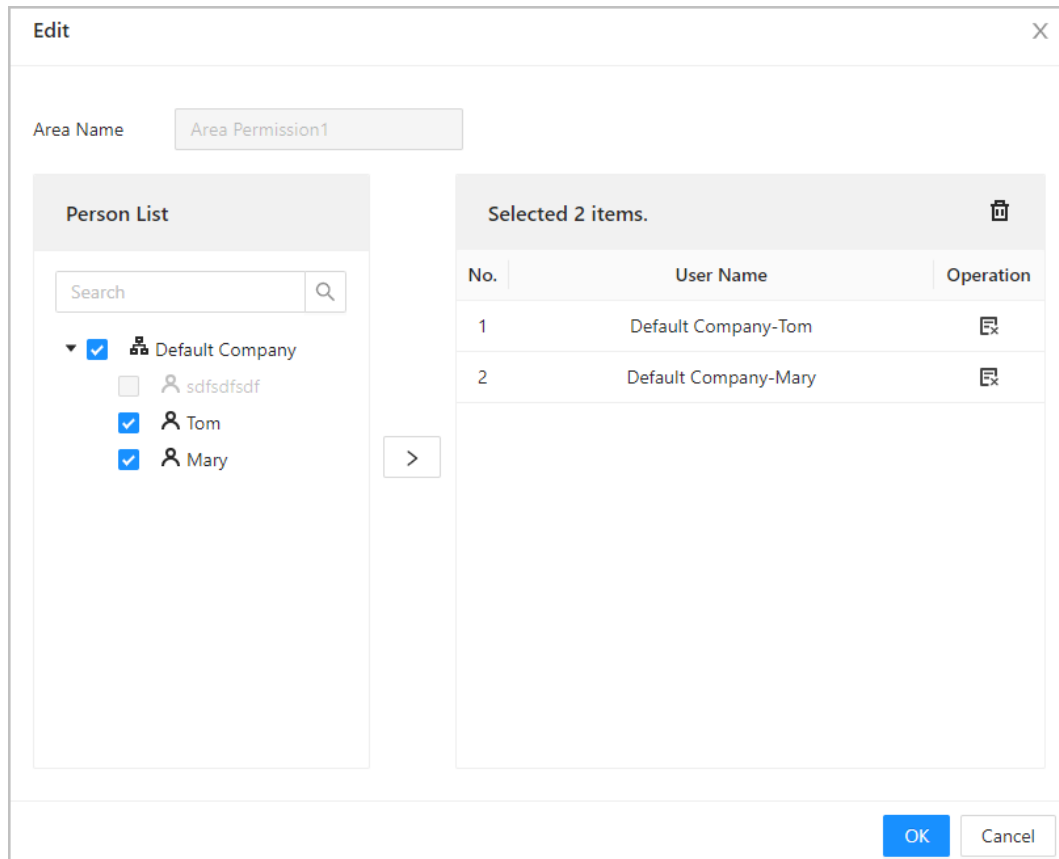
Step 3   Click **OK**.

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.

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 5-20 Authorization progress

Area Permission	Device Name	Type	Progress	Results	Time	Operation
		Sync SubControl Person		Succeed: 1, Failed: 0	2022-08-12 20:01:59	
		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.

Background Information

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.

Procedure

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

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 5-21 Alarm output
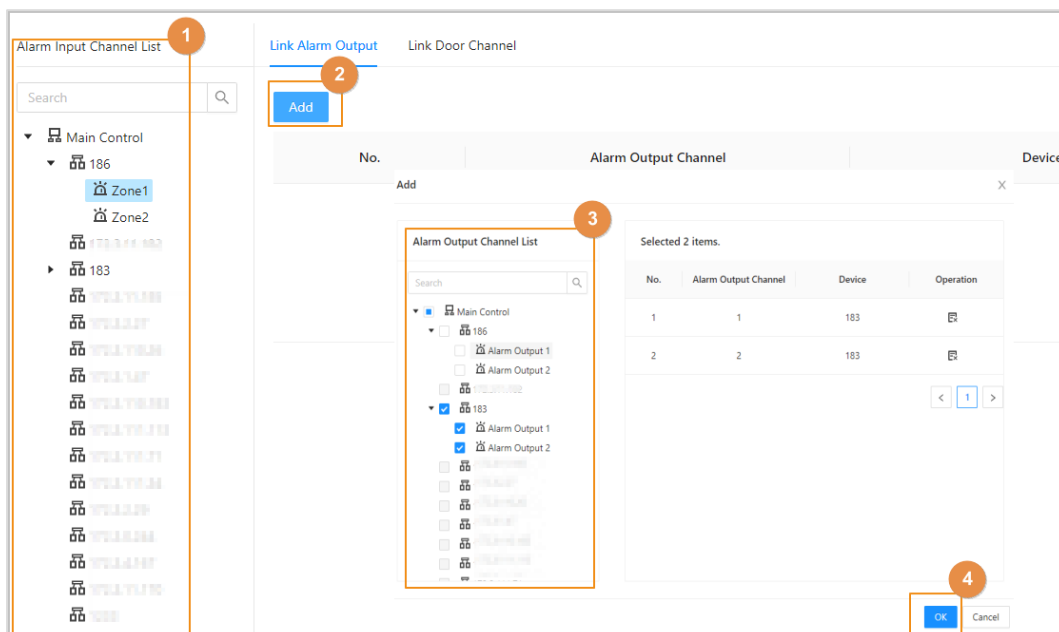
3. Turn on the alarm output function and then enter the alarm duration.

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 5-22 Door linkage

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.
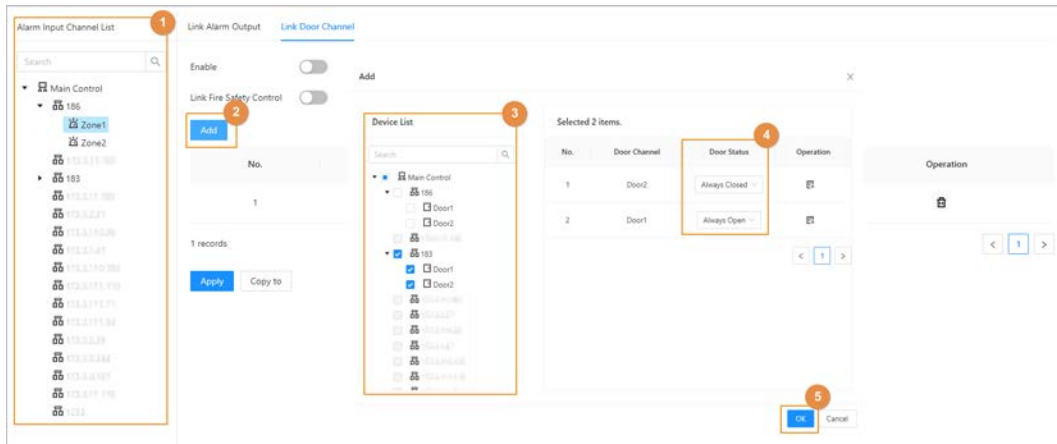
4. Click **Apply**.

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

5.3 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 equipment 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 equipment (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 equipment 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 equipment network security:

1. **Physical Protection**

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