ARMATURA

User Manual

Armatura Horizon Controller
IP-Based Biometric Door Unit

Applicable Models: AHSC-1000, AHDU-Series, AHEB Series

Date: December 2024

Version: 2.6

Copyright © 2024 ARMATURA LLC. All rights reserved.

Trademark

ARMATURA is a registered trademark of ARMATURA LLC. Other trademarks involved in this manual are owned by their respective owners.

Disclaimer

This manual contains information on the operation and maintenance of the Armatura equipment. The copyright in all the documents, drawings, etc. in relation to the Armatura supplied equipment vests in and is the property of Armatura. The contents hereof should not be used or shared by the receiver with any third party without express written permission of Armatura.

The contents of this manual must be read as a whole before starting the operation and maintenance of the supplied equipment. If any of the content(s) of the manual seems unclear or incomplete, please contact Armatura before starting the operation and maintenance of the said equipment.

It is an essential pre-requisite for the satisfactory operation and maintenance that the operating and maintenance personnel are fully familiar with the design and that the said personnel have received thorough training in operating and maintaining the machine/unit/ equipment. It is further essential for the safe operation of the machine/unit/ equipment that personnel has read, understood and followed the safety instructions contained in the manual.

In case of any conflict between terms and conditions of this manual and the contract specifications, drawings, instruction sheets or any other contract-related documents, the contract conditions/documents shall prevail. The contract specific conditions/documents shall apply in priority.

Armatura offers no warranty, guarantee or representation regarding the completeness of any information contained in this manual or any of the amendments made thereto. Armatura does not extend the warranty of any kind, including, without limitation, any warranty of design, merchantability or fitness for a particular purpose.

Armatura does not assume responsibility for any errors or omissions in the information or documents which are referenced by or linked to this manual. The entire risk as to the results and performance obtained from using the information is assumed by the user.

Armatura in no event shall be liable to the user or any third party for any incidental, consequential, indirect, special, or exemplary damages, including, without limitation, loss of business, loss of profits, business interruption, loss of business information or any pecuniary loss, arising out of, in connection with, or relating to the use of the information contained in or

referenced by this manual, even if Armatura has been advised of the possibility of such damages.

This manual and the information contained therein may include technical, other inaccuracies or typographical errors. Armatura periodically changes the information herein which will be incorporated into new additions/amendments to the manual. Armatura reserves the right to add, delete, amend or modify the information contained in the manual from time to time in the form of circulars, letters, notes, etc. for better operation and safety of the machine/unit/ equipment. The said additions or amendments are meant for improvement /better operations of the machine/unit/equipment and such amendments shall not give any right to claim any compensation or damages under any circumstances.

Armatura shall in no way be responsible (i) in case the machine/unit/equipment malfunctions due to any non-compliance of the instructions contained in this manual (ii) in case of operation of the machine/unit/equipment beyond the rate limits (iii) in case of operation of the machine and equipment in conditions different from the prescribed conditions of the manual.

The product will be updated from time to time without prior notice. The latest operation procedures and relevant documents are available on http://www.armatura.us.

If there is any issue related to the product, please contact us.

Armatura LLC. Co., Ltd.

Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005 USA

Phone: +1-650-4556863

For business related queries, please write to us at: sales@armatura.us.
To know more about our global branches, visit www.armatura.us.

About the Manual

This manual introduces the operations of **Armatura Horizon Controller IP-Based Biometric Door Unit**.

All figures displayed are for illustration purposes only. Figures in this manual may not be exactly consistent with the actual products.

Features and parameters with ★ are not available in all devices.

Table of Contents

1. Safety Instructions

1.1 Important Security Instructions

1. Read and follow the instructions carefully before operation. Please keep the instructions for future reference.

2. **Accessories:** Please use the accessories recommended by the manufacturer or delivered with the product. Other accessories are not recommended, including major alarming systems and monitoring systems. The primary alarming and monitoring system should comply with the local applicable fire-prevention and security standards.

3. **Installation cautions:** Do not place this equipment on an unstable table, tripod mount, support, or base, lest the equipment falls and get damaged or any other undesirable outcome resulting in severe personal injuries. Therefore, it is essential to install the equipment as instructed by the manufacturer.

4. All peripheral devices must be grounded.

5. No external connection wires can be exposed. All the connections and idle wire ends must be wrapped with insulating tapes to prevent any damage to the equipment by accidental contact of the exposed wires.

6. **Repair:** Do not attempt to have an unauthorized repair of the equipment. Disassembly or detachment is risky and likely to cause shock. All repairs should be done by a qualified technician.

7. If any of the following cases arise, disconnect the power supply from the equipment first and intimate the technician immediately.

   - *The power cord or connector appears to be damaged.*
   - *Any liquid or material spilled into the equipment.*
   - *The equipment is wet or exposed to inclement weather conditions (rain, snow, etc.).*
   - *If the equipment cannot function properly, even when operated as instructed, please make sure to adjust only the control components specified in the operating instructions. Making incorrect adjustments to other control components may cause damage to the equipment or result in permanent operational failure.*
   - *The equipment falls, or its performance changes dramatically.*

8. **Replacing components:** If it is necessary to replace a component, only an authorized technician can replace the accessories specified by the manufacturer.

9. **Security inspection:** After the equipment is repaired, the technician must conduct a security inspection to ensure the proper working condition of the equipment.

10. **Power supply:** Operate the equipment only with the type of power supply indicated on the label. If there is any uncertainty about the type of power supply, please contact the technician.

Violation of any of the following cautions is likely to result in personal injury or equipment failure. We will not be responsible for the damages or injuries caused thereby.

- Before installation, switch off the external circuit (that supplies power to the system), including locks.
- Before connecting the equipment to the power supply, ensure the output voltage is within the specified range.
- Never connect the power before completion of installation.

1.2 Installation Instructions

1. The conduits of wires under the relay must match with the metal conduits; for other wires, PVC conduits can be used to prevent failure caused by rodent damage. The control panel is designed with proper antistatic, lightning-proof, and leakage-proof functions. Ensure that its chassis and the AC ground wire are correctly connected and that the AC ground wire is physically grounded.

2. It is recommended not to plug/unplug connection terminals frequently when the system is powered on. Be sure to unplug the connection terminals before starting any relevant wiring job.

3. Do not detach or replace any control panel chip without permission, and an unauthorized operation may cause damage to the control panel.

4. It is recommended not to connect any other auxiliary devices without permission. All non-routine operations must be communicated to our engineers in advance.

5. A control panel should not share the same power outlet with any other high-current device.

6. It is recommended to install card readers and buttons at the height of **55.12 inches to 59.06 inches (1.4m to 1.5m)** above the ground or subject to customers' usual practice for proper adjustment.

7. It is recommended to install control panels in easily accessible locations to facilitate maintenance, such as in a well-ventilated electrical room.

8. For safety reasons, it is strongly recommended that the exposed part of any connection terminal should not exceed **0.16 inches (4mm)** in length. Consider using specialized clamping tools to prevent short-circuits or communication failures caused by accidental contact with excessively exposed wires.

9. To ensure access control event records are saved, regularly export the data from control panels.

10. Prepare appropriate countermeasures for unexpected power failures based on application scenarios, such as selecting a power supply with an uninterruptible power supply (UPS) system.

11. If an RS-485 reader is externally connected and shares the power supply with the device (Note: The control panel does not support fingerprint verification of RS-485 reader), it is recommended to keep the connection between the RS-485 reader port and the reader no longer than **328 ft (100m)**. Alternatively, it is advised to use a separate power supply for the reader.

12. To safeguard the access control system from any self-induced electromotive force generated by an electronic lock during switching off/on, it is essential to **connect a diode in parallel** (FR107, supplied with the system) with the electronic lock. This diode will dissipate the self-induced electromotive force during onsite connection, ensuring the proper application of the access control system.

13. It is advisable to use separate power supplies for the electronic lock and the control panel.

14. It is recommended to use the power supply provided with the system as the control panel power supply.

15. In locations with significant magnetic interference, it is advisable to use galvanized steel pipes or shielded cables, and ensure proper grounding is implemented.

16. Wiring methods used shall be in accordance with the National Electrical Code, ANSI/ NFPA 70.

2. Overview

2.1 Packing List

Please ensure that your box contains all the items listed. If any pieces are missing, kindly contact your distributor for assistance. It is advisable to retain the original box and packing materials in case you need to ship your equipment in the future.

AHSC-1000

- ARMATURA Horizon Controller (AHSC-1000) (1pc)
- 35mm DIN rail adapter: T=0.03" 9.39"x1.34"x0.25" (T=0.7mm 238.5x35x6.3mm) (1pc)
- WIFI external antenna (3pcs)
- Screwdriver (1pc)
- Fast Recovery Diode(FR107) (4pcs)
- Grub screw/Countersunk 7#1-5/8inch (KA3.6x40mm) self – tapping screws (2pcs) and Anchors (2pcs)

  – for mounting directly to a wall
- Grub screw/Countersunk TM3x6mm screw (1pc)

AHDU-1160/1260/1460

- ARMATURA Horizon Controller (AHDU-1160/1260/1460) (1pc)
- 35mm DIN rail adapter: T=0.03" 9.39"x1.34"x0.25" (T=0.7mm 238.5x35x6.3mm) (1pc)
- WIFI external antenna (3pcs)
- Screwdriver (1pc)
- Fast Recovery Diode(FR107) (4pcs)
- Grub screw/Countersunk 7#1-5/8inch (KA3.6x40mm) self – tapping screws (2pcs) and Anchors (2pcs)

  – for mounting directly to a wall
- Grub screw/Countersunk TM3x6mm screw (1pc)

AHEB-0808/AHEB-1602/AHEB-1616

- ARMATURA expansion board (AHEB-0808/AHEB-1602/AHEB-1616) (1pc)
- Screwdriver (1pc)
- Fast Recovery Diode(FR107) (8pcs)
- Mounting screws (4pcs)
- Hexagonal copper column (4pcs)

2.2 Introduction

The ARMATURA Horizon Controller Series is an access control system developed by ARMATURA LLC. It is designed for the enterprise-level market. Particularly for large projects with a large number of access points, and stringent security requirements. The entire product series offers comprehensive improvements in hardware, architecture, and system security encryption.

2.3 Features

- Ultimate Authentication Performance
- PoE and 3rd Party Integration
- Threat Levels and Port Failover
- Advanced Access Control Functions
- Supervised Inputs and NC/NO Configurable Ports

Key Features

Ultimate authentication performance

- Supports up to 400,000 (1:1) RFID card/mobile credentials and 100,000 (1:N) fingerprints authentications in a single controller.

PoE

- Supports Power-over-Ethernet (PoE) 802.3at/ 9-24VDC from power sourcing equipment (PSE) according to PoE 802.3at/af standards.

Threat Levels

- Unlimited threat levels, which are used to instantly adjust users access right during lockdown and lockout.

3rd Party Integration

- Supports various reader protocols, including ARMATURA Explorer series readers, along with 3rd party Wiegand and OSDP readers. ARMATURA One provides a RESTful API for seamless integration with 3rd Party software.

Advanced Access Control Functions

- The controller supports advanced access control functions such as multi-frequency RFID card support, multi-biometric authentication support, mobile credential support, anti-passback, multi-level authentication and cross panel linkage (global linkage).

Port Failover

- The AHDU controller series has dual ethernet ports. If the primary communication port fails, it will then switch to the secondary port automatically (the controller supports separate network configurations for both ports). 100Base-TX Ethernet data transfer is included on the AHDU controller. 100Base-TX communication between the AHDU security core allows users to take full advantage of high-speed network technology.

- The AHDU controller series has 3 RS-485 ports on the board, which support port failover function dedicated on ports 2 & 3. If one of the RS-485 connections experiences problems, the other port will activate automatically to avoid disconnection.

Supervised Inputs

- The AHDU controller series is equipped with 4 state-monitoring inputs, which gradually avoids short circuit attacks. The AHDU controller can detect abnormal changes as low as 5% Ohms in the circuits and filter out all possible attacks.

- REX inputs and dedicated fire alarm inputs are independently managed by isolated microchips to ensure these inputs can work normally under various extreme and catastrophic situations, even if the motherboard isn't functioning properly

NC / NO Configurable Ports

- All on-board output ports can be configured to change their NO/NC status through the ARMATURA One security platform, which greatly enhances the flexibility.

Scalable

- At the maximum capacity, up to 384 inputs are supported between boards through OSDP V2.2 connection (when using AHEB-0216 IO expansion board). The AHDU can also act as an edge device under the AHSC-1000 security core, which supports cascading to manage up to 128 doors under single AHSC-1000 controller.

Innovative MQTT based communication protocol

- MQTT is a lightweight messaging protocol designed for IoT devices and its characteristics make it a perfect solution for intelligent security systems. This enables the controller to communicate with more edge devices (Door Unit, reader, sensor, etc.) under the same network environment.

Advanced Communication

- The serverless design enables the controller to operate independently.

- Peer-to-peer cross-controller linkage through the AHSC-1000 security core allows communication between controllers and can be active while the ARMATURA One server is unavailable. All the preset linkages/global linkage can operate normally.

- With the onboard webserver design, the controller can be configured and programmed through the Armatura Connect mobile app and web browser through TCP/IP connection. The simple diagnostics can also be done by the built-in monitor and keypad on the controller.

Advanced Security Protocols

- Connection between Software and Device: MQTT+One Way SSL (Two Way SSL optional), AES 256.
- Connection between Primary and Secondary Controller: MQTT+Two Way SSL, AES256.
- RS-485: OSDP Secure Channel v2.2, AES128.
- Controller Webserver: HTTPS with TLS 1.2.
- Crypto Chip Storage: EAL5+ chip (anti-tampering, anti-electronic attack, anti-copying) for securing important data on the controller and reader. Ensures private data desensitization and encrypted storage.
- The controller webserver has successfully undergone penetration testing and vulnerability assessment conducted by reputable brand products. All identified medium and high-risk vulnerabilities have been mitigated and resolved.
- Supports IP/MAC address filtering functions, and VLAN isolation to enhance cybersecurity standards.

Level

- Destructive attack level: I
- Line security level: II
- Endurance level: IV
- Standby power level: I

2.4 General Information

	AHDU-1160	AHDU-1260	AHDU-1460
Primary Power	PoE 802.3at/af / 9 - 24 VDC ± 20%, 550 mA maximum (reader current not included)		
PoE	PoE Standard: IEEE 802.3at PoE Input Voltage: DC50-57 V PoE Input Current: 10-600 mA		
Primary Host Communication	Ethernet: 100Base-TX 256bit AES* symmetric encryption for Controller to Server and Inter-Controller communications		
Secondary Host Communication	Bluetooth 4.2+HS, BLE(Only versions produced after June 2024 are supported)		
Third Host Communication	Wi-Fi IEEE 802.11ac 5GHz , or 2.4GHz/5GHz IEEE 802.11n 256bit AES* symmetric encryption for Controller to Server and Inter-Controller communications		

Ethernet network connection	Port 1: Ethernet: 100Base-TX Port 2: Ethernet: 100Base-TX (Configurable for Port Failover)		
RS-485 connection	Port 1: RS-485 standard / OSDP V2.2 Port 2: RS-485 standard / OSDP V2.2 Port 3: RS-485 standard / OSDP V2.2 (Configurable for Port Failover dedicated on port 2 & 3)		
Number of Ports	2*TCP/IP 3*RS-485 2*wiegand	2*TCP/IP 3*RS-485 4*wiegand	2*TCP/IP 3*RS-485 4*wiegand
Inputs	4 state supervision, resistor values (5% tolerance), Normally open contact: use 1.2k, 2.2k. 4.7k or 10k/ Normally closed contact: use 1.2k, 2.2k. 4.7k or 10k/ Dedicated Panel Tamper IO Input* Dedicated Mircochip Control Fire Alarm IO Input & REX Input for catastrophic situation		
Outputs	1 relay, 1* Form-C with dry contacts	2 relay, 2* Form-C with dry contacts	4 relay, 4* Form-C with dry contacts
Normally Open Contact Rating	5A @ 30Vdc resistive		
Normally Closed Contact Rating	5A @ 30Vdc resistive		
On-Board Monitor	Size: 2.4", Resolution: 320*240, TFT Monitor Quickly view status of board, connected doors and for configuration information display		
On-Board WebServer	Webserver for System Configuration and Management Dashboard for Controller Status Monitoring, Device Connection Status Monitoring & Configuration, Performance Status, server Primary Controller Setting, Network Status Monitoring & Setting, IP Access Filter, SSL / TLS Certificates Setting, Access Log Export, Controller Reset, Debug Status Monitoring, Operation Log Monitoring, User Management, Date & Time Setting, Daylight Saving Time Setting, NTP server Setting, General Status, Controller Information		
RFID Card Capacity	400,000 (1:N) / 800,000 (1:1)		
Maximum RFID Card Number Length	Supports up to 512bits card number length		
Mobile Credentical Capacity	400,000 (1:N) (Bluetooth) 400,000 (1:N) (NFC) 400,000 (1:N) (Dynamic QR Code)		
Fingerprint Capacity	100,000 (1:N)		
Transaction Buffer	300,000 Events		

Access Level	100,000 Levels		
On-Board Access Point Control	1 Access point on board	2 Access point on board	4 Access point on board
On-Board Reader Support	3 (OSDP over RS-485) or 2 (wiegand) with on-board IO	3 (OSDP over RS-485) or 4 (wiegand) with on-board IO	3 (OSDP over RS-485) or 4 (wiegand) with on-board IO
Maximum Access Points	1	2	4
Maximum Readers	2	4	8
Maximum Inputs	388 (using Armatura AHEB-0216)		
Maximum Outputs	388 (using Armatura AHEB-0216)		
Maximum IO Board	24pcs (3*High Speed RS-485 communication)		

2.5 Power Specification

2.5.1 Product Main Specifications

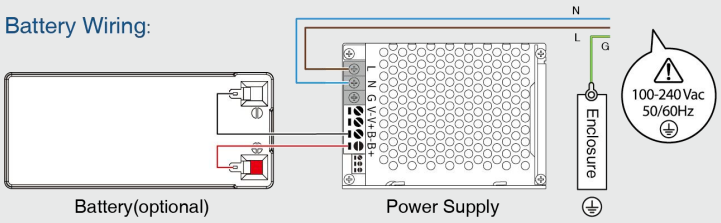
Items	Specifications
Maximum Output Power	68.5W
Input Voltage Range	100Vac to 240Vac
Output Voltage	12Vdc to 14Vdc
Maximum Output Current	0.5A, 4.5A

2.5.2 Environmental Conditions

Items	Specifications
Operating Temperature	-20°C to 50°C
Storage Temperature	-40°C to 80°C
Relative Humidity	10% to 95%, non-condensing
Heat Dissipation Method	Natural Cooling

2.5.3 Electrical Characteristics

Items	Specifications	Remarks
Input Characteristics		
Rated Input Voltage	100Vac to 240Vac	
Input Voltage Range	90Vac to 264Vac	Normal Operation
Input Voltage Frequency	47Hz to 63Hz	
Maximum Input Current	1.5A	90Vac
Input Inrush Current	≤30A	110Vac, Full capacity, 25°C
	≤60A	220Vac, Full capacity, 25°C
Output Characteristics		
Output Rated Voltage	13.7Vdc	
No-Load Output Voltage Range	13.6Vdc to 13.8Vdc	Battery full voltage
Maximum Output Current	5A	
Output Power	0W to 68.5W	Maximum battery charge output included
Output Efficiency	⩾85%	Rated Voltage 220Vac / Rated Load
Protecting Characteristics		
Output Overvoltage	20.55V	Not recoverable after overvoltage protection.
Current Limiting Protection	6A to 9A	Automatic recovery is possible with other circuits carrying full load at the same time.
Output Short Circuit Protection	Can be short-circuited for a long time without damage, short-circuit removal can be automatically restored.	

Battery Management		
Constant Current Charge Output	0.5A ± 0.2A	No output from the battery terminal when no battery is connected. When the battery voltage is greater than 6V ± 0.3V, battery charging is turned on.
Battery Charging Alert	Normal charging output, green light flashes. Green light is always on when the battery is fully charged.	When the battery is charging, the charging indicator is always on when the battery voltage reaches 13.5V ± 0.2V.
	Battery Wiring:  	
Ac Indicator	The green light is on when the AC input is normal and off when the battery is discharged.	
Reverse Battery Protection	Reverse battery connection does not damage any components, light up red LED3.	
Battery Pre-Undervoltage Alarm	BAT_FAIL outputs low when the battery voltage is less than 10.8V ± 0.2V.	
Battery Overdischarge Protection	The output is turned off when the battery voltage is less than 10.2V ± 0.2V.	
Battery Output Short Circuit Protection	Can be short-circuited for a long time without damage, short-circuit removal can be automatically restored.	

2.6 Appearance

2.6.1 AHSC-1000 Primary Controller

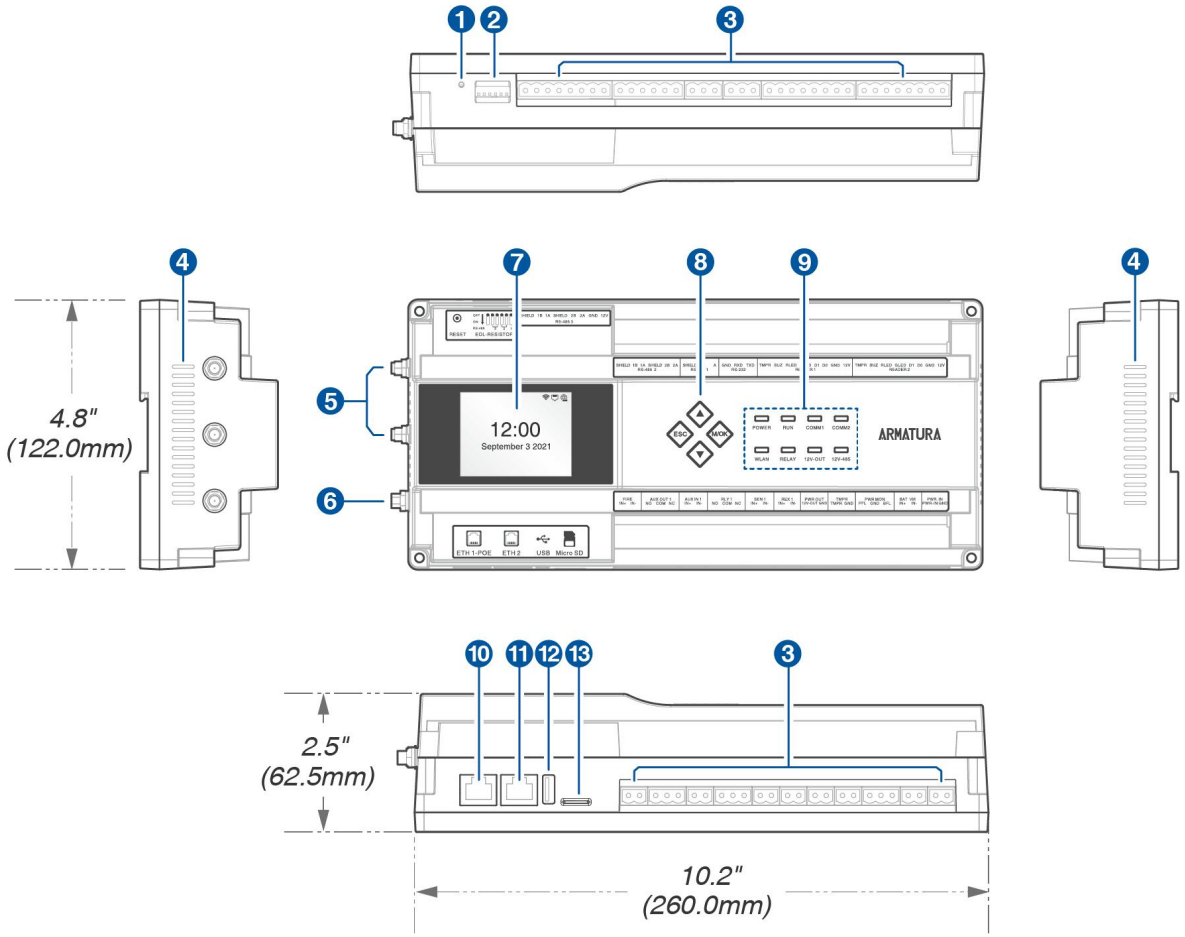


Figure 2-1 AHSC-1000 Primary Controller Appearance

NO.	Descriptions	NO.	Descriptions
1	Reset Button	8	Keypad
2	DIP Switch	9	Status LED Indicator
3	Terminal Block	10	Ethernet 1-POE
4	Heat Dissipation Hole	11	Ethernet 2
5	Wi-Fi Antenna Port	12	USB Port*
6	Bluetooth Antenna Port	13	Micro SD Slot
7	2.4" TFT LCD		

* **Note:**Hardware reservation function is currently not supported.

2.6.2 AHDU-1X60 Secondary Controller

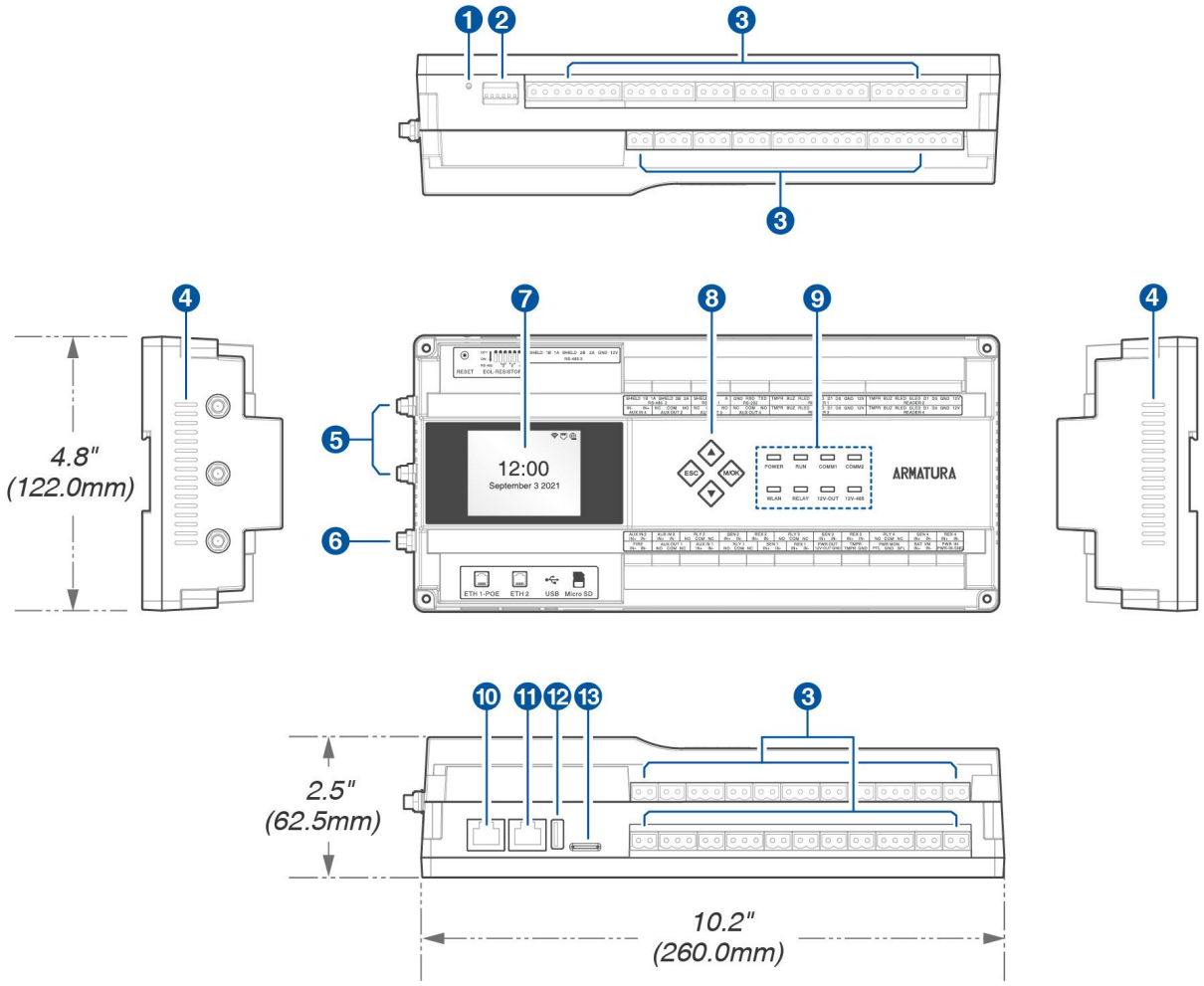


Figure 2-2 AHDU-1X60 Secondary Controller Appearance

NO.	Descriptions	NO.	Descriptions
1	Reset Button	8	Keypad
2	DIP Switch	9	Status LED Indicator
3	Terminal Block	10	Ethernet 1-POE
4	Heat Dissipation Hole	11	Ethernet 2
5	Wi-Fi Antenna Port	12	USB Port
6	Bluetooth Antenna Port	13	Micro SD Slot
7	2.4" TFT LCD		

Remarks:

- ***Reset Button:*** *To restart the device, press and hold the reset button for **1 to 5** seconds. To restore the factory settings, press and hold the reset button for more than **5** seconds.*
- ***DIP Switch:*** *When connecting an RS-485 reader for long-distance communication, it is necessary to enable End of Line (EOL) and configure the EOL resistance of RS-485 using DIP switches.*

2.6.3 AHEB-0808 Expansion Board

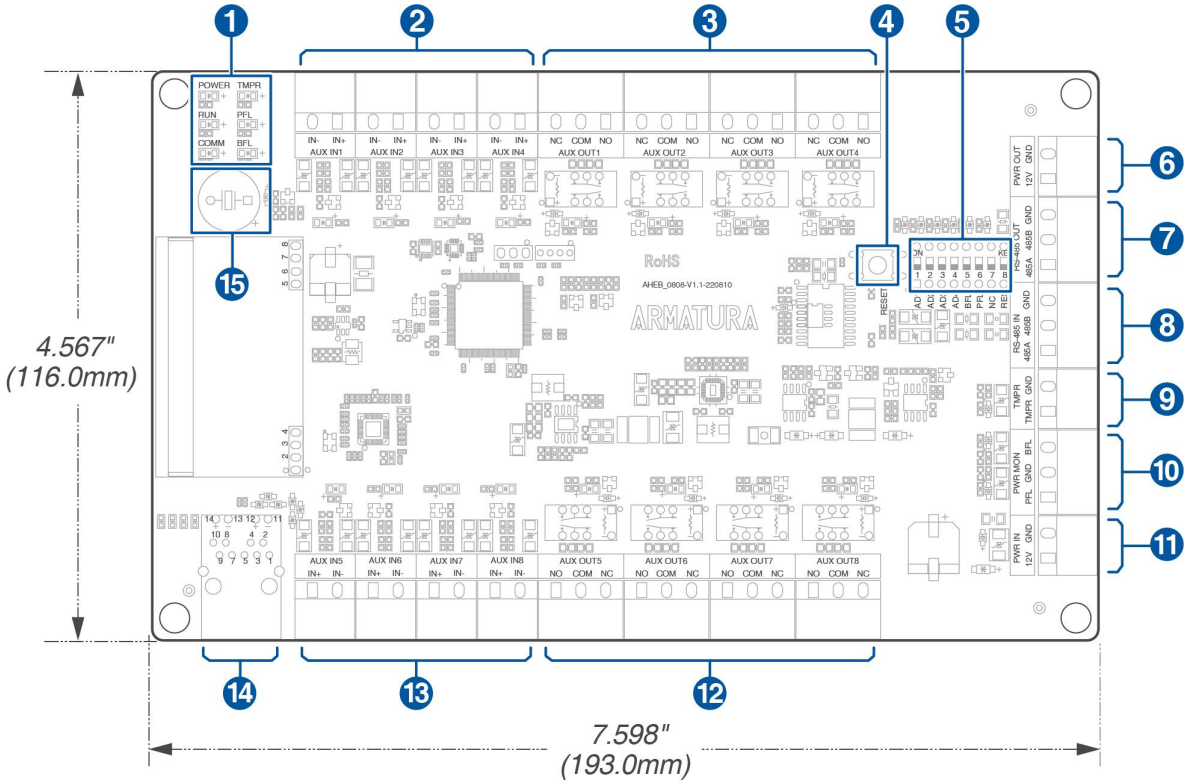


Figure 2-3 AHEB-0808 Appearance

NO.	Descriptions	NO.	Descriptions
1	Status LED Indicator	9	Tampering Alarm
2	Auxiliary Input (1-4)	10	Power MON
3	Auxiliary Output (1-4)	11	Power Input
4	Reset Button	12	Auxiliary Output (5-8)
5	DIP Switch	13	Auxiliary Input (5-8)
6	Power Output	14	Ethernet Port
7	RS-485 Out	15	Buzzer
8	RS-485 In		

2.6.4 AHEB-1602 Expansion Board

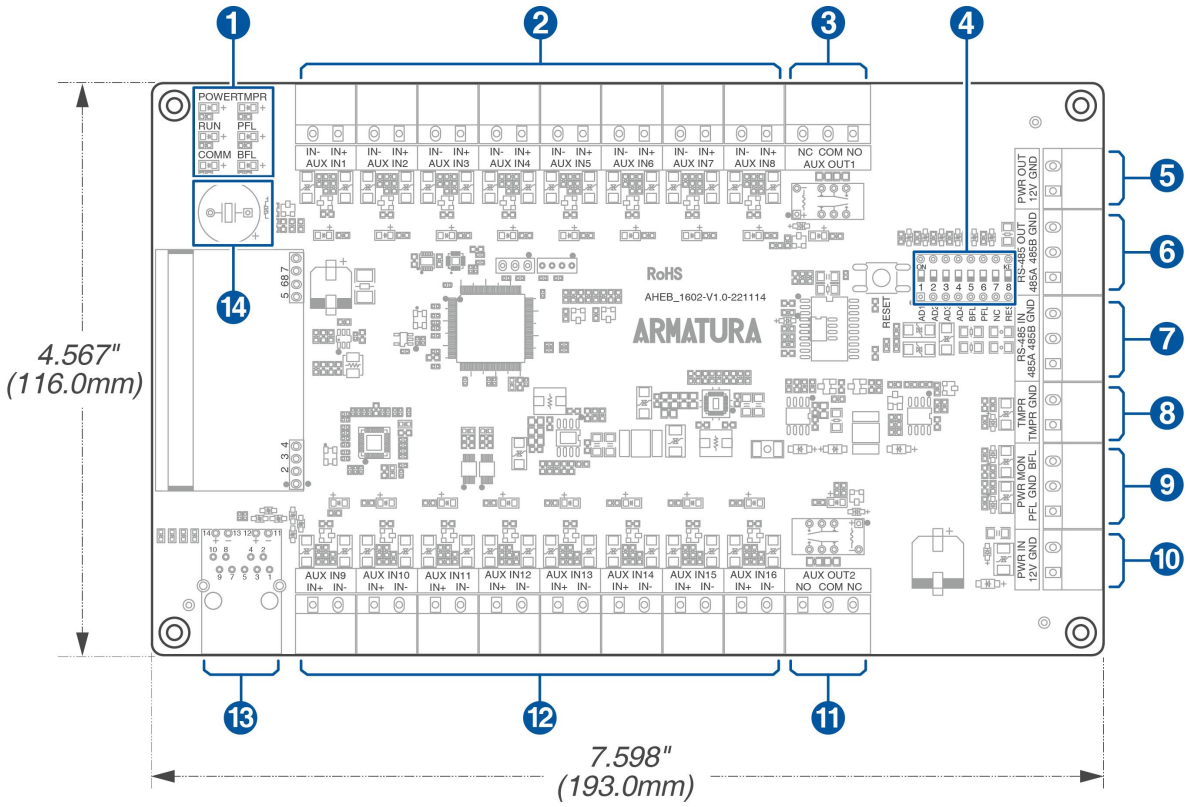


Figure 2-4 AHEB-1602 Appearance

NO.	Descriptions	NO.	Descriptions
1	Status LED Indicator	8	Tampering Alarm
2	Auxiliary Input (1-8)	9	Power MON
3	Auxiliary Output 1	10	Power Input
4	DIP Switch	11	Auxiliary Output 2
5	Power Output	12	Auxiliary Input (9-16)
6	RS-485 Out	13	Ethernet Port
7	RS-485 In	14	Buzzer

2.6.5 AHEB-1616 Expansion Board

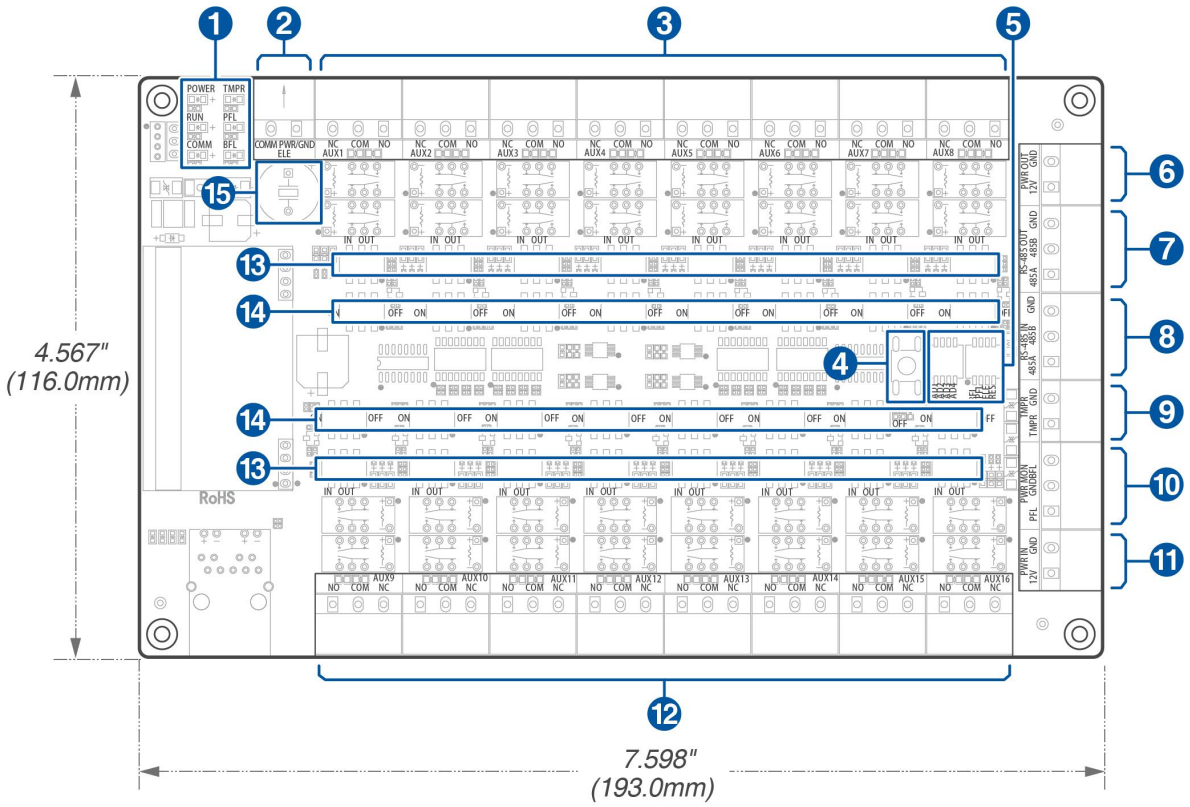
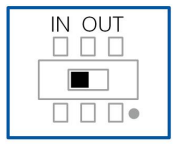


Figure 2-5 AHEB-1616 Appearance

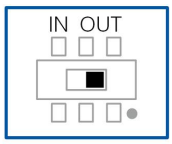
NO.	Descriptions	NO.	Descriptions
1	Status LED Indicator	9	Tampering Alarm
2	Power ELE	10	Power MON
3	Auxiliary Input / Output (1-8)	11	Power Input
4	Reset Button	12	Auxiliary Input / Output (9-16)
5	DIP Switch	13	Auxiliary Input / Output Toggle Switches*
6	Power Output	14	Key Detection Switches
7	RS-485 Out	15	Buzzer
8	RS-485 In		

Remarks:

- **Users can switch ports to input or output ports by toggling the auxiliary input/output toggle switch. When the switch is flipped to IN for input port, NO corresponds to IN+ and NC corresponds to IN-. When the switch is toggled to OUT, it is the output port.*



Auxiliary Input



Auxiliary Output

2.6.6 ENC1 Enclosure (optional)

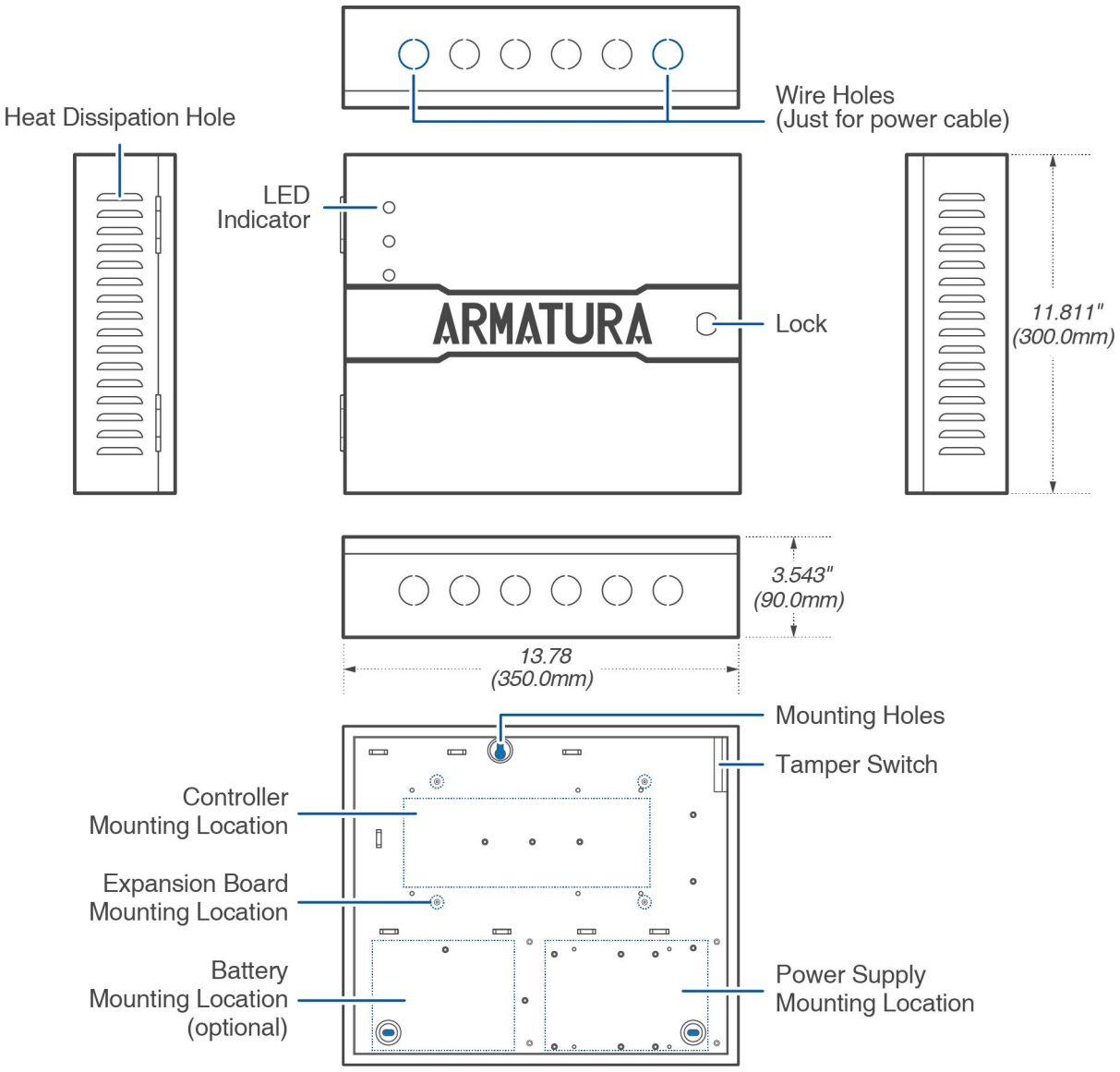


Figure 2-6 ENC1 Enclosure Appearance

Remarks:

- ***Input Voltage:*** *100 - 240 VAC*
- ***LED Indicator:*** *There is 3 LED indicator present in the* enclosure*, they are POWER (Red), RUN (Green) & COMM. (Yellow).When the device is powered on, normally the POWER indicator (Red) is lit constantly and the RUN indicator(Green) flashes slowly (indicating the system is functioning normally). COMM. indicator (Yellow) flashes when the system is communicating with other devices (e.g., PC). When the indicator is flashing rapidly it indicates data transmission. When the indicator is flashing slowly, it indicates real-time monitoring status.*
- ***Wire Holes (Just for power cable):*** *Other low voltage cables should not be routed through it. And the power cables need to be separated from other cables.*

3. Installation and Connection

Ensure that the device is installed following the provided installation instructions. Failure to do so may result in voiding of the devices warranty.

3.1 Installation Procedure

Users have the flexibility to select from various installation methods based on their specific requirements.

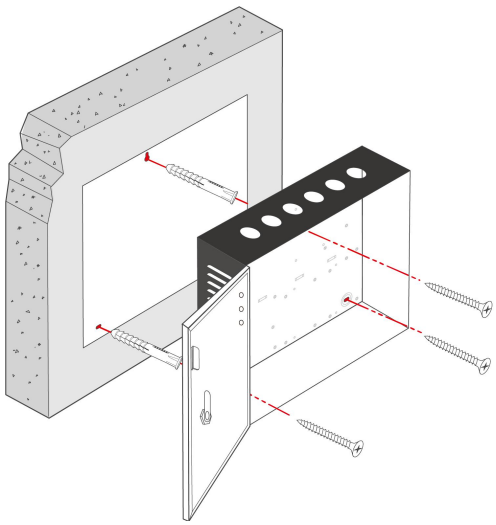
Remarks:

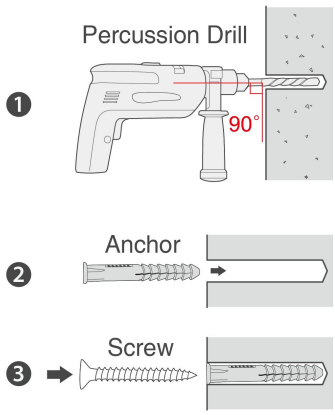
1. *The AHDU Series (1160/1260/1460) share the same casing, installation, and wiring methods. This document will refer to the AHDU-1460 model as a reference for wiring and connections.*
2. *The images in this manual are for reference purposes only. The actual product may vary depending on the model.*

3.1.1 Installing the ENC1 enclosure (optional) on the wall

Users can refer to the following installation steps to install the ENC1 enclosure (optional) on the wall.

1. Attach the mounting template sticker to the wall, and drill three holes according to the mounting paper. The recommended mounting height is approximately **114 inches (2.9 meters)** above the ground, which can be adjusted according to actual needs. Take care to leave at least **3.937 inches (100 mm)** on the left side of the enclosure.
2. Position the anchors in the designated mounting holes.
3. Next, secure the enclosure using the provided self-tapping screws, as demonstrated in the illustration below.





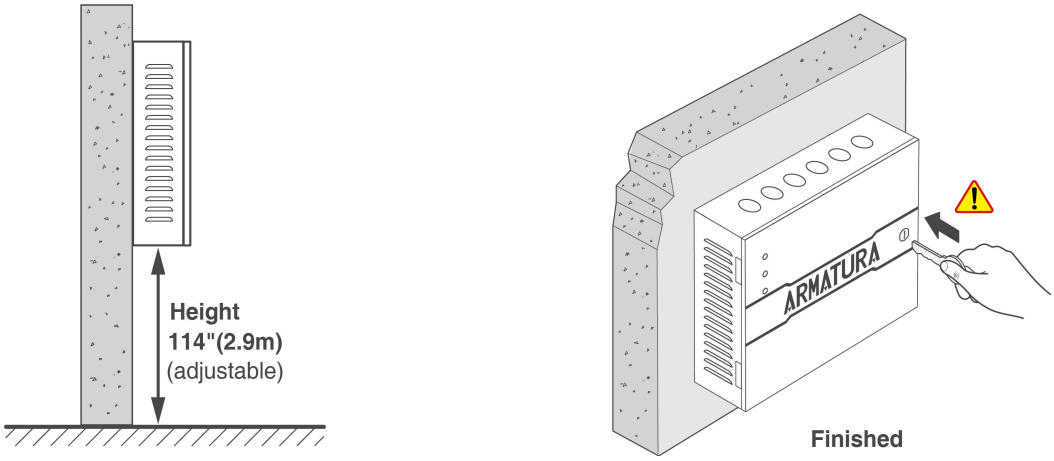


Figure 3-1 Installation the ENC1 enclosure on the wall

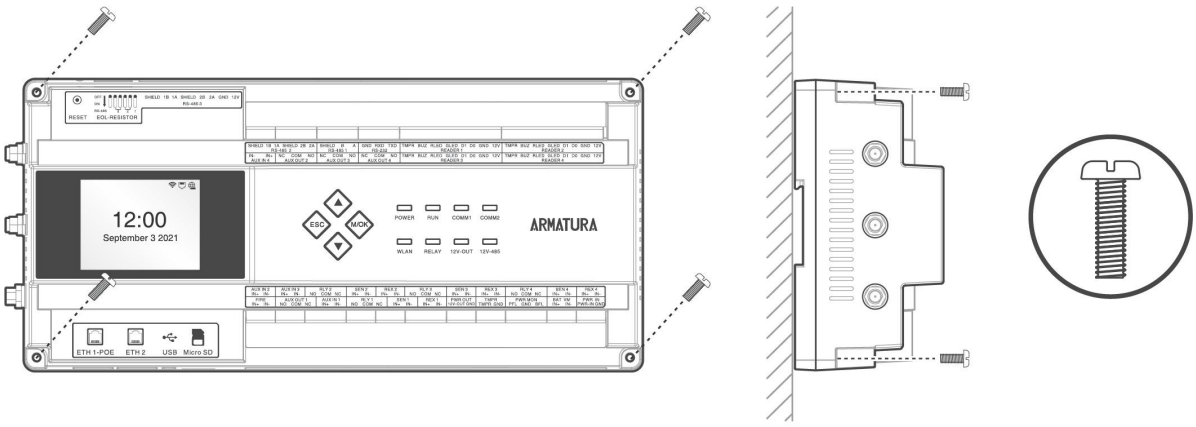
Notes:

- *The enclosure is equipped with tamper monitoring. Please ensure that the enclosure remains closed while the equipment is in normal operation.*
- *To ensure the security of the equipment, make sure the enclosure is locked during normal operation of the device. The key is kept by the manager.*

3.1.2 Installation with screws

Mount the controller or expansion board securely to the enclosure or a flat surface using screws, as illustrated in the figure below.

Mount the controller on a flat surface using screws



Mount the expansion board to the enclosure using screws

1. Mount the hexagonal copper pillar securely to the enclosure first.
2. And then secure the expansion board to the hexagonal copper pillar with screws as, illustrated in the figure below.

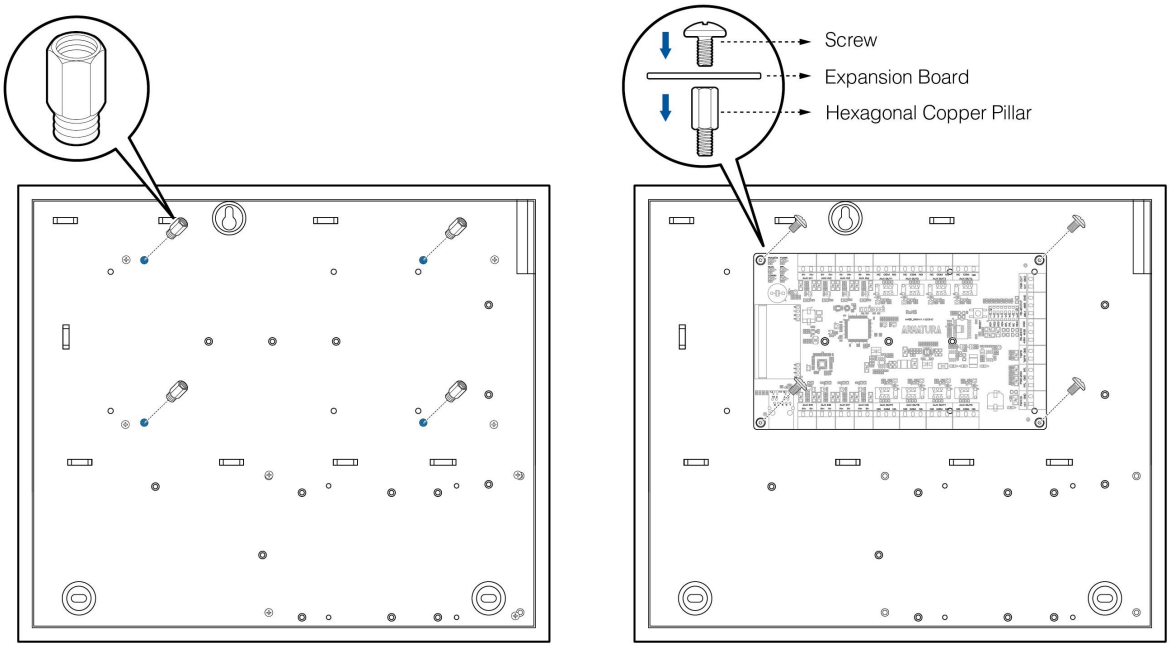


Figure 3-2 Schematic diagram of screw installation

Remarks:

- ***Screw specification:*** *Cross recessed pan head screws M3.5*23mm*
- ***Applicable Models:*** *AHSC-1000, AHDU-1160/1260/1460, AHEB-0808, AHEB-1602, AHEB-1616*

3.1.3 Installation with original 35mm DIN rail

1. Mount the original DIN rail directly onto the enclosure or a flat surface, as illustrated in the figure below.

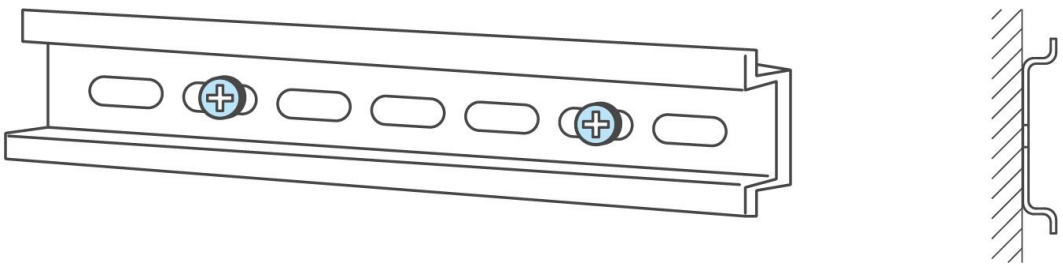


Figure 3-3 Mount the DIN rail

2. Engage the hooks on the top of the controller with the DIN rail and firmly press the controller onto the rail until it locks into place, as depicted in **Figure 3-4** below.

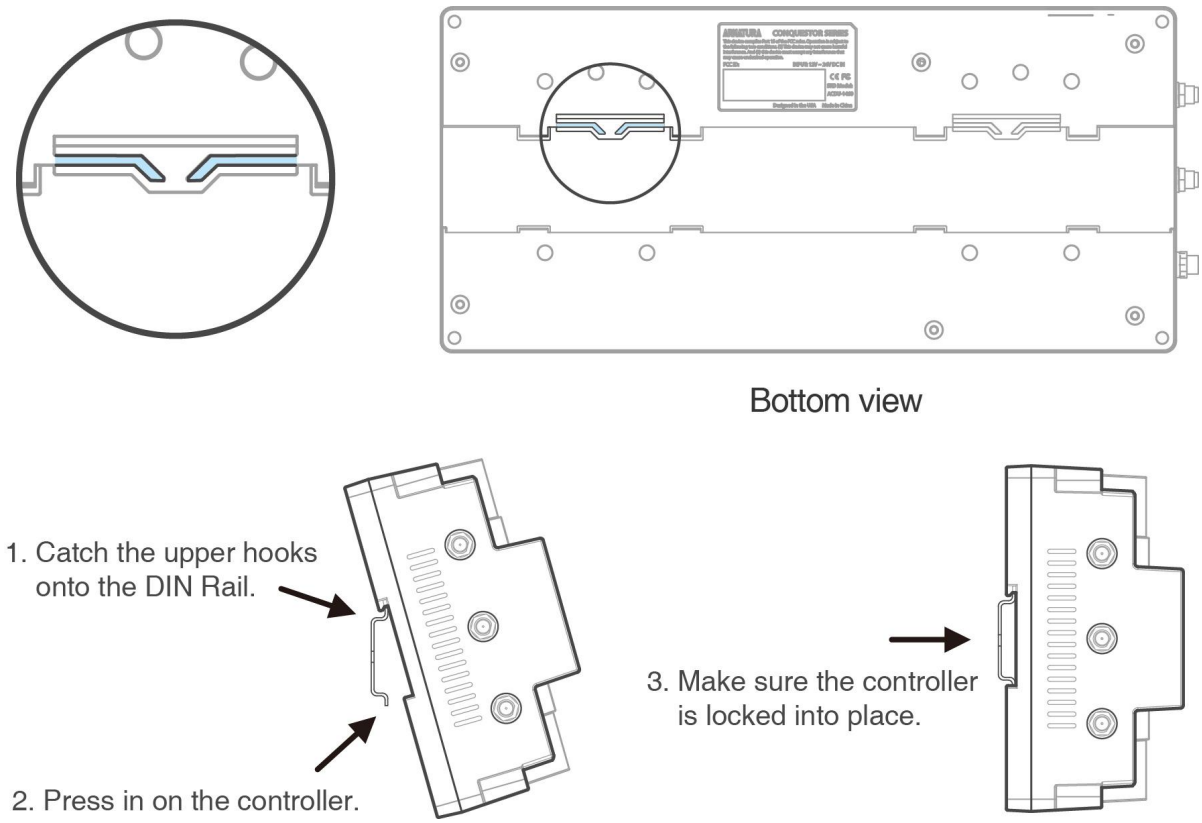


Figure 3-4 Mount the controller to the DIN rail adapter

Remarks:

- ***DIN rail specification:*** *T=0.03" 9.39"*1.34"*0.25" (T=0.7mm 238.5mm*35mm*6.3mm)*
- ***Applicable Models:*** *AHSC-1000, AHDU-1160/1260/1460*

3.1.4 Installation with extended 35mm DIN rail adapter

If required, users have the option to purchase a third-party rail adapter to mount the controller, and then securely snap it onto the original 35mm DIN rail, as demonstrated in the figure below.

1. Refer to the steps of section 3.1.3 to install the original DIN rail to the enclosure or flat surface.

2. Mount the two extended 35mm DIN rail adapters in the locations, as shown in **Figure 3-5** below.

3. Snap the mounted units into the original 35mm DIN rail, as shown in **Figure 3-6** below.

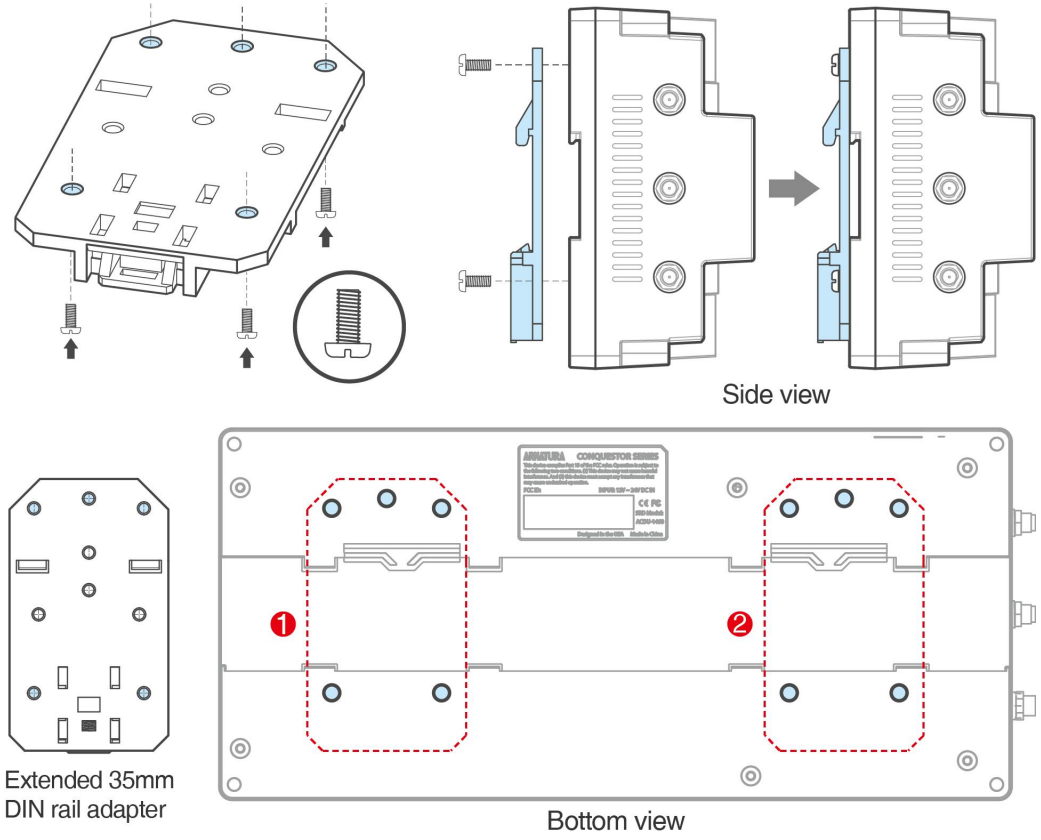


Figure 3-5 Mount the extended 35mm DIN rail adapters to the controller

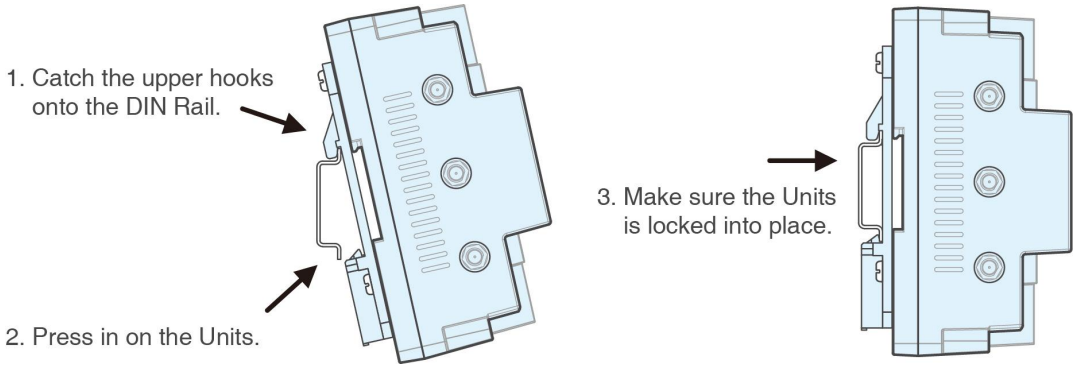


Figure 3-6 Mount the Units to the original 35mm DIN rail

Remarks:

- ***Recommended the extended 35mm DIN rail adapter specifications:***

  UTA89 Phoenix Contact, Part Number: 2853970. Link URL:
  https://www.phoenixcontact.com/zh-cn/products/din-rail-adapter-uta-89-2853970.
- *Users have the option to purchase third-party rail adapters as required. Please note that the pictures in the manual are for reference purposes only.*
- ***Screw specification:*** *Cross recessed pan head screws M3*7mm*
- ***Applicable Models:*** *AHSC-1000, AHDU-1160/1260/1460*

3.1.5 Installing the Power Supply

1. Secure the power supply to the power supply mounting plate with screws from the bottom.

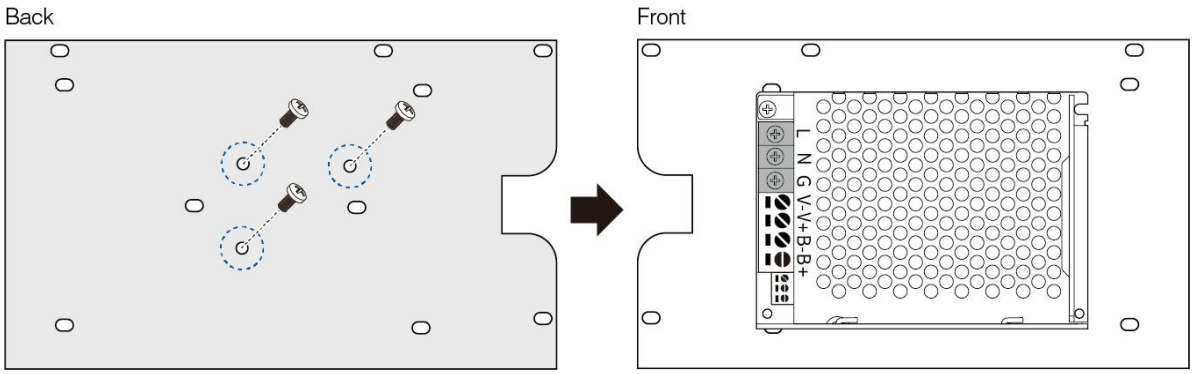


Figure 3-7 Mount the power supply to the mounting plate

2. Then mount the hexagonal copper pillar securely to the enclosure.

3. Finally, screw the mounting plate to the hexagonal brass post with screws, as illustrated in the figure below.

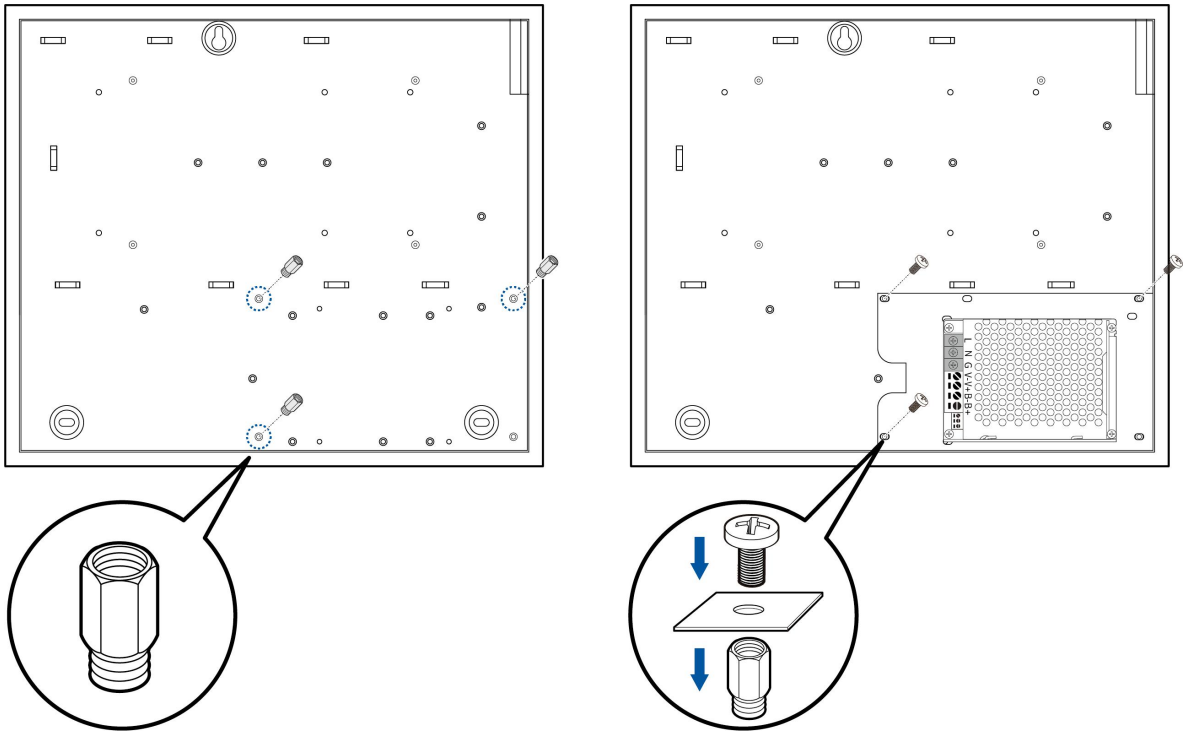


Figure 3-8 Mount the power supply mounting plate to the enclosure

3.1.6 Installing the Backup Battery (optional)

1. Place the backup battery in the appropriate location in the enclosure as shown in the figure.
2. Place the fixing bracket in the manner shown below and secure it with screws.

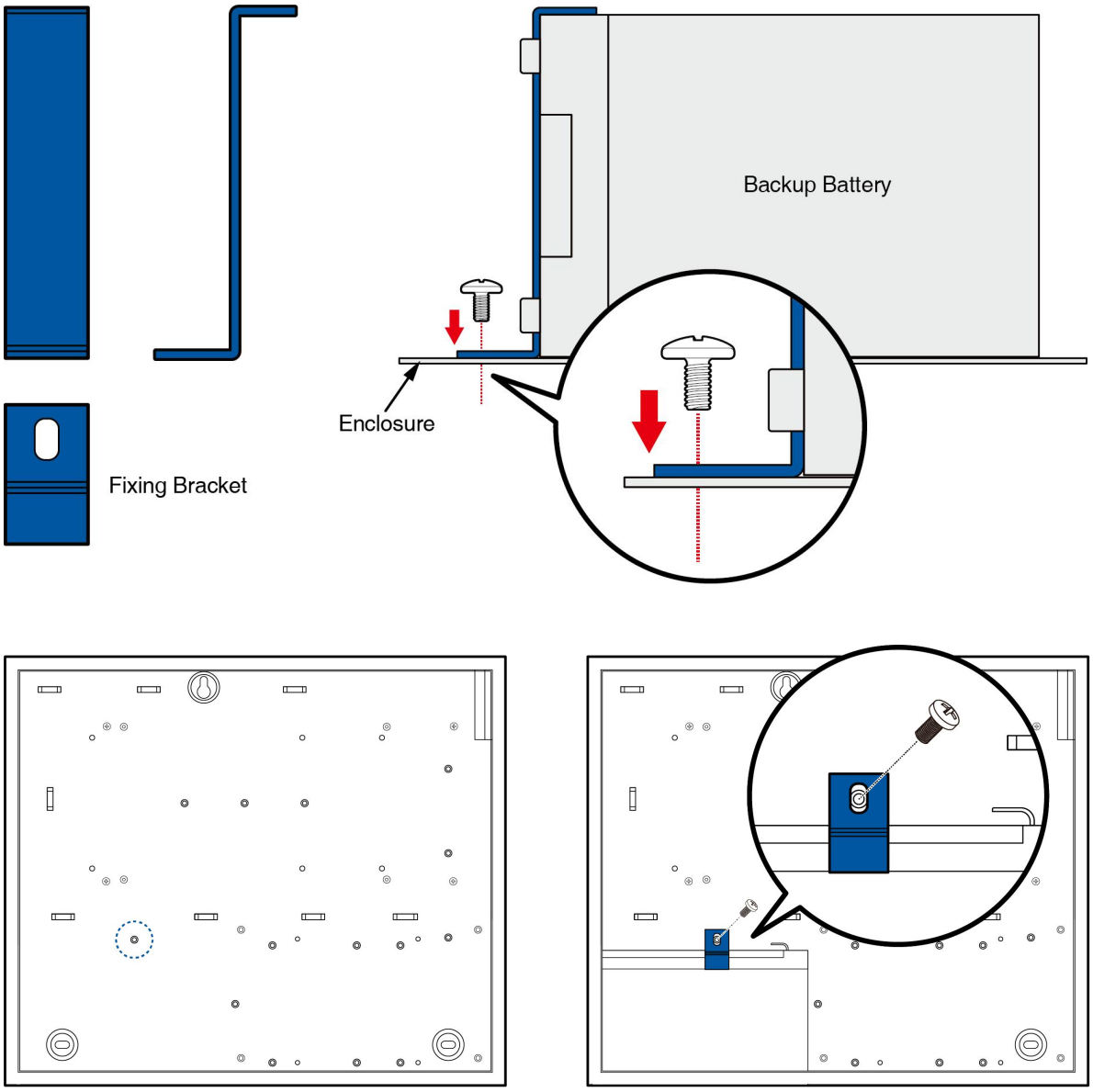


Figure 3-9 Mount the backup battery (optional) to the enclosure

3.2 Access Control System Installation

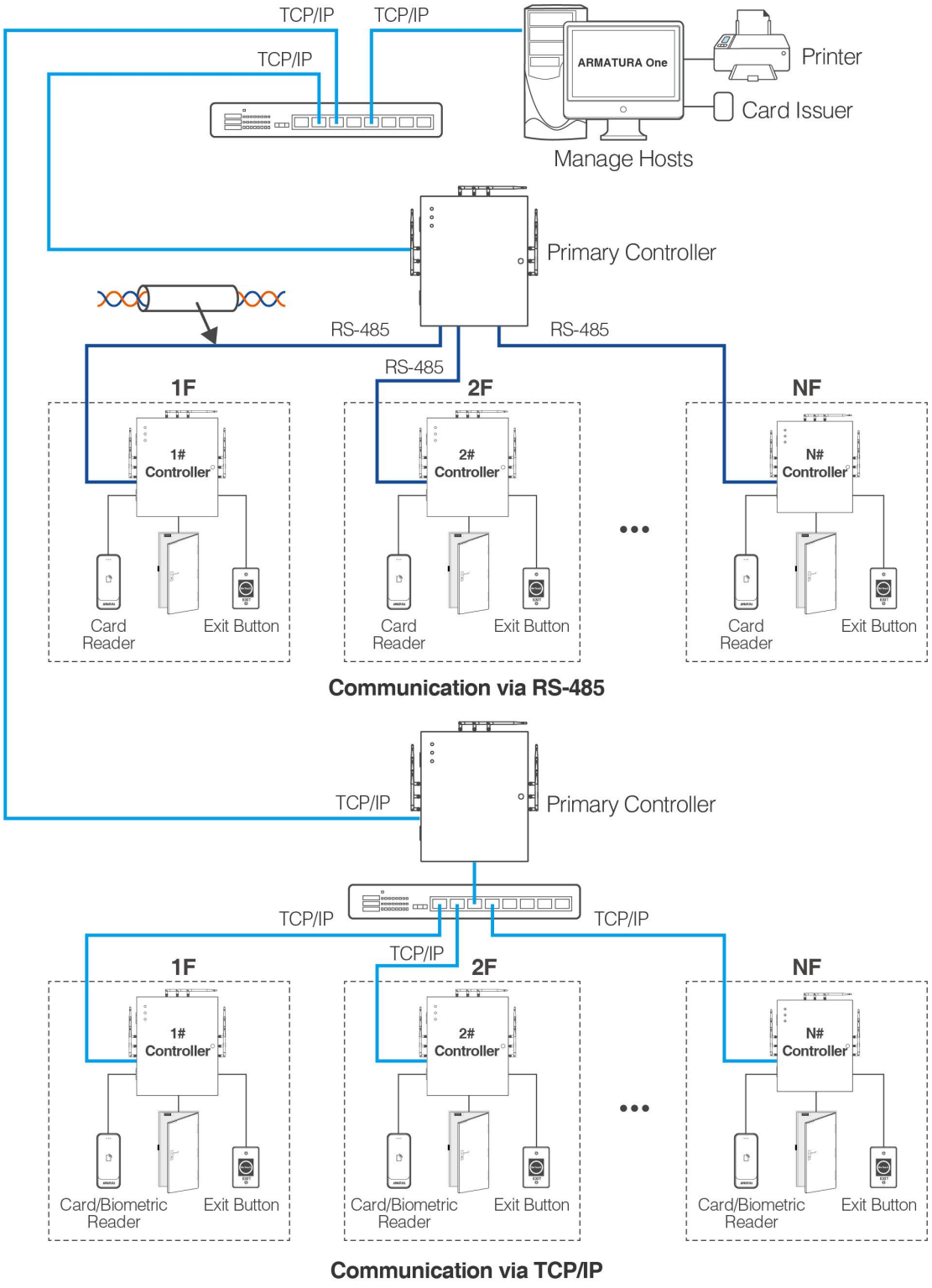


Figure 3-10 Schematic Diagram of Access Control System Installation

Remarks:

1. The access control management system comprises two main components: the Management Workstation (PC) and the Controller. These two parts communicate with each other via TCP/IP.
2. The communication wires should be kept as far away as possible from high voltage wires, and they should not be routed in parallel with or bundled together with power wires.
3. The management workstation is a network-connected PC. Access control management personnel can perform various management functions remotely by running the access control management software installed on the PC. These functions include adding/ deleting a user, viewing event records, opening/closing doors, and monitoring the real-time status of each door.
4. When the controller communicates via TCP/IP, card/biometric readheads can be connected. When the controller communicates with primary controller via RS-485, only pure card readers can be connected.

3.3 Controller System Installation

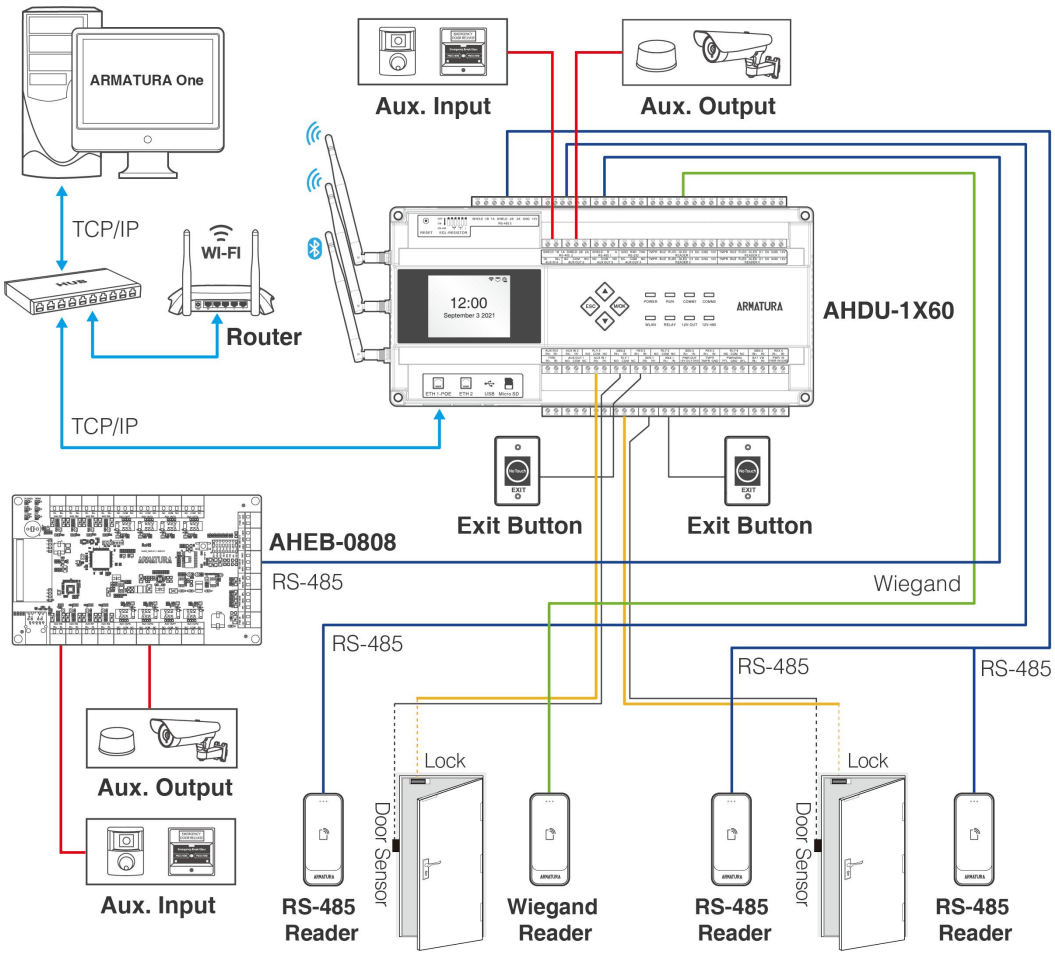


Figure 3-11 Schematic Diagram of AHDU-1X60 System Installation

3.4 Access Control System Power Supply Structure

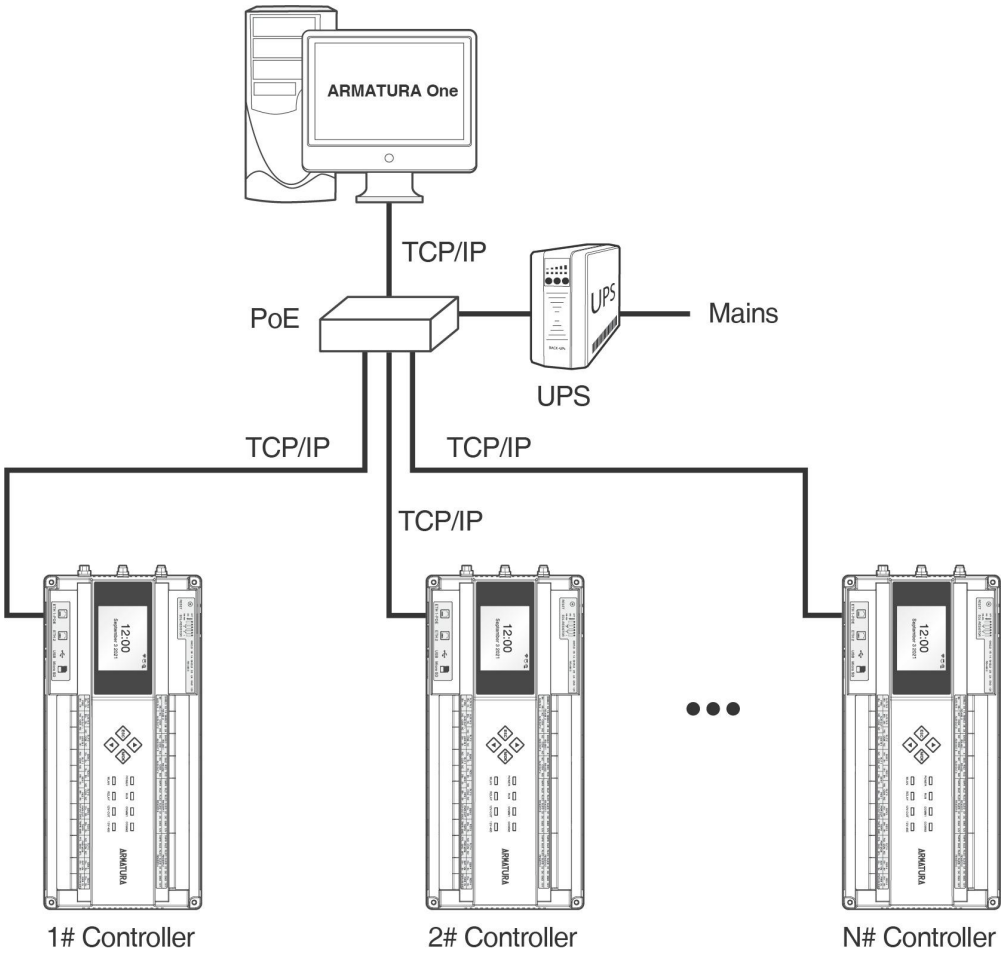


Figure 3-12 PoE System

Remarks:

1. The Armatura Horizon Controller can be powered through either a +12V DC power adapter or PoE, depending on availability.
2. If using a +12V DC power adapter, it is recommended to power each controller separately to minimize power interference between controllers.
3. If using PoE, the TCP/IP network interface of the access controller can function as both a PoE interface and a PC communication interface. The PoE switch must comply with IEEE 802.3at standards.
4. To prevent controller power failures that may lead to the entire system's inability to function, it is essential for the access control management system to have at least one UPS (Uninterruptible Power Supply). Additionally, access control locks are powered externally to ensure that the access control management system can operate normally during power outages.

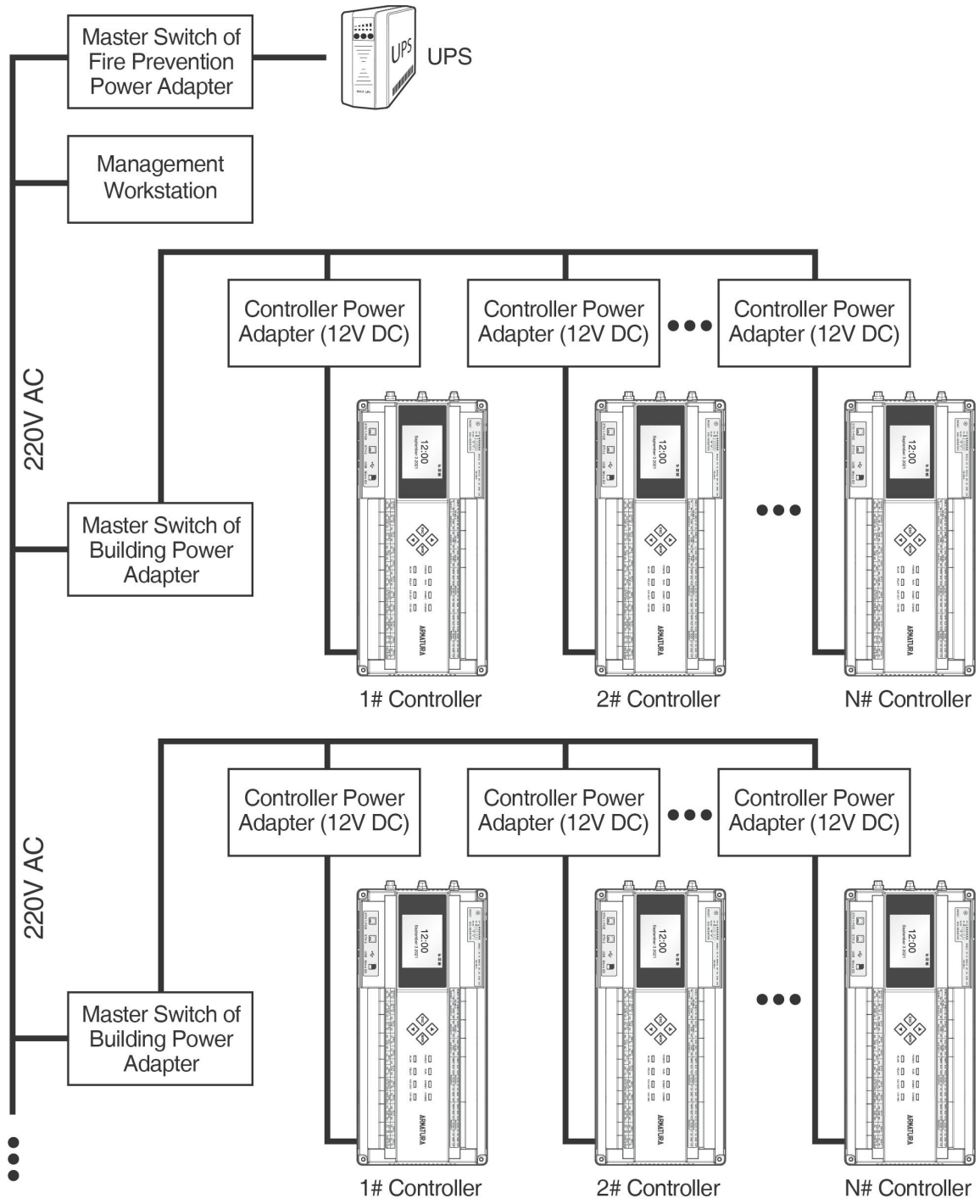


Figure 3-13 Access Controller System Power Supply

4. Terminal and Wiring Description

4.1 Controller Connection Terminals

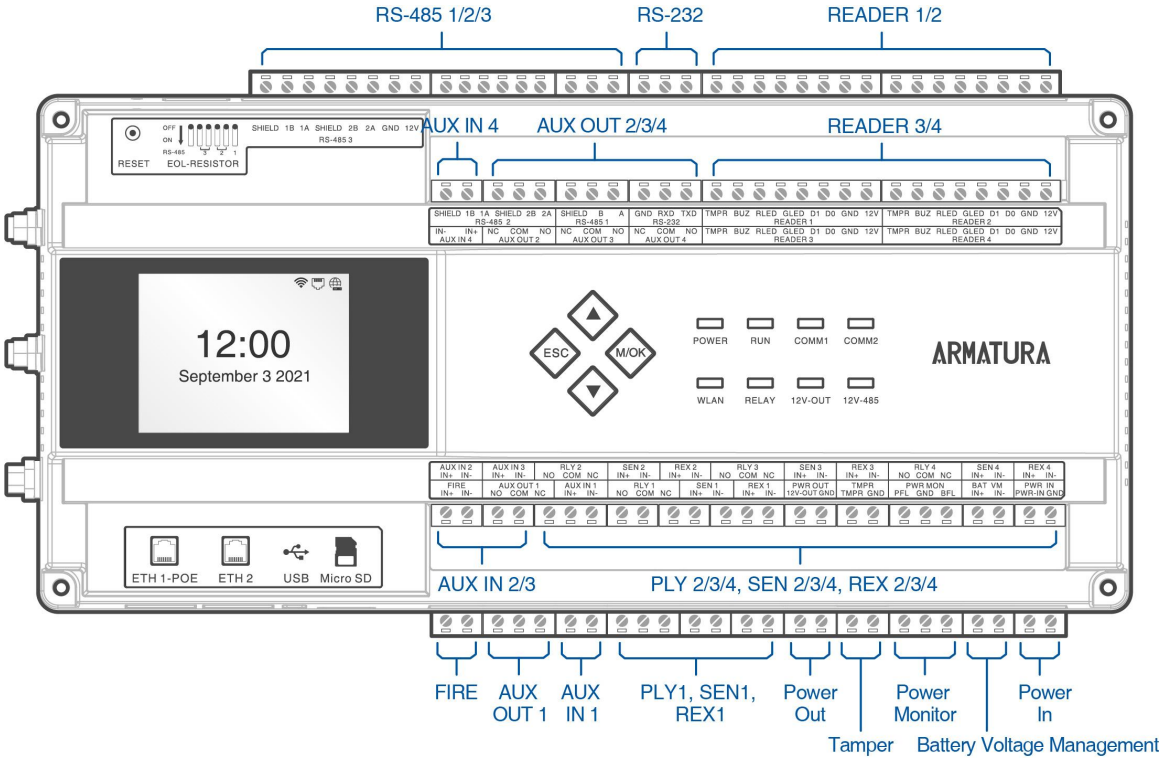


Figure 4-1 AHDU-1X60 Terminal connection diagram

Description of the terminals:

1. **RS-485:** The RS-485 reader port allows for external connection to a RS-485 reader.

2. **READER:** The reader port allows for external connection to a wiegand reader.

3. **Auxiliary Input (AUX IN):** The auxiliary input may connect to external monitoring devices such as fire alarms, door & window contacts, smoke detectors & more.

4. **Auxiliary Output (AUX OUT):** The auxiliary output may connect to alarms, doorbells, etc.

5. **FIRE, Auxiliary Input (AUX IN), Sensor(SEN), Request to Exit(REX):** The fire, auxiliary input, sensor and request to exit ports all support line monitoring. To enable the line monitoring function, you can configure this from the ARMATURA One software. For a supervised circuit, it is recommended to add two resistors as close to the sensor as possible. Custom End of Line (EOL) resistances can be configured through the software.

6. The terminals above are set through the relevant access control software. Please see the respective software manual for further details.

4.2 Terminal Description

4.2.1 AHSC-1000

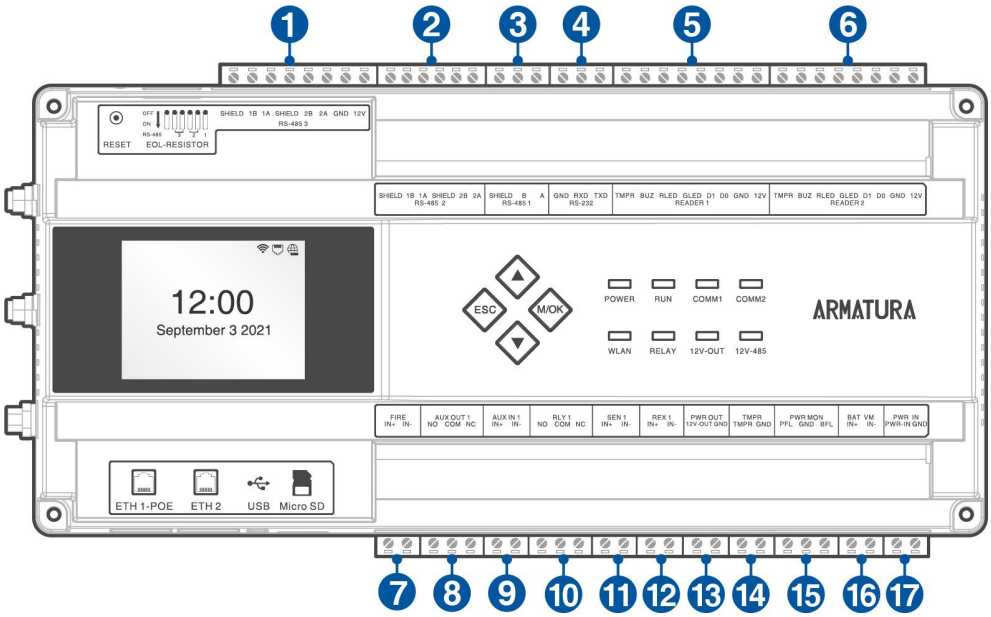


Figure 4-2 AHSC-1000 terminal description

NO.	Terminal	NO.	Terminal
1	RS-485 3	10	Relay 1
2	RS-485 2	11	Sensor 1
3	RS-485 1	12	Request to Exit 1
4	RS-232	13	Power Output
5	Reader 1	14	Tamper
6	Reader 2	15	Power Monitor
7	FIRE	16	Battery Voltage Management
8	Auxiliary Output 1	17	Power Input
9	Auxiliary Input 1		

4.2.2 AHDU-1160

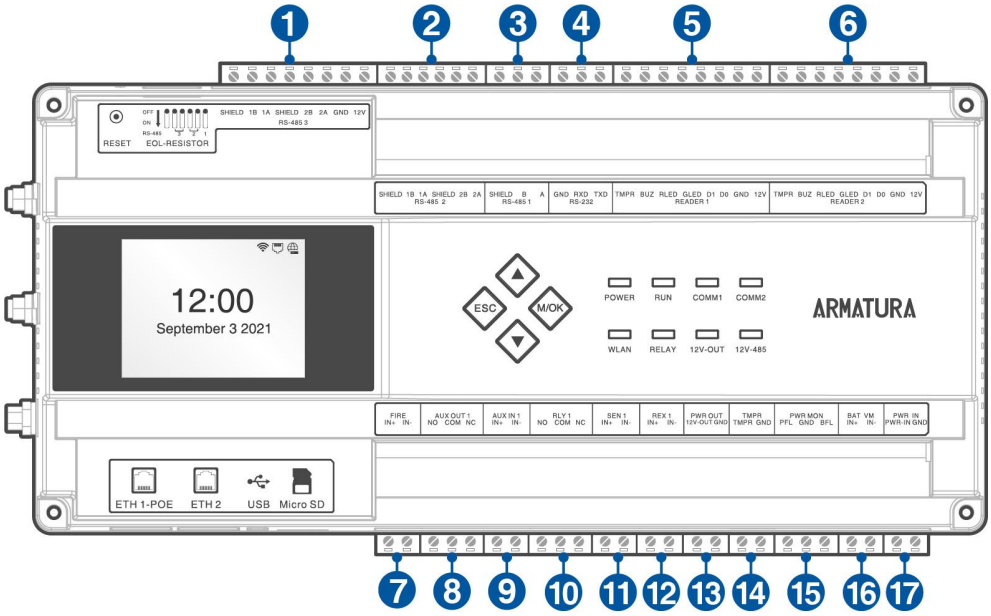


Figure 4-3 AHDU-1160 terminal description

NO.	Terminal	NO.	Terminal
1	RS-485 3	10	Relay 1
2	RS-485 2	11	Sensor 1
3	RS-485 1	12	Request to Exit 1
4	RS-232	13	Power Output
5	Reader 1	14	Tamper
6	Reader 2	15	Power Monitor
7	FIRE	16	Battery Voltage Management
8	Auxiliary Output 1	17	Power Input
9	Auxiliary Input 1		

4.2.3 AHDU-1260

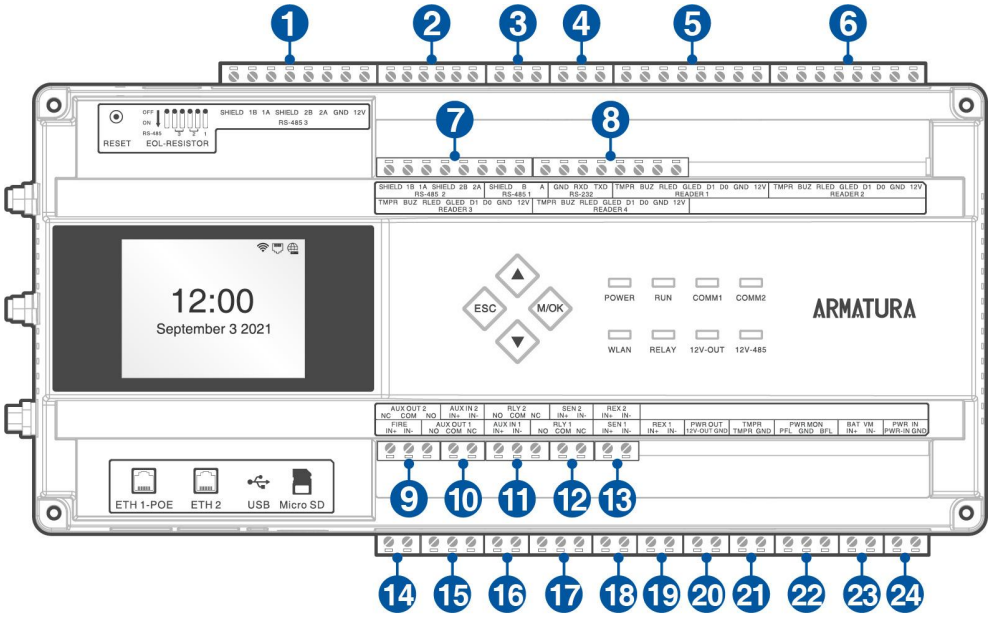


Figure 4-4 AHDU-1260 terminal description

NO.	Terminal	NO.	Terminal
1	RS-485 3	13	Request to Exit 2
2	RS-485 2	14	FIRE
3	RS-485 1	15	Auxiliary Output 1
4	RS-232	16	Auxiliary Input 1
5	Reader 1	17	Relay 1
6	Reader 2	18	Sensor 1
7	Reader 3	19	Request to Exit 1
8	Reader 4	20	Power Output
9	Auxiliary Output 2	21	Tamper
10	Auxiliary Input 2	22	Power Monitor
11	Relay 2	23	Battery Voltage Management
12	Sensor 2	24	Power Input

4.2.4 AHDU-1460

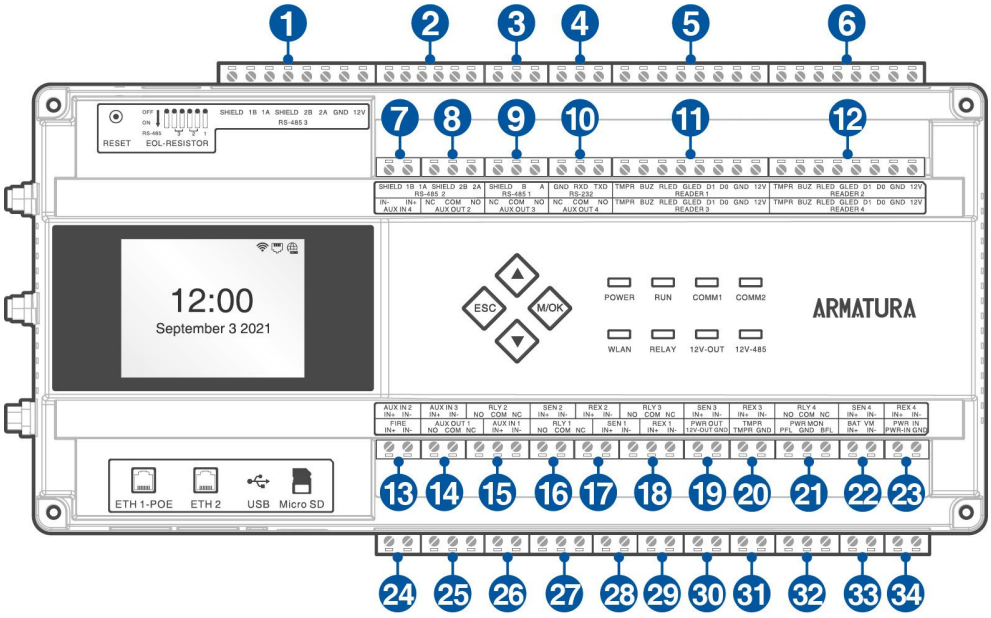


Figure 4-5 AHDU-1460 terminal description

NO.	Terminal	NO.	Terminal
1	RS-485 3	18	Relay 3
2	RS-485 2	19	Sensor 3
3	RS-485 1	20	Request to Exit 3
4	RS-232	21	Relay 4
5	Reader 1	22	Sensor 4
6	Reader 2	23	Request to Exit 4
7	Auxiliary Input 4	24	FIRE
8	Auxiliary Output 2	25	Auxiliary Output 1
9	Auxiliary Output 3	26	Auxiliary Input 1
10	Auxiliary Output 4	27	Relay 1
11	Reader 3	28	Sensor 1
12	Reader 4	29	Request to Exit 1
13	Auxiliary Input 2	30	Power Output
14	Auxiliary Input 3	31	Tamper
15	Relay 2	32	Power Monitor
16	Sensor 2	33	Battery Voltage Management
17	Request to Exit 2	34	Power Input

4.2.5 AHEB-0808

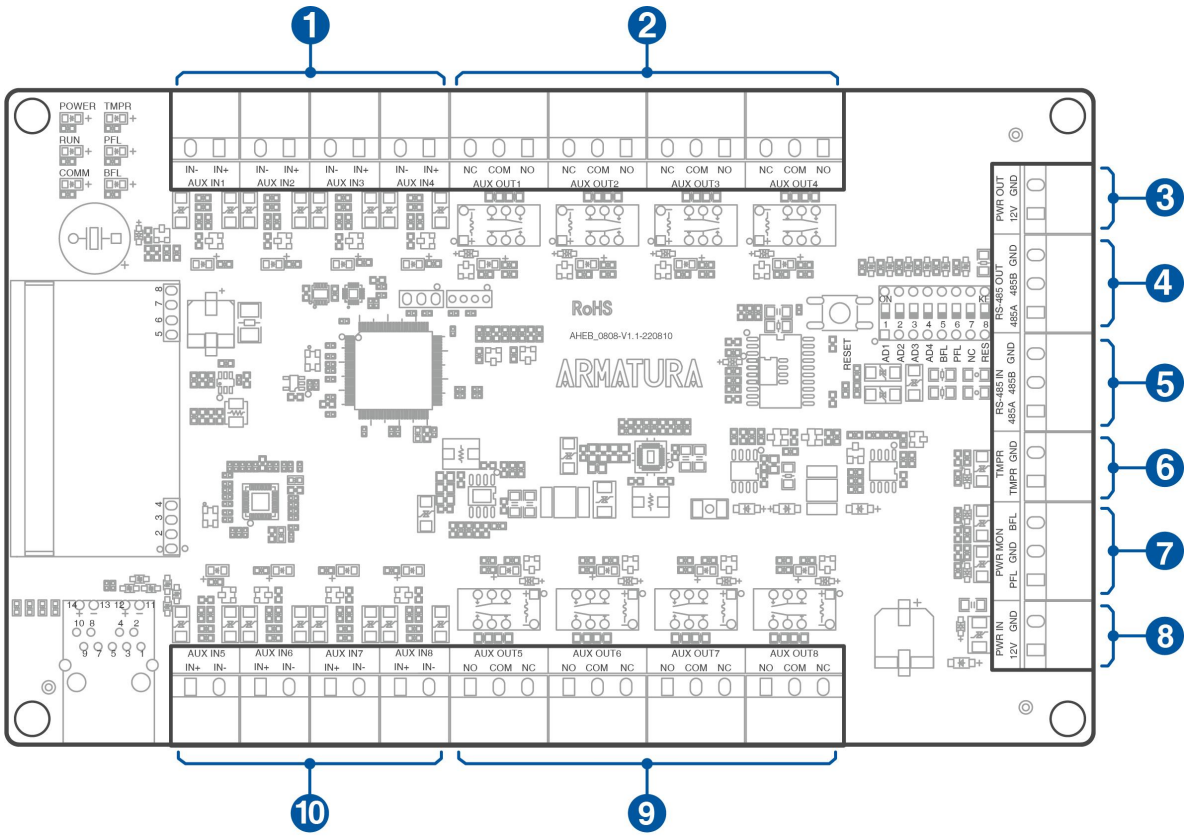


Figure 4-6 AHEB-0808 terminal description

NO.	Terminal	NO.	Terminal
1	Auxiliary Input (1-4)	6	Tampering Alarm
2	Auxiliary Output (1-4)	7	Power MON
3	Power Output	8	Power Input
4	RS-485 Out	9	Auxiliary Output (5-8)
5	RS-485 In	10	Auxiliary Input (5-8)

4.2.6 AHEB-1602

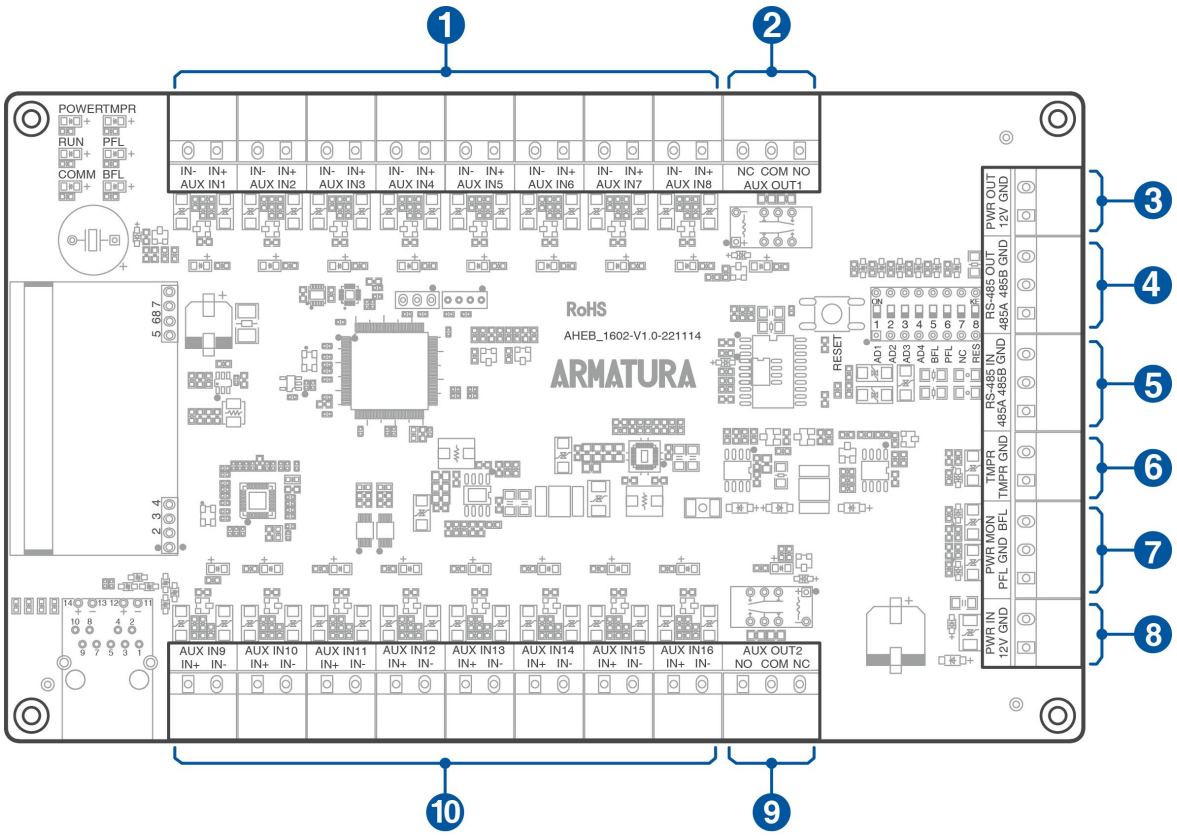


Figure 4-7 AHEB-1602 terminal description

NO.	Terminal	NO.	Terminal
1	Auxiliary Input (1-8)	6	Tampering Alarm
2	Auxiliary Output 1	7	Power MON
3	Power Output	8	Power Input
4	RS-485 Out	9	Auxiliary Output 2
5	RS-485 In	10	Auxiliary Input (9-16)

4.2.7 AHEB-1616

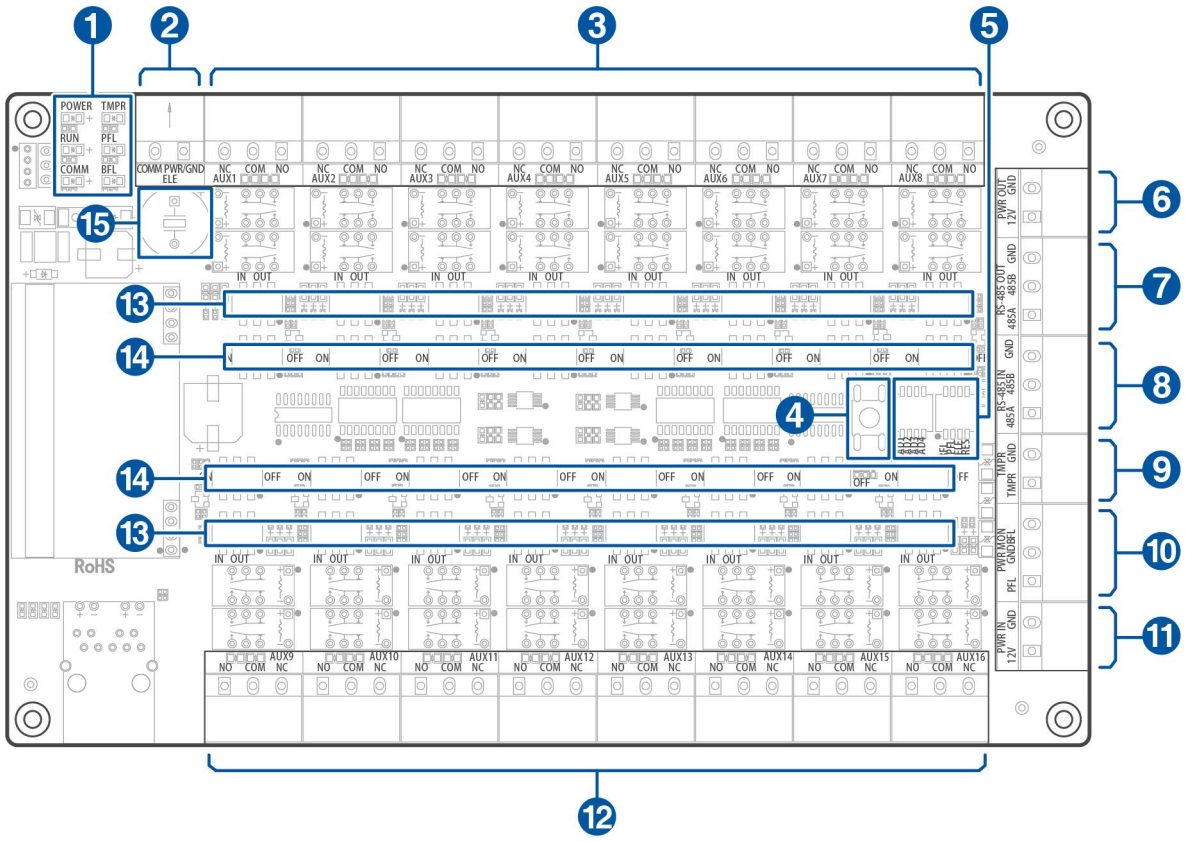


Figure 4-8 AHEB-1616 terminal description

NO.	Terminal	NO.	Terminal
1	Status LED Indicator	9	Tampering Alarm
2	Power ELE	10	Power MON
3	Auxiliary Input / Output (1-8)	11	Power Input
4	Reset Button	12	Auxiliary Input / Output (9-16)
5	DIP Switch	13	Auxiliary Input / Output Toggle Switches
6	Power Output	14	Key Detection Switches
7	RS-485 Out	15	Buzzer
8	RS-485 In		

4.3 Wiring Description

4.3.1 ENC1 Enclosure Internal Wiring Diagram

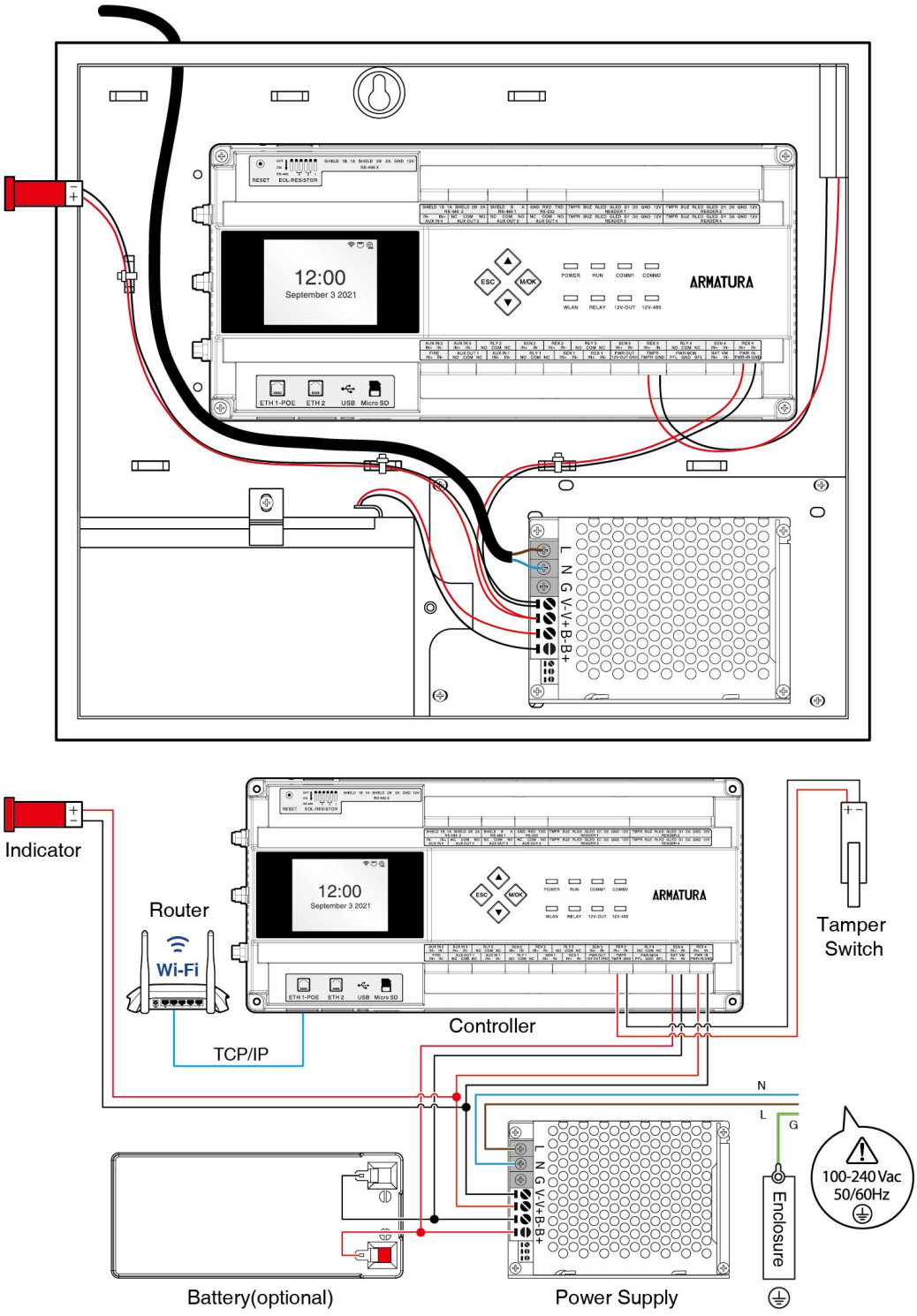


Figure 4-9 ENC1 Enclosure Internal Wiring Diagram

4.3.2 Power Wiring

The Armatura Horizon Controller can be powered using either a 12V-24V DC power adapter or PoE, depending on availability. The wiring diagram is illustrated below:

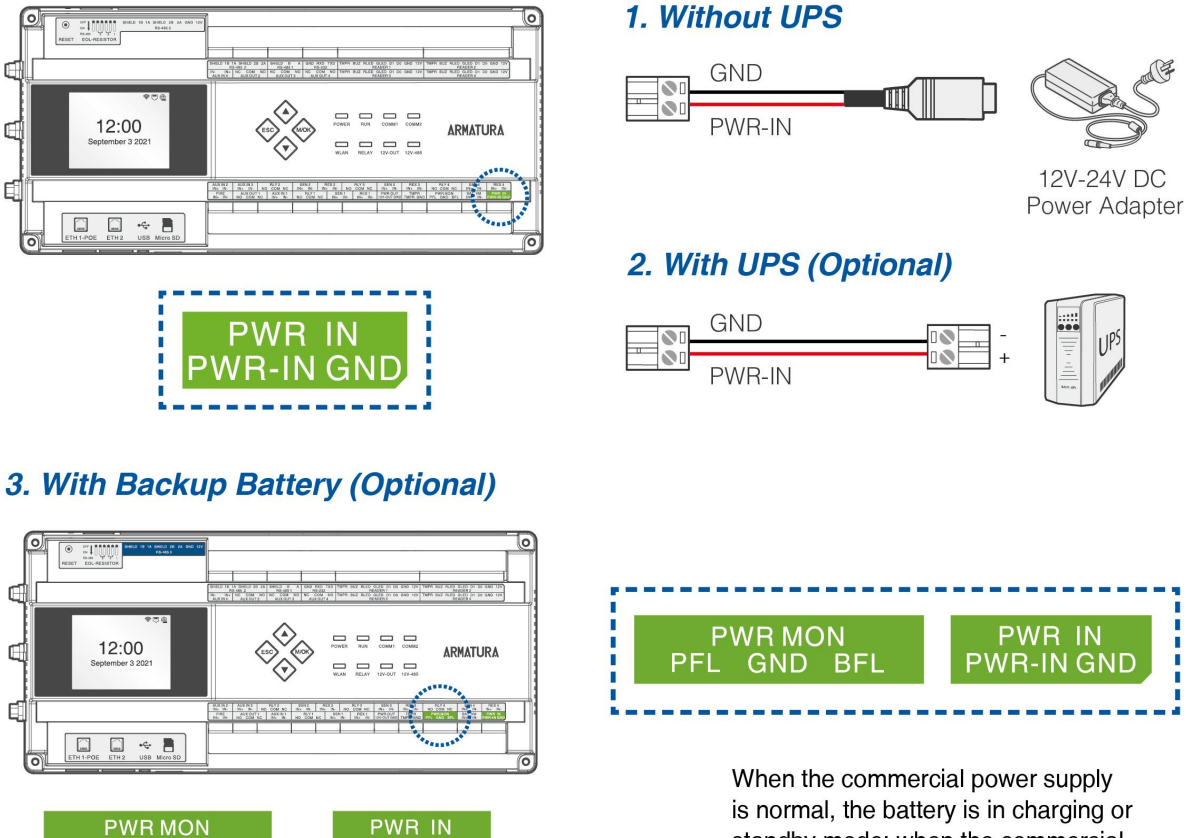


Figure 4-10 Power Wiring

Recommended Power Supply:

- 12V-24V DC ±20%, minimum 1.5A.

- Use an AC adapter with higher current ratings if power needs to be shared with other devices.

4.3.3 Network Wiring

Establish the connection between the device and the software using an Ethernet cable. An illustrative example is provided below:

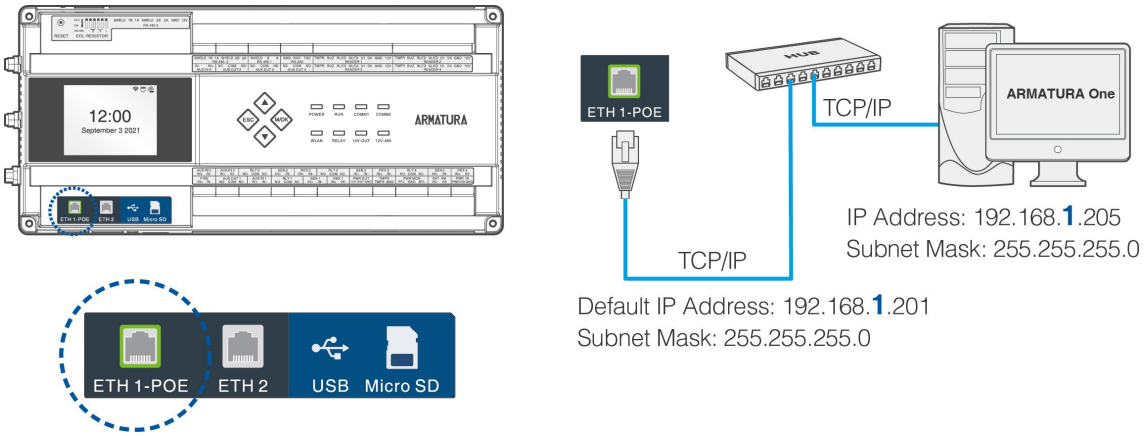


Figure 4-11 Network Wiring

Notes:

1. *In LAN, the IP addresses of the server (PC) and the device must be in the same network segment when connecting to the **ARMATURA One** software.*

2. *Dual Ethernet interfaces: the default IP address **192.168.1.201** for the primary NIC and **192.168.2.202** for the expansion NIC.*

4.3.4 Auxiliary Output Wiring

The auxiliary output interface which may connect to alarms, monitors and doorbells, etc.

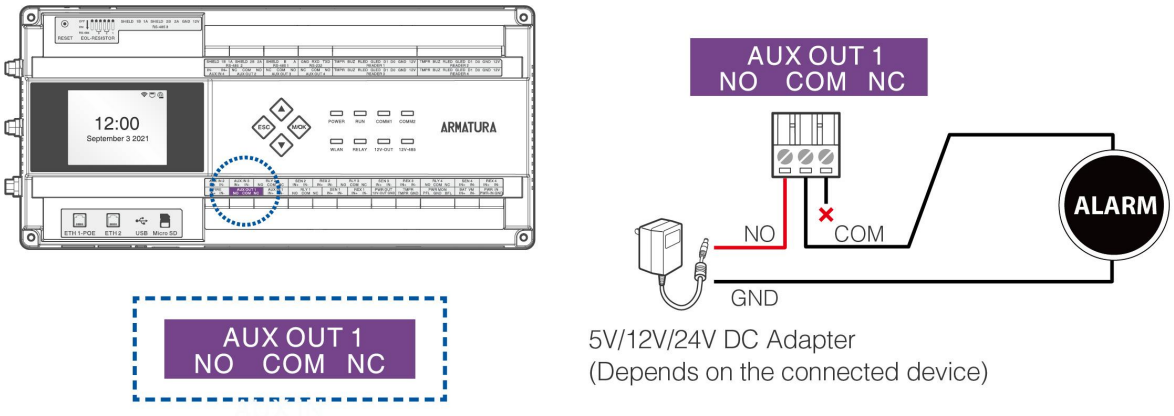


Figure 4-12 Auxiliary Output Wiring

Notes:

1. *For proper operation, the device must be connected to a separate power adapter.*
2. *Select an appropriate power adapter source based on the device's specifications.*

4.3.5 Auxiliary Input Wiring

The auxiliary input interface may connect to external monitoring devices such as smoke detectors, air quality sensors, door & window contacts, wireless exit switches, etc. Auxiliary inputs are configured through the relevant access control software. For further details, please refer to the respective software manual.

The auxiliary input ports support line monitoring with both unsupervised and supervised circuit options, as depicted in the figure below. When using a supervised circuit, it is recommended to add two resistors, such as R1 and R2 shown in the figure, as close to the sensor as possible.

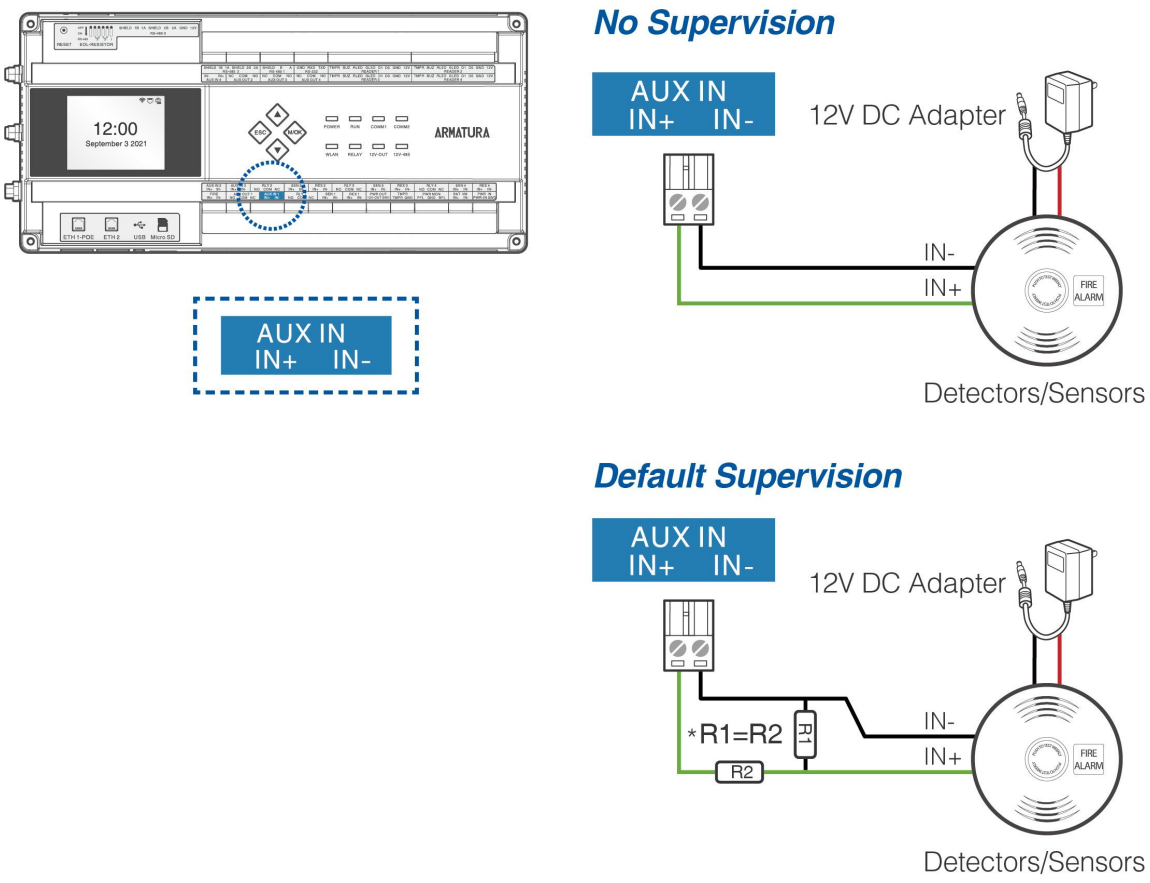


Figure 4-13 Auxiliary Input Wiring

Note:

- *Custom End of Line (EOL) resistances can be configured using the host software. The system supports 1.2K, 2.2K, 4.7K, and 10K resistors. For more information, refer to section 4.3.12 Line Monitoring.*

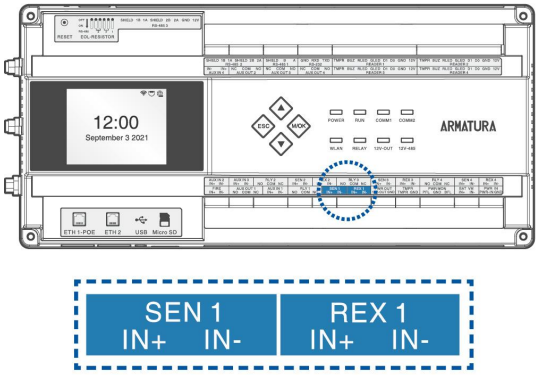
4.3.6 Door Sensor, Exit Button Wiring

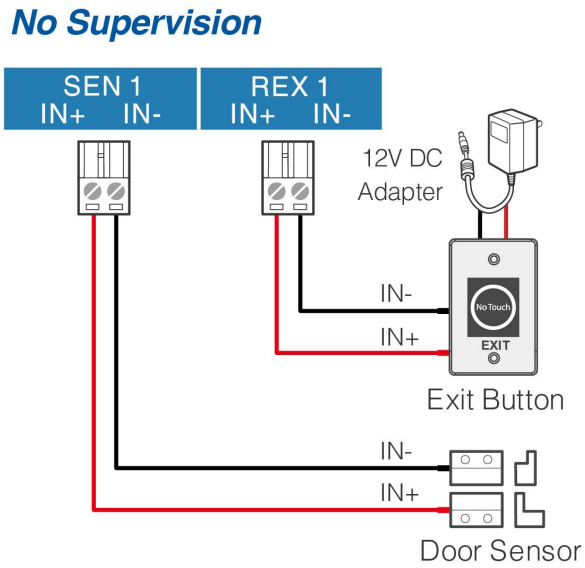
A door sensor is utilized to detect the open/close status of a door. When connected to a door sensor, an access control panel can detect unauthorized door openings and trigger an alarm output. Additionally, if a door remains open for an extended period of time, the door control panel can trigger an alarm as well. It is recommended to use two-core wires with a gauge over 0.22mm2 for this purpose. However, if there is no need to monitor the open/closed status of a door, trigger alarms for prolonged open durations, track unauthorized access, or use the interlock function, a door sensor can be omitted.

An exit switch is installed indoors to open a door. When switched on, the door will be opened. The exit button should be fixed at a height of about **55.12 inches (1.4m)** above the ground, ensuring it is in the correct position without any slant and securely connected. Any unused wire should have its exposed end cut off and wrapped with insulating tape. Be cautious of electromagnetic interference, such as from light switches and computers. For the connection wire between an exit switch and the controller, it is recommended to use two-core wires with a gauge over 0.3mm^2.

The sensor and request to exit ports both support line monitoring. The figure below illustrates both the unsupervised circuit and the supervised circuit.

For a supervised circuit, add two resistors as close to the sensor as possible, similar to R1 and R2 shown in the figure below.





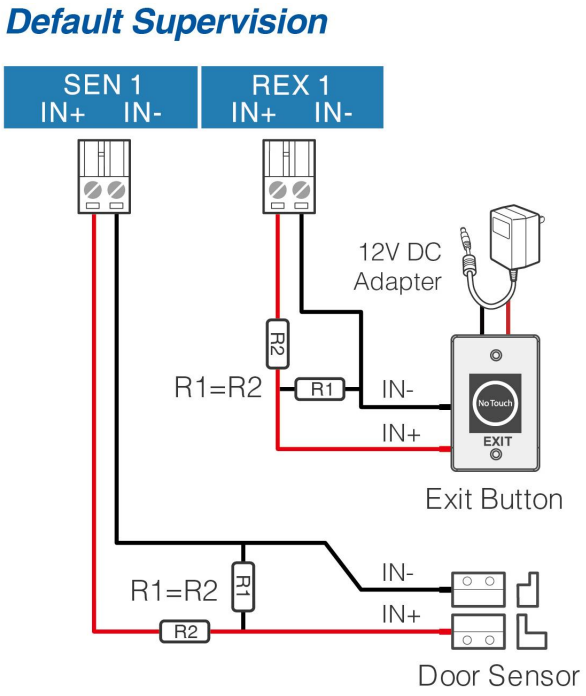


Figure 4-14 Door Sensor, Exit Button Wiring

Note:

- *Custom End of Line (EOL) resistances can be configured using the host software. The system supports 1.2K, 2.2K, 4.7K, and 10K resistors. For more information, refer to section 4.3.12 Line Monitoring.*

4.3.7 Wiegand Reader Wiring

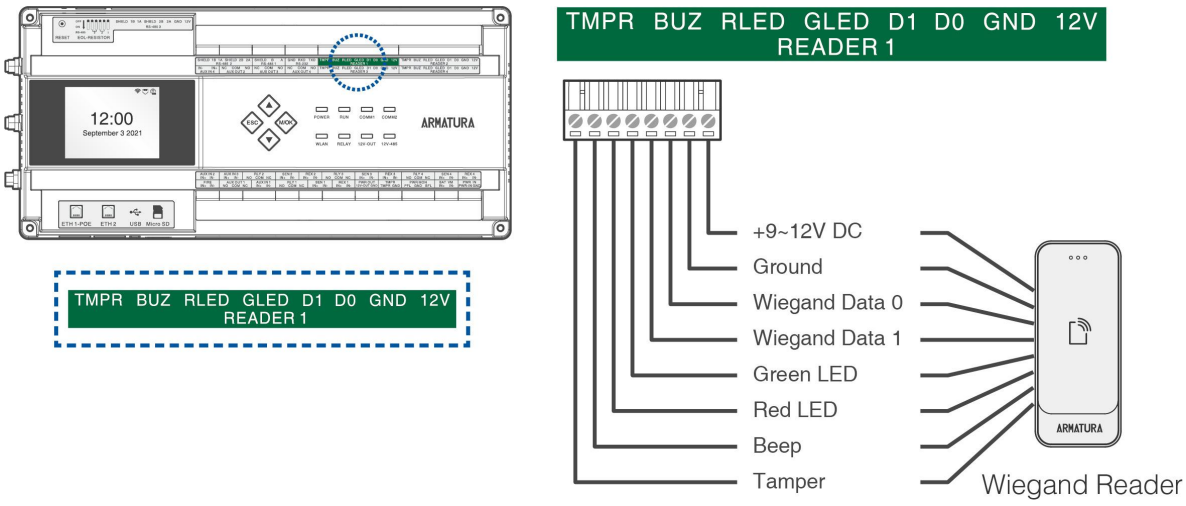


Figure 4-15 Wiegand Reader Wiring

4.3.8 Lock Relay Wiring

1. The ARMATURA Horizon Controller provides one or multiple electronic lock outputs. The **COM** and **NO** terminals are used for locks that unlock when power is connected and lock when power is disconnected. The **COM** and **NC** terminals are used for locks that lock when power is connected and unlock when power is disconnected.

2. The system supports both **Normally Opened Lock** and **Normally Closed Lock**. The **NO Lock** (Normally Opened when powered) is connected with '**NO**' and '**COM**' terminals, and the NC Lock (Normally Closed when powered) is connected with '**NC**' and '**COM**' terminals. The device does not share power with the lock, as shown in the example with NC Lock below:

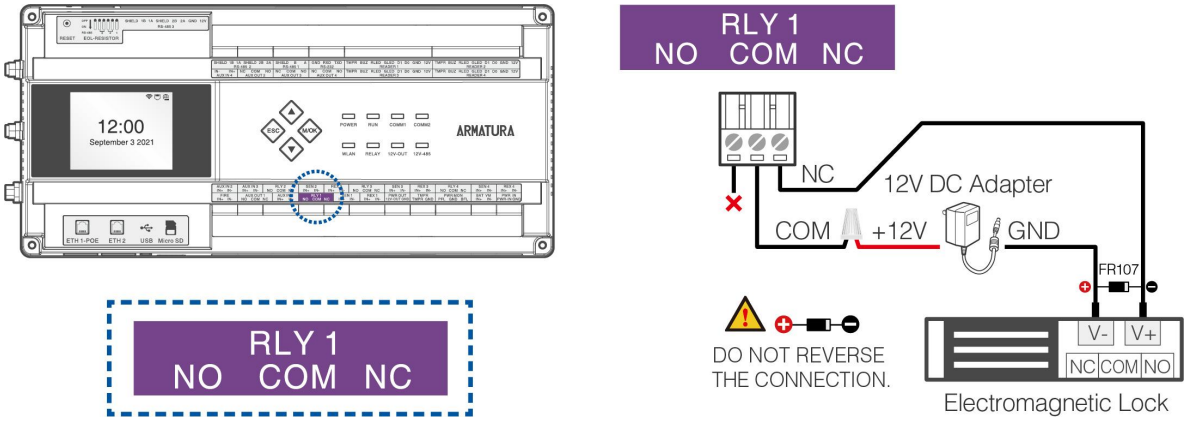


Figure 4-16 Wiring diagram of lock connection

3. Our access control panel is powered by standard PoE or access control power. You can choose either one of the power supplies as needed.

4. To protect the access control system against the self-induced electromotive force generated by an electronic lock at the instant of switching off/on, it is necessary to connect a diode in parallel (please use FR107 delivered with the system) with the electronic lock to release the self-induced electromotive force during the onsite connection for application of the access control system.

4.3.9 Fire Alarm Monitoring Wiring

The Input FIRE port circuits can be configured in either No Supervision mode or Default Supervision mode, with the default being No Supervision mode, where all doors are normally open in case of a short circuit. After connecting the ARMATURA One software and enabling line monitoring, custom End of Line (EOL) resistances can be configured. The FIRE wiring method is illustrated in the figure below. For a monitored circuit, it is advised to add two resistors as close to the sensor as possible.

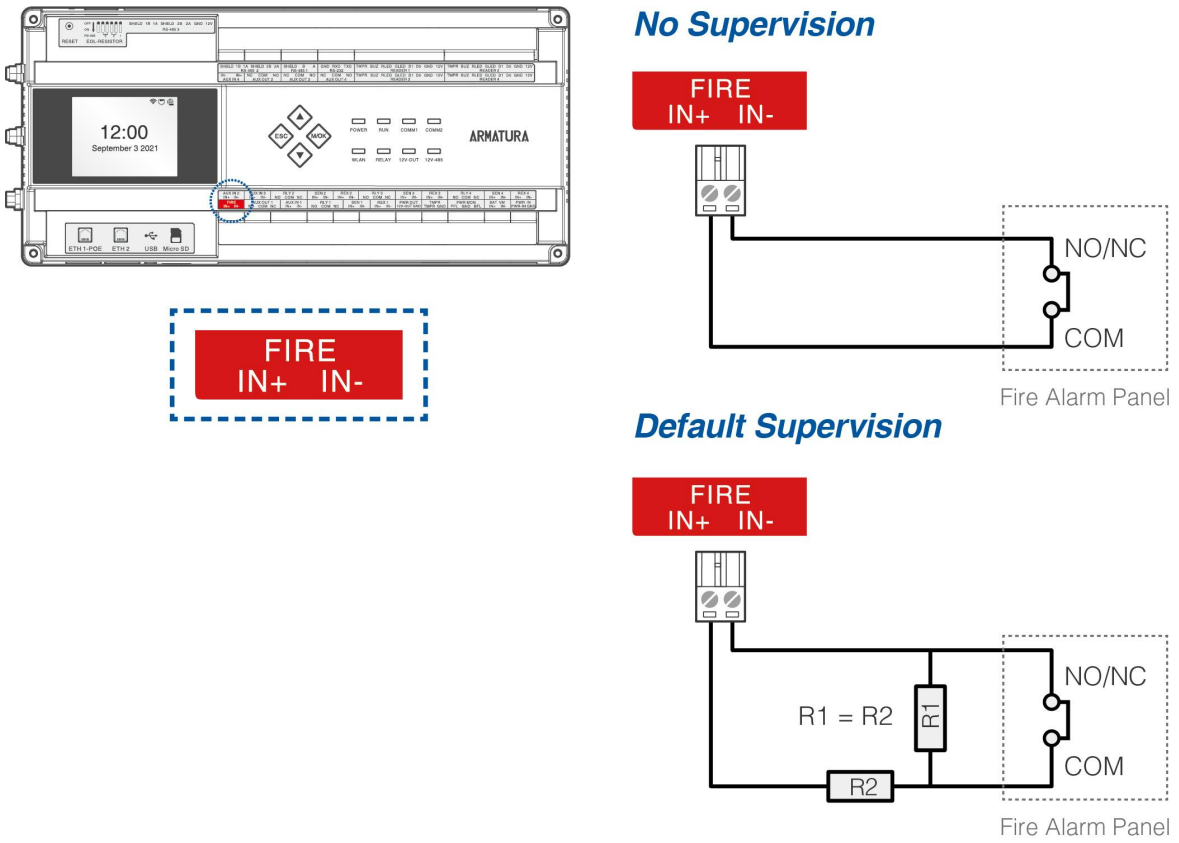


Figure 4-17 Fire Alarm Monitoring Wiring

Note:

- *Custom End of Line (EOL) resistances can be configured using the host software. The system supports 1.2K, 2.2K, 4.7K, and 10K resistors. For more information, refer to section 4.3.12 Line Monitoring.*

4.3.10 RS-485 Reader Wiring

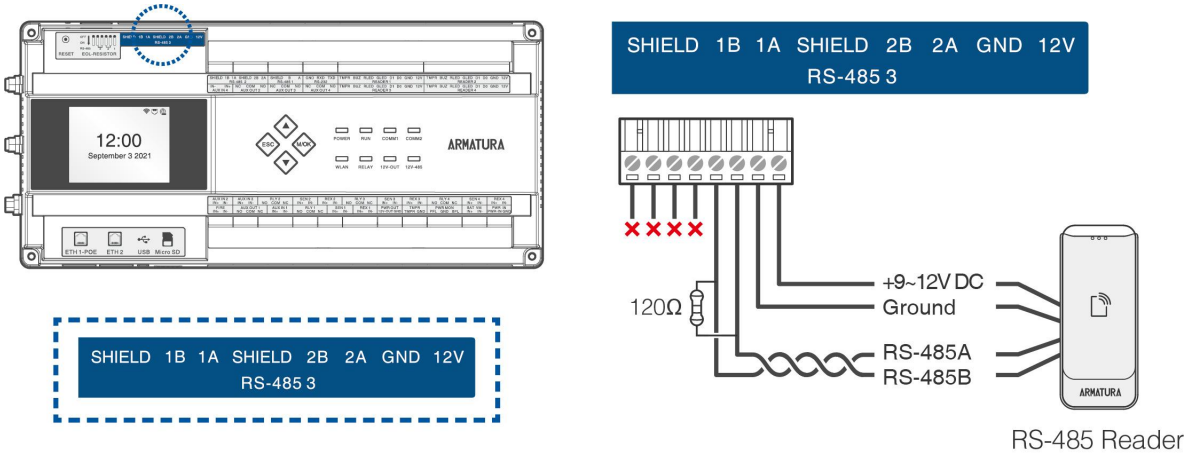
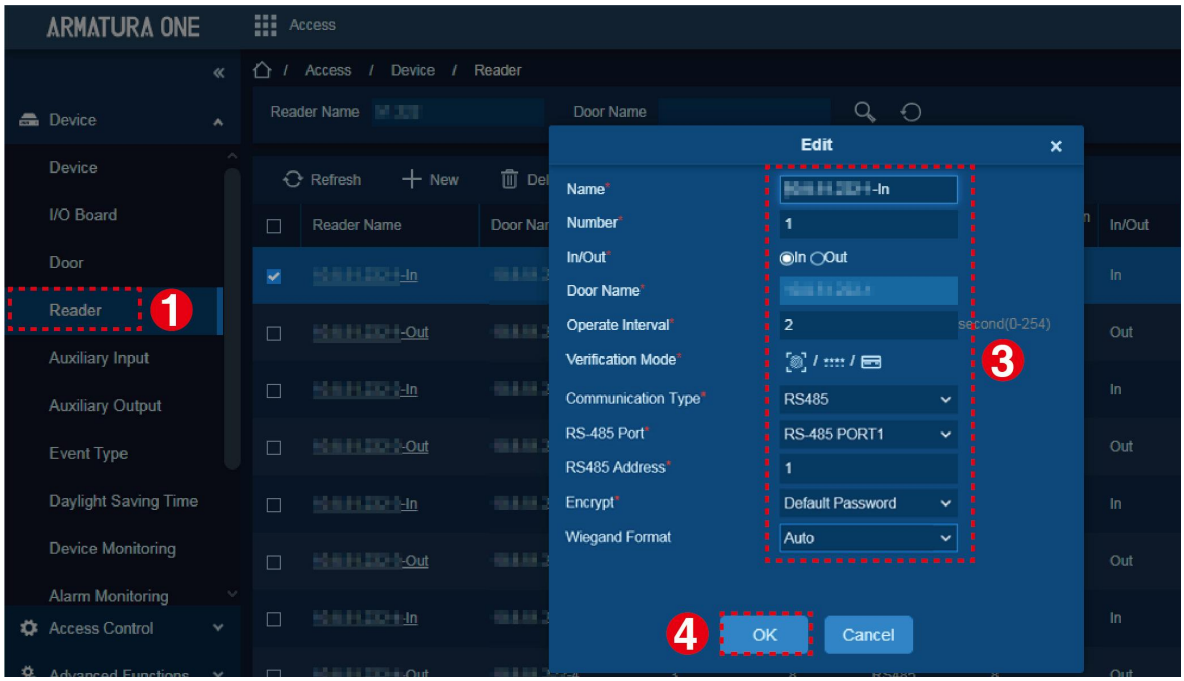


Figure 4-18 RS-485 Reader Wiring

Important Notes

When connecting the RS-485 reader, please follow the instructions carefully and adhere to the following guidelines.

1. The RS-485 port supports using the OSDP protocol, but it requires configuring the parameters on the ARMATURA One software. To make the necessary changes, follow the modification path: **Access > Device > Reader > New**, as illustrated below:



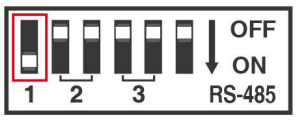
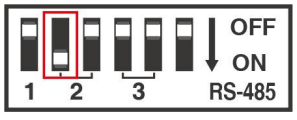
In the pop-up edit window, configure each parameter of the RS-485 reader. Once done, click **OK** to finalize the configuration.

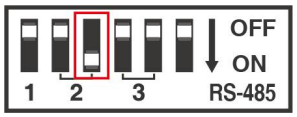
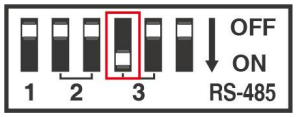
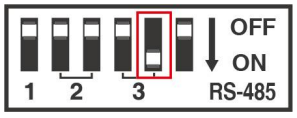
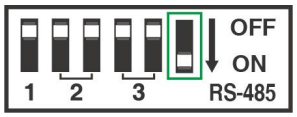
- **RS-485 Port:** Select the port that the RS-485 reader is connected.
- **RS485 Address:** Each RS-485 port is associated with a specific terminating resistor bit number.

Note: *The RS485 address set by the software must match the RS-485 address of the reader.*

2. EOL needs to be enabled when communicating over longer distances. Please refer to the following DIP switch settings to configure the EOL resistor of RS-485.

Table 1 - Configure EOL Resistor of RS-485

EOL-RESISTOR	DIP Number	DIP Switch Settings
RS-485 1 (A，B)	**1**	
RS-485 2 (1A，1B)	**2**	

RS-485 2 (2A，2B)	**3**	
RS-485 3 (1A，1B)	**4**	
RS-485 3 (2A，2B)	**5**	
Reserve	**6**	

3. When connecting the RS-485 reader, shielded twisted pair communication wires with a maximum length of **3937ft (1200m)** are recommended. A maximum of **8** readers can be connected.

4. For communication distances equal to or exceeding **984ft (300m)**, configure the EOL resistor of the RS-485 through the dip switch to enable the terminal. Simultaneously, connect a **120-ohm** terminal matching resistor between the RS-485+ and RS-485- terminals of the last terminal device.

5. The figure below illustrates two methods of RS-485 reader connection.

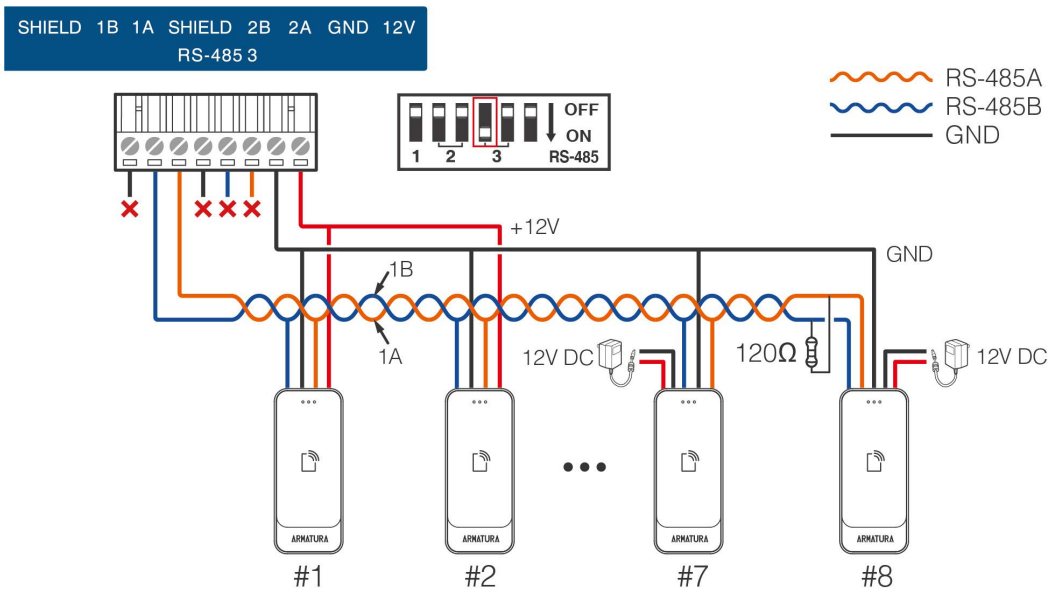


Figure 4-19 Hand-to-hand connection of controller and RS-485 readers

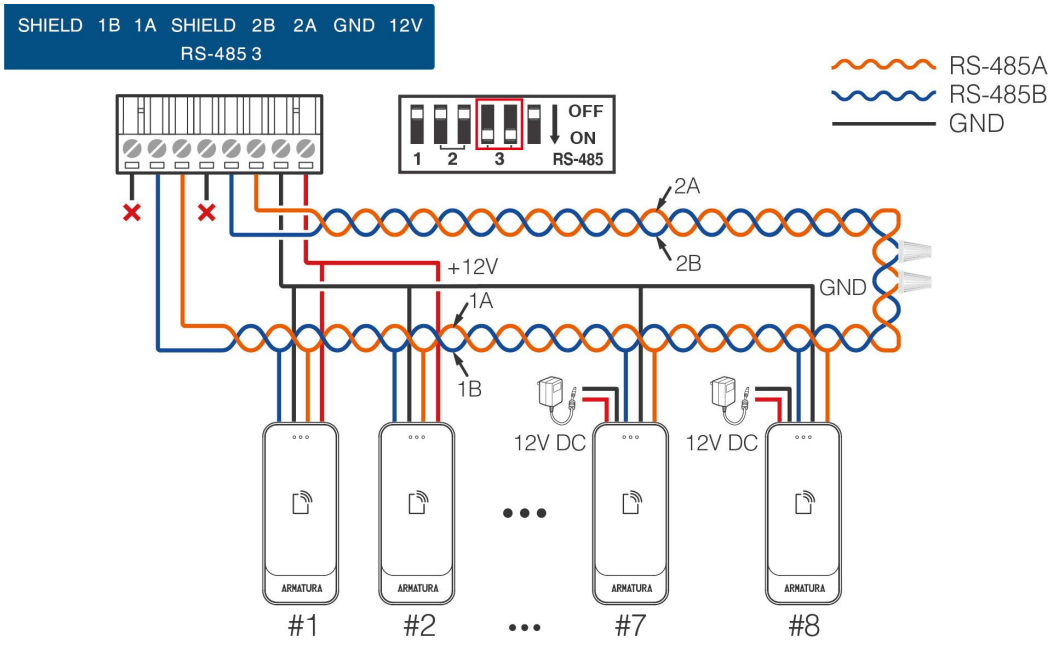


Figure 4-20 RS-485 redundancy backup connection of controller and RS-485 readers

Notes:

1. *When using RS-485 redundant backup mode, ensure that the DIP switches of the connected ports are simultaneously turned to the **ON** position.*

2. *When the DIP switch is set to the **ON** position, it is the equivalent to adding a 120 ohm terminal resistor between the 485+ and 485- terminals.*

4.3.11 I/O Board Wiring

4.3.11.1 Connect AHEB-0808 / AHEB-1602 / AHEB1616 via RS-485

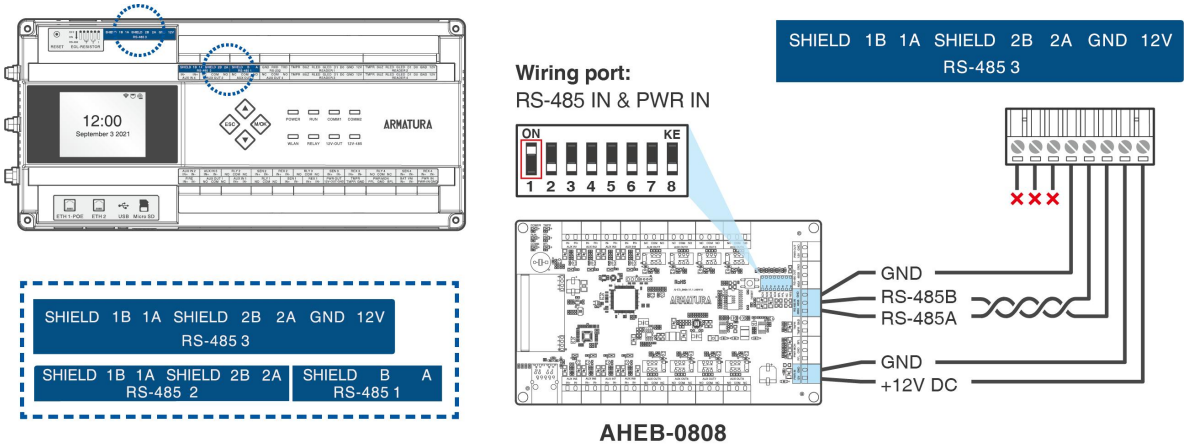


Figure 4-21 I/O Board Wiring

Remarks:

- The AHEB-0808, AHEB-1602 & AHEB-1616 share the same installation, and wiring methods. This document will refer to the AHEB-0808 model as a reference for wiring and connections.

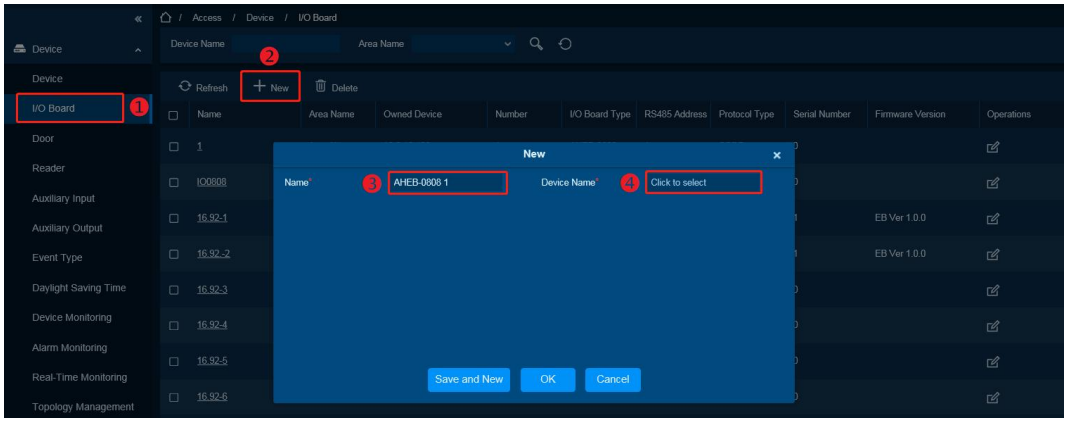
Operating Steps

When connecting the AHEB-0808/AHEB-1602/AHEB-1616 expansion board to the controller, please follow the steps below.

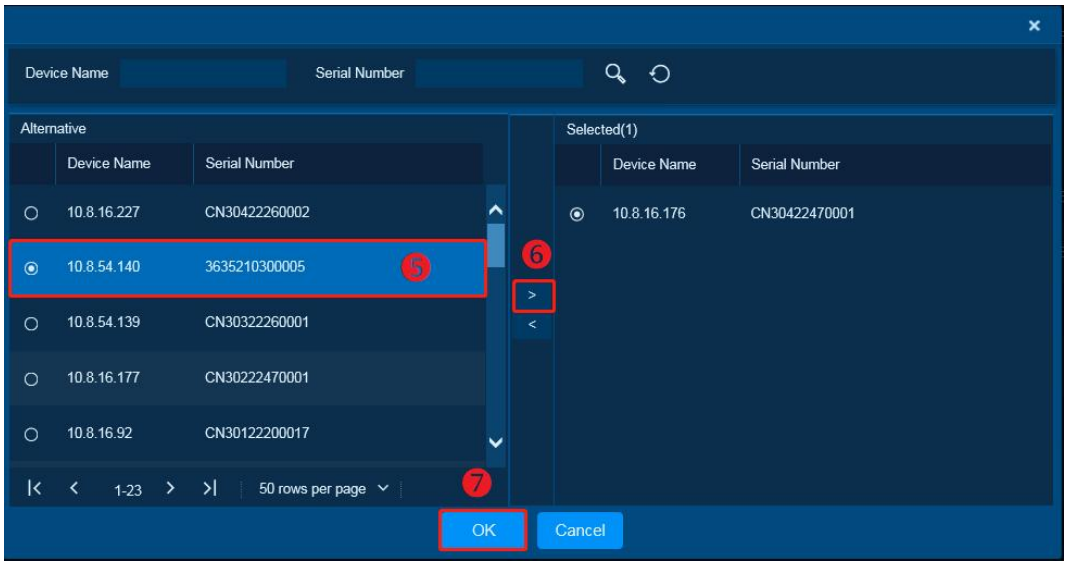
1. Connect the AHEB-0808/AHEB-1602/AHEB-1616 to the AHSC-1000 or the AHDU-1X60 using the RS-485 interface. It can be connected to any of the RS-485 1, RS-485 2, and RS-485 3 wiring ports.

2. Login to the ARMATURA One software using the current account with the necessary authority. Then, follow the instructions in Section 6.3 Add Device on the Software to add the controller to the software.

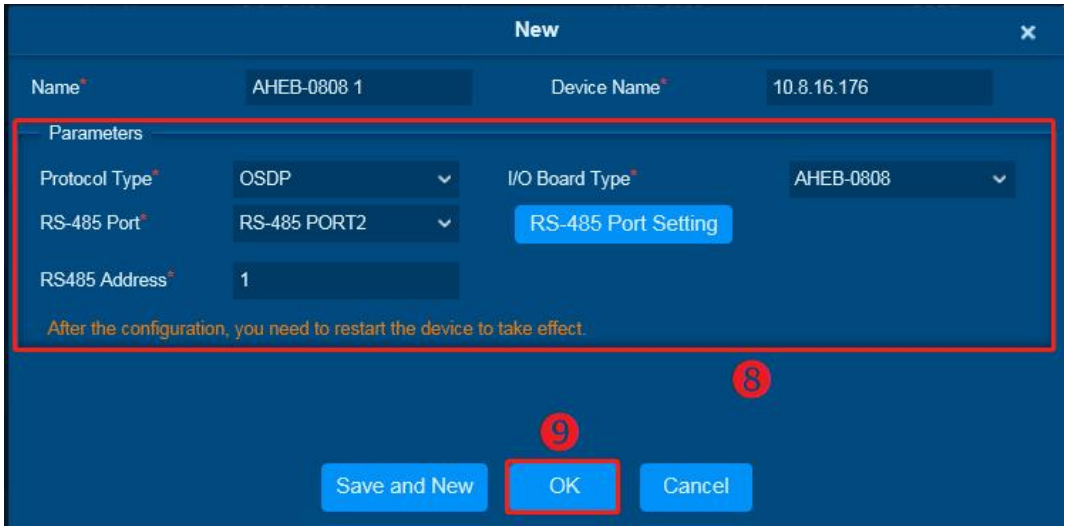
3. Then click **Access > Device > I/O Board > New** to display the new page.



4. Click on '**Device Name**' to open a device selection window. Choose the added controller from the list, and then click '**OK**' to save and exit.

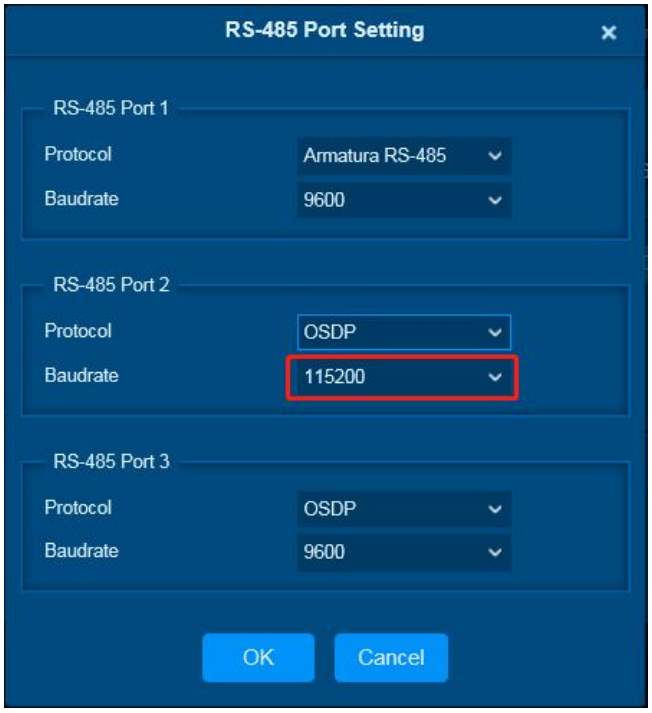


5. Enter corresponding parameters and click **OK** to save the expansion board.



- **RS-485 Port:** Select the port to which the expansion board is connected.
- **RS485 Address:** The RS-485 address of expansion board.

  Note: *The RS485 address set by the software must match the RS-485 address of the* expansion board.
- **I/O Board Type:** Select AHEB-0808/AHEB-1602/AHEB-1616 expansion board.
- **RS-485 Port Setting:** Make sure the baudrate of the corresponding port is the same as that of the expansion board. The default baud rate for AHEB-0808/AHEB-1602/ AHEB-1616 is 115200.



Port Introduction

Parameter		Introduction
RS-485 Port 1	Protocol	Armatura RS-485/OSDP/Aperio
	Baudrate	4800/9600/19200/38400/57600/115200
RS-485 Port 2	Protocol	Armatura RS-485/OSDP/Aperio
	Baudrate	4800/9600/19200/38400/57600/115200
RS-485 Port 3	Protocol	Armatura RS-485/OSDP/Aperio
	Baudrate	4800/9600/19200/38400/57600/115200

Protocol Introduction

Protocol	Purpose	Supported Device
OSDP	For Reader/Expansion Board	AHSC1000, AHDU1X60
Armatura RS-485	For primary and secondary controllers	AHSC1000, AHDU1X60
Aperio	For ASSA ABLOY Aperio AH30	AHSC1000

Remarks:

1. A maximum of eight AHEB-0808/AHEB-1602/AHEB-1616 expansion boards can be connected to each RS-485 port.

2. Each AHEB-0808 can support up to eight auxiliary input devices and eight auxiliary output devices. Each AHEB-1602 can accommodate a maximum of sixteen auxiliary input devices and two auxiliary output devices. While each AHEB-1616 can accommodate a maximum of sixteen auxiliary input devices or sixteen auxiliary output devices.

3. Configure the RS-485 addresses of each AHEB-0808/AHEB-1602/AHEB-1616 using the DIP switch before supplying power.

4. The RS-485 interface can supply a maximum current of 3A (12V). Therefore, when the expansion boards share power with the panel, the total current consumption should not exceed this maximum value. For calculations, please consider the maximum current of the expansion board, keeping in mind that the starting current is typically more than twice the normal working current. If the total current consumption exceeds the maximum limit or to avoid potential issues with starting current, it is recommended to power the expansion board separately.

5. Please find the wiring instructions for connecting multiple expansion boards below.

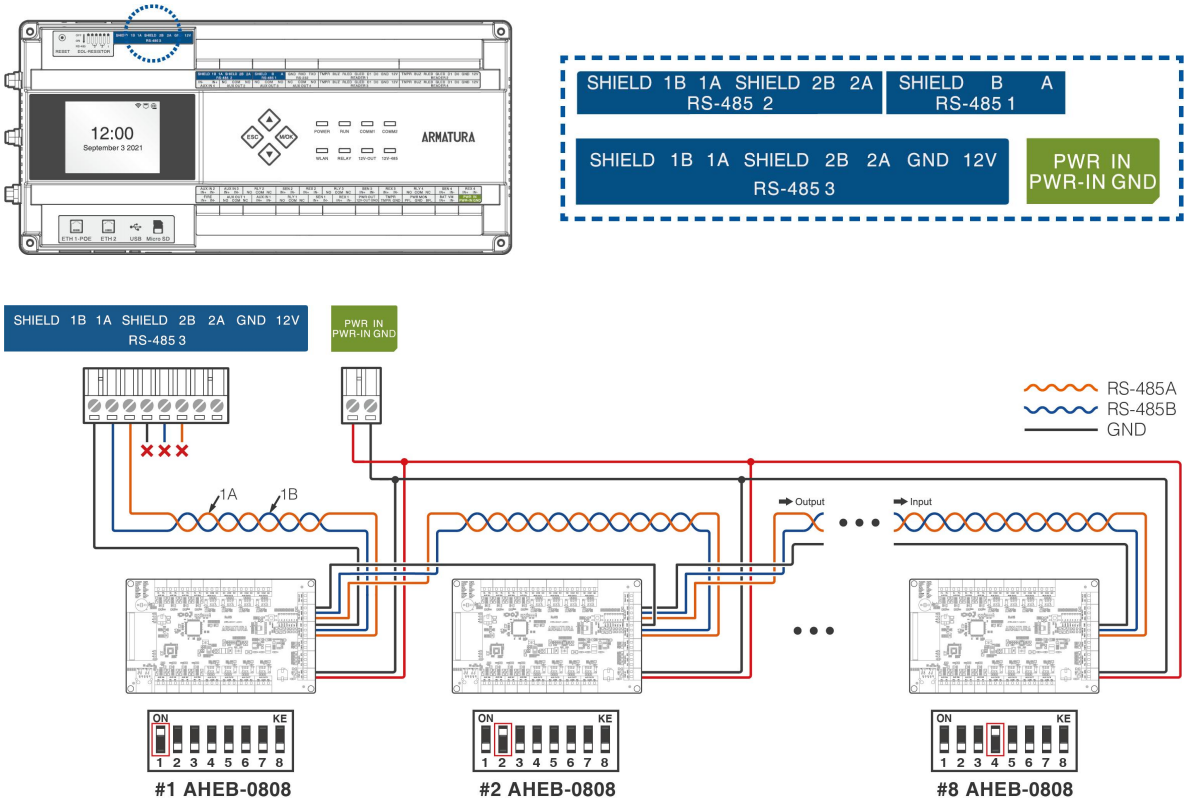
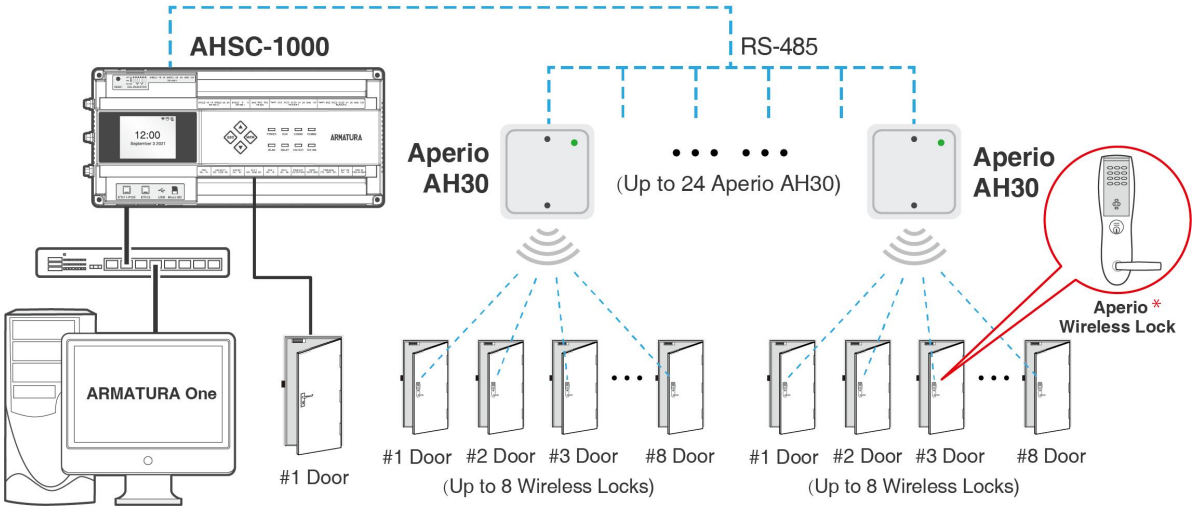


Figure 4-22 I/O Board Wiring

4.3.11.2 Connecting the Aperio AH30 hub to AHSC-1000 via RS-485



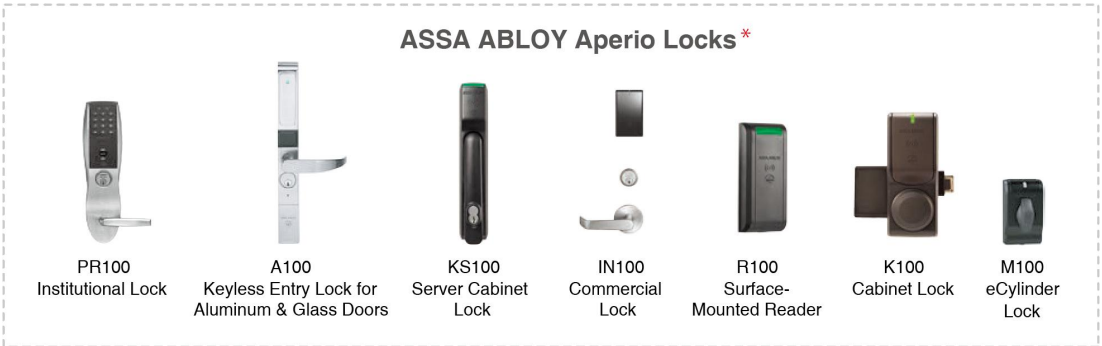
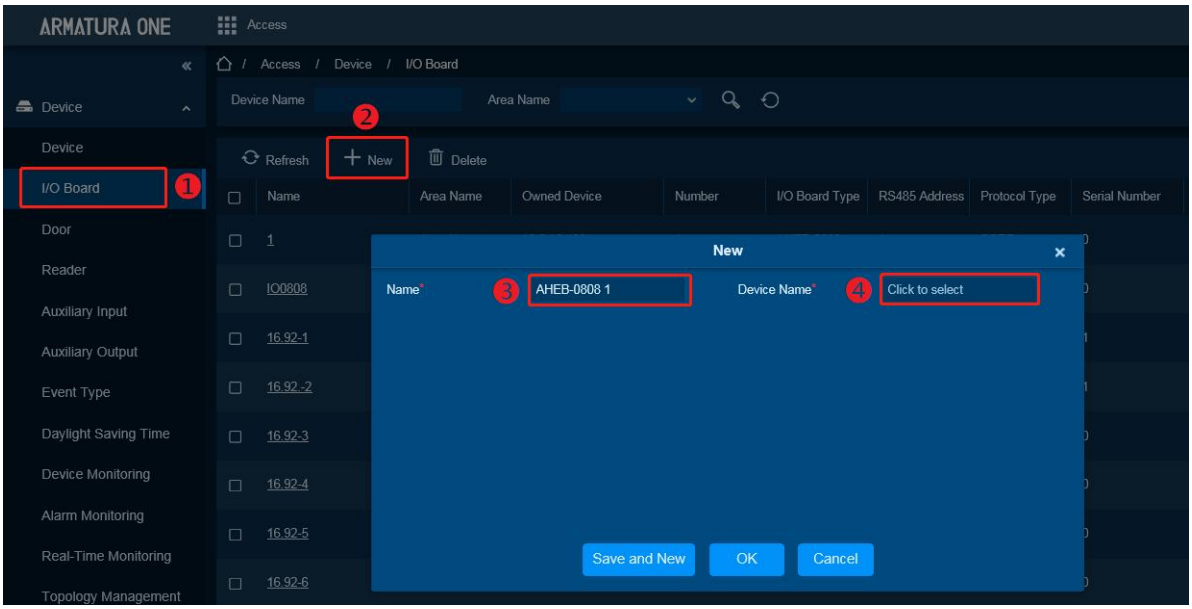


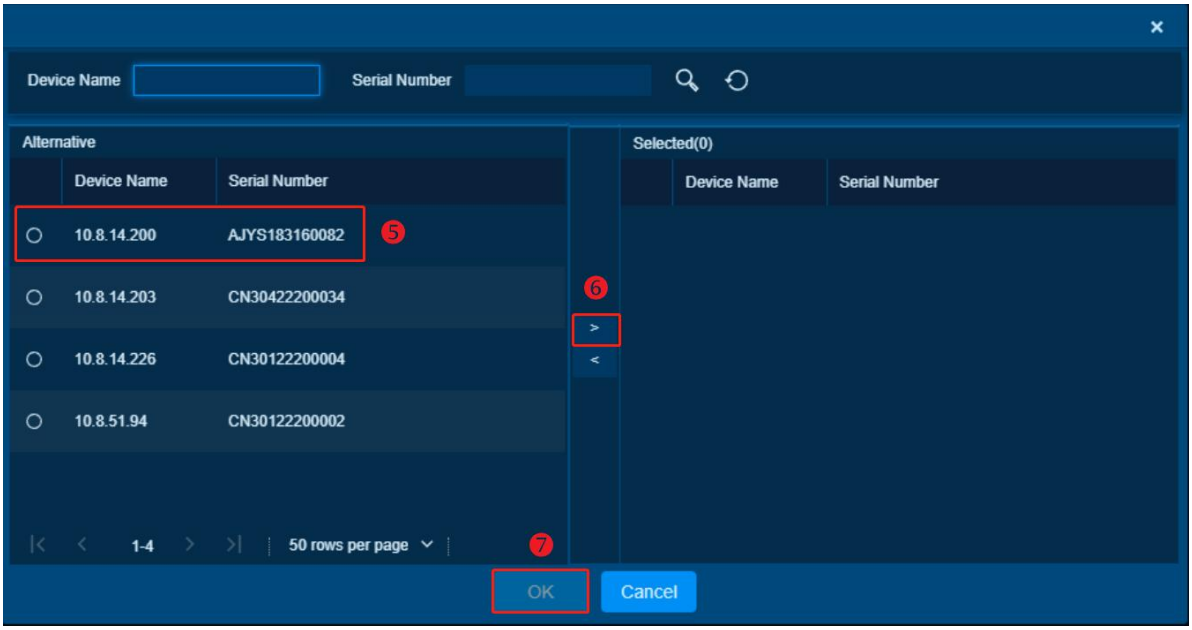
Figure 4-23 Aperio AH30 hub Wiring

1. Click **Access** > **Device** > **I/O Board** > **New** to display the new page.

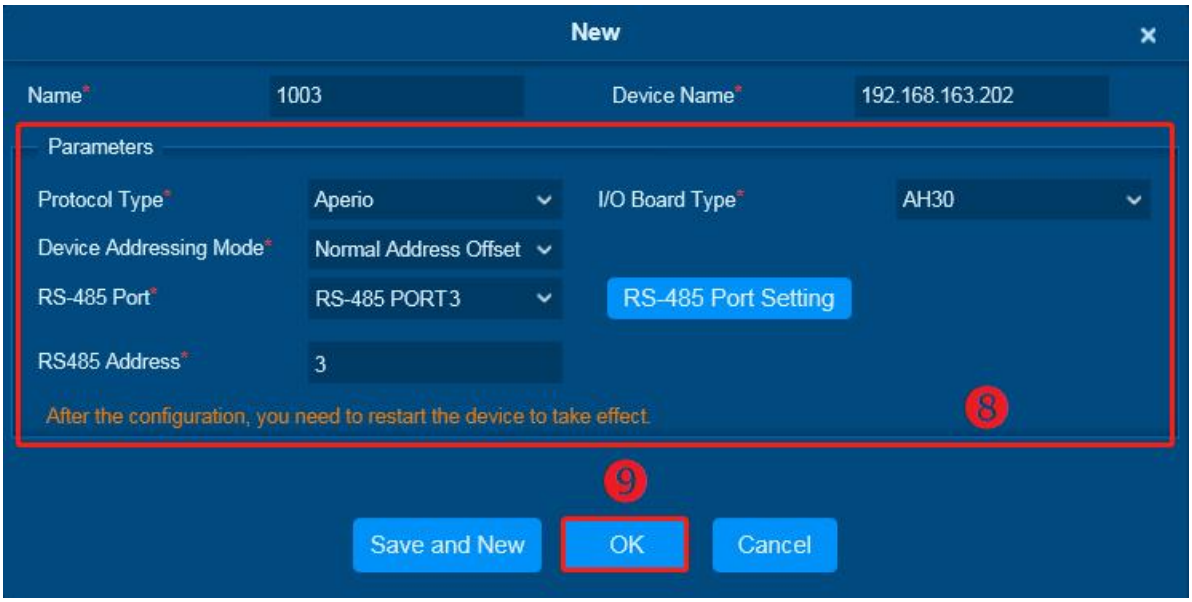
2. Enter **Name**.



3. Click on '**Device Name**' to open a device selection window. Choose the added controller from the list, and then click '**OK**' to save and exit.



4. Enter each corresponding parameters.



- **Device Addressing Mode:**

➢ Normal Address Offset

Addressing table – normal address offset

An AH30 communication hub can pair with up to 8 locks. When pairing several locks to a communication hub, the following addresses are used for the address range 1-15. Above this range only one lock can be paired.

DIP 4 – DIP 1	AH30 Hub address	Lock addresses
0000		Reserved
0001	0x01	0x01, 0x11, 0x21, 0x31, 0x41, 0x51, 0x61, 0x71
0010	0x02	0x02, 0x12, 0x22, 0x32, 0x42, 0x52, 0x62, 0x72
0011	0x03	0x03, 0x13, 0x23, 0x33, 0x43, 0x53, 0x63, 0x73
0100	0x04	0x04, 0x14, 0x24, 0x34, 0x44, 0x54, 0x64, 0x74
0101	0x05	0x05, 0x15, 0x25, 0x35, 0x45, 0x55, 0x65, 0x75
0110	0x06	0x06, 0x16, 0x26, 0x36, 0x46, 0x56, 0x66, 0x76
0111	0x07	0x07, 0x17, 0x27, 0x37, 0x47, 0x57, 0x67, 0x77
1000	0x08	0x08, 0x18, 0x28, 0x38, 0x48, 0x58, 0x68, 0x78
1001	0x09	0x09, 0x19, 0x29, 0x39, 0x49, 0x59, 0x69, 0x79
1010	0x0A	0x0A, 0x1A, 0x2A, 0x3A, 0x4A, 0x5A, 0x6A, 0x7A
1011	0x0B	0x0B, 0x1B, 0x2B, 0x3B, 0x4B, 0x5B, 0x6B, 0x7B
1100	0x0C	0x0C, 0x1C, 0x2C, 0x3C, 0x4C, 0x5C, 0x6C, 0x7C
1101	0x0D	0x0D, 0x1D, 0x2D, 0x3D, 0x4D, 0x5D, 0x6D, 0x7D
1110	0x0E	0x0E, 0x1E, 0x2E, 0x3E, 0x4E, 0x5E, 0x6E, 0x7E
1111	0x0F	0x0F, 0x1F, 0x2F, 0x3F, 0x4F, 0x5F, 0x6F, 0x7F

When configuring installations that differ from the default configuration described in section DIP 1-5 – Selecting the EAC address/Automatic paring on page 38, use this table to keep track of what addresses are used by the locks/sensors in your installation in order to avoid addressing conflicts according to section *"Installation examples" on page 44* for mixed installations.

Aperio® Online Mechanical Installation Guide, Document No: ST-001323-E Date: 30 mars 2016

- Legacy Address Offset

Addressing table – legacy address offset

Legacy addressing mode is an alternative addressing mode that can be set by the Programming Application in the configuration wizard. The lock addresses in this mode are set consecutively. For example, if communication hub has address 1, the locks will get address 1-8, 9-16, 17-24 etc.

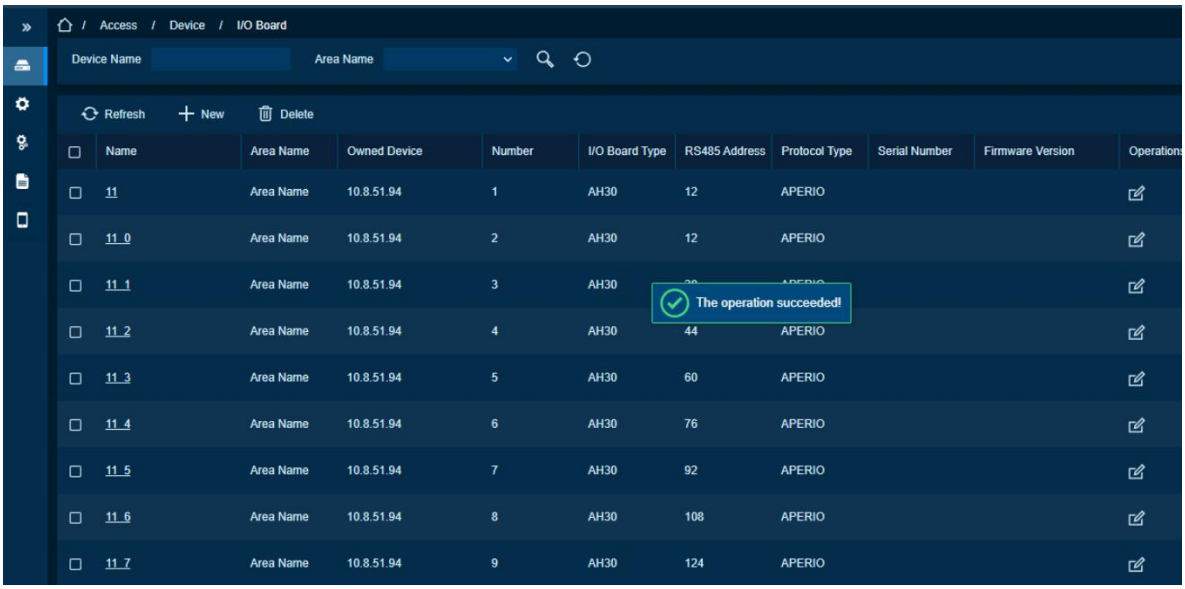
DIP 5 – DIP 1	AH30 Hub address	Lock addresses
0000		Reserved
0001	0x01	0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08
0010	0x02	0x09, 0x0A, 0x0B, 0x0C, 0x0D, 0x0E, 0x0F, 0x10
0011	0x03	0x11, 0x12, 0x13, 0x14, 0x14, 0x16, 0x17, 0x18
0100	0x04	0x19, 0x1A, 0x1B, 0x1C, 0x1D, 0x1E, 0x1F, 0x20
...		

This mode is used for older EAC systems that cannot handle high EAC addresses where the limit for example is 32 or 64.

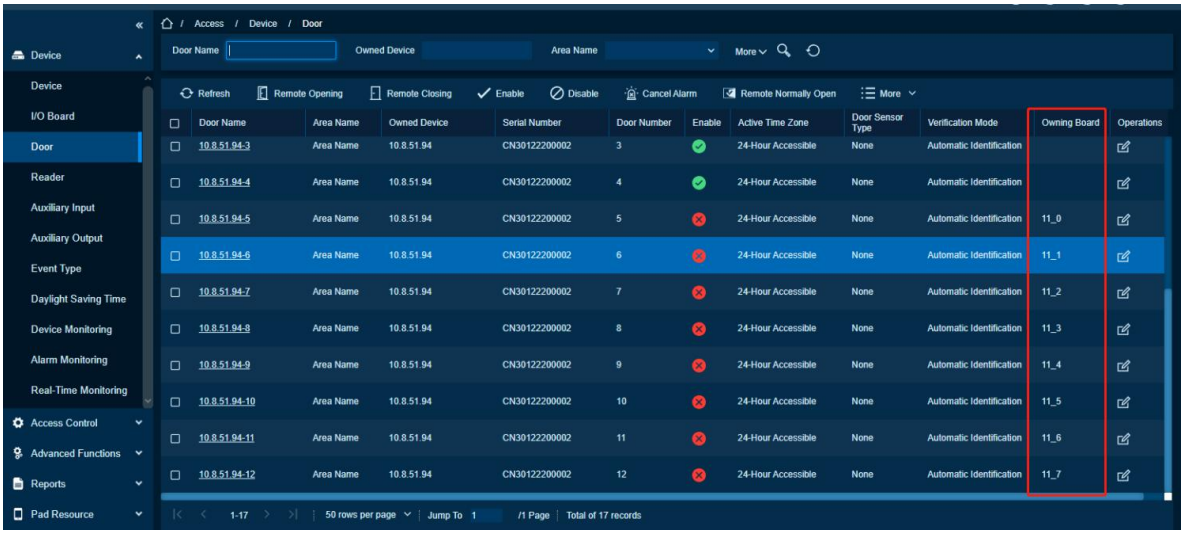
Note: *Image references the ST-001323-Aperio Online Mechanical Installation Manual-E-US.pdf.*

- **RS-485 Port:** The system will perform filtering based on the protocol.
- **RS-485 Address:** The RS-485 address range for Aperio AH30 is from 1 to 15.

5. Click **OK** to save and exit.



6. The system will generate several virtual devices in the I/O Board.



7. The system will automatically generate several doors that are bound to the corresponding owning board, which is created in the I/O Board Page.

Remarks:

1. Only the AHSC-1000 supports the connection with the Aperio AH30

2. **Feature Trigger Result:** This action will generate multiple virtual I/O Boards in [I/O Board] and Virtual Doors in [Door].

4.3.12 Line Monitoring

This device supports monitoring the status of various lines, such as the door sensor, exit button, and auxiliary input (e.g., alarm inputs). It can detect four types of line statuses: open, closed, short circuit, and broken circuit. The open and closed states represent the normal switching conditions of the line.

As depicted in the figure below, in case of a short circuit, the lines in positions 1 and 2 are connected, and in the event of a broken circuit, either the line in position 1 or 2 is disconnected.

Note:

- *The line monitoring feature requires the installation of two resistors on the door sensor, exit button, and auxiliary input lines. Custom End of Line (EOL) resistances can be configured via the host software, supporting resistors of 1.2K, 2.2K, 4.7K, and 10K.*

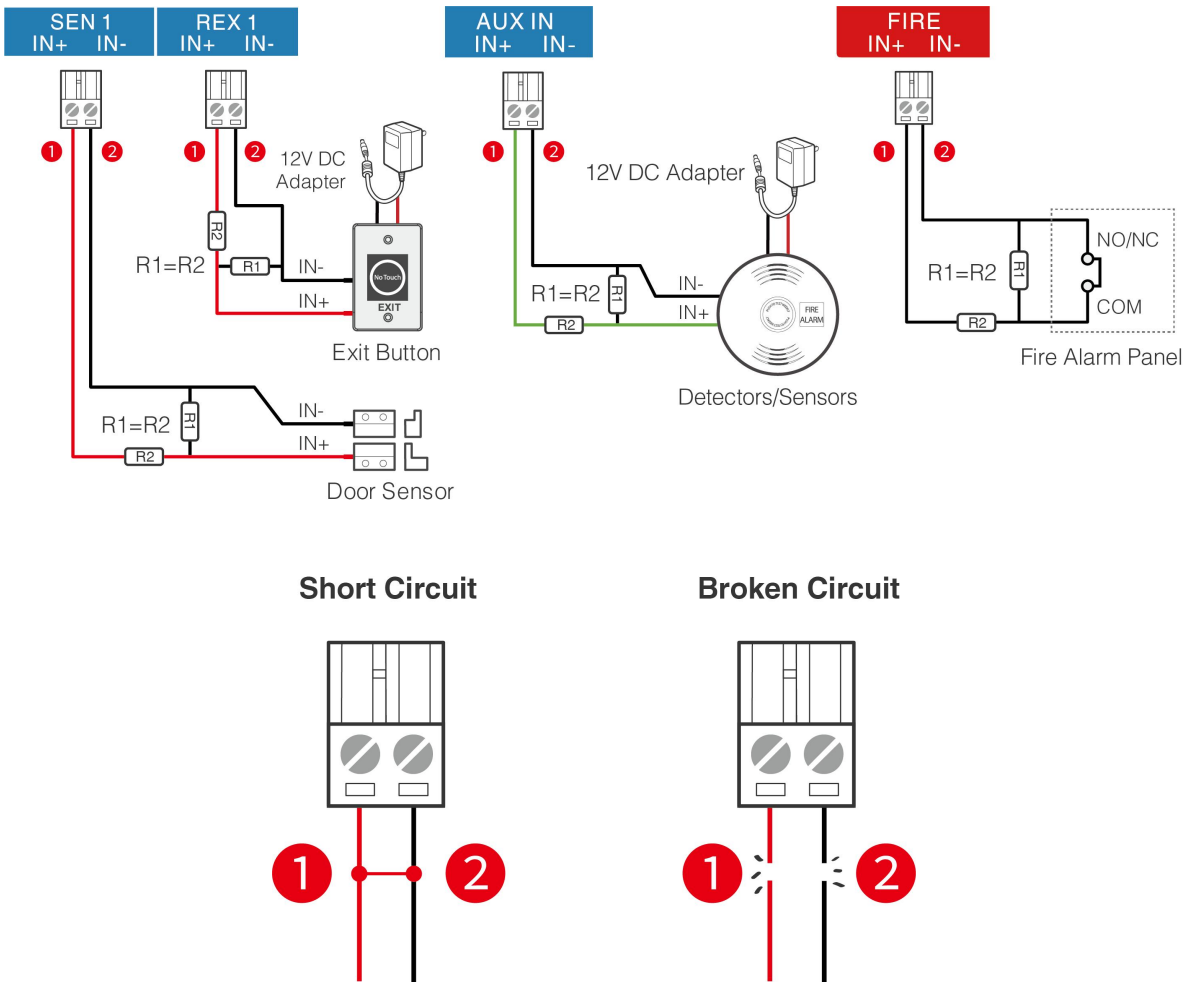


Figure 4-24 Line monitoring diagram

5. Equipment Communication

The server-based software can communicate with the system using two protocols (TCP/IP and Wi-Fi) for data exchange and remote management.

5.1 Access Control Network Wires and Wiring

1. The power supply is 12V DC converted from 220V or PoE.
2. Wiegand readers utilize 6-core shielded communication wires (RVVSP 6×0.5mm) to minimize interference during transmission. Users can choose between 6-core, 8-core, and 10-core options based on the available ports.
3. Due to its significant current, an electronic lock generates strong interference signals during operation. To mitigate this effect, it is recommended to use 4-core wires (RVVP 4×0.75mm^2), with two cores dedicated to the power supply and two for the door sensor.
4. RS-485 readers use 4-core communication shielded wires (RVVSP 4×0.5mm).
5. Other device cabling, such as exit switches, are typically constructed with 2-core wires (RVVSP 2×0.5mm^2).
6. Wiring Notes:
   - Signal wires, such as network cables, must not be run in parallel or share a casing pipe with large-power electric wires like electronic lock wires and power cables. If parallel wiring is necessary due to environmental constraints, ensure a minimum distance of 50cm between them.
   - Attempt to minimize the use of connectors when distributing conductors. If a connector is necessary, it must be crimped or welded. Avoid applying any mechanical force to the joint or branch of conductors.
   - For installations within a building, distribution lines must be laid either horizontally or vertically. To ensure proper protection, these lines should be encased in suitable casing pipes, such as plastic or iron water pipes, chosen based on the technical requirements of indoor distribution. For ceiling wiring, metal hoses can be used, provided they are securely fastened and have an aesthetically pleasing appearance.
   - Shielding Measures and Shielding Connection: If a survey before construction reveals significant electromagnetic interference in the wiring environment, it is essential to incorporate shielding protection for data cables when designing the construction plan. In cases where there is a substantial radioactive interference source or the wiring needs to run parallel to a large-current power supply on the construction site, overall shielding protection becomes necessary. Generally, shielding measures involve maintaining a maximum distance from any interference source and utilizing metal wiring troughs or galvanized metal water pipes to ensure reliable grounding of the connection between the shielding layers of data cables and the metal troughs or pipes. It is important to note that a shielding enclosure can only provide effective shielding when it is reliably.

- Ground Wire Connection Method: To establish a reliable ground wire connection in compliance with applicable national standards, employ sturdy large-diameter ground wires at the wiring site. Connect these ground wires in a tree-like configuration to avoid DC loops. Ensure these ground wires are positioned far away from lightning fields to prevent interference. Note that lightning conductors should not be used as ground wires, and precautions must be taken to prevent any lightning current from passing through ground wires during a lightning event.

  Metal wiring troughs and pipes must be continuously and securely connected, linking them to ground wires through large-diameter wires. The impedance of this wire section should not exceed 2 ohms. Additionally, the shielding layer must be connected reliably and grounded at one end to ensure a uniform current direction. Connect the ground wire of the shielding layer using a large-diameter wire, not smaller than 2.5mm².

5.2 TCP/IP Communication

100BASE-TX: For twisted pair connections, use either two unshielded twisted pairs or two Category 1 shielded twisted pairs, with a transmission distance of up to 328ft (100m). The Controller to Server and Inter-Controller communications are secured with 256-bit AES* symmetric encryption.

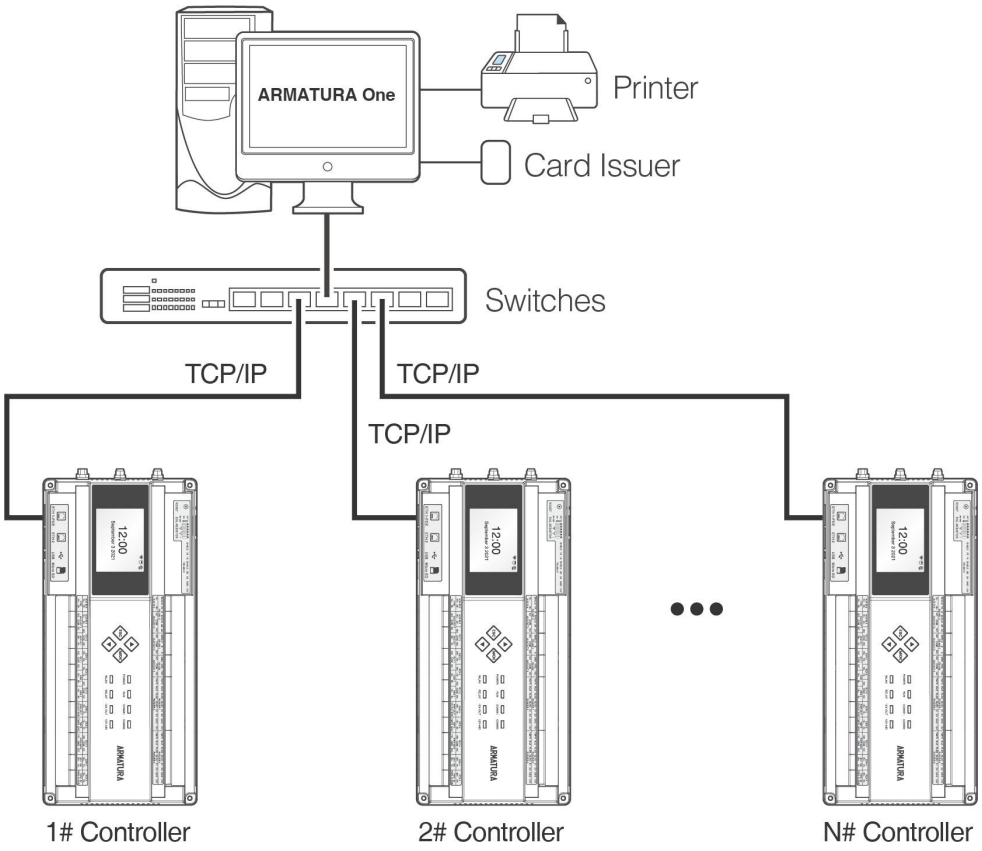


Figure 5-1 TCP/IP Communication System Networking

In the **ARMATURA One** software: Click **Access** > **Device** > **Device** > **Search** to find access controllers in the network, and directly add from the searching result.

5.3 Configuring Network Settings on the Controller Webserve

System admins can perform the following tasks by accessing the device's webserver.

1) Configuring the network and connecting to the software server.

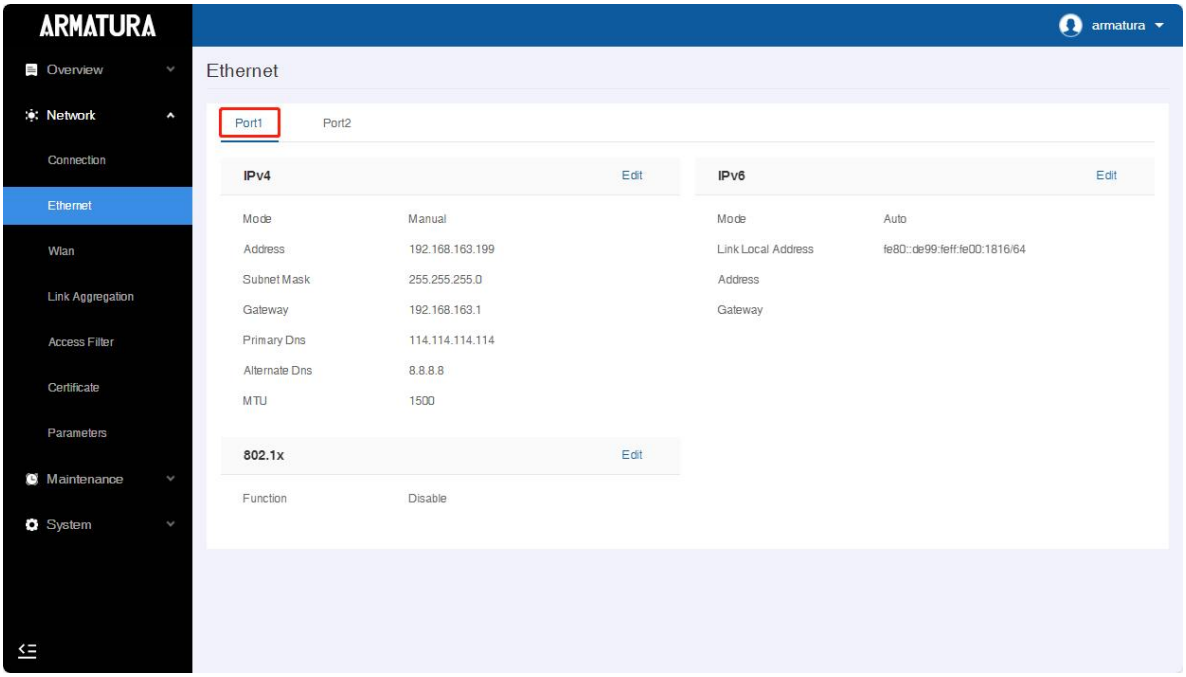
2) Real-time monitoring and troubleshooting of expansion devices, such as card readers, IO expansion boards, etc.

3) Perform equipment maintenance. Such as pulling debug records, remote initialization, reset parameters, and restart the equipment.

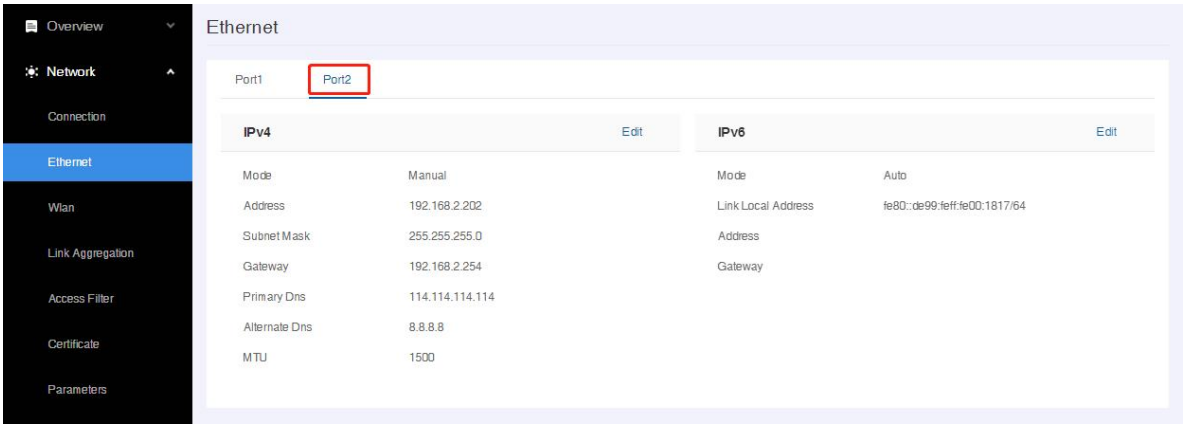
5.3.1 TCP/IP Settings

The ARMATURA Horizon Controller features dual Ethernet interfaces, and configuration of the IP addresses for both Port 1 and Port 2 is required. It's essential to ensure that the gateways of Port 1 and Port 2 are different, and their IP addresses must also be distinct. When connecting the controller to a TCP/IP reader, it is necessary to set the IP address of the expansion network card.

To access the setting interface for Ethernet. Please log in to the controller's Webserver, see 7.2 Login to the Webserver for details. Then click on **Network** > **Ethernet**. Modify the IP address and gateway address, as shown below.



For ETH 1, the parameters for IPv4, IPv6, and 802.1x configurations can be accessed and modified on the Port 1 page.



For ETH 2, the parameters for IPv4, IPv6, and 802.1x configurations can be accessed and modified on the Port 2 page.

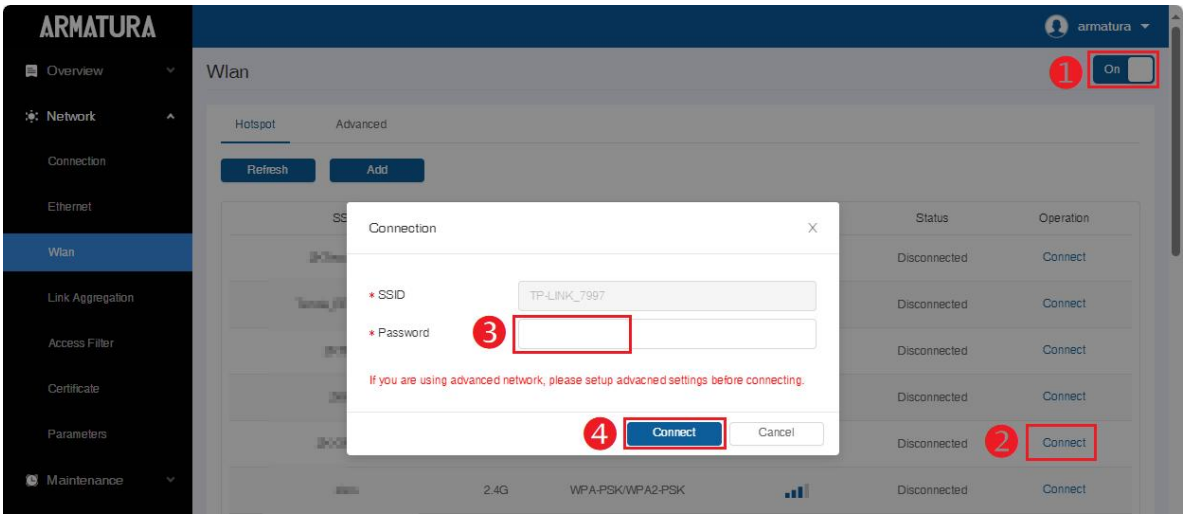
5.3.2 Wireless Network Settings

The Wi-Fi module facilitates data transmission via the Wi-Fi antenna, creating a wireless network environment. The controller comes with Wi-Fi enabled by default. If Wi-Fi is not required, you can toggle the Wi-Fi using the enable/disable button.

Searching the Wi-Fi Network

1. Click **Network** > **Wlan** to enter the wlan setting interface on the webserver. Then click the On switch in the upper right corner of the interface to turn on the wireless network function. Once the Wi-Fi is turned on, the controller will automatically search for the available Wi-Fi within the network range.

2. Select the required Wi-Fi SSID from the available list and click **Connect**, and then input the correct password in the pop-up password interface, and click **Connect** when complete.

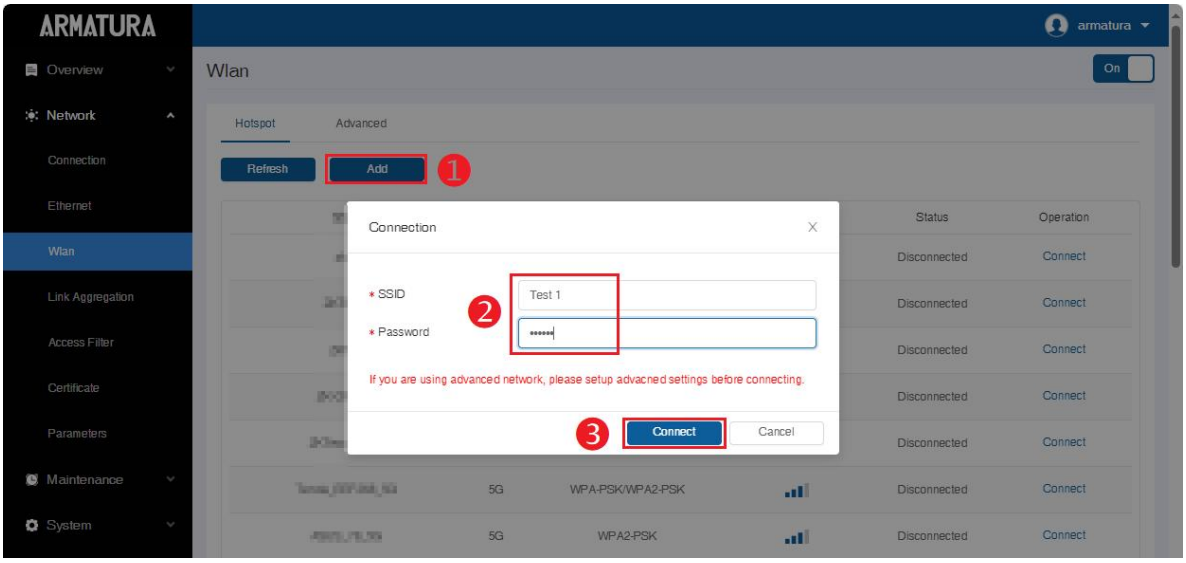


3. When the Wi-Fi is connected successfully, the Wi-Fi status shows as **Connected**.

Adding Wi-Fi Network Manually

The Wi-Fi can also be added manually if the preferred Wi-Fi does not show on the list.

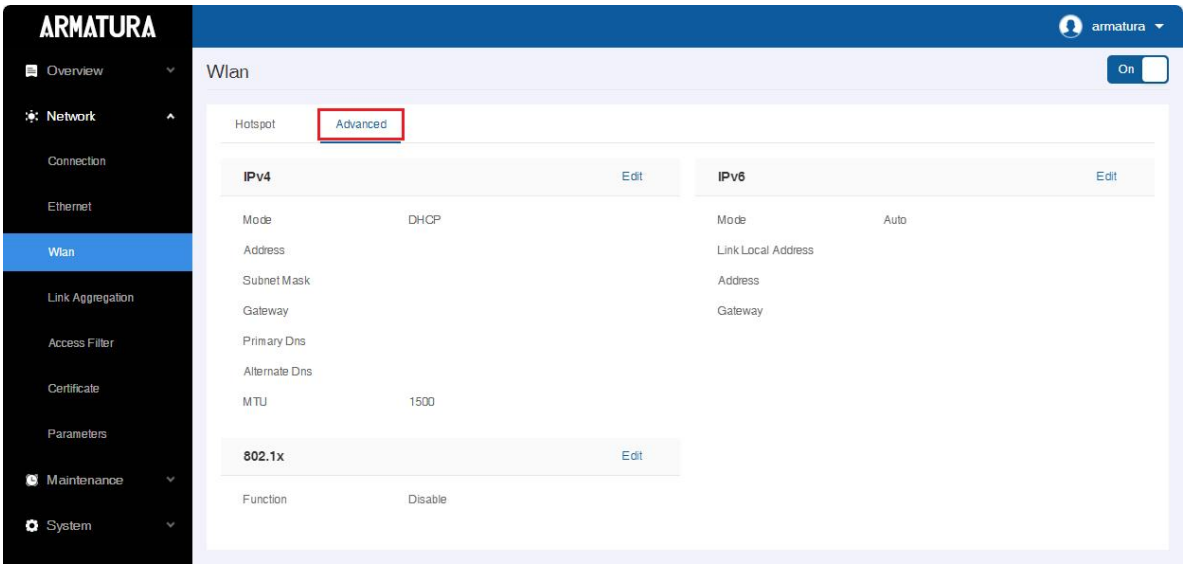
Click **Add** on the wlan setting interface. On the pop-up interface, enter the Wi-Fi network parameters. (The added network must exist.)



***Note:** After the preferred Wi-Fi is successfully added manually, click **Refresh** to search for this Wi-Fi and then click **Connect** to enter the password to connect.*

Advanced Setting

To configure the relevant parameters as required, navigate to the Advanced settings on the Wireless Network interface. In the advanced settings interface, you can configure the parameters for IPv4, IPv6, and 802.1x as needed.



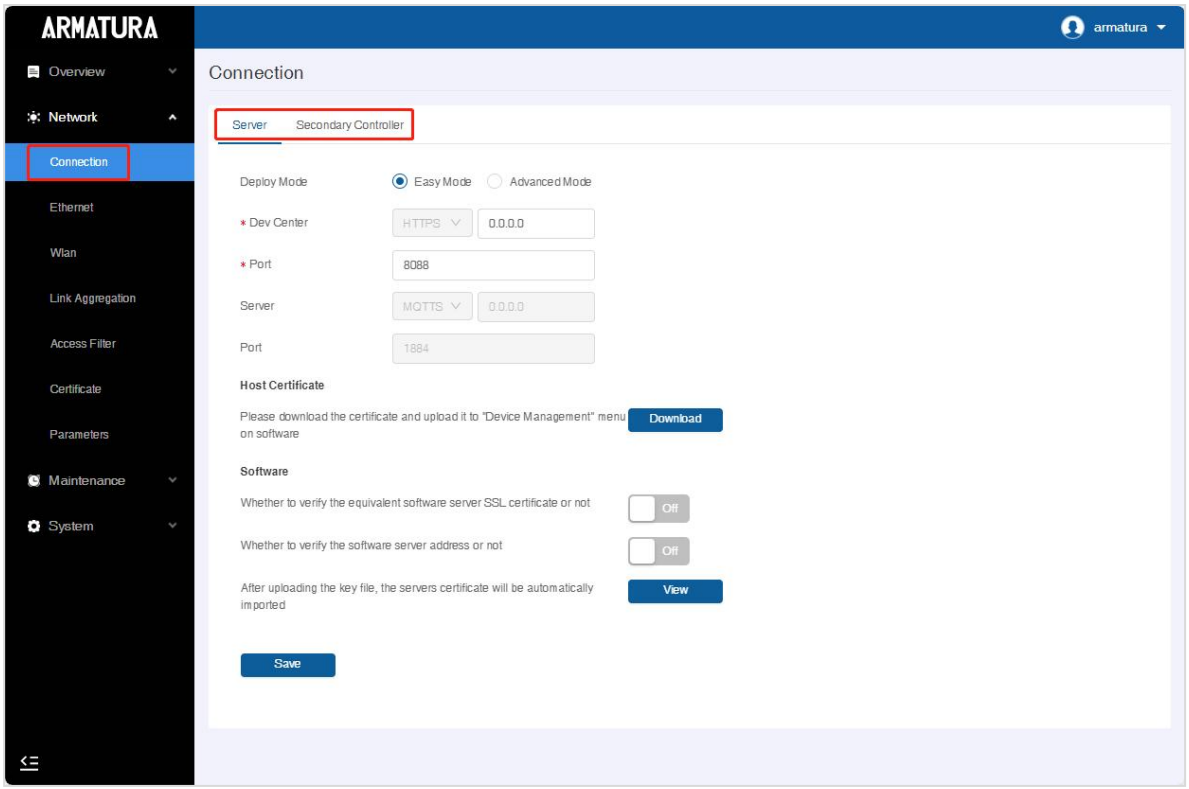
Remarks:

1. *The PC (server) must share the same network segment with the router (wireless network).*
2. *You must add the control panel to the software through TCP/IP before setting Wi-Fi parameters.*

5.3.3 Setting up the Server/Secondary Controller

The Armatura Horizon Controller can only be configured to connect with either a server or a secondary controller.

Click on "**Network**" and then select "**Connection**" to access the Server/Secondary Controller Setting interface on the webserver. Refer to 7.3.1 Connection Settings for details.

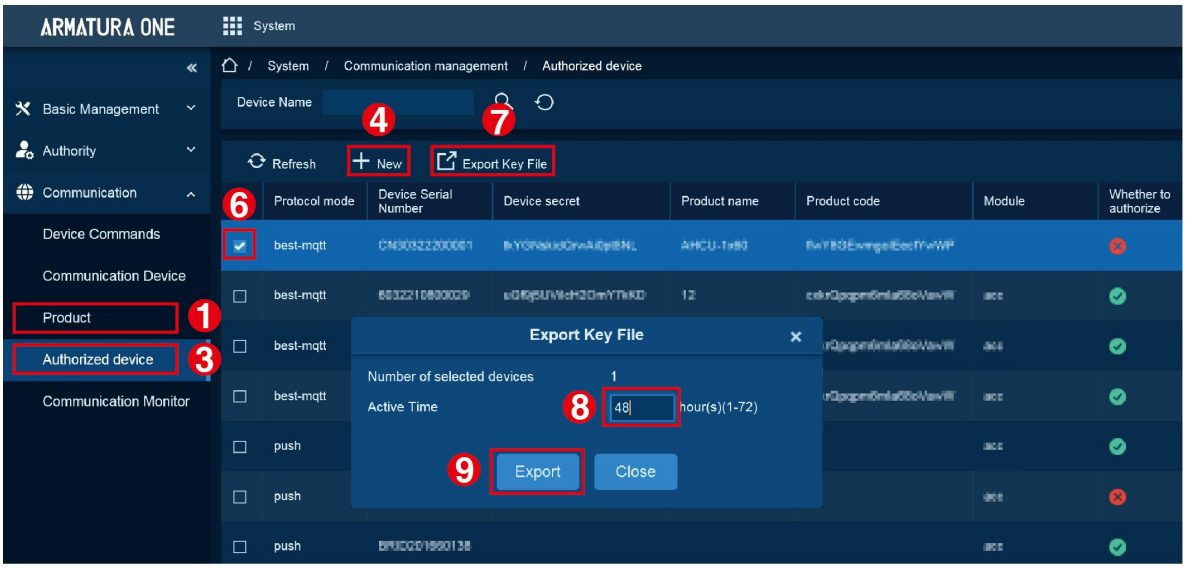


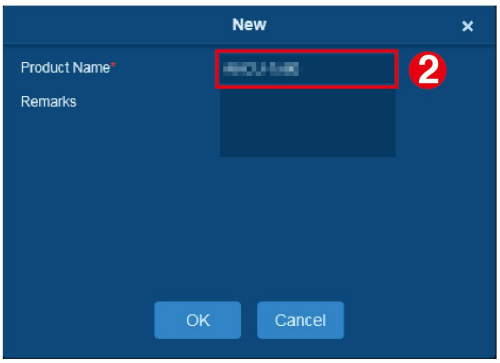
6. Connect to the ARMATURA One Software

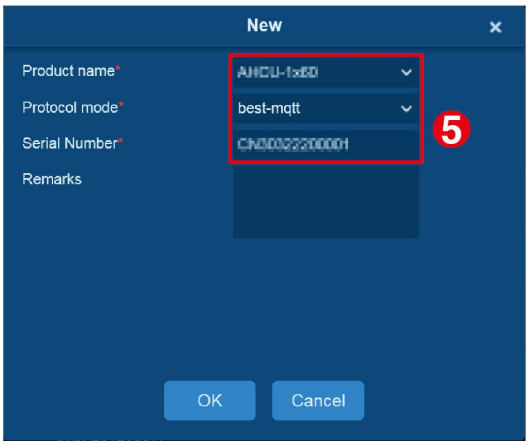
6.1 Export the Key File

Log in to the ARMATURA One software and perform the following steps.

1. Click **System** > **Communication** > **Product** > **New** to add a new product name.
2. Click **System** > **Communication** > **Authorized device** > **New** to add a new authorized device. You can click **System** > **About** to view the serial number.
3. To export the device key, check the key to be exported, click '**Export Key File**', enter the active time, and then click '**Export**'. This action will generate a key file.

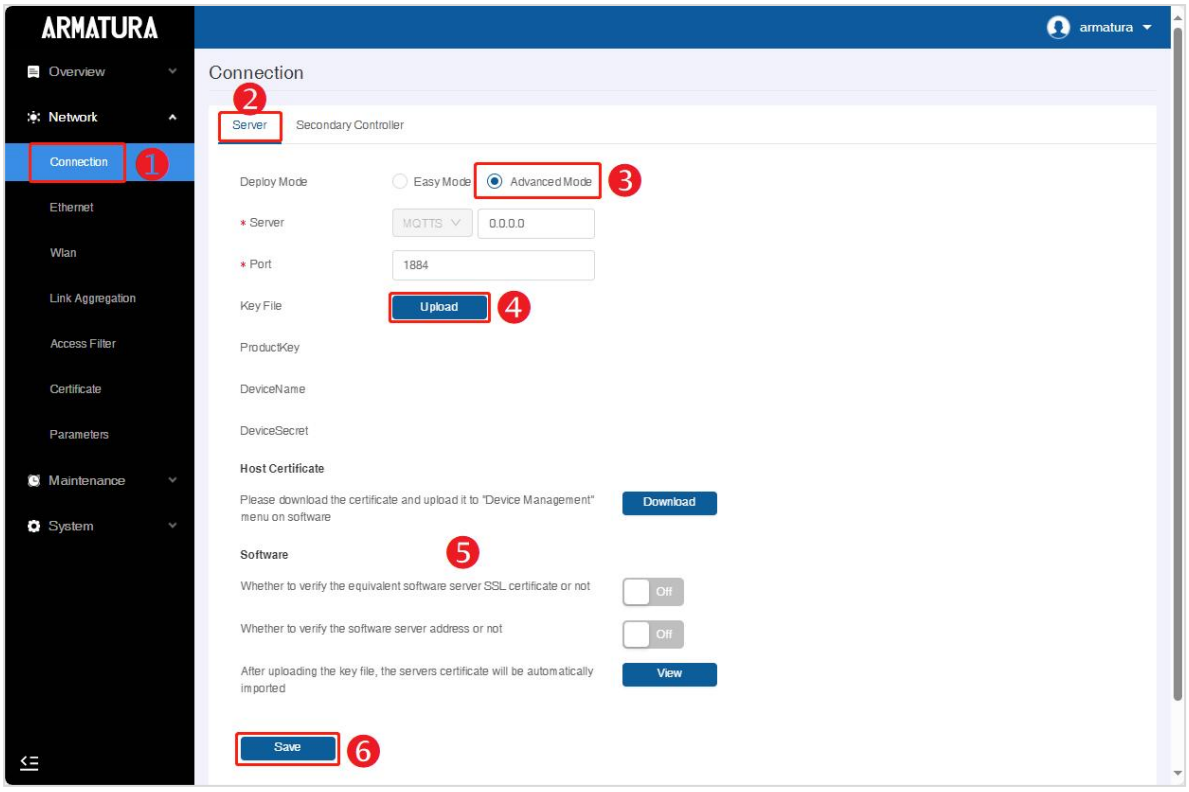






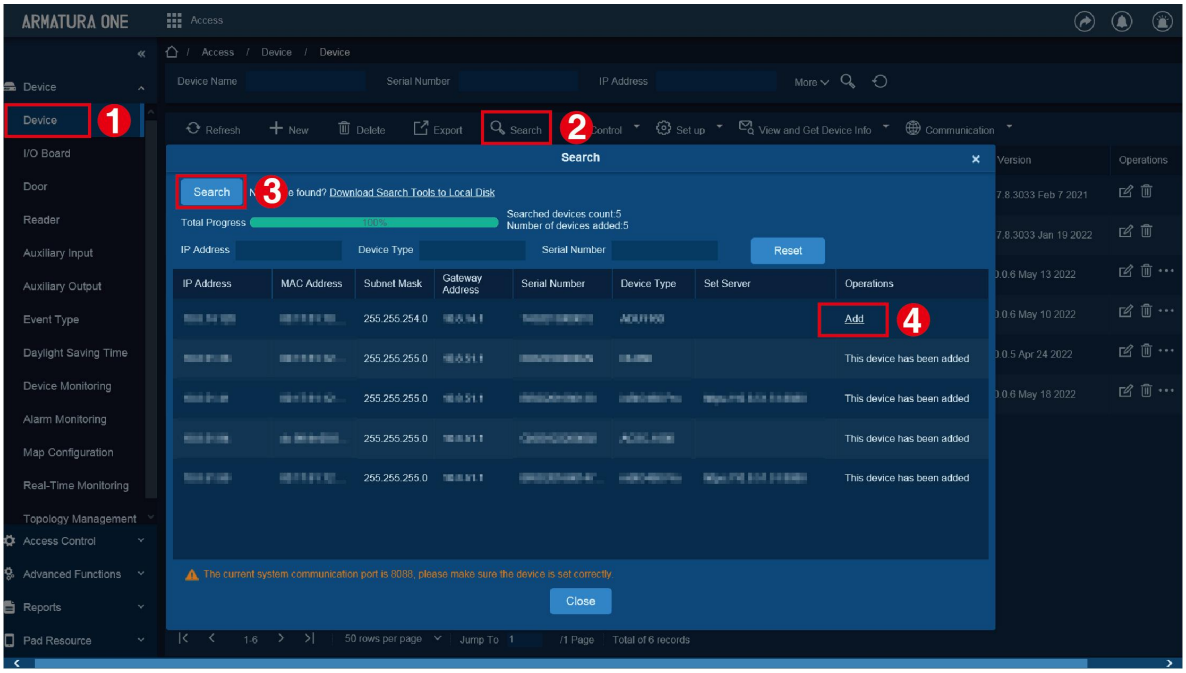
6.2 Server Connection Configuration

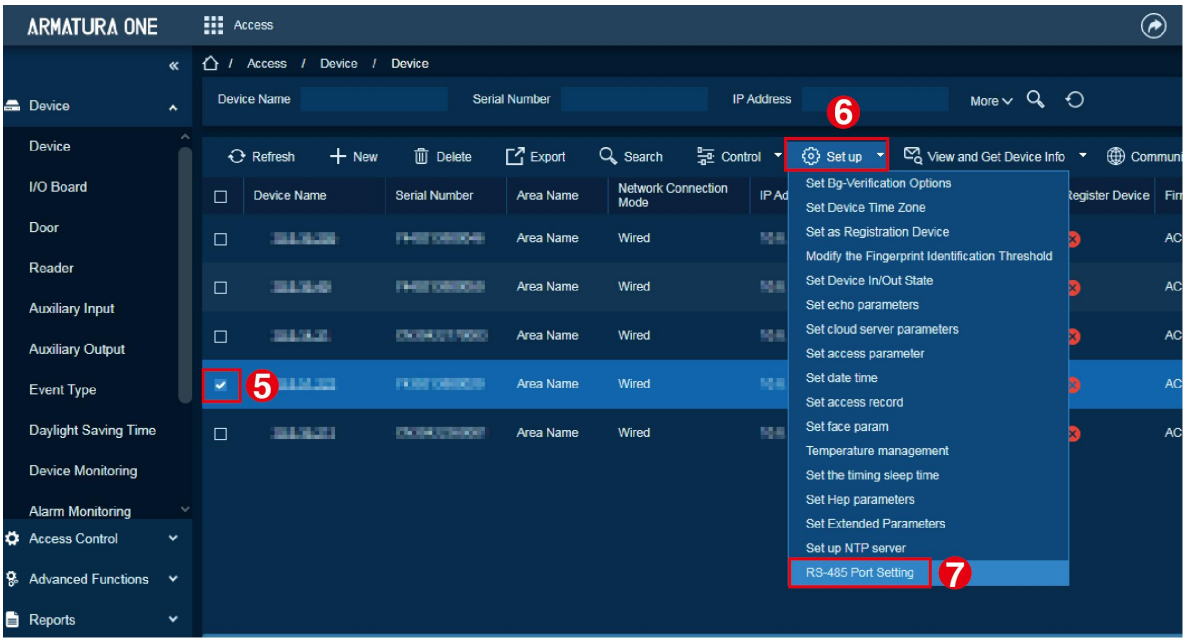
1. Click **Network** > **Connection** > select **Server** to enter the Server/Secondary Controller Setting interface on the webserver.
2. Enter the address and port of the server.
3. Click **Upload** to upload the key file obtained in step 1, then click **Save**.

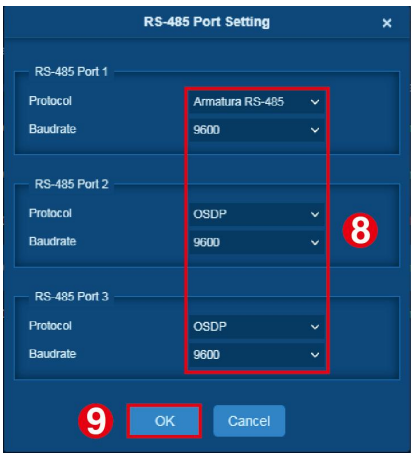


6.3 Add Device on the Software

1. Click **Access** > **Device** > **Device** > **Search**, to open the Search interface.
2. After clicking **Search**, the list and the total number of Access Control Devices will be displayed.
3. Click the **Add** button next to the Device to add the Device.
4. Click **Set up** > **RS-485 Port Setting** to configure the device's RS-485 port.



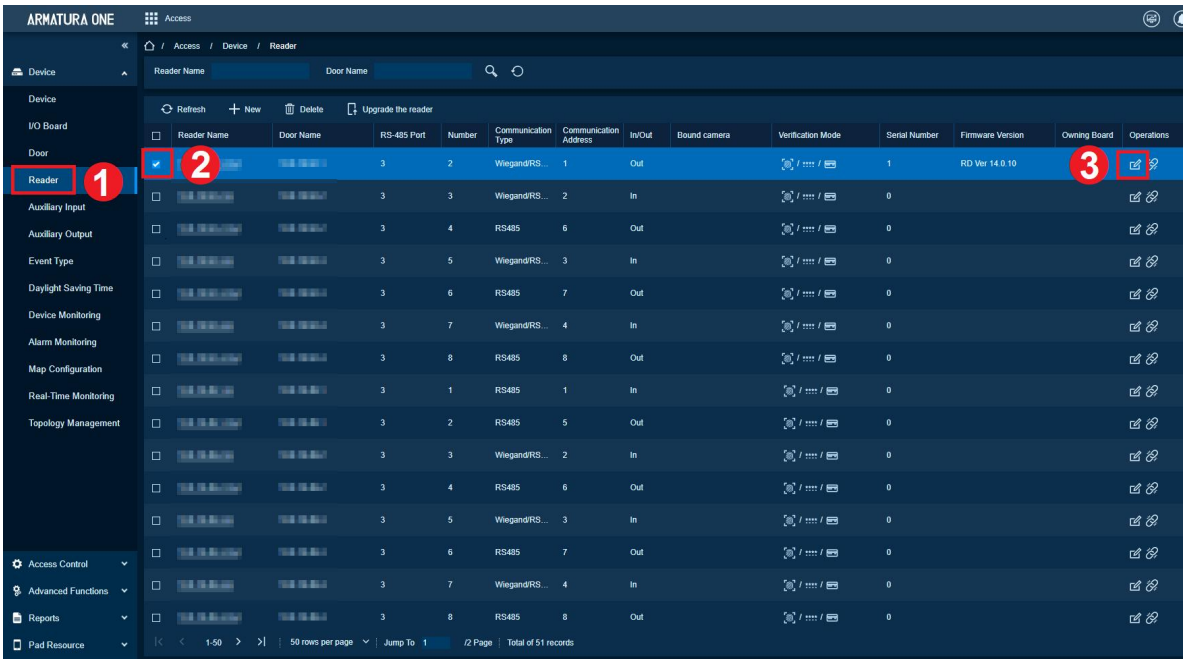


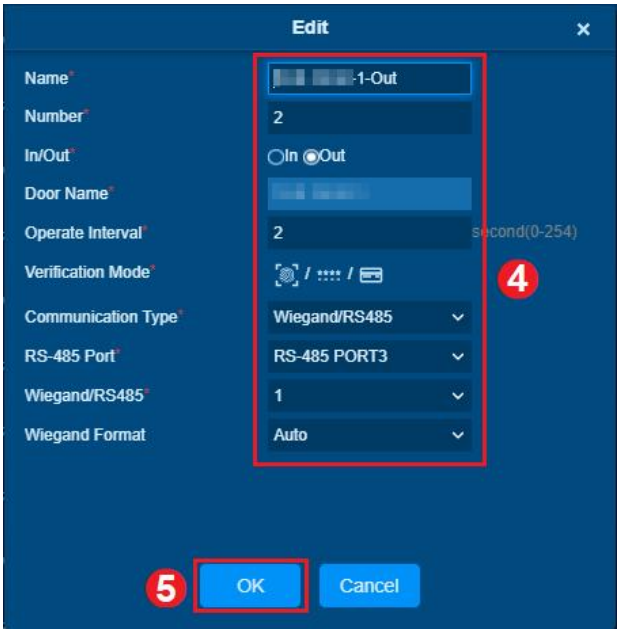


6.4 Configuring the Reader

1. When an RS-485 reader is connected. Refer to 4.3.10 RS-485 Reader Wiring to configure the EOL resistor for the RS-485 port.

2. Click **Access** > **Device** > **Reader**, to configure the parameters of the reader. As shown in the figure below.



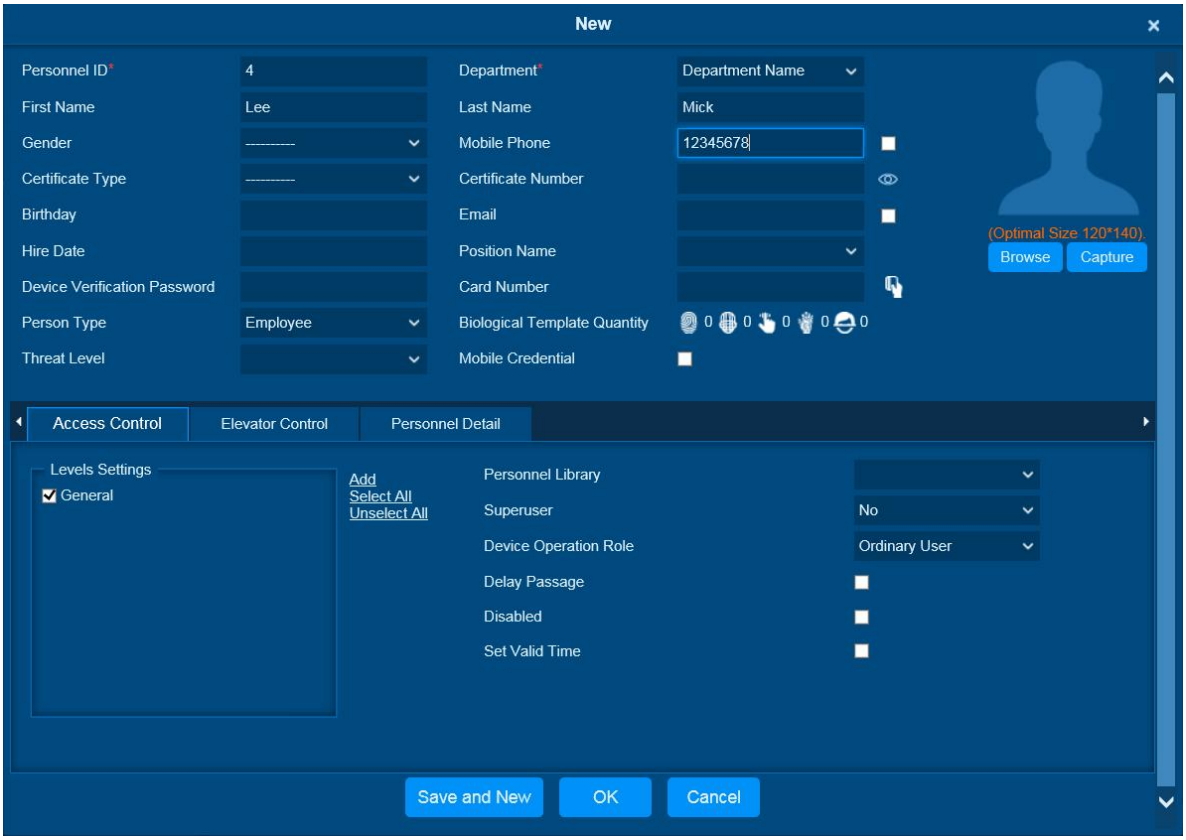


3. After the configuration is completed, the reader can be used normally.

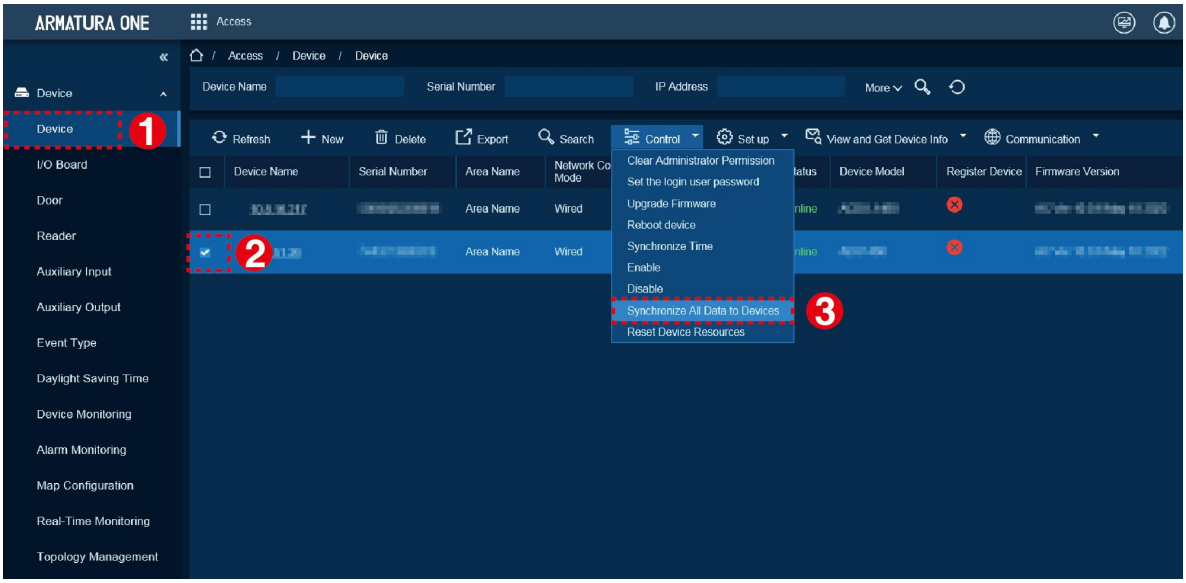
6.5 Add Personnel on the Software

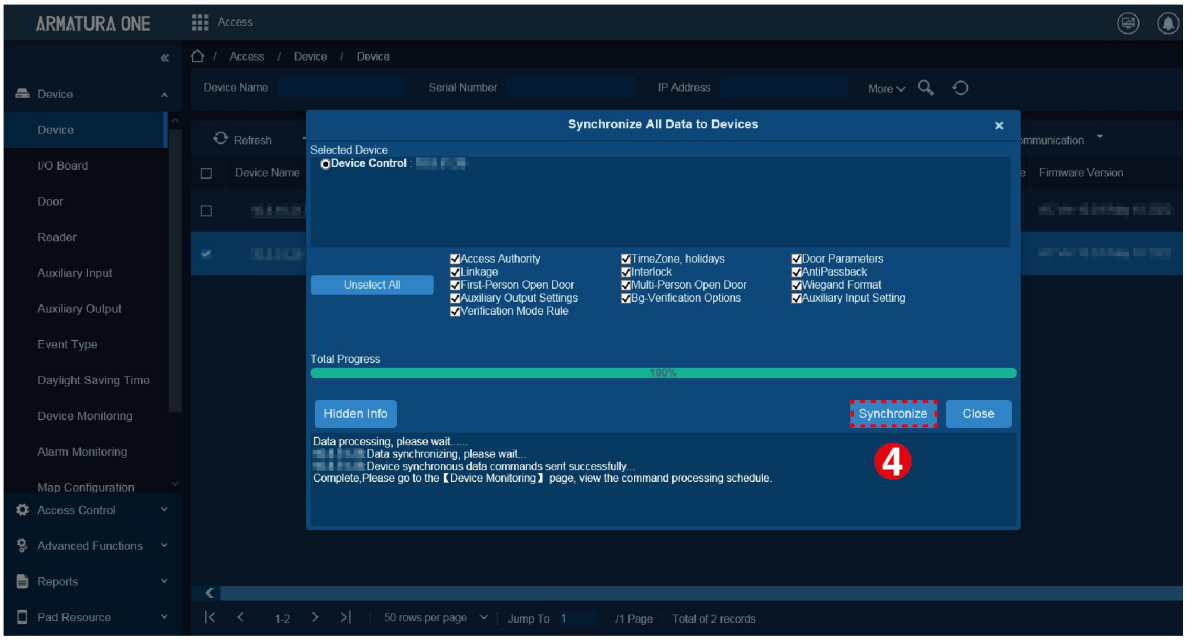
1. Click **Personnel** > **Personnel** > **New** to add a new personnel.

2. Fill in all the required fields and click **OK** to register a new user.



3. Click **Access** > **Device** > **Control** > **Synchronize All Data to Devices** to synchronize all the data to the device including the new users.





Note: *For other specific operations, please refer to the relevant software user manual.*

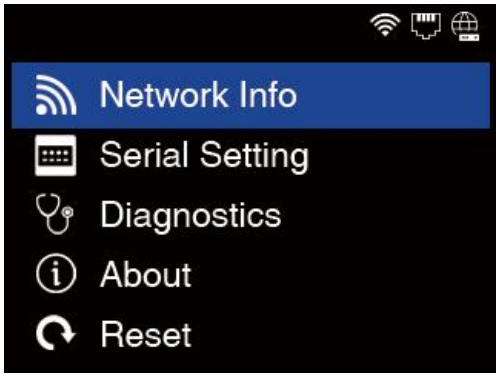
7. Connect to the Webserver

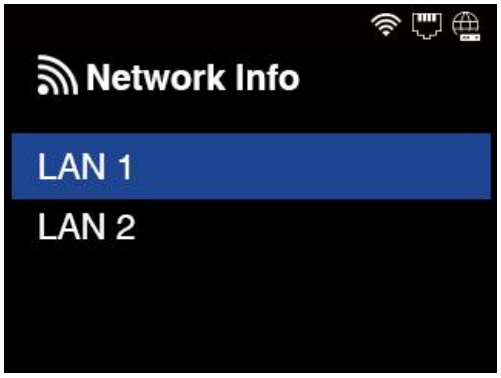
7.1 Opening the Webserver on the Browser

After powering on the controller, connect it using a network cable. Access the webserver by entering the IP address and server port in the address bar of your browser. The IP address is set as follows:

- **IP address: https://device's IPv4(or IPv6) address:port**.The default IP is 192.168.1.201. (for example: https://192.168.1.201:443).
- **Port:** By default, the port is **443**. The default port 443 for HTTPS service can be ignored.

- You can also click the **M/OK** button > **Network Info** > **LAN1/LAN2** to view the device IP address on the screen of the controller. As shown below.



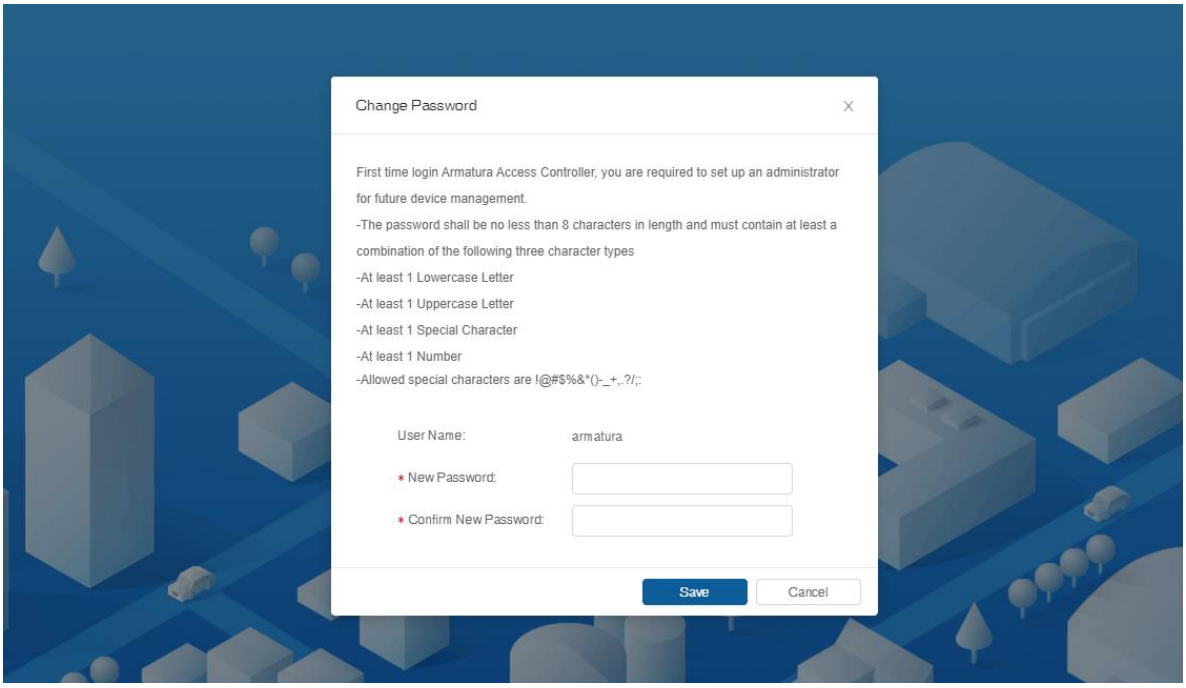


Status of Icons:

Status Icon	Name	Description
	Wi-Fi signal	The Wi-Fi connection is normal.
	Ethernet	Indicates that the connection to Ethernet has been established.
	ADMS Server	Indicates that the connection between device and ADMS server is successful.

7.2 Login to the Webserver

To begin, access the login interface and enter the default administrator account and password (default is **armatura**). Click on the '**Login**' button. Upon the first-time login to the webserver, you will be prompted to modify the admin's password(default is armatura account).



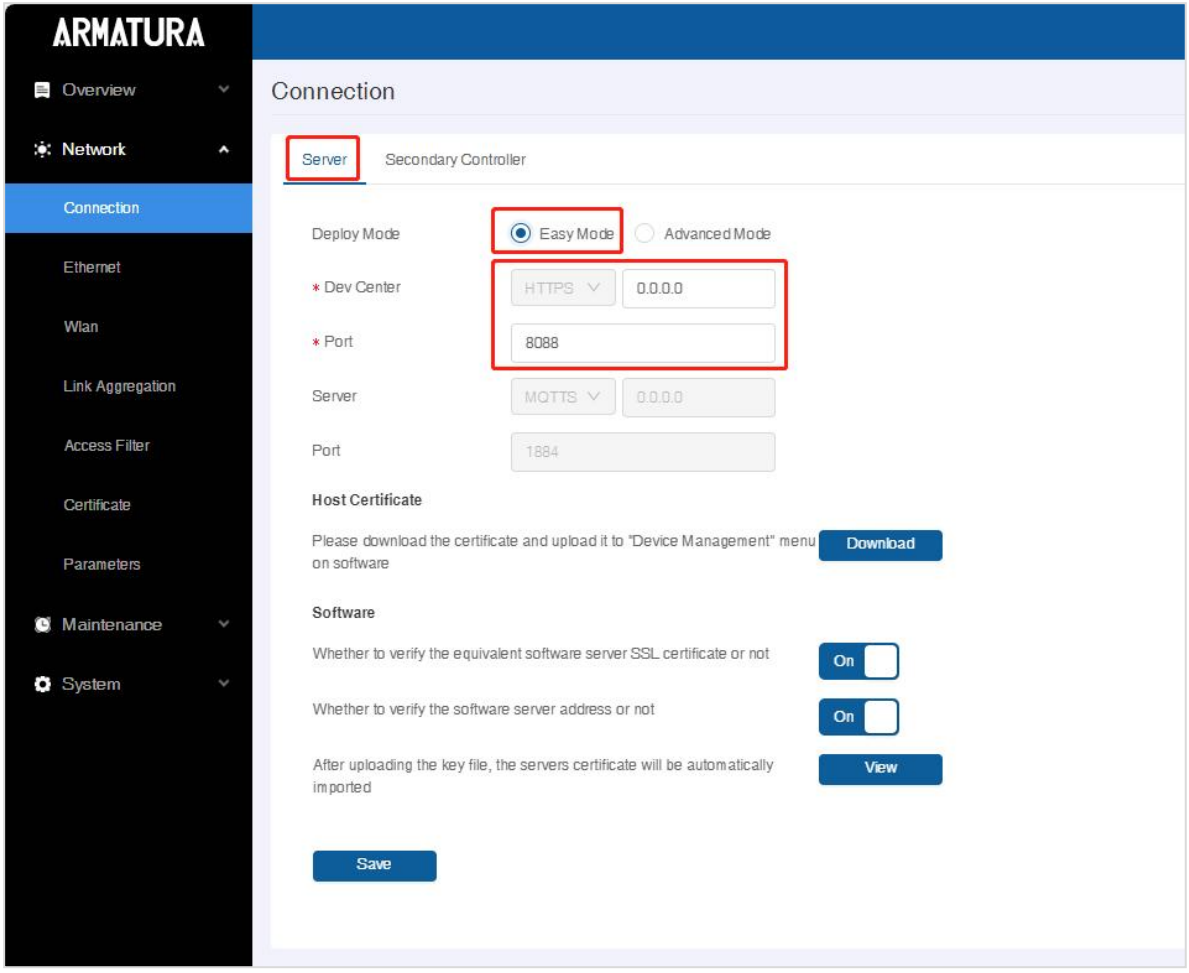
7.3 Network Settings

7.3.1 Connection Settings

The Armatura Horizon Controller can only be configured to connect with either a server or a secondary controller. Users can set the relevant parameters here.

Server Connection Configuration

- **Easy Mode**



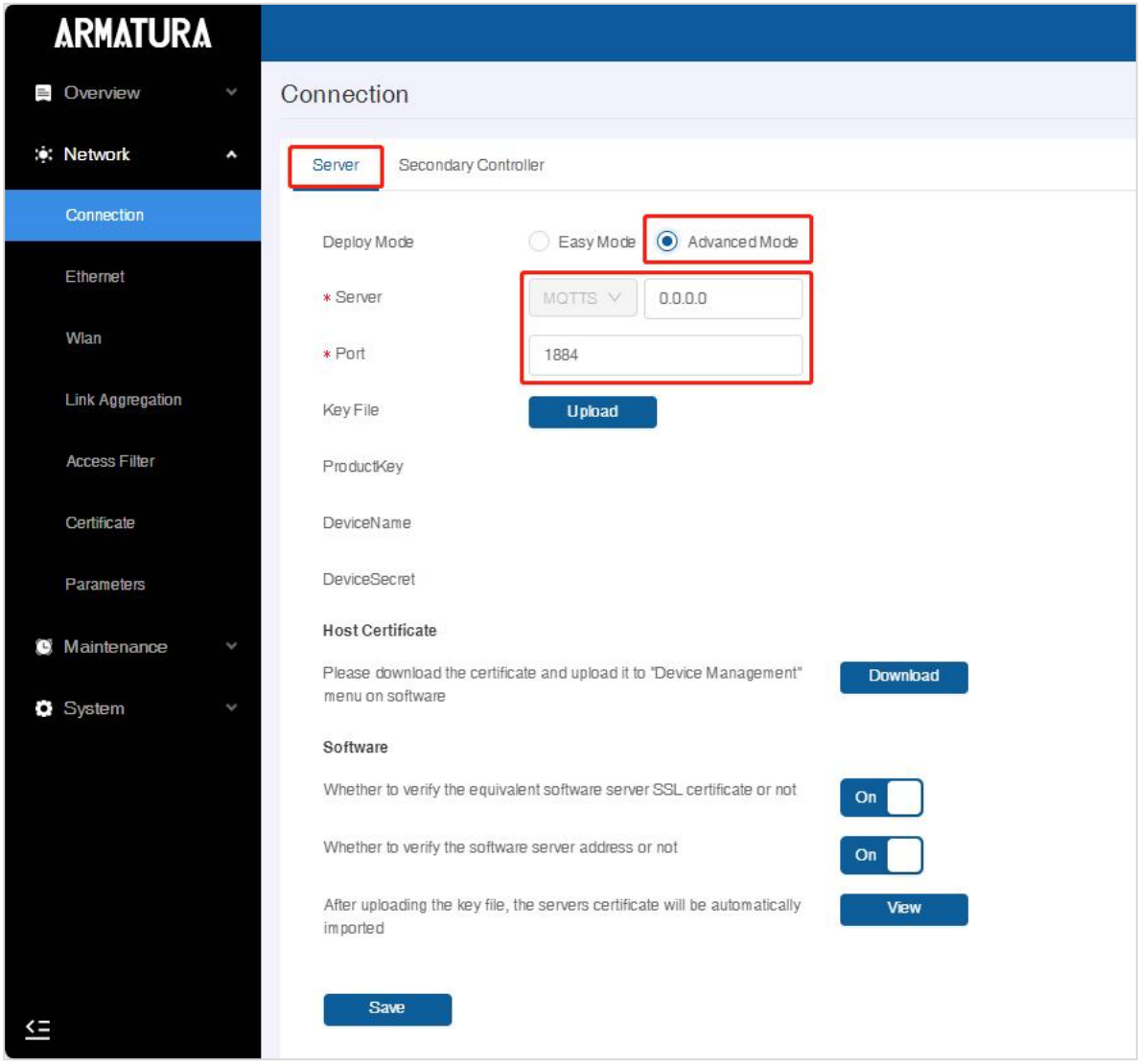
Dev Center: The protocol and address of the server.

Port: The port of the server, usually defaults to **8088** (depending on the situation).

Host Certificate: For two-way authentication, download the controller certificate and import it into the software. The default setting is one-way authentication.

Software: To view the software certificate.

- **Advanced Mode**



Server: The protocol and address of the server.

Port: The port of the server, the default is **1884**.

Key File: Click '**Upload**' to upload the key file exported from the ARMATURA One software. The system will automatically backfill any other relevant information.

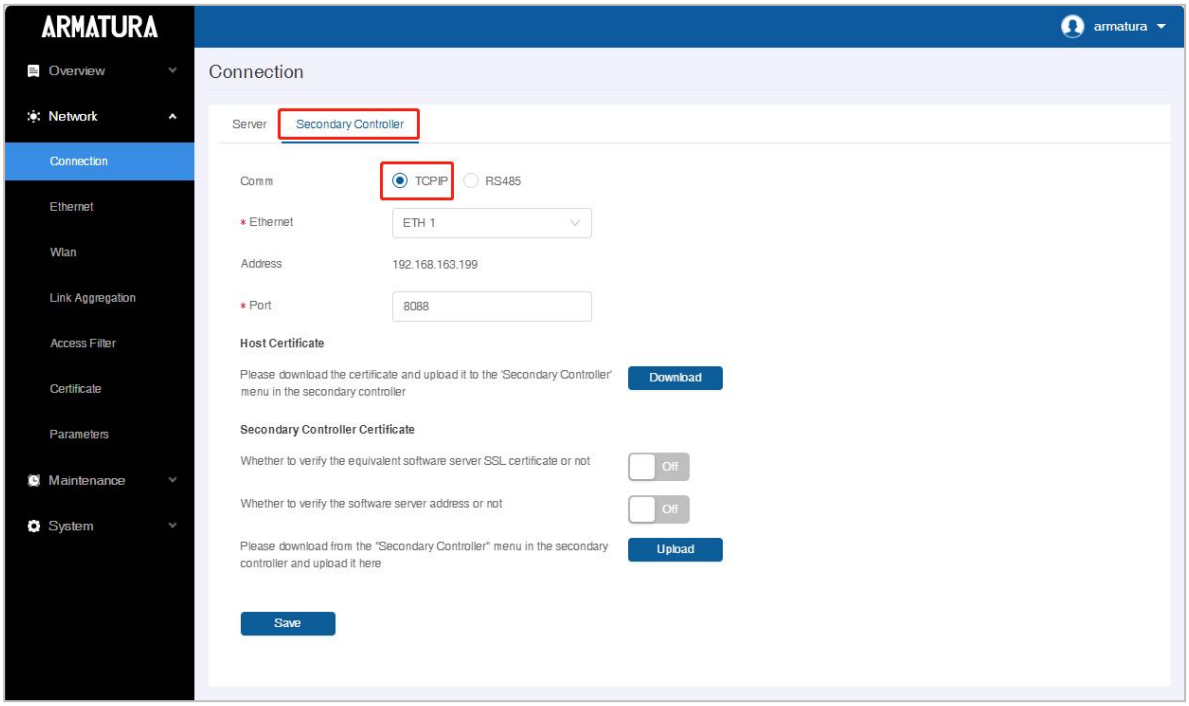
Host Certificate: For two-way authentication, download the controller certificate and import it into the software. The default setting is one-way authentication.

Software: To view the software certificate.

Secondary Controller Connection

The secondary controller has two communication methods, including TCP/IP and RS-485. As shown below.

- **TCP/IP**



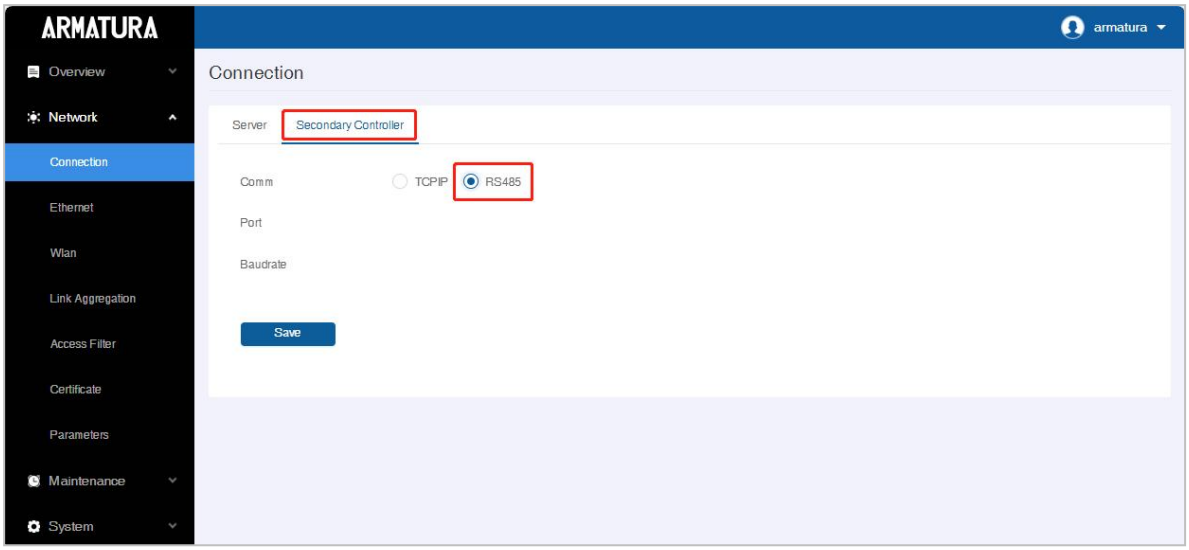
Ethernet: You can select the controller's ETH1 (default IP 192.168.1.201) or ETH2 (default IP 192.168.2.202).

Port: This port is usually used for slave connection use and can be set according to the actual situation. The default is 6666.

Host Certificate: For two-way authentication, download the controller certificate and import it into the slave AHDU. The default setting is one-way authentication.

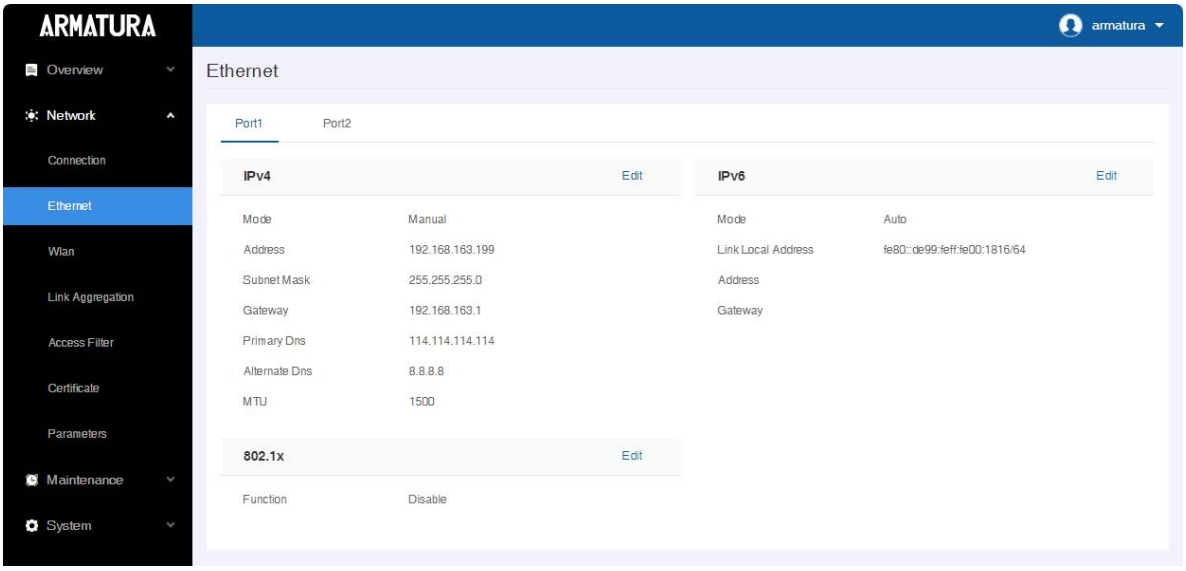
Software: To view the software certificate.

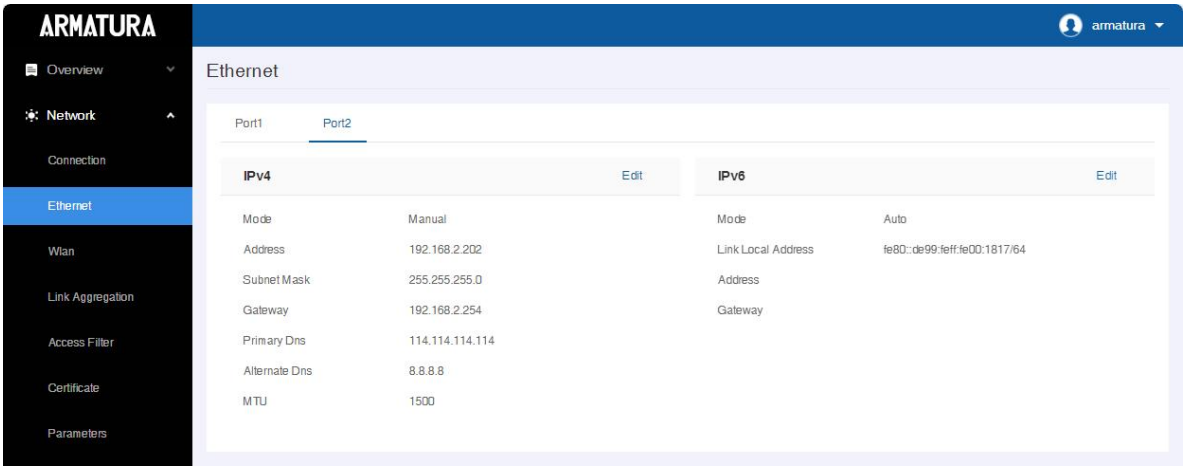
- **RS485**



7.3.2 Ethernet Settings

When the device needs to communicate with the Websever over the Ethernet, you need to configure the Ethernet settings.





Mode: Includes manual, DHCP and Off modes.

- **Manual:** The IP address can be changed manually.
- **DHCP:** DHCP (Dynamic Host Configuration Protocol) dynamically allocate the IP addresses for clients via server. If DHCP is enabled, IP addresses cannot be set manually.
- **Off:** Prohibit modification of the IP address.

Address: The controller has dual ethernet interfaces. The default IP address **192.168.1.201** for the primary NIC and **192.168.2.202** for the expansion NIC. It can be modified according to the network availability.

Subnet Mask: The default value is 255.255.255.0, it can be modified according to the available network parameters.

Gateway: The default value is 0.0.0.0, it can be modified according to the available network

parameters.

Primary Dns: The default value is 0.0.0.0, it can be modified according to the available network parameters. This DNS is preferred over the alternate DNS server.

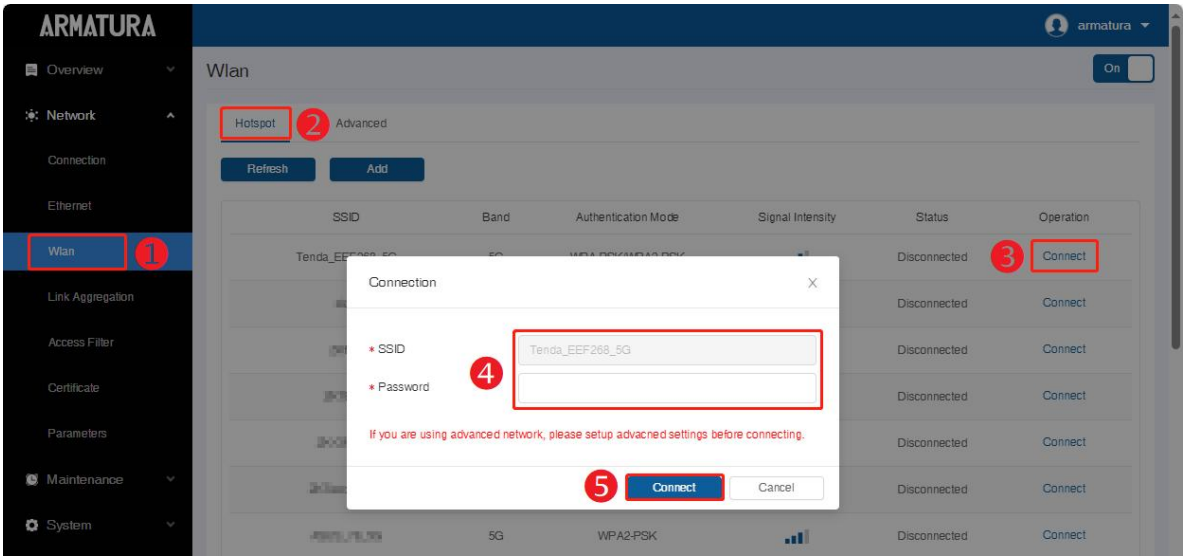
Alternate Dns: he default value is 0.0.0.0, it can be modified according to the available network parameters.

7.3.3 Wireless Network Settings

The controller supports the Wi-Fi module which is built-in within the hardware, to enable data transmission via Wi-Fi and establish a wireless network environment. By default, the Wi-Fi is turned off. The user needs to enable and set the related parameters on the webserver.

Search the Wi-Fi Network

1. Click the On button to enable Wi-Fi function.
2. Once the Wi-Fi is enabled, the device will search for the available Wi-Fi within the network range.
3. Choose the appropriate Wi-Fi name from the available list, and input the SSID and correct Password in the connection interface, and then click **Connect**.
4. After successful verification, the initial interface of the device will display the logo.

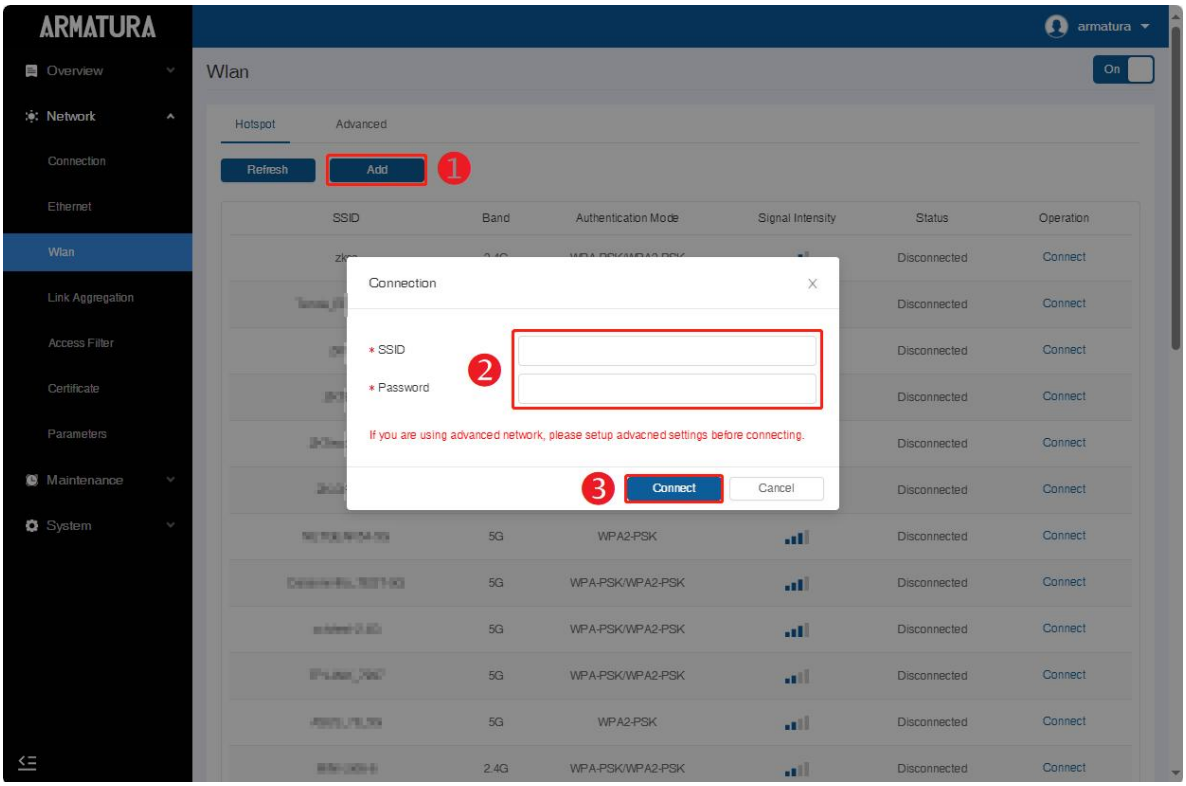


Add Wi-Fi Network Manually

The Wi-Fi can also be added manually if the required Wi-Fi does not show on the list.

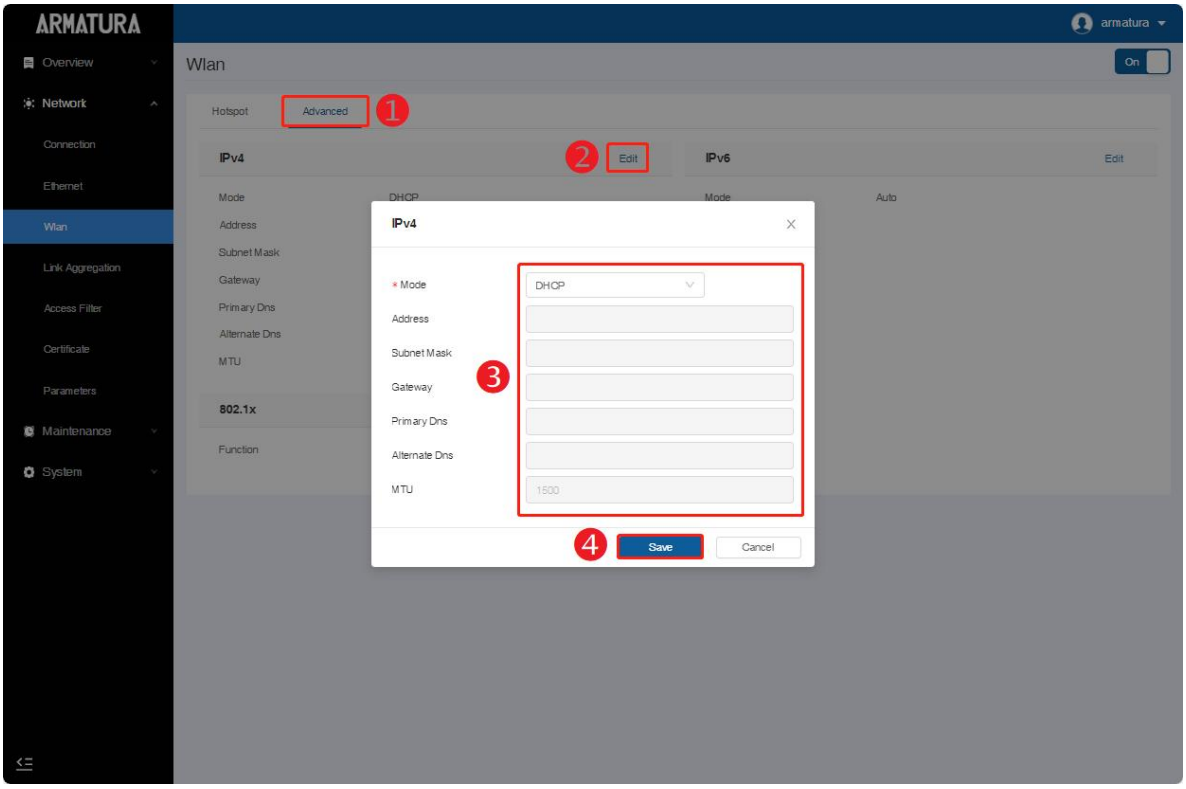
1. Click **Add** to add the Wi-Fi manually.
2. Input the SSID and Password in the connection interface, and then click **Connect** to add a new Wi-Fi manually(the added network must exist).

3. After successfully adding the Wi-Fi manually, follow the same process to search for the added Wi-Fi name.



Advanced Setting

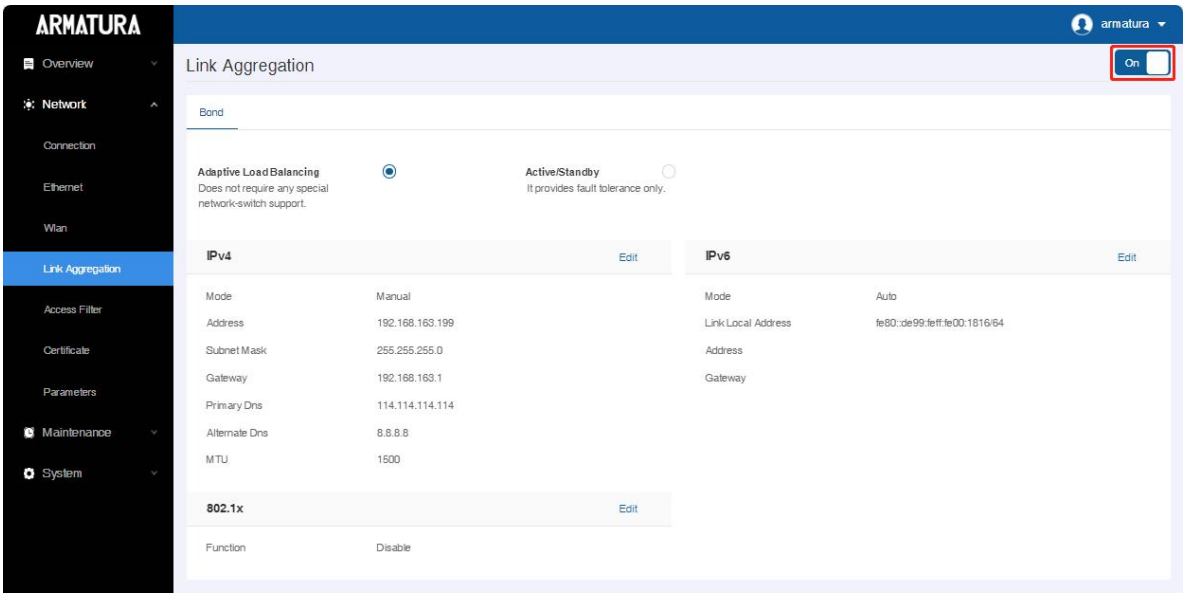
On the **Wireless Network** interface, click on **Advanced** to set the relevant parameters as required.



7.3.4 Link Aggregation Settings

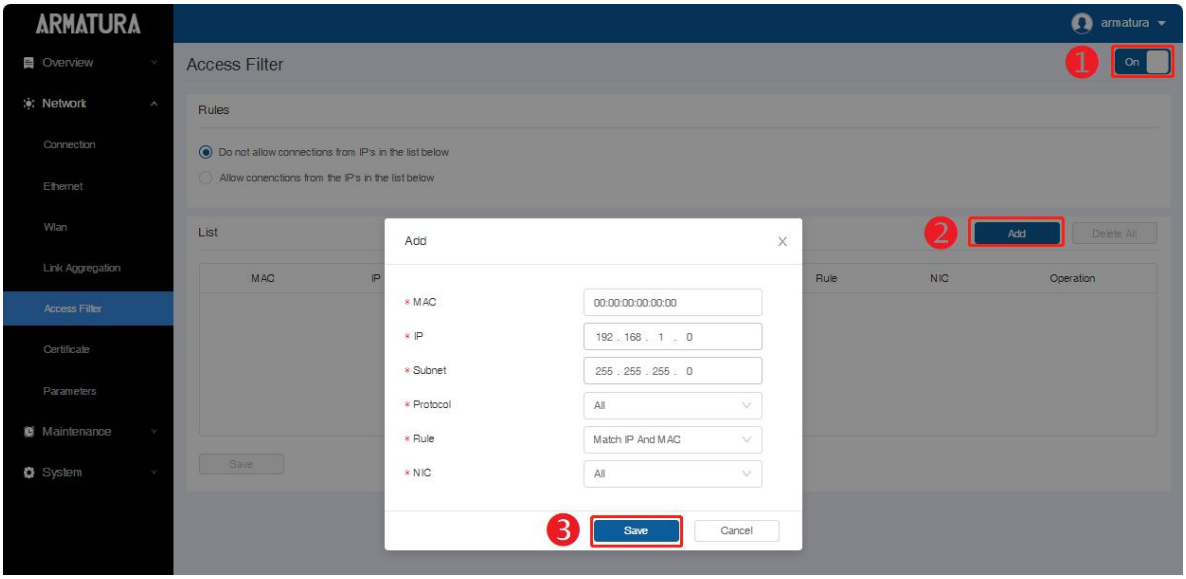
AHSC-1000 and AHDU series controllers supports Link Aggregation function, when this function is enabled, the network cable is connected to any one of the interface of ETH 1 and ETH 2, it can communicate with the server normally, and ETH 1 and ETH 2 form the function of backing up each other.

For example, when ETH 1 of the controller's TCP is connected to the router/switch's network cable, the device can automatically switch to ETH 2 of the TCP when the corresponding port of the router/switch fails resulting in network interruption.

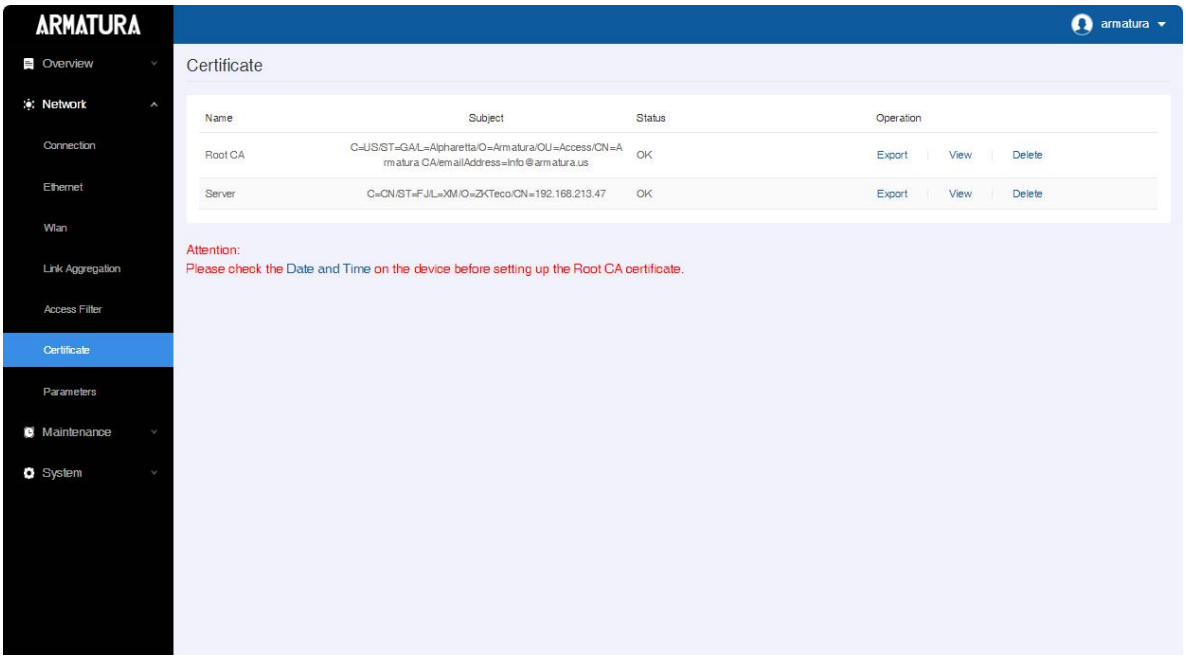


7.3.5 Access Filte Settings

Turn on the Access Filte function to filter out specific IP addresses. Click **Add** to add the addresses to be filtered.

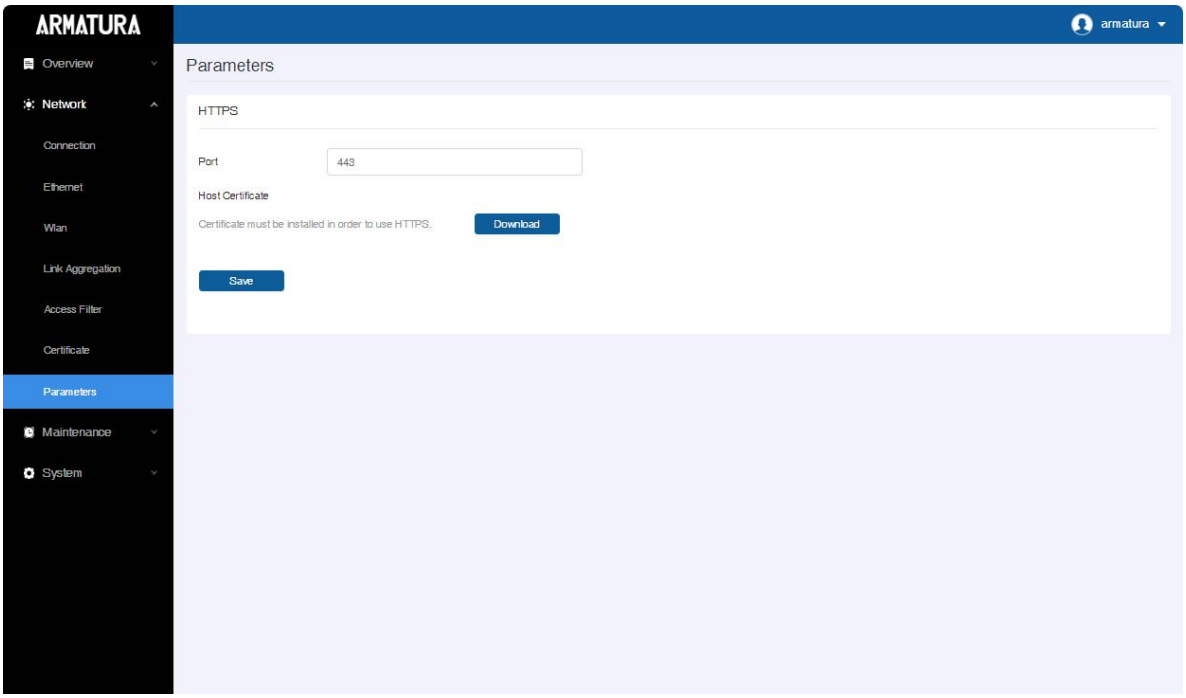


7.3.6 Certificate Settings



Attention: *Please check the Date and Time on the device before setting up the Root CA certificate.*

7.3.7 Parameters Settings



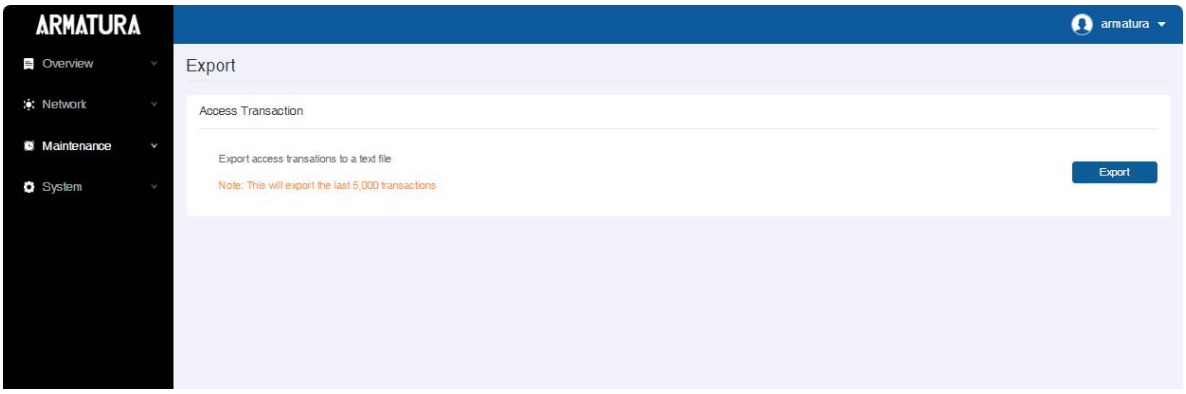
Note: *In order to use the HTTPS protocol on the webserver, the host certificate must be installed, click* ***Download*** *to download and install it.*

7.4 Maintenance

7.4.1 Export

Export access transactions to a text file.

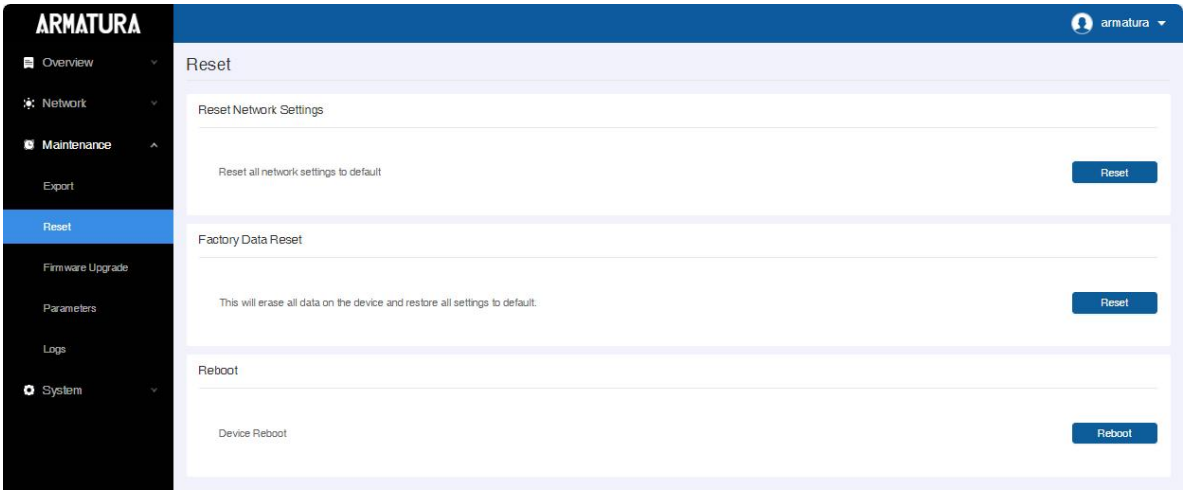
Click **Export** to export the access transaction.



Note: *This will export the last 5,000 transactions.*

7.4.2 Reset

Here you can reset network settings, restore factory data and reboot your device.



Rest Network Settings

Reset all network settings to default.

Factory Data Reset

The Factory Data Reset function restores the device settings such as communication settings and system settings, to the default factory settings.

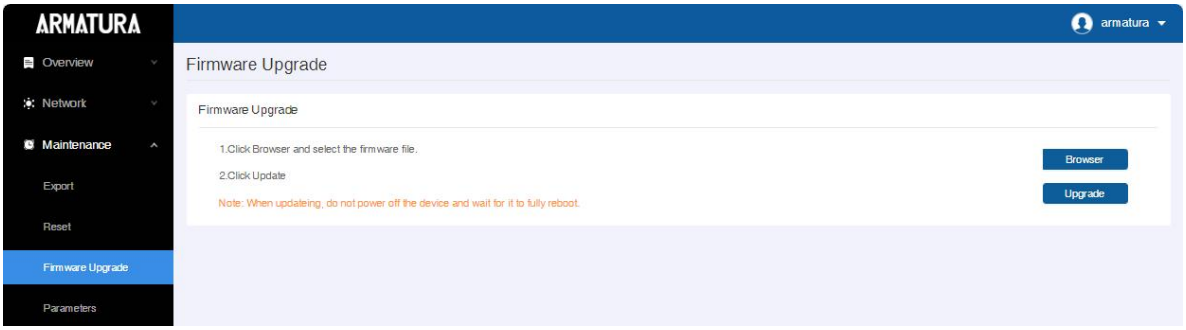
Reboot

Reboot the device.

7.4.3 Firmware Upgrade

With this option, the device firmware can be upgraded by using the upgrade file.

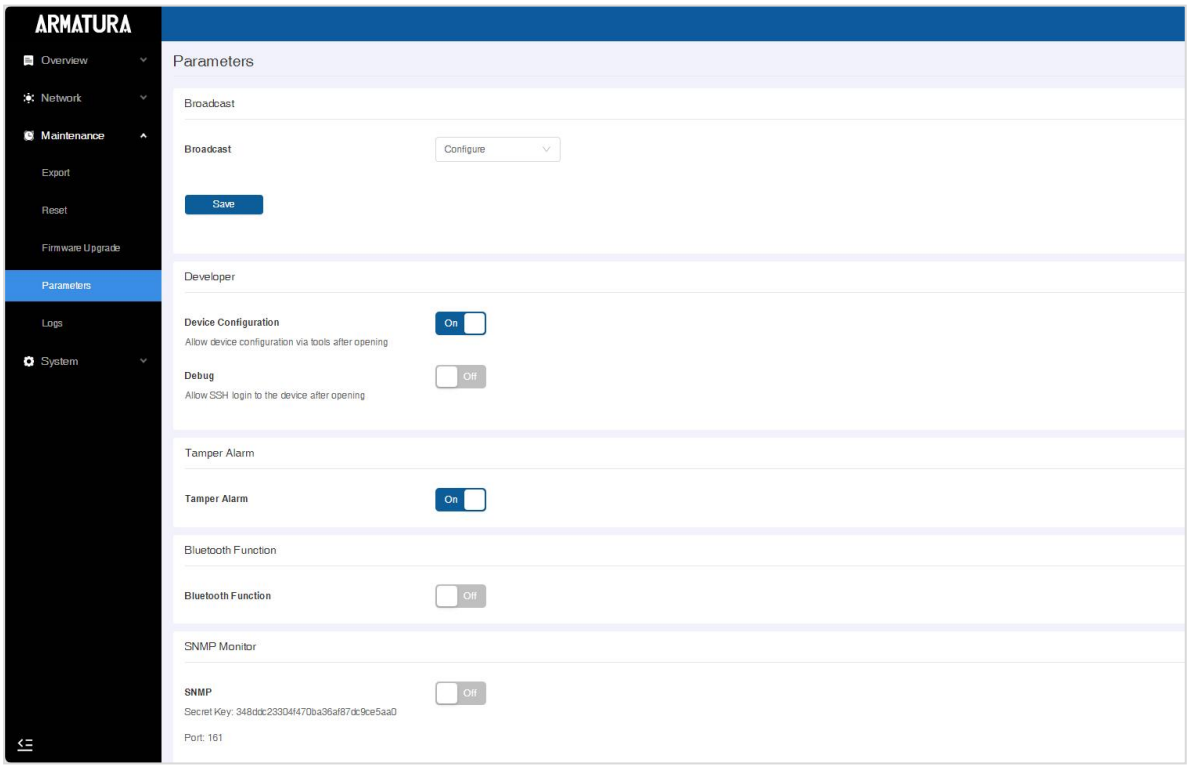
Click **Browser** to select the firmware file. Then click **Update** to update the firmware.



Note: *When updateing, do not power off the device and wait for it to fully reboot.*

7.4.4 Parameters

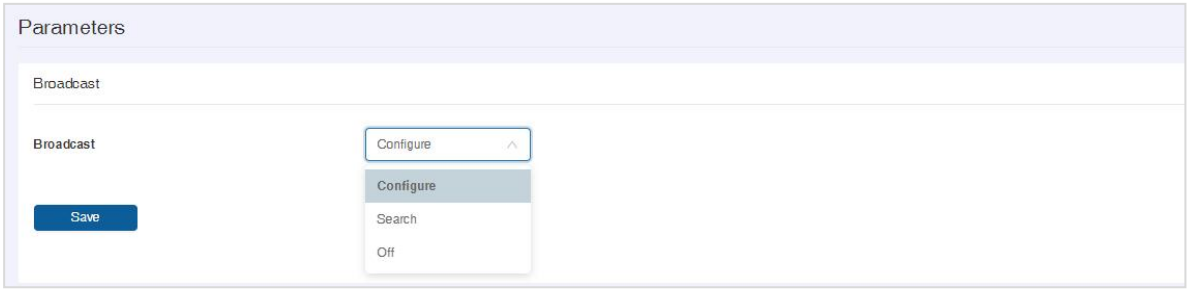
Parameters can be set for broadcast function, developer options, tamper alarm, Bluetooth function and SNMP monitoring.



Broadcast

UDP broadcast function, factory device is configured by default and can be selected manually (Configure, Search and Off).

After the configuration function is turned on, users can use the deviceSettingTool.exe tool to search and modify the controller IP address.



Configure: Allow device IP search and be able to change IP address.

Search: Only device IP search is allowed.

Off: Prohibit searching.

Note: *The **deviceSettingTool.exe** can be downloaded via the path **Access** > **Device** > **Device** >*

New > ***Download Search Tools to Local Disk*** *on the ARMATURA One software.*

Developer

Device Configuration: factory device default on (turned on to allow demo tool to set device parameters).

Debugging Function: factory device default off (open to allow access to the device background via ssh).

Tamper Alarm

Tamper Alarm: factory device default on (when turned off, the device does not detect the tamper function).

Bluetooth Function(Only versions produced after June 2024 are supported. Please contact the technician for details.)

Bluetooth: Support app search view, set bluetooth function via web (On or Off).

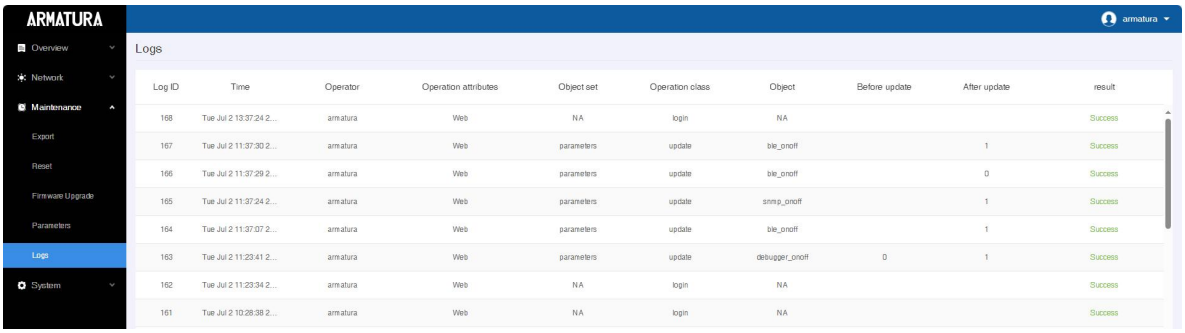
SNMP Monitor

SNMP Monitor: factory device is turned off by default and can be turned on manually.

Turn on SNMP button, web display corresponding port number 161 and default key 348ddc23304f470ba36af87dc9ce5aa0.

7.4.5 Logs

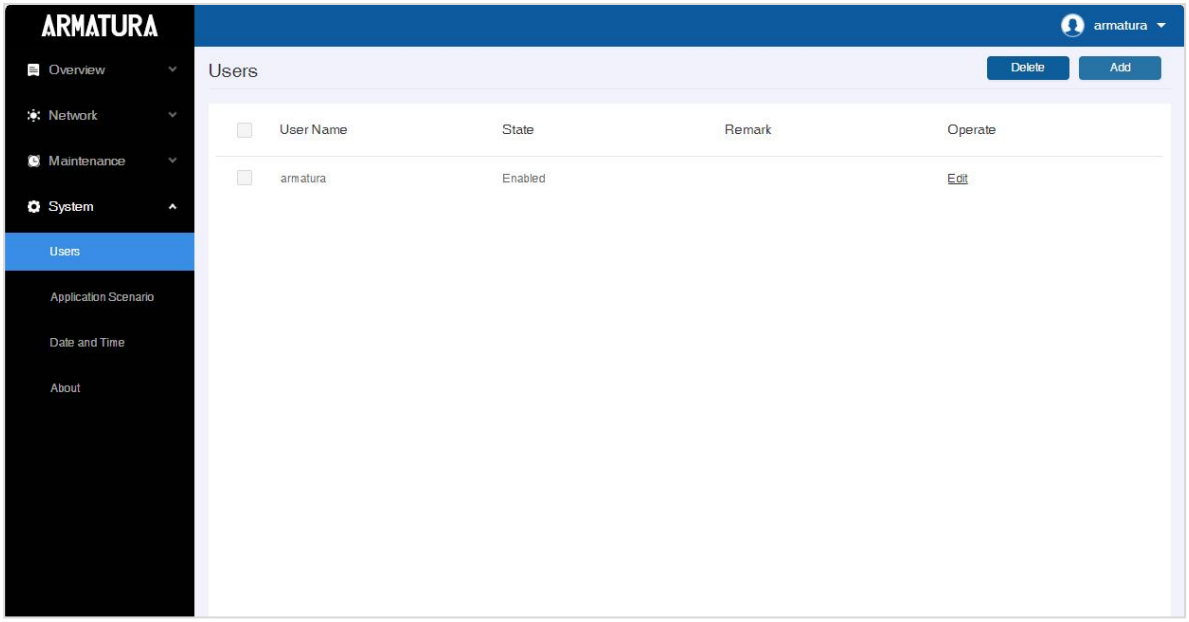
You can quickly view all operation logs in the device log list, including operating users, operation attributes, operation class, result and so on.



7.5 System Settings

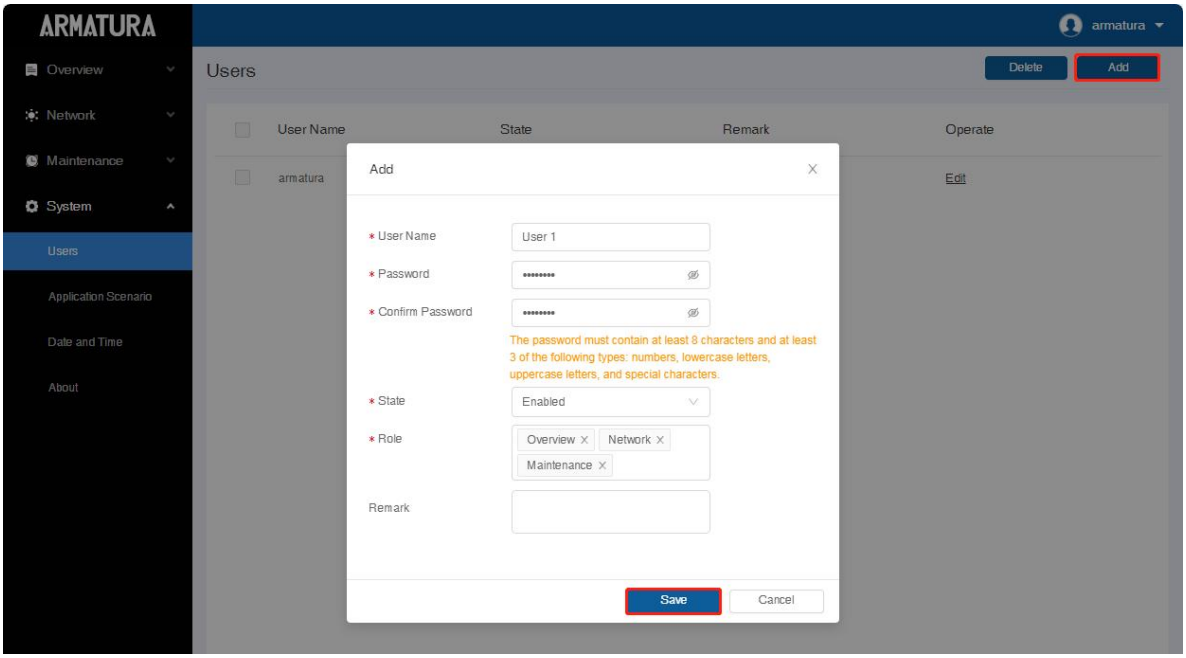
7.5.1 Users

Add new users and implement levels for the user in the system.



Add User

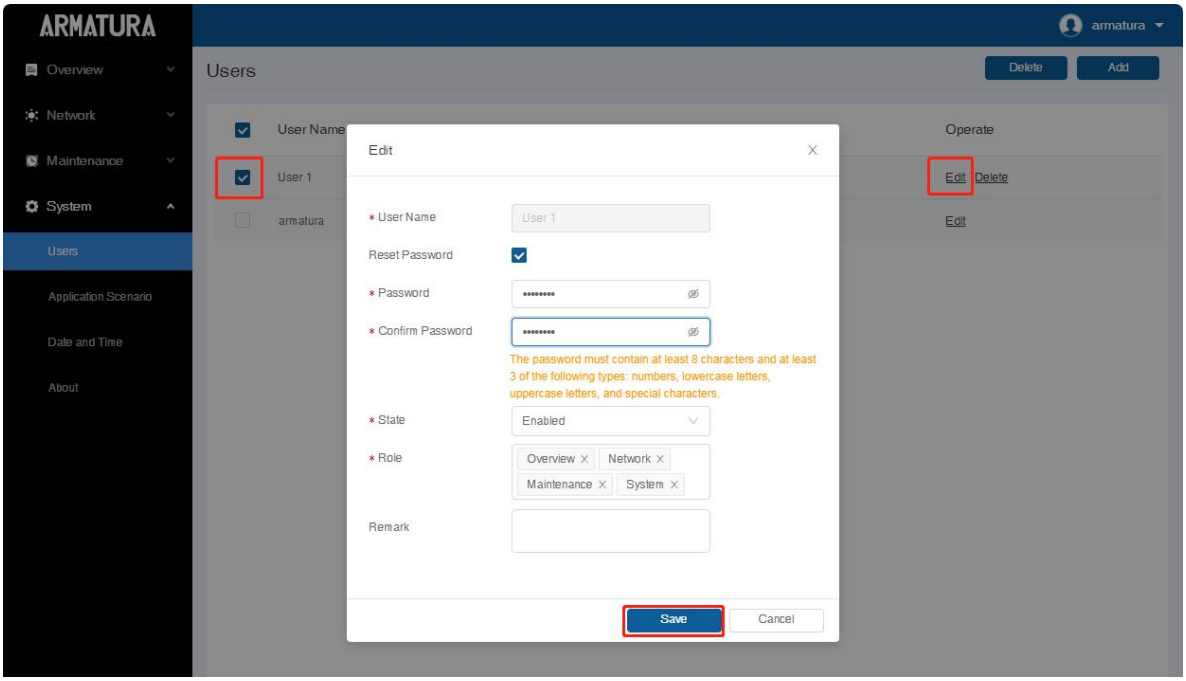
Click **System** > **Users** > **Add** to add a new user.



Enter the user name, password, set state and roles, click **Save** to save and exit when finished.

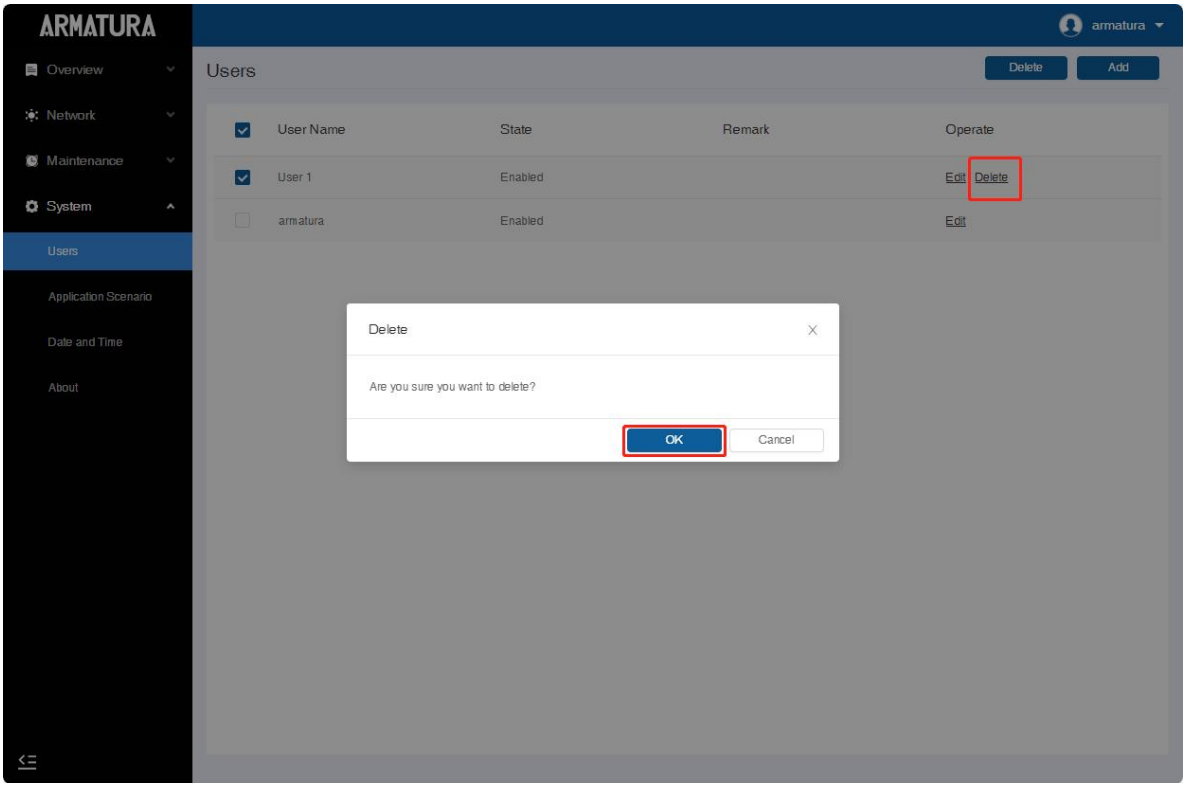
Edit User

Select the user in the user list and click **Edit** to modify.



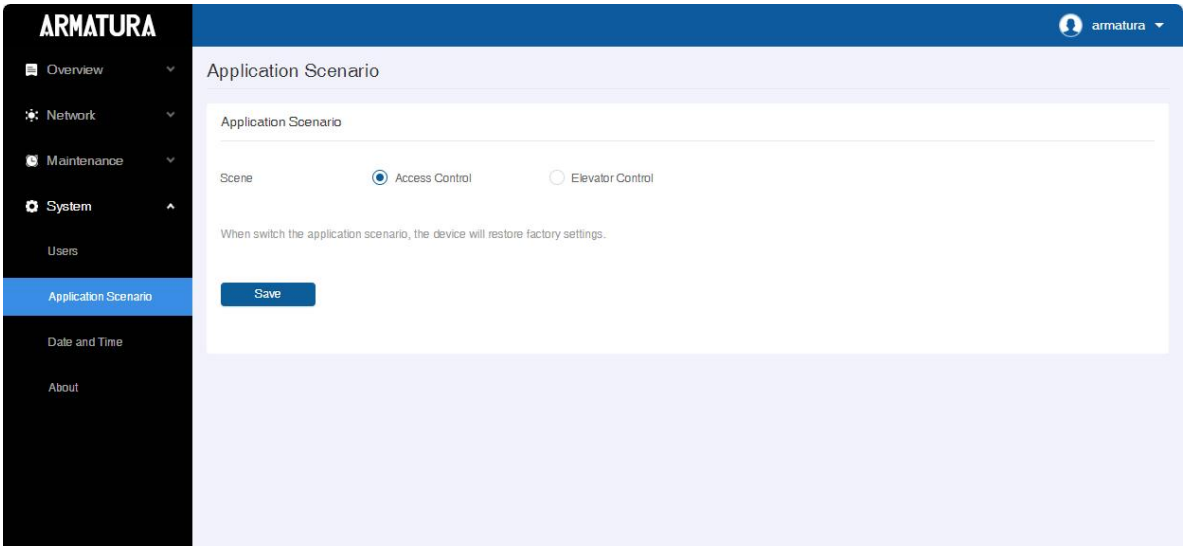
Delete User

Select the user you want to delete in the user list and click **Delete**. Then click **OK** to confirm.



7.5.2 Application Scenario

You can *switch the* Access Control or the Elevator Control application scenarios here.

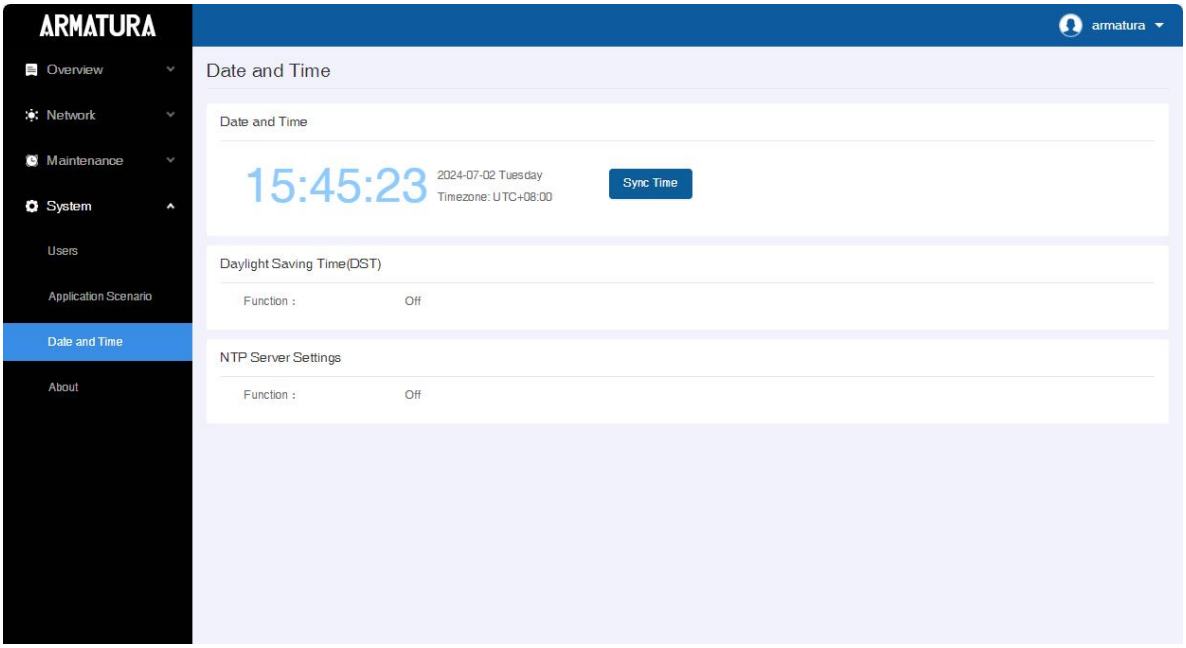


Notes:

- *If you are unable to find the [**Application Scenario**] option under [**System**], you will need to contact technical support or headquarters for assistance. They can help upgrade the controller's firmware and import the activation license.*
- *After switching to elevator control mode, the controller will revert to factory settings and automatically restart.*

7.5.3 Date and Time

This function automatically synchronizes the time.

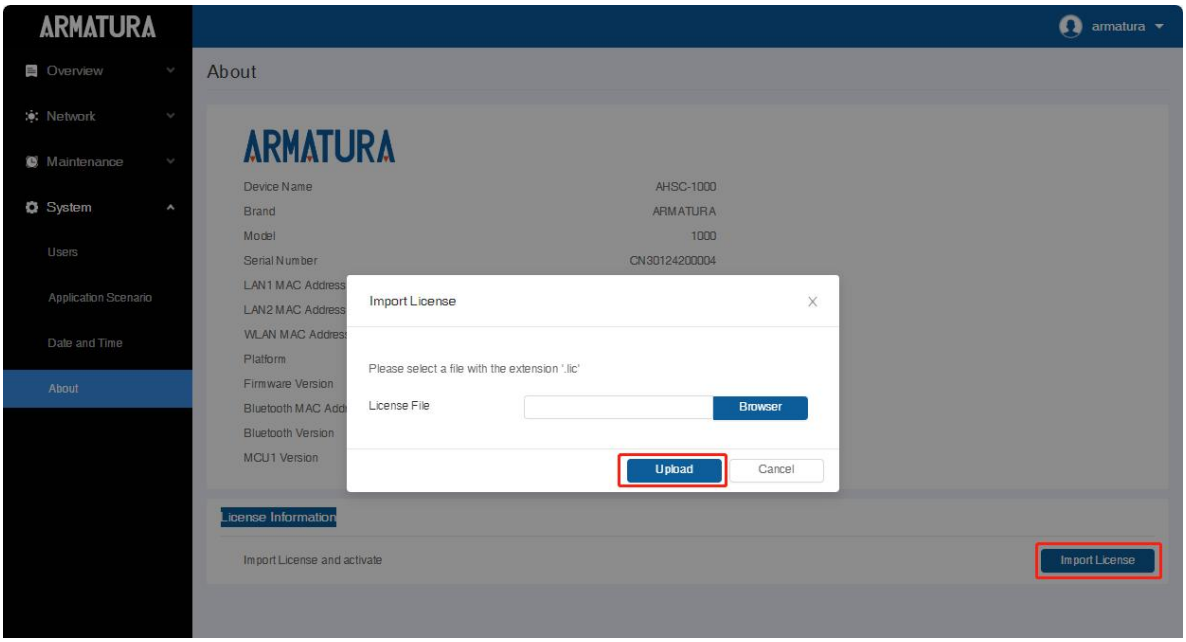


7.5.4 About

This function to check all the software version and license information.

License Information

Click **Import License** to import the license.



8. System Management Mode Connection

The system supports standard security levels for adding Horizon Series controllers. It also provides support for both Primary-Secondary Modes and Primary management modes.

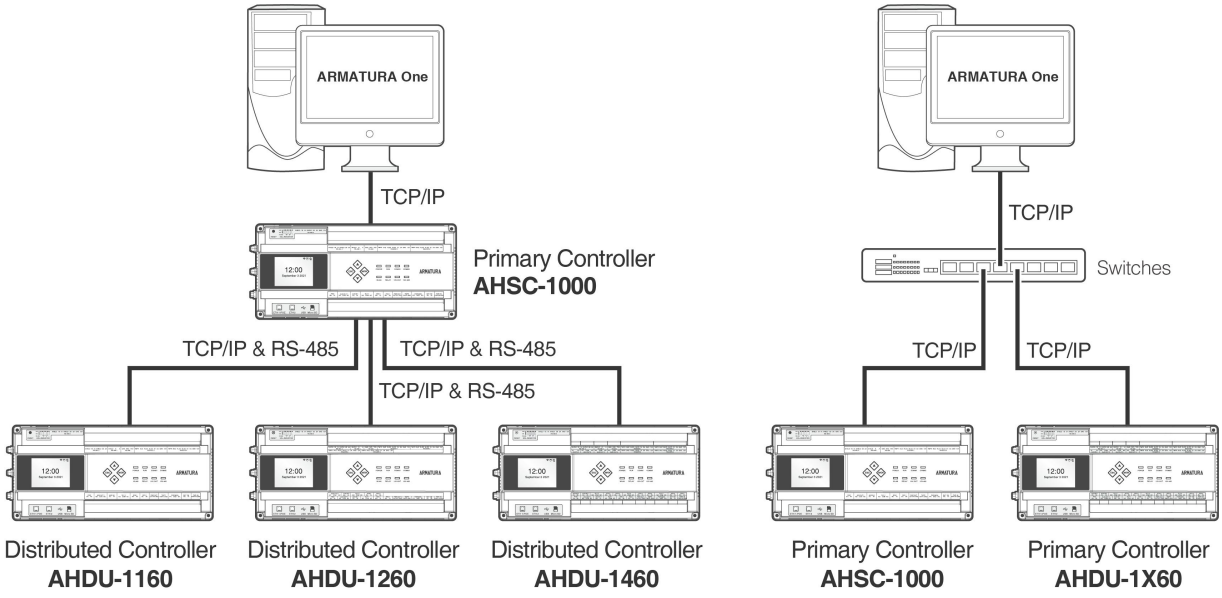


Figure 7-1 Schematic Diagram of System Management Mode

Remarks:

- ***Horizon Series Controller:*** *Horizon Series Controllers including AHSC-1000/AHDU-1X60*
- ***Normal Security Level:*** *MQTTs, One-Way SSL authentication*

8.1 Master-Slave Mode

An AHDU-1X60 can be connected to AHSC-1000 via TCP/IP or RS-485.

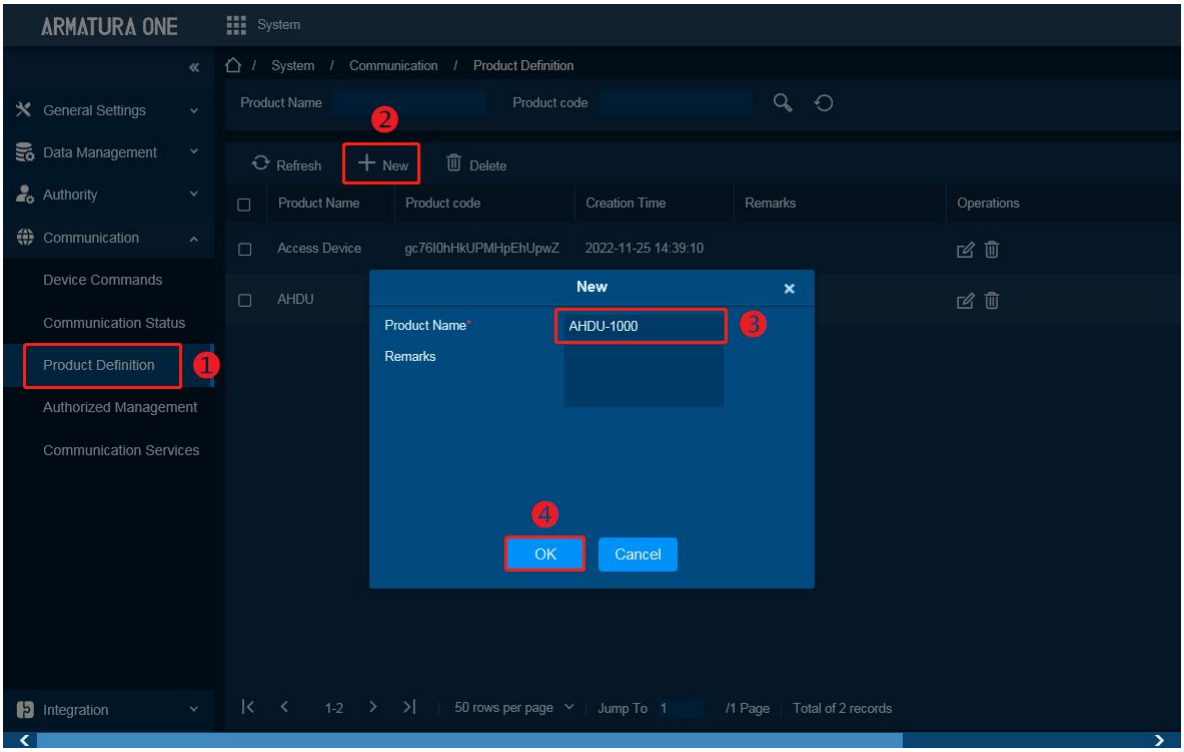
8.1.1 Connect AHDU-1X60 to AHSC-1000 via TCP/IP

8.1.1.1 Adding the Primary Controller

1. Add a product

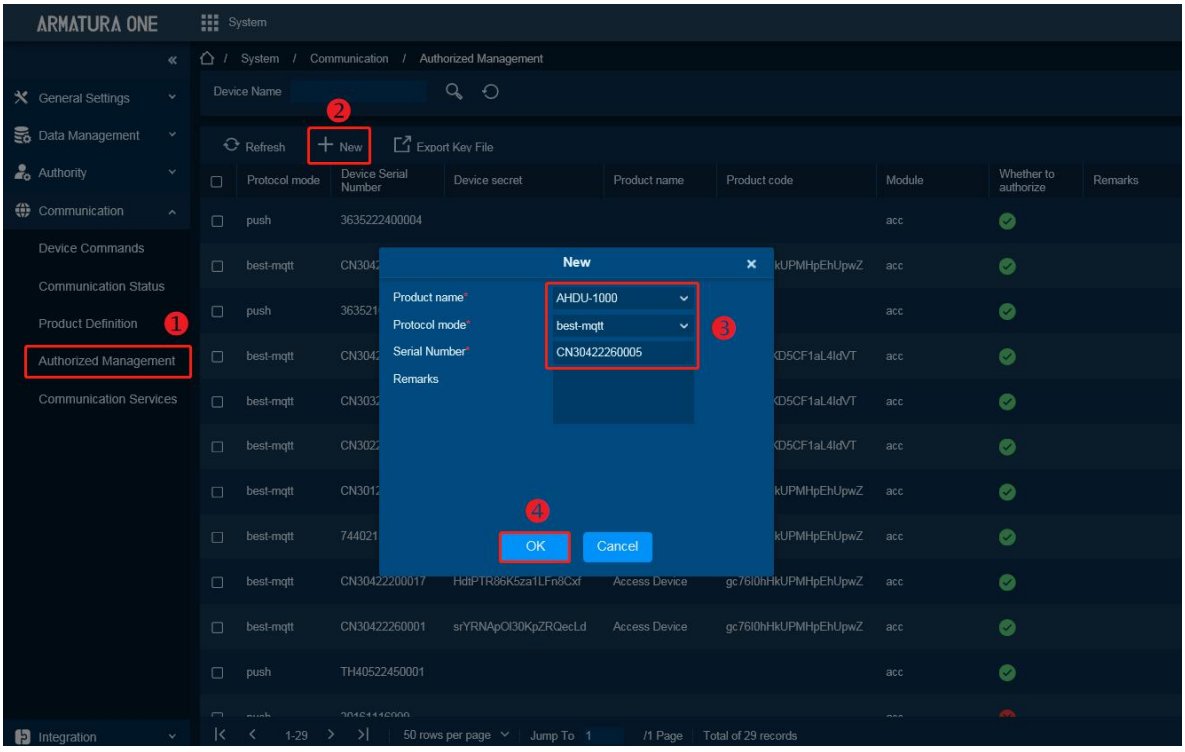
Click **System > Communication > Product Definition > New** to add a product on the software.

Enter the product name and click **OK** to save and exit.



2. Add a device

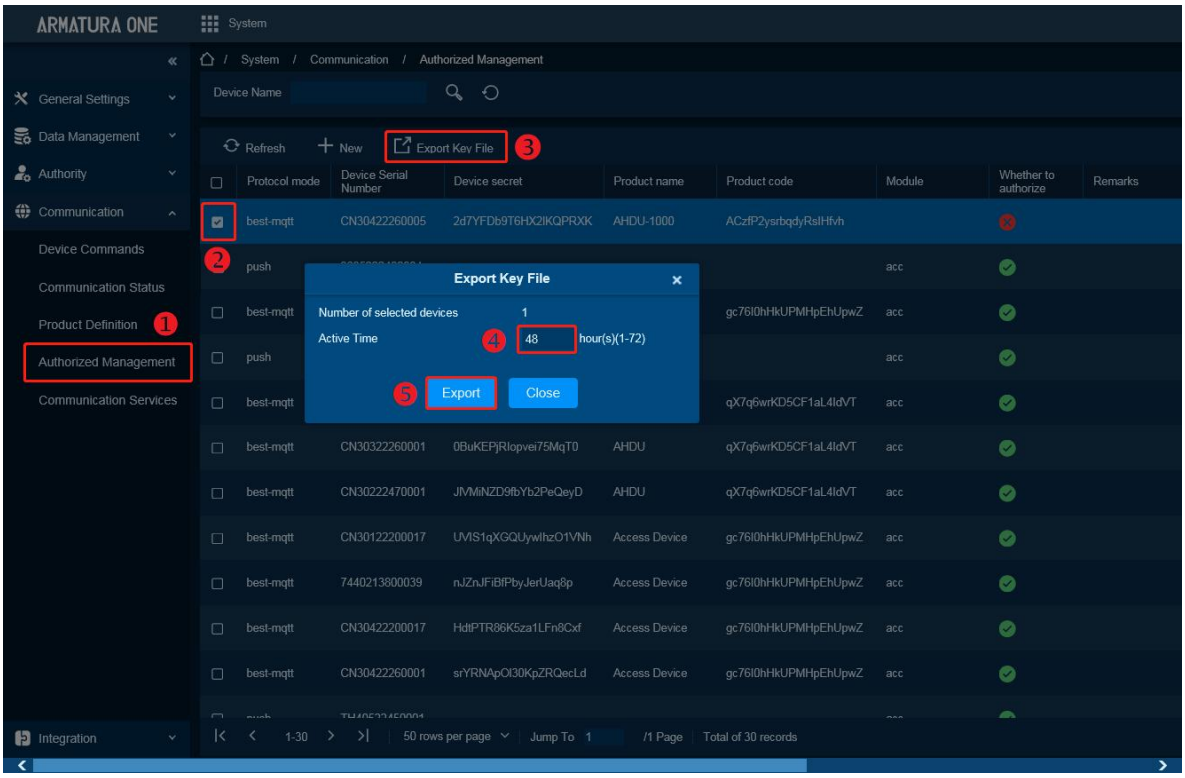
Click **System > Communication > Authorized Management > New** to add a device on the software.



Select the product you just created and input the serial number. Click '**OK**' to save and exit.

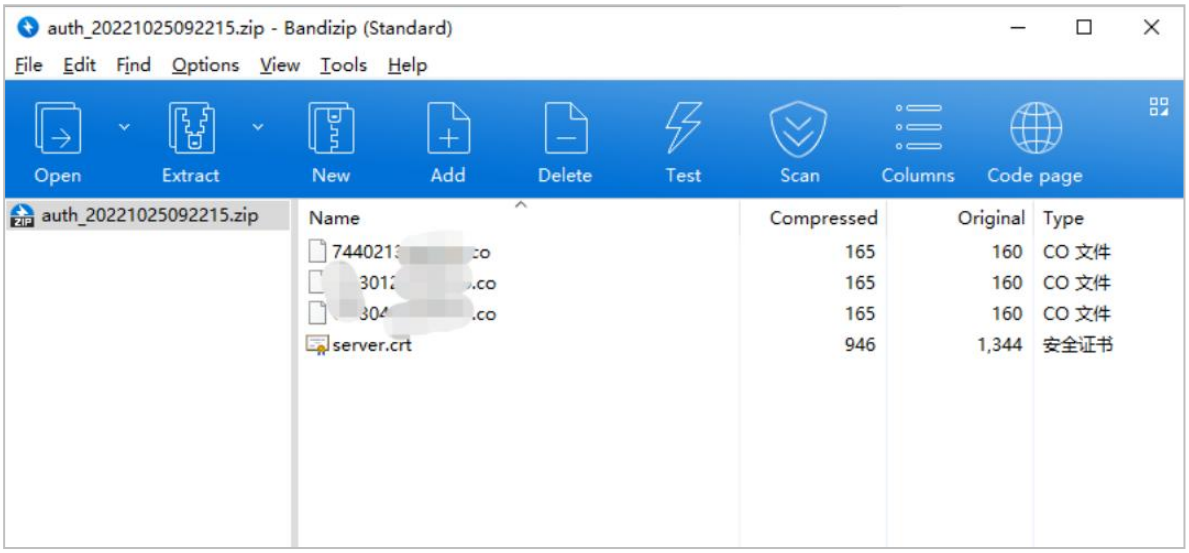
3. Export Key File

Navigate to **System > Communication > Authorized Management** to check the recently added devices, then click on "**Export Key File**".



- **Active time**：Key file validity, value can be 1-72 Hours.

After clicking **Export**, the browser will download the .zip file.



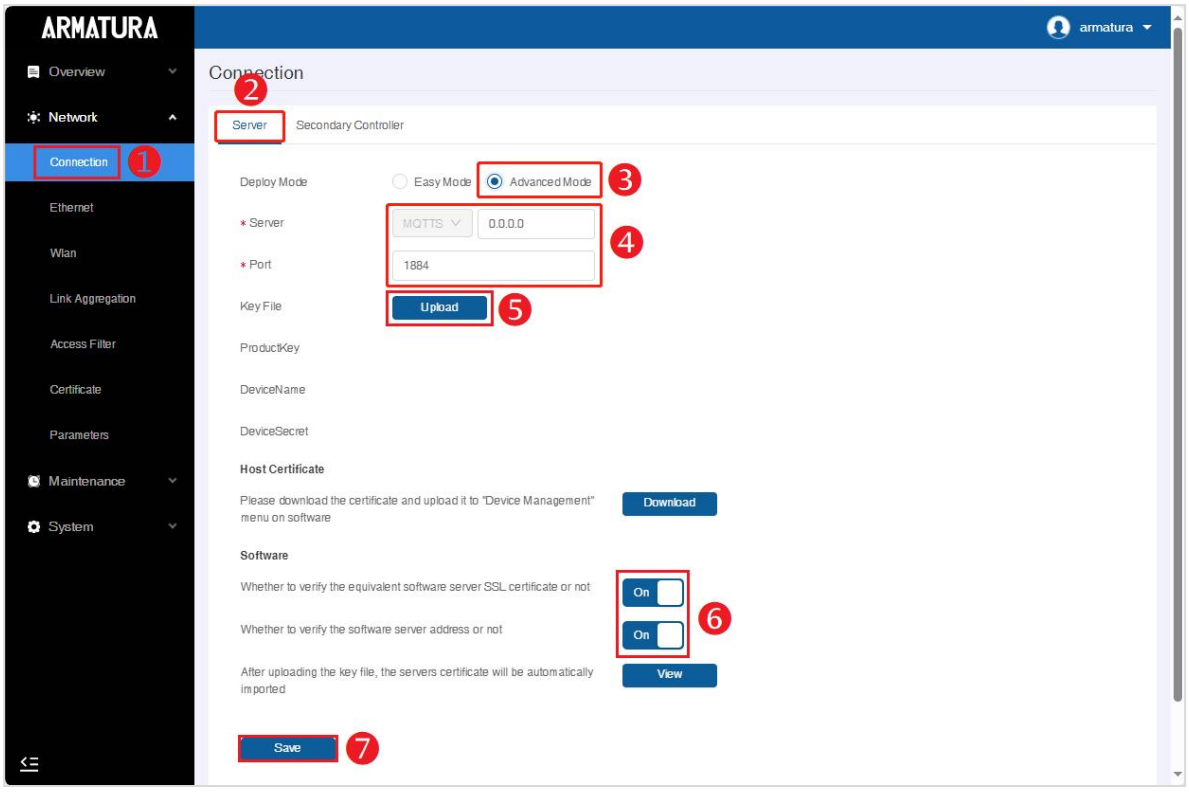
Note: *This function supports selecting multiple devices and clicking on the icon to generate all controller.co files and server certificates in a .zip package. Simply upload this .zip package to the controller webserver.*

4. Import Key file to the controller

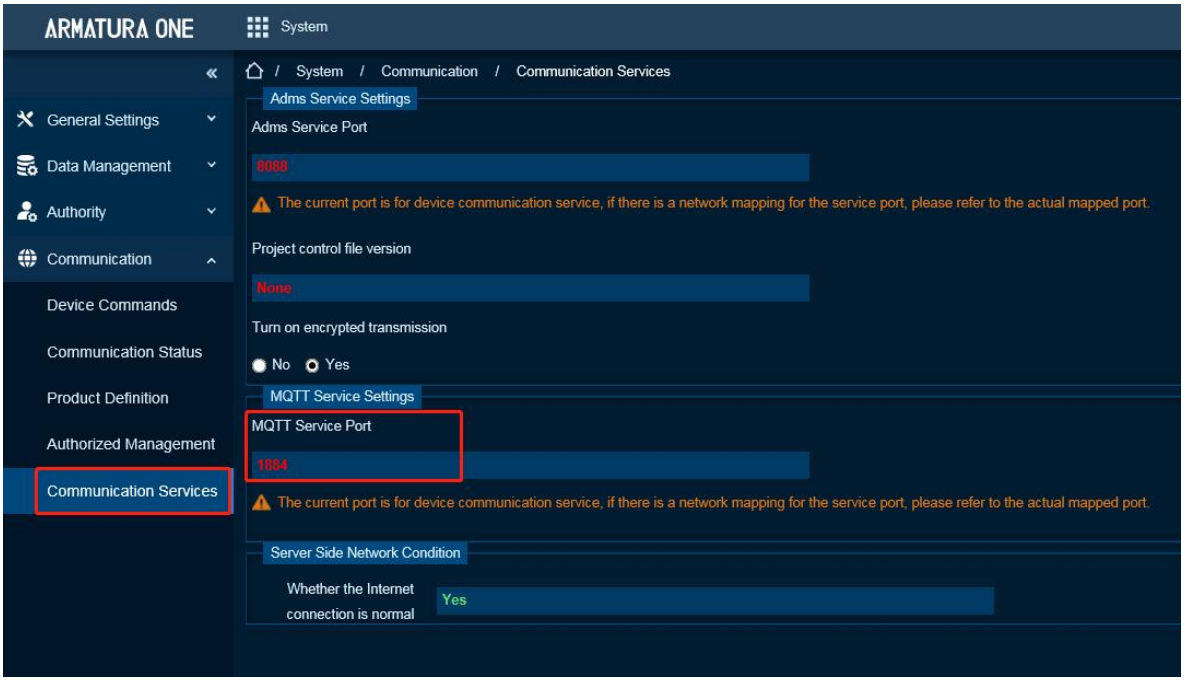
1) Open your web browser and enter the controller's IP address in the URL (https://[controller's IP address]) to access the login interface.

For the first-time login, use '**armatura**' as the default username and password. Upon login, you will be prompted to change the password for the admin account.

2) Click **Network > Connection > Server > Advanced Mode** on the Webserver interface.

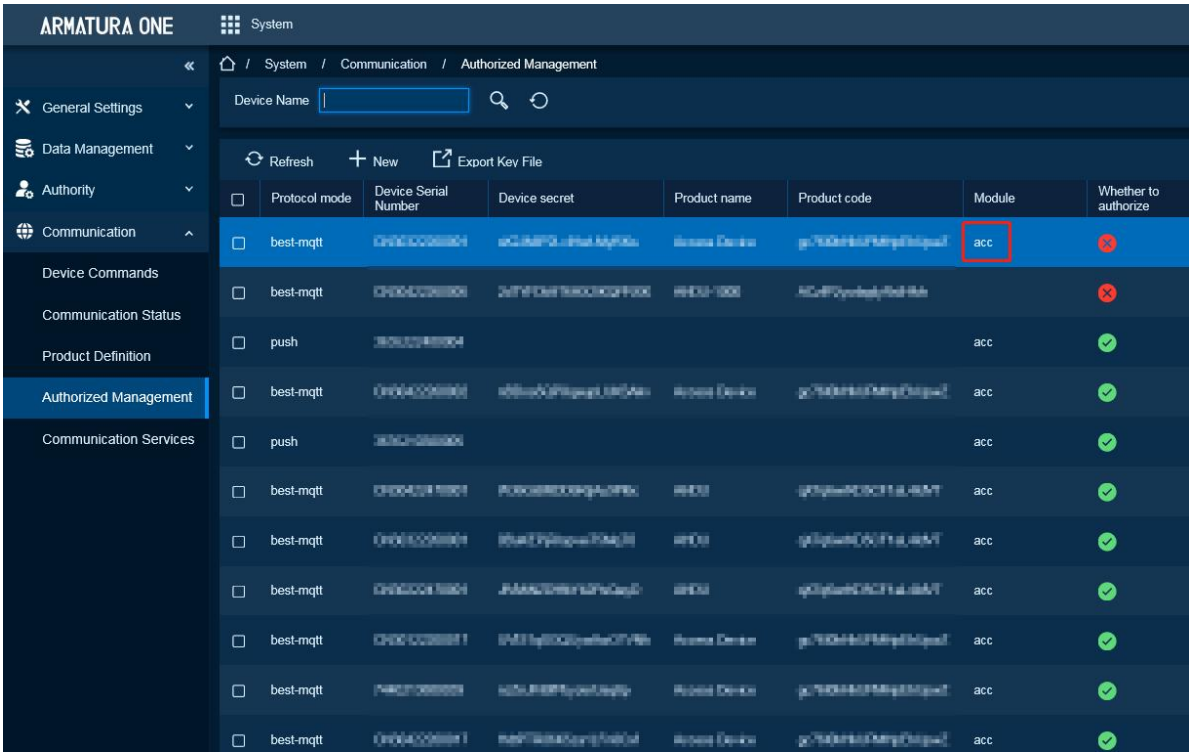


- **Server:** The default protocol is MQTTs, and the address should be set to the server address.
- **Port:** The default port is 1884. You can verify this port by navigating to **System > Communication > Communication Services > MQTT Service Port**.



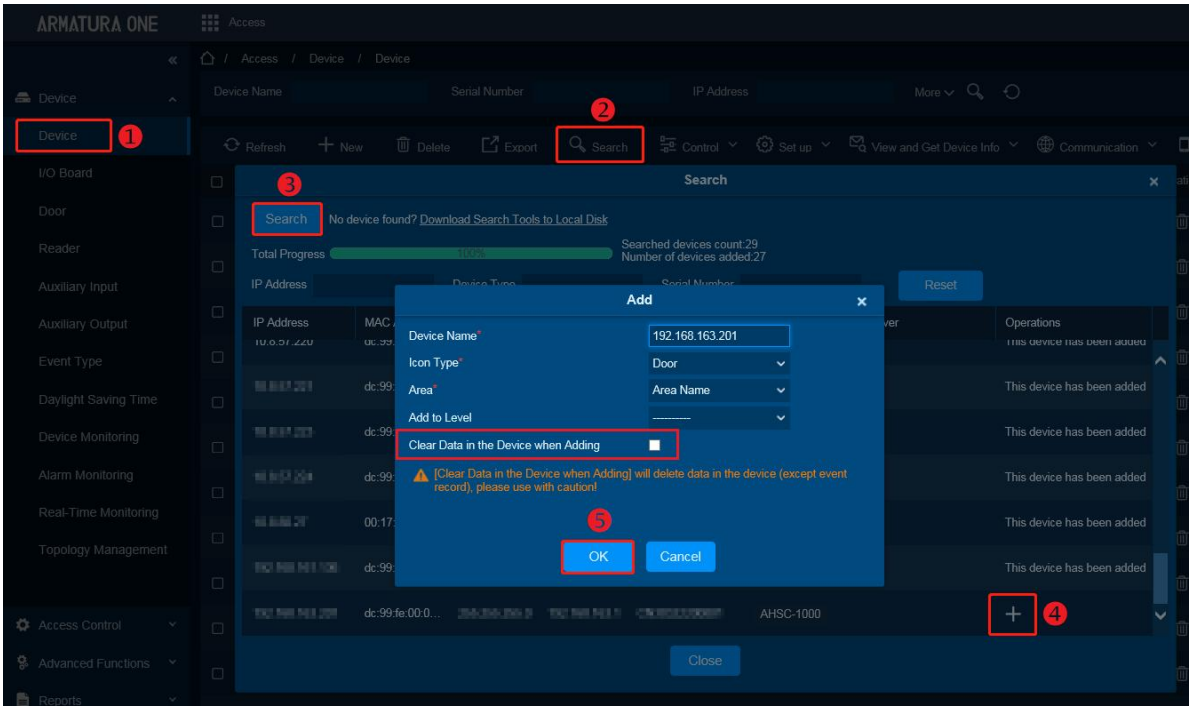
- **Key File:** This file is exported from **System > Communication > Authorized Management**.

  After successfully connecting the controller to MQTT, the Column Module will display 'acc'. However, since the device is not yet authorized to access the Access Module, it will show .



5. Adding The Controller To The Software

1) Click **Access > Device > Device > Search**, to open the Search interface.
2) After clicking **Search**, the list and the total number of Access Control Devices will be displayed.
3) Click the "**Add**" button located next to the Device to add it.
4) Click **OK** to save and exit.



Note: *Suggest select* ***[Clear Data in Device when Adding]*** *to clear device data.*

8.1.1.2 Set the Secondary Controller Communication Port

1. Click **Network > Connection > Secondary Controller** on the Webserver screen of the Primary Controller.

2. Select **TCP/IP** button in Comm.

3. Click **Download** to download the Host Certificate of the primary controller.

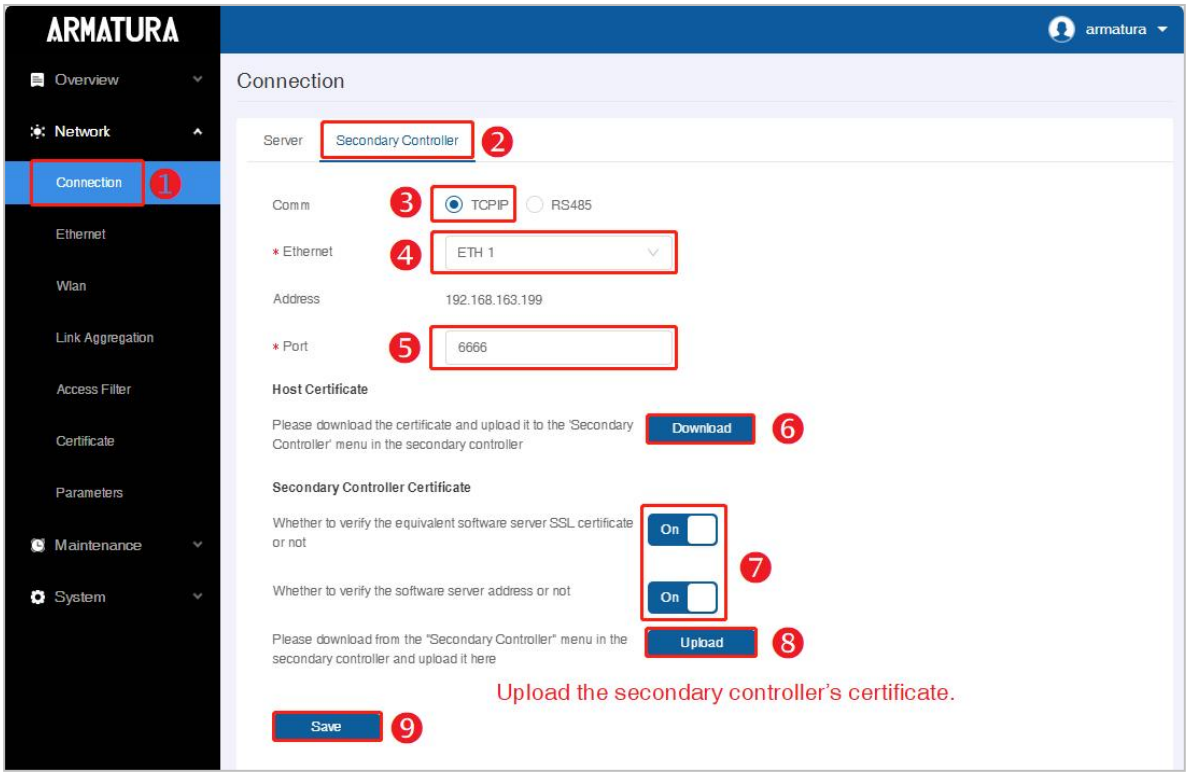
4. Click **Upload** to upload the secondary controller's certificate.

5. Click **Save** to complete the configuration..

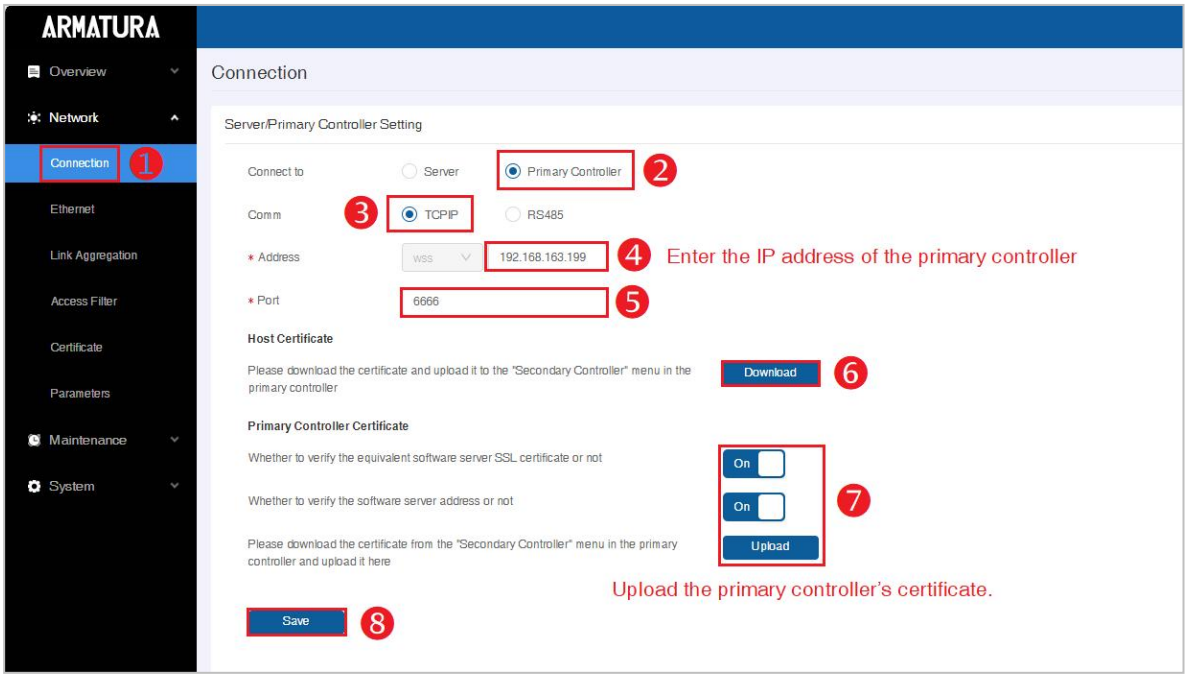
6. Then click **Network > Connection > Primary Controller** on the Webserver screen of the secondary controller.

7. Click **Upload** to upload the primary controller's certificate.

8. Click **Save** to exit.



- **Ethernet:** Select 'Eth 0' or 'Eth 1'.
- **Address:** The IP address will be displayed for confirmation after selection.
- **Port:** This port serves as a connection point for the secondary controller to utilize the WSS protocol.
- **Secondary Controller:** Download the [Host Certificate] and upload it on the Primary Controller page under [Secondary Controller Certificate].



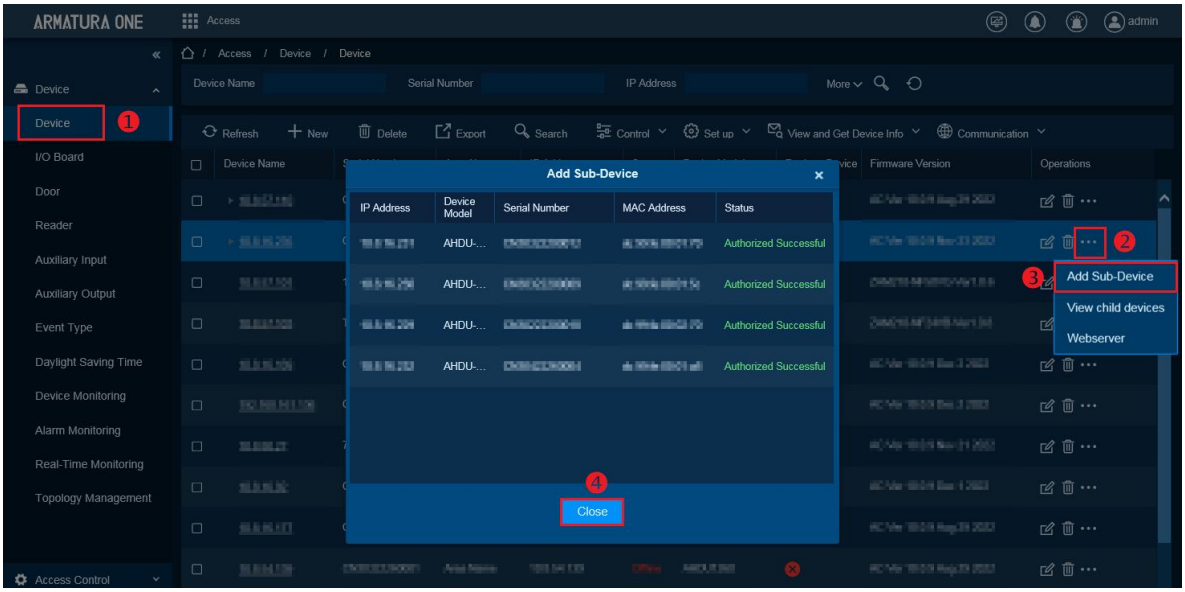
- **Address:** Enter the IP address of the primary controller.
- **Port:** This port serves as a connection point for the secondary controller to utilize the WSS protocol.
- **Primary Controller:** Download the [Host Certificate] and upload it on the Secondary Controller page as the [Primary Controller Certificate].

9. After uploading the certificates to each other, proceed to add the secondary controller.

Note: *For TCP master-slave connections, it is currently one-way authentication, i.e., only the slave needs to import the host certificate.*

8.1.1.3 Add the Secondary Controller

1. Click **Access > Device > Device** to enter the device list interface.
2. Select a primary controller and click **> Add Sub-Device** to add the secondary controller**.**
3. Click **Close** to save and exit.



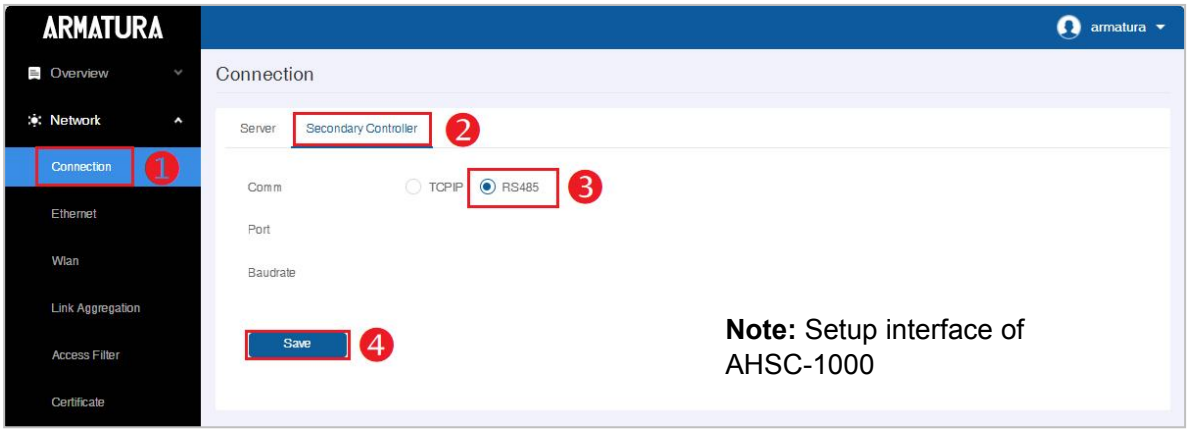
8.1.2 Connect AHDU-1X60 to AHSC-1000 via RS-485

8.1.2.1 Step 1 Add Primary Controller

The method of adding a primary controller is the same as that of **8.1.1 Connecting AHDU-1X60 to AHSC-1000 via TCP/IP**, please see 8.1.1.1 Adding the Primary Controller for details on how to add it.

8.1.2.2 Step 2 Set Secondary Controller Communication Port

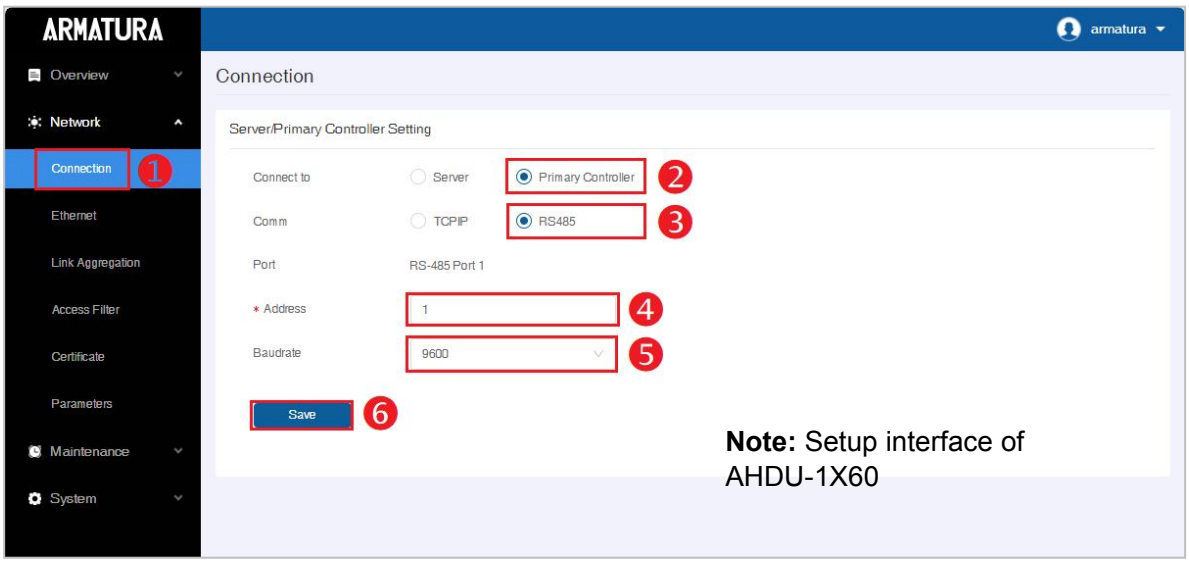
1. Click **Network > Connection > Secondary Controller** on the Webserver screen of the primary controller.
2. Select the RS-485 button in the Communication settings.
3. Click '**Save**' to save your options and exit.



Port: This is the RS-485 port used for connecting the secondary controller. The specific port to be used depends on the setting in Armatura RS-485 Port Settings.

Baudrate: This is parameter for RS-485 communication. This depends on which port is set Armatura RS-485 in RS-485 Port Settings.

4. Click **Network > Connection > Primary Controller** on the Webserver screen of the secondary controller. Then select the RS-485 button in Comm.

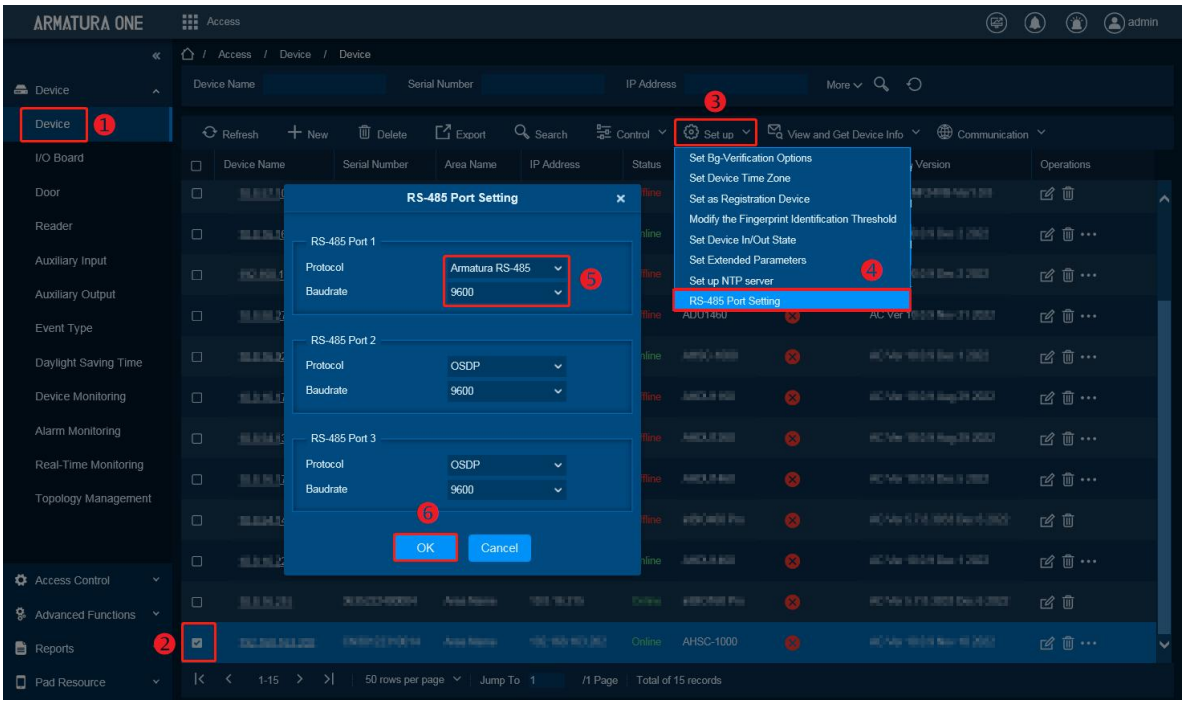


Port: The default system wiring for the primary and secondary controller is RS-485 Port 1.

Address: Enter the device address of the secondary controller.

Baudrate: Must be the same baudrate as the primary controller.

5. In the software, navigate to **Access > Device > Device**, select the desired device, and then click on "**Set up**" in the operation bar. Next, click on "**RS-485 Port Setting**".

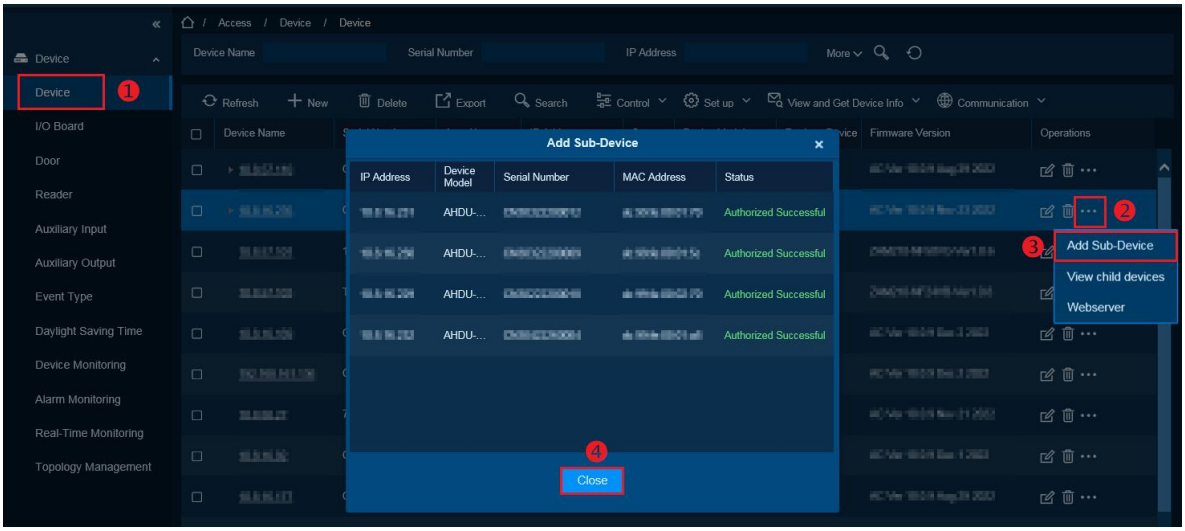


Device has three physical interface, RS-485 Port 1/Port 2/Port 3.

Armatura RS-485 is the Protocol used for primary-secondary connection.

8.1.2.3 Step 3 Add Secondary Controller

1. Click **Access > Device > Device** to enter the device list interface.
2. Select a primary controller and click ••• **> Add Sub-Device** to add the secondary controller**.**
3. Click **Close** to save and exit.



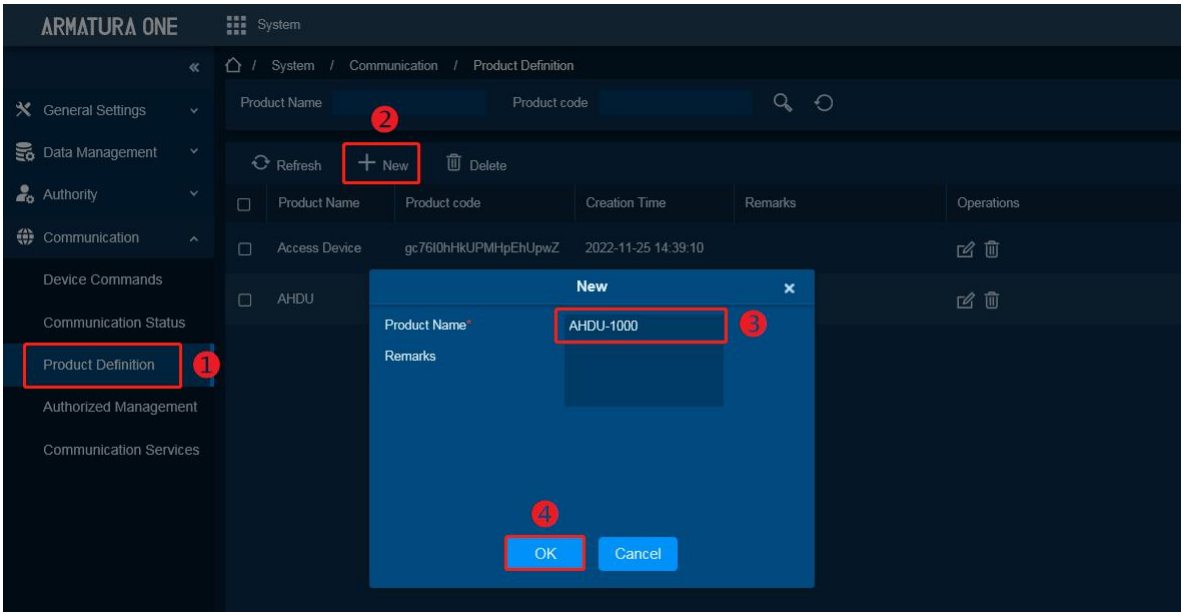
8.2 Master Mode

8.2.1 Adding a Primary Controller

1. Add a product

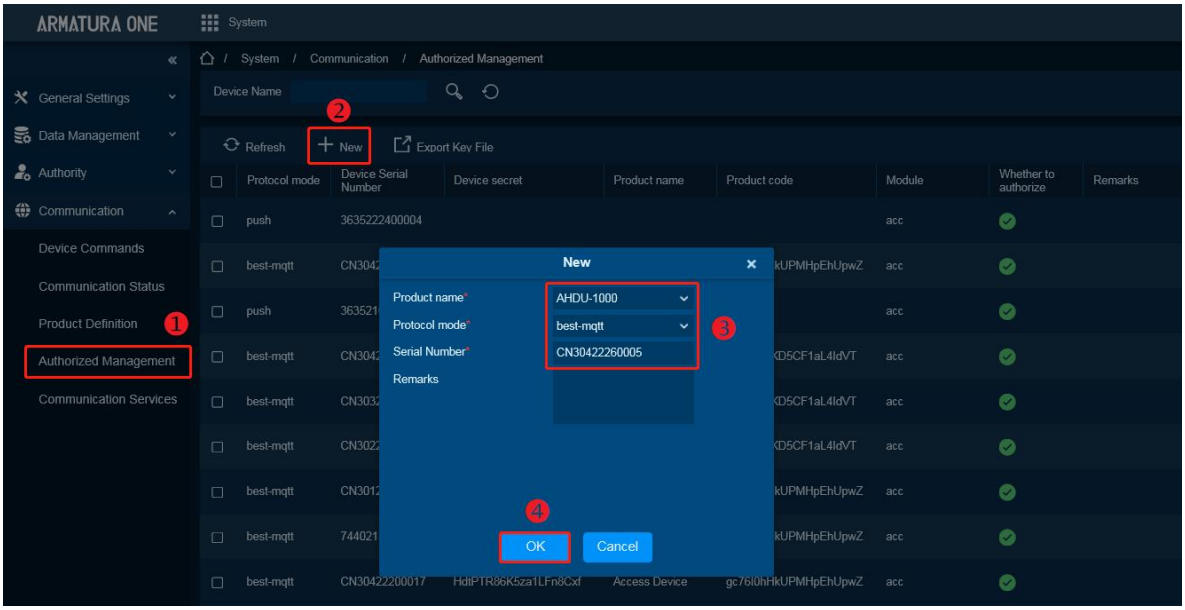
Click **System > Communication > Product Definition > New** to add a product on the software.

Enter the product name and click **OK** to save and exit.



2. Add a device

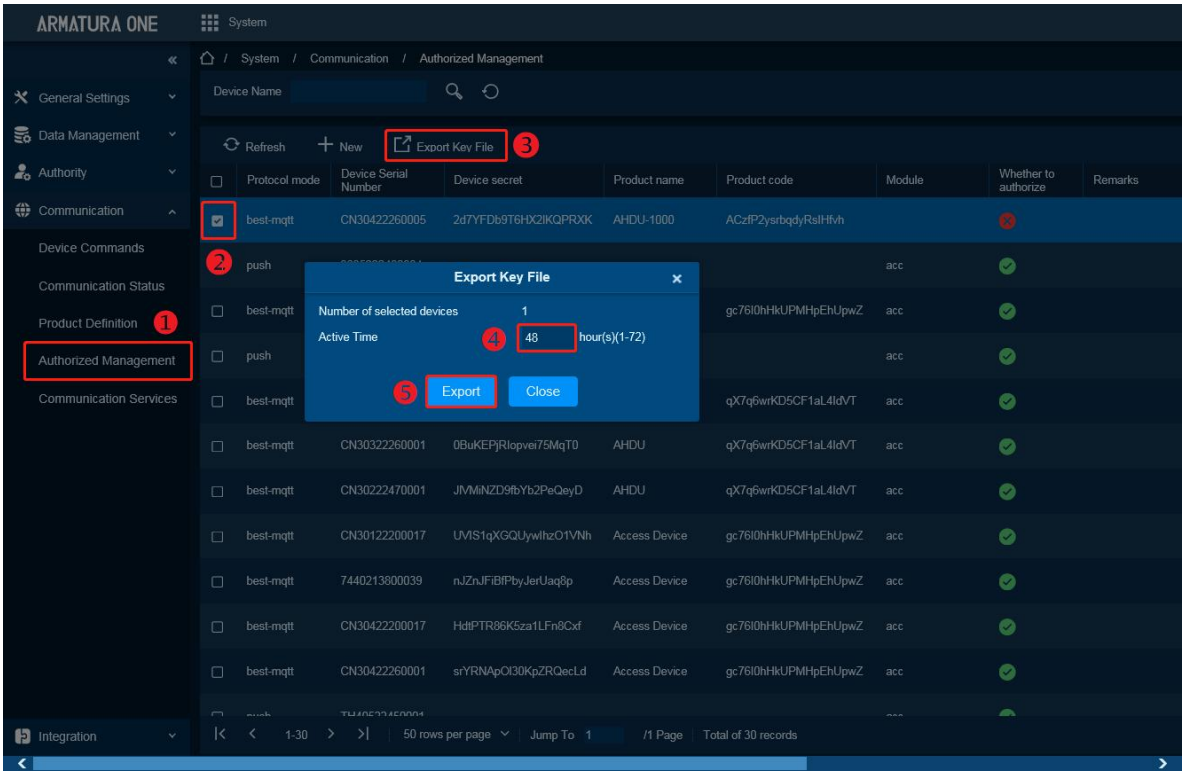
Click **System > Communication > Authorized Management > New** to add a device on the software.



Select the newly created product and enter the serial number. Click '**OK**' to save and exit.

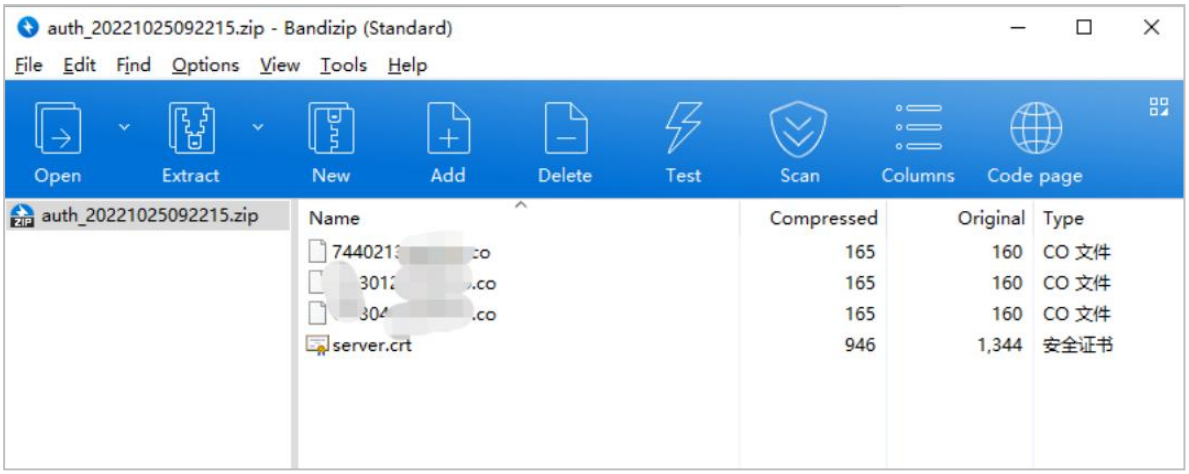
3. Export Key File

Go to **System > Communication > Authorized Management** to verify the newly added device, and then select **Export Key File**.



- **Active time**：Key file validity, value can be 1-72 Hours.

After clicking '**Export**', the browser will download a .zip file.



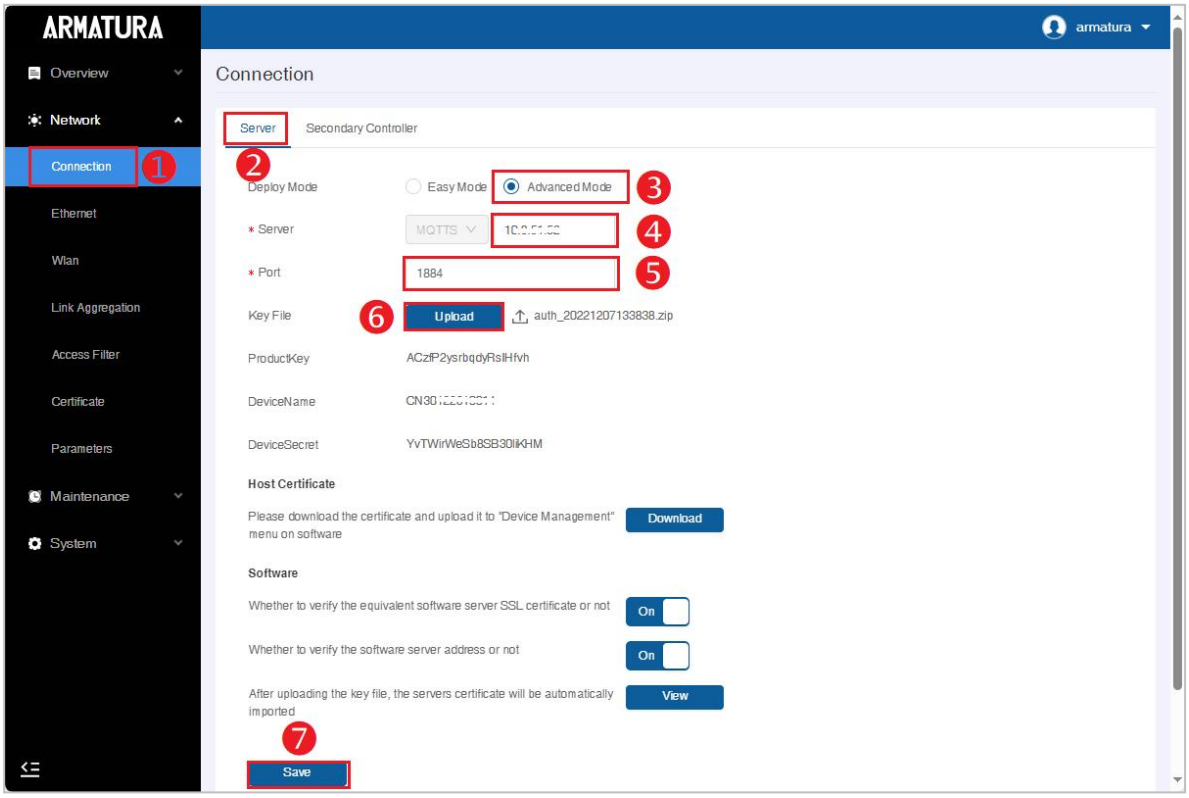
Note: *This function supports selecting multiple devices. By clicking the icon, it will generate all controller .co files and server certificates in a .zip package. Simply upload this .zip package to the controller webserver.*

4. Import Key file to controller

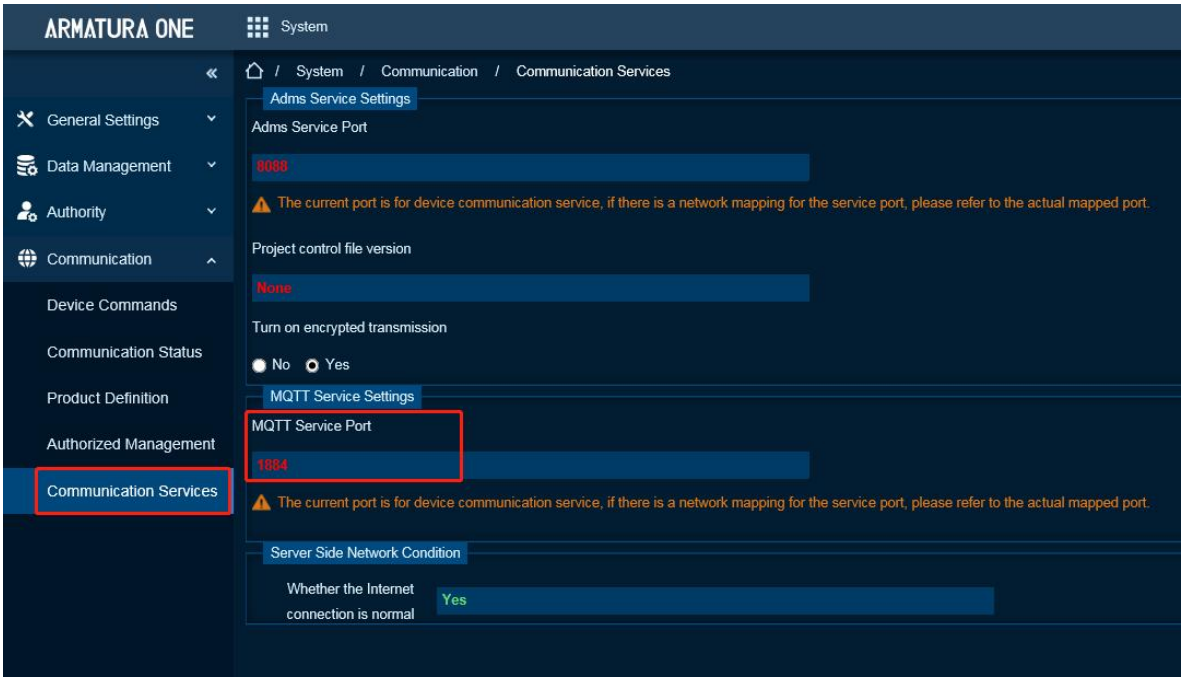
1) Open https:// [controller's IP address] in browser to enter the login interface.

During the first login, use '**armatura**' as the default username and password. The system will prompt the admin to change the password upon logging in.

2) Click **Network > Connection > Server > Advanced Mode** on the Webserver interface.

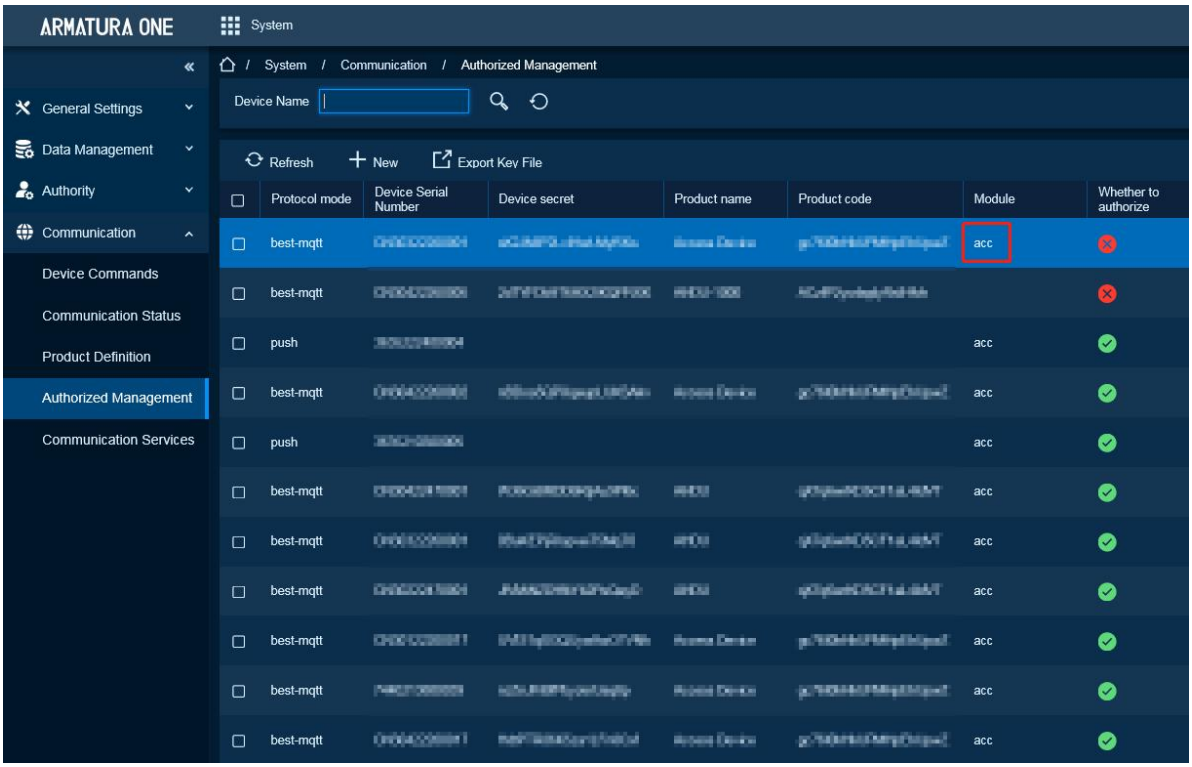


- **Server:** The default protocol is MQTTs, and the address is the server address.
- **Port:** The default port is 1884, and you can verify this port by navigating to **System > Communication > Communication Services > MQTT Service Port**.



- **Key File:** This file is exported from **System > Communication > Authorized Management**.

  After successfully connecting the controller to MQTT, the Column Module will display 'acc'. However, since the device is not yet authorized to access the Access Module, it will show .



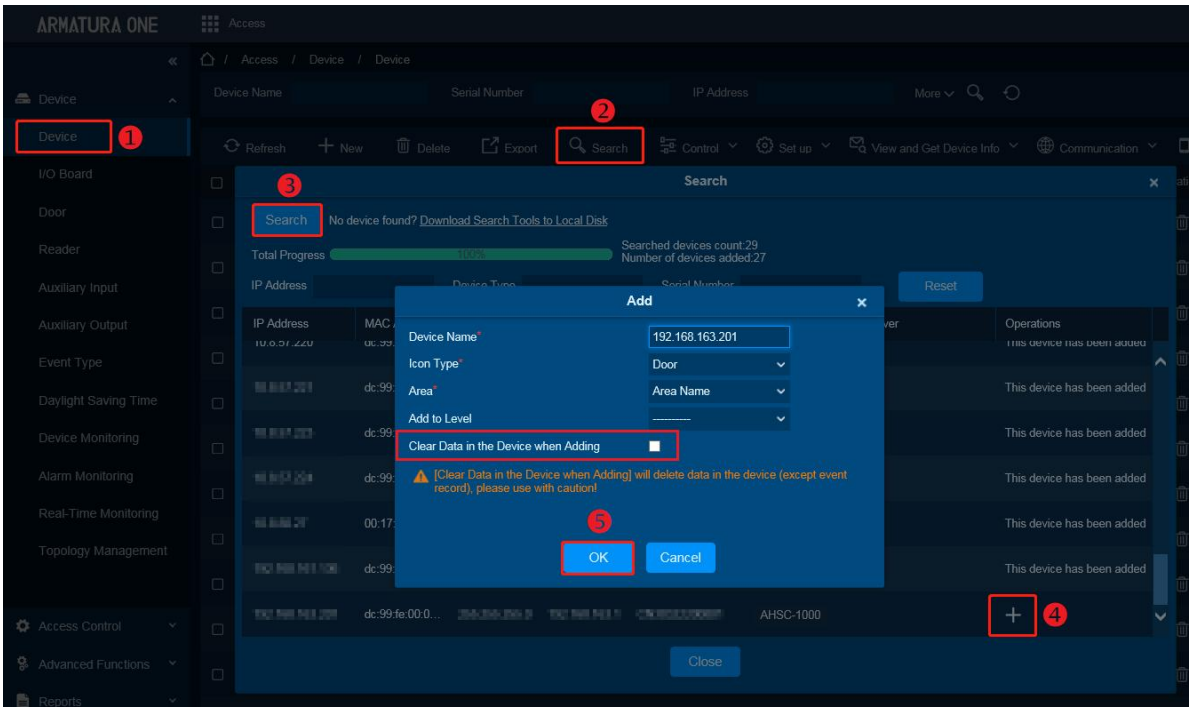
5. Add Controller on the Software

1) Click **Access > Device > Device > Search**, to open the Search interface.

2) After clicking **Search**, the list and the total number of Access Control Devices will be displayed.

3) Click the "**Add**" button adjacent to the Device to include it

4) Click **OK** to save and exit.



Note: *We recommend selecting* ***[Clear Data in Device when Adding]*** *to clear device data during the addition process.*

9. Elevator Control System

9.1 System Overview

1. The Armatura Horizon series controllers and I/O boards are designed to be used not only for access control, but also for elevator control applications. Although a single controller supports both application modes, it can only be selected for either elevator control or access control at a time.

2. The Armatura One software can manage both access control and elevator control simultaneously. By utilizing Armatura One, along with the compatible AH series controllers and I/O boards, as well as Armatura readers, a complete one-stop solution can be provided to customers.

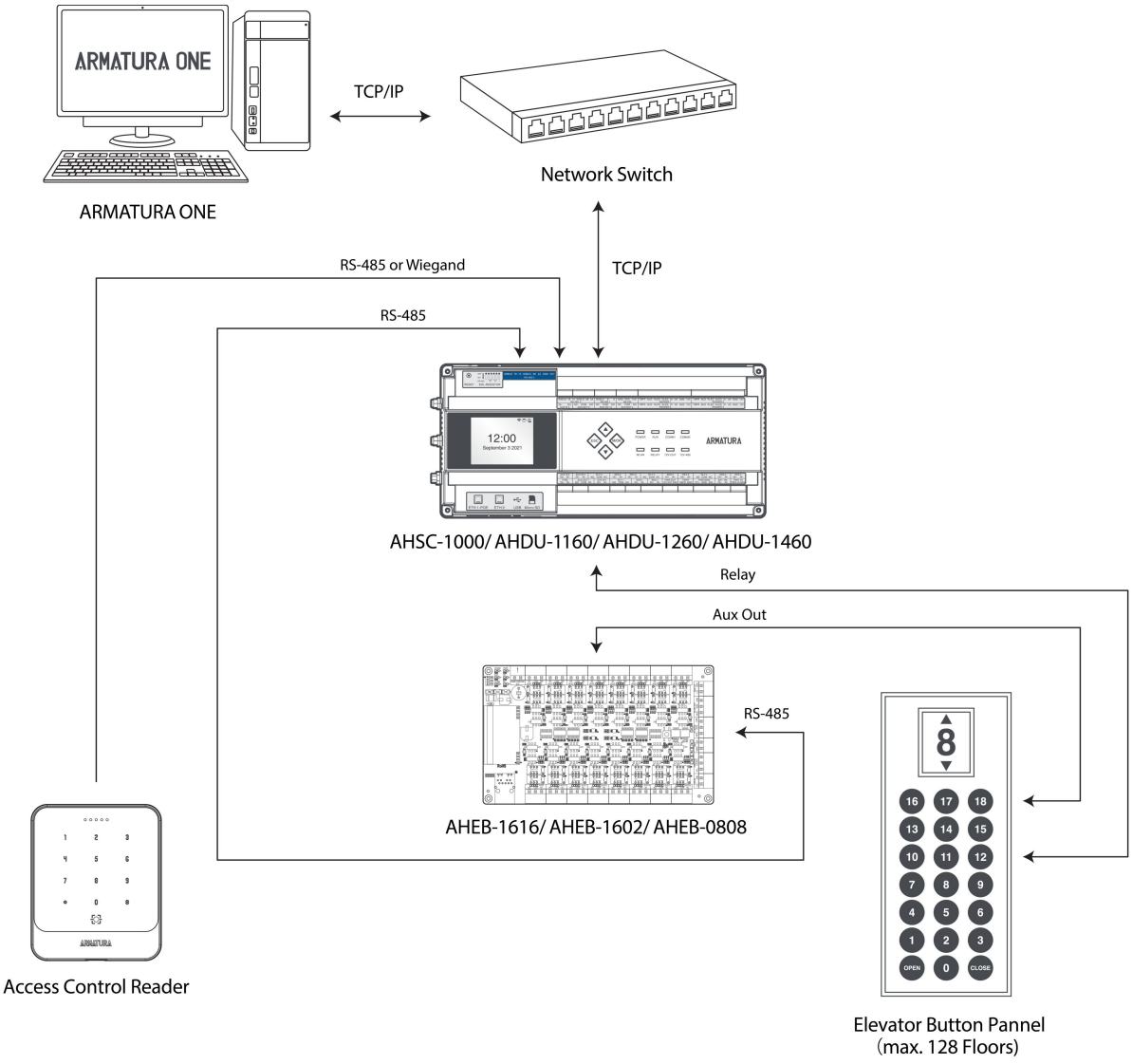


Figure 9-1 Elevator Control System Wiring Diagram

Notes:

- *To access the elevator buttons, it is necessary to remove the elevator button panel. The manufacturer should provide the control circuits for the corresponding floor buttons. If the manufacturer cannot provide them, it will be necessary to check each wire individually to ensure that the circuits are functioning properly.*
- *One controller can support up to **128** floors.*
- *AHEB-0808/AHEB-1602 are available to support connecting to AHSC/AHDU panels for elevator control purpose now by upgrading the firmware. AHEB-1616 is coming soon.*
- *The AHSC/AHDU controller must be running the MCU firmware version 6.3.2.5 or higher to utilize the onboard relay for floor control. If the controller is not updated to this version, floor control must be achieved through the auxiliary outputs of the I/O board. Should you require assistance, please contact the headquarters for technical support.*

9.2 Elevator Control Wiring

9.2.1 AHEB-0808 / AHEB-1602 Connect with Elevator Panel

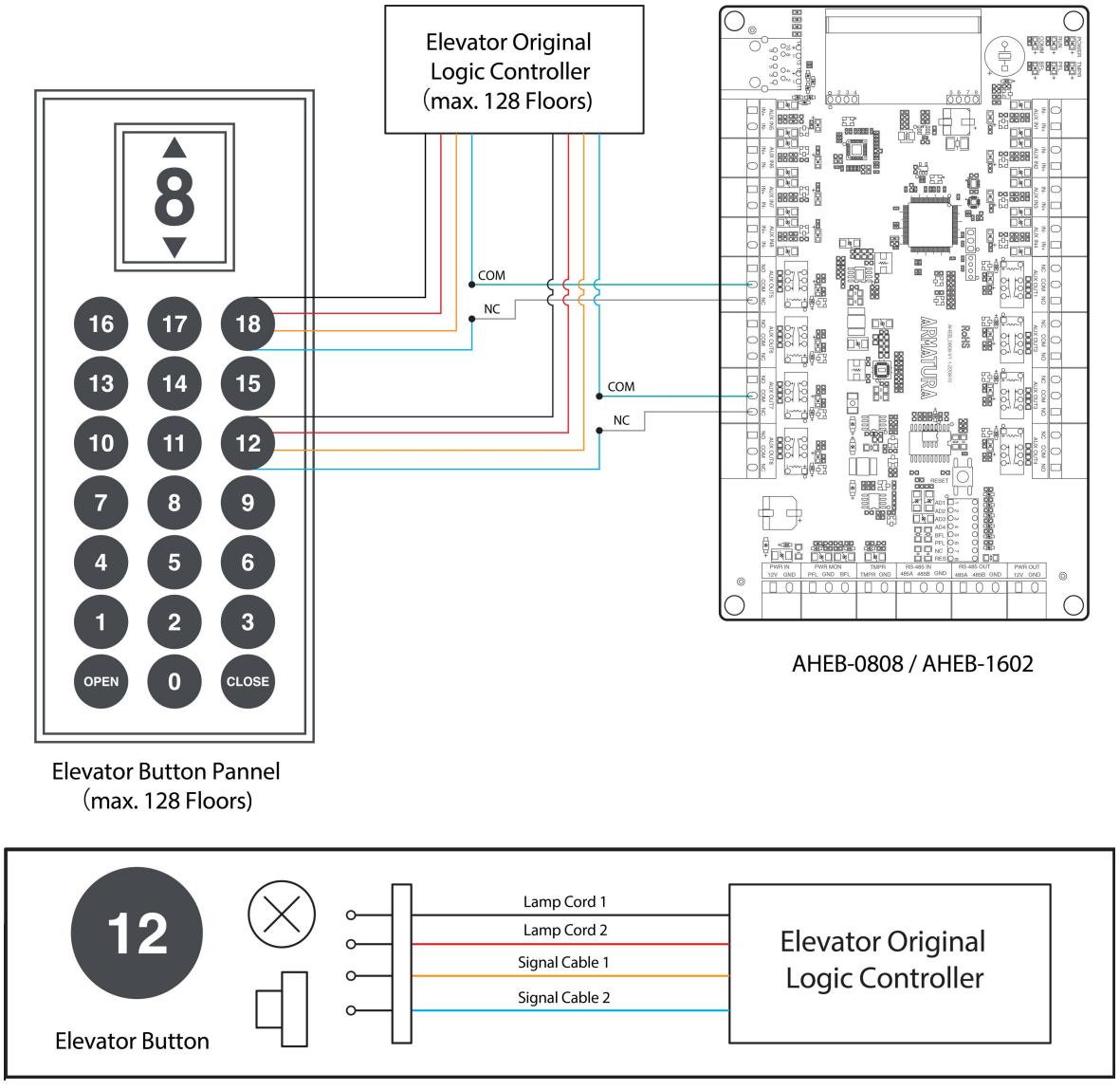


Figure 9-2 AHEB-0808 / AHEB-1602 Wiring Diagram with Elevator Panel

Notes:

- *AHEB-0808 and AHEB-1602 do not support **Direct Floor Selection** and **Button Feedback** functions. In this case, you only need to connect the normally closed (NC) terminals and common (COM) terminals of the auxiliary output ports in series to the signal lines of the elevator buttons.*
- *Refer to Appendix 1 Elevator Control and Elevator Button Wiring for detailed wiring.*

9.2.2 AHEB-1616 Connect with Elevator Panel

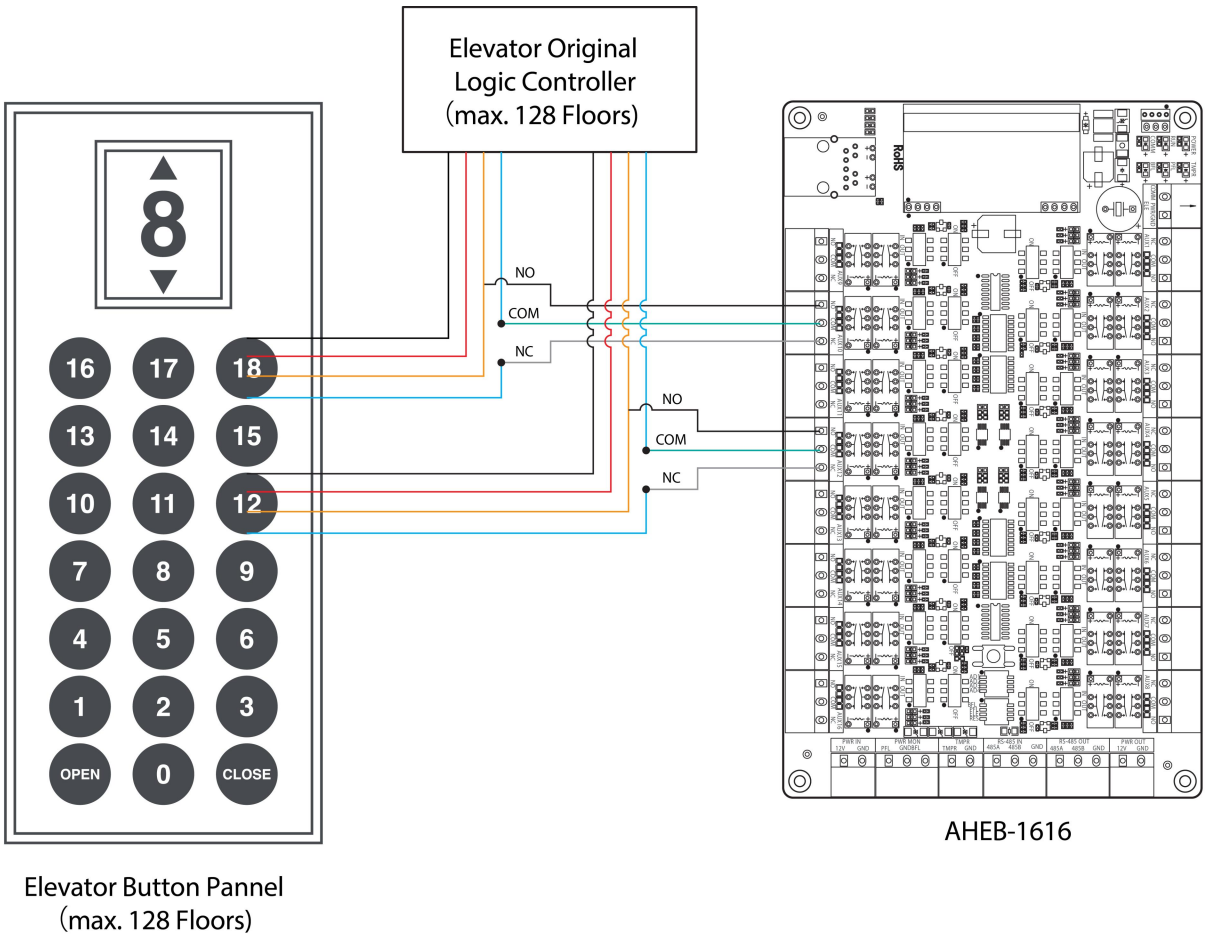


Figure 9-3 AHEB-1616 Wiring Diagram with Elevator Panel

Elevator Button Wiring Description

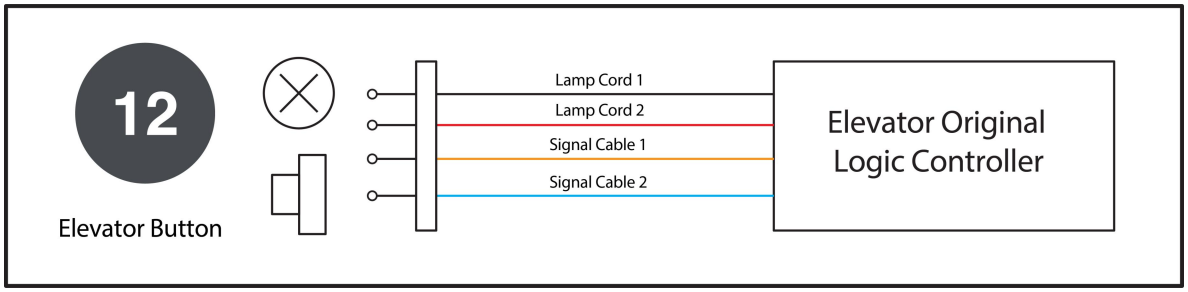


Figure 9-4 Elevator button wiring schematic

Instruction:

- *Connect **Signal Cable 1** to the **NO** terminal on the corresponding floor of the elevator logic controller. After Signal Cable 2 is disconnected, **COM** and **NC** terminals are connected to the **COM** and **NC** terminals of the corresponding floor respectively.*

Wiring for swipe to select floor and direct floor selection

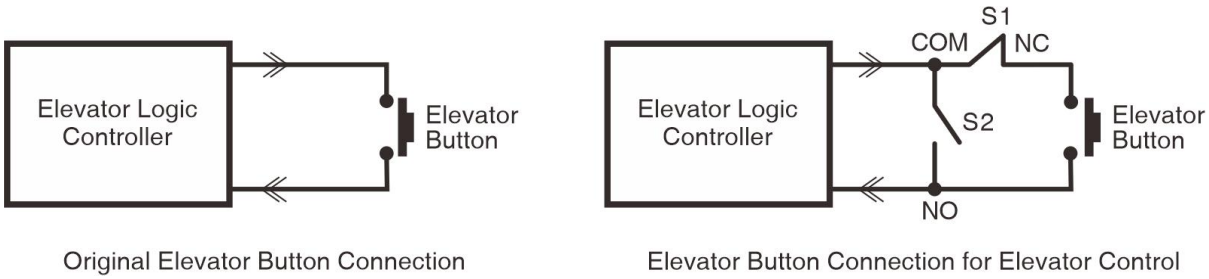


Figure 9-5 Swipe card to select the floor and direct selection of floor wiring diagram

Instruction:

- *S1 and S2 switches are two relays (S1 relay is normally closed and S2 relay is normally open) of the elevator control board respectively. S1 is disconnected after power on, and S1 is closed after swiping the layer selection card, then the elevator button can be lit by pressing; S2 is closed after swiping the direct access card, then the elevator button will be lit automatically.*
- *Refer to Appendix 1 Elevator Control and Elevator Button Wiring for detailed wiring.*

9.2.3 Multiple I/O Boards Wiring

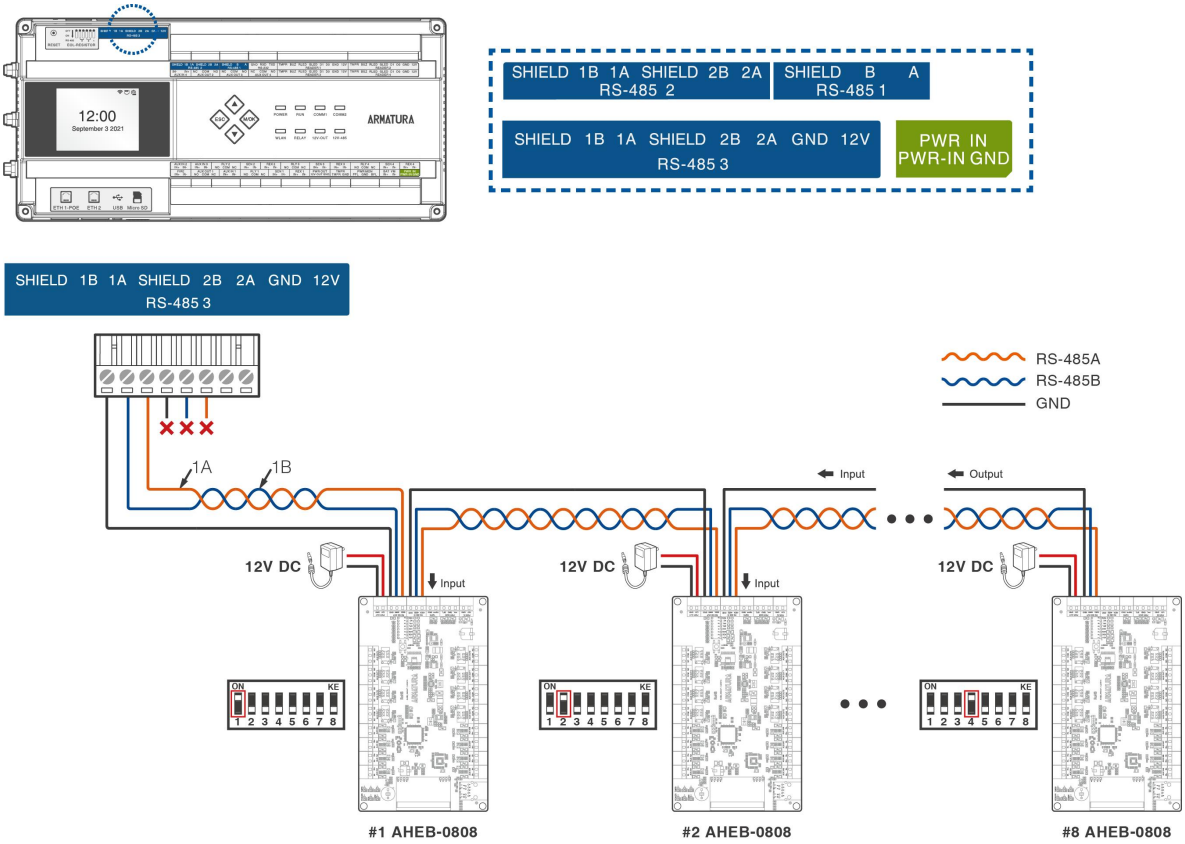


Figure 9-6 Hand-to-hand connection of multiple I/O board

Notes:

- *As shown in the above figure, the RS-485 interface of the controller is first connected to the RS-485 **OUT**/IN port of the first I/O board, and then the RS-485 **IN**/OUT port of the first I/O board is connected to the RS-485 **OUT**/IN port of the next I/O board in turn, adopting the hand-in-hand wiring method, and so on.*
- *A maximum of **24** AHEB-0808/AHEB-1602/AHEB-1616 expansion boards can be connected to each RS-485 port. However, the total number of floors cannot exceed **128**.*
- *Please set the DIP switches on each I/O board to allocate unique RS-485 addresses, ensuring there are no overlaps among the boards.*
- *Please supply power to the I/O board with an independent 12V 3A DC power to ensure its stable operation. A single 12V 3A DC power can power up to 8 I/O boards.*

9.2.4 Fire Alarm Interface Wiring

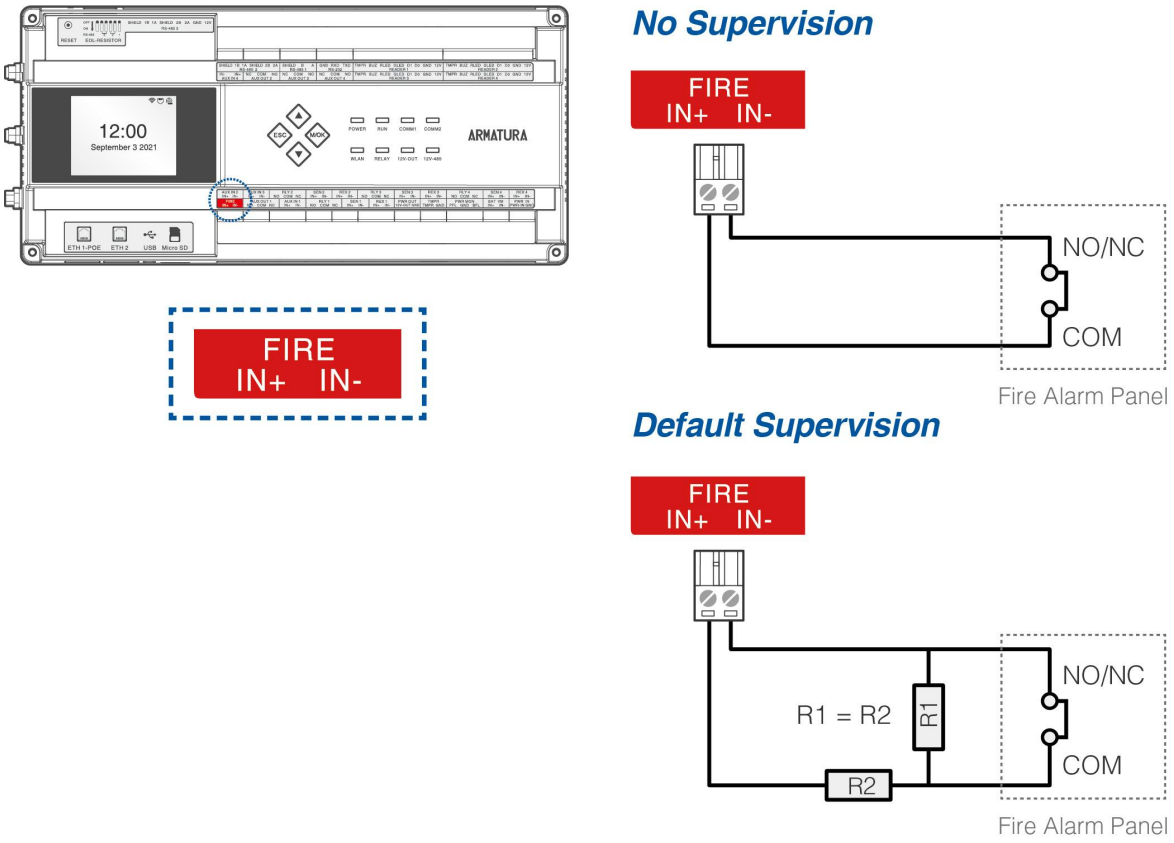


Figure 9-7 Fire Alarm Interface Wiring

Notes:

- *Once a fire alarm is triggered, all elevator buttons will become unusable. The fire alarm condition can only be cleared by either restarting the device or by a power cycle.*
- *The Fire Alarm is an optional feature and is not required to be connected. Please connect it according to your specific needs.*
- *To activate this feature, the controller's MCU must be upgraded to **version 6.3.2.5** or above.*
- *In this elevator control system, the fire alarm interface has the highest priority, followed by the emergency interface, with the manual interface being the lowest in the hierarchy.*

9.2.5 Emergency Interface Wiring

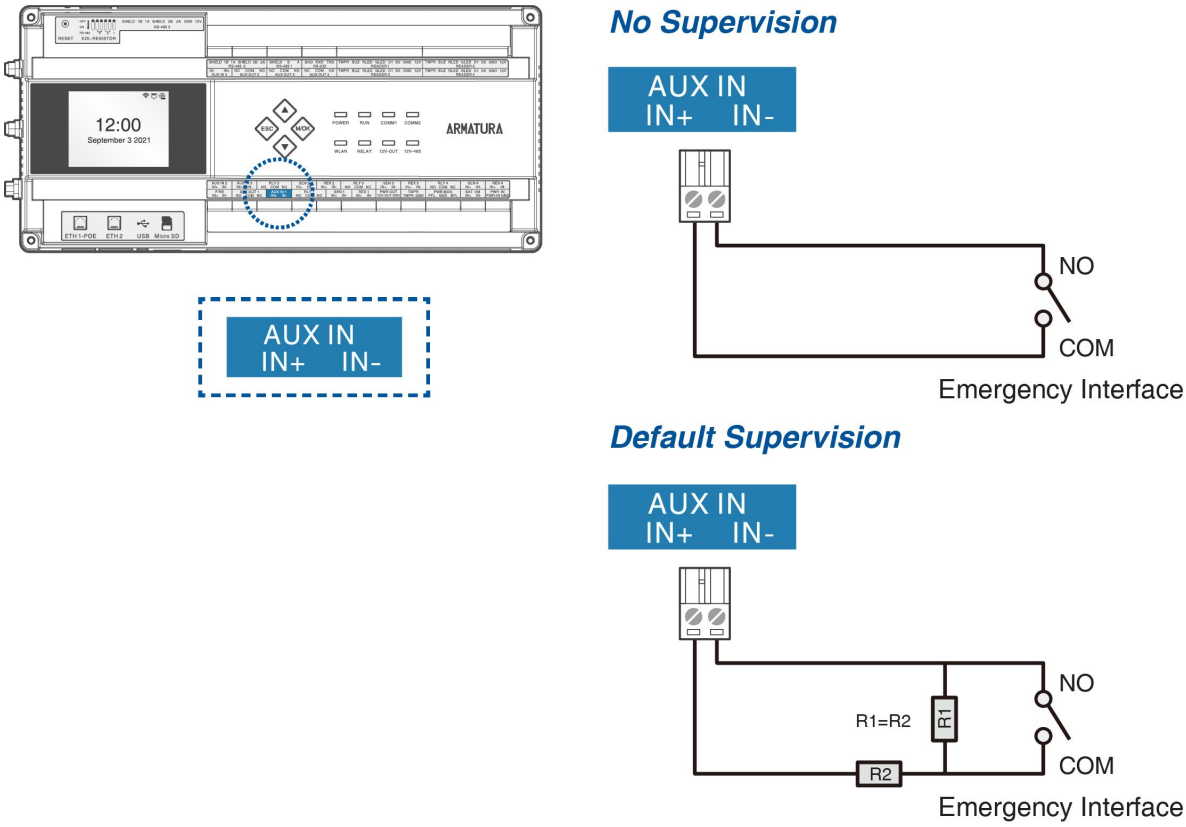
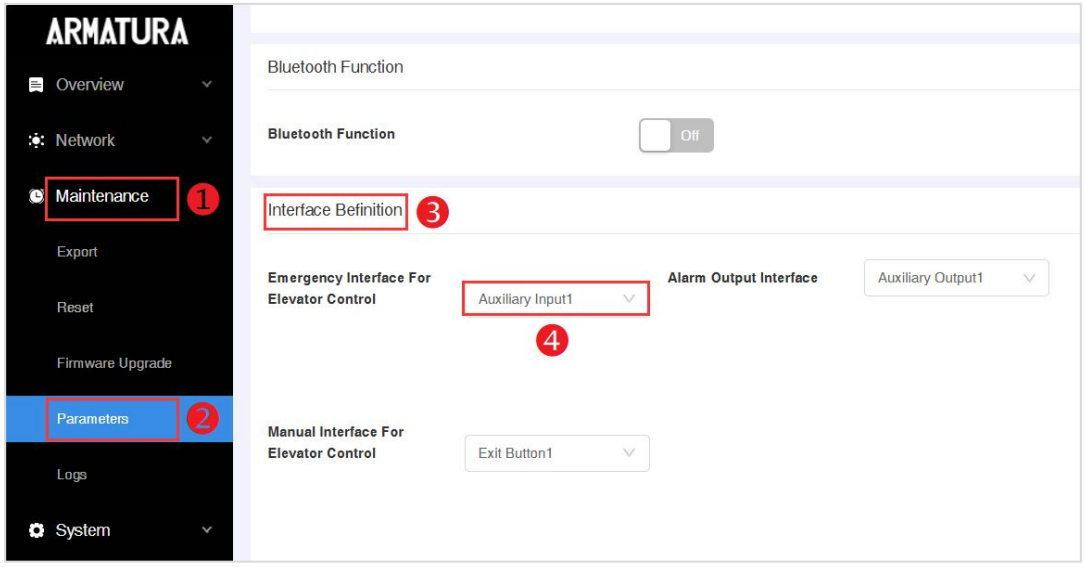


Figure 9-8 Emergency Interface Wiring

Notes:

- *In an emergency, upon receiving a short circuit signal by the emergency interface, the elevator control system will cease to govern the elevator buttons, releasing all floor buttons for free operation. The control system can only be restored by either a power-off restart of the device or through software settings adjustments.*
- *The Emergency Interface is an optional feature and is not required to be connected. Please connect it according to your specific needs.*
- *The system's default interface is **Auxiliary Input 1**. You can also modify it in the controller's **Webserver** under **[Maintenance]** > **[Parameters]** > **[Interface Definition].***



- *To activate this feature, the controller's MCU must be upgraded to **version 6.3.2.5** or above.*
- *In this elevator control system, the fire alarm interface has the highest priority, followed by the emergency interface, with the manual interface being the lowest in the hierarchy.*

9.2.6 Manual Interface Wiring

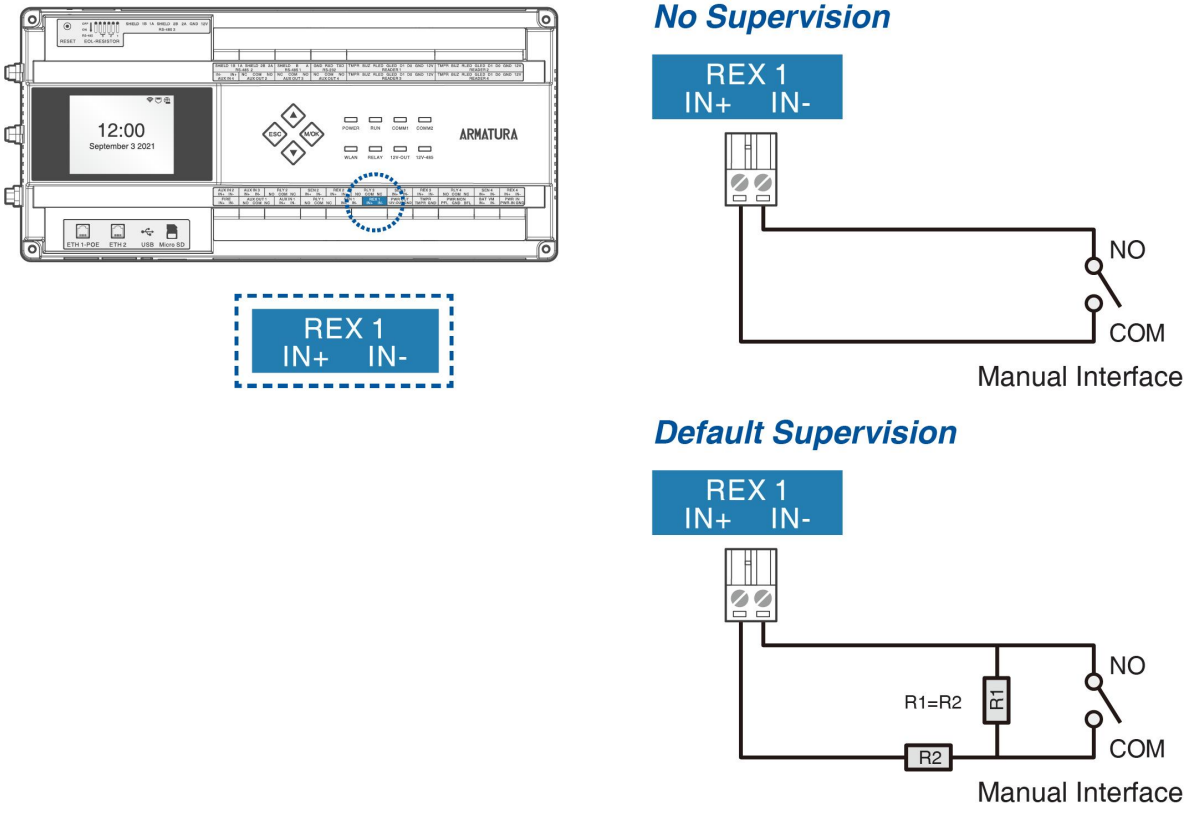
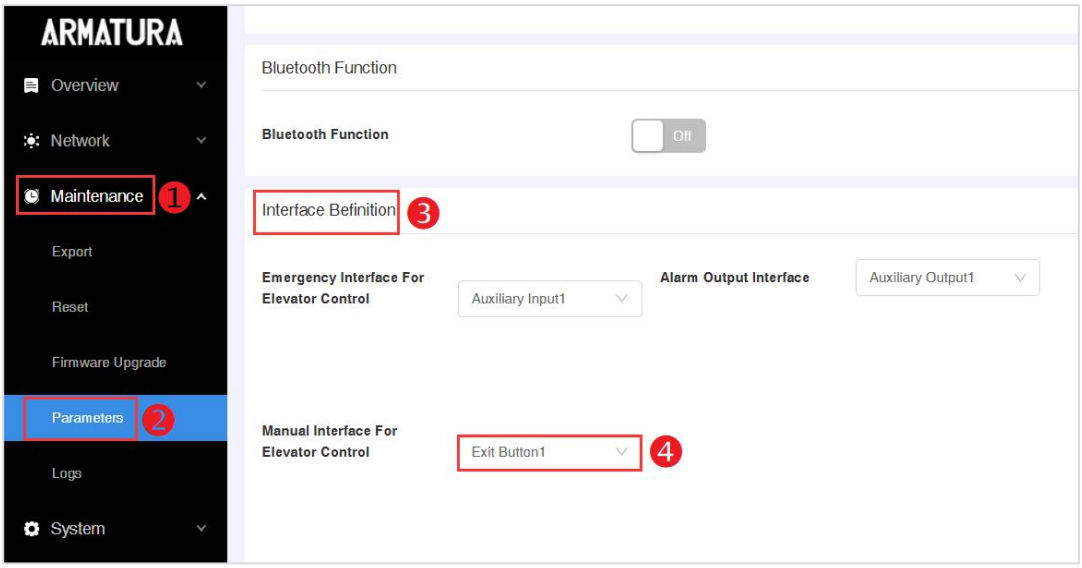


Figure 9-9 Manual Interface Wiring

Notes:

- *In the event of a short circuit at the manual interface, the elevator control system will relinquish control over the elevator buttons, allowing all floor buttons to be freely pressed. Once the manual interface is restored, the elevator will automatically resume its controlled status.*
- *The Manual Interface is an optional feature and is not required to be connected. Please connect it according to your specific needs.*
- *The system's default interface is **REX 1**. You can also modify it in the controller's **Webserver** under **[Maintenance]** > **[Parameters]** > **[Interface Definition].***



- *To activate this feature, the controller's MCU must be upgraded to **version 6.3.2.5** or above.*
- *In this elevator control system, the fire alarm interface has the highest priority, followed by the emergency interface, with the manual interface being the lowest in the hierarchy.*

9.2.7 Alarm Output Interface Wiring

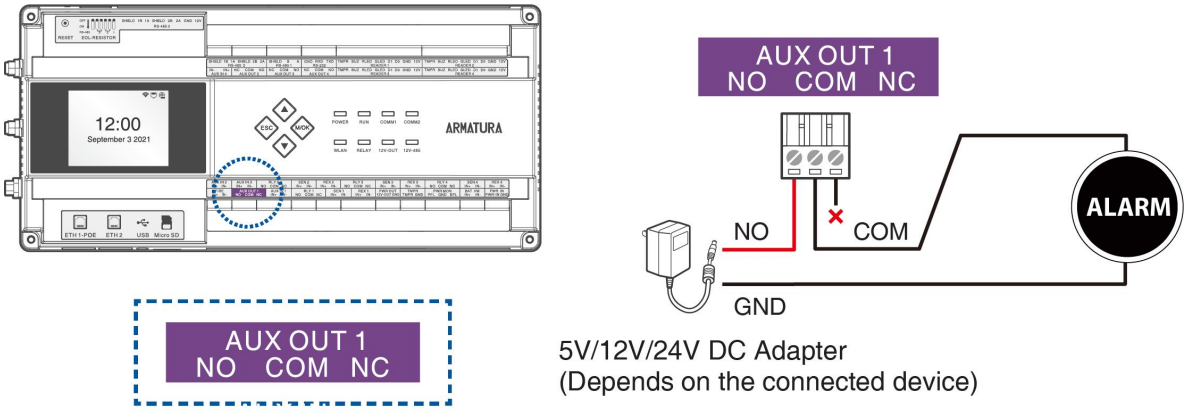


Figure 9-10 Alarm Output Interface Wiring

Notes:

- *The Alarm Output is an optional feature and is not required to be connected. Please connect it according to your specific needs.*
- *Use the Alarm Output Interface to connect an alarm.*

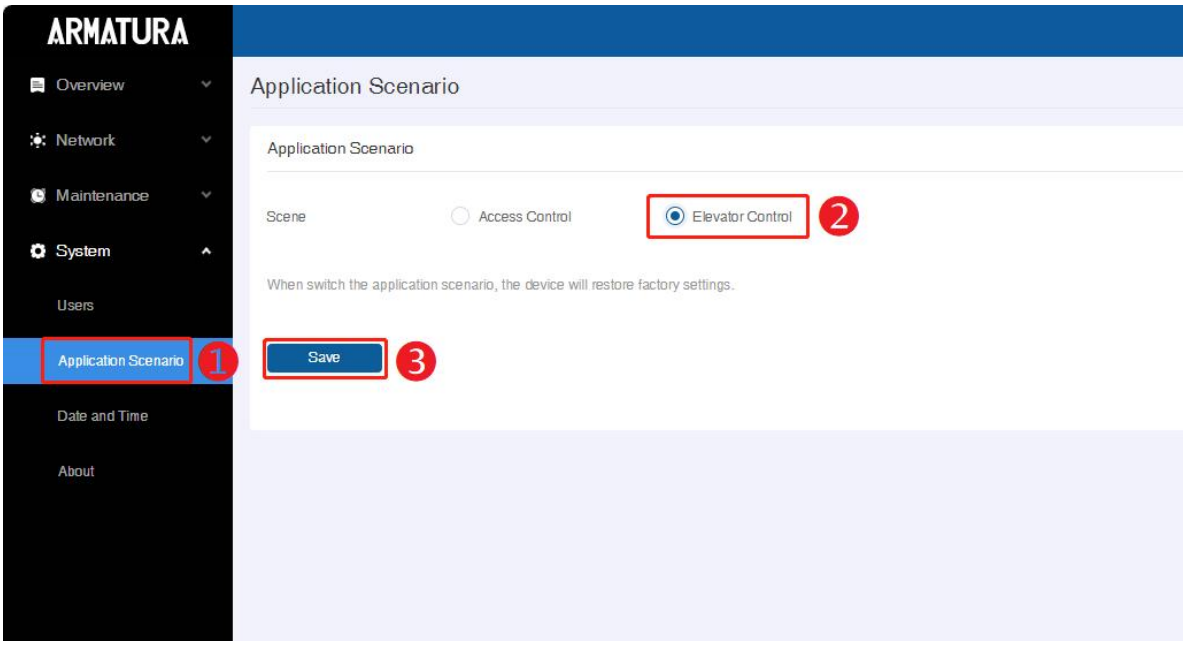
9.3 Configuring Parameters on the Webserver

Remarks:

- *Please confirm that your controller's firmware is at least **version 10.0.15** to enable the elevator control function.*
- *If the current version is lower than this requirement, please contact your local branch or the headquarters' technical support for assistance.*

9.3.1 Switching Controller to Elevator Control

1. Log in to the controller's webserver. For details, refer to 7.2 Login to the Webserver.
2. Click **System** > **Application Scenario** to change the **Scene** setting to **Elevator Control**.
3. Click **Save** to apply the changes. After switching to elevator control mode, the controller will revert to factory settings and automatically restart.

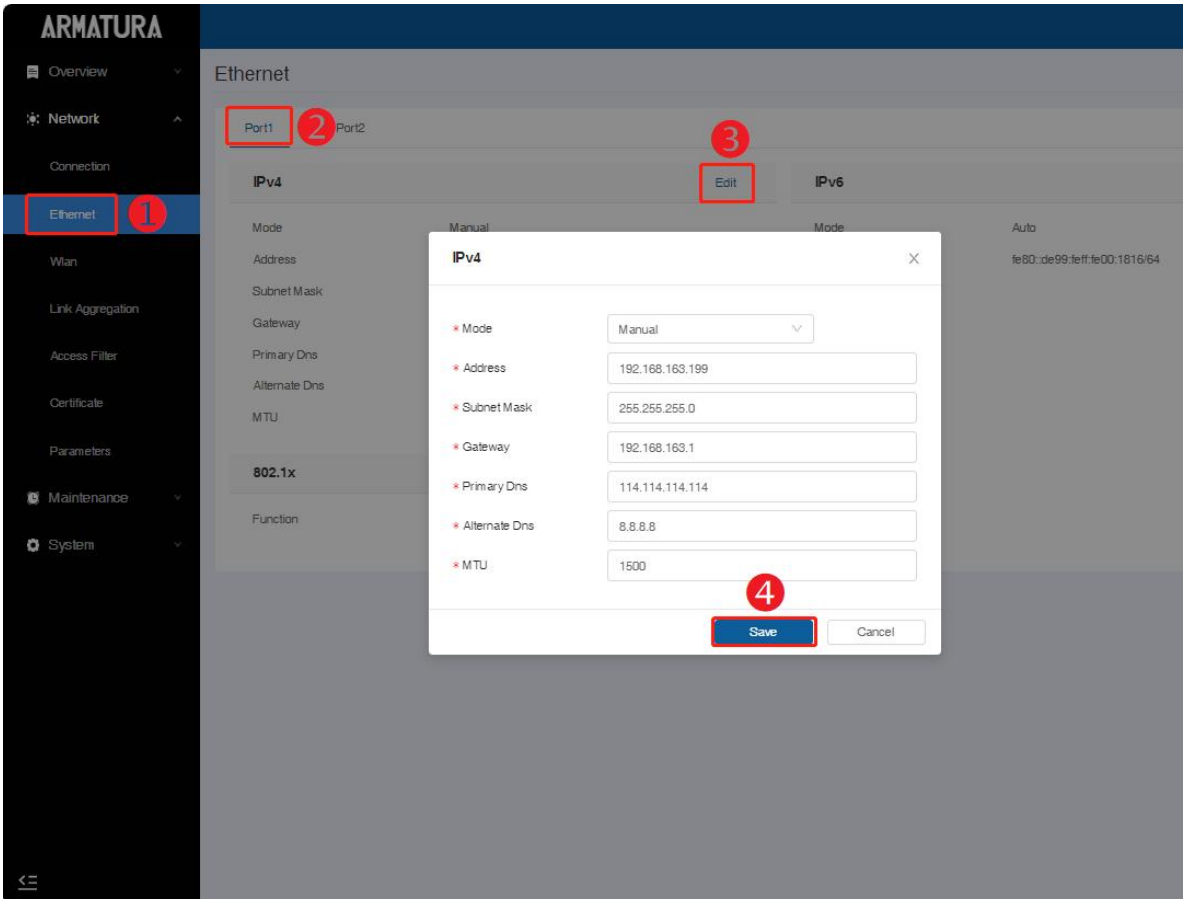


Notes:

- *If you are unable to find the **[Application Scenario]** option under **[System],** you will need to contact technical support or headquarters for assistance. They can help upgrade the controller's firmware and import the activation license.*
- *You can also import the license by clicking **System** > **About** > **Import License**.*

9.3.2 Modifying Controller Network Parameters

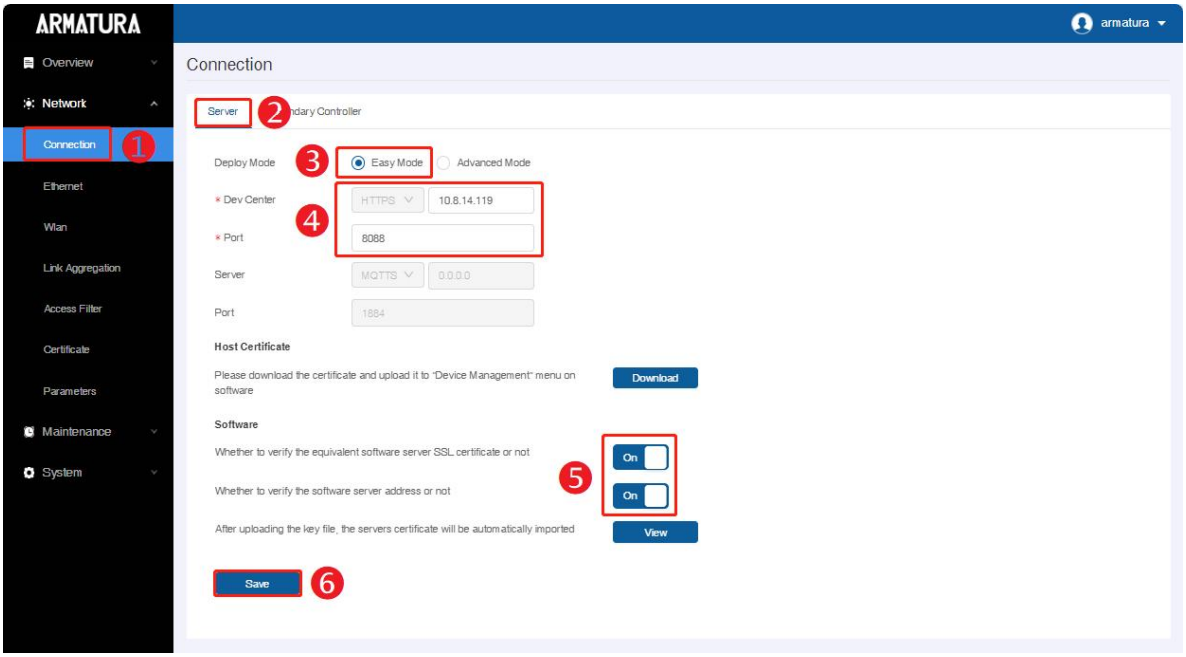
1. After the controller reboots, log back into the controller's webserver using the default IP (**192.168.1.201**), default username (**armatura**) and default password (**armatura**).
2. Then click **Network** > **Ethernet** > **Port1/Port2** to modify the network parameters of the controller (You can connect to the controller's Eth1 (default IP **192.168.1.201**) or Eth2 (default IP **192.168.2.202**).The settings in the image below are for reference only.



9.3.3 Configuring Controller Connection to Platform Parameters

The latest firmware for the controller supports both **Easy Mode** and **Advanced Mode** for adding it to the software. The following is an explanation of the operation of the Easy Mode as an example.

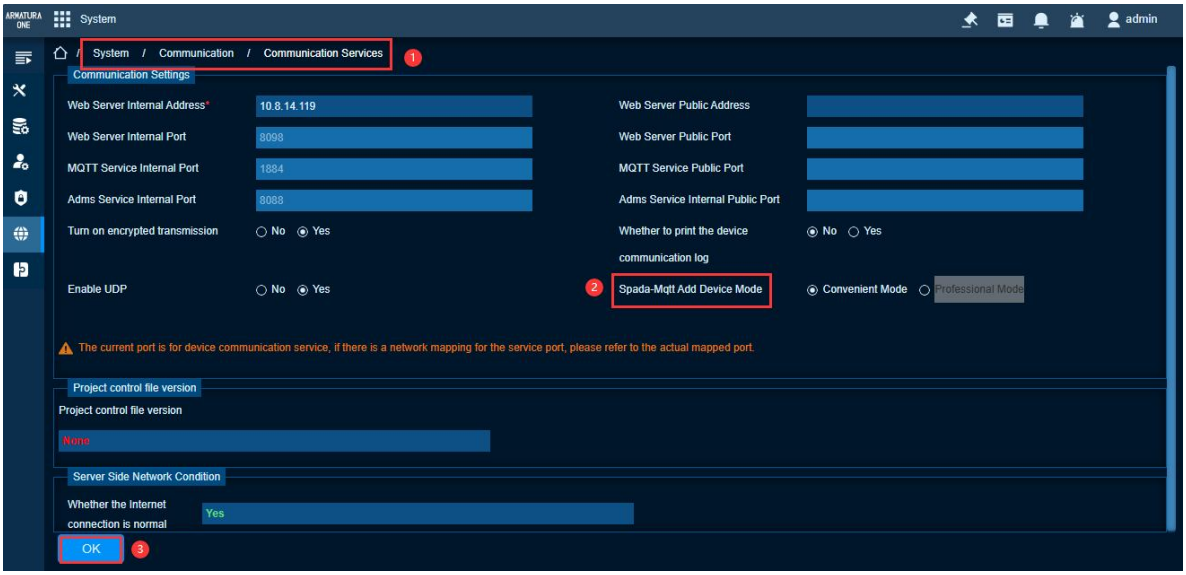
1. On the webserver page of the controller, click **Network** > **Connect**, and then select **Easy Mode** in the Deploy Mode**.**
2. Enter the IP address or domain name of the ARMATURA One software, with the default port set to **8088** (depending on the situation).
3. Enable both options in [**Software**].
4. Finally, click **Save** to save the settings and exit.



9.4 Configuring Parameters on the Armatura One

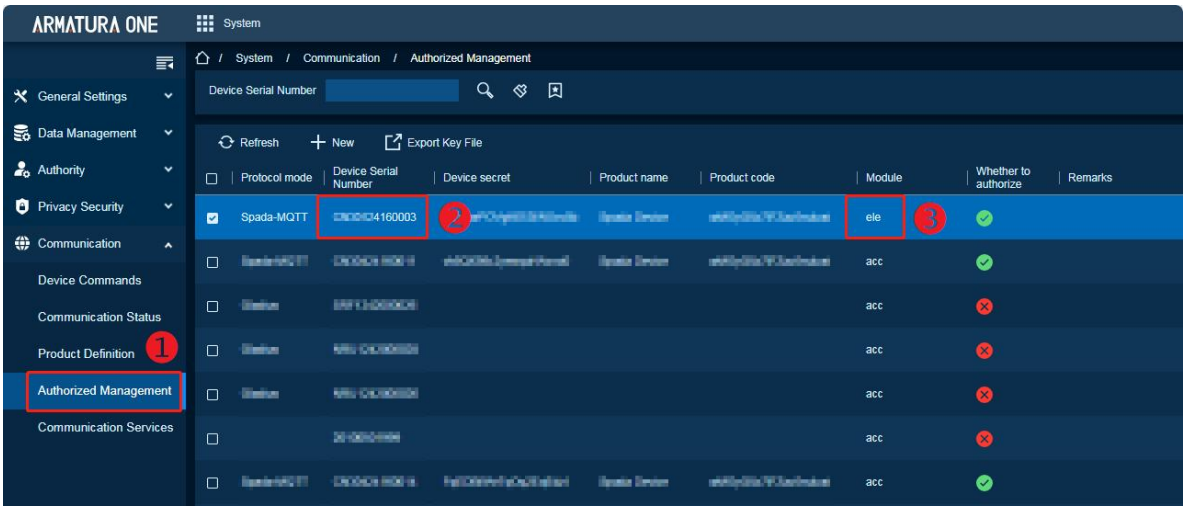
9.4.1 Modifying Spada-MQTT to Add Device Mode

1. Log in to the Armatura One software.
2. Click on **System** > **Communication** > **Communication Services** to configure the '**Spada-Mqtt Add Device Mode**' parameter as Convenient Mode or Professional Mode.
   - Select [**Convenient Mode**] when the controller is set to **Easy Mode**.
   - Select [**Professional Mode**] when the controller is set to **Advanced Mode**.
3. Click the **OK** to save and exit.



9.4.2 Checking Controller Authorization

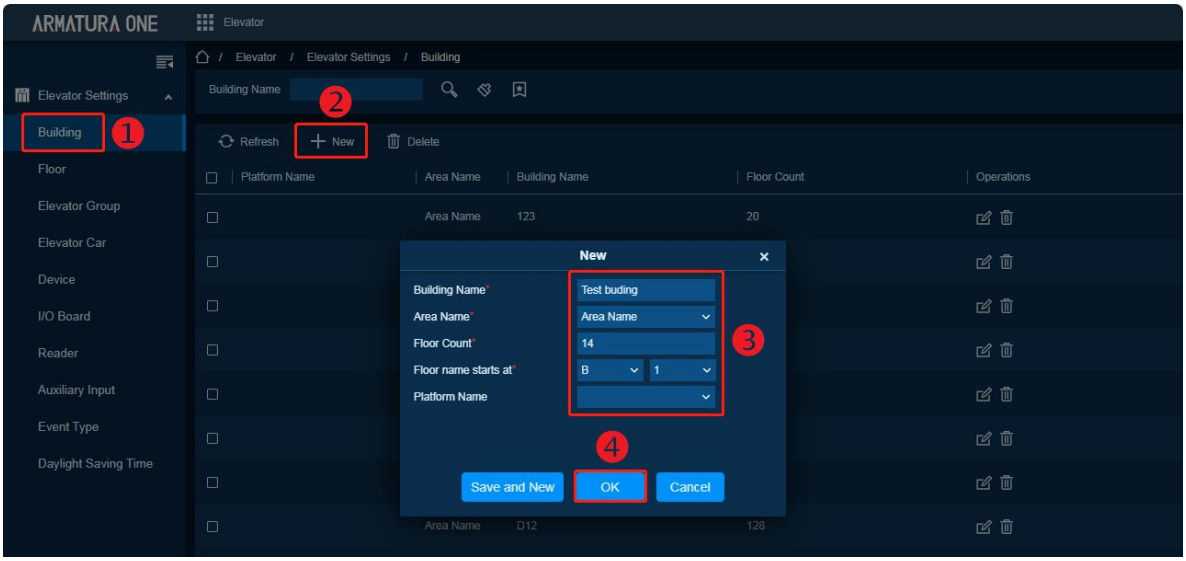
1. Click on **System** > **Communication** > **Authorized Management** to enter the authorized management interface.
2. Find the appropriate serial number in the list and check that the **Module** column shows **ele**.
   - Displaying [**ele**] indicates that the device is authorized.
   - If [**ele**] is not displayed, please check the connection settings of the controller.



9.4.3 Add Building, Floor, Elevator Groups and Elevator

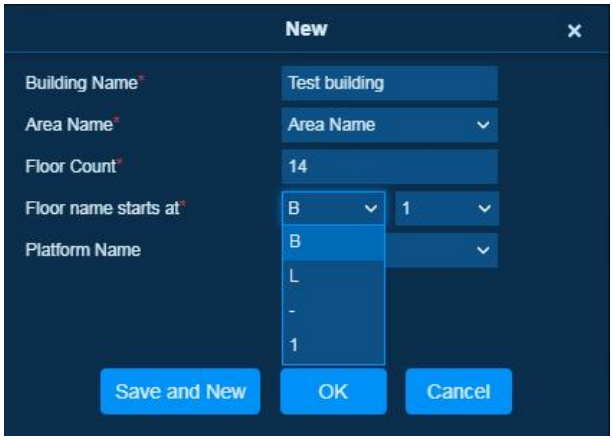
Add building and floor

1. Click on **Elevator** > **Elevator Settings** > **Building** > **New** to add a building.
2. In the **New** window that pops up, set the building information according to the actual situation.
3. Finally, click **OK** to save and exit.



For example, the Test building, 13 floors above ground and 1 floor below ground, totaling 14 floors.

Enter the appropriate information in the **New** window as shown below.



Building Name: Enter the building name.

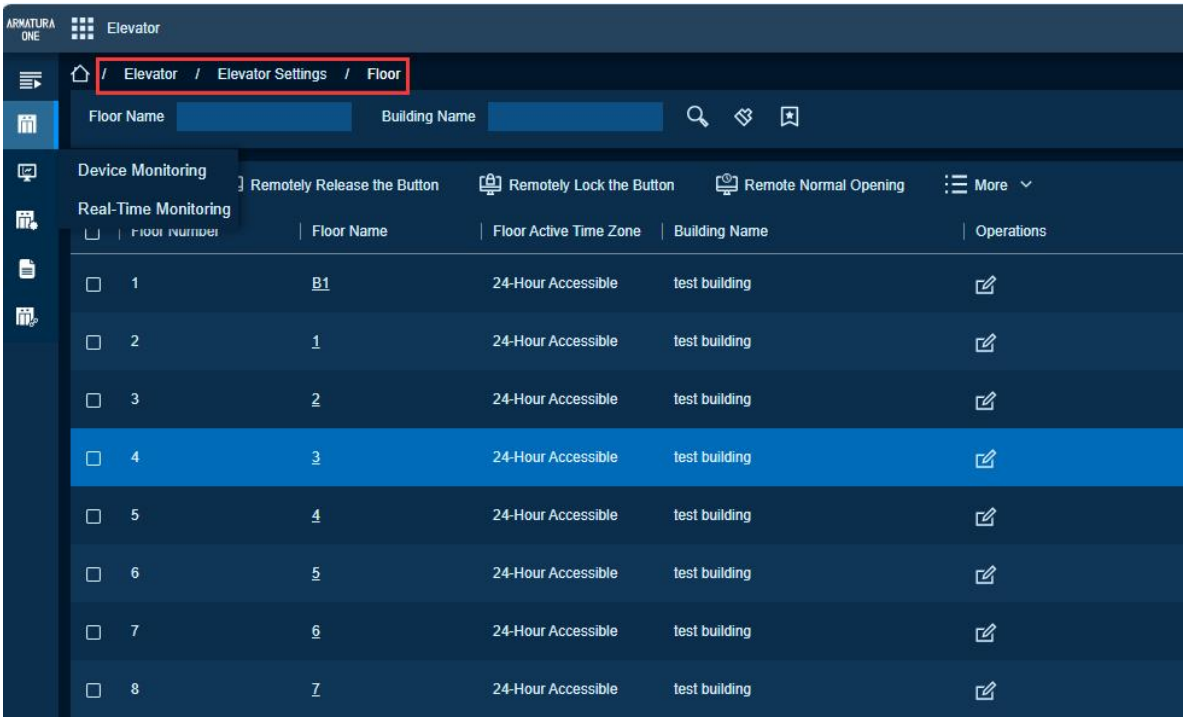
Area Name: Enter the area name.

Floor Count: Enter the total number of floors.

Floor name starts at:

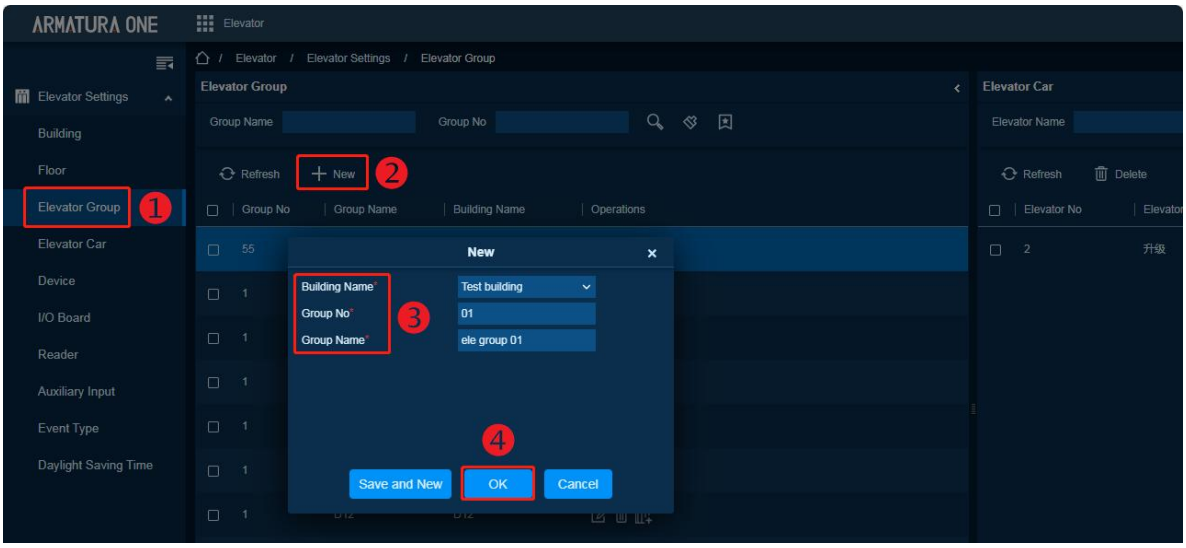
- **B / -** : Indicates basement floors. For example, the second basement level is indicated as [**B2**] or [**-2**]
- **1 / L**: Represents the first floor or lobby, usually indicated by [**1**] or [**L**].

4. After adding, you can view the generated floors on the [**Elevator** > **Elevator Settings** > **Floor**] page.



Add elevator group to the building

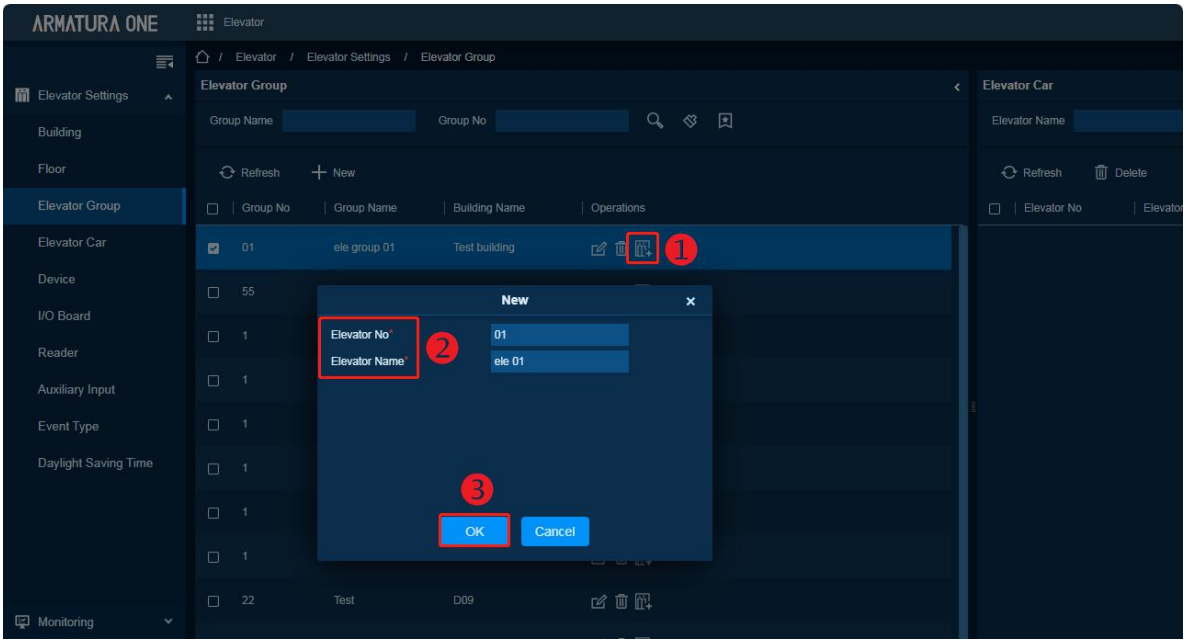
1. Click on **Elevator** > **Elevator Settings** > **Elevator Group** > **New** to add a new elevator group to the building.
2. In the **New** window that pops up, select building, fill in the No and name of the elevator group.
3. Click **OK** to save and exit.



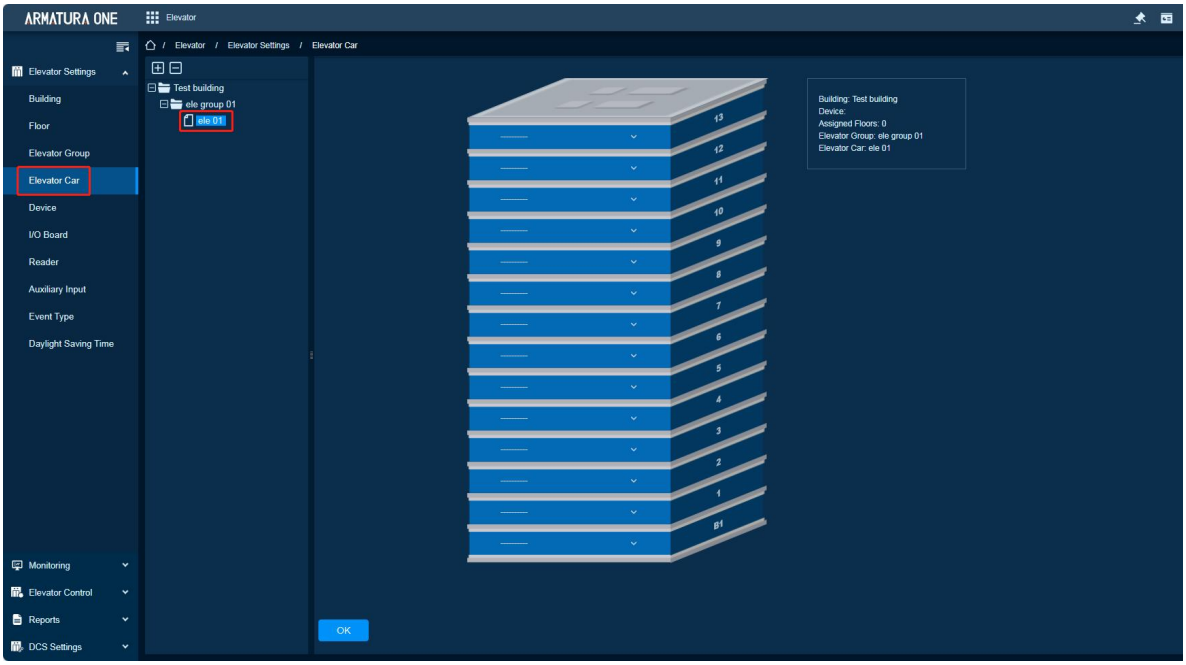
Add elevator to the elevator group

1. In the Elevator Group list, click the  icon to add elevators to the elevator group.

2. Enter the elevator number and name in the pop-up **New** window according to the actual situation.
3. Click **OK** to save and exit.



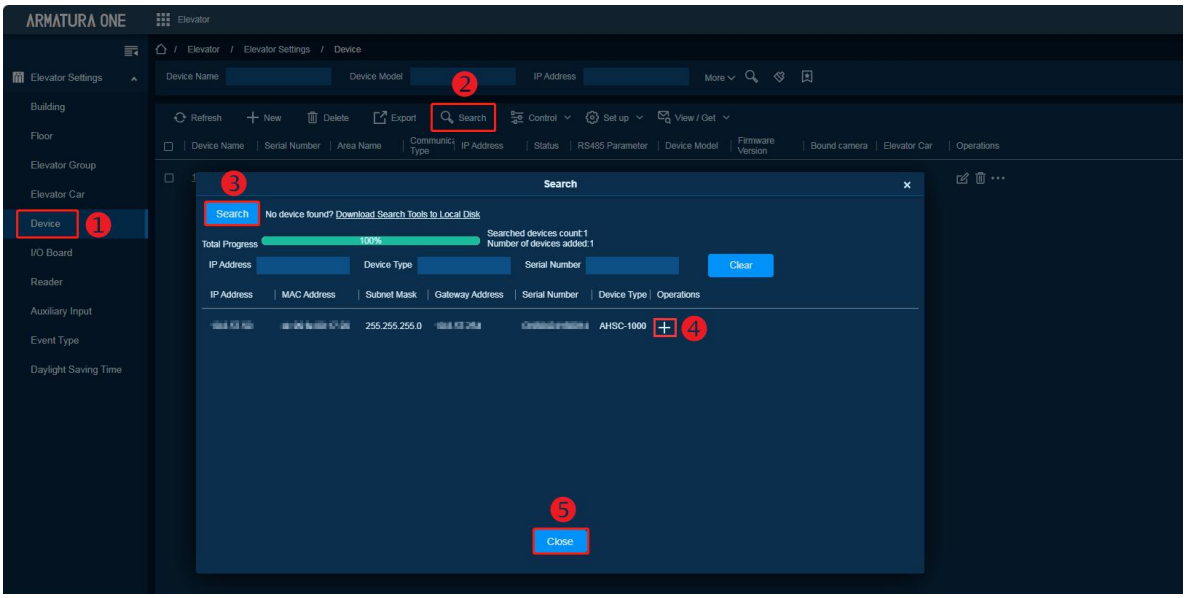
4. After adding, you can view the generated elevator car on the [**Elevator** > **Elevator Settings** > **Elevator Car**] page.
5. However, the auxiliary outputs have not yet been assigned to [**Elevator Car**], and it is currently not operational.



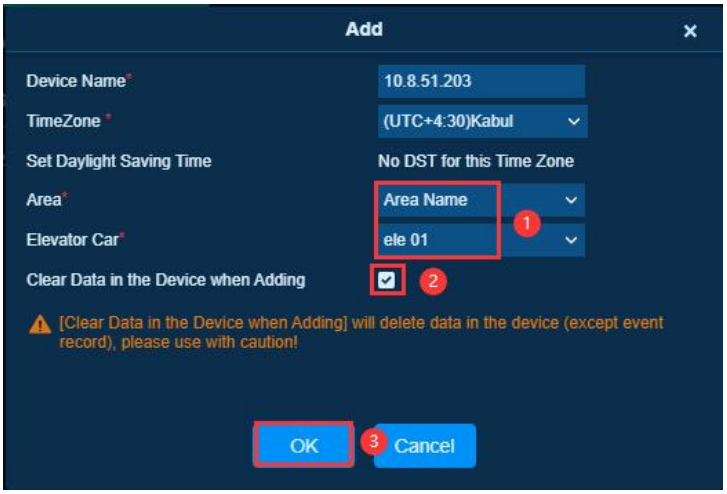
9.4.4 Add Elevator Controller

The following is an example of adding a **Easy Mode**.

1. Click **Elevator** > **Elevator Settings** > **Device** > **Search** to search for the device.
2. Click the [**Search**] button, and when the search is complete, click the [**+**] icon next to the target device to add it.



3. In the **Add** window that pops up, specify the area and elevator car for the device, and check [**Clear Data in the Device when Adding**].



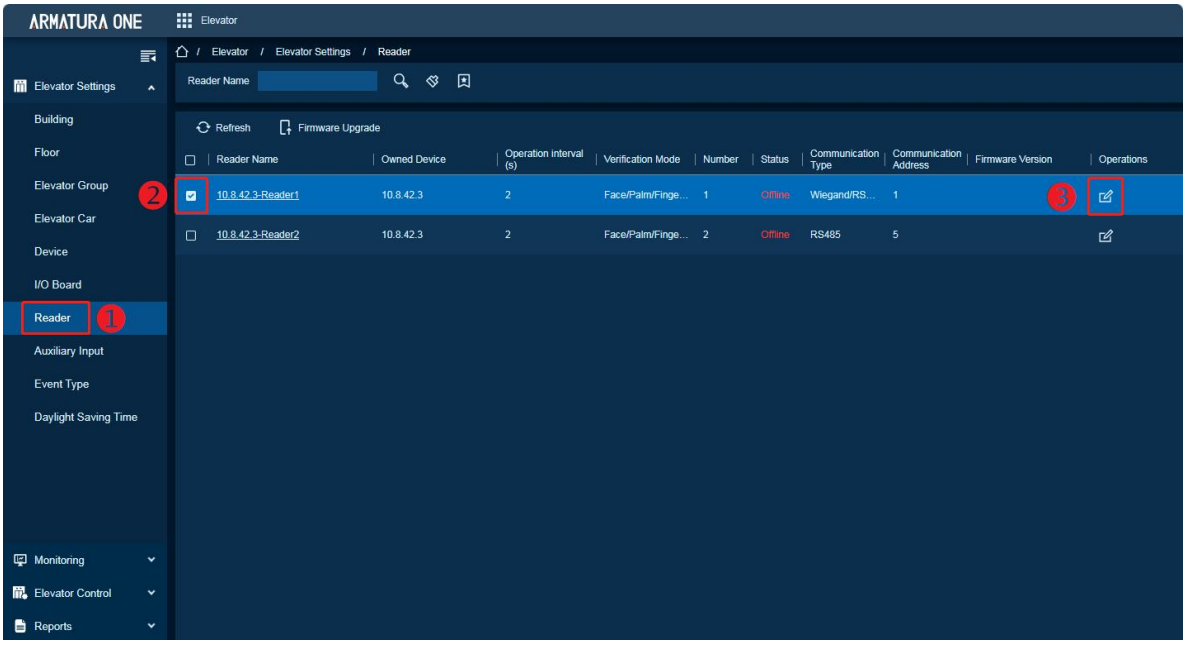
4. Finally, click **OK** to save and exit.

9.4.5 Configuring Reader Parameters

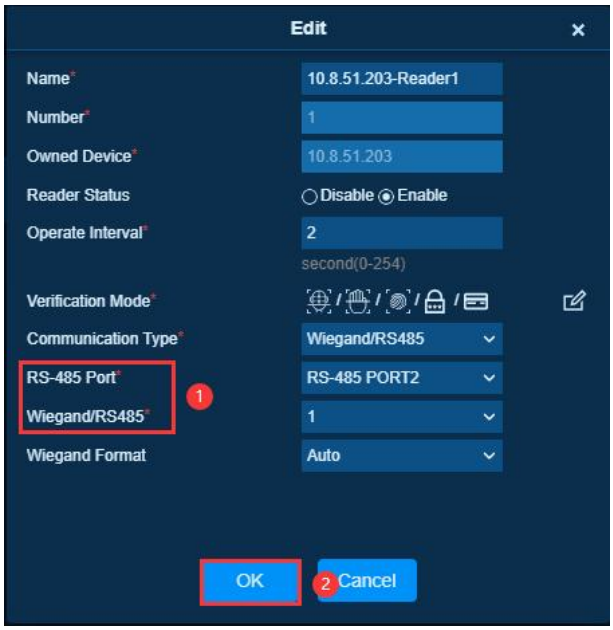
After adding devices, different controllers will automatically generate the corresponding number of readers: 2 for AHSC-1000 or AHDU-1160 controllers, 4 for AHDU-1260 controllers, and 8 for AHDU-1460 controllers.

You can view the readers on the [**Elevator** > **Elevator Settings** > **Reader**] page.

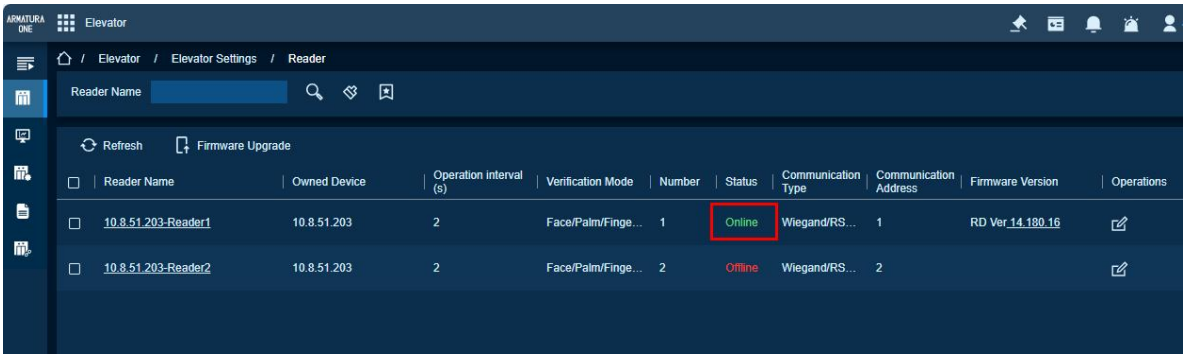
1. Select the reader and click the icon to modify the configuration information of the reader.



2. The images below are for reference only. Please make modifications according to the actual wiring and settings of the readers.

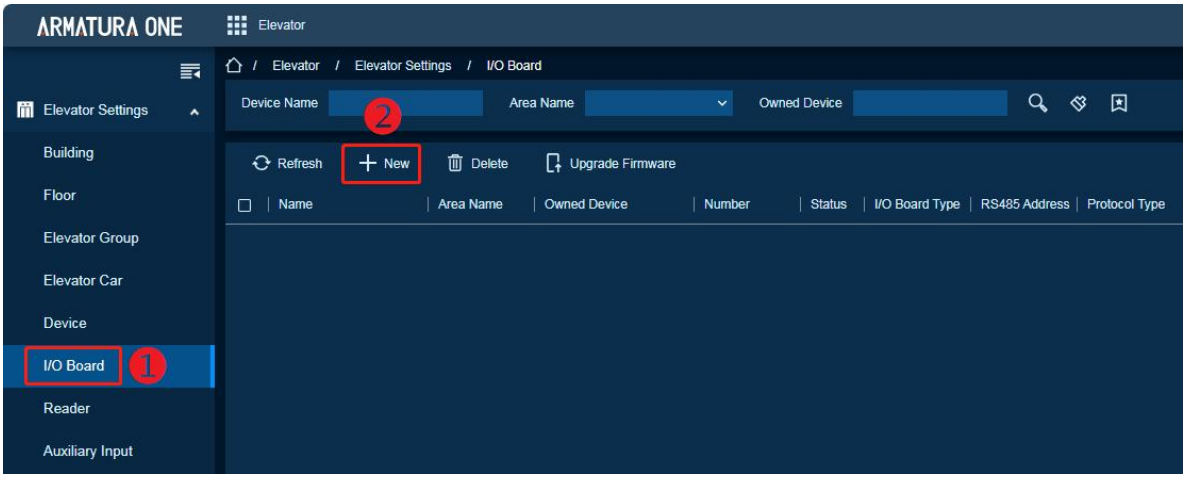


3. After modification, the status of the reader will be displayed as online.

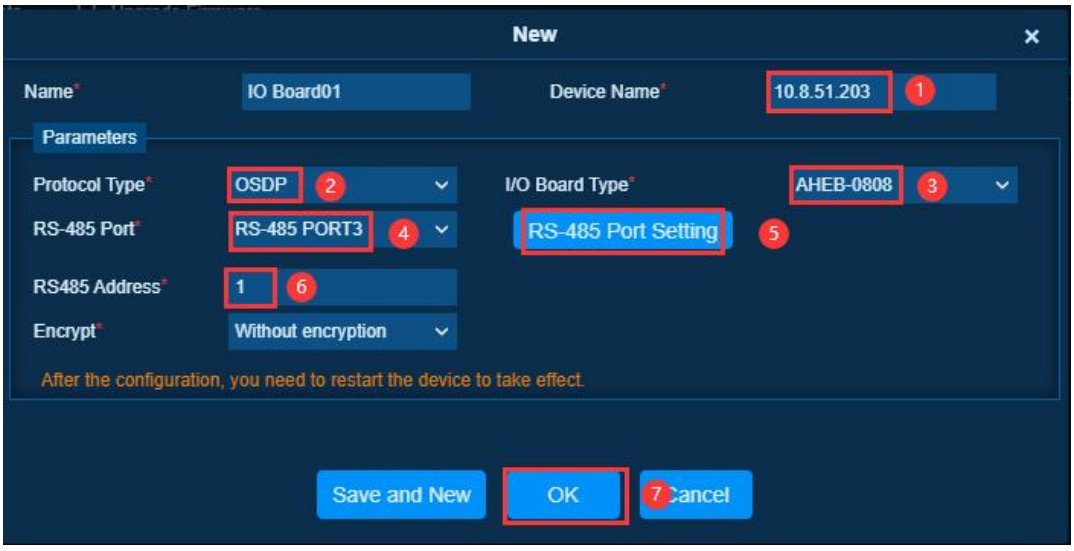


9.4.6 Add I/O Boards

1. Click on **Elevator** > **Elevator Settings** > **I/O Board** > **New** to add an I/O Boards.



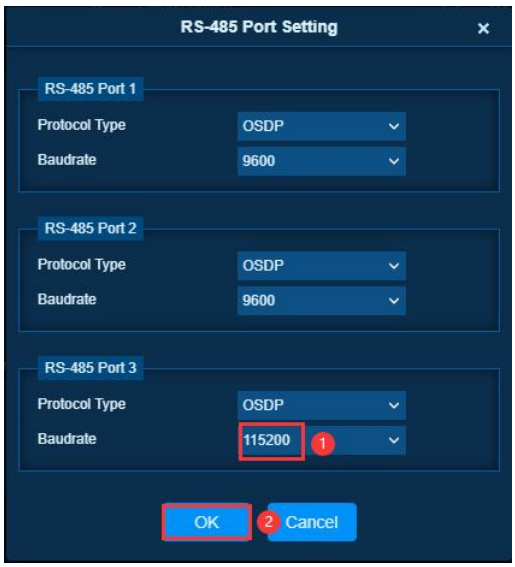
2. In the **New** window that pops up, name the I/O board and select the target controller.



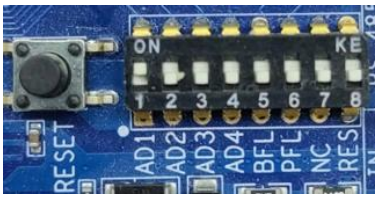
Key fields are as follows:

- **Protocol Type:** Select [OSDP].

- **I/O Board Type:** Select according to the actual model of the I/O board.
- **RS-485 Port:** Select according to the actual wiring port of the I/O board.
- **RS-485 Port Setting:** Please change the baudrate of the port connecting to the I/O board to 115200.



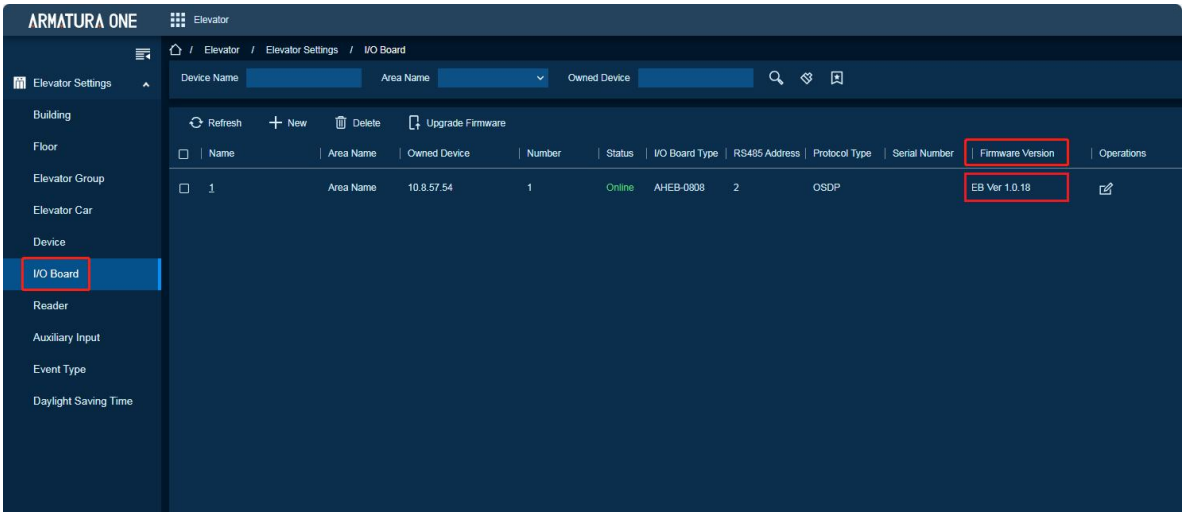
- ***RS-485 Address:*** *Please fill in according to the DIP switches on the I/O board. The DIP switches are in binary format and are read from left to right.*



3. After configuring the parameters, click **OK** to save and exit.

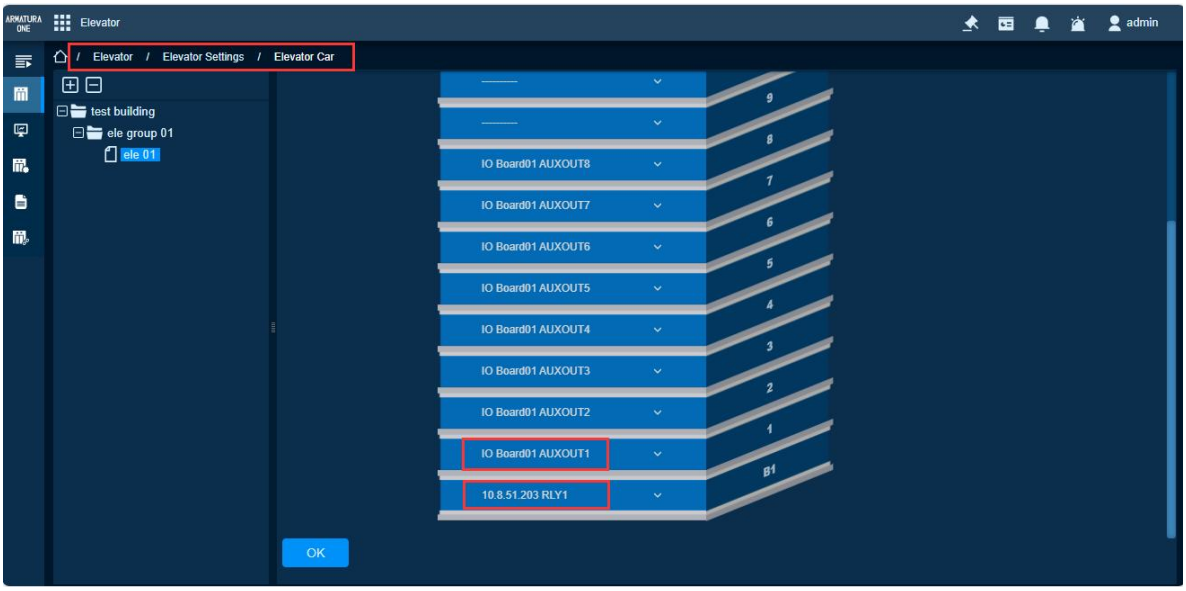
Remarks:

- *Please ensure that your I/O board's firmware is at least **version 1.0.18** to support the elevator control function. If the current version is below this requirement, please contact your local branch or the headquarters' technical support for assistance.*



9.4.7 Modifying Auxiliary Output Points for Floor Assignment

1. After successfully adding the elevator controller and I/O boards and bringing them online, the system will automatically assign all auxiliary output points to the respective floors.
2. You can navigate to the **Elevator** > **Elevator Settings** > **Elevator Car** page, and based on the actual wiring, click the icon on the right side of the floor to modify it to the correct auxiliary output point.



Notes：

- *The I/O board uses auxiliary output ports to connect to the elevator's button signal lines.*
- *the controller connects to the elevator's button signal line using relay ports instead of auxiliary outputs. The controller must be running the MCU firmware **version 6.3.2.5** or higher to utilize the onboard relay for floor control. If the controller is not updated to this version, floor control must be achieved through the auxiliary outputs of the I/O board.*

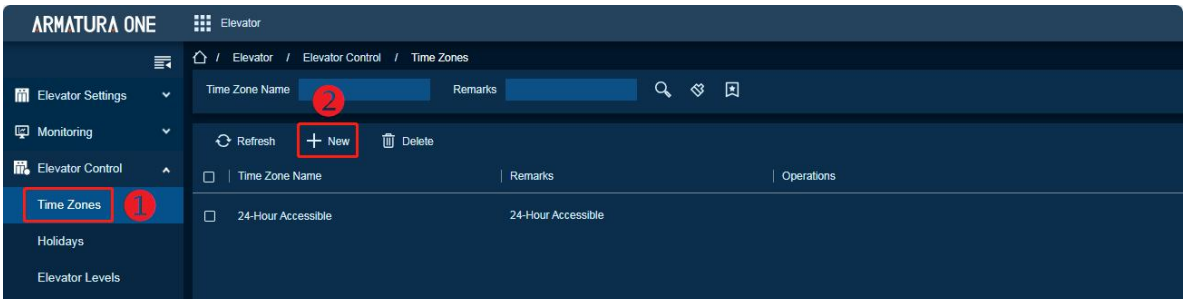
Should you require assistance, please contact the headquarters for technical support.

9.4.8 Add Time Zones and Elevator Levels

Add Time Zones

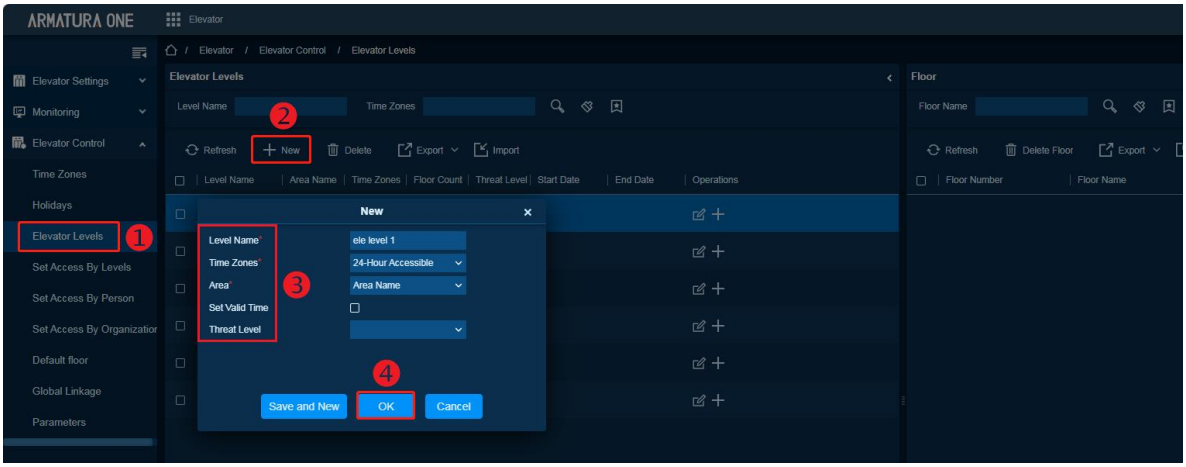
The system already has a default time zone named [**24-hour Accessible**], which can be used directly. You can add new time zones according to your needs.

1. Click **Elevator** > **Elevator Control** > **Time Zones** > **New** to add a time zone.

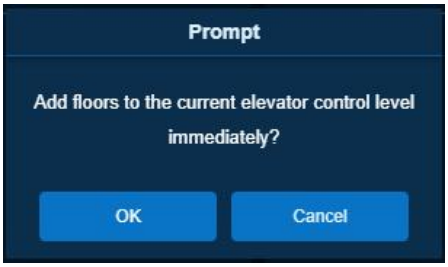


Add Elevator Levels

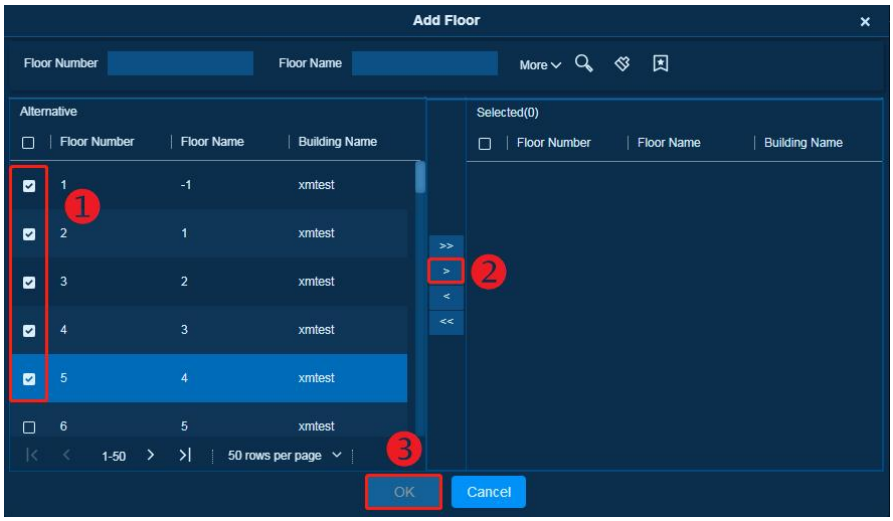
1. Click **Elevator** > **Elevator Control** > **Elevator Levels** > **New** to add an elevator level.
2. In the **New** window that pops up, name the elevator layer, select the area, and perform other actions.
3. Click the **OK** to save and exit.



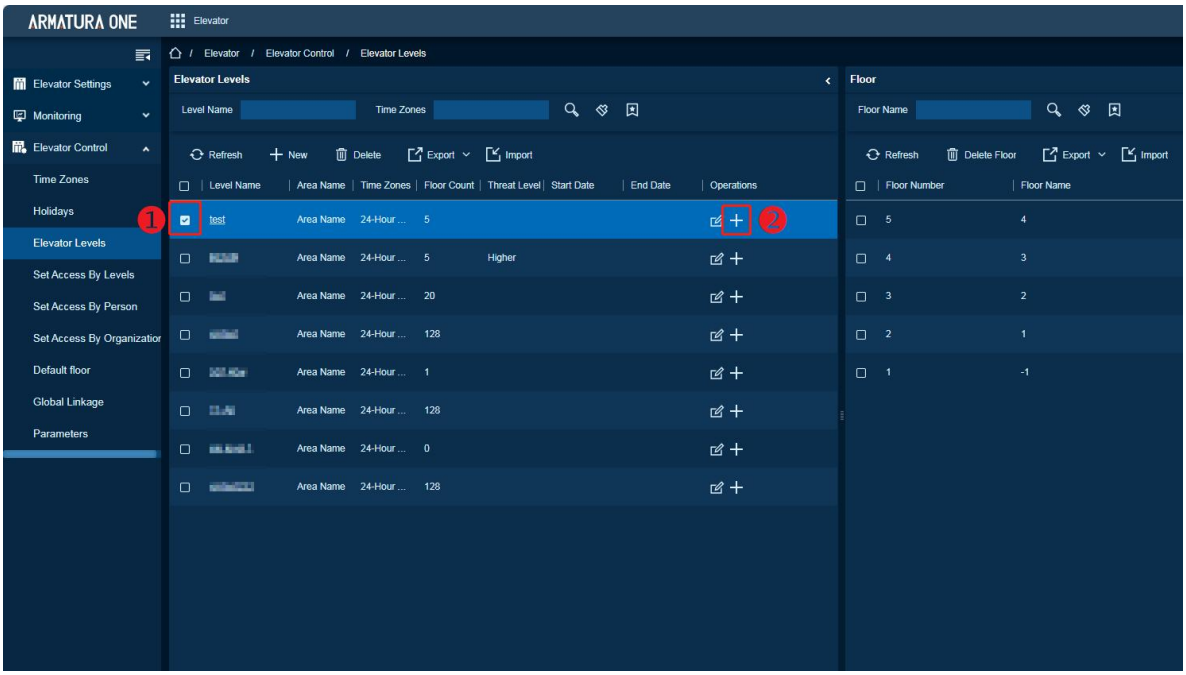
4. After adding the elevator level, the system will display the following prompt. Click **OK** to continue.



5. Select the floors you want to add to this level by checking the appropriate boxes, then click the > button to add them.

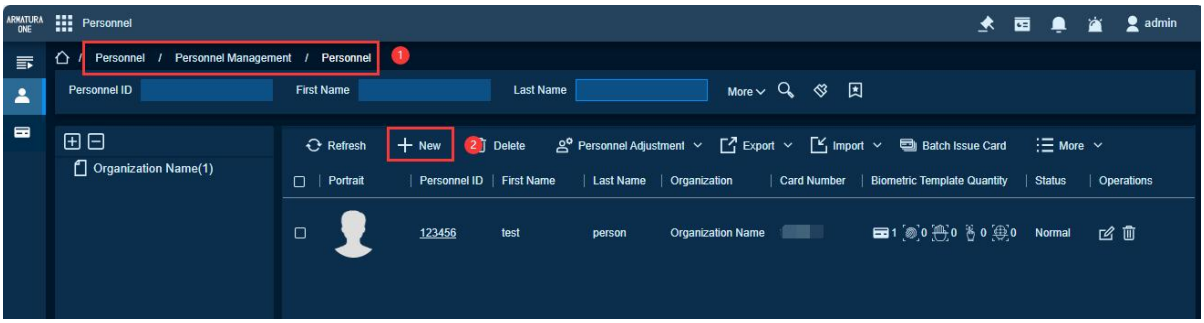


6. If you cancel the prompt, you can also select elevator level in the list and click the + icon after it, then select the floor you want to add to the elevator level.

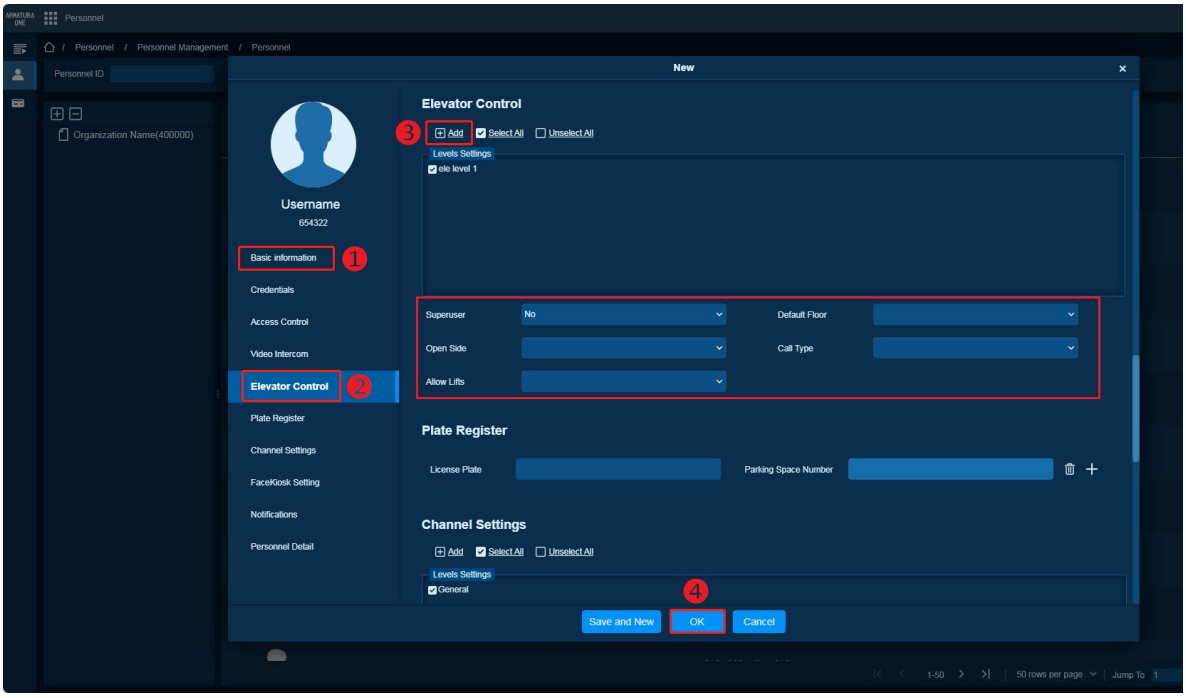


9.4.9 Adding Personnel and Setting up Elevator Control

1. Click **Personnel** > **Personnel Management** > **Personnel** > **New** to add new personnel.



2. In the **New** window that pops up, first fill in the basic information about the person.
3. Then click **Elevator Control** in the left menu and click **Add** to assign appropriate permissions to the person.
4. Click **OK** to save and exit when settings are complete.

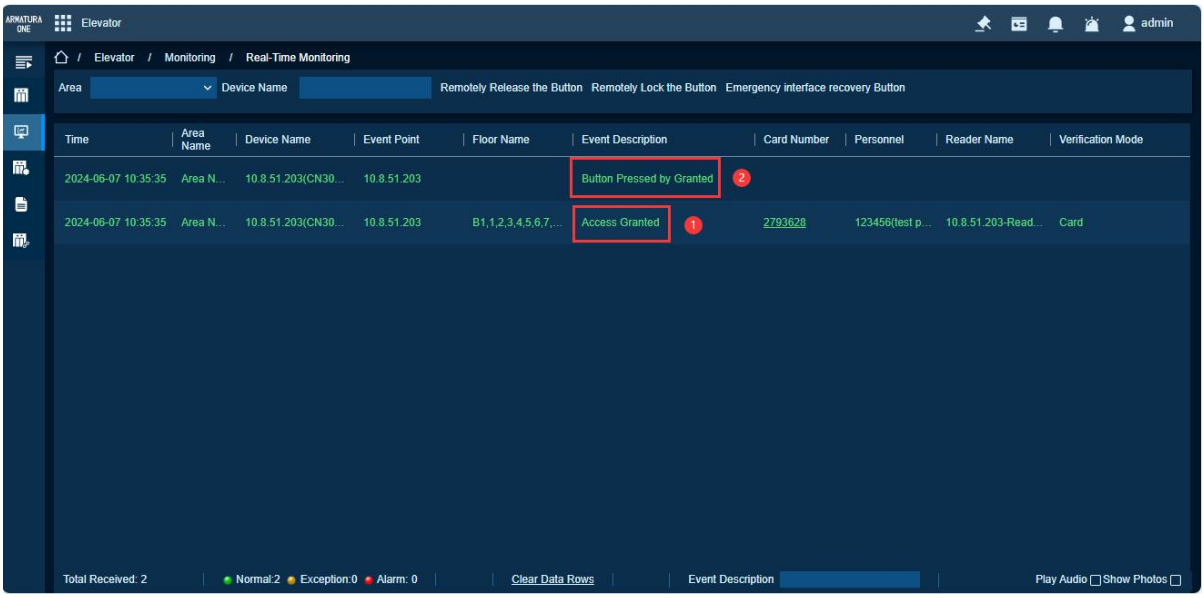


Notes:

- ***Superuser:*** *Has access to each floor.*
- ***Default Floor:*** *A building can only have one default floor. Only the AHEB-1616 or DCS elevator supports this feature; the AHEB-0808 and AHEB-1602 do not.*
- ***Open Side:*** *Do not operate, only DCS elevators support this feature.*
- ***Call Type:*** *Do not operate, only DCS elevators support this feature.*
- ***Allow Lifts:*** *Do not operate, only DCS elevators support this feature.*

9.5 Verify Elevator Control

1. After all configurations have been completed, you can use a card on the reader connected to the elevator controller for verification.
2. Once verified, the elevator system will illuminate the buttons for the floors the user has access to.
3. At the same time, an event record of "**Access Granted**" will receive on the software side. This can be viewed via the path [**Elevator**] > [**Monitoring**] > [**Real-Time Monitoring**].
4. The software will receive another event record "**Button Pressed by Granted**" when the user presses the button on the target floor.



Note:

- *The [**Button Pressed by Granted**] record can be accurately captured only when using the AHEB-1616 I/O board.*

10. P2P Function

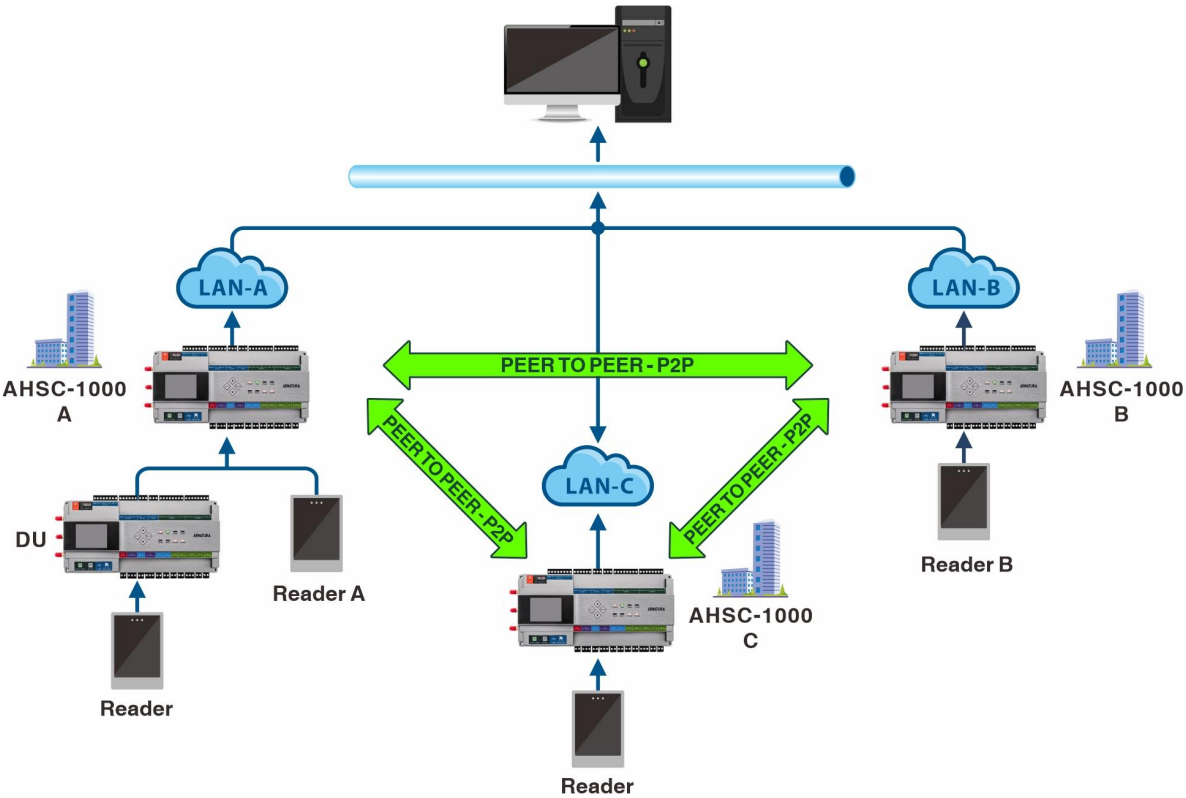
10.1 Functional Definition

P2P (Peer to Peer) function means that multiple controllers can directly establish communication links between them to exchange data and make business logic judgment through the data shared between controllers. For example, it can be used for global anti-submarine/global linkage/global interlocking and other business rules. The AHSC-1000 controller supports P2P function.

10.2 Application Scenario

Case: Global Anti-Passback + P2P Application

A building has three large entrances/exits on the first floor, each with a AHSC-1000 and a corresponding number of DUs and card readers. In this case, we can use a P2P solution to realize the entrance/exit anti-passback (Global Anti-Passback) between all the card readers. This is shown in the following diagram.



Notes：

- *When the client need to setting the anti-passback between Reader A and Reader B. The Controller A and Controller B need to setting the peer to peer with each other.*
- *The networks between controllers need to be interoperable in order to support peer-to-peer support.*

10.3 Parameter Configuration

This unit describes how to configure the parameters of P2P.

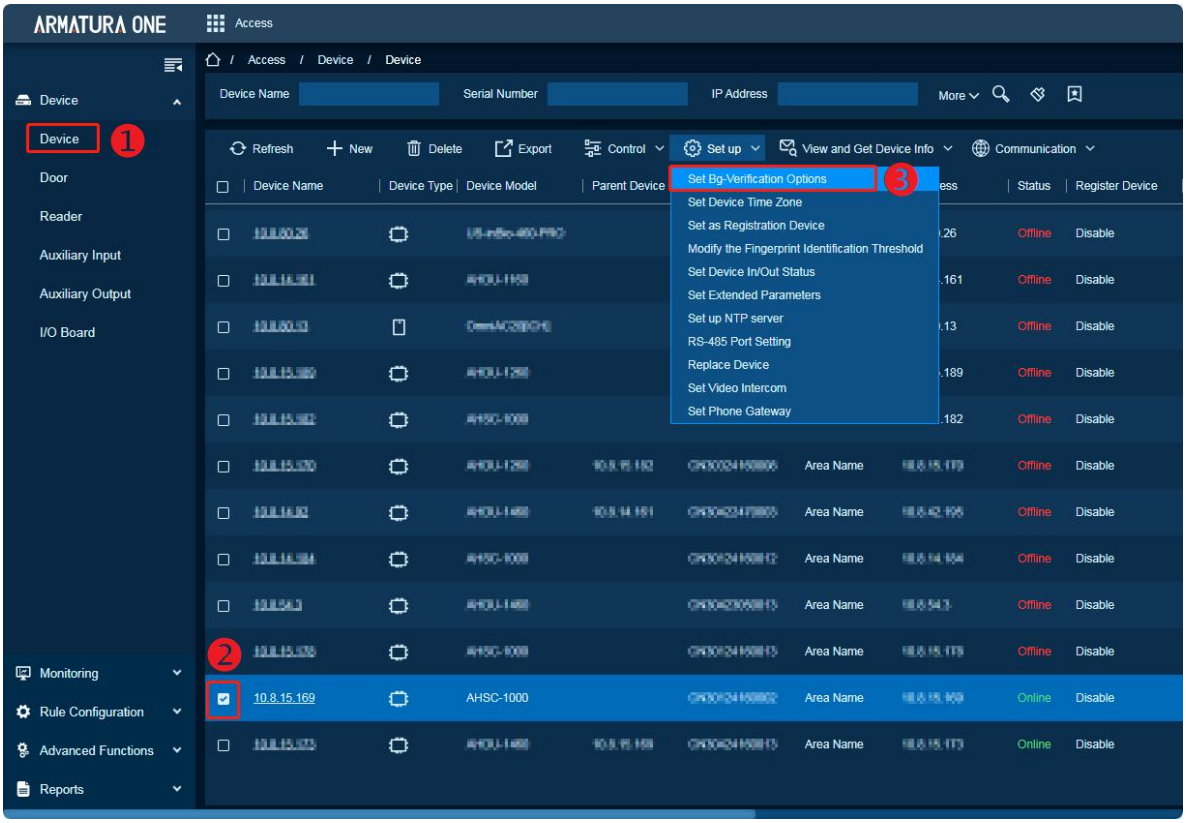
Remarks:

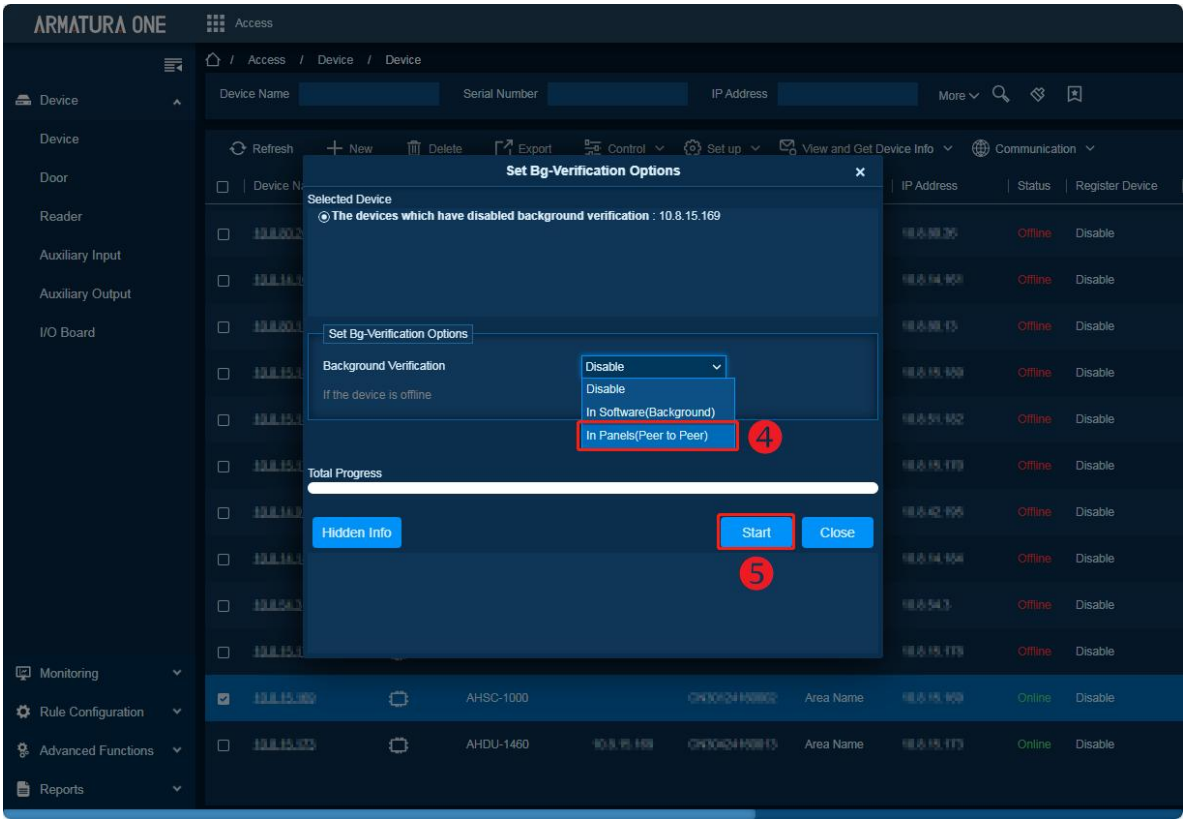
1. *In LAN, the IP addresses of the server (PC) and the controller must be in the same network segment when connecting to the ARMATURA One software.*
2. *Currently, only the **AHSC-1000** controller can support setting the P2P function.*
3. *P2P is composed of adding at least 2 AHSC-1000s.*
4. *Each Global Anti-Passback Rule can be associated with a maximum of six master controllers.*

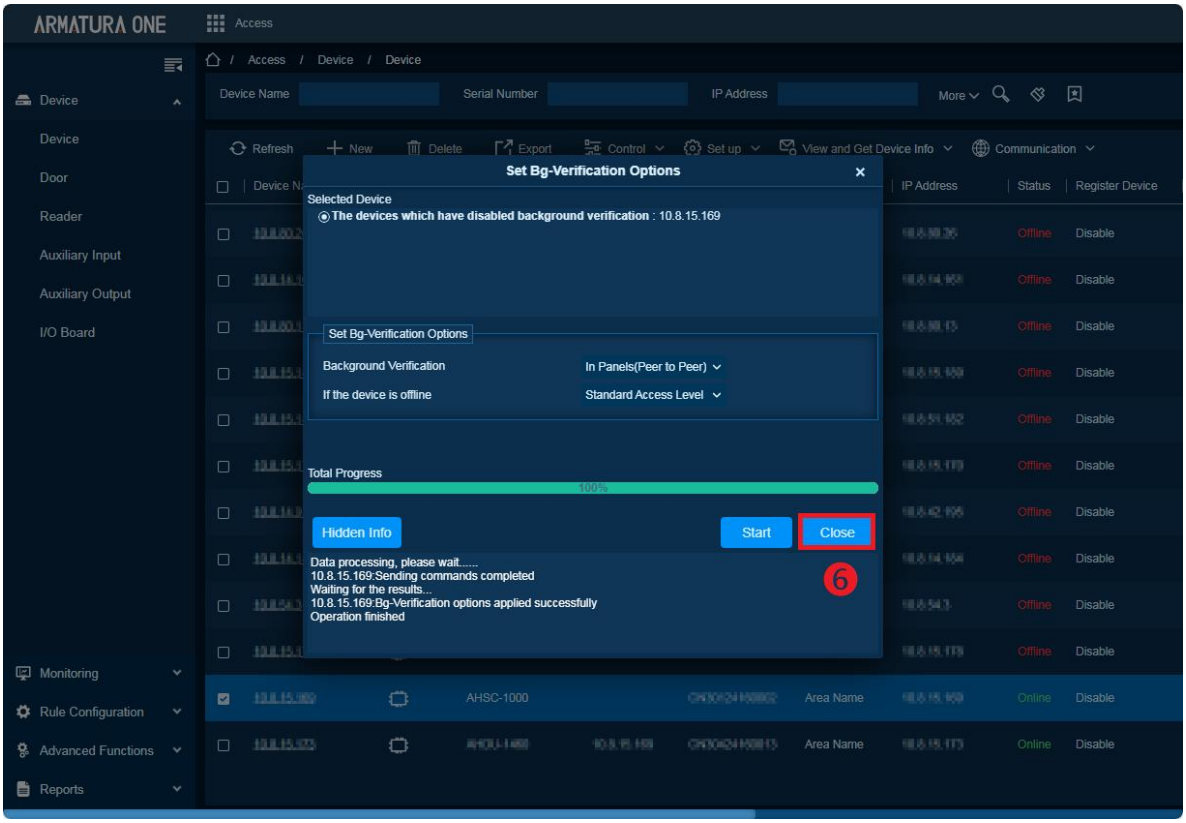
10.3.1 Setting the Background Verification Parameters

Log in to the ARMATURA One software and perform the following steps.

1. Add the controller to the software first, refer to 6.3 Add Device on the Software for details.
2. Click **Access > Device > Setup > Set Bg-Verification Options** to set the background verification parameters.
3. Then in the pop-up window, click **Background Verification** > **In Panels(Peer to Peer)** > **Start** to configure the parameters. Click **Close** to exit.

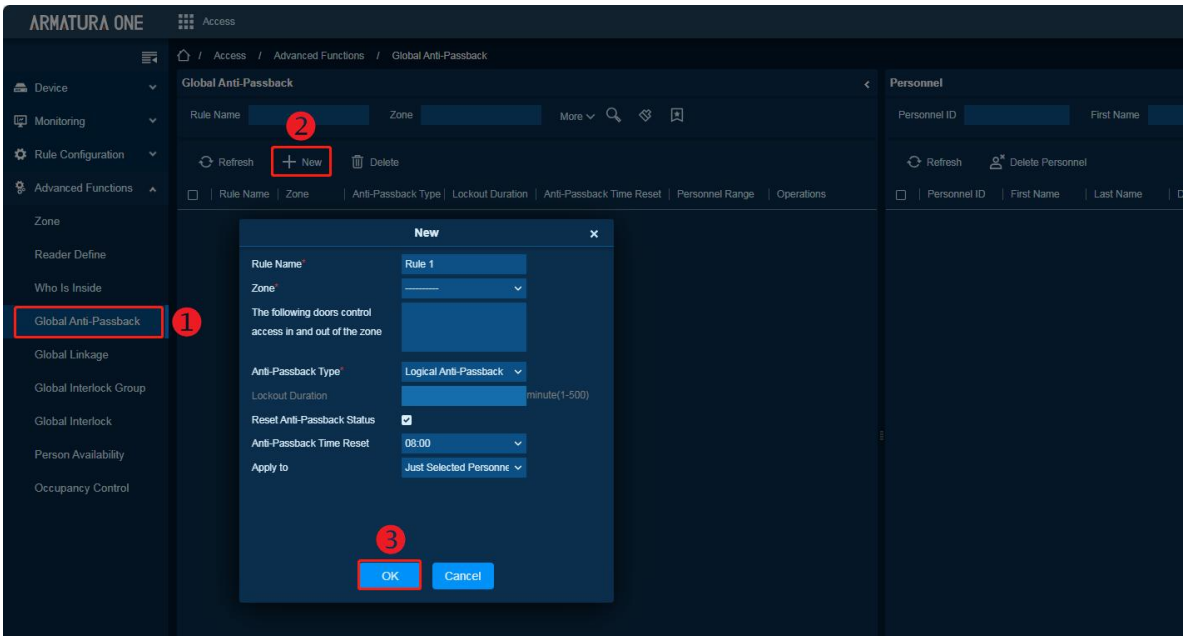






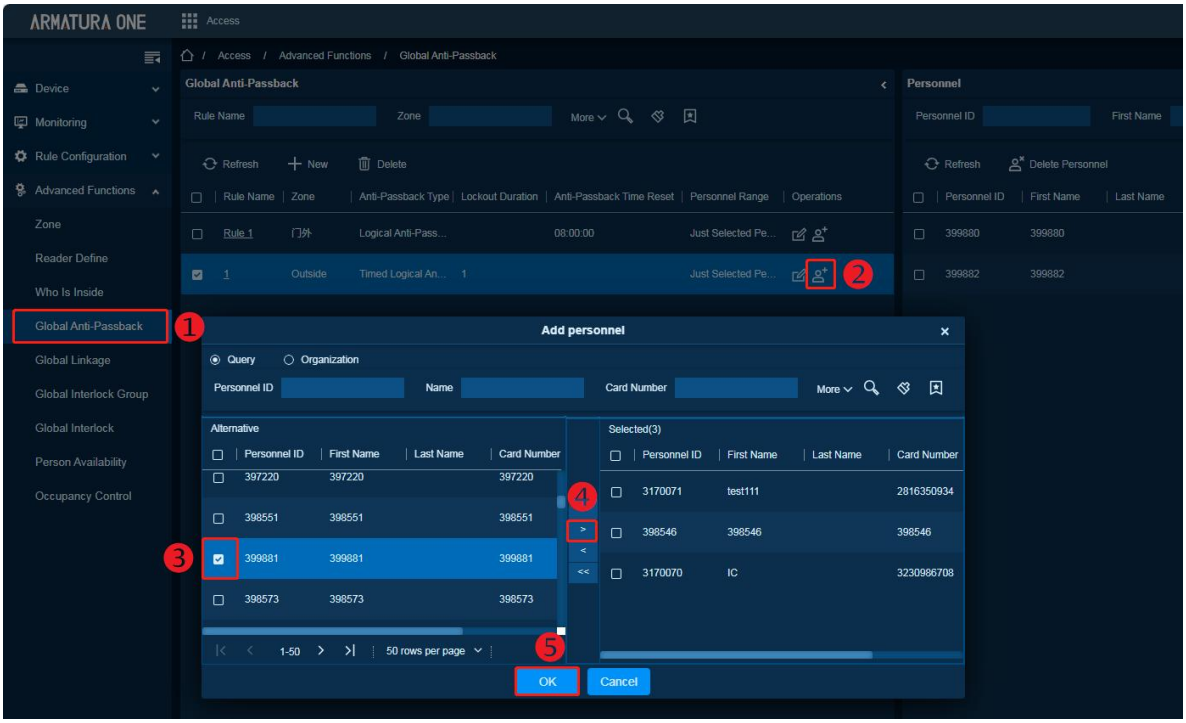
10.3.2 Creating the Global Anti-Passback Rules

1. Click **Access** > **Advanced Functions** > **Global Anti-Passback** > **New** to add a global anti-passback rule.



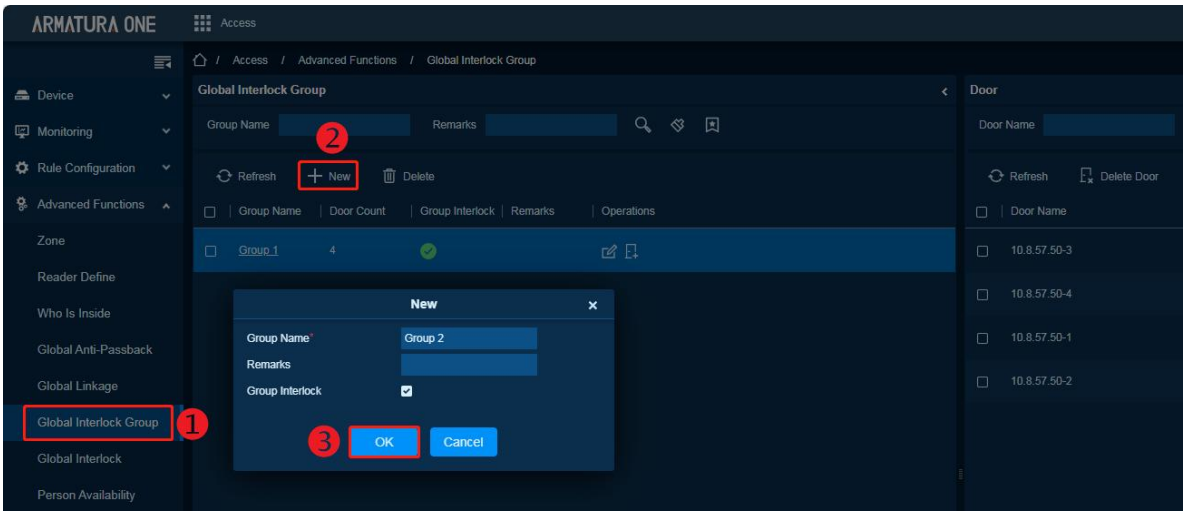
2. After setting the parameters, click **OK** to save and exit.

3. Once you are done adding rules, then add people to the rules. As shown in the figure below, select the global anti-passback rule that has been created, click the icon, and select the personnel to be added in the pop-up window. Click > to move the person into the option and then click **OK** to confirm.



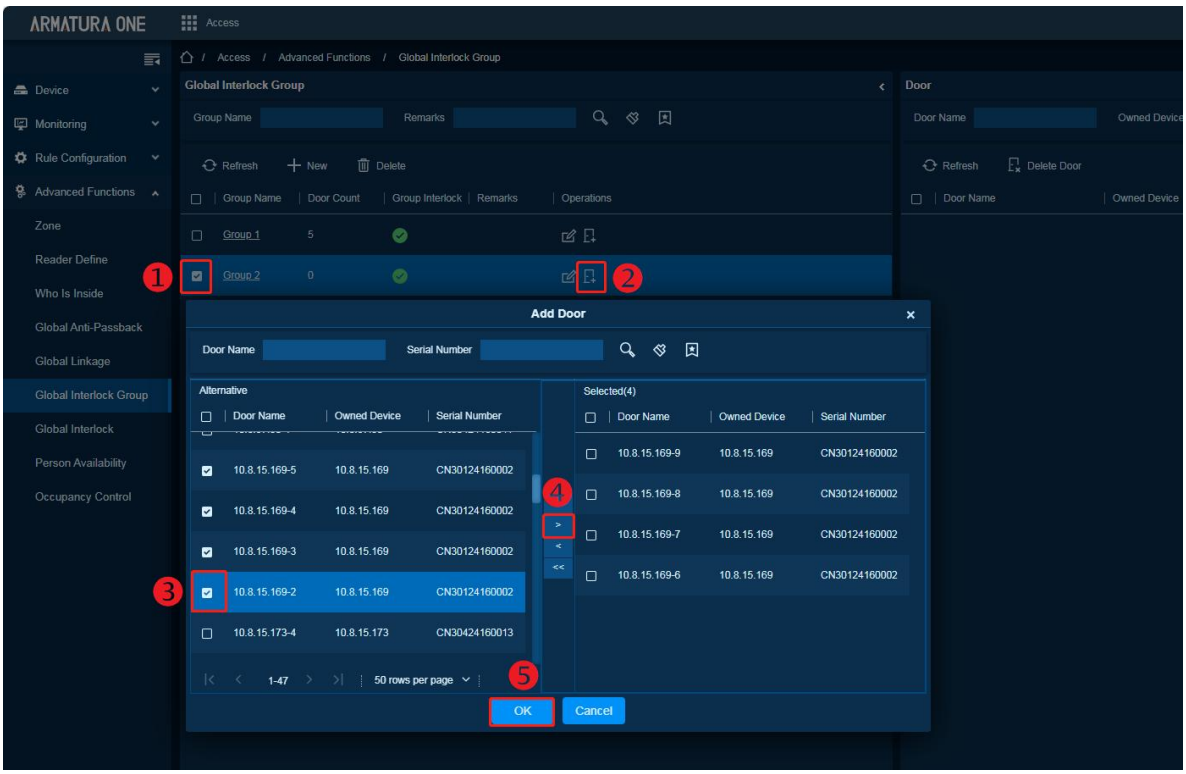
10.3.3 Creating the Global Interlock Group

1. Click **Access** > **Advanced Functions** > **Global Interlock Group** > **New** to add a global interlock group.

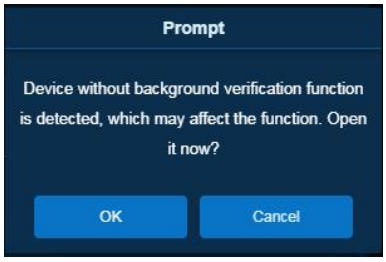


2. After setting the parameters, click **OK** to save and exit.

3. After adding the group, add the door to the group. As shown in the figure below, select the group and then click icon, and select the door to be added in the pop-up window. Click > to move the door into the option and then click **OK** to confirm.

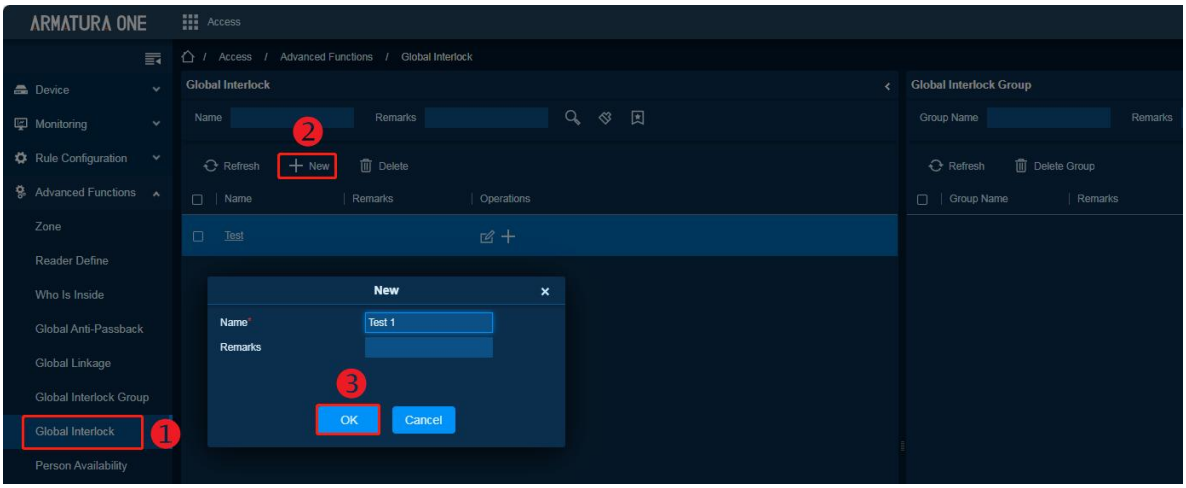


4. When it is detected that the device does not have the function of background verification enabled, the following prompt will pop up. Click **OK** and refer to 10.3.1 to set it.

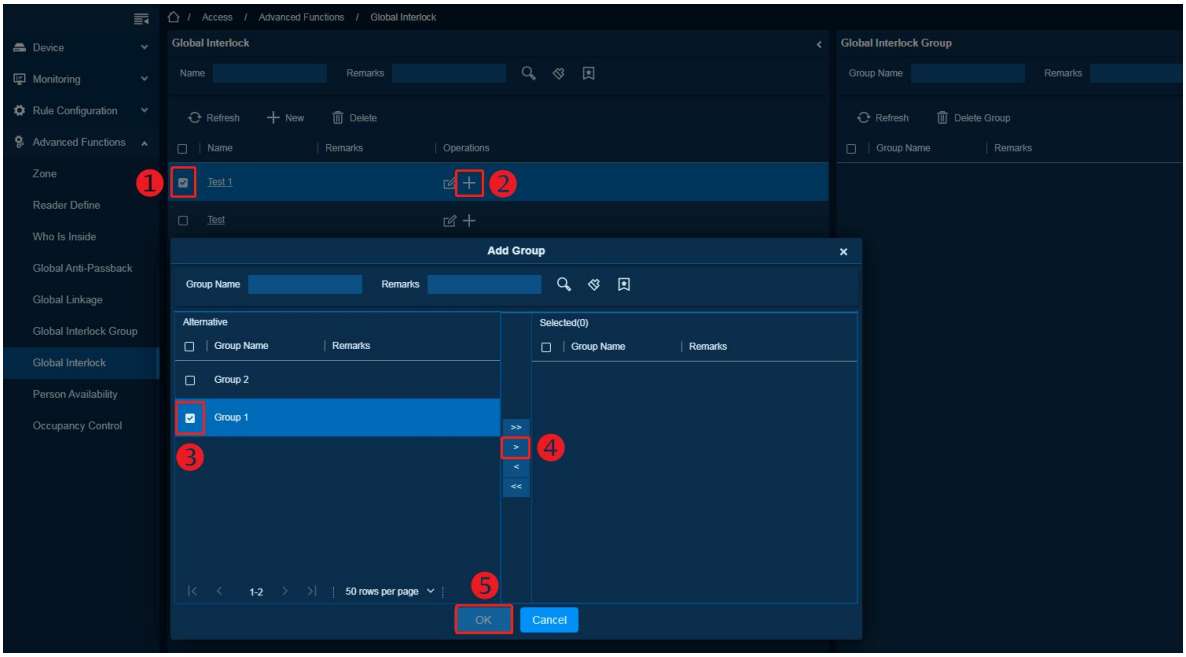


10.3.4 Creating the Global Interlock Rules

1. Click **Access** > **Advanced Functions** > **Global Interlock** > **New** to add a global interlock rule.



2. After setting the parameters, click **OK** to save and exit.
3. After adding the rule, add the group to the rule. As shown in the figure below, select the rule and then click + icon, and select the group to be added in the pop-up window. Click > to move the group into the option and then click **OK** to confirm.



11. FAQ

Q1: How to retrieve the IP address of the device if it is forgotten?

A: To view the device IP address on the controller screen, follow these steps: Click the **M/OK** button **> Network Info > LAN1/LAN2/WLAN**.

Q2: How to reset the network settings?

A: To reset the network settings, follow these steps on the controller screen:

1. Click the **M/OK** button.
2. Go to **Reset > Reset Network Settings > M/OK**.

Please be aware that all network settings will be reset to their default values.

The default IP address for the main NIC is **192.168.1.201**, and for the extended NIC, it is **192.168.2.202**.

Q3: How to reset the administrator password of the web server?

A: To restore the device to factory settings, you have two options:

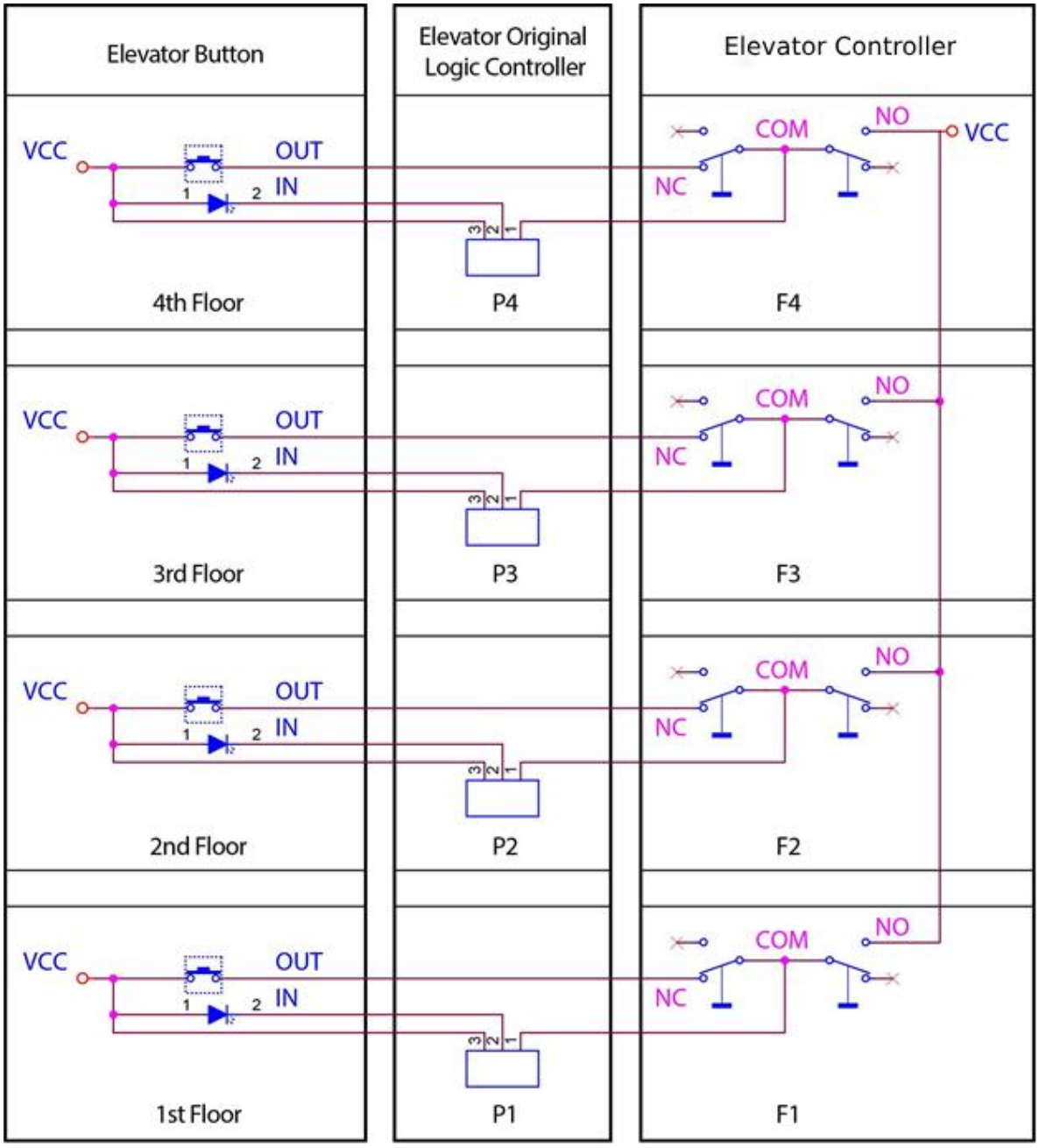
1. Click the **M/OK** button on the controller screen, then select **Reset > Factory Reset**.
2. Alternatively, you can press and hold the **Reset** button for more than **5** seconds to restore the factory settings.

12. Appendix

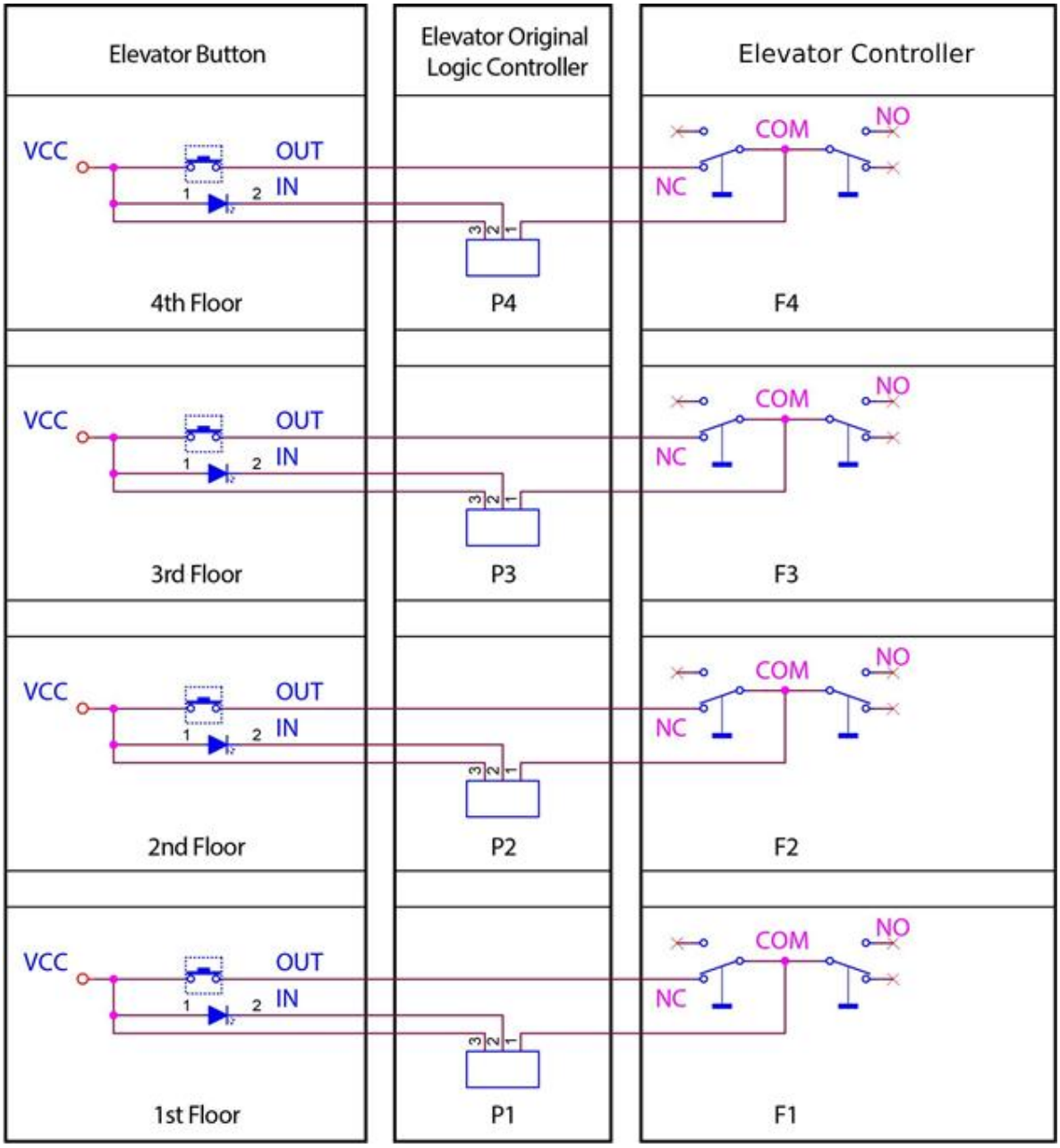
12.1 Appendix 1 Elevator Control and Elevator Button Wiring

12.1.1 Method 1 Common Anode Button Connection

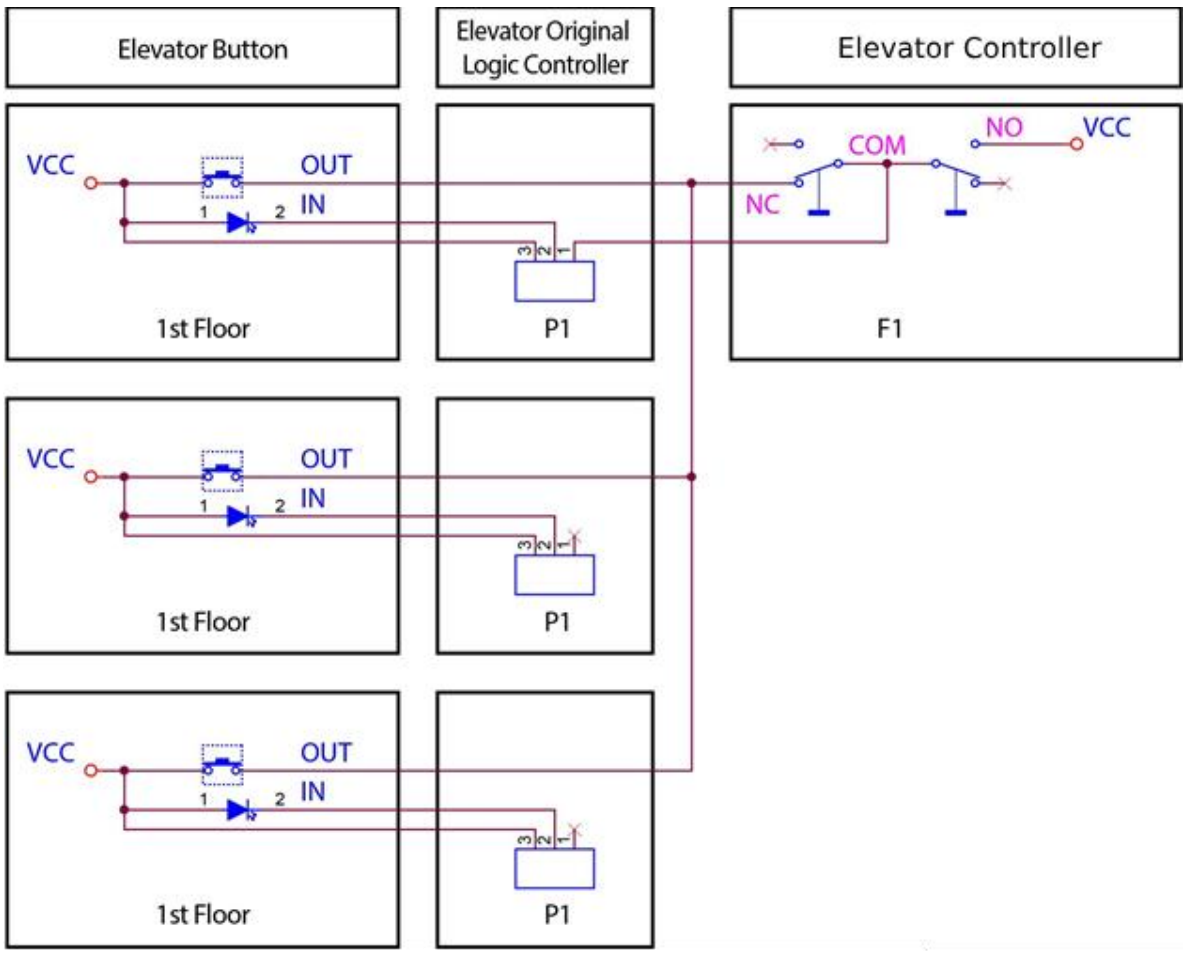
1. Supports for floor selection and direct floor selection.



2. Supports floor selection only.



3. Wiring method when there are multiple identical buttons on the same floor.

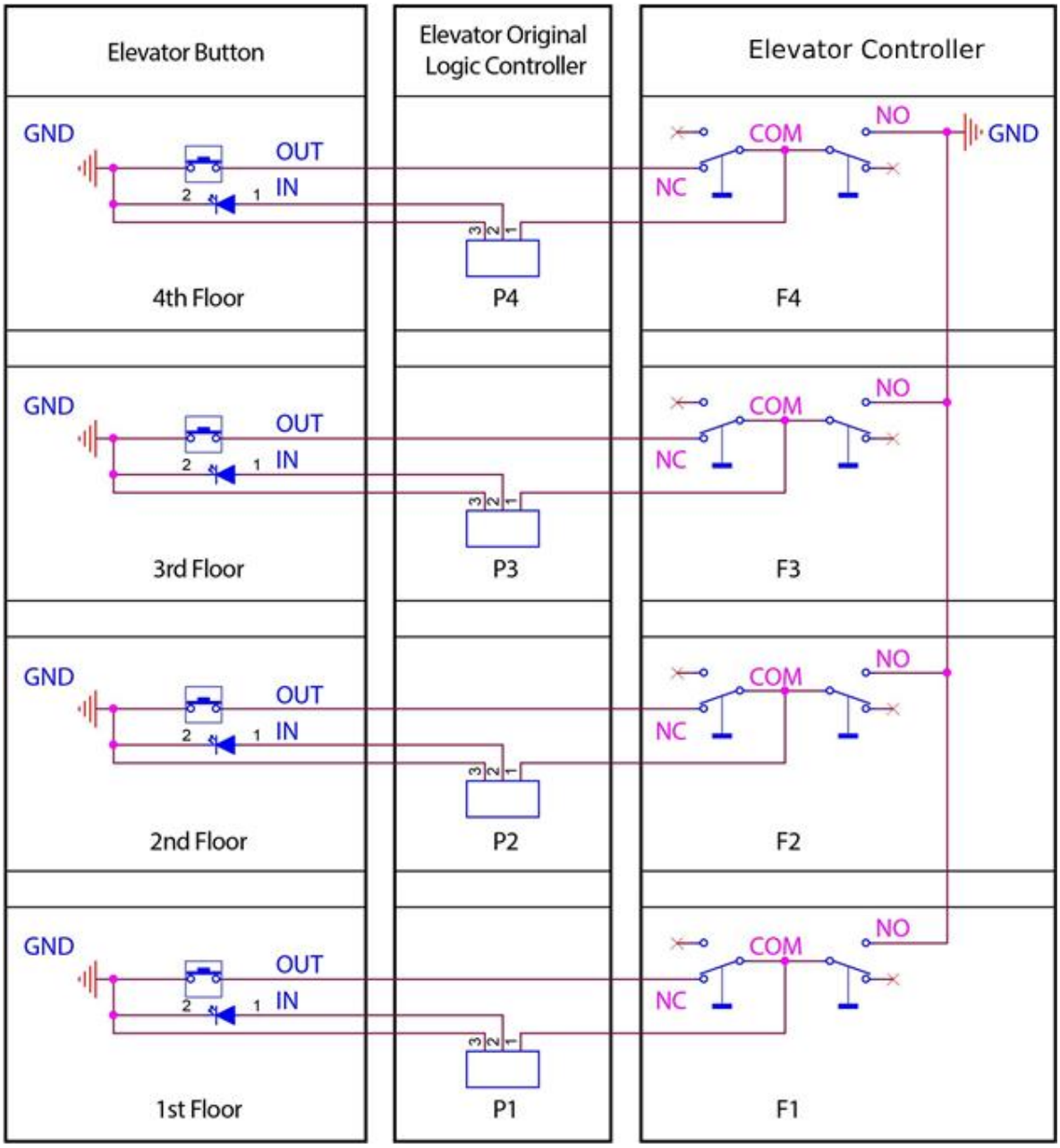


Note:

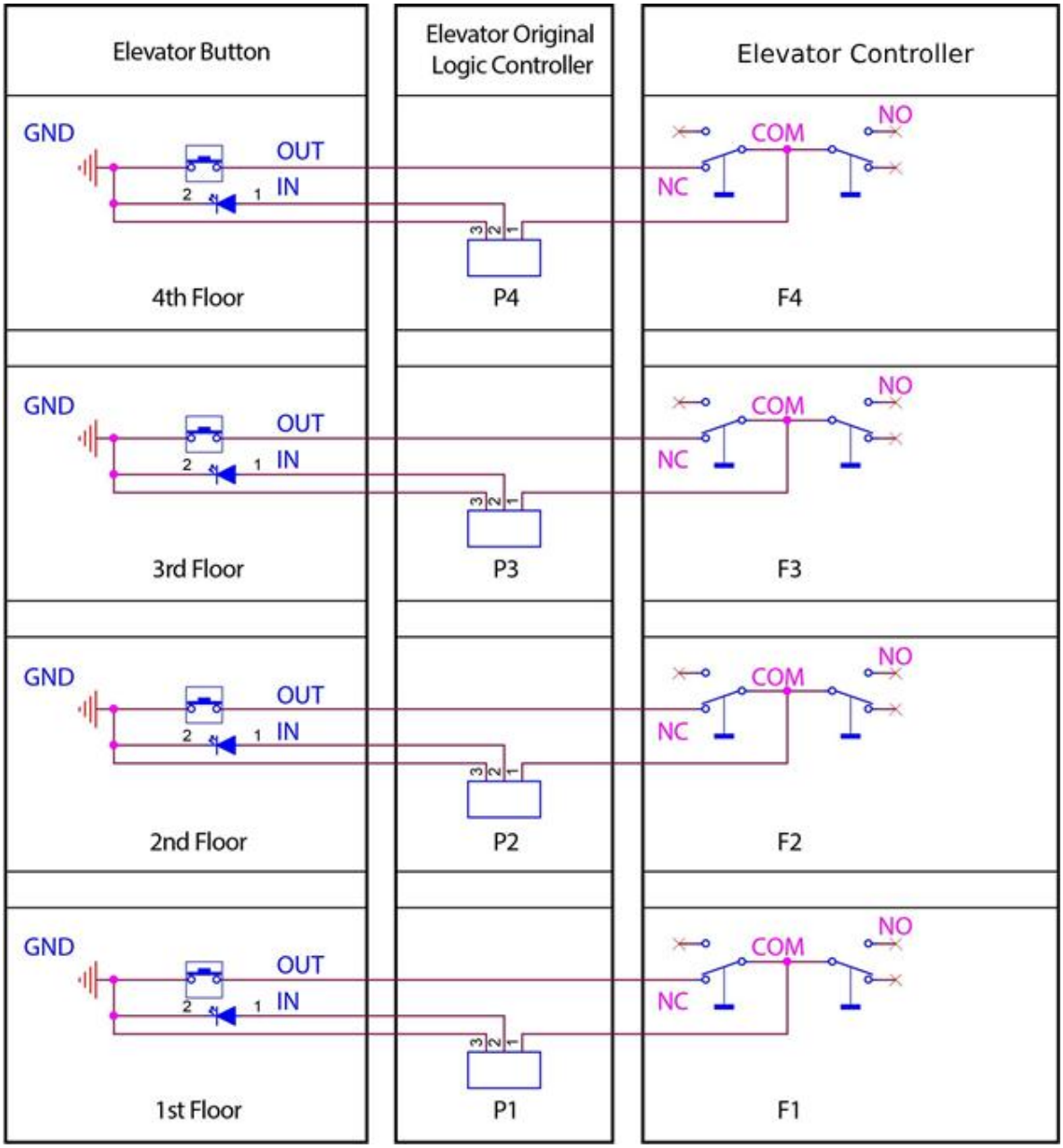
- *The following figure shows the wiring method for an elevator with three button boards, and this connection method avoids button cancellation exceptions.*

12.1.2 Method 2 Common Cathode Button Connection

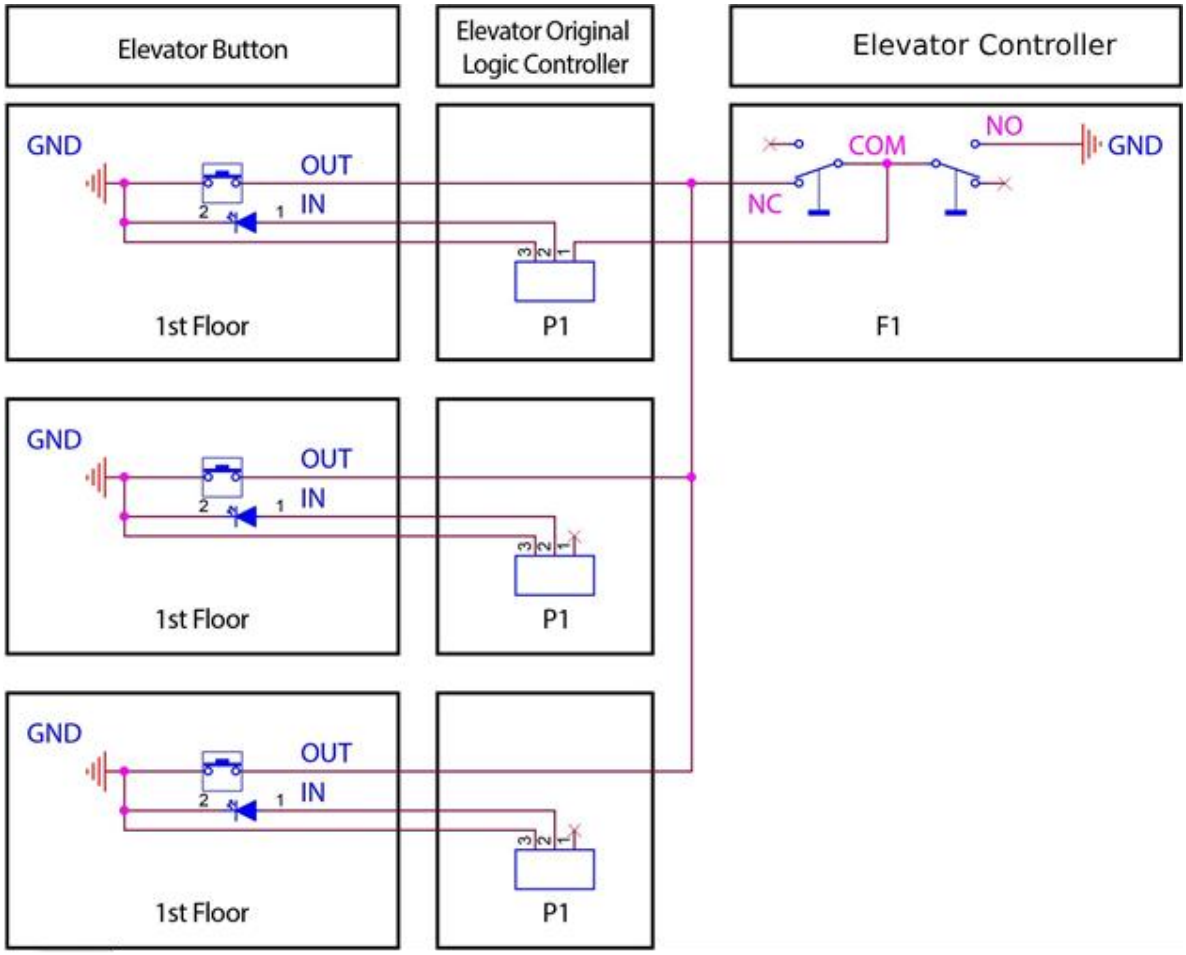
1. Supports for floor selection and direct floor selection.



2. Supports for floor selection and direct floor selection.



3. Wiring method when there are multiple identical buttons on the same floor.



Note：

- *The following figure shows the wiring method for an elevator with three button boards, and this connection method avoids button cancellation exceptions.*

12.2 Appendix 2 Privacy Policy

Notice:

To help you better use the products and services of Armatura LLC, hereinafter referred to as "we", "our", or "us", the smart service provider, we consistently collect your personal information. Since we understand the importance of your personal information, we took your privacy sincerely and we have formulated this privacy policy to protect your personal information. We have listed the privacy policies below to precisely understand the data and privacy protection measures related to our smart products and services.

Before using our products and services, please read carefully and understand all the rules and provisions of this Privacy Policy. If you do not agree to the relevant agreement or any of its terms, you must stop using our products and services.

I. Collected Information

To ensure the normal product operation and help the service improvement, we will collect the information voluntarily provided by you or provided as authorized by you during registration and use or generated as a result of your use of services.

1. **User Registration Information:** At your first registration, the feature template (**Fingerprint template/Face template/Palm template**) will be saved on the device according to the device type you have selected to verify the unique similarity between you and the User ID you have registered. You can optionally enter your Name and Code. The above information is necessary for you to use our products. If you do not provide such information, you cannot use some features of the product regularly.

2. **Product information:** According to the product model and your granted permission when you install and use our services, the related information of the product on which our services are used will be collected when the product is connected to the software, including the Product Model, Firmware Version Number, Product Serial Number, and Product Capacity Information. **When you connect your product to the software, please carefully read the privacy policy for the specific software.**

II. Product Security and Management

1. When you use our products for the first time, you shall set the Administrator privilege before performing specific operations. Otherwise, you will be frequently reminded to set the Administrator privilege when you enter the main menu interface. **If you still do not set the Administrator privilege after receiving the system prompt, you should be aware of the possible security risk (for example, the data may be manually modified).**

2. All the functions of displaying the biometric information are disabled in our products by default. You can choose Menu > System Settings to set whether to display the biometric information. If you enable these functions, we assume that you are aware of the personal privacy security risks specified in the privacy policy.

3. Only your user ID is displayed by default. You can set whether to display other user verification information (such as Name, Department, Photo, etc.) under the Administrator privilege. **If you choose to display such information, we assume that you are aware**

of the potential security risks (for example, your photo will be displayed on the device interface).

4. The camera function is disabled in our products by default. If you want to enable this function to take pictures of yourself for attendance recording or take pictures of strangers for access control, the product will enable the prompt tone of the camera. **Once you enable this function, we assume that you are aware of the potential security risks.**

5. All the data collected by our products is encrypted using the AES 256 algorithm. All the data uploaded by the Administrator to our products are automatically encrypted using the AES 256 algorithm and stored securely. If the Administrator downloads data from our products, we assume that you need to process the data and you have known the potential security risk. In such a case, you shall take the responsibility for storing the data. You shall know that some data cannot be downloaded for sake of data security.

6. All the personal information in our products can be queried, modified, or deleted. If you no longer use our products, please clear your personal data.

III. How we handle personal information of minors

Our products, website and services are mainly designed for adults. Without consent of parents or guardians, minors shall not create their own account. If you are a minor, it is recommended that you ask your parents or guardian to read this Policy carefully, and only use our services or information provided by us with consent of your parents or guardian.

We will only use or disclose personal information of minors collected with their parents' or guardians' consent if and to the extent that such use or disclosure is permitted by law or we have obtained their parents' or guardians' explicit consent, and such use or disclosure is for the purpose of protecting minors.

Upon noticing that we have collected personal information of minors without the prior consent from verifiable parents, we will delete such information as soon as possible.

IV. Others

You can visit www.armatura.us to learn more about how we collect, use, and securely store your personal information. To keep pace with the rapid development of technology, adjustment of business operations, and to cope with customer needs, we will constantly deliberate and optimize our privacy protection measures and policies. Welcome to visit our official website at any time to learn our latest privacy policy.

12.3 Appendix 3 Eco-friendly Operation

The product's "eco-friendly operational period" refers to the time during which this product will not discharge any toxic or hazardous substances when used in accordance with the prerequisites in this manual.

The eco-friendly operational period specified for this product does not include batteries or other components that are easily worn down and must be periodically replaced. The battery's eco-friendly operational period is 5 years.

Hazardous or Toxic substances and their quantities

Component Name	Hazardous/Toxic Substance/Element					
	Lead (Pb)	Mercury (Hg)	Cadmium (Cd)	Hexavalent Chromium (Cr6+)	Polybrominated Biphenyls (PBB)	Polybrominated Diphenyl Ethers (PBDE)
Chip Resistor	×	○	○	○	○	○
Chip Capacitor	×	○	○	○	○	○
Chip Inductor	×	○	○	○	○	○
Diode	×	○	○	○	○	○
ESD component	×	○	○	○	○	○
Buzzer	×	○	○	○	○	○
Adapter	×	○	○	○	○	○
Screws	○	○	○	×	○	○

○ indicates that the total amount of toxic content in all the homogeneous materials is below the limit as specified in SJ/T 11363—2006.

× indicates that the total amount of toxic content in all the homogeneous materials exceeds the limit as specified in SJ/T 11363—2006.

Note: 80% of this product's components are manufactured using non-toxic and eco-friendly materials. The components which contain toxins or harmful elements are included due to the current economic or technical limitations which prevent their replacement with non-toxic materials or elements.

12.4 Appendix 4 Attachment

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-- Reorient or relocate the receiving antenna.
-- Increase the separation between the equipment and receiver.
-- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
-- Consult the dealer or an experienced radio/TV technician for help.

Caution: Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Supplier's Declaration of Conformity

Unique Identifier

Trade Name: ARMATURA

Model No.: AHSC-1000, AHDU-1160, AHDU-1260, AHDU-1460, AHDU-1860, AHDU-11660; AHEB-0808, AHEB-1602,AHEB-1616; EP10C, EP20, EP30CF, VG10,VG20,FT10CMQ.EP20/VG10/VG20 may be followed by C/CK/CQ/CKQ. All the readers may be followed by [LF]/[HF]/[LHF]/[NI]/[NP]/[NO]/[DF]/[SFMH]/[IDL]/[ICH]/[RNI]/[RNP]/[RNPL] /[NIH] /[NISH] /[NPL] /[NPSL] /[MNO]/[MNP] /[MNPSL], etc.

Responsible Party – U.S. Contact Information

US Company Name: Armatura LLC.

Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005 USA

Telephone number or internet contact information: 678-831-3345

"Hereby, Armatura LLC declares that this Product is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.

The full text of the EU declaration of conformity is available at the following internet address: www.Armatura.us

The functions of Wireless Access Systems including Radio Local Area Networks(WAS/RLANs) within the band 5150-5350 MHz for this device are restricted to indoor use only within all European Union countries (BE/BG/CZ/DK/DE/EE/IE/EL/ES/FR/HR/ IT/CY/LV/LT/LU/HU/MT/NL/AT/PL/PT/RO/SI/SK/FI/SE/TR/N O/CH/IS/LI/UK(NI)

Customer: ZKTECO EUROPE SL

Customer Address: Crta.de Fuencarral 44. Edificio 1. Planta 2.28108, Alcobendas.

Madrid.SPAIN

12.5 Appendix 5 Risk Level - Grade 4

Requirement	Indication/Display	Alert	Logging	Remarks
Access point interface requirement				
Provide access control for entry into a protected (controlled) area				
Provide access control for exit from a protected (controlled) area				
Hard anti-passback				
Global anti-passback				
Anti-passback override/disabling				
Timed anti-passback				
Access granted conditional upon effective/expiry date				
Access granted conditional upon credential validity (blocked, suspended, invalid)				
Dual access (two-person access)				
Access point/ status shall be monitored				
Access point open time shall be configurable per portal				
Digital input signals (i.e. other than communication signals) with an active period exceeding 400 ms shall be processed				

Indication and annunciation requirements				
Visual and/or audible indication required when access is granted	√			
Visual and/or audible indication required when access is denied	√			
Visual and/or audible indication is required for the last time period (pre-alert time) of the maximum permitted portal open time if portal remaining open, to warn user(s) that the portal open time is running out. To cease when the portal is closed. Pre-alert time shall be system wide defined or configurable portal by porta (recommenced default: 10 seconds)	√			
Logging is required when access is granted			√	
Visual annunciation, alert and logging required for duress conditions	√	√	√	
Visual annunciation. alert and logging required for denial of access due to an attempt to use a token with expired validity	√	√	√	
Visual annunciation, alert and logging required for denial of access due to a configurable number of attempts to use a valid teken with invalid memorized information. Where the number of attempts is not configurable it shall be limited to 5	√	√	√	
Visual indication of access points alerts on the floor plan of the controlled areas	√			
Instructions shall be displayed following alerts	√			
Transactions			√	
Visual annunciation and logging for portal open status following access gramed. It may be configurable by portal in accordance with the grade requirement.	√		√	
Visual annunciation, alert and logging for portal remain closed status following access granted. It may be configurable by portal in accordarce with the grade requirement	√	√	√	
Access denied. It may be configurable by portal in accordance with the graderequirement	√	√	√	
Cause of access denial. It may be configurable by portal and/or cause of denial in accordance with the grade regurement	√	√	√	
Scheduled or manual portal status change			√	
Primary power failure	√	√	√	
Primary power restoration	√		√	

Standby power supply trouble condition (low battery voltage level and no battery present)	√	√	√	
Entering and leaving configuration mode	√		√	
Loss of communication between access control unit and monitoring console	√	√	√	
Roll call	√		√	
Portal closed following portal forced open or portal opened too long	√		√	
AI events shall be identified by type, location, time and date of occurrence	√		√	
Alerts shall contain an indication of their respective priority level if the system allows assigning of such priority levels	√		√	
Concurrently received alerts shall be displayed by order of priority if the system allows assigning of such priority levels	√			
Tamper detection	√	√	√	
Portal forced open	√	√	√	
Visual annunciation, alert and logging for expiry of portal allowed open time (portal opened too long)	√	√	√	
Card trace	√		√	
Reader trace	√		√	
Reader condition off-line	√	√	√	
Locking device abnormal status	√	√	√	
Annunciation of reaching the limit of 90 % from maximum logging capacity	√	√	√	
Maximum delay time for signals reaching the monitoring console (90 s, 45 s and 15 s)	√	√	√	15s
Maximum delay time for displaying text instructions following alert reaching the monitoring console (5 s)	√	√		
Maximum delay time for displaying image and graphics following alert reaching the monitoring console (6 s)	√	√		6s
System shall be capable of assigning priority levels to specific alert events	√			

Alerts received at the monitoring console require acknowledgement by the operator	√	√	√	
All operator initiated changes shall be logged with type, operator ID, time and date of the occurrence			√	
Operator comments to alerts shall be logged with operator ID, time and date of entering the comment. The specific alert covered by the comments shall be identified	√		√	
Accessing logged information for retrieving (e.g. displaying, printing, exporting) events shall be logged with operator ID. time and date of occurrence			√	
Minimum number of system events logging capacity on average per reader			√	1000
Recoginition requirement				
The built-in real time clock shall have an accuracy of + 10 seconds a week and be capable of adjusting to daylight saving time, leap year				
For systems with multpie interconnected control units, the clocks shall be synchronized with the master clock or other relable synchronization source, at least once every 24 h				
Synchronize the master clock of the system to the official time				
Real time clock shall be kept for the indicated minimum period of time in case of total power loss (except for loss of data retention battery)				120h
Minimum number of user access levels				64
Minimum number of configurable time periods				15
Minimum resolution for time within access level includes day of week, hour and minute of day				
Minimum resolution for time within access level includes day of month, month and year				
System shall be capable to handle a number of configurable days (e.g. statutory holidays, special business days and non-business days)				24
The system shall assign unique identity to each authorized user				
The system shall use biometrics alone or in combination with other recognition methods				
The system shall use token				

The system shall use memorized information and token				
Access shali be denied after each attempt to gain access using a valid token with invalid memorized information, and after a predetermined number of unsuccessful attempts the access rights for that token shall be suspended for a pre-set duration. The number of attempts can be configurable. Where it is not configurable the number of attempts shall be limited to 5				
For systems using recognition by memorized information combined with token or biometrics the memor zed information requires 4 digits minimum				
In normal mode of operation the system shall use complete token information (facility code and card number, or unique card number) for recognition				
Support for multiple facility codes if the system utilizes facility coding				
Tokens with coding system structure visible to unaided human eye shall not be used				
The token identity number readable on the token not to be a direct representation of the entire coding				
Duress signalling requirements				
Enabling of the duress functionality shall be configurable				
The duress alert at the monitoring console to be distinct from other alerts				
The operation of the duress initiating device shall not produce a signal which may be audible or visible at the location where the duress has been initiated				
Overriding requirements				
Single free access granting, single portal				
The electronic access control system shall not prohibit the free exit granted by other emergency systems (e.g. fire, environmental)				
System self-protection requirements				
Memory stored information (settings) shall be kept for the indicated minimum period of time in case of total power loss (except for loss of data retention battery)				2 wks

Following a total loss of power automatic restart of the access control system is required upon primary power source restoral				
If full functionality of the access control unit cannot be restored (data corrupted or lost) following the automatic restart a trouble condition shall be annunciated				
Means of access to the internal elements of components of an access control system shall require the use of a tool				
Opening of the enclosure of the user interface intended to be installed outside of the controlled area or that could be accessible from outside the controlled area shall result in tamper detection if manipulation of the internal elements can cause an access granted condition. The tamper detection shall occur before the tamper mechanism can be defeated				
Devices intended to be installed outside the controlled area or that could be accessible from outside the controlled area shall detect removal from mounting if that provides access to the internal elements and manipulation of these elements can cause an access granted condition				
The enclosures of the EACS components accessible from outside the controlled area shall meet the required IP and IK ratings				IP4X IK04
In case of loss of communication between the control unit(s) and the monitoring console, the control unit should be capable of storing and subsequently transmitting upon restoration of communications a minimum number of events per portal				1000
Communication between control unit and the EACS components shall be monitored. The loss of the communication for the indicated duration shall result in an alert at the monitoring console				2 min
System administration including configuration shall only be logically accessed with the use of valid credentials (e.g. password, token)				
There shall be separate access levels that categorize the ability of the operators to perform different functions in the system. Minimum number of logical access levels is:				4
The minimum number of required characters for logical access by memorized information only shall be as indicated (N=numeric/A=alphanumeric)				8A
If numeric codes are used for logical access by memorized information, sequential ascending or descending pass-code digits and use of same digit more than twice shall not be allowed				

Use of minimum 4-digit memorized information for logical access when combined with token or biometrics (to be system generated or by system administrator)				
Logical access credential can only be assigned by the system administrator				
Manufacturer's pre-set values for logical access shall be capable of being overwritten.				
After operational power loss minimum data retention time for logged events stored on the access control unit (due to loss of communication with monitoring console; shall be as indicated				120 h
Encryption required for communication signals between components of the EACS when using publicly shared networks (e.g. the Internet)				
The information stored on the token shall be protected against unauthorized modification or reproduction				
Either failure or restoration of the communication channel shall not result in the release of an access point				
Failure of communication with monitoring console shall not interrupt the access decision process.				
Processing rules stored in an access point reader shall not be visible to system users				
Light or sound keystroke keypad activation indicators shall not be a direct representation of actual codes, but shall be identical in pitch and duration				
Communication between readers and access control units shall support encryption with authentication				
The change in state (open, closed, tamper (open tamper or closed tamper)) of a digital input detection circuit shall be designed by the manufacturer to ensure that the tolerance for each circuit input state shall not overlap an adjacent state				
Data entry system validation. System shall provide annunciation when invalid data has been entered during configuration mode at the monitoring console				
Access to the configuration mode shall time out after a pre-set period of inactivity				
Power supply requirements				
The access control unit shall be provided with standby power source capable of operating the unit and its accessories under specified full load condition for the period of time indicated. (The loading conditions do not include the monitoring console or access point actuators)				4 h

Following an extended primary power source failure (system shutdown occurred) and restoration of power, rechargeable batteries shall be recharged to 80 % of rated capacity within 24 hours and 100 % of rated capacity within 72 hours				
Either loss of primary power source or restoration shall not adversely affect the normal operation of the system				
If standby power source is provided provisions shall be made to monitor for the following conditions: low voltage level and no battery present (single common annunciation for both conditions is acceptable)				

Current fuse specification: MST3.15A, 250V

Risk level: Grade 4

Environmental class: class II

ARMATURA

ARMATURA LLC www.armatura.us E-mail:sales@armatura.us