



Web Access Controller (C-2PA)

User Manual

Foreword

General

This manual provides an overview of the functions, configuration, general operation, and system maintenance of the access controller. Please read it carefully before using the platform and store it safely for future reference.

Revision History

Revision	Content	Release Date
1	Initial Release	July 2025

Privacy Protection Notice

As a device user or data controller, you may collect personal data such as facial images, fingerprints, and license plate numbers. It's essential to comply with local privacy laws to safeguard individuals' rights. This includes providing clear identification of surveillance areas and necessary contact information.

Disclaimer

While we strive to ensure the accuracy and completeness of this document, we do not provide any formal guarantees. The use and results derived from this document are the sole responsibility of the user. We also reserve the right to modify its contents without prior notice.

About the Manual

- This manual is for reference only and may have minor discrepancies with the actual product.
- We are not liable for damages resulting from improper operation contrary to this manual.
- The manual will be updated to align with the latest laws and regulations. For more information, refer to the paper manual, scan the QR code, use our CD-ROM, or visit our official website. Minor differences may exist between electronic and paper versions.
- All designs and specifications are subject to change without notice. Product updates may lead to discrepancies between the manual and the actual product. Contact customer service for the latest information and documentation.
- There may be errors or inaccuracies in the descriptions of functions, operations, and technical data. We reserve the right of final interpretation in case of questions or disputes.
- If the manual cannot be opened, please update your reader software or try another compatible reader.
- All trademarks and company names mentioned are the properties of their respective owners.
- For assistance, visit our website or contact your supplier or customer service.
- We reserve the right of final interpretation in case of questions or disputes.

Safety Instructions

The following symbols might appear in the manual.

Symbol	Definition
	Indicates a risk hazard that, if not avoided, may result in death, injury, property damage, data loss, decreased performance, or unpredictable outcomes.

Symbol	Definition
	Offers methods to help you troubleshoot issues or save time.
	Provides more context and information.

Important Safeguards and Warnings

Transportation and Storage Requirements

- Only transport and store the device under the allowed humidity and temperature conditions.

Installation Requirements

- Do not connect the power adapter to the access controller while it is powered on.
- Strictly follow local electrical safety codes and standards. Ensure the ambient voltage remains stable and meets the access controller's power requirements.
- Do not connect the access controller to multiple power sources.
- Incorrect battery usage may cause fire or explosion.
- Follow the specified electrical requirements when powering the access controller.
- The power supply must comply with IEC 60950-1 and IEC 62368-1 standards.
- The voltage must meet SELV (Safety Extra Low Voltage) requirements and must not exceed ES-1 standards.
- If the device's power does not exceed 100 W, the power supply must meet LPS standards and remain below PS2 limits.
- It is recommended to use the manufacturer-provided power adapter.
- When selecting a power adapter, refer to the access controller label for the required power specifications.
- Personnel working at heights must take all necessary precautions, including wearing helmets and safety belts.
- Keep the access controller away from direct sunlight, heat sources, moisture, dust, and soot.
- Install the access controller on a stable surface to prevent it from falling.
- Ensure the access controller is installed in a well-ventilated area and that its ventilation is not obstructed.
- Use power cords recommended for the region that meet the rated power specifications.
- The access controller is a Class I electrical device. Ensure its power supply is connected to a socket with protective grounding.

Operation Requirements

- Confirm the power supply is correct before use.
- Ground the device properly before powering it on.
- Do not unplug the power cord from the access controller while the adapter is powered on.
- Operate the access controller within its specified power input and output range.
- Use the access controller within the permitted humidity and temperature conditions.
- Prevent liquid exposure; do not allow liquid to spill on the access controller or place liquid-filled objects on it to avoid internal damage.
- Do not disassemble the access controller unless instructed by a professional.
- This product is intended for professional use only.
- The access controller is not suitable for environments where children may be present.



Table of Contents

Foreword..... I

General I

 Revision History I

Privacy Protection Notice I

Disclaimer I

About the Manual..... I

Safety Instructions I

Important Safeguards and Warnings III

 Transportation and Storage Requirements III

 Installation Requirements III

 Operation Requirements III

Introduction 1

 About the Device..... 1

 Features and Functions..... 1

 Networking Modes 1

 Wiring Magnetic Locks 1

 Wiring of Dual Magnetic Locks with PoE (12V and Relay)..... 2

 Wiring of Dual Magnetic Locks with a 12 V External Power Supply (12 V and Relay) 3

 Wiring of Dual Electric Strikes with 12 V External Power Supply 4

Main Controller – Sub Controller 6

 Main Controller Configurations..... 6

 Initialization 6

 Login..... 7

Navigating the Home Page	10
Managing Devices	10
User Management	12
Access Rules.....	22
Access Monitoring.....	38
Configuring Always Locked and Always Unlocked Settings.....	38
Reports	38
System Settings.....	39
Network Configuration.....	40
Account Management	49
Maintenance Center	51
Security.....	52
Device Certificates	54
Sub-Controller Configurations.....	57
Initialization	57
Log in to the Device	57
LumiViewer Sub-Controllers	57
Appendix: Cybersecurity Recommendations	58
Account Management.....	58
Service Configuration.....	58
Network Configuration	59
Security Auditing.....	59
Software Security.....	59
Physical Protection	59

Introduction

About the Device

The Luminys access controller is designed for flexible, convenient access control. Users can access controllers using a web browser. The intuitive management system allows networking of main and sub controllers efficient and easy.

Features and Functions

- Made from flame-retardant PC and ABS, it is durable, stylish, and rated IK06.
- Supports TCP/IP connection and standard PoE.
- Connects to card readers via Wiegand and RS-485 protocols.
- Provides 12 VDC power output for locks, with a maximum output current of 1000 mA.
- Supports up to 1,000 users, 5,000 cards, 5,000 Bluetooth cards, 3,000 fingerprints, and 300,000 records.
- Offers multiple unlock methods, including card, password, and fingerprint, with customizable combinations.
- Supports various alarm events such as duress, tampering, intrusion, unlock timeout, and unauthorized card use.
- Accommodates different user types, including general, manager, VIP, guest, and blocklisted users.
- Supports both manual and automatic time synchronization.
- Retains stored data even when powered off.
- Offers extensive functionality, configurable system settings, and remote updates via a webpage.
- Provides main and sub-control modes. The main mode manages users, access control devices, and configurations, while sub-control devices can integrate with multiple platforms.
- A main controller can manage up to 14 sub-controllers.
- A watchdog feature enhances system stability and performance.
- Sub-controllers are compatible with LumiViewer

Networking Modes

The controller can be set as the main access controller (herein referred to as “main controller” or “Main Controller”) or the sub controller (herein referred to as the “sub controller” or “Sub Controller”).

There are two networking modes available to choose from based on your needs.

Method	Description
Main Controller—Sub Controller	The main controller includes a built-in management platform (herein referred to as the "platform" or “Platform”). Sub-controllers must be integrated into the main controller’s platform. Each main controller can manage up to 14 sub-controllers. ① Using additional management platforms with this networking method is not recommended.
LumiViewer—Sub Controller	Sub-controllers must be integrated into a standalone management platform, such as LumiViewer. The platform can manage up to 64 doors, assuming each sub-controller connects to two doors.

Wiring Magnetic Locks

This section provides lock wiring examples for a two-door solution. Wiring may vary based on the lock type.





- **Relay**
 - **Relay Open = Unlocked:** The lock unlocks when the relay is open.
 - **Relay Open = Locked:** The lock remains locked when the relay is open.
- **12V**
 - **Fail Secure:** The lock stays locked during power outages.
 - **Fail Safe:** The lock unlocks during power outages.

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

This lock wiring model provides power to the access controller through the same Ethernet cable. One door is powered by an external power supply, while the other receives power directly from the access controller. Follow the steps below to wire dual magnetic locks with PoE.

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

Power Supply of Locks

☐ 12V	Fail Secure	▼	?
☒ Relay	Relay Open = Unlock...	▼	?

Lock 1 (Door 1)

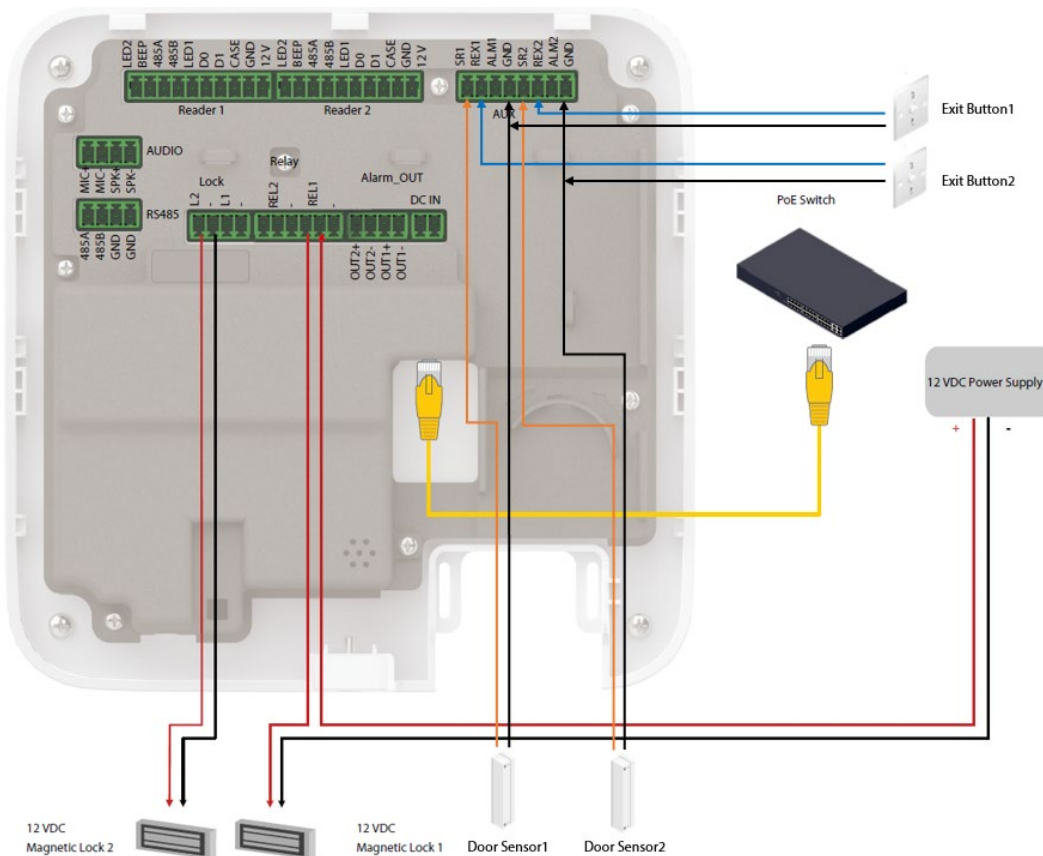
2. Choose **Fail Safe** from the 12V list for lock 2 (door 2).

Power Supply of Locks

☒ 12V	Fail Safe	▼	?
☐ Relay	Relay Open = Locked	▼	?

Lock 2 (Door 2)

3. Follow the wiring diagram below.



Wiring Diagram

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

This lock wiring model provides power to the access controller using an external 12 V power supply. One door is powered by an external power supply, while the other receives power directly from the access controller. Follow the steps below to wire dual magnetic locks with a 12 V external power supply.

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

Power Supply of Locks

☒ 12V
 Fail Secure
 ▼
?

☐ Relay
 Relay Open = Locked
 ▼
?

Lock 1 (Door 1)

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

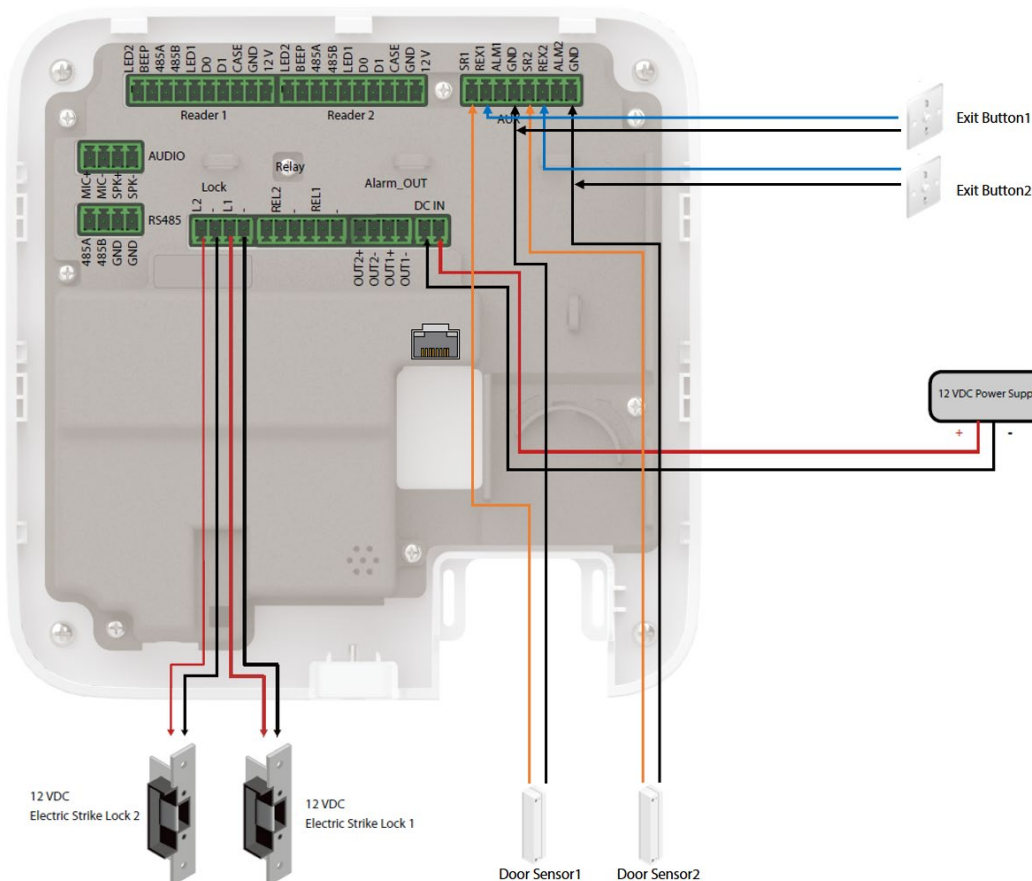
Power Supply of Locks

☒ 12V
 Fail Secure
 ▼
?

☐ Relay
 Relay Open = Locked
 ▼
?

Lock 2 (Door 2)

3. Follow the wiring diagram below.

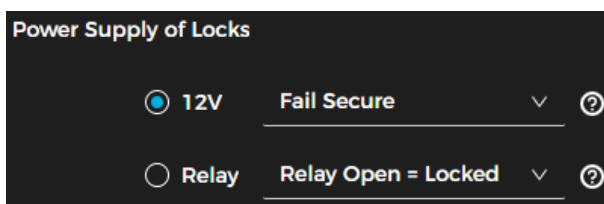


Wiring Diagram

Wiring of Dual Electric Strikes with 12 V External Power Supply

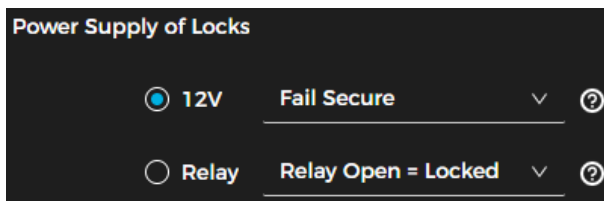
This lock wiring model provides power to the access controller using an external 12 V power supply. Both locks are powered by the access controller. Follow the steps below to wire dual electric strikes with a 12 V external power supply.

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



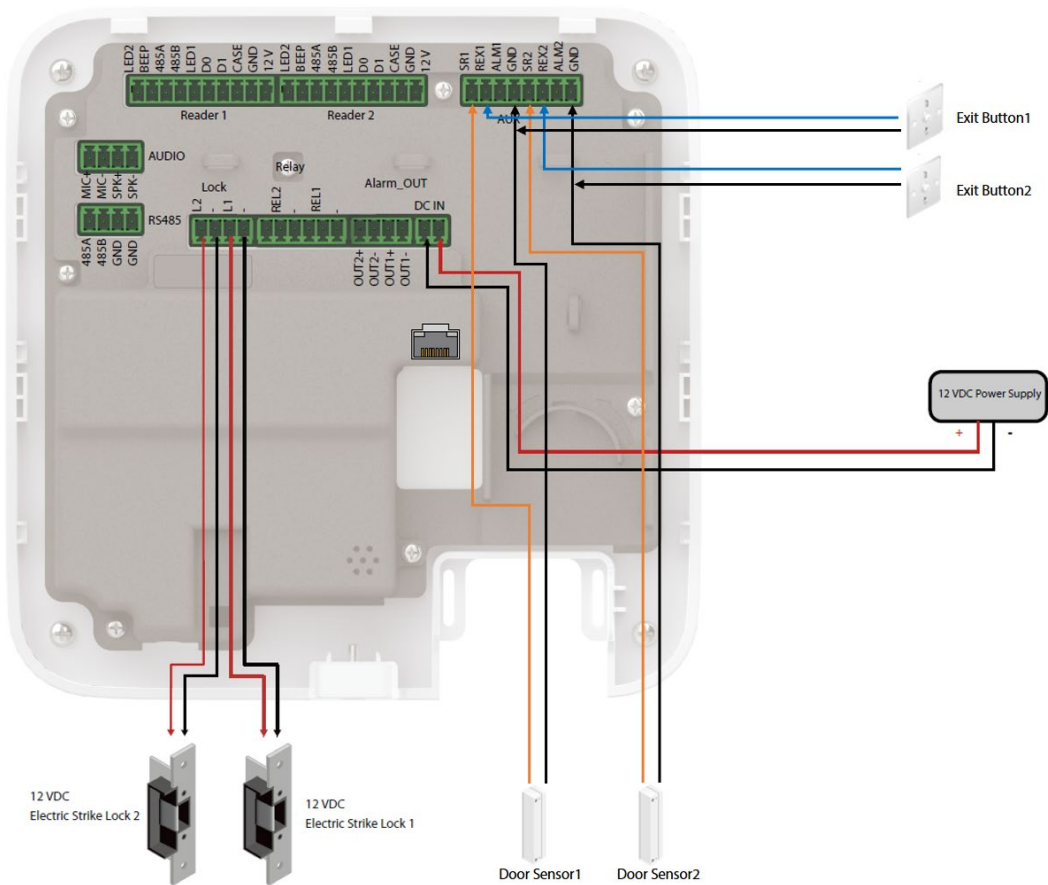
Lock 1 (Door 1)

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



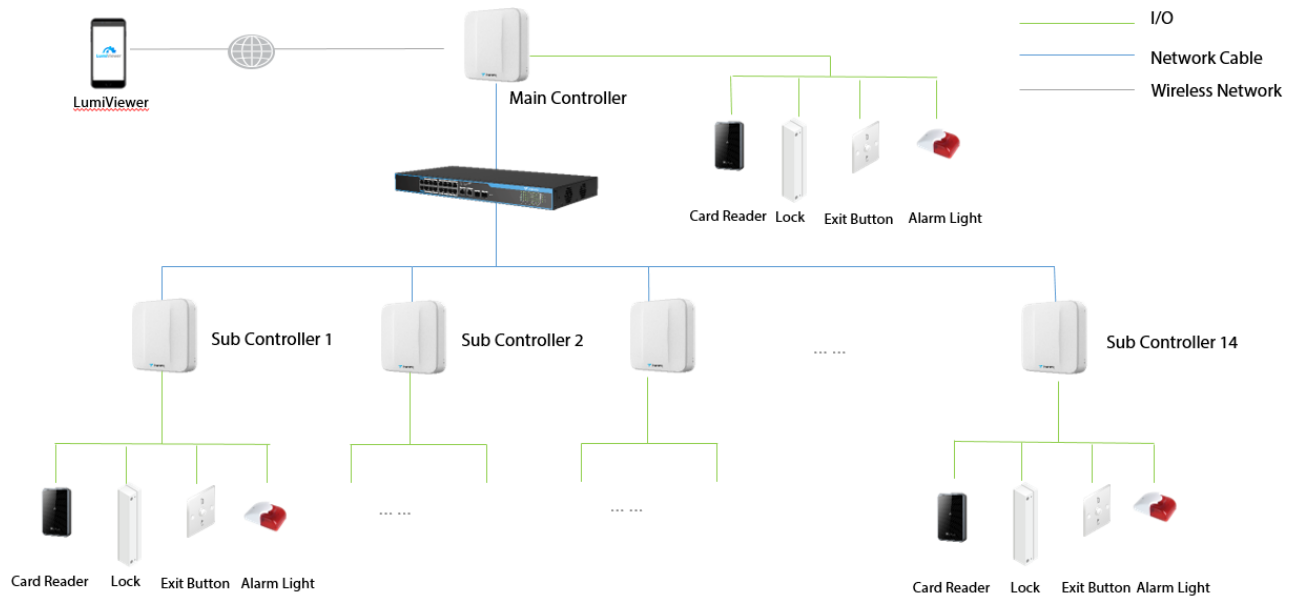
Lock 2 (Door 2)

3. Follow the wiring diagram below.



Wiring Diagram

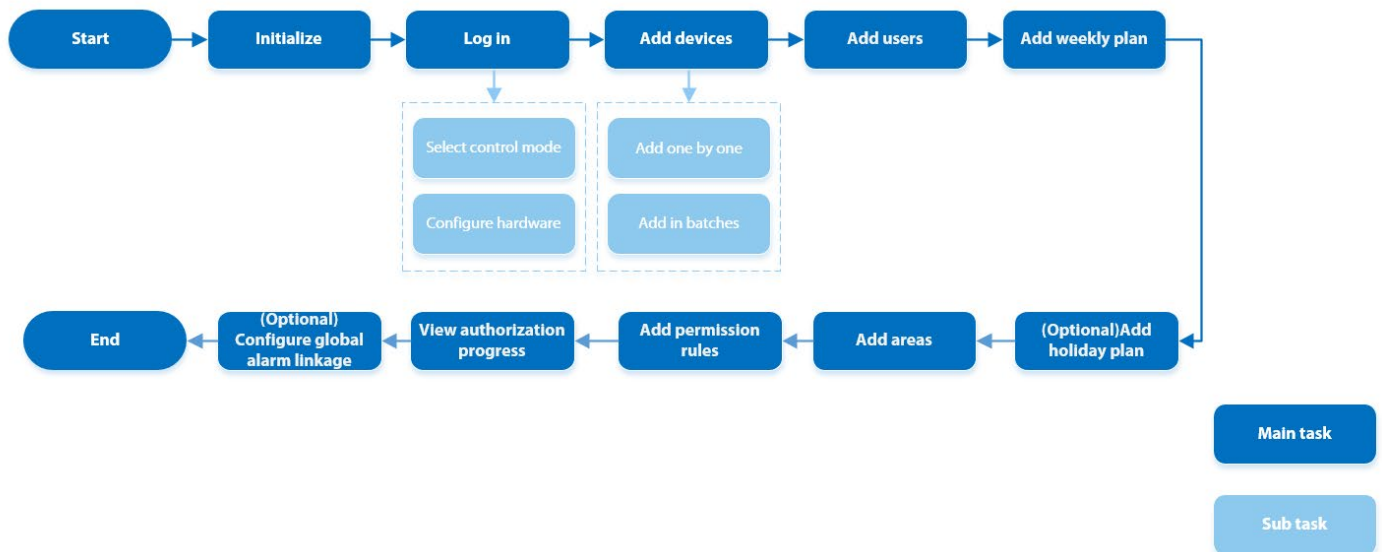
Main Controller – Sub Controller



Networking Diagram

The main controller includes a built-in management platform (herein referred to as the "platform" or "Platform"). Sub-controllers must be integrated into the main controller's platform. Each main controller can manage up to 14 sub-controllers.

Main Controller Configurations



Configuration Flowchart

Initialization

Follow the instructions to initialize the device prior to first use or after a factory reset. Prior to initialization, ensure the computer used to log in to the webpage is on the same LAN as the main controller.

1. Open your browser (Chrome or Firefox is recommended) and enter the main controller's IP address in the address bar. Hit the enter button.

① The main controller's default IP address is 192.168.1.101.

2. Choose a default language. Click .

3. Input the user password and email address. Click .

①

- The password must be 8 to 32 non-blank characters long and include at least two of the following: uppercase letters, lowercase letters, numbers, and special characters (excluding ' " ; : &). Follow the password strength prompt to set a secure password.
 - Store the password securely after initialization and update it regularly to enhance security.
4. Set the system time. Click .
5. (Optional) Select **Auto Check for Updates**. By enabling this function, the system automatically checks for available updates and notifies the user when a higher version is detected.
6. Click .

Login

After initialization, follow the steps below to use the login wizard to configure the main controller and its hardware.

1. Enter the username and password on the login page.

①

- The default administrator username is **admin**; the password is the one set during initialization. Change it regularly for better security.
 - If you forget the password, click **Forgot password?**
2. Select Main Control and click **Next**.
3. Select the number of doors, enter each door's name, then click **Next**.
4. Configure the door parameters and click **Next**.
5. Configure the parameters. See the table for more details.

Interface

Parameter	Description
Entry Card Reader	Choose the card reader protocol.
Exit Card Reader	Choose between the following options: • Wiegand: Connects to a Wiegand reader. Attach the LED wire to the controller's LED port so the reader beeps and flashes when the door unlocks • OSDP: Connects to an OSDP reader. • RS-485: Connects to an RS-485 reader.
Exit Button	Connect to an exit button. This feature is not available when Single Door is selected.
Door Sensor	Connects to a door detector.
Power Supply of Locks	Choose the power supply for the door locks. • 12 V: Controller powers the lock. There are two modes: fail secure (lock remains closed if power is lost) and fail safe (unlocks automatically if power is lost). • Relay Power: Relay powers the lock. There are two modes: relay open = locked (lock remains closed when relay is open) or relay open = unlocked (unlocks if relay is open). ① An electromagnetic lock will briefly unlock and re-lock during a soft reboot of the access controller.

6. In Unlock Settings, choose between **Or** (any one of the selected unlock methods can open the door) / **And** (all selected unlock methods must be used to open the door).

① Bluetooth card is unavailable when **And** is selected.

7. Select the unlock methods and configure the remaining parameters. See the table below for more details.

✓ Main/Sub Control

✓ Door

✓ Interface

4 Access Control Parameters

5 OK

Card Rule Settings

Facility Code

HID26

Door1 Door2

Unlock Settings

Combination Method

Or And

Unlock Method (Multi-sel...

Card Password Bluetooth Card Fingerprint

Bluetooth Mode

Short-range Mid-range Long-range

Door Unlock Duration

3.0 s (0.2-600)

Unlock Timeout

60 s (1-9999)

Alarm Settings

Duress Alarm

Door Sensor

Intrusion Alarm

Unlock Timeout Alarm

Normally Open Normally Closed

Card reader beeps

Card reader beeps

Back Next

Access Control Parameters

Parameter	Description
Unlock Method (Multi-Select)	Supports unlocking via card, fingerprint, password, or Bluetooth card. ① Bluetooth card is disabled by default.
Bluetooth Mode	The Bluetooth card must be within a specific range of the access control device to exchange data and unlock the door: Short-Range: < 0.66 ft (0.2 m) Mid-Range: < 6.56 ft (2 m) Long-Range: < 32.81 ft (10 m) ① Actual range may vary by phone model and environment.
Door Unlock Duration	After access is granted, the door stays unlocked for a specified duration between 0.2 and 600 seconds.
Unlock Timeout	A timeout alarm is triggered if the door stays unlocked beyond the set duration.

8. Set the alarm parameters in **Alarm Settings**. See the table below for more details.

Parameter	Description
Duress Alarm	Triggers an alarm when a duress card, duress password, or duress fingerprint is used to unlock the door.
Door Sensor	Choose the type of door sensor.
Intrusion Alarm	

Unlock Timeout Alarm	• If the door sensor is active, an intrusion alarm sounds when the door is forced open. • A timeout alarm activates if the door stays unlocked beyond the set duration. • If card reader beeps are enabled, the reader emits a beep when either alarm is triggered.
----------------------	---

9. Click **Next**. A wiring diagram is created from your settings. Connect the device following this diagram.

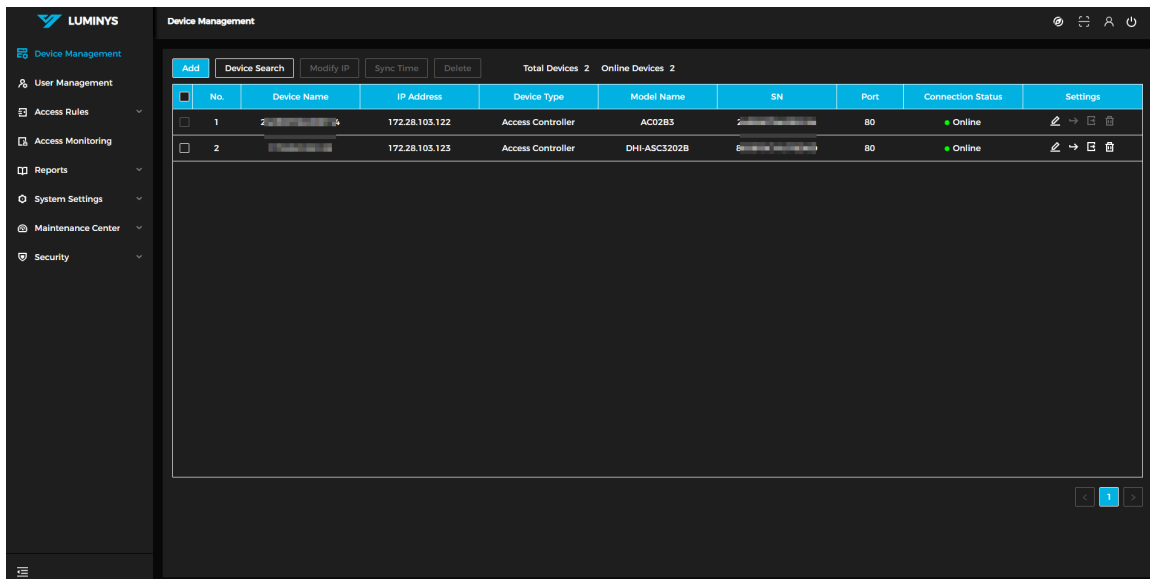
10. Click **Apply**. After logging in, go to **System Settings → Hardware Wiring** to adjust the settings. Select **Download Image** to save the diagram to your computer.

Related Operations

To modify hardware settings, navigate to **System Settings → Hardware Wiring**.

Navigating the Home Page

After logging in, the main controller's home page is displayed. See the table below for more information about the home page.



Home Page for Main Controller

Parameter	Description
Device Management	Register devices to the main controller's platform.
User Management	Add users and assign their area access rights.
Access Rules	Create time templates, set and assign area access rights, configure door settings and global alarm linkages, and monitor authorization progress.
Access Monitoring	Operate doors remotely and review event records.
Reports	Audit and download alarm and door-unlock event logs.
System Settings	Set local device parameters, including network settings and local alarm linkages.
Maintenance Center	Set up packet capture and run logs.
Security	Configure system services, attack protection, and CA certificates.

Managing Devices

You can register devices to the main controller's management platform individually or in batches. If the controller was designated as the main controller during the login wizard, you can add and manage sub-controllers through the platform.

① Only main controllers include a management platform.



Adding Devices Individually

Follow the instructions below to add sub-controllers to the main controller individually.

- 1. Navigate to **Device Management**. Click **Add**.
- 2. Enter the device information. See the table below for more details.

Add

* Device Name

Add Mode

IP

IP Address

0 . 0 . 0 . 0

* Port

80

* Username

* Password

OK

Cancel

Device Information

Parameter	Description
Device Name	Enter the access controller name. It is recommended to name the controller based on its installation location.
Add Mode	Choose IP and enter the IP address to add the access controller.
IP Address	Ente the controller’s IP address.
Port	The default port number is 80.
Username	Enter the login information of the access controller.
Password	

- 3. Click **OK**. You can view the added controllers on the Device Management page.
- ❗ If the controller was designated as the main controller during the login wizard, it will be automatically added to the management platform and operate as both main and sub controller.

Related Operations

- Click  to edit the device information.
- Click  to go to the sub-controller webpage. (Sub-Controller Only)
- Click  to log out of a device. (Sub-Controller Only)
- Click  to delete a device. (Sub-Controller Only)

Adding Devices in Batches

Follow the instructions below to add sub-controllers to the main controller in batches. When adding multiple sub-controllers, use the auto-search feature. Ensure all sub-controllers are on the same network segment.

- 1. Go to **Device Management** and click **Search Device**. Select **Start Search** to find devices on the same LAN or enter a network segment range, then click **Search**.



- All detected devices will be listed. Select the desired devices and click **Device Initialization** to batch initialize them.
 - For security, devices on different network segments cannot be initialized.
2. Select the access controllers to add to the platform, then click **Add**.
 3. Enter the sub-controller's username and password, then click **OK**. The added sub-controllers will appear on the **Device Management** page.

Related Operations

- **To modify the devices' IP addresses**, select devices and click **Modify IP**.
- **To match device time with the NTP server**, select devices and click **Sync Time**.
- **To delete devices**, select devices and click **Delete**.

User Management

You can add users to groups, enter their basic details, and set authentication methods for identity verification.

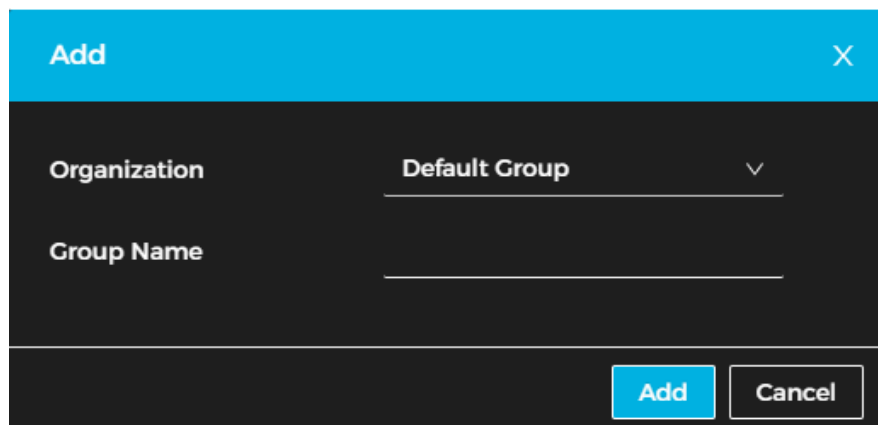
Related Operations

- **Export all users to Excel:** On the **User Management** page, click **Export** to save all user data. You can also import this data into other controllers. Regularly export user data to prevent loss from equipment damage.
- **Import users:** On the **User Management** page, click **Import** → **Download Template**, fill in the user details, then select **Import** → **Import** to upload all users.
- **Extract all users:** On the **User Management** page, click **More** → **Extract Person Info**, choose a device, and transfer all users from the sub-controller to the main controller's platform.

Add a Group

Follow the steps below to add a user group.

1. Click User Management.
2. Click .
3. Enter the group name and click **Add**.



The image shows a modal dialog box titled "Add" with a close button (X) in the top right corner. The dialog has a dark background. It contains two input fields: "Organization" with a dropdown menu showing "Default Group" and a downward arrow, and "Group Name" with a text input field. At the bottom right, there are two buttons: "Add" (highlighted in blue) and "Cancel".

Add Group

Configure Basic User Information

Follow the steps below to configure basic user information.

1. Click User Management.



2. Add users using one of the following methods. See the table below for more information.
 - Add Users Individually
 - From the left panel, select a user group, click **Add**, and enter the user's basic information.
 - Add Users via Import
 - Click **Import** → **Download Template** to get the user template.
 - Fill in the user details in the template and save it.
 - Click **Import** → **Import** and upload the template to the platform.
 - Add Users in Batches

Batch Add

* User ID

001

* Total Users

5

Group

Default Company

Effective Time

09-23-2024 12:00:00 AM → 12-31-2037 11:59:59 PM

User ID	Card Number
001	
002	
003	
004	
005	

Issue Card Config

Card Reader

Enrollment Reader

Modify

Card Number

Press the Enter key to enter.

Start Issuing Cards

Add

Cancel

Batch Add

- Click **Batch Add**.
- Enter the starting user ID and the total number of users. The platform will create a sequence of IDs beginning with the specified start number. For example, if the start ID is **001** and the total is **5**, the system will generate IDs **001** to **005**.
- Select the group and set the validity period.

- Batch issue cards to users by entering the card number manually or reading it with an enrollment or card reader.

Add

General

Authentication

* User ID ⓘ

* User Name

* Group

Default Group

▼

* User Type

General

▼

Valid from

01-21-2025 12:00:00 AM

📅

Valid to

12-31-2037 11:59:59 PM

📅

Email

* Use limit

Unlimited

Add

Add More

Cancel

User Information

Parameter	Description
User ID	Enter the user ID.
User Name	Enter the user's name.
Group	Assign the user a group.
User Type	Select the type of user from the following options: • General: Can unlock the door. • VIP: Triggers a notification to service staff upon unlocking. • Guest: Can unlock only within a set time or for a limited number of uses; access ends when limits expire. • Staff: Permissions are recognized but cannot unlock the door. • Blocklist: Triggers a notification to service staff upon unlocking. • Manager: Has full permissions, unaffected by unlock mode or door status. • Other: Keeps the door unlocked for an extra 5 seconds after access.
Valid from	Define the time period during which the person's access permissions are valid.
Valid to	
Email	Enter the user's email address. The email address must match the one used to register for LumiViewer.
Use Limit	Set the number of times a user can unlock the door.

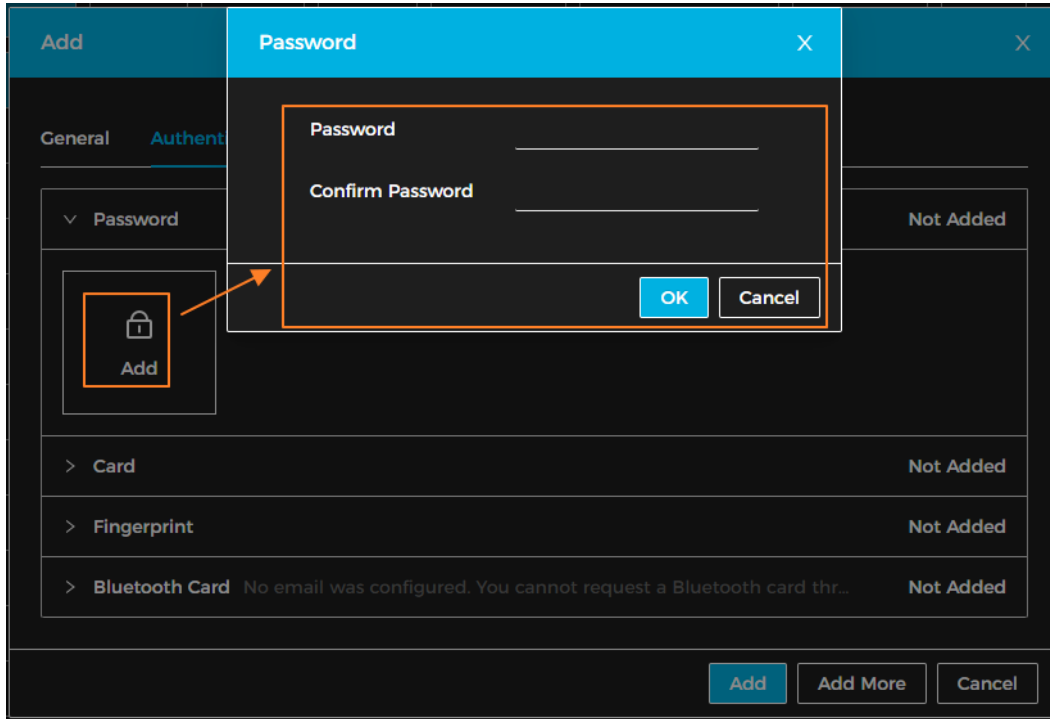
Adding a User Password

Follow the steps below to assign passwords to users so they can unlock the door by entering them. Each user can have up to one (1) password.

1. When adding a user, open the **Authentication** tab.



2. Click **Add**, then enter and confirm the password.
3. Click **OK**.



Add a User Password

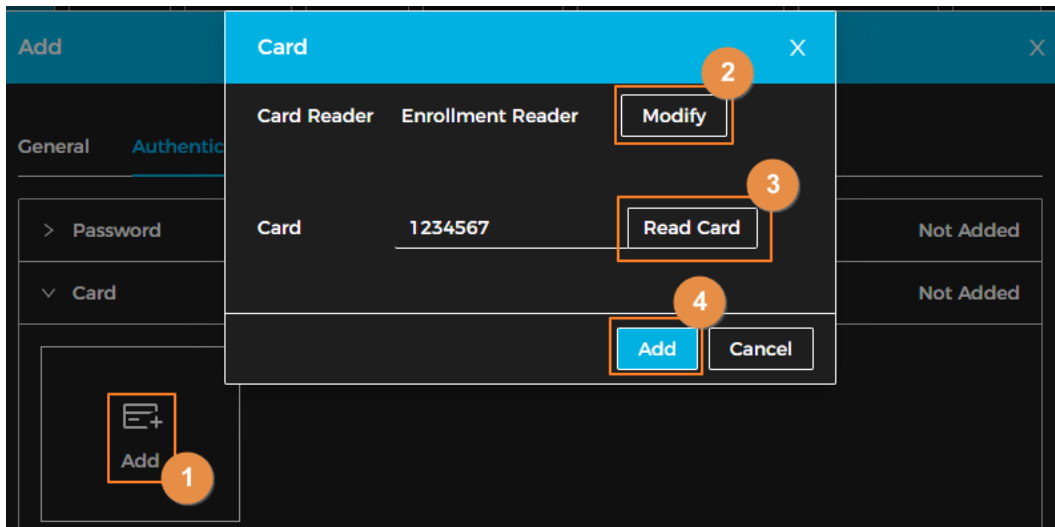


- **Pin code authentication disabled:** Unlock by entering `UserID#Password#`.
Example: For User ID **123** and password **12345**, enter `123#12345#`.
- **Pin code authentication enabled:** Unlock by entering `Password#`.
Example: For password **12345**, enter `12345#`.

Adding an IC or ID Card

Follow the steps below to assign passwords to users so they can unlock the door by using a card. Each user can have up to five (5) IC/ID cards.

1. (Optional) Before assigning cards to users, configure the card type and card number format.
 - On the User Management page, select **More → Card Type**.
 - If issuing cards with an enrollment reader, choose the card type and click **OK**. Ensure the selected card type matches the type used when issuing via the enrollment reader.
 - Select **More → Card No. System**.
 - Choose **Decimal** or **Hexadecimal** format for the card number.
2. When adding a user, open the **Authentication** tab and click **Card** to add cards using one of the following methods:
 - Manually
 - Click **Add** and enter card number. Click **Add** when done.
 - Using an Enrollment Reader/Card Reader



Enrollment Reader

- Click **Add**.
- Click **Modify**, then select **Enrollment Reader** or your card reader. Ensure the enrollment reader is connected to your computer.
- Follow the prompts to download and install the plug-in.
- Click **Read Card**, then swipe the card on the enrollment reader. A 60-second timer appears for swiping. The system reads the card number automatically. If the timer expires, click Read Card to restart.
- Click **Add**.
- Add in Batches

Batch Issue Cards

Card
Bluetooth Card

Issue Cards

User ID	User Name	Card Number	Hide User
105	105	The number of cards f...	⊖
106	106	The number of cards f...	⊖

User ID

User Name

User Type

Email

Group

Effective Time

Issue Card Config

Card Reader

Enrollment Reader

Modify

Card Number

Press the Enter key to enter.

Start Issuing Cards

OK

Cancel

Batch Issue Cards

- On the **User Management** page, click **Batch Issue Cards**, then choose **Issue Cards to Selected Users** or **Issue Cards to All Users**.
- Enter the card number manually, or click **Modify** to issue cards using an enrollment reader or card reader.

Adding Fingerprints

Follow the steps below to assign passwords to users so they can unlock the door by using their fingerprint. Each user can have up to three (3) fingerprints associated with their ID.

- When adding a user, open the **Authentication** tab and click **Fingerprint**.
- Connect a fingerprint scanner to the computer and follow the prompts to register the fingerprint.
- Click **Add**.

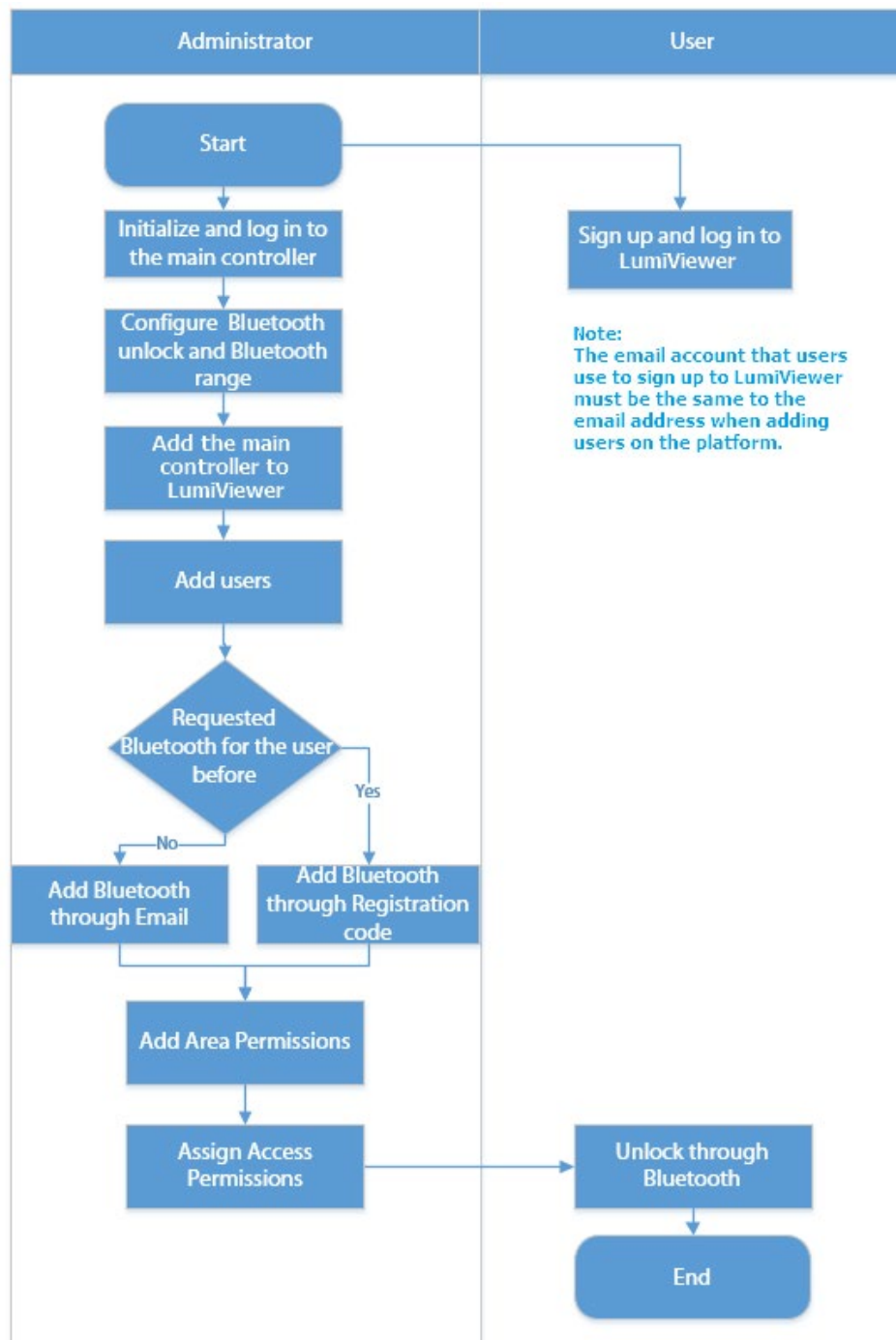
Adding Bluetooth Cards

Follow the steps below to assign passwords to users so they can unlock the door by using their fingerprint. Each user can have up to five (5) Bluetooth cards.

Prior to adding Bluetooth cards, ensure the following conditions are met:

- Bluetooth unlock is enabled.
- The main controller is added to LumiViewer.
- Users are registered on the access controller's platform.
- General users, such as employees, have installed LumiViewer and signed up with their email.
- The LumiViewer registration email must match the email used to add them to the access controller.

See the Bluetooth unlock flowchart below. Administrators and general users follow different steps. General users, such as employees, only need to register and log in to LumiViewer with their email to unlock doors using their issued Bluetooth cards.



Bluetooth Unlock Flowchart

In the **Authentication** tab, click **Bluetooth Card**. Choose one of the following methods to add Bluetooth cards:

- **Add Individually:** Click **Request through Email**. A Bluetooth card is generated automatically. Each user can have up to 5 cards.
 - **Add in Batches:** On the User Management page, click Batch Issue Cards. Click Issue Cards to All Users or select specific users and click Issue Cards to Selected Users. Click Bluetooth Card. Click Request through Email.
- ❗
- Users without an email or with 5 existing Bluetooth cards appear in the non-requestable list.
 - **To update missing emails,** click **Export Users that Lack Emails**, add emails in the correct format, then click **Import**. These users will be moved to the requestable list.

Batch Issue Cards

Card
Bluetooth Card

❗ Bluetooth cards can only be generated in batches through emails.

Issue Cards

Requestable (992)
Non-Requestable (0)
Export Users that Lack Emails
Import

User ID	User Name	Email	Bluetooth Card No.	Status	Settings
6	6	1...@...c...	0		⊖
7	7	1...@...c...	0		⊖
8	8	1...@...c...	0		⊖
9	9	1...@...c...	0		⊖
10	10	1...@...c...	0		⊖
11	11	1...@...c...	0		⊖

User ID
1

User Name
123...

User Type
General

Email
...@...com

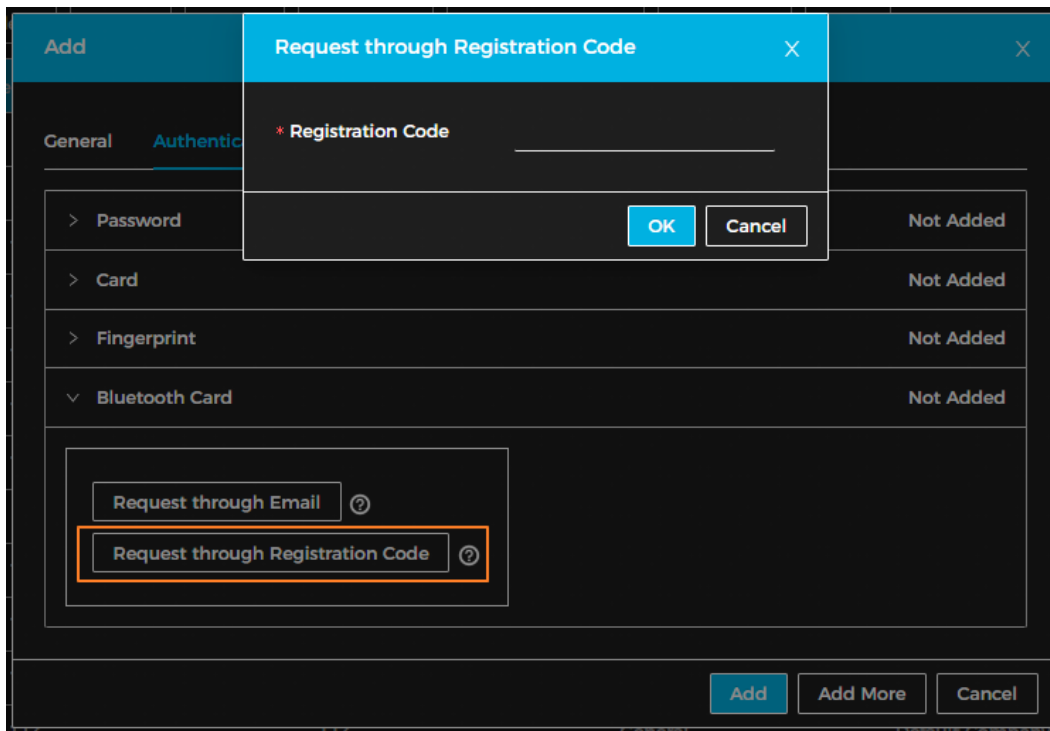
Group
BBB

Effective Time
2024-06-29 00:00:00-2037-12-31 23:59:59

Request through Email

Batch Issue Bluetooth Cards

- **Add Using Registration Code:** If you have requested Bluetooth cards for the user before, you can add the Bluetooth cards through registration code.
- In LumiViewer, tap Registration Code for a Bluetooth card.
- Copy the registration code.
- In the Bluetooth Card tab, click Request through Registration Code, paste the code, and click OK.



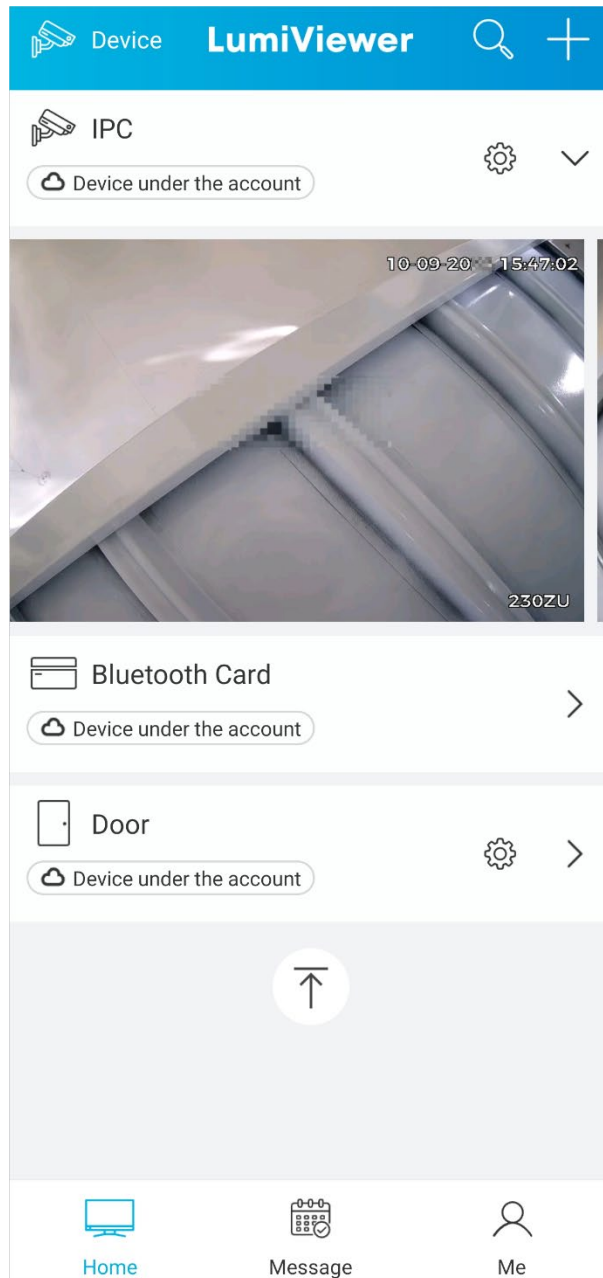
Add Using Registration Code

After signing up and logging in to LumiViewer with their email, users can use Bluetooth cards in LumiViewer to unlock doors. For more details, see the LumiViewer user manual.

- **Automatic Unlock:** The door unlocks automatically when you enter the defined Bluetooth range, allowing the card to communicate with the reader.

① In this mode, the card may repeatedly unlock the door if you remain in range for an extended time until a failure occurs. Turn Bluetooth off and back on to reset.

- **Shake to Unlock:** Shaking the phone triggers the Bluetooth card to send signals to the reader, unlocking the door.



Shake to Unlock

Related Operations

- To manage Bluetooth cards in LumiViewer:
- **Move to the Top:** Prioritize active cards when multiple Bluetooth cards are added.
- **Rename:** Change the Bluetooth card name.
- **Delete:** Remove the Bluetooth card.
- **To export users without emails:** Click **Export**, add emails in the correct format, then click **Import**. These users will be moved to the requestable list.
- **To view request records:** On the User Management page, select More > Bluetooth Card Records to check request status.
- **View Details:** See request details, including user info and reasons for failures; you can also re-request for failed users.
- **Request Again:** Retry requests for failed users.

Access Rules

This section goes over access rules such as schedules and zones.

Adding Weekly Schedules

Follow the steps below to add weekly schedules. The weekly schedule defines door unlock times for the week. The platform provides a default full-day template, or you can create custom templates.

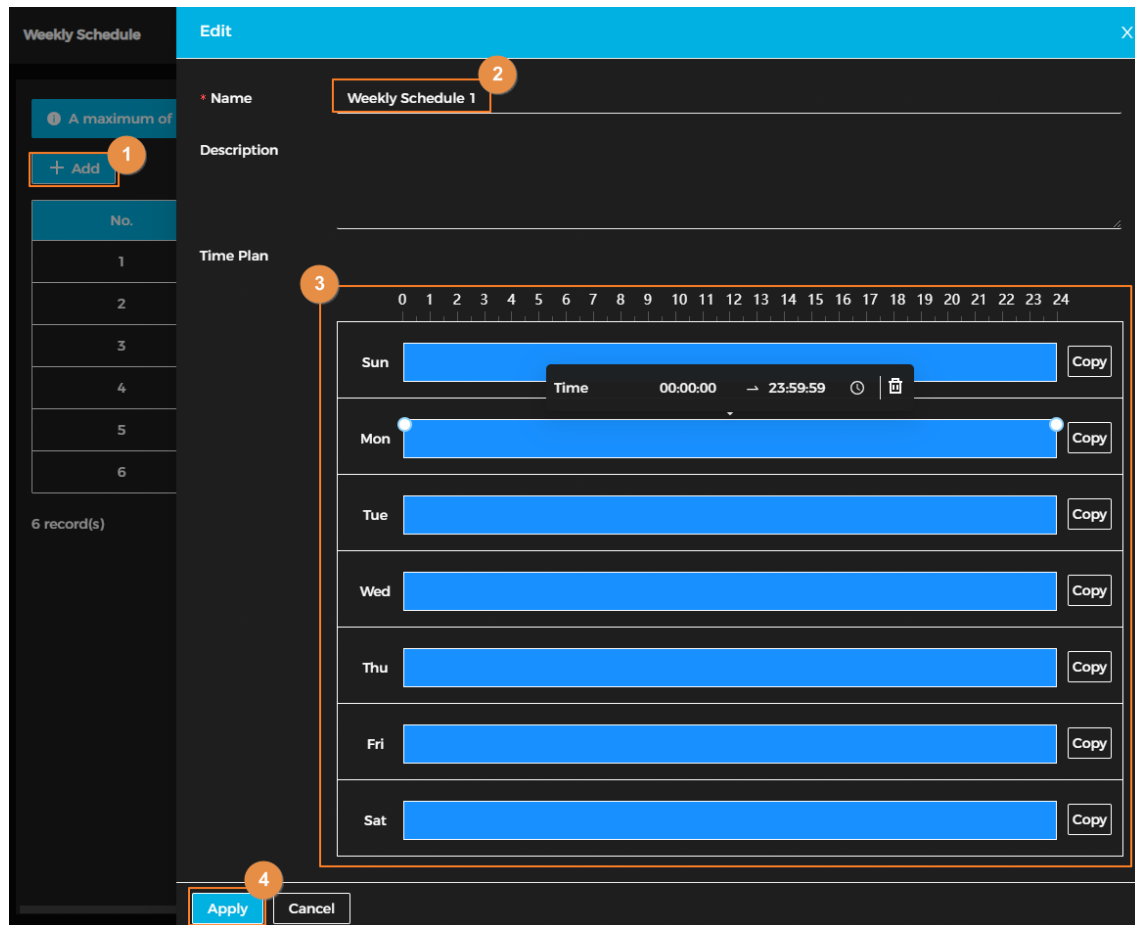
1. Navigate to Access Rules → Weekly Schedule. Click Add.

①

- The default full-day time template cannot be changed.
- Up to 128 weekly schedules can be created.

2. Click  to edit the time template. Name the template and use the sliders to set up to four (4) time periods a door can be locked or unlocked during the day. Click **Copy** to apply the same time period(s) across multiple days.

3. Click **Apply**.



Weekly Schedule

(Optional) Adding Holiday Schedules

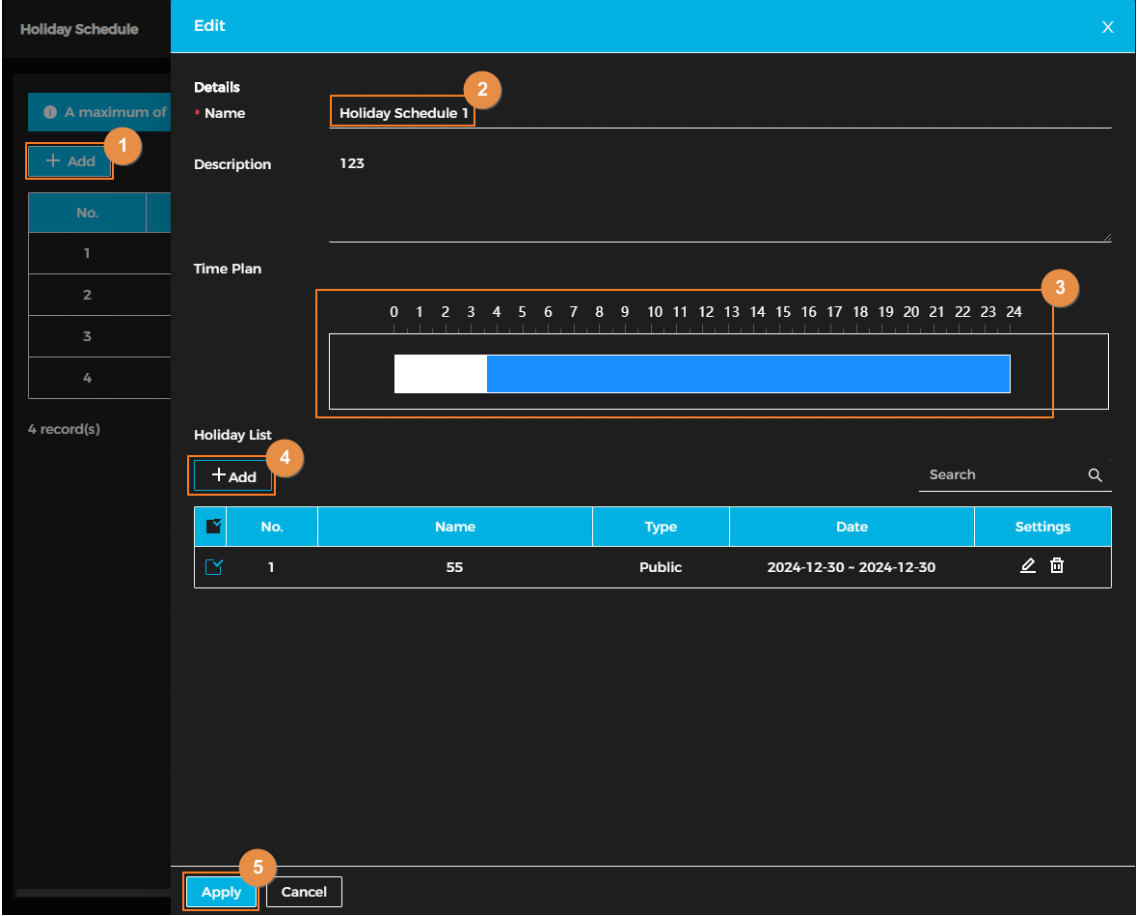
Follow the steps below to add holiday schedules.

1. Navigate to Access Rules → Holiday Schedule. Click Add.

①

- Up to 128 holiday schedules can be created.

- Click  to edit the time template. Name the template and use the sliders to set up to four (4) time periods a door can be locked or unlocked during the day.
- Click **Add** to include holidays in the holiday schedule. Enter the holiday name. Set the start date and duration. Select the type of holiday schedule: **public** (shared across all holiday schedules) or **custom** (used only in the current holiday schedule).



The screenshot shows the 'Holiday Schedule' edit window. It features a sidebar on the left with a '+ Add' button (callout 1) and a list of time periods (1-4). The main area is divided into 'Details' and 'Time Plan' sections. The 'Details' section includes a 'Name' field (callout 2) and a 'Description' field. The 'Time Plan' section shows a 24-hour timeline (callout 3) with a blue bar indicating a locked period from approximately 4 AM to 10 PM. Below this is a 'Holiday List' section with a '+ Add' button (callout 4) and a table of existing holidays. At the bottom, there are 'Apply' and 'Cancel' buttons (callout 5).

Holiday Schedule Edit

Details

Name:

Description:

Time Plan

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

Holiday List

+ Add

No.	Name	Type	Date	Settings
1	55	Public	2024-12-30 - 2024-12-30	

Apply Cancel

Holiday Schedule

Add [X]

* **Name** _____

* **Start Time** 09-23-2024 [Calendar Icon]

Duration 1 **Days**

Type (?) ☒ **Public** ☐ **Custom**

[OK] [Cancel]

Add Holiday

4. Click **Apply**.

Adding a Zone

Follow the steps below to add a zone. A zone is a group of door access permissions. Create a zone and assign users to it to grant them the zone's access rights.

1. Navigate to Access Rules → Zone Settings.
2. Click **Add**. You can add up to 40 zone permissions.
3. Name the zone.
4. Select the applicable doors.
5. Click **OK**.

Add [X]

• **Zone Name** Zone2

Door List

Search [Q]

- ▶ ☒ 24 [icon] 174
- ▶ ☐ 10. [icon] .106
- ▶ ☐ 10. [icon] .95
- ▶ ☐ 10. [icon] .112
- ▶ ☐ 10. [icon] .113
- ▶ ☐ 10. [icon] .96

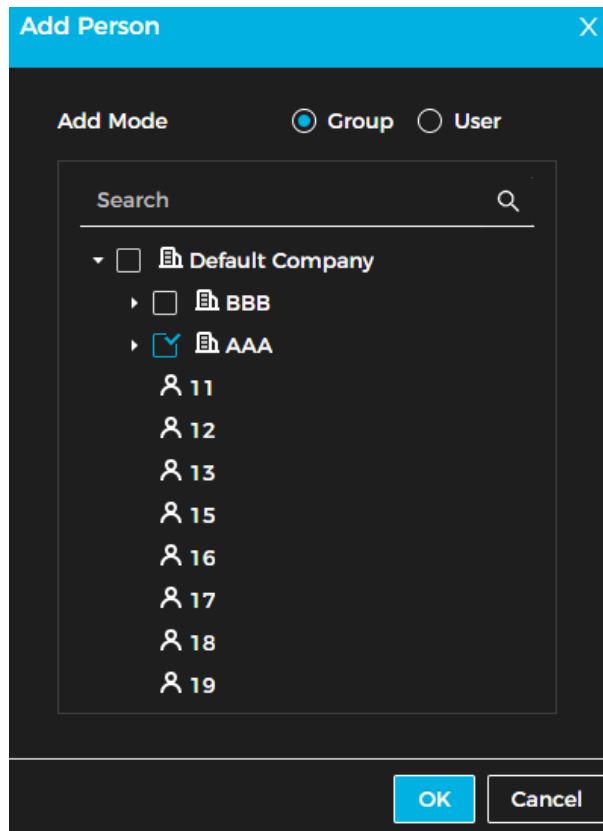
[OK] [Cancel]

Adding a Zone

Adding Permission Rules

Follow the steps below to add permission rules. Permission rules link users to zones, granting them access to the secured areas within those zones.

1. Navigate Access Rules → Permission Settings.
2. Click **Add**.
3. Name the rule.
4. Select the weekly and holiday schedule.
5. Navigate to **User Info**. Click **Add** to select a user or group. Click **OK**.



Add Person [X]

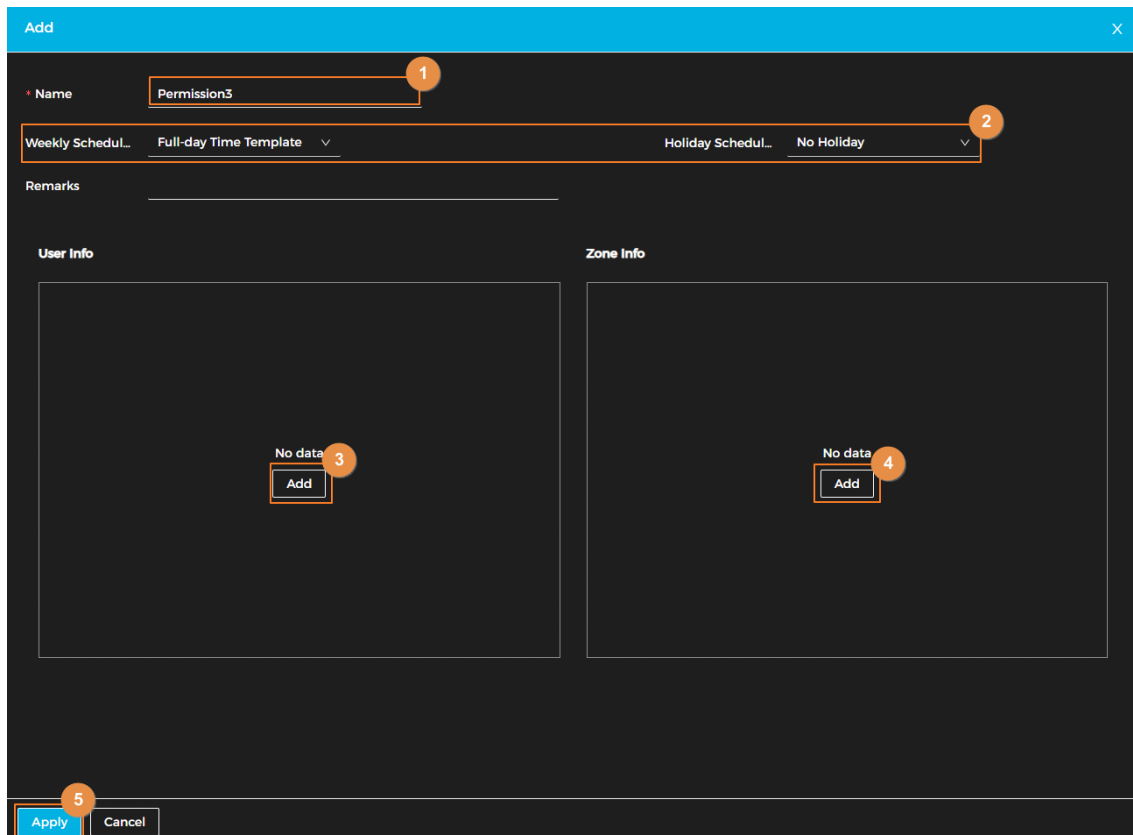
Add Mode ☒ **Group** ☐ **User**

Search [magnifying glass icon]

- [-] ☐ **Default Company**
 - [+] ☐ **BBB**
 - [+] ☒ **AAA**
 - [person icon] 11
 - [person icon] 12
 - [person icon] 13
 - [person icon] 15
 - [person icon] 16
 - [person icon] 17
 - [person icon] 18
 - [person icon] 19

OK **Cancel**

Add Person



Add [X]

* Name: 1

Weekly Schedul... Full-day Time Template Holiday Schedul... No Holiday 2

Remarks:

User Info

No data 3

Add

Zone Info

No data 4

Add

Apply 5 **Cancel**

Add Permission Rule

① To assign permissions to a new user or update an existing user's access, add them to an existing group. They will automatically receive the group's defined permissions.

6. Navigate to **Zone Info**. Click **Add**. Click **OK**.
7. Click **Apply**.

Review Data Synchronization Progress

Follow the steps below to review data synchronization progress. You can view this information after you assign access permission to users.

1. Navigate to Access Rules → Data Sync.
2. View the data synchronization progress.

Time	Zone Permission	Device Name	Details	Results	Settings
09-13-2024 01:37:02 PM		10-1113	Sync Person Info to Sub Controller	✓: 1, ✗: 0	
09-13-2024 01:37:02 PM		24-1174	Sync Person Info to Sub Controller	✓: 1, ✗: 0	
09-13-2024 01:37:01 PM		10-1106	Sync Person Info to Sub Controller	✓: 1, ✗: 0	

Data Synchronization Progress

Configure Basic Door Parameters

Follow the steps below to configure basic door parameters.

1. Navigate to Access Rules → Door Parameters.
2. Select the door from the left panel.
3. Set the parameters in the **Basic Settings** section. Refer to the table below for more information.

Door List
2
 Door1
 Door2
1
 Door1
 Door2

Basic Settings
Name: Door1
Unlock Type: ☒ Fail Secure ⓘ ☐ Fail Safe ⓘ
Door Status: ☒ Normal ☐ Always Unlocked ☐ Always Locked
Keep Door Unlocked for: Weekly Sched... Disabled ▾ Holiday Sched... Disabled ▾
Keep Door Locked for: Weekly Sched... Disabled ▾ Holiday Sched... Disabled ▾
Holiday Schedule Authen...: Disabled ▾
Public Unlock Password: ☐

Basic Parameters

Parameter	Description
Name	The door name.
Unlock Type	Choose between: Fail Secure: Lock stays closed during power outage. Fail Safe: Lock will activate during a power outage.
Door Status	Choose the door status: Normal: Door locks and unlocks based on configured settings. Always Unlocked: Door is always unlocked. Always Locked: Door always remains locked.
Keep Door Unlocked for	The door stays unlocked during the specified weekly or holiday schedule.

Keep Door Locked for	The door stays locked during the specified weekly or holiday schedule.
Holiday Schedule Authentication	Authorized access is permitted for an always-closed door during the specified holiday schedule.
Public Unlock Password	Enabling this function allows a user to unlock the door using a public password.

Configure Unlock Methods

Follow the steps below to configure unlock methods. You can unlock the door using various methods—Bluetooth card, fingerprint, card, or password—or combine them to create a custom unlock method.

1. Navigate to Access Rules → Door Parameters.
 2. Choose a door from the left panel.
 3. Select an unlock mode in the **Unlock Settings**.
 - If you select **Combination Unlock**, choose between **Or** (Any one of the selected methods can unlock the door) / **And** (All selected methods must be used to unlock the door). Choose the unlock method(s) and set the other parameters. See the table below for more information.
- ① Bluetooth cards cannot be used with the **And** option.

Combination Unlock

Parameter	Description
Unlock Method (Multi-Select)	Supports unlocking via card, fingerprint, password, or Bluetooth card. ① Bluetooth card is disabled by default.
Bluetooth Mode	The Bluetooth card must be within a specific range of the access control device to exchange data and unlock the door: • Short-Range: < 0.66 ft (0.2 m) • Mid-Range: < 6.56 ft (2 m) • Long-Range: < 32.81 ft (10 m) • ① Actual range may vary by phone model and environment.
Door Unlock Duration	• After access is granted, the door stays unlocked for a specified duration between 0.2 and 600 seconds.
Unlock Timeout	A timeout alarm is triggered if the door stays unlocked beyond the set duration.

Unlock by Period

- If you select **Unlock by Period**, drag the slider to set the time periods for each day. Click **Copy** to apply the same time periods to other days. Choose an unlock method for each period and configure the related parameters.

ⓘ A maximum of 4 time periods can be set per day.

Configure Alarms

Follow the steps below to configure alarms to trigger when an abnormal access event occurs.

- Navigate to Access Rules → Door Parameters → Alarm Settings.
- Set the alarm parameters. See the table below for more information.

Alarm Parameters

Parameter	Description
Duress Alarm	An alarm triggers when a duress card, password, or fingerprint is used to unlock the door.
Door Sensor	Choose the type of door sensor.
Intrusion Alarm	- When the door sensor is enabled, a forced or abnormal open triggers an intrusion alarm. - If the door remains unlocked past the configured duration, a timeout alarm activates.
Unlock Timeout Alarm	

	• If reader beeps are enabled, the card reader beeps when either alarm occurs.
--	--

3. Click **Apply**.

Configure Password Unlock

Follow the steps below to use a password to unlock a door. When PIN code authentication is enabled, users can unlock the door by entering only the password.



- **Disabled:** Enter `UserID#Password#` (e.g., User ID **123**, password **12345** → `123#12345#`).
- **Enabled:** Enter `Password#` (e.g., password **12345** → `12345#`).

1. Navigate to Access Rules → PIN Code Unlock.
2. Enable Pin Code Authentication.
3. Click **Apply**.

⚠ Enabling PIN code authentication introduces security risks because user types become ineffective, resulting in the following:

- First-card holders and multi-person unlock group members must use defined methods other than passwords. If they use a password, the first-person or multi-person unlock function is bypassed.
- Users must use defined methods other than passwords. If they use a password, the anti-passback function is bypassed.
- Patrol users and block-listed users can unlock doors by entering a password.
- Frozen or expired accounts can still unlock doors with a password.
- If password unlock is disabled at the same time, no user type can unlock doors using a password.

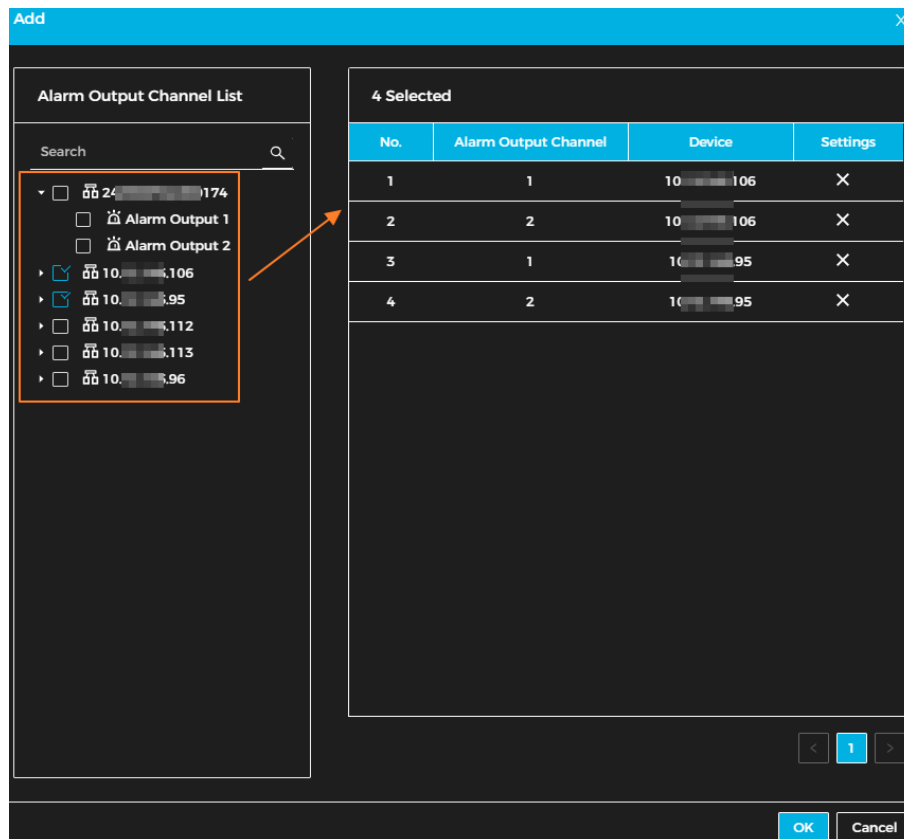
(Optional) Configure Global Alarm Linkages

Follow the steps below to set global alarm linkages across different access controllers.

1. Go to Access Rules → Global Alarm Linkage.



- If both global and local alarm linkages are set and conflict, the most recently configured linkage takes effect.
 - If sub-controller linkages are configured through the main controller and the main controller is reset to factory defaults, it is recommended to also reset the sub-controller.
2. From the alarm input channel list, select an input and click **Link Alarm Output**.
 3. Click **Add**, choose an alarm output channel, and click **OK**.
 4. Enable the alarm output function and set the alarm duration. Click **Apply**.



Alarm Output

- Click the Link Door Channel tab.
- From the channel list, select an alarm input and click Add.
- Choose the linkage door.
- Set the door status: **always unlocked** (door automatically unlocks when an alarm is triggered) or **always locked** (door automatically locks when alarm is triggered).
- Click **OK**.
- Click **Enable**.

Configuring First-Person Unlock

You can assign specific users as first-card holders. Other users can unlock the door only after a first-card holder has verified their identity.

Follow the steps below to configure this setting.

- Navigate to **Access Rules → First-person Unlock**.
- Click **Add** in the device list. Select the desired door.
- Choose the door status: **normal** (non-first-card users can unlock only after a first-card user grants access on the controller) or **always unlocked** (the door remains unlocked after a first-card user grants access on the controller).
- Select the weekly and holiday schedules. First-card access is valid only within the defined time.
- Click  to add first-card users. Click **OK**.

First Card Users (1)

No.	User Name	Settings
1	Default Company-105	X
2	Default Company-106	X
3	Default Company-107	X
4	Default Company-108	X
5	Default Company-109	X

First Card Users (2)

Configuring Multi-Person Unlock

When multi-person unlock is enabled, users must authenticate on the access controller in a set order before the door unlocks. It is not recommended to include first-card users in multi-person unlock groups.

Follow the steps below to configure this feature.

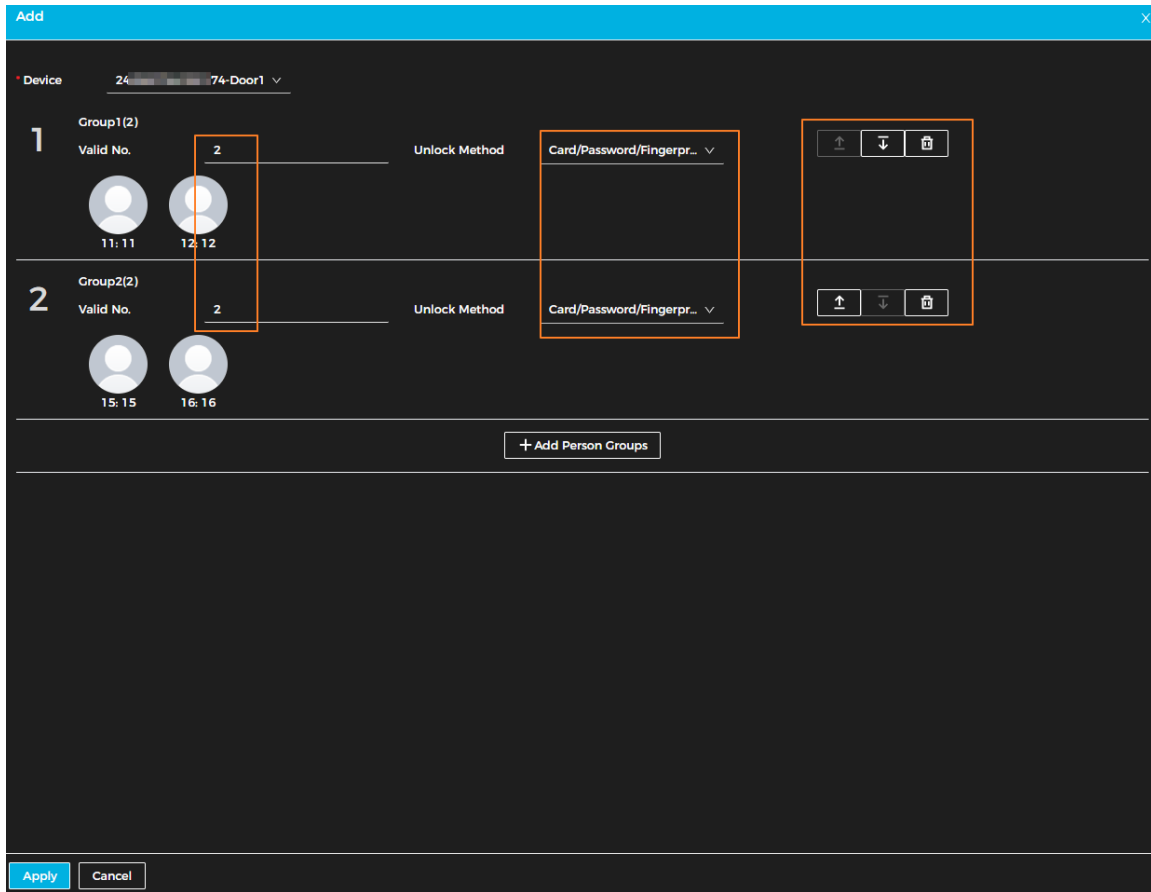
1. Navigate to **Access rules → Multi-person Unlock**.
2. Add doors to the device list by clicking **Add**.
3. Click **Add Person Groups**.
4. Click **Add** to create multi-person unlock groups.
5. Enter a group name, select users from the user group, and click **OK**.
6. Choose a door.
7. Click **Add Person Groups**.
8. Select groups.
9. Click **OK**.

⑩ Each door can have up to 4 groups, and each group can include up to 50 users.

10. Configure multi-person unlock parameters. See the table for more information.

Parameter	Description
Valid No.	The number of users in the group who must verify on the access controller before the door unlocks.
Unlock Method	Group members must authenticate using the defined methods.
	Use the arrows to adjust the group sequence. If multiple groups are added, users must verify in the set group order.

11. Click **Apply**.



Multi-Person Unlock

Configuring Anti-Passback

Anti-passback requires users to verify their identity for both entry and exit. If not followed, an anti-passback alarm is triggered, preventing a cardholder from passing their card to another person for unauthorized access. When enabled, the cardholder must exit the secure area before being granted re-entry.

Prior to enabling anti-passback, please consider the following information:

- If a user enters with authorization but exits without authorization, an alarm triggers and access is denied when they attempt to re-enter.
- If a user enters without authorization but exits with authorization, an alarm triggers and access is denied when they attempt to re-enter.
- If anti-passback is configured on sub-controllers via the main controller, and the main controller is reset to factory defaults, also reset the sub-controllers.

- In unstable networks, doors may open after identity verification, but the card reader might trigger a timeout alarm. Ensure network stability.
- If anti-passback is set on sub-controllers through the main controller and the main controller is reset to factory defaults, also reset the sub-controllers.
- With an unstable network, the door may open after verification, but the card reader could trigger a timeout alarm. Ensure network stability.

Follow the steps below to configure anti-passback.

1. Navigate to **Access Rules → Anti-passback**.
2. Enable the **Reset Anti-Passback** function, then set a reset time. At the specified time, the anti-passback status of all users will be cleared.

Reset Time

3. Click **Anti-passback Group List**, then click **Add** to create a new anti-passback group.

Add Group

4. Name the anti-passback group, set a reset time, and choose the execution mode.



- **Reset Mode:** Define the time period for triggering anti-passback alarms. For example, if the reset time is 60 minutes, a user who enters with authorization but exits without authorization will trigger an anti-passback alarm if they try to re-enter within 60 minutes.
- **Strong Execution:** Both main and sub-controllers enforce anti-passback even when offline.
- **Weak Execution:** Anti-passback is not enforced if controllers go offline.

5. Select the weekly and holiday schedules. Anti-passback applies only during the defined times.

6. In Group 1, click **Add**, then select card readers.

7. In Group 2, click **Add**, then select card readers.

8. (Optional) Click **Add Door Groups** to add more groups. Multiple readers can be added to a group; users may swipe at any of them for access.

9. Hit **Apply**.

The group number defines the swipe sequence. Cards must be used in sequential order (i.e., Group 1 must go first, then Group 2, then Group 3, and so on).

Multi-Door Interlock

Multi-door interlock links two or more doors so that when one door is unlocked, the others remain locked and cannot be accessed.



- If multi-door interlock is configured on sub-controllers through the main controller and the main controller is reset to factory defaults, it is recommended to reset the sub-controllers.
- In unstable networks, a door may open after identity verification, but the card reader may trigger a timeout alarm. Ensure network stability.

Configuring Interlock Within a Group

Follow the steps below to configure interlocking within a group.

1. Navigate to **Access Rules** → **Interlock** → **Interlock Within Group**.
2. Click **Add** to add an interlock group.
3. Name the interlock group.
4. Choose the execution mode: **strong execution** (main and sub-controllers enforce the interlock function even when offline) or **weak execution** (interlock function is not enforced if the controllers go offline).
5. Click **Add** to add doors to a device group.

① At least two doors must be added.

The screenshot shows a modal window titled "Add" with a close button (X). Inside, there are two input fields: "Name" with the value "Interlock within Group 1" and "Execution" with a dropdown menu set to "Strong Execution" and a help icon. Below these is a section titled "Device Group Config" with a help icon. It contains a table with the header "Device Group" and one row with the value "Group 1". Below the table is a "No data" message and an "Add" button. At the bottom of the modal are "Apply" and "Cancel" buttons.

Add Interlock

6. Click **Apply**.

After a user verifies their identity and opens a door, they must close it before unlocking the next door.

Configuring Interlock Between Groups

Follow the steps below to configure an interlock between a group.

1. Navigate to **Access Rules** → **Interlock**.
2. Click **Interlock between groups**.

The screenshot shows a modal window titled "Add" with a close button (X) in the top right corner. The window has a dark background. At the top, there are two fields: "Name" with the value "Interlock between Groups 3" and "Execution" with a dropdown menu showing "Strong Execution" and a help icon (?). Below these is a section titled "Device Group Config" with a help icon (?). This section contains two columns, "Group 1" and "Group 2", under the heading "Device Group". Each column is empty and contains the text "No data" and an "Add" button. At the bottom of the modal are two buttons: "Apply" and "Cancel".

Add Interlock Group

3. Click **Add** to add an interlock group.
4. Name the interlock group.
5. Choose the execution mode: **strong execution** (main and sub-controllers enforce the interlock function even when offline) or **weak execution** (interlock function is not enforced if the controllers go offline).
6. In Group 1, click **Add**, then select doors.
7. In Group 2, click **Add**, then select doors.
8. Click **Apply**.

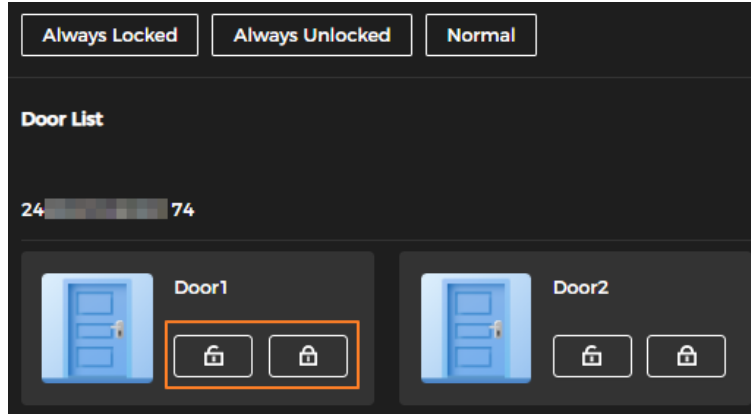
If a door in one group is unlocked, doors in the other group cannot be opened.

Access Monitoring

Lock and Unlock Doors Remotely

Follow the steps below to remotely lock and unlock doors.

1. Click **Access Monitoring**.
2. Click  or  to control the door lock.



Remote Unlock or Lock

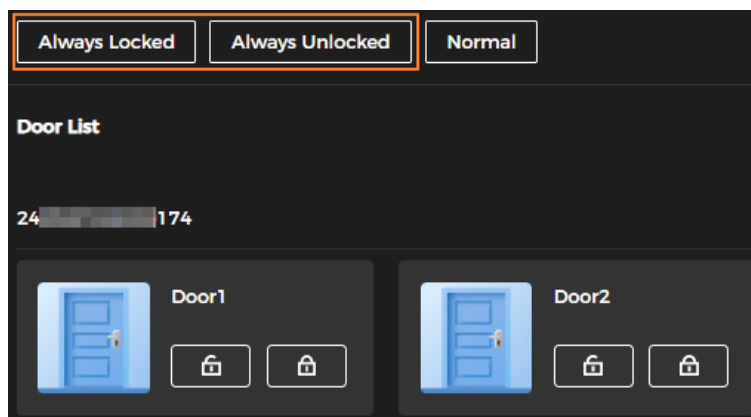
Related Operations

- To filter events by type, choose the event type from **Event Info**.
- To delete events, click  to delete all the events from the event list.

Configuring Always Locked and Always Unlocked Settings

Follow the steps below to set a door to remain locked or unlocked.

1. Click **Access Monitoring**.
2. Click **Always Locked** or **Always Unlocked**.



Always Locked or Always Unlocked

The door stays permanently locked or unlocked. Click **Normal** to restore standard access control, allowing the door to lock or unlock according to the configured verification methods.

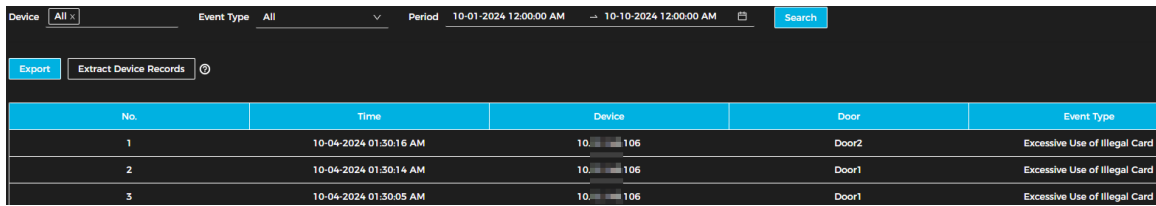
Reports

This section goes over alarm logs and unlock logs.

View Alarm Records

Follow the steps below to view alarm records.

1. Navigate to **Reports → Alarm Records**.
2. Choose the device, group, and period.
3. Click **Search**.



Device	All x	Event Type	All	Period	10-01-2024 12:00:00 AM	10-10-2024 12:00:00 AM	Search
Export	Extract Device Records						
No.	Time	Device	Door	Event Type			
1	10-04-2024 01:30:16 AM	10.106	Door2	Excessive Use of Illegal Card			
2	10-04-2024 01:30:14 AM	10.106	Door1	Excessive Use of Illegal Card			
3	10-04-2024 01:30:05 AM	10.106	Door1	Excessive Use of Illegal Card			

Alarm Records

Related Operations

- **To export**, save unlock logs from the main controller to a local computer.
- **To extract device records**, import logs from a sub-controller to the main controller when the sub-controller comes online.

View Unlock Records

Follow the steps below to view unlock records.

1. Navigate to **Reports → Unlock Records**.
2. Choose the device, group, and period.
3. Click **Search**.

Related Operations

- **To export**, save alarm logs from the main controller to a local computer.
- **To extract device records**, import logs from a sub-controller to the main controller when the sub-controller comes online.

System Settings

You can configure system settings to local access controllers.

Configure System Time

1. Navigate to **System Settings → Time Settings**.
2. Set the platform time. See the table for more information.
3. Click **Apply**.

System Time

09-29-2024 5:50:02 PM

Synchronize PC

Time Zone

(UTC+08:00) Beijing, Chongqing

▼

Date Format

Month_Day_Year

▼

Time Format

12-Hour

▼

NTP Settings

☐

NTP Server

time.windows.com

Manual Update

Port

123

(1-65535)

Update Cycle

1440

min

Daylight Saving TI...

☒

Start Time

March

▼

Second

▼

Sunday

▼

02 AM

🕒

End Time

November

▼

First

▼

Sunday

▼

02 AM

🕒

Apply

Refresh

Default

Time Settings

Parameter	Description
System Time	Enter the time manually, or click Synchronize PC to match the computer’s time.
Time Zone	Set the access controller’s time zone, date format, and time format.
Date Format	
Time Format	
NTP Settings	The access controller automatically syncs time with the NTP server. Enable NTP Settings, then configure the NTP server domain, port, and update cycle (synchronization interval).
NTP Server	
Port	
Update Cycle	
Daylight Savings Time	Enable this feature and set the start and end time.

Network Configuration

This section goes over network configuration.

Configure TCP/IP

Follow the steps below to configure the access controller’s IP address to ensure communication with other devices.

1. Navigate **System Settings → Network Setting → TCP/IP**.
2. Set the parameters. See the table for more information.
3. Click **Apply**.



NIC

NIC 1

Mode

☐ DHCP
☒ Static

MAC Address

IP Version

IPv4

IP Address

10 . . 89

Subnet Mask

255 . . 0

Default Gateway

10 . . 254

Preferred DNS

8 . . 8

Alternate DNS

8 . . 4

MTU

1500

Apply

Refresh

Default

TCP/IP Settings

Parameter	Description
Mode	Static: Manually set the IP address, subnet mask, and gateway. DHCP: When enabled, the access controller automatically receives an IP address, subnet mask, and gateway. After initializing a sub-controller, switch its network mode to Static. DHCP should only be used during initialization.
MAC Address	Access controller's MAC address.
IP Version	IPv4
IP Address	In Static mode, set the IP address, subnet mask, and gateway. The IP address and gateway must be on the same network segment.
Subnet Mask	
Default Gateway	
Preferred DNS	IP address of the preferred DNS server.
Alternate DNS	IP address of the alternate DNS server.

Configure Ports

You can restrict access to the access controller simultaneously via webpage, desktop client, and mobile app. Follow the steps below to do this.

1. Navigate to **System Settings → Network Setting → Port**.
2. Configure the ports. See the table below for more information.
3. Click **Apply**.

Max Connection	50	(1-50)
HTTP Port	80	(1-65535)
HTTPS Port	443	(1-65535)

Port Configuration

Parameter	Description
Max Connection	Set the maximum number of clients—webpage, desktop client, and mobile app—that can connect to the access controller simultaneously.
HTTP Port	The default port is 80. To change it, enter the new port number after the IP address when logging in to the webpage.
HTTPS Port	The default is 443.

Configure Cloud Service

Follow the steps below to configure cloud service. Prior to configuring, add the main controller to LumiViewer before requesting Bluetooth cards for users. If the main controller password is changed or the device is restored to factory defaults, delete the controller from LumiViewer and add it again.

1. Navigate **System Settings** → **Network Setting** → **Cloud Service**.
2. Enable the cloud service function.
3. Click **Apply**.
4. Download LumiViewer and create an account.
5. Scan the access controller's QR code to add it to LumiViewer.

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
Offline

SN
24 74

Cloud Service

Configure Automatic Registration

Follow the steps below to configure automatic registration. The access controller will send its address to the designated server, allowing access through the management platform.

- 1. Navigate to **System Settings → Network Settings → Auto Registration**.
- 2. Enable the function and set the parameters. See the table below for more information.
- 3. Click **Apply**.

Enable

☒

Server Address

172.217

Port

7000

Sub-Device ID

none

Apply

Refresh

Default

Automatic Registration

Parameter	Description
Server Address	IP address of the server.
Port	Server port used for automatic registration.
Sub-Device ID	Enter the sub-device ID. This is user-defined. When adding the access controller to the management platform, ensure the sub-device ID matches the one defined on the access controller.

Configuring Basic Services

Follow the steps below to enable **CGI** and **ONVIF** functions to connect the access controller to a third-party platform.

- 1. Navigate **System Settings → Network Settings → Basic Services**.
- 2. Configure basic service. See the table below for more information.
- 3. Click **Apply**.

SSH

☒

CGI

☒

ONVIF

☒

Private Protocol Authentication ...

Security Mode (Recommen... ▾)

TLS1.1

☐

Apply

Refresh

Default

Basic Services



Parameter	Description
SSH	SSH (Secure Shell) is a remote management protocol that lets users securely access, control, and configure remote servers over the internet.
CGI	The Common Gateway Interface (CGI) is a standard that enables data exchange between web servers and external applications.
ONVIF	ONVIF (Open Network Video Interface Forum) defines a standard interface for IP-based security devices. Its specifications act as a common language, enabling different devices to communicate seamlessly.
Private Protocol Authentication Mode	Set the authentication mode to either Security Mode (recommended) or Compatibility Mode . Security Mode (Recommended): Blocks Digest, DES, and plaintext authentication methods, enhancing device security. Compatibility Mode: Allows Digest, DES, and plaintext authentication methods but lowers security.
TLS1.1	The platform connects devices using the TLSv1.1 protocol. Please note that enabling TLSv1.1 may introduce security risks.

Updating the System

Prior to updating the system, ensure the following requirements are met:

- Ensure you use the correct update file provided by technical support.
- Do not disconnect power or network and avoid restarting or shutting down the access controller during the update.

File Update

Follow the steps below to update the system using a file.

1. Navigate **System Settings** → **System Update**.
2. In the **File Update** section, click **Browse** and upload the update file (.bin format).
3. Click **Update**.

The access controller restarts automatically after the update is complete.

Online Update

Follow the steps.

1. Navigate **System Settings** → **System Update**.
2. In the **Online Update** section, choose an update method: **auto check for updates** (access controller automatically checks for the latest version) or **manual check** (check immediately for the latest version).
3. Click **Manual Check** to update the access controller.

Importing and Exporting Configuration Files

When multiple access controllers need the same settings, you can speed up configuration by importing or exporting configuration files. Import a configuration file to apply the same settings to other devices or export one for reuse. Device management, advanced access control, time schedules, and hardware configurations cannot be exported.

Follow the steps below to import and export configuration files.

1. Navigate to **System Settings** → **Advanced Settings**.
2. To export a configuration file, click **Export Configuration File**. To import a configuration file, click **Browse**, select the configuration file, and click **Import File**.



- IP will not export.
- Configuration files can only be imported into devices of the same model.

Import and Export Configuration Files

Configure the Card Reader

Follow the steps below to configure the card reader.

1. Navigate to System Settings → Advanced Settings.
2. Configure the card reader. See the table below for more information.

Card Reader Configuration

Parameter	Description
Door Channel	Select the door channel where you want to enable card number inversion. For single-channel devices, selecting a channel is not required. To change the door type, go to System Settings → Hardware Wiring → Reset Hardware Config.
Card No. Inversion	Enable Card No. Inversion to reverse card numbers during collection or swiping (i.e., card number 123456 becomes 654321). This function is only supported for card readers connected via Wiegand.
Reader	Choose the card reader.
Baud Rate	Choose the card reader's baud rate. The default is 9600.

3. Click **Apply**.

Configure RS-485 Expansion

If the access controller is installed in a metal case, go to **System Settings → Advanced Settings → RS-485 Expansion**, then select **Access Control Metal Case**.

Reset to Factory Settings

Follow the steps below to reset the device to factory settings. Please note that restoring the access controller to the default configurations will erase data.



1. Navigate to **System Settings → Advanced Settings**.
2. Choose an option: **Factor Defaults** (resets all configurations and deletes all data) or **Restore to Default Settings (Except for User Info)**.



- **Restore to Default Settings (Except for User Info)** resets configurations and deletes all data except user information and settings made during the login wizard.
- Only the main controller supports **Restore to Default Settings (Except for User Info)**.

Configure Card Rules

Follow the steps below to configure card rules. The platform supports five default Wiegand formats with the option to add custom formats.

1. Navigate to System Settings → Card Rule Settings.
2. Click **Add**.
3. Configure new Wiegand formats. You can also click **Add Protocol** to import a Wiegand file. See the table below for more information.
4. Click **Apply**.

Add

Wiegand Format

Total Bits

(1-128)

Facility Code

Add

No.	Start Bit	End Bit	Total Bits	Settings
No data				

Card Number

Add

No.	Start Bit	End Bit	Total Bits	Settings
No data				

Parity Code

Add

Parity Code	Type	Start Bit	End Bit	Total Bits	Settings
No data					

Apply

Cancel

Wiegand Format



Parameter	Description
Wiegand Format	The name to identify the Wiegand format.
Total Bits	The total number of bits.
Facility Code	Click Add . Enter the facility code's start and end bit.
Card Number	Click Add . Enter the card number's start and end bit.
Parity Code	Click Add . Enter the even and odd parity start and end bit.

Related Operations

- **Facility Code:** When enabled and **Card No. System** is set to decimal format in User Management, the facility code and card number are converted separately into decimal format, then combined.
- **When HID26 is enabled:**
 - Only **Wiegand 26** is supported.
 - Cards are displayed only in decimal format.
 - The card number must be 5 digits, and the facility code up to 3 digits.
 - If a manually entered card number is shorter than 5 digits (e.g., **56**), leading zeros are added (e.g., **00056**). An additional zero is added for the facility code, making the final card number **000056**.

Restart the Access Controller

You can schedule regular restarts of the access controller during idle periods to improve performance. The default is **Never**; we recommend setting it to once per week. Follow the steps below to schedule regular restarts of the access controller.

1. Navigate to **System Settings → Restart**.
2. Choose the restart time from the drop-down menu.
3. Click **Apply**.
4. (Optional) Click **Restart** to restart the access controller immediately.

Restart System

Back Up System Logs

Follow the steps below to back up system logs.

1. Navigate to **System Settings → System Logs**.
2. Choose the type of log and time period.
3. Click .
4. Click **Encrypt Log Backup**.
5. Enter the password to back up encrypted logs.

6. (Optional) Click **Export** to export logs.

Export

Type All

Period 09-27-2024 12:00:00 - 09-28-2024 12:00:00

☐ Encrypt Log Backup

No.	Username	Type	Time	Settings
1	admin	Save Config	09-27-2024 02:09:53 PM	
2	admin	Login	09-27-2024 01:38:42 PM	
3	admin	Logout	09-27-2024 12:50:11 PM	
4	admin	Login	09-27-2024 11:56:10 AM	
5	admin	Logout	09-27-2024 09:24:58 AM	
6	admin	Login	09-27-2024 09:24:55 AM	

System Log Backup

Configure Local Alarm Settings

Local alarm settings can only be configured on the same access controller. Each controller supports 2 alarm inputs and 2 alarm outputs. Follow the steps below to configure local alarm settings.

- 1. Go to **System Settings → Local Alarm Linkage**.
- 2. Click to set the local alarm settings. See the table below for more information.
- 3. Click **OK**.

Modify

Alarm Input Channel1

Alarm Input NameZone1

Alarm Input TypeNormally Open

Link Fire Safety Contr...☐

Alarm Output☐

Duration30s (1-300)

Alarm Output Channel☒ 1 ☐ 2

Access Control Linka...☐

Door1Always Unlocked

Door2Always Unlocked

OK

Cancel

Local Alarm Settings

Parameter	Description
Alarm Input Channel	Alarm input channel number. Each controller provides 2 alarm inputs and 2 alarm outputs.
Alarm Input Name	The name of the alarm input.
Alarm Input Type	Alarm input type: normally open or normally closed.
Link Fire Safety Control	When fire safety control is enabled, all doors unlock automatically if a fire alarm is triggered.
Alarm Output	Enable Alarm Output, set the duration, and select output channels. When an alarm is triggered, it stays active for the defined duration and triggers the selected channels with linkage actions. Each controller supports 2 alarm inputs and 2 alarm outputs.
Duration	
Alarm Output Channel	

Access Control Linkage	Enable this function to configure door linkage. Set the door to Always Locked or Always Unlocked . When an alarm is triggered, the door will automatically lock or unlock.
Door1/Door2	

Account Management

This section goes over how to add or remove users, update user passwords, and set an email address for password recovery.

Add Administrator Accounts

Follow the steps below to add administrators to the access controller

1. Navigate to **System Settings → Account Management → Account**.
2. Click **Add**.
3. Input the user information.
4. Click **OK**.

The screenshot shows a modal window titled "Add" with a close button (X) in the top right corner. The form inside has the following fields and options:

- Username:** A text input field with a red asterisk indicating it is required.
- Password:** A text input field with a red asterisk.
- Confirm Password:** A text input field with a red asterisk.
- Remarks:** A text input field.
- Permission:** A list of checkboxes with corresponding labels:
 - ☒ Device Management
 - ☒ User Management
 - ☒ Access Rules
 - ☒ Weekly Schedule
 - ☒ Holiday Schedule
 - ☒ Zone Settings
 - ☒ Permission Settings

At the bottom right of the dialog are two buttons: "OK" (highlighted in blue) and "Cancel".

Add Administrator Accounts



- **Username:** Must be unique, up to 31 characters, and may include letters, numbers, underscores (_), dots (.), and @.
- **Password:** Must be 8–32 non-blank characters and include at least two of the following: uppercase letters, lowercase letters, numbers, or special characters (excluding ' " ; : &). Follow the strength prompt to set a secure password.
- Only the administrator account can change passwords, and the admin account cannot be deleted.

Reset the Device Password

If you forget your password, a security code will be sent to the linked email address, allowing you to reset it. Follow the steps below to reset the device password.

1. Navigate to **System Settings → Account Management → Account**.
2. Enter the email address and set the password expiration time.

3. Enable the password reset function.
4. Click **Apply**.

Password Reset

Add ONVIF Users

ONVIF (Open Network Video Interface Forum) is a global industry forum that defines open standards for IP-based security devices, enabling cross-manufacturer compatibility. ONVIF users are authenticated through the ONVIF protocol. The default ONVIF user is **admin**.

Follow the steps below to add ONVIF users.

1. Navigate **System Settings** → **Account Management** → **ONVIF User**.
2. Click **Add**.
3. Set the parameters. See the table below for more information.
4. Click **OK**.

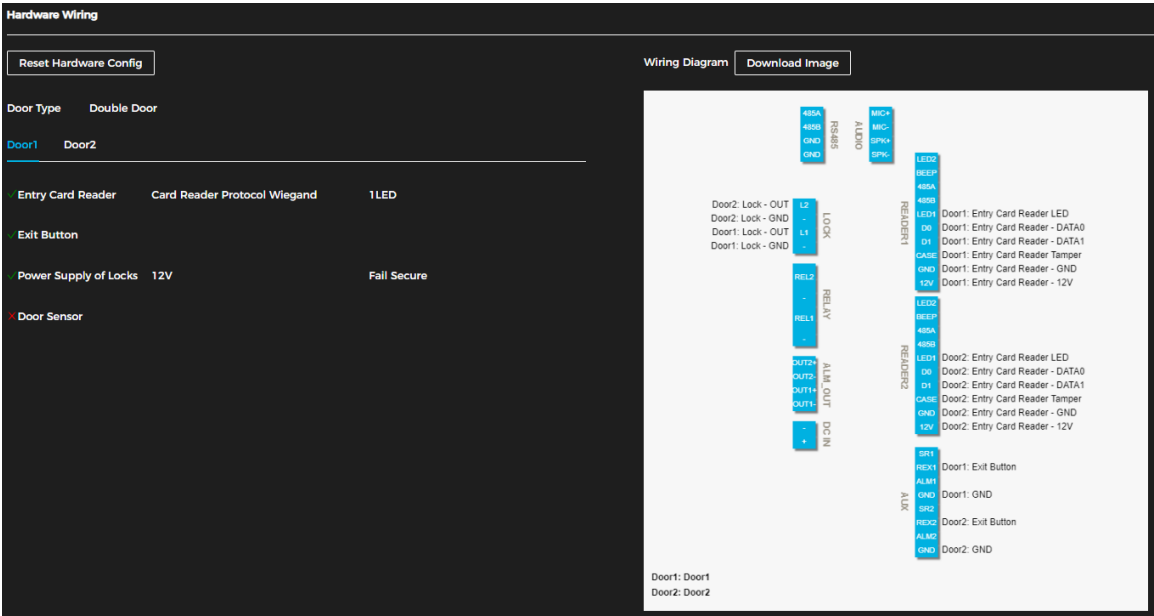
Add ONVIF User

Parameter	Description
Username	The username must be unique and can contain up to 31 characters. Only numbers, letters, underscores (_), hyphens (-), dots (.), and @ are allowed.
Password	The password must be 8–32 non-blank characters and include at least two of the following: uppercase letters, lowercase letters, numbers, or special characters (excluding ' " ; : &).

Group	There are three permission groups, each with different access levels: • Admin: Full access, including user management in ONVIF Device Manager. • Operator: No access to user management. • User: No access to user management or system logs.
-------	---

Configure Hardware

Go to **System Settings** → **Hardware Wiring** to view the hardware configured during your first login. Click **Reset Hardware Config** to reconfigure hardware. When switching between single-door and double-door setups, it is recommended to restore the main controller to factory defaults. A wiring diagram is generated for reference and can be downloaded to your computer.



Wiring Diagram

View Legal Information

Go to **System Settings** → **Legal Info** to view the software license agreement, privacy policy, and open-source software notice.

View Version Information

Go to **System Settings** → **Version Info** to view details such as device model, serial number, hardware version, legal information, and other version information.

Maintenance Center

This section goes over functions of the maintenance center.

Packet Capture

Follow the steps below to capture network interaction data between the device and a specified client network card, then save it to the computer.

1. Navigate to **Maintenance Center** → **Packet Capture**.
2. Click ► to start capturing packets. Packet Sniffer Size will show the size of the packet. Click || to end capture. The capture file will be saved to your local device.

Packet Capture						
NIC	Device Address	IP 1: Port 1		IP 2: Port 2		Packet Sniffer Size
eth0	172.28.103.122	Optional	Optional	Optional	Optional	0.00MB

Packet Capture

Run Log

Follow the steps below to run a debug log and export it.

1. Navigate to **Maintenance Center → Run Log**.
2. Click **Start** to begin logging, then click **End** to stop.
3. Click **Export** to download the debug log.

Security

This section goes over how to configure security functions of the device.

Configure HTTPS

Follow the steps below to configure HTTPS. Create or upload a verified certificate to enable HTTPS login from your computer. HTTPS ensures secure communication over the network.

1. Navigate to **Security → System Service**.
2. Enable HTTPS service.
- ⚠ Enabling HTTPS with TLS v1.1 or earlier may pose security risks.
3. Choose the certificate. If no certificates are listed, click **Certificate Management** to upload one.
4. Click **Apply**.
5. In a web browser, enter https://IP address:HTTPS port. If a valid certificate is installed, the login page opens successfully. If not, the browser shows the certificate as invalid or untrusted.

Enable ☐

HTTPS is a service entry based on Transport Layer Security (TLS). HTTPS provides web service, ONVIF access service and RTSP access service.

Select a device certificate

Certificate Management

No.	Custom Name	Certificate Serial Number	Valid from	User	Issued by	Used by
1		31	09-01-2054 10:48:35 AM	24	BSC	HTTPS, RTSP over TLS

Apply

Refresh

Default

Download Root Certificate

HTTPS

Configure a Firewall

Follow the steps below to configure a firewall to limit access to the controller.

1. Navigate to **Security → Attack Defense → Firewall**.
2. Click ☐ to enable the firewall.
3. Choose **allowlist** (grants access to the access controller only for IP/MAC addresses on the list) or **blocklist** (denies access to the access controller for IP/MAC addresses on the list).
4. Click **Add** and enter the IP information.
5. Click **OK**.

Firewall

Related Information

- To delete the IP address, click .
- To edit the IP information, click .

Configure Account Lockout

Follow the steps below to lock an account after the wrong password is entered a set number of times.

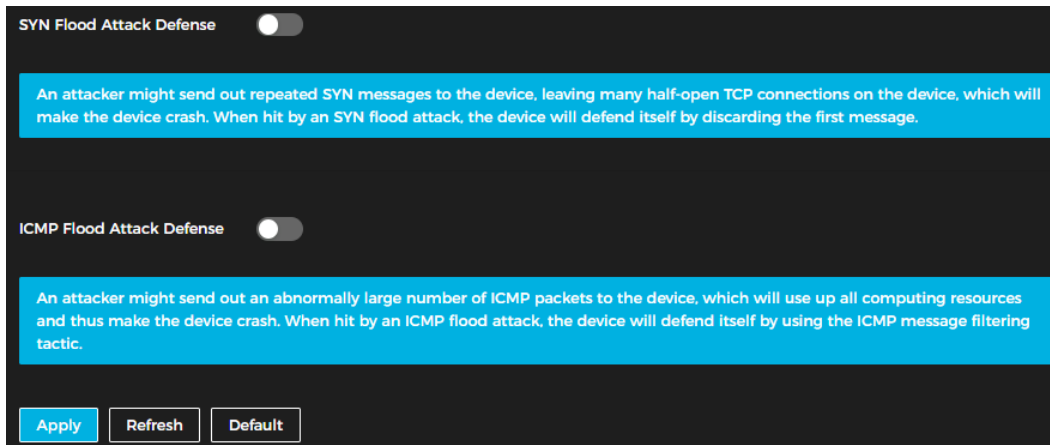
1. Navigate to **Security → Attack Defense → Account Lockout**.
2. Set the maximum number of failed logins and duration the account lockout for the administrators and ONVIF users.
3. Click **Apply**.

Account Lockout

Configure Anti-DoS Attack

Follow the steps below to enable SYN Flood Attack Defense and ICMP Flood Attack Defense to protect the access controller from DoS attacks.

1. Navigate to **Security → Attack Defense → Anti-DoS Attack**.
2. Enable **SYN Flood Attack Defense** or **ICMP Flood Attack Defense**.
3. Click **Apply**.



Anti-DoS Attack

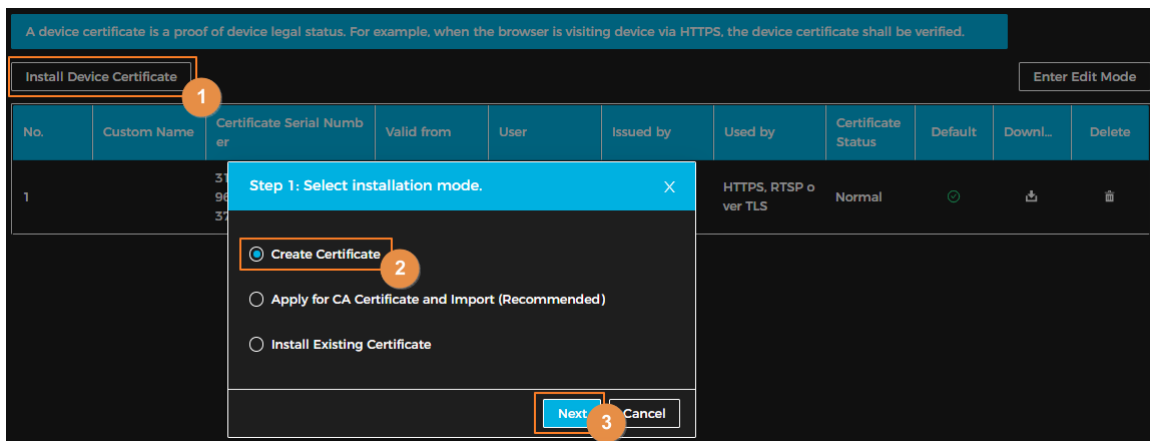
Device Certificates

This section outlines how to create and upload an authenticated certificate.

Create a Certificate

Follow the steps below to create a certificate for the access controller.

1. Navigate to **Security** → **CA Certificate** → **Device Certificate**.
2. Click **Install Device Certificate**.
3. Click **Create Certificate**. Hit **Next**.



Device Certificate Creation

4. Input the certificate information.
- ① The country/region name must not exceed 2 characters. Use the standard abbreviation.
5. Click **Create and install certificate**. After successful installation, the new certificate appears on the **Device Certificate** page.

Related Operations

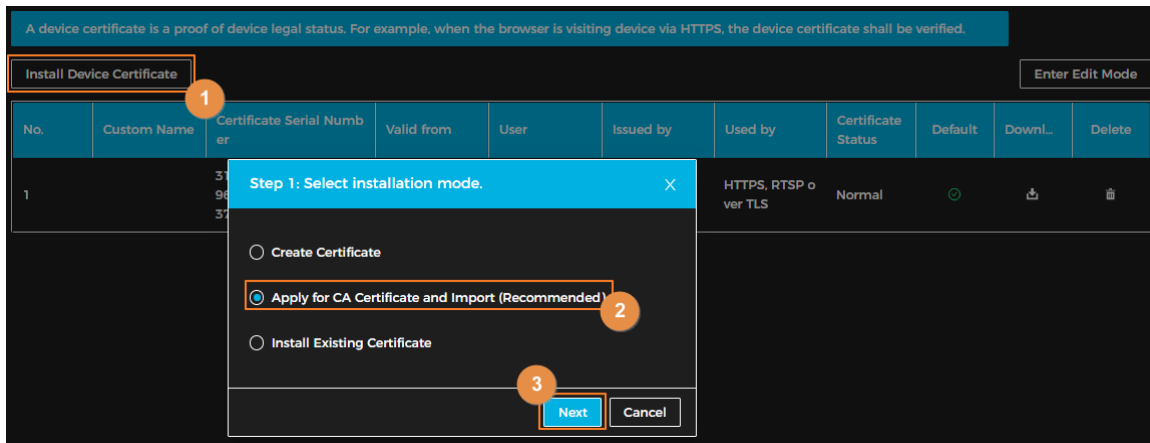
- To edit the name of the certificate, click **Enter Edit Mode** on the **Device Certificate**.
- To download the certificate, click .
- To delete the certificate, click .

Apply for and Import a CA Certificate



Follow the steps below to import a third-party CA certificate.

1. Navigate to **Security → CA Certificate → Device Certificate**.
2. Hit **Install Device Certificate**.
3. Click **Apply for CA Certificate and Import (Recommended)**. Hit **Next**.



CA Certificate

4. Enter the IP address or the domain of the access controller and the device's country and region.
① The country/region name must not exceed 3 characters. Use the standard abbreviation.
5. Click **Create and Download**.
6. Send the certificate to a third-party CA authority to authenticate by using the request file.
7. When the CA certificate is signed, save the certificate to your computer.
8. Click **Browse** and select the signed CA certificate.
9. Click **Import and Install**. After successful installation, the new certificate appears on the **Device Certificate** page.

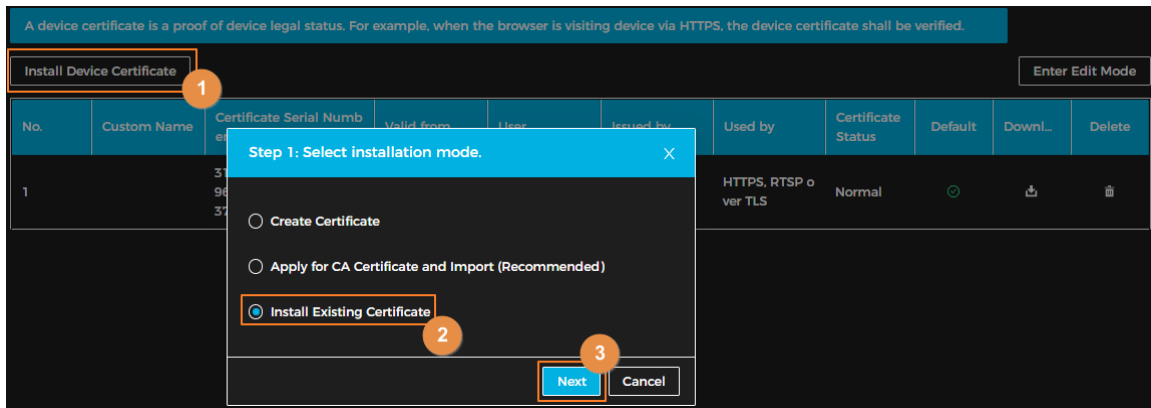
Related Operations

- To edit the name of the certificate, click **Enter Edit Mode** on the **Device Certificate**.
- To download the certificate, click .
- To delete the certificate, click .
- To request the file again, click **Recreate**.
- To import the certificate later, click **Import Later**.

Install an Existing Certificate

Follow the steps below to import an existing device certificate and private key file.

1. Navigate to **Security → CA Certificate → Device Certificate**.
2. Hit **Install Device Certificate**.
3. Click **Install Existing Certificate**, then hit **Next**.



Existing Certificate

4. Click **Browse**, select the certificate and private key file, and input the private key password.
5. Click **Import and Install**. After successful installation, the new certificate appears on the **Device Certificate** page.

Related Operations

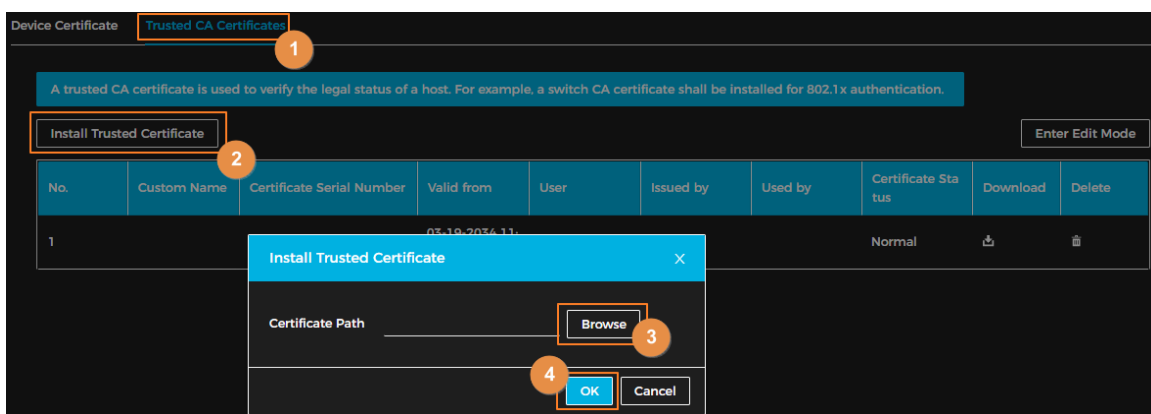
- To edit the name of the certificate, click **Enter Edit Mode** on the **Device Certificate**.
- To download the certificate, click .
- To delete the certificate, click .

Install a Trusted CA Certificate

A trusted CA certificate is a digital certificate used to verify the identity of websites and servers. For example, when using the 802.1X protocol, a CA certificate for switches is required to authenticate their identity. 802.1X is a network authentication protocol that grants port access only after verifying a user's identity and authorizing network access.

Follow the steps below to install a trusted CA certificate.

- Navigate to **Security** → **CA Certificate** → **Trusted CA Certificate**.
- Click **Install Trusted Certificate**.
- Click **Browse** and select the trusted certificate.
- Click **OK**. After successful installation, the new certificate appears on the **Trusted CA Certificates** page.



Install Trusted CA Certificate

Related Operations

- To edit the name of the certificate, click **Enter Edit Mode** on the **Device Certificate**.

- To download the certificate, click .
- To delete the certificate, click .

Sub-Controller Configurations

This section goes over how to initialize and log into sub controllers.

Initialization

Initialize the sub-controller when logging in to the webpage for the first time or after restoring it to factory defaults. See the Initialization section of this manual for more information.

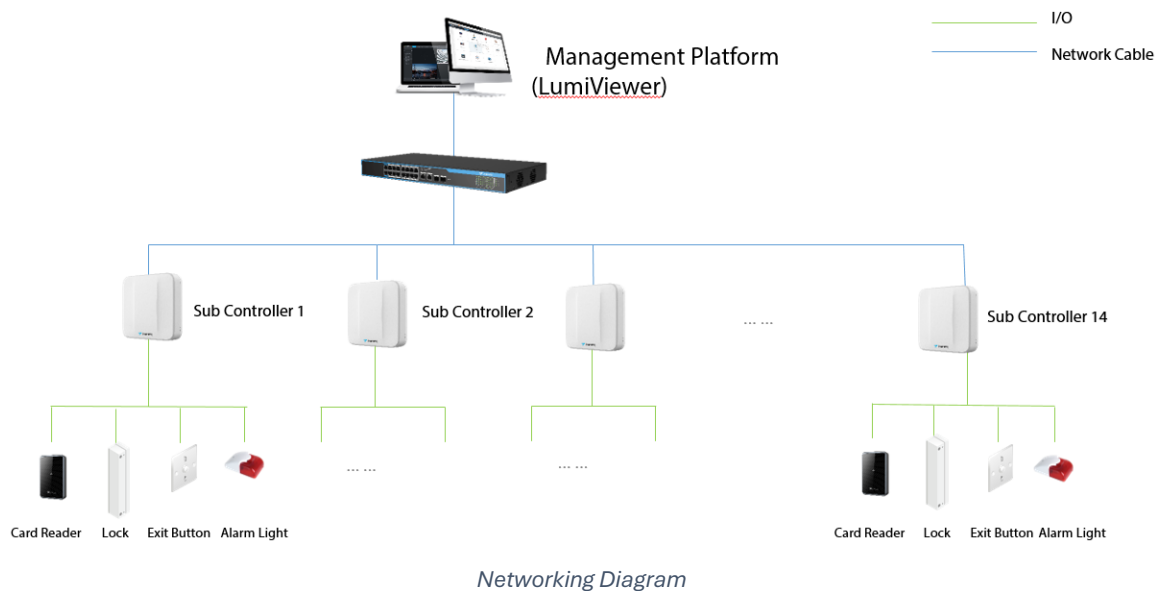
After initialization, change the network mode to **Static**. **DHCP** should only be used during initialization.

Log in to the Device

During the login wizard, set the access controller as a sub-controller. See the Login portion of this manual for more information.

LumiViewer Sub-Controllers

Sub-controllers can be added to a standalone management platform, such as **LumiViewer**, where all sub-controllers can be managed centrally.



1.

Appendix: Cybersecurity Recommendations

Account Management

1. Use complex passwords.

Follow the guidelines below to create a strong password:

- The password should be at least 8 characters long.
- Include at least two types of characters: uppercase letters, lowercase letters, numbers, and symbols.
- Avoid using the account name or its reverse.
- Do not use consecutive characters (e.g., 123, abc).
- Do not use repeating characters (e.g., 111, aaa).

2. Change passwords periodically.

It's advisable to regularly change the device password to minimize the risk of it being guessed or cracked.

3. Allocate accounts and permission appropriately.

Add users based on service and management needs, assigning the minimum necessary permissions

4. Enable account lockout function.

The account lockout function is enabled by default. Keep it enabled to enhance account security; after multiple failed login attempts, the corresponding account and source IP address will be locked.

5. Set and update password reset information in a timely manner.

The device supports a password reset function. To reduce the risk of unauthorized access, update this information promptly if there are any changes. When setting security questions, avoid using easily guessed answers

Service Configuration

1. Enable HTTPS.

It's recommended to enable HTTPS for secure access to web services

2. Change passwords periodically.

If your audio and video data contents are important or sensitive, use encrypted transmission function to reduce the risk of your audio and video data being eavesdropped on during transmission.

3. Allocate accounts and permission appropriately.

It's advisable to disable services such as SSH, SNMP, SMTP, UPnP, and AP hotspot when not in use or required to reduce attack surfaces. If these services are necessary, consider the following safe modes:

- **SNMP:** Use SNMP v3 with strong encryption and authentication passwords.
- **SMTP:** Use TLS for accessing the mailbox server.
- **FTP:** Use SFTP with complex passwords.
- **AP Hotspot:** Use WPA2-PSK encryption with complex passwords.

4. Enable account lockout function.

It is advisable to change the default ports for HTTP and other services to any port between 1024 and 65535 to reduce the risk of being targeted by threat actors.

Network Configuration

1. Enable Allowlist.

It is recommended to enable the allow list function and only permit IP addresses on the allow list to access the device. Be sure to add your computer's IP address and any supporting device IP addresses to the allow list

2. MAC address binding.

It is advisable to bind the gateway's IP address to the device's MAC address to mitigate the risk of ARP spoofing.

3. Build a secure network environment.

To enhance device security and reduce potential cyber risks, the following measures are recommended:

- **Disable Port Mapping:** Turn off the port mapping function on the router to prevent direct access to internal devices from the external network.
- **Network Partitioning:** Based on actual network needs, partition the network. If there is no communication requirement between two subnets, consider using VLANs and gateways to achieve network isolation.
- **Implement 802.1x Access Authentication:** Establish an 802.1x access authentication system to minimize the risk of unauthorized terminal access to the private network.

Security Auditing

1. Check online users.

Check online users regularly to identify illegal users

2. Check device logs.

Review logs to learn about the IP addresses attempting to log in and track key operations performed by authorized users

3. Configure network logs.

The device can only retain a limited number of logs. To save logs for an extended period, it's recommended to enable the network log function to synchronize critical logs to a network log server for future reference

Software Security

1. Update firmware on time.

It is important to update device firmware to the latest version to ensure access to the latest features and security enhancements. If the device is connected to the public network, enable the automatic detection function for online upgrades to receive timely firmware update notifications from the manufacturer

2. Update client software on time.

It is recommended to download and use the latest client software.

Physical Protection

It is recommended to implement physical protection for devices, especially storage devices. Consider placing them in a dedicated machine room or cabinet and establish access control and key management to prevent unauthorized personnel from damaging hardware and peripheral equipment (e.g., USB flash drives, serial ports).