ARMATURA

User Manual

Armatura Horizon Controller
IP-Based Biometric Door Unit

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

Date: February 2023

Version: 1.8

Copyright © 2023 ARMATURA LLC. All rights reserved.

Without the prior written consent of ARMATURA LLC, no portion of this manual can be copied or forwarded in any way or form. All parts of this manual belong to ARMATURA LLC and its subsidiaries (hereinafter the "Company" or "Armatura").

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 is damaged.*
- *Any liquid or material spilled into the equipment.*
- *The equipment is wet or exposed to bad weather (rain, snow, etc.).*
- *If the equipment cannot work properly, even if it is operated as instructed, please be sure to adjust only the control components specified in the operating instructions. Incorrect adjustments on other control components may cause damage to the equipment; even the equipment may fail to operate permanently.*
- *The equipment falls, or its performance changes dramatically.*

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

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

10. **Power supply:** Operate the equipment with only the type of power supply indicated on the label. Contact the technician for any uncertainty about the type of power supply.

ⓘ 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 relay must match with the metal conduits; other wires can use PVC conduits, to prevent failure caused by rodent damage. The Control panel is designed with proper antistatic, lightning-proof, and leakage-proof functions, ensure its chassis and the AC ground wire are correctly connected and the AC ground wire is grounded physically.

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 welding job.

3. Do not detach or replace any control panel chip without permission, and an unpermitted 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 socket with any other large-current device.

6. It is preferable 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 advised to install control panels at places where maintenance is easy, like **a weak electric well**.

8. It is strongly recommended that the exposed part of any connection terminal should **not be longer than 0.16 inches (4mm)**, and specialized clamping tools may be used to avoid short-circuit or communication failure resulting from accidental contact with excessively exposed wires.

9. To save access control event records, export the data periodically from control panels.

10. Prepare countermeasures according to application scenarios for unexpected power failure, like **selecting power supply with UPS**.

11. If RS-485 reader is connected externally and shared the power supply with the device (The control panel does not support fingerprint verification of RS-485 reader), it is recommended that the connection between the RS-485 reader port and the reader be no longer than

328 ft (100m). Otherwise, it is recommended that the reader use a separate power supply.

12. 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 the FR107 delivered with the system) with the electronic lock to release the self-induced electromotive force during onsite connection for application of the access control system.

13. It is recommended that an electronic lock and a control panel should use separate power supplies.

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

15. In a place with substantial magnetic interference, galvanized steel pipes or shielded cables are recommended, and proper grounding is required.

- Matters needing attention:

--- replacement of a battery with an incorrect type that can defeat a safeguard (for example, in the case of some lithium battery types);

--- disposal of a battery into fire or a hot oven, or mechanically crushing or cutting of a battery, that can result in an explosion;

--- leaving a battery in an extremely high temperature surrounding environment that can result in an explosion or the leakage of flammable liquid or gas; and

--- a battery subjected to extremely low air pressure that may result in an explosion or the leakage of flammable liquid or gas.

2. Overview

2.1 Introduction

ARMATURA Horizon Controller is a regional access control system developed by ARMATURA LLC. It is highly favored in the enterprise level market, especially in large projects with a high number of doors and high security requirements, the entire series of products to comprehensively improvethe hardware, architecture, system security encryption.

2.2 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 credential, 100,000 (1:N) fingerprint, 50,000 (1:N) facial, 3,000 (1:N) palm authentication in one single controller.

PoE

- 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 RESTful based API for 3rd Party software Integration.

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.

Cyber Security

- 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, AES128.
- Web view Controller webserver: HTTPS, TLS 1.2.
- Crypto Chip Storage: EAL5+ chip (anti-tampering, anti-electronic attack, anti-copying) for important data on the controller and reader, private data desensitization, encrypted storage.
- Webserver has passed the penetration test and vulnerability test of well-known brand products, and all medium and above risks have been repaired.
- Supports IP/MAC address filtering functions, and VLAN isolation to enhance cybersecurity standard.

2.3 Appearance

2.3.1 AHSC-1000 Primary Controller

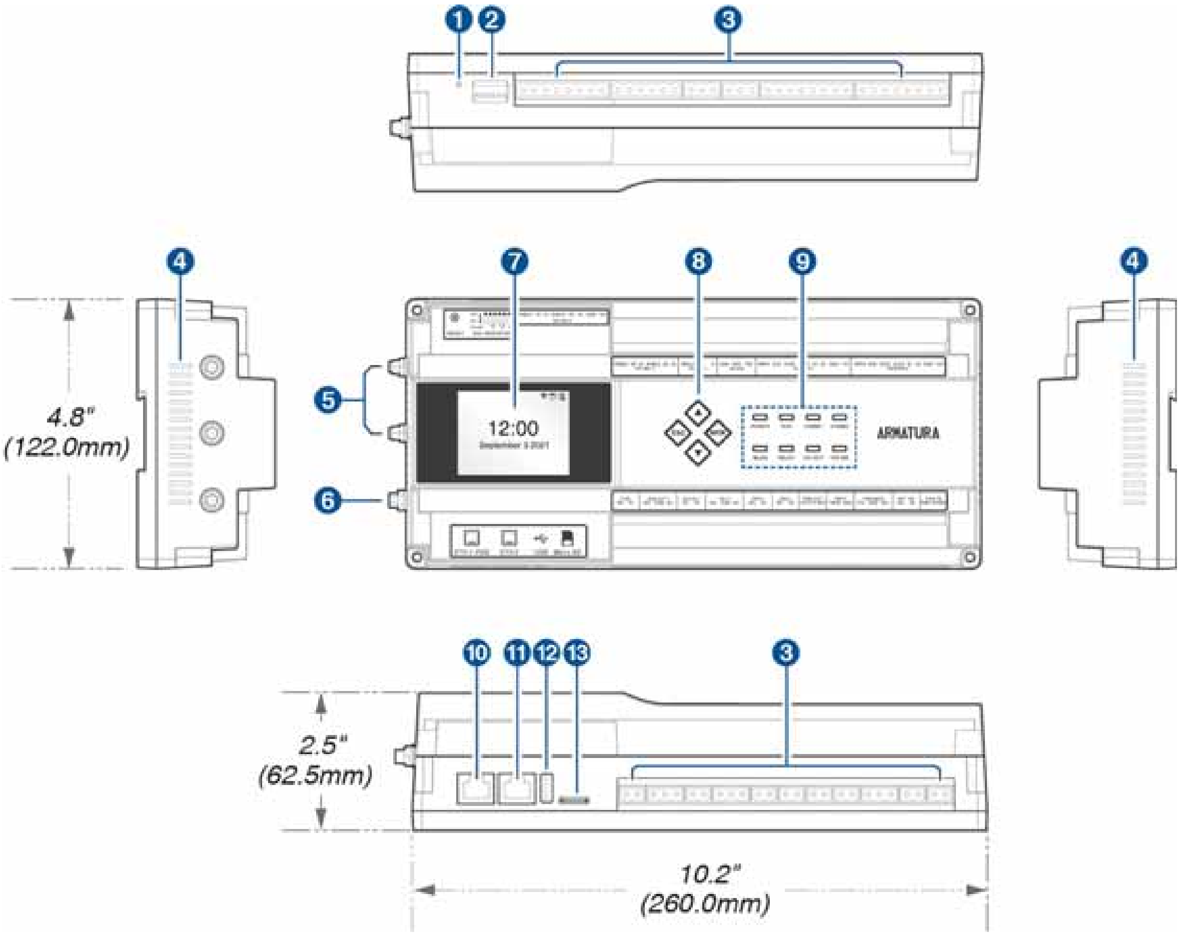


Figure 2-1 AHSC-1000 Primary Controller Appearance

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		

2.3.2 AHDU-1X60 Secondary Controller

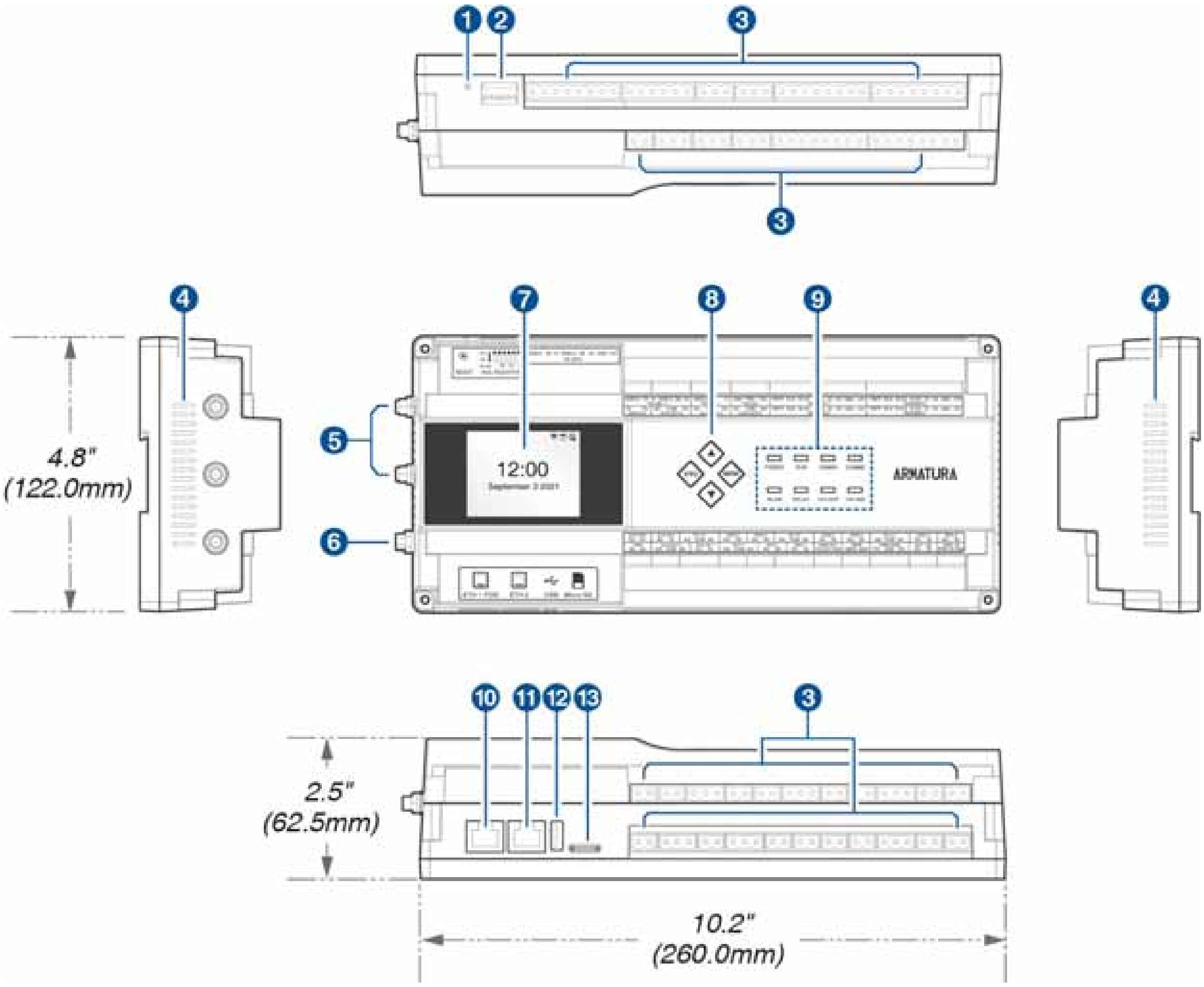


Figure 2-2 AHDU-1X60 Secondary Controller Appearance

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:*** *Long press the reset button for* ***1 to 5*** *seconds to restart the device, long press for more than* ***5*** *seconds to restore the factory settings.*

- ***DIP Switch:*** *When connecting an RS-485 reader for long-distance communication, it is necessary to enable EOL, and configure the EOL resistance of RS-485 through DIP switches.*

2.3.3 AHEB-0808 Expansion Board

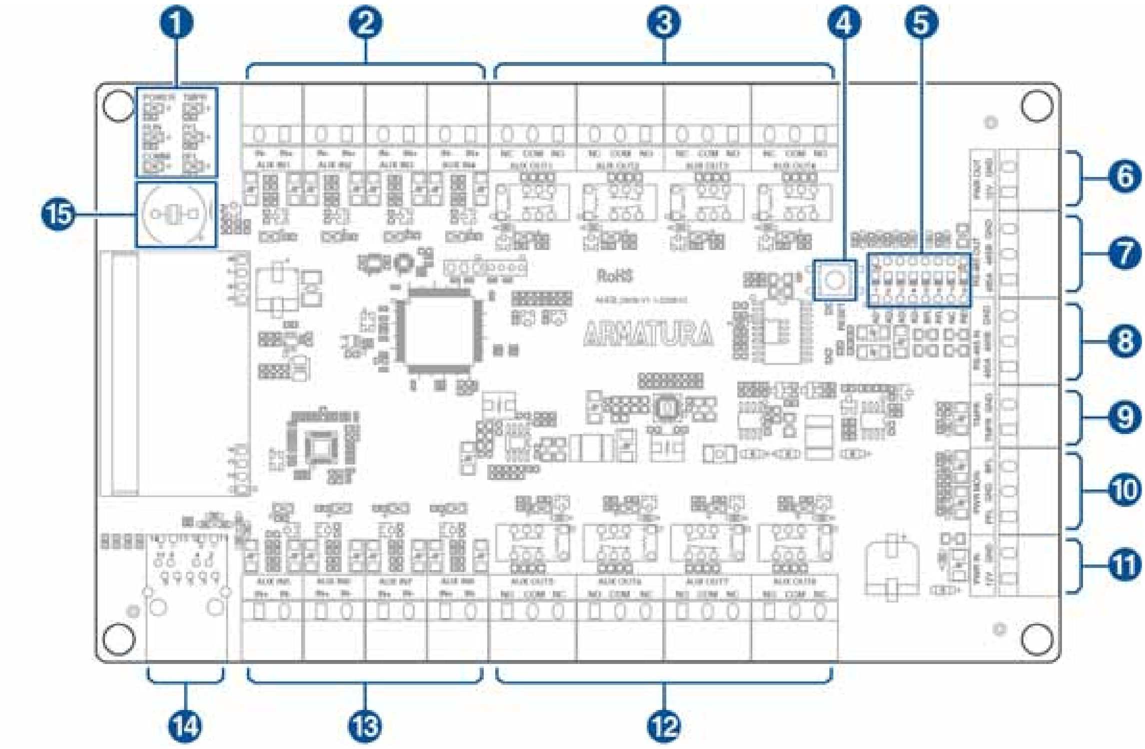


Figure 2-3 AHEB-0808 Appearance

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		

2.3.4 ENC1 Enclosure (optional)

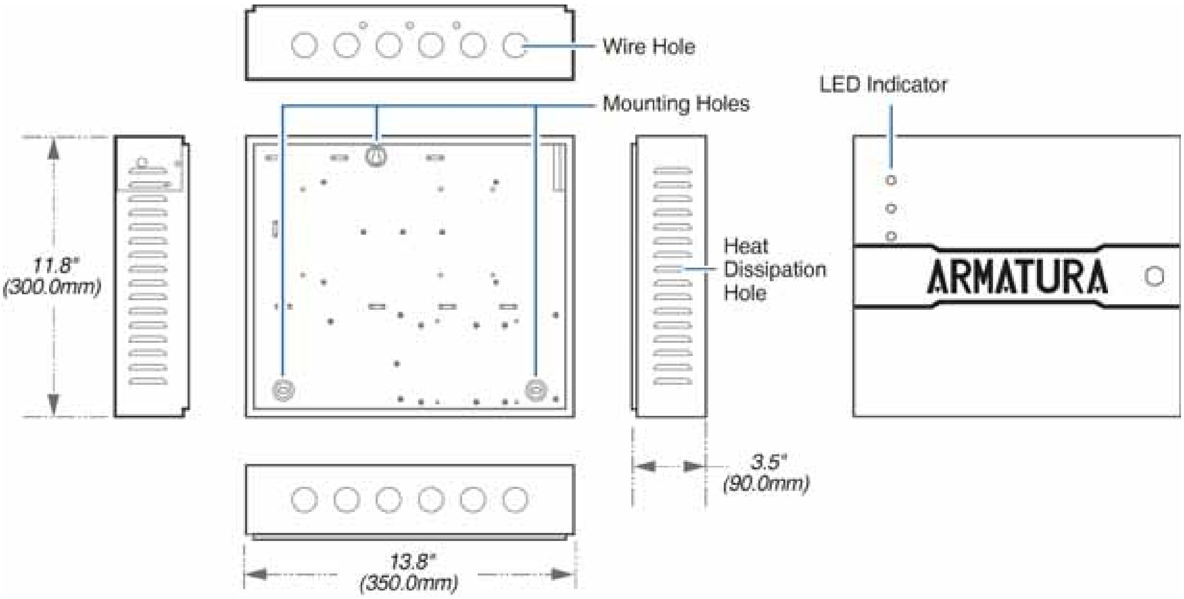


Figure 2-4 ENC1 Enclosure Appearance

Remarks:

- ***Input Voltage***：*100 - 240 VAC*
- USB ports are only used for data transfer,with a maximum output of DC 5V/3A

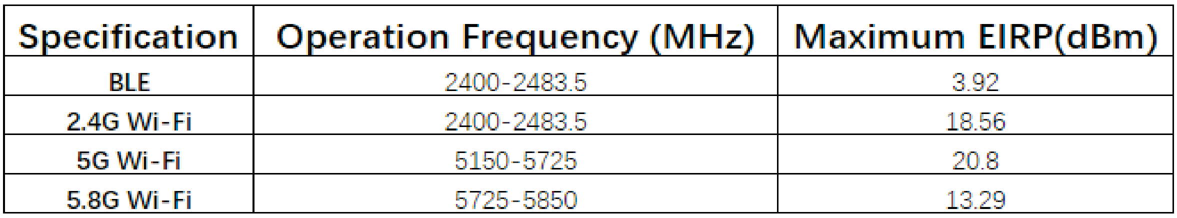
2.4 General Information

	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: DC44-57 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 5.2 , BLE		
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 Credential Capacity	400,000 (1:N) (Bluetooth) 400,000 (1:N) (NFC) 400,000 (1:N) (Dynamic QR Code)		
Fingerprint Capacity	100,000 (1:N)		
Face Capacity	50,000 (1:N)		
Palm Capacity	3,000 (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)		

For EU



Specification	Operation Frequency (MHz)	Maximum EIRP(dBm)
BLE	2400-2483.5	3.92
2.4G Wi-Fi	2400-2483.5	18.56
5G Wi-Fi	5150-5725	20.8
5.8G Wi-Fi	5725-5850	13.29

3. Installation and Connection

Make sure that the device is installed as per the installation instructions. Otherwise, you will bear any consequence resulting from your actions.

3.1 Installation Procedure

Users can choose the following different installation methods according to their actual needs.

Remarks:

1. *AHDU Series (1160/1260/1460) shares the same casing, and the installation and wiring methods are the same. Only AHDU-1460 is used as an example, and will not be repeated here again.*
2. *The pictures in the manual are for reference only, and the actual product purchased by the customer shall prevail.*

3.1.1 Installation with screws

Mount the controller or expansion board directly to the enclosure or flat surface with screws. As shown in the figure below.

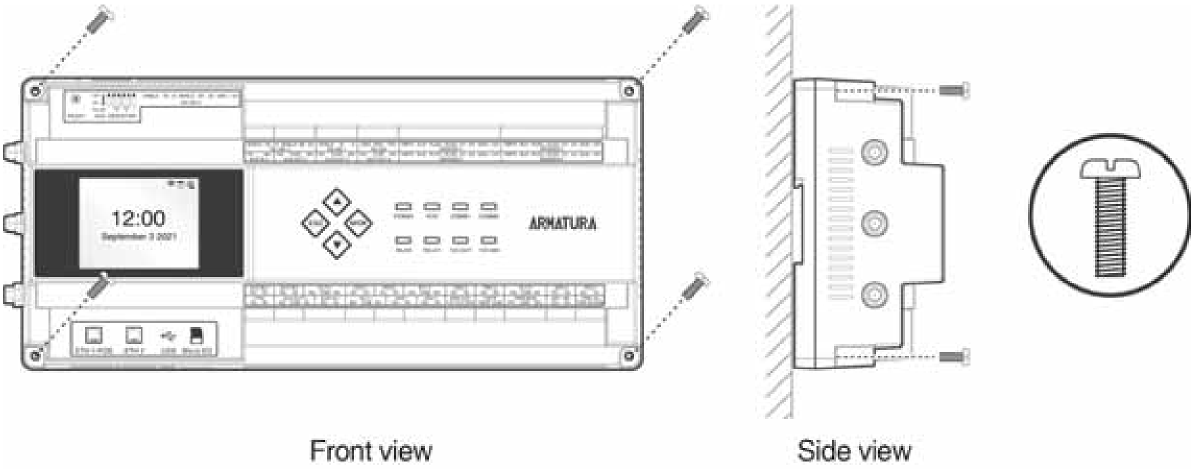


Figure 3-1 Schematic diagram of screw installation

Remarks:

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

3.1.2 Installation with original 35mm DIN rail

1. Mount the original DIN rail directly to the enclosure or flat surface. As shown in the figure below.

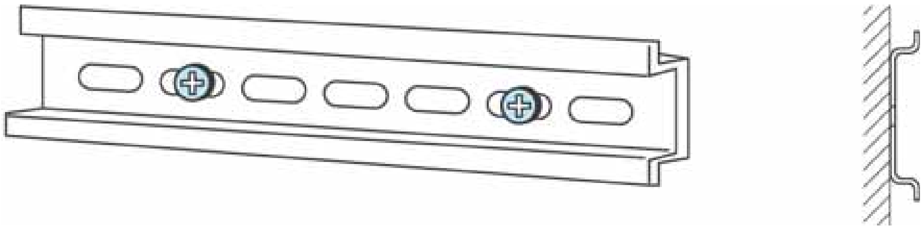


Figure 3-2 Mount the DIN rail

2. Catch the hooks on the tops of the controller onto the DIN rail and press the controller onto the DIN rail until they lock into place, as shown in **Figure 3-3** below.

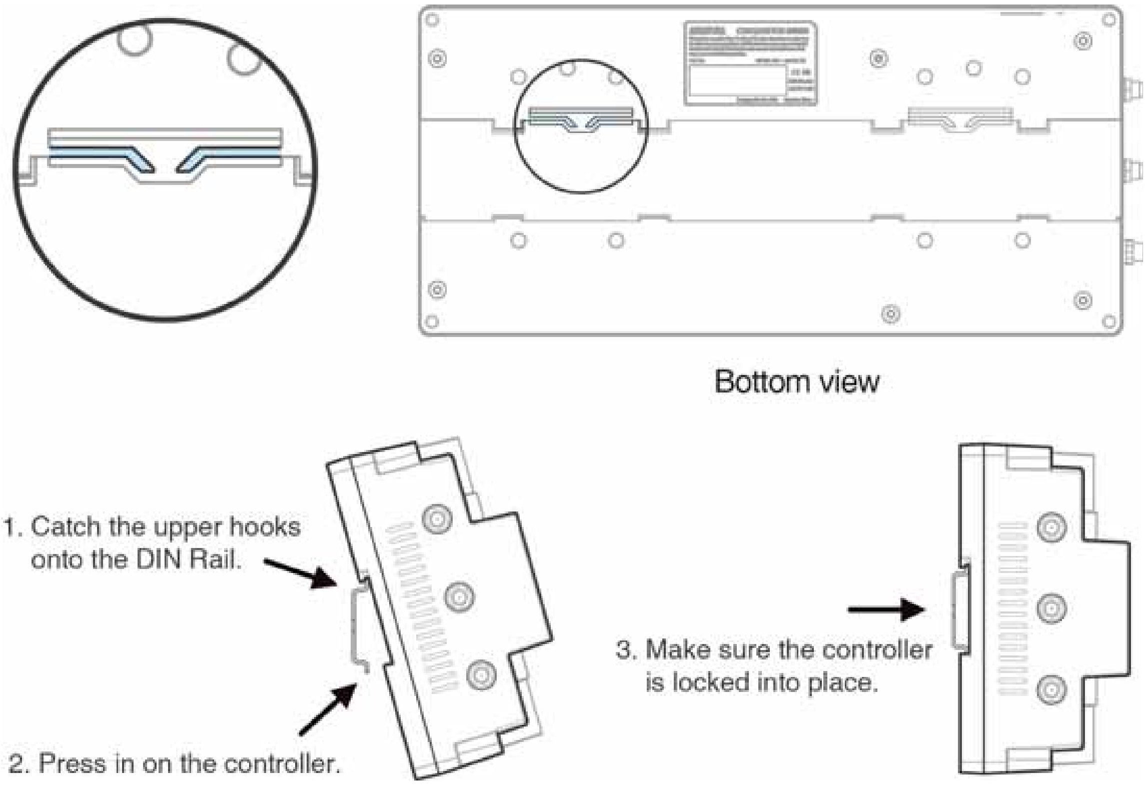

Bottom view
1. Catch the upper hooks onto the DIN Rail.
2. Press in on the controller.
3. Make sure the controller is locked into place.

Figure 3-3 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*

3.1.3 Installation with extended 35mm DIN rail adapter

Users can purchase a third-party rail adapter as needed, mount the controller to it, and then snap it into the original 35mm DIN rail. As shown in the figure below.

1. Refer to the steps of section 3.1.2 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 3-4** below.
3. Snap the mounted units into the original 35mm DIN rail, as shown in **Figure 3-5** below.

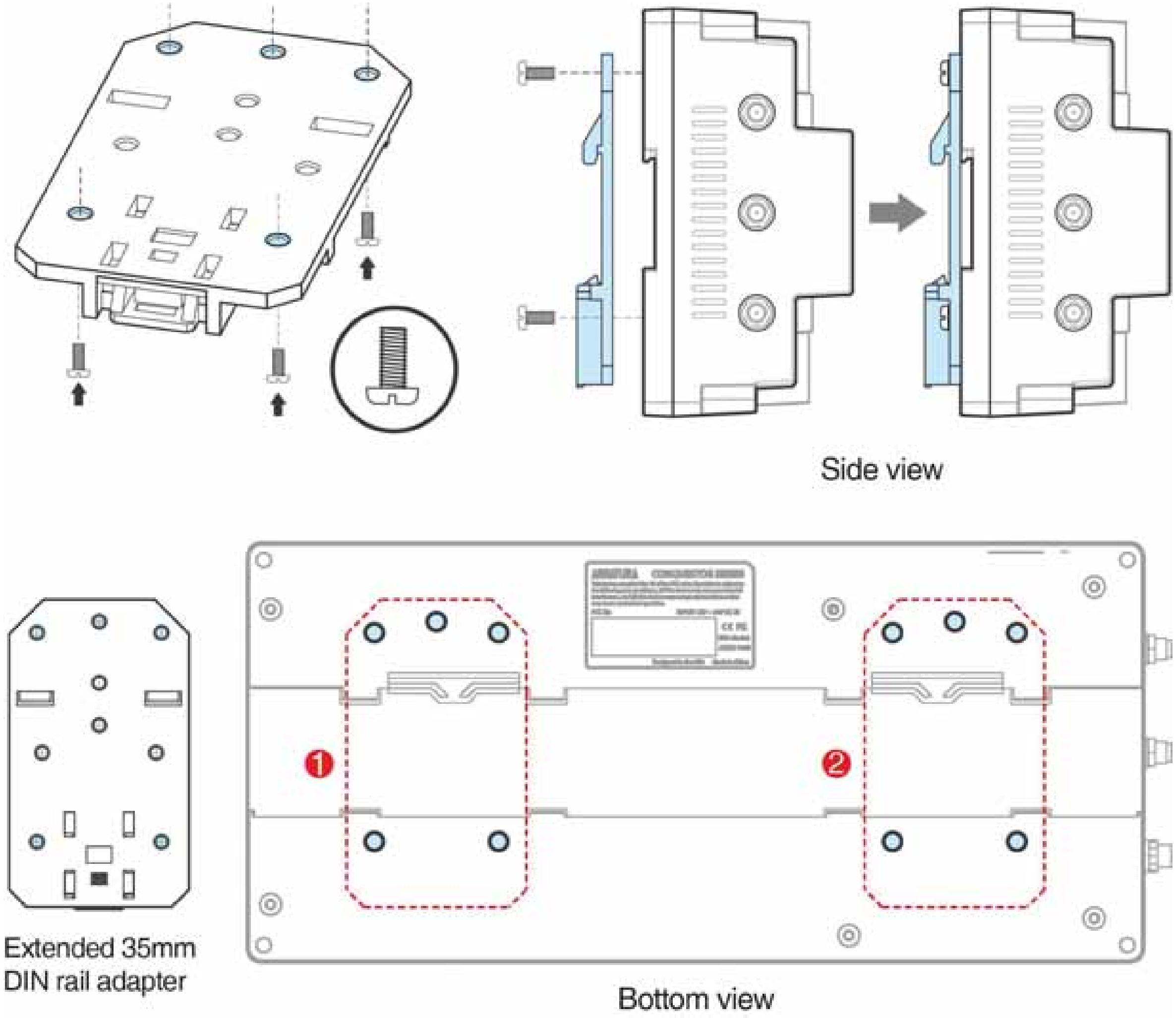


Figure 3-4 Mount the extended 35mm DIN rail adapters to the controller

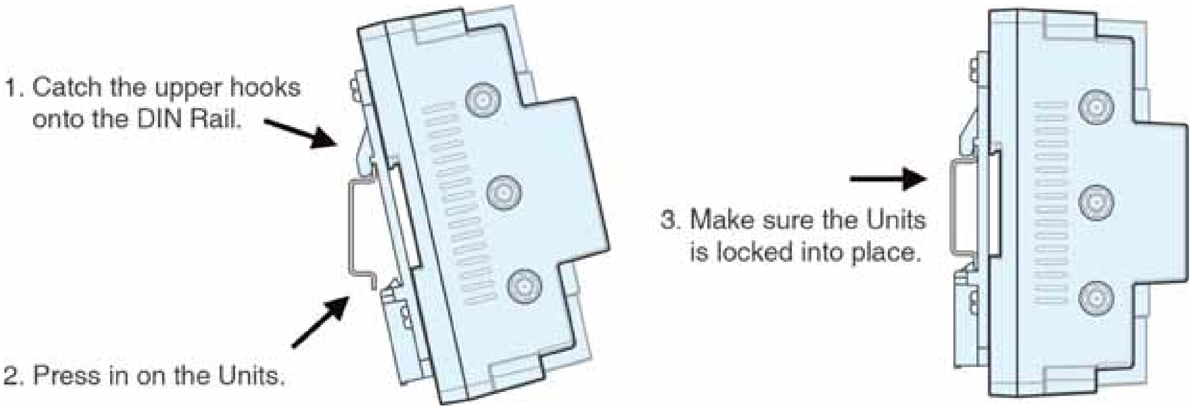

1. Catch the upper hooks onto the DIN Rail.
2. Press in on the Units.
3. Make sure the Units is locked into place.

Figure 3-5 Mount the Units to the original 35mm DIN rail

Remarks:

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

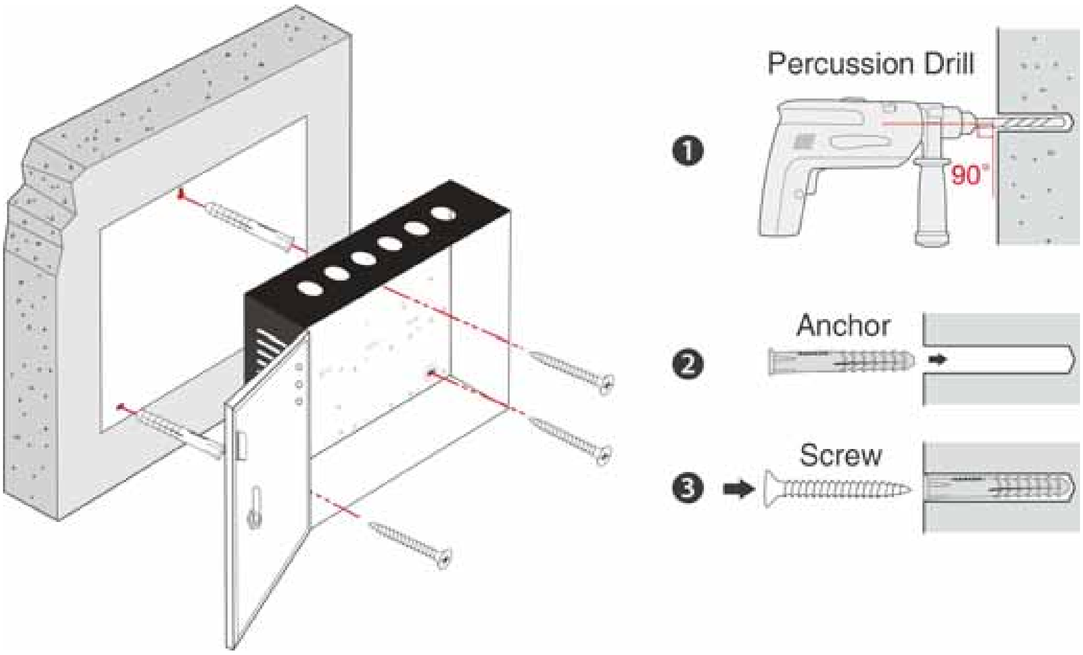
  UTA89 Phoenix Contact, Part Number: 2853970. Link URL: https://www.phoenixcontact.com/zh-cn/products/din-rail-adapter-uta-89-2853970.

- *Users can purchase third-party rail adapters as needed. And the pictures in the manual are for reference only.*
- ***Screw specification:** Cross recessed pan head screws M3*7mm*
- ***Applicable Models:** AHSC-1000, AHDU-1160/1260/1460*

3.2 Installation the ENC1 enclosure on the wall

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

1. According to the mounting holes position of the enclosure. Drill three mounting holes in a suitable spot on the wall and make sure it is about 114 inches (2.9m) above the ground, which can be adjusted according to actual needs.
2. Place the Anchors in the mounting holes.
3. Then fix the enclosure with the self–tapping screws as shown below.



- Three screws are recommended.The dimensions are 3*40mm

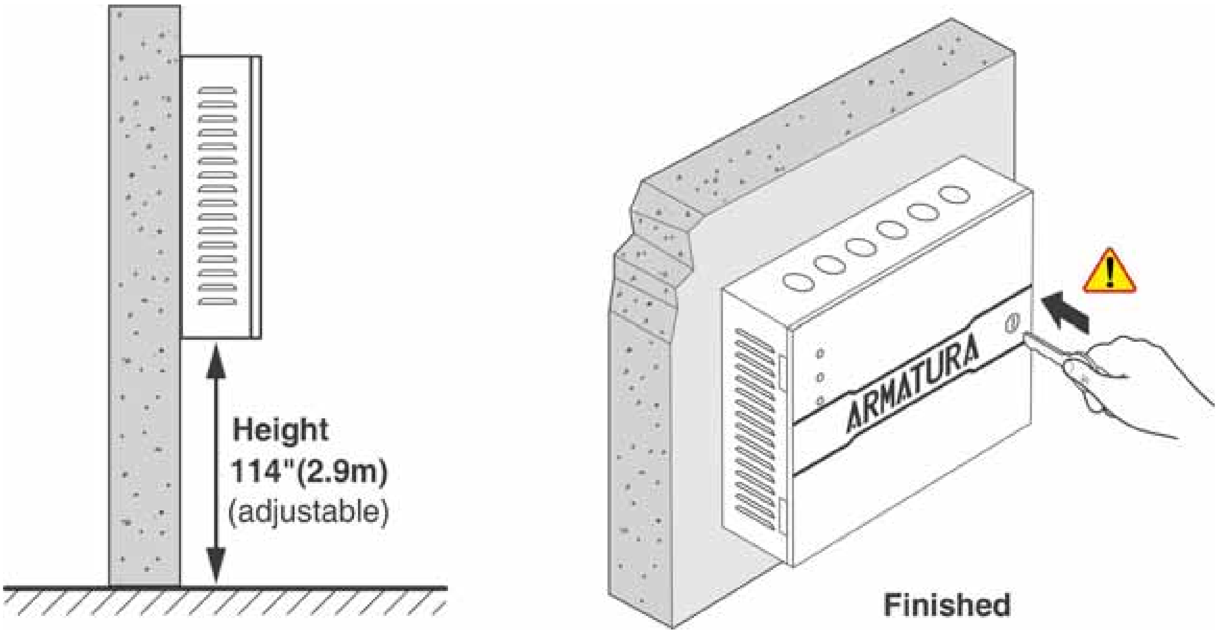


Figure 3-6 Installation the ENC1 enclosure on the wall

Notes:

- *The enclosure is equipped with an tamper alarm switch. When the equipment works normally, please keep the enclosure closed.*
- *For the safety of the equipment, when it is necessary to open the enclosure, please inform the equipment administrator to open the enclosure with the management key.*

3.3 Access Control System Installation

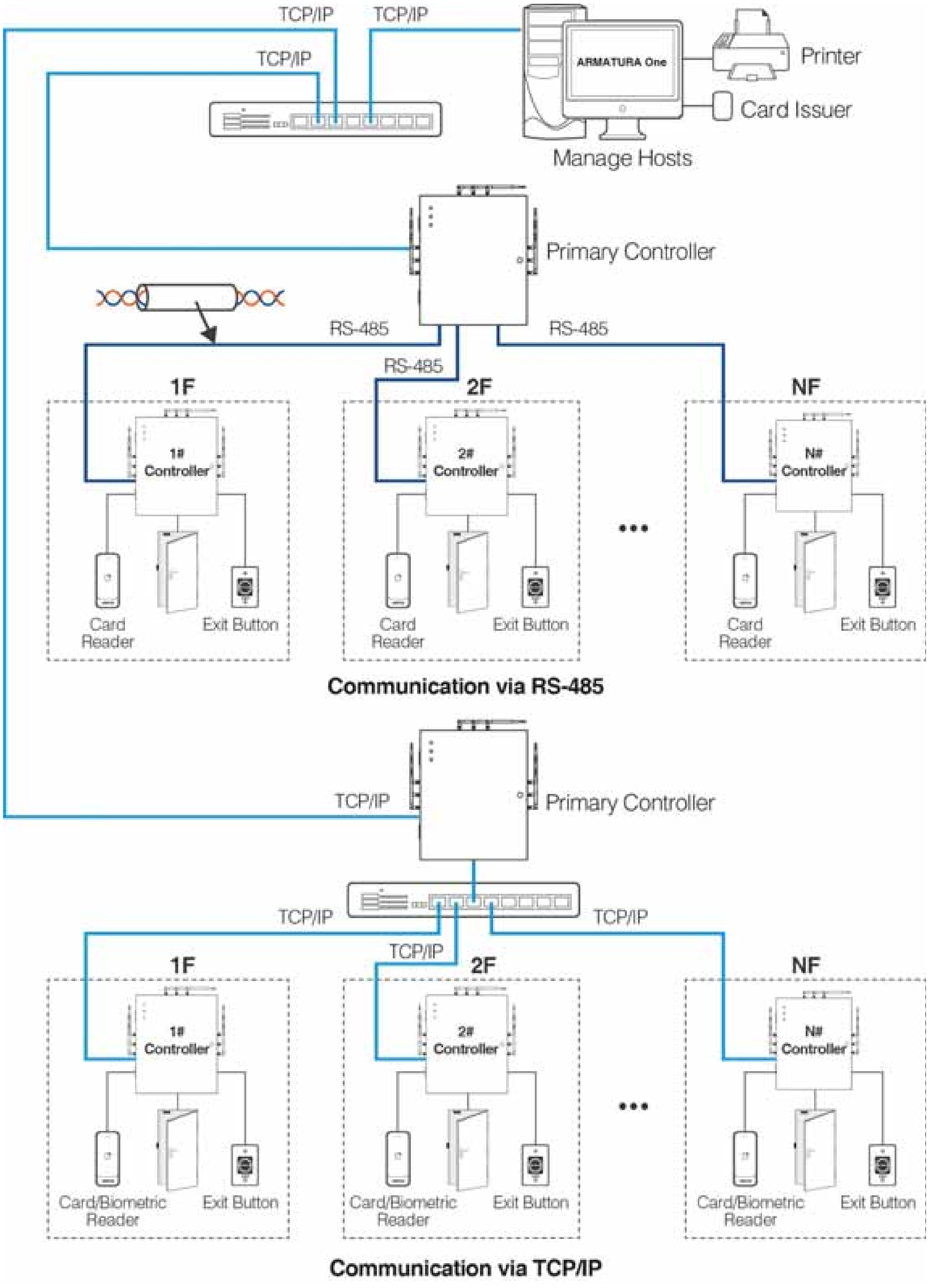


Figure 3-7 Schematic Diagram of Access Control System Installation

Remarks:

1. The access control management system consists of two parts: Management Workstation (PC) and Controller. The management workstation and controller communicate through TCP/IP.
2. The communication wires should be kept away from high voltage wires as far as possible and should be neither routed in parallel with nor bundled with power wires.
3. A management workstation is a PC connected with the network. By running the access control management software installed in the PC, access control management personnel can remotely perform various management functions, like adding/deleting a user, viewing event records, opening/closing doors, and monitoring the status of each door in real-time.
4. When the controller communicates via RS-485, only pure card readers can be connected. When the controller communicates via TCP/IP, card/biometric readheads can be connected.

3.4 Controller System Installation

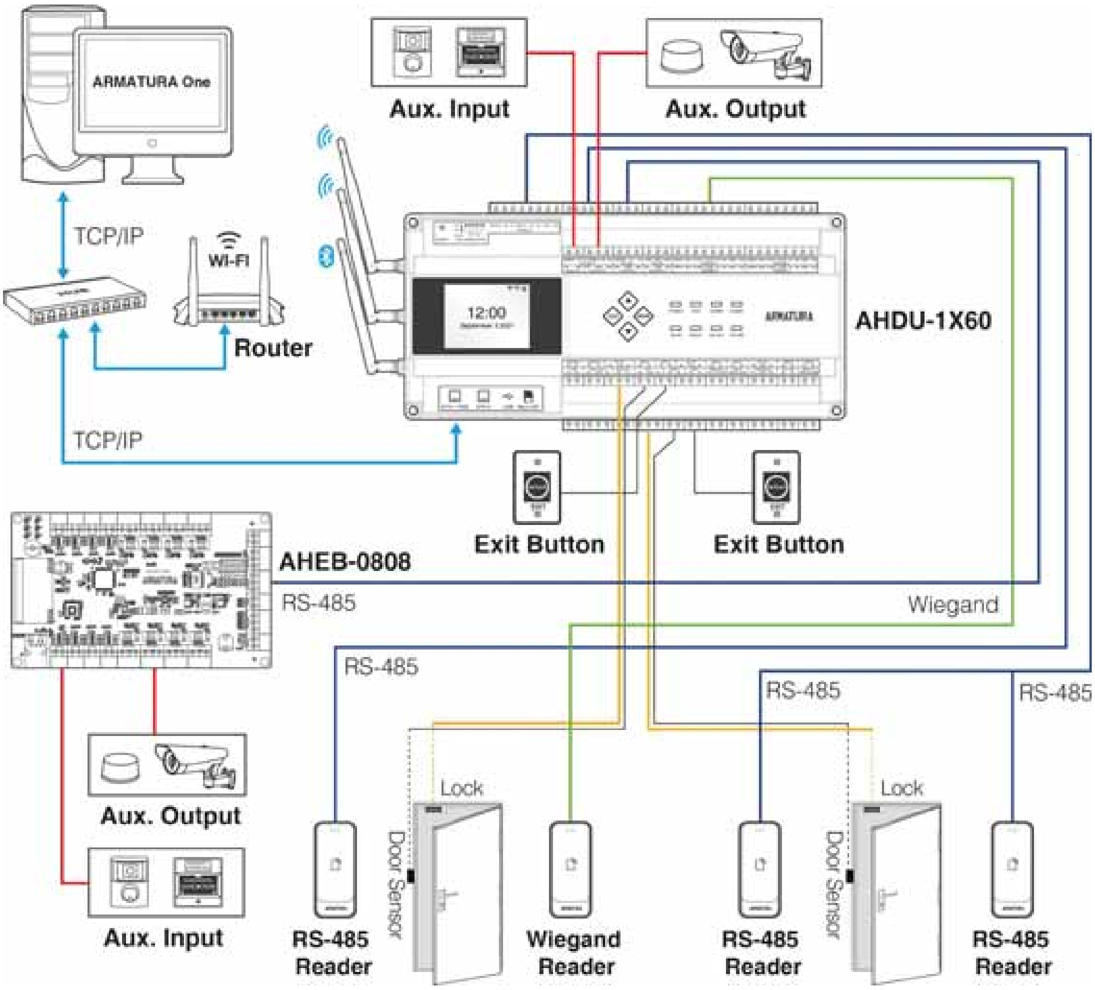


Figure 3-8 Schematic Diagram of AHDU-1X60 System Installation

3.5 Access Control System Power Supply Structure

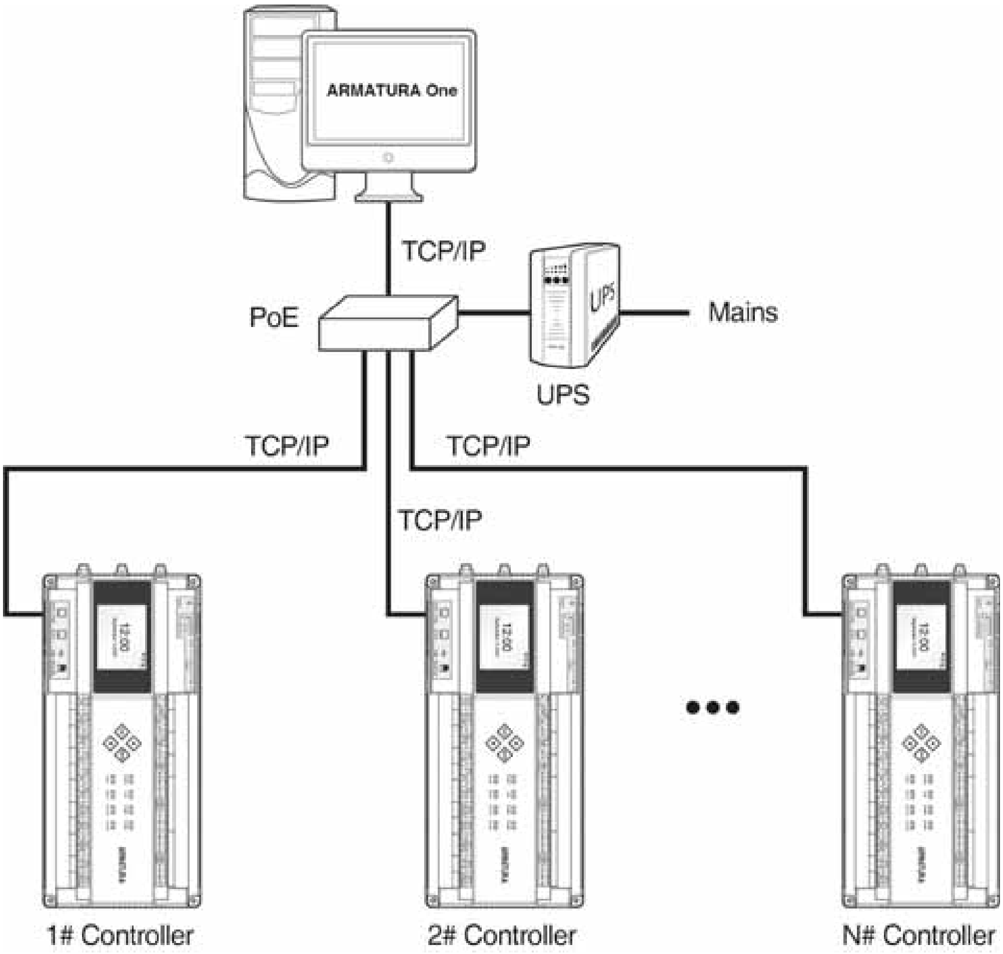


Figure 3-9 PoE System

Remarks:

1. The Armatura Horizon Controller is powered through a +12V DC power adapter or PoE, whichever available.
2. If you choose a +12V DC power adapter, generally, each controller should be powered separately to reduce power interference between controllers.
3. If you choose PoE, the TCP/IP network interface of the access controller can serve as a PoE interface and a PC communication interface. The PoE switch must conform to IEEE 802.3at standards.
4. To prevent power failure of a controller which may end up with making the whole system unable to work, the access control management system is usually required to have one UPS at least, and access control locks are powered externally to guarantee the access control management system can still work normally during power failure.

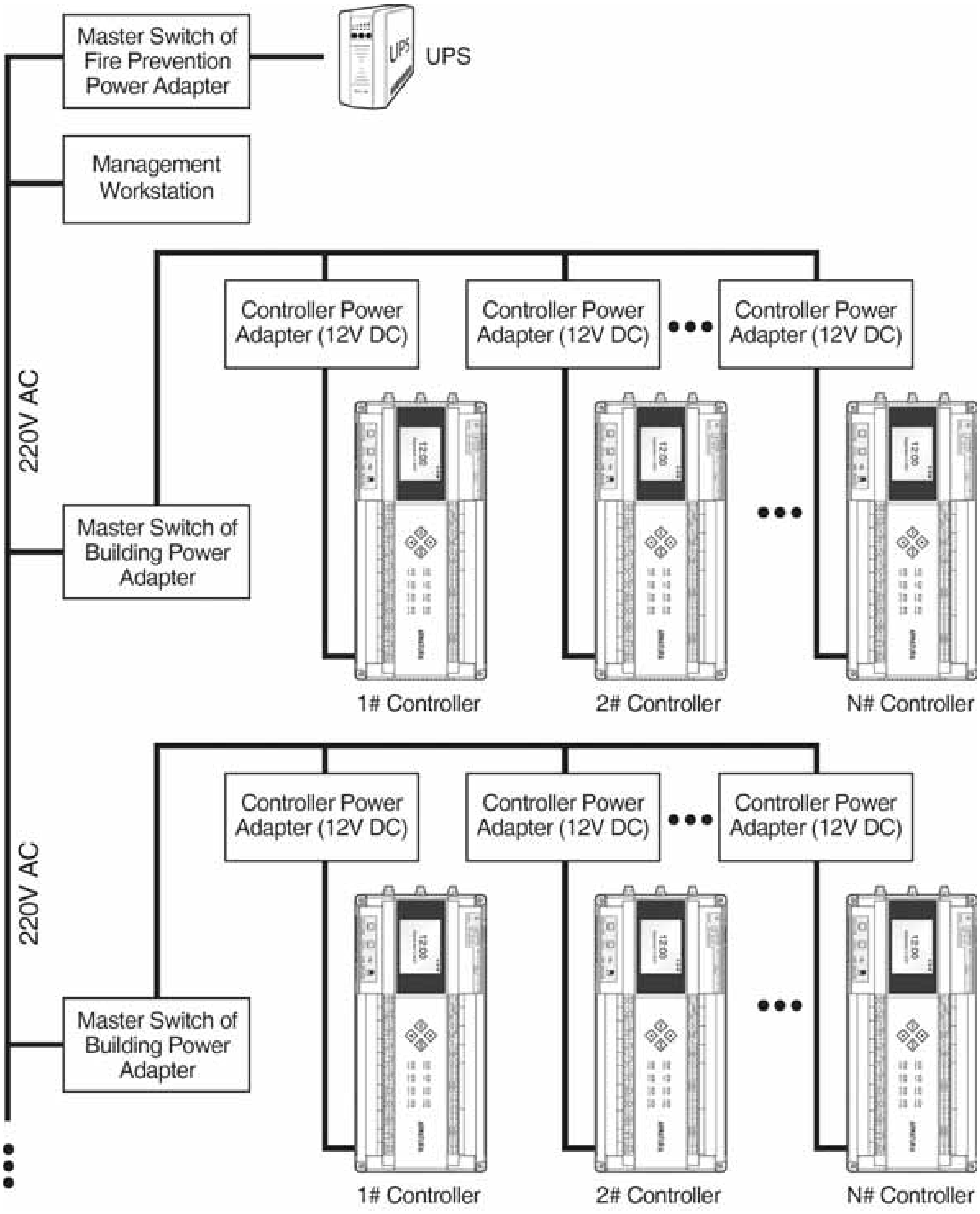

Master Switch of Fire Prevention Power Adapter
UPS
Management Workstation
220V AC
Controller Power Adapter (12V DC)
Controller Power Adapter (12V DC)
Controller Power Adapter (12V DC)
Master Switch of Building Power Adapter
1# Controller
2# Controller
N# Controller
220V AC
Controller Power Adapter (12V DC)
Controller Power Adapter (12V DC)
Controller Power Adapter (12V DC)
Master Switch of Building Power Adapter
1# Controller
2# Controller
N# Controller

Figure 3-10 Access Controller System Power Supply

4. Terminal and Wiring Description

4.1 Controller Connection Terminals

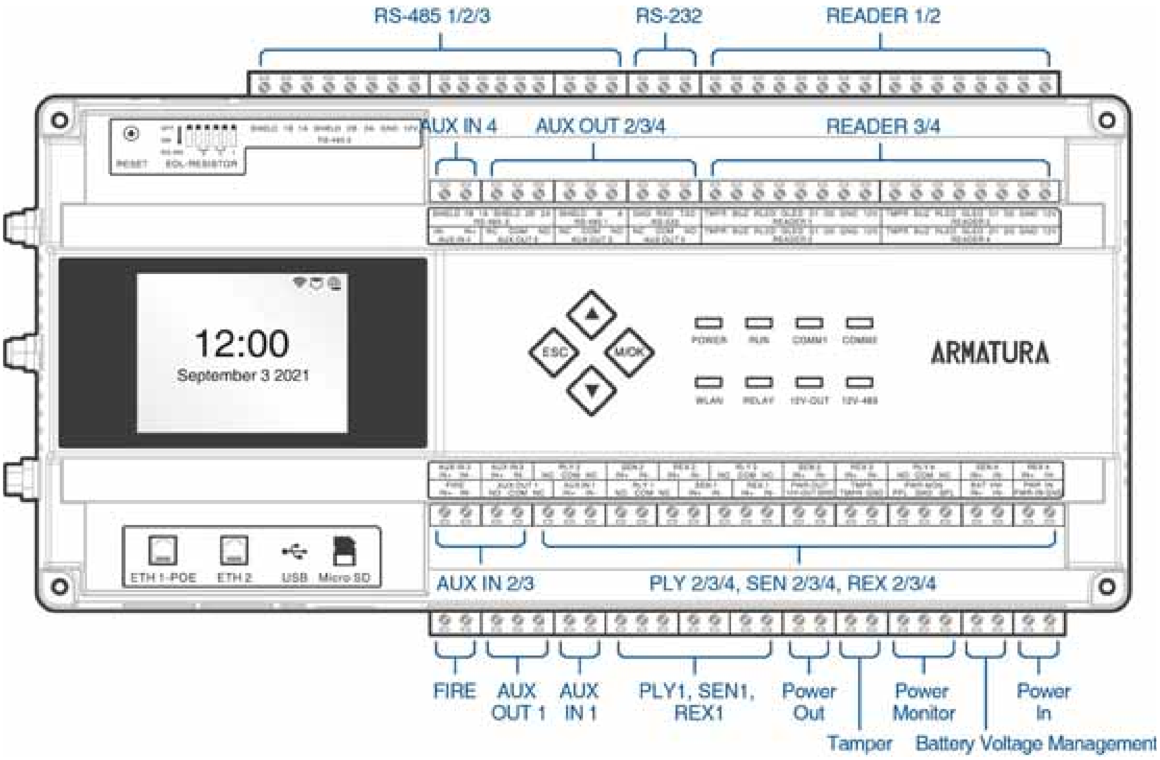


Figure 4-1 AHDU-1X60 Terminal connection diagram

Description of the terminals:

1. **RS-485:** The RS-485 reader port can be connected externally to RS-485 reader.

2. **READER:** The reader port can be connected externally to wiegand reader.

3. **Auxiliary Input (AUX IN):** The auxiliary input may connect to infrared body detectors, fire alarms, or smoke detectors.

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

5. **FIRE, Auxiliary Input (AUX IN), Sensor(SEN), Request to Exit(REX):** The fire port, auxiliary input, sensor port and request to exit port support line monitoring. The line monitoring function needs to be enabled by connecting to the ARMATURA One software side. For a supervised circuit, add two resistors as close to the sensor as possible. Custom end of line (EOL) resistances may be configured via 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

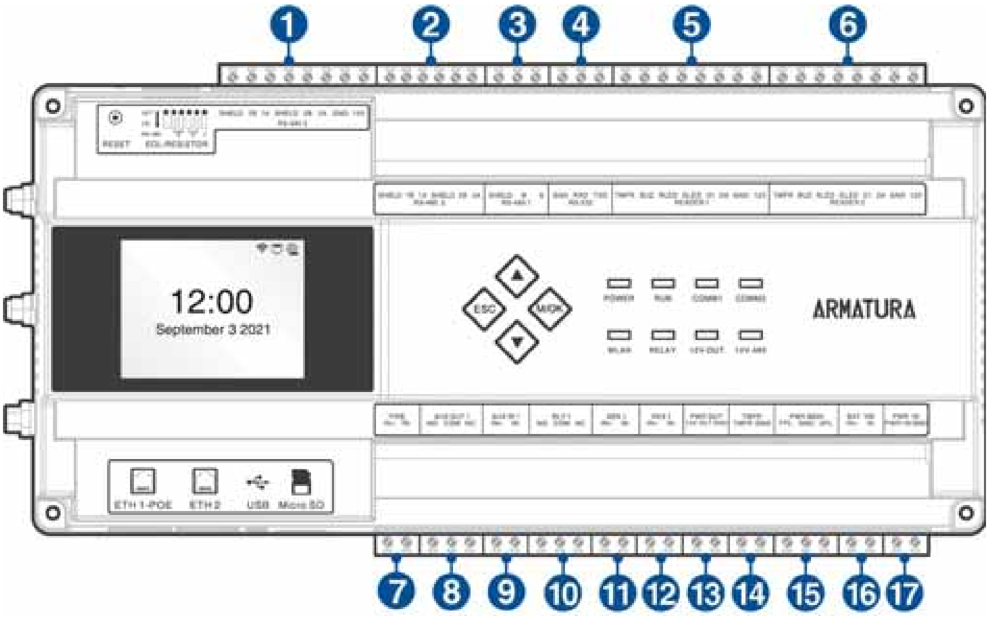


Figure 4-2 AHSC-1000 terminal description

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

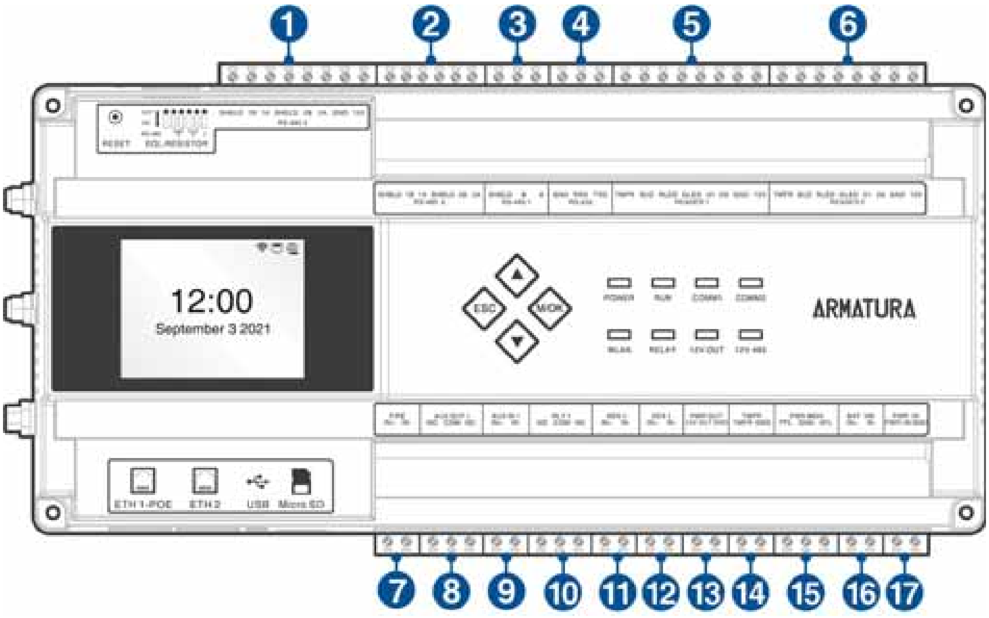


Figure 4-3 AHDU-1160 terminal description

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

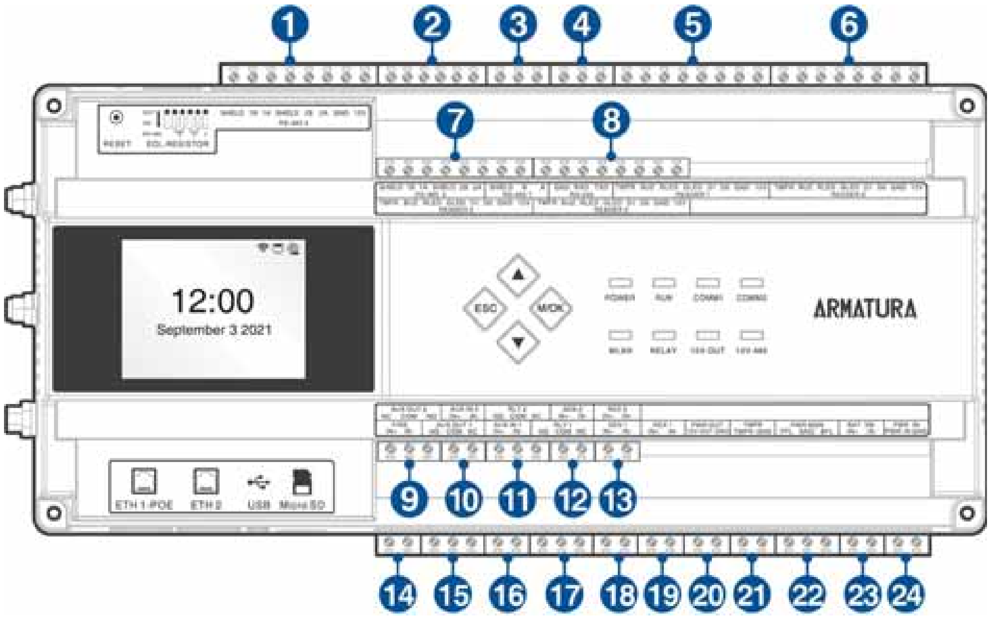


Figure 4-4 AHDU-1260 terminal description

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

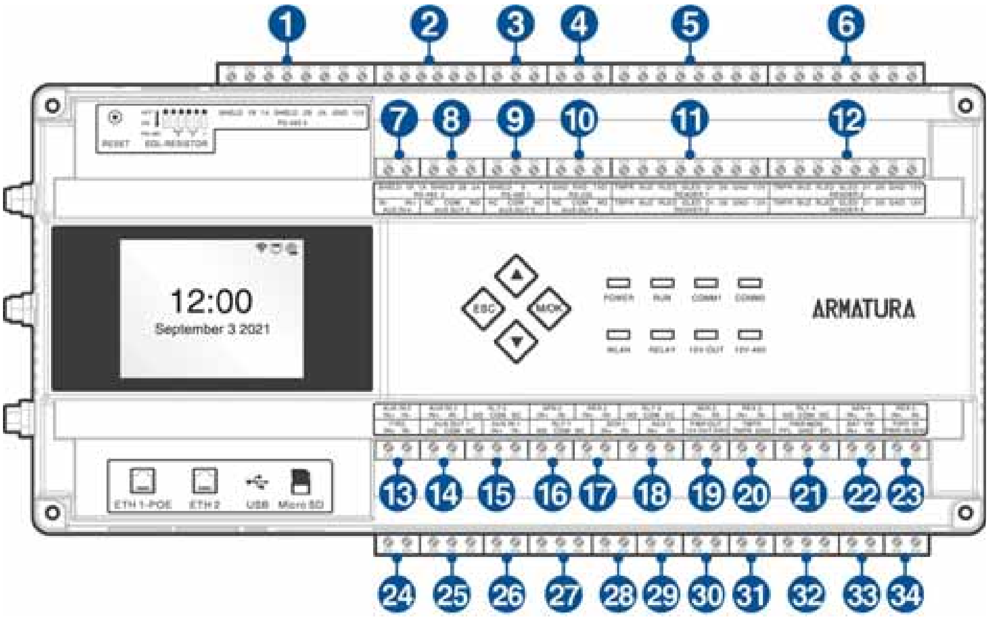


Figure 4-5 AHDU-1460 terminal description

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

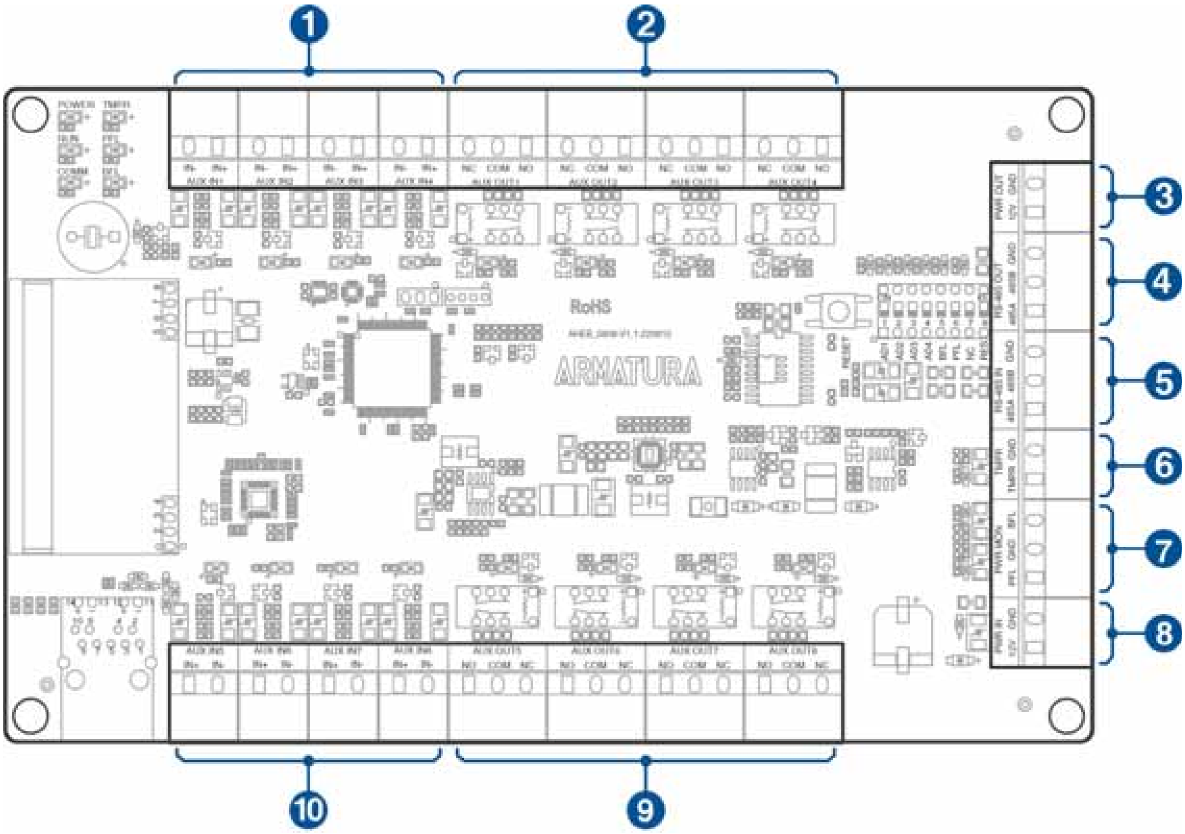


Figure 4-6 AHEB-0808 terminal description

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)

4.3 Wiring Description

4.3.1 Power Wiring

The Armatura Horizon Controller is powered through a 12V-24V DC power adapter or PoE, whichever available. The wiring is as shown below:

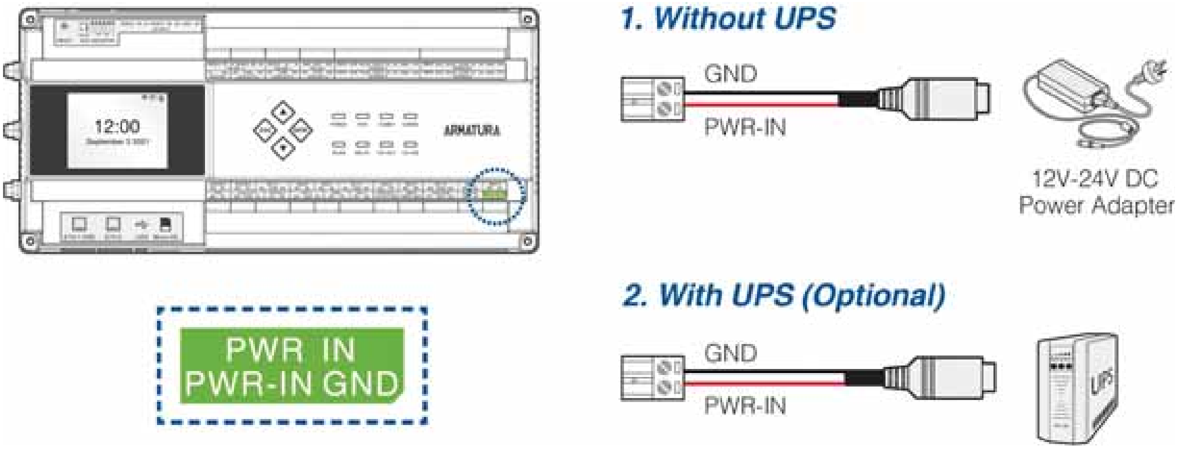


Figure 4-7 Power Wiring

Recommended Power Supply:

- 12V-24V DC ±20%, at least 1.5A.
- Use an AC adapter with a higher current ratings to share the power with other devices.

4.3.2 Network Wiring

Connect the device and the software over an Ethernet cable. An example is shown below:

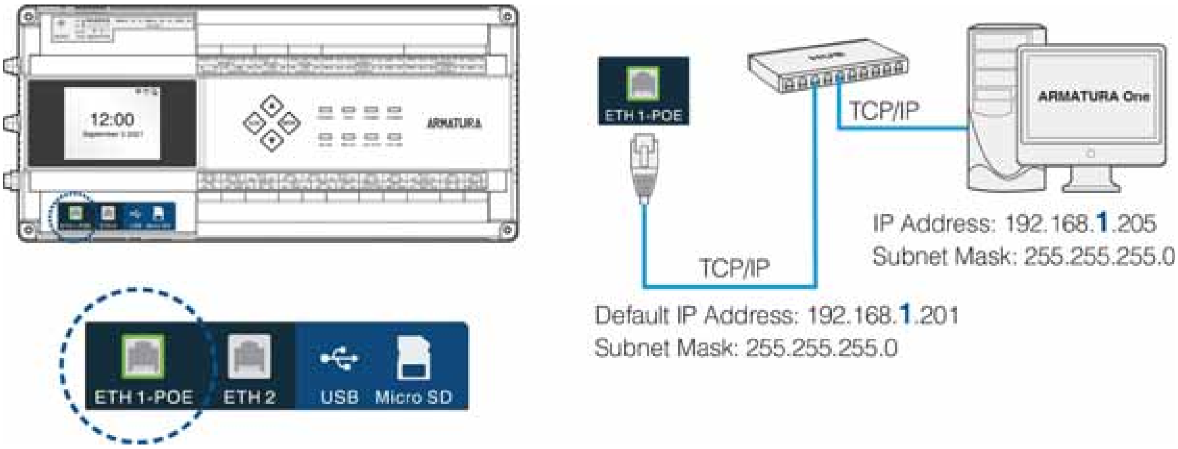

12:00
ARMATURA
ETH 1-POE
ETH 2
USB
Micro SD
ETH 1-POE
TCP/IP
TCP/IP
ARMATURA One
IP Address: 192.168.1.205
Subnet Mask: 255.255.255.0
Default IP Address: 192.168.1.201
Subnet Mask: 255.255.255.0

Figure 4-8 Network Wiring

Note:

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.*

4.3.3 Auxiliary Output Wiring

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

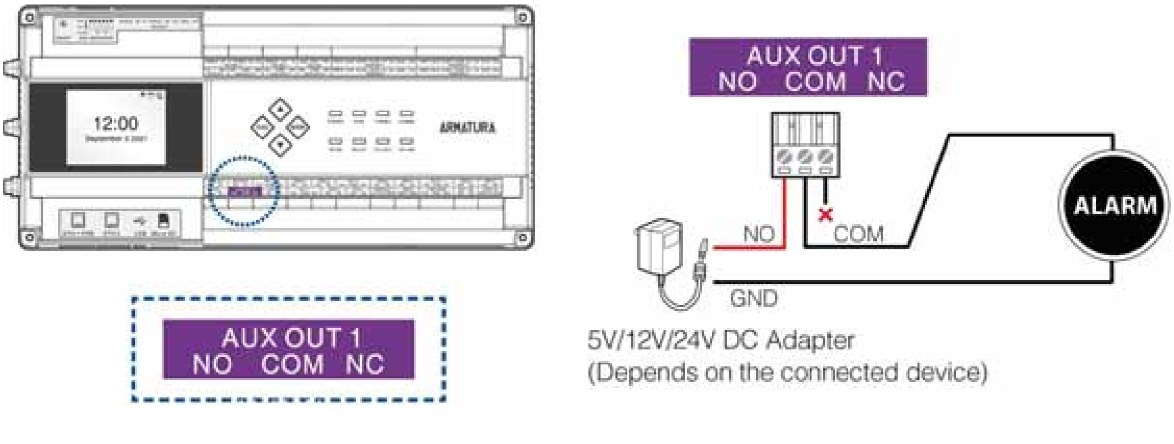


Figure 4-9 Auxiliary Output Wiring

Note:

1. *The device needs to be connected to the power adapter separately.*
2. *Choose a different power adapter source according to the device.*

4.3.4 Auxiliary Input Wiring

The auxiliary input interface which may connect to infrared body detectors, smoke detectors, gas detectors, window magnetic alarms, wireless exit switches, etc. Auxiliary inputs are set through the relevant access control software. Please see the respective software manual for further details.

Auxiliary input port supports line monitoring, the unsupervised circuit and the supervised circuit are shown in the figure below. For a supervised circuit, add two resistors as close to the sensor as possible, like R1 and R2 in the figure.

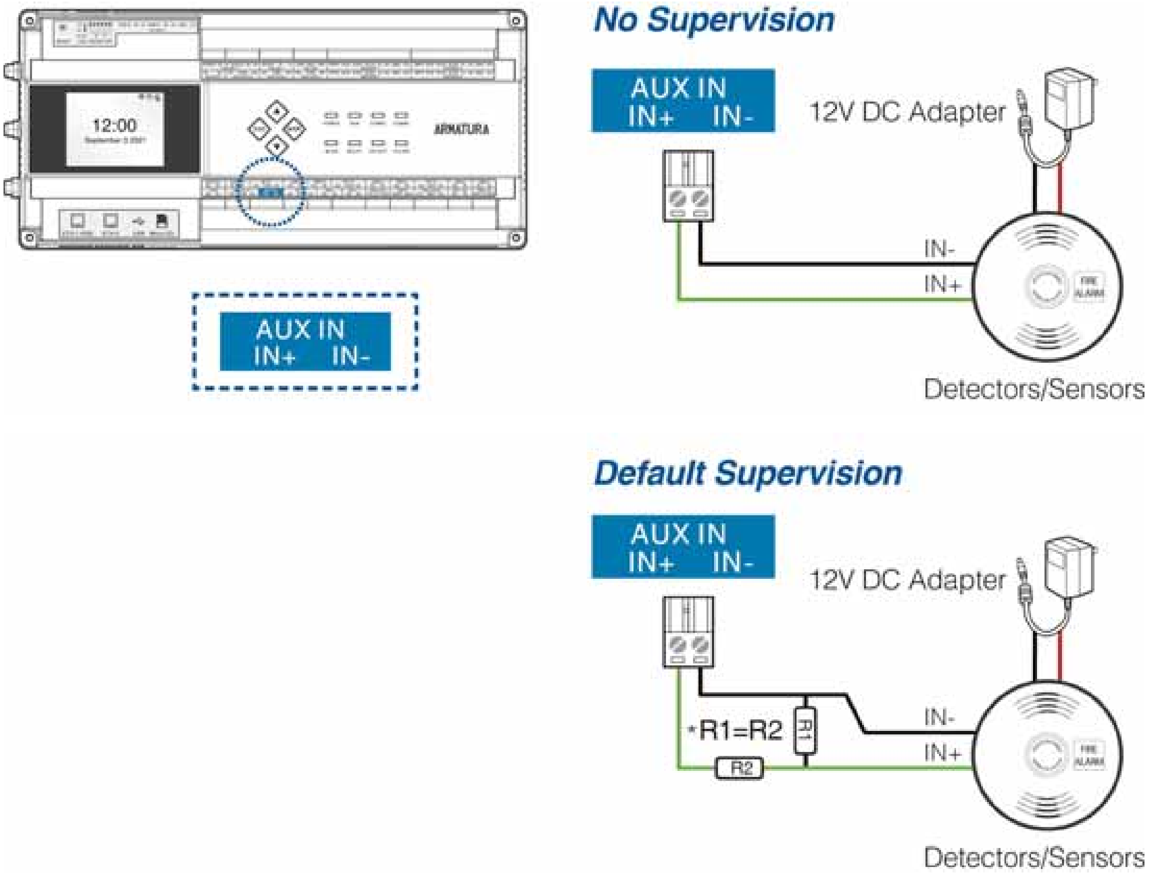


Figure 4-10 Auxiliary Input Wiring

Note:

Custom end of line (EOL) resistances may be configured via the host software. Support 1.2K, 2.2K, 4.7K, 10K resistors. For details, see 4.3.11 Line Monitoring.

4.3.5 Door Sensor, Exit Button Wiring

A door sensor is used to sense the open/close status of a door. With a door sensor switch, an access control panel can detect the unauthorized opening of a door and will trigger the output of alarm. Moreover, if a door is not closed within a specified period after it is opened, the door control panel will also raise the alarm. It is recommended to select two-core wires with a gauge over 0.22mm^2. A door sensor can be omitted if it is unnecessary to monitor the open/closed status of a door, raise the alarm when the door is not closed for a long time, monitor if there is unauthorized access, and use the interlock function.

An exit switch is a switch installed indoor to open a door. When it is switched on, the door will be opened. An exit button is fixed at the height of about **55.12 inches(1.4m)** above the ground. Ensure it is located in the right position without slant, and its connection is correct and secure. (Cut off the exposed end of any unused wire and wrap it with insulating tape.) Make sure to avoid electromagnetic interference (such as light switches and computers). It is recommended to use two-core wires with a gauge over 0.3mm^2 as the connection wire between an exit switch and the controller.

Sensor port and request to exit port support line monitoring, the unsupervised circuit and the supervised circuit are shown in the figure below.

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

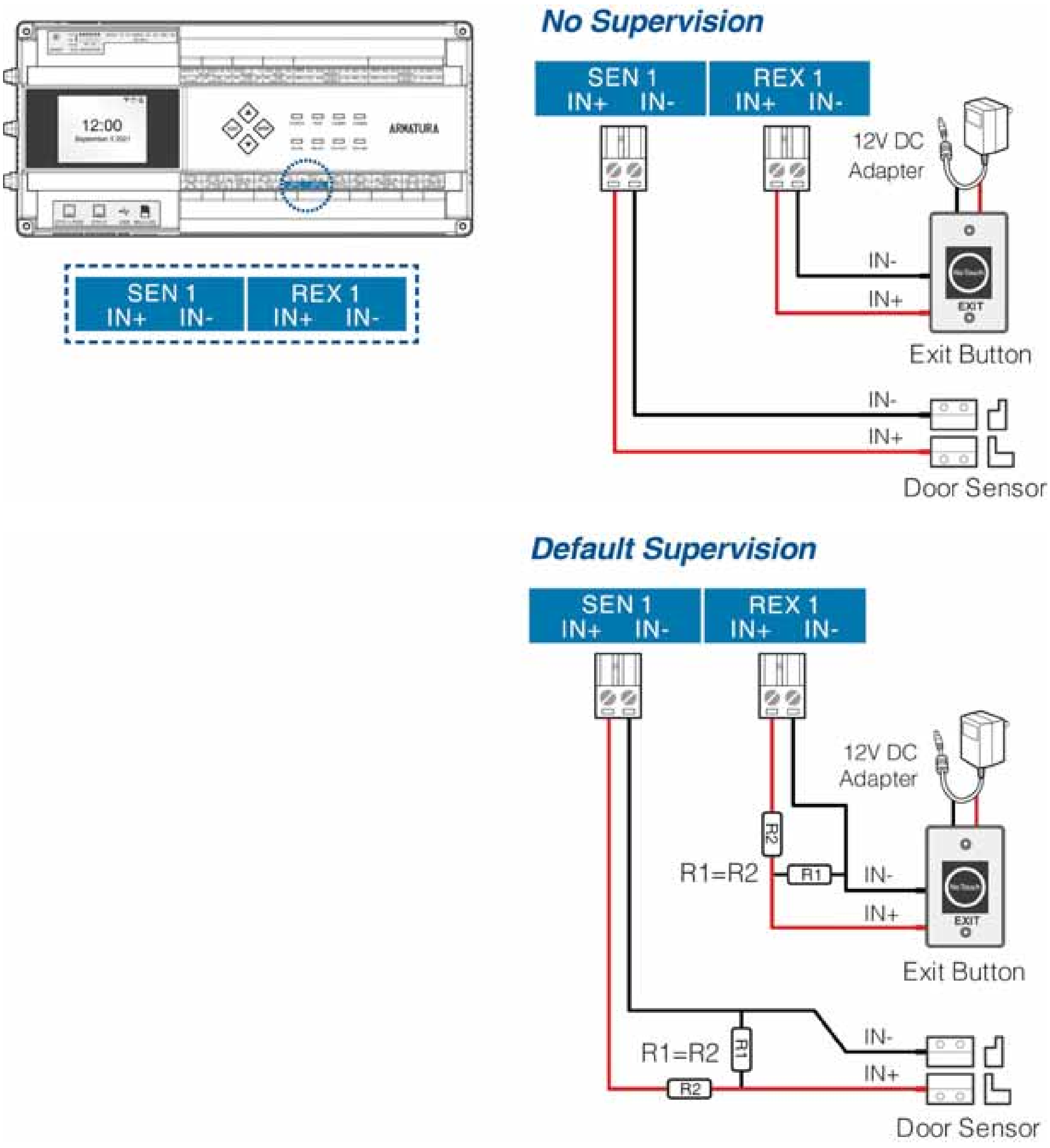


Figure 4-11 Door Sensor, Exit Button Wiring

Note:

Custom end of line (EOL) resistances may be configured via the host software. Support 1.2K, 2.2K, 4.7K, 10K resistors. For details, see 4.3.11 Line Monitoring.

4.3.6 Wiegand Reader Wiring

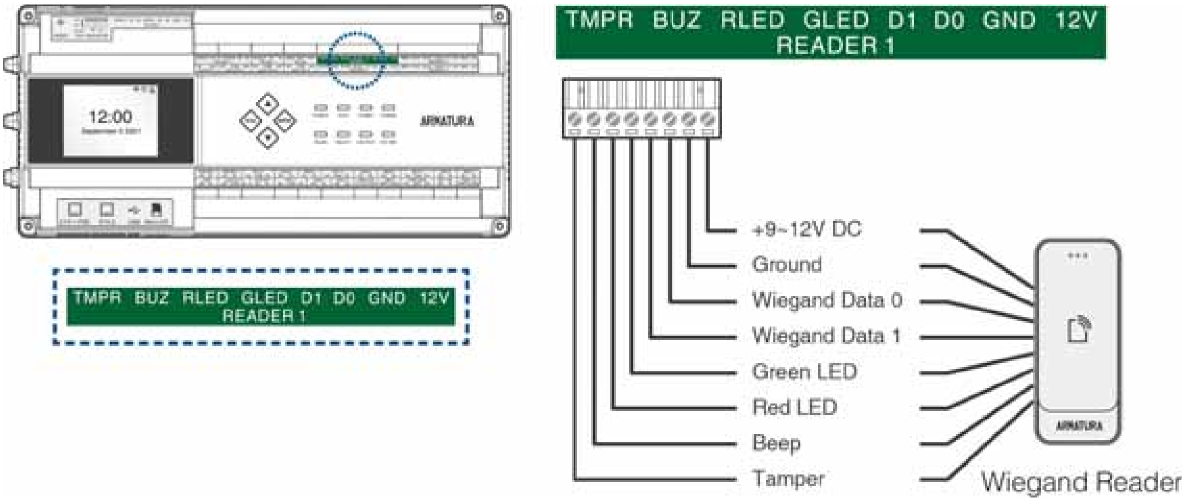


Figure 4-12 Wiegand Reader Wiring

4.3.7 Lock Relay Wiring

1. An ARMATURA Horizon Controller provides one or multiple electronic lock outputs. The **COM** and **NO** terminals apply to the locks that are unlocked when power is connected and locked when power is disconnected. The **COM** and **NC** terminals use the locks that are locked when power is connected and unlocked 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:

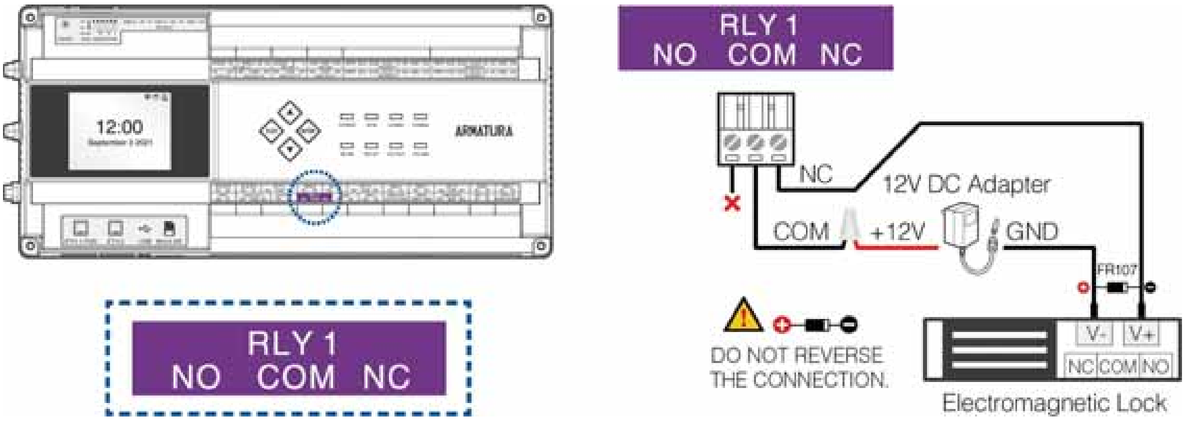


Figure 4-13 Wiring diagram of lock connection

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.

4.3.8 Fire Alarm Monitoring Wiring

Input FIRE port circuits can be configured as No Supervision mode or Default Supervision mode, the default is No Supervision mode, all doors are normally open in case of short circuit. After connecting the ARMATURA One software to enable line monitoring, custom end of line (EOL) resistances can be configured, and the FIRE wiring method is shown in the figure below. For a monitored circuit, add two resistors as close to the sensor as possible.

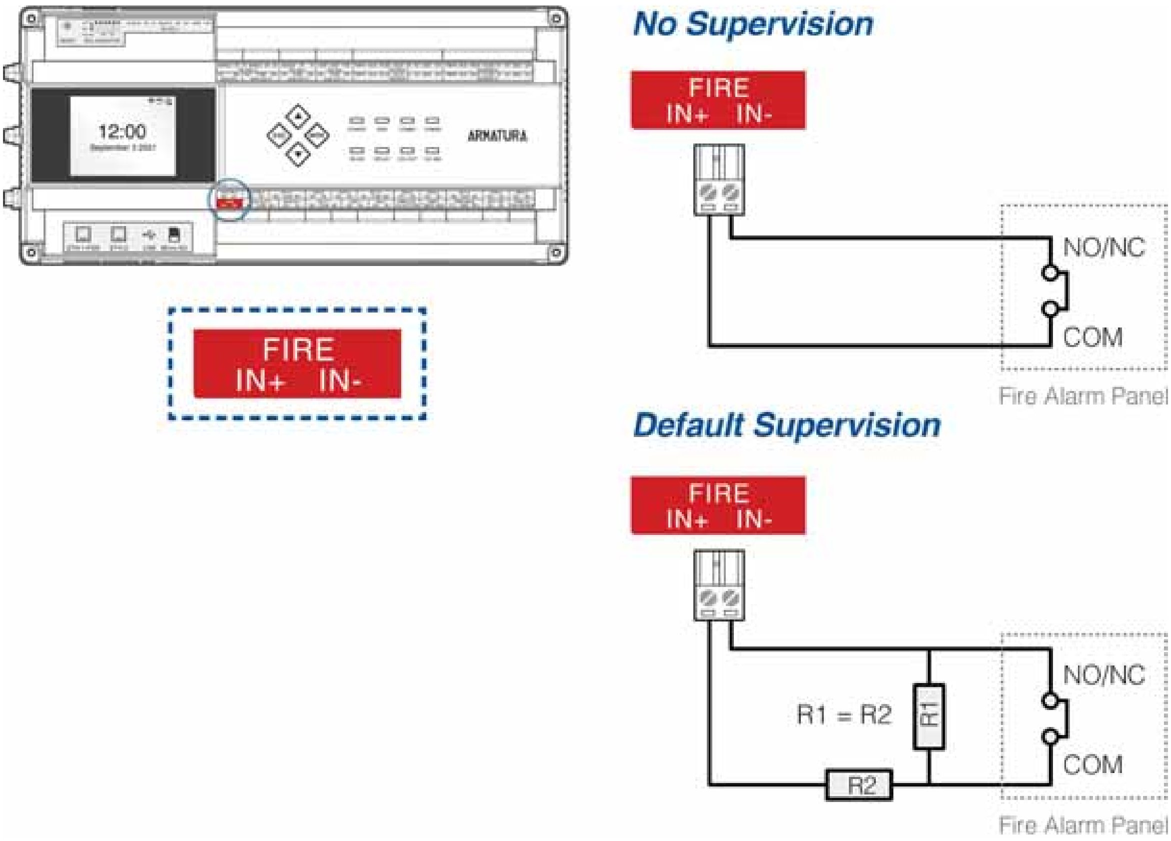


Figure 4-14 Fire Alarm Monitoring Wiring

Note:

Custom end of line (EOL) resistances may be configured via the host software. Support 1.2K, 2.2K, 4.7K, 10K resistors. For details, see 4.3.11 Line Monitoring.

4.3.9 RS-485 Reader Wiring

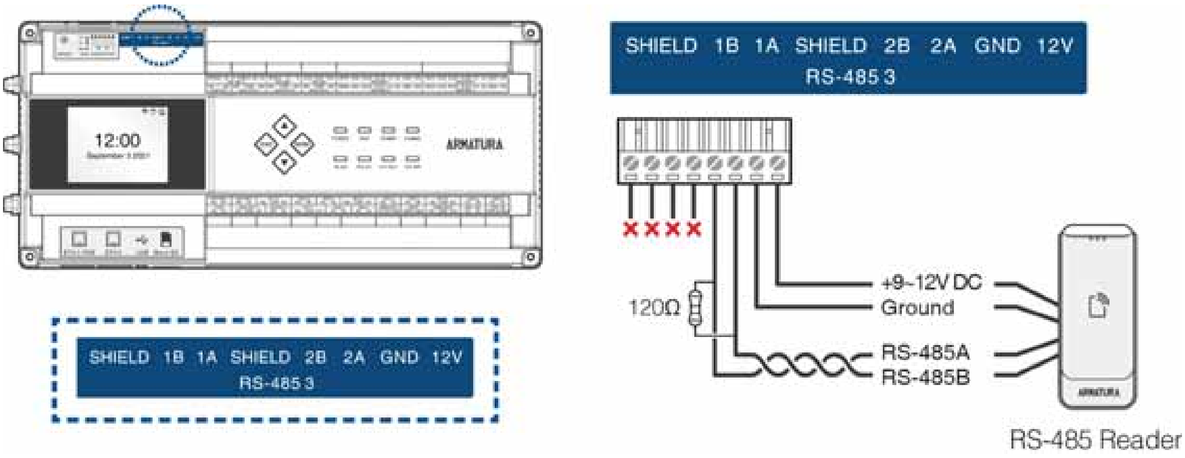
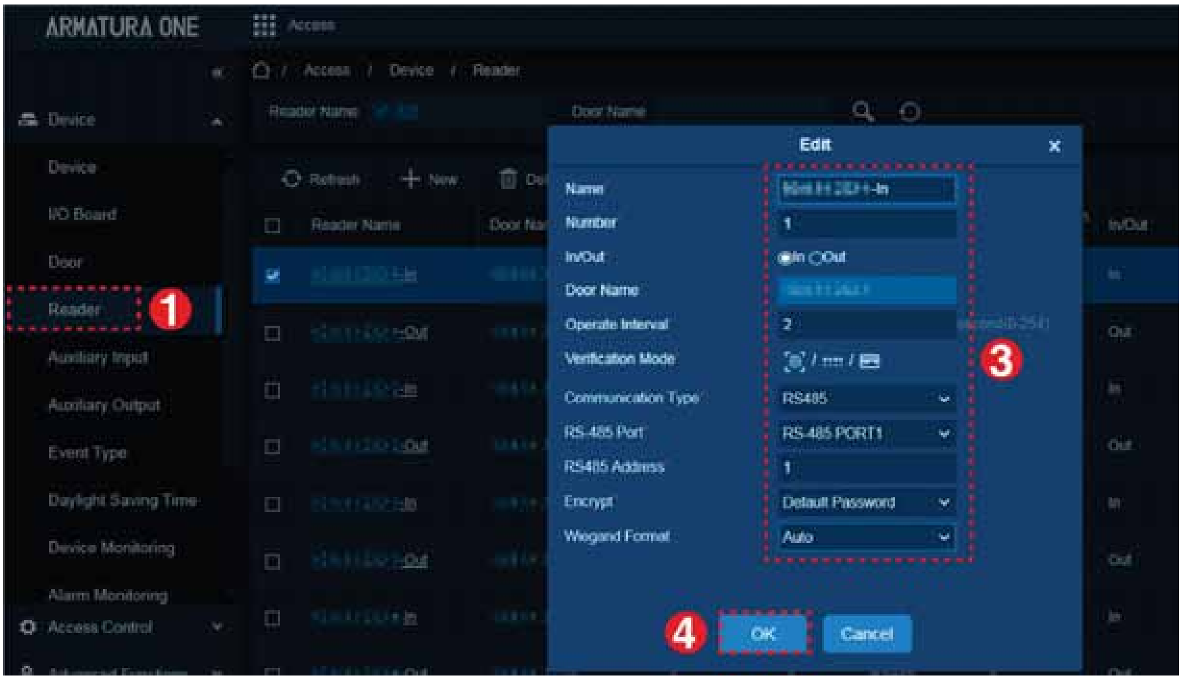


Figure 4-15 RS-485 Reader Wiring

Important Notes

When connecting the RS-485 reader, please operate in strict accordance with the following contents.

1. The RS-485 reader can support OSDP protocol, need to configure the parameters on the ARMATURA One software, and the modification path is **Access > Device > Reader > New**. As shown below:



Name: [illegible]-In
Number: 1
In/Out: ● In ○ Out
Door Name: [illegible]
Operate Interval: 2
Verification Mode:
Communication Type: RS485
RS-485 Port: RS-485 PORT1
RS485 Address: 1
Encrypt: Default Password
Wiegand Format: Auto

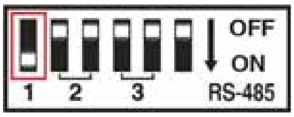
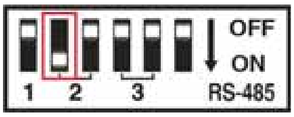
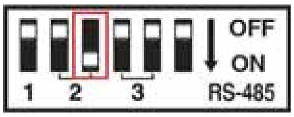
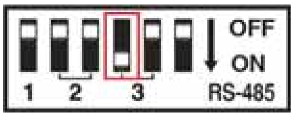
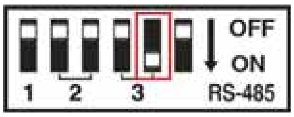
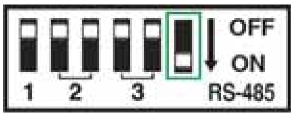
In the pop-up edit window, set each parameter of the RS-485 reader. Then click **OK** to complete the configuration.

- **RS-485 Port:** Select the port to which the RS-485 reader is connected.
- **RS485 Address:** The terminating resistor bit number corresponding to the RS-485 port.

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

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

4. When the communication distance is greater than or equal to **984ft (300m)**, you need to configure the EOL resistor of 485 through the dip switch to turn on the terminal enable. At the same time, you need to connect a **120 ohm** terminal matching resistor between the 485+ and 485- terminals of the most terminal device.

5. The following figure shows two ways of RS-485 reader connection.

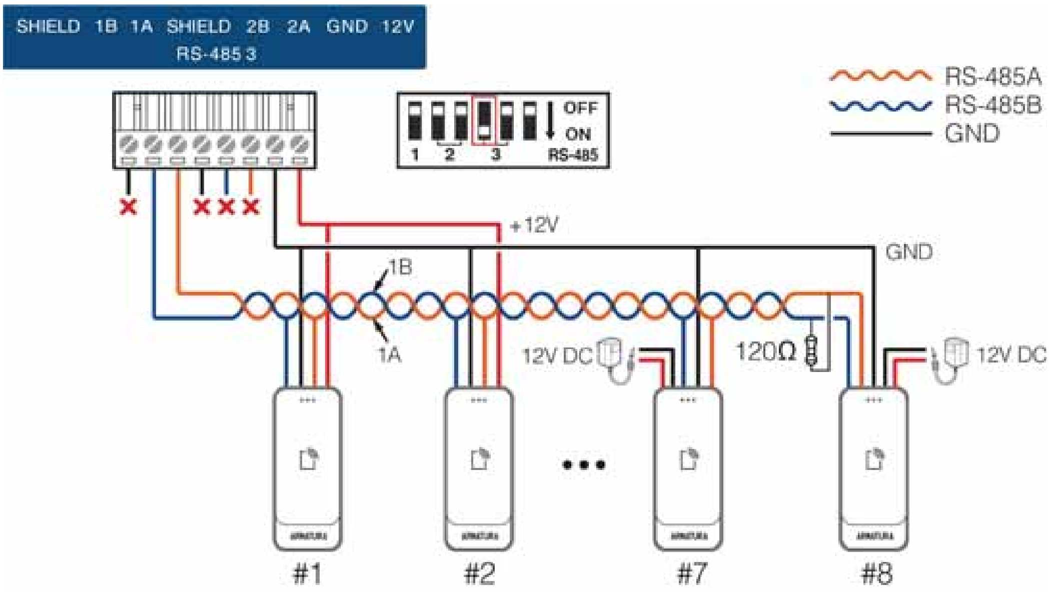


Figure 4-16 Hand-to-hand connection of controller and RS-485 readers

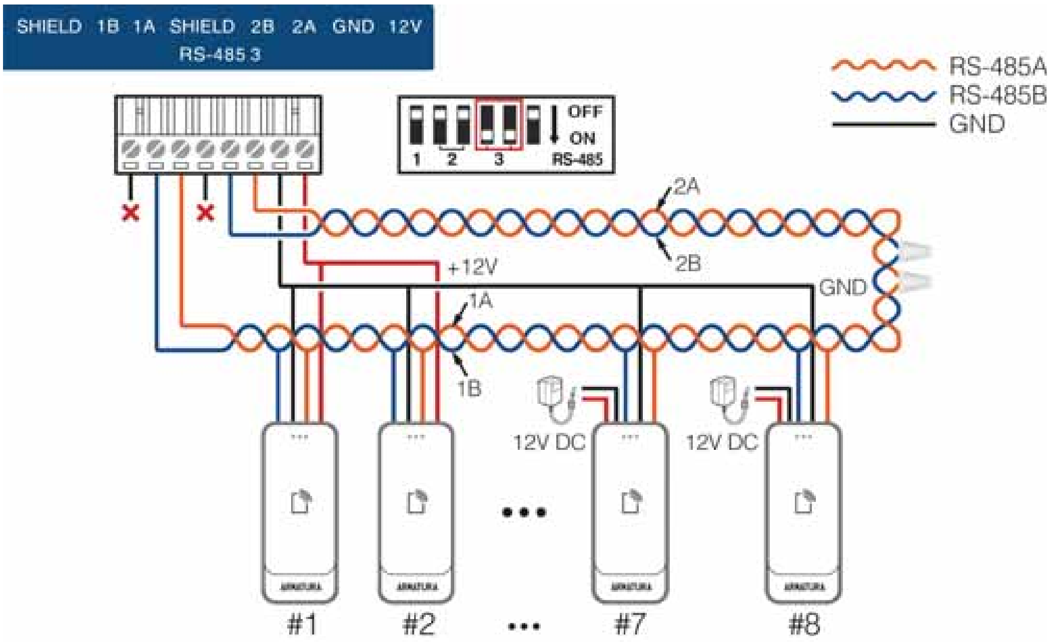


Figure 4-17 RS-485 redundancy backup connection of controller and RS-485 readers

Note:

1. *When connected using RS-485 redundant backup mode, the DIP switches of the connected ports must be turned to the **ON** position at the same time.*

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

4.3.10 I/O Board Wiring

4.3.10.1 Connect AHEB-0808 via RS-485

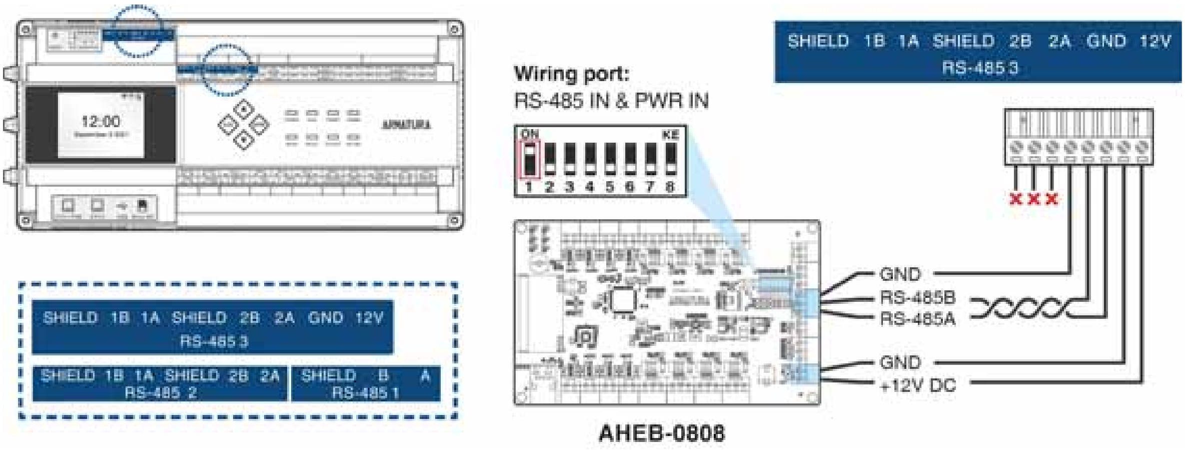


Figure 4-18 I/O Board Wiring

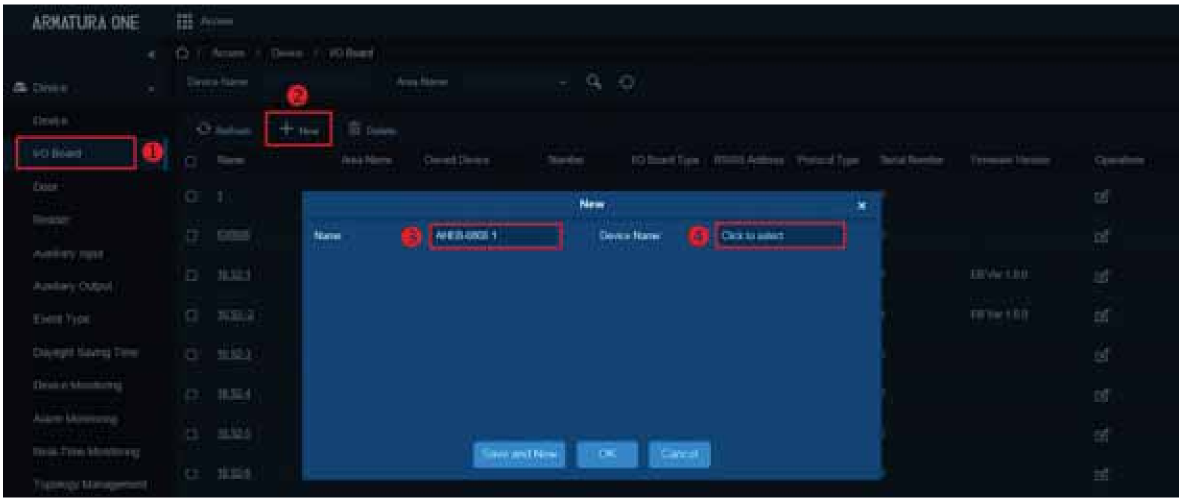
Operating Steps

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

1. Connect the AHEB-0808 to the AHSC-1000 or the AHDU-1X60 via RS-485. Can be connected to the RS-485 1, RS-485 2 and RS-485 3 wiring ports.

2. Log in to the ARMATURA One software with the current account and have the authority. And refer to 6.3 Add Device on the Software to add the controller on the software.

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

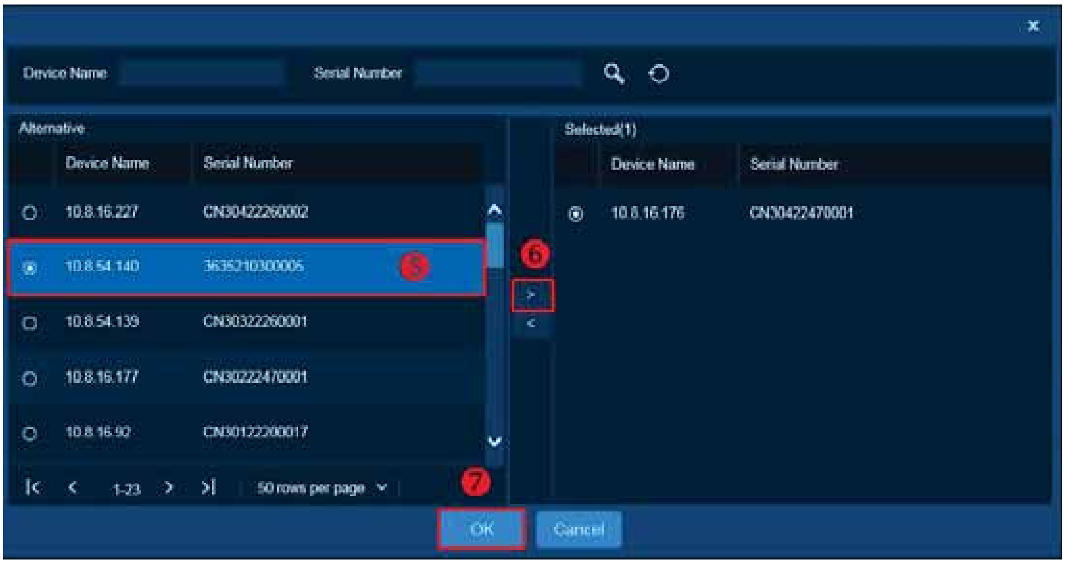


New

Name AHEB-0808 1

Device Name Click to select

4. Click **Device Name** to pop-up a device select window. Select the added controller, click **OK** to save and exit.



Device Name Serial Number

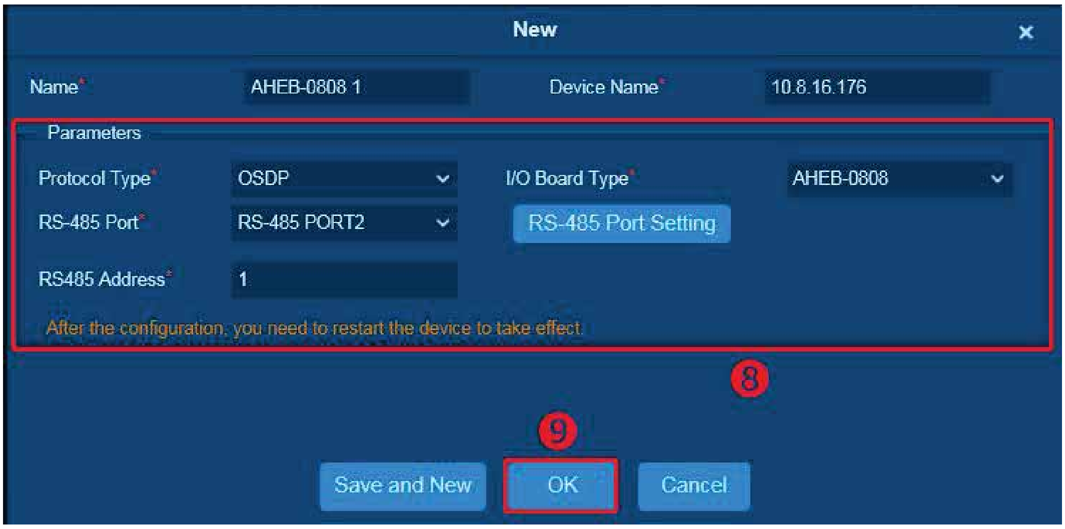
Alternative

	Device Name	Serial Number
○	10.8.16.227	CN30422260002
●	10.8.54.140	3635210300005
○	10.8.54.139	CN30322260001
○	10.8.16.177	CN30222470001
○	10.8.16.92	CN30122200017

Selected(1)

	Device Name	Serial Number
●	10.8.16.176	CN30422470001

5. Enter each parameter, click **OK** to save the expansion board.



New

Name* AHEB-0808 1

Device Name* 10.8.16.176

Parameters

Protocol Type* OSDP

I/O Board Type* AHEB-0808

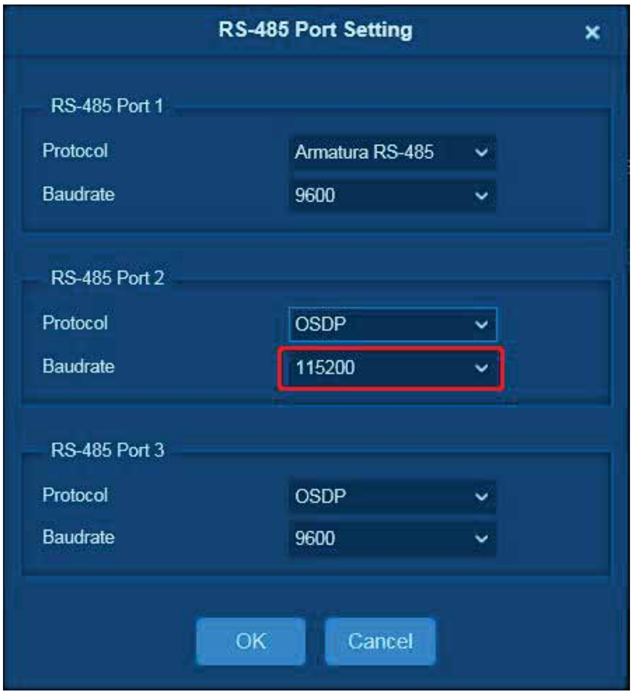
RS-485 Port* RS-485 PORT2

RS485 Address* 1

After the configuration, you need to restart the device to take effect.

- **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 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 is 115200.



RS-485 Port Setting

RS-485 Port 1

Protocol: Armatura RS-485

Baudrate: 9600

RS-485 Port 2

Protocol: OSDP

Baudrate: 115200

RS-485 Port 3

Protocol: OSDP

Baudrate: 9600

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 extended boards can be connected to each RS-485 port.

2. Each AHEB-0808 can connect a maximum of eight auxiliary input devices and eight auxiliary output devices.

3. Set the RS-485 addresses of each AHEB-0808 by the DIP switch before power is supplied.

4. The RS-485 interface can supply for maximum 3A (12V) current. So the entire current consumption should be less than this max value when the expansion boards share power with the panel. For calculation, please use max current of the expansion board, and starting current is usually more than twice of the normal work current, please consider this situation. Otherwise, it is recommended to power the expansion board separately.

5. The wiring for connecting multiple expansion boards is shown below.

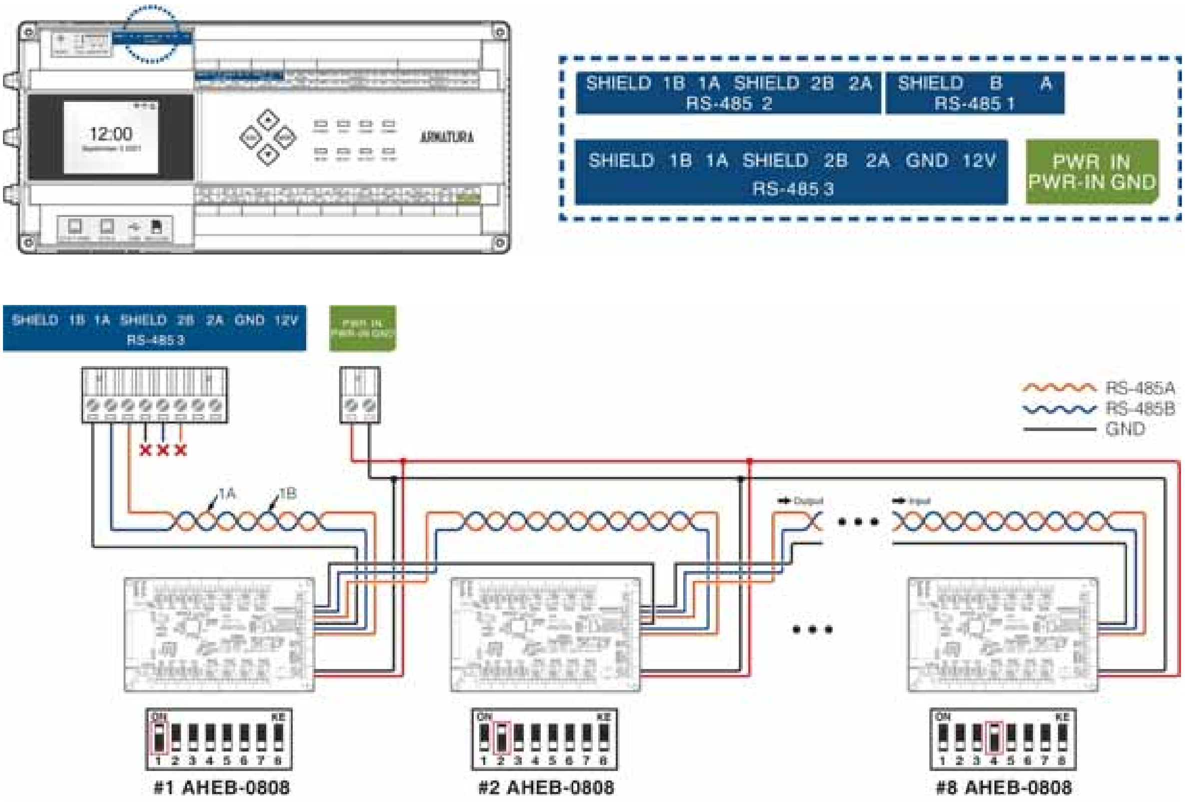


Figure 4-19 I/O Board Wiring

4.3.10.2 Connect Aperio AH30 hub to AHSC-1000 via RS-485

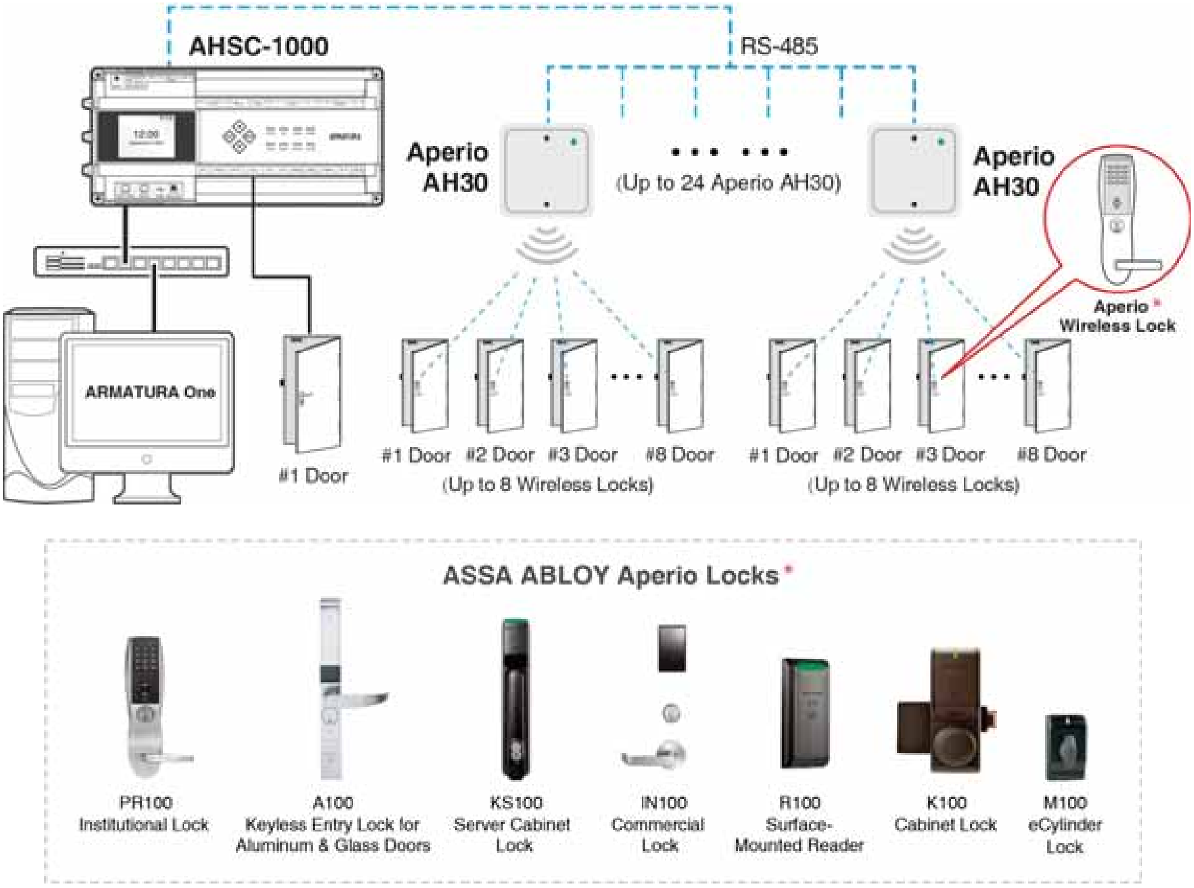
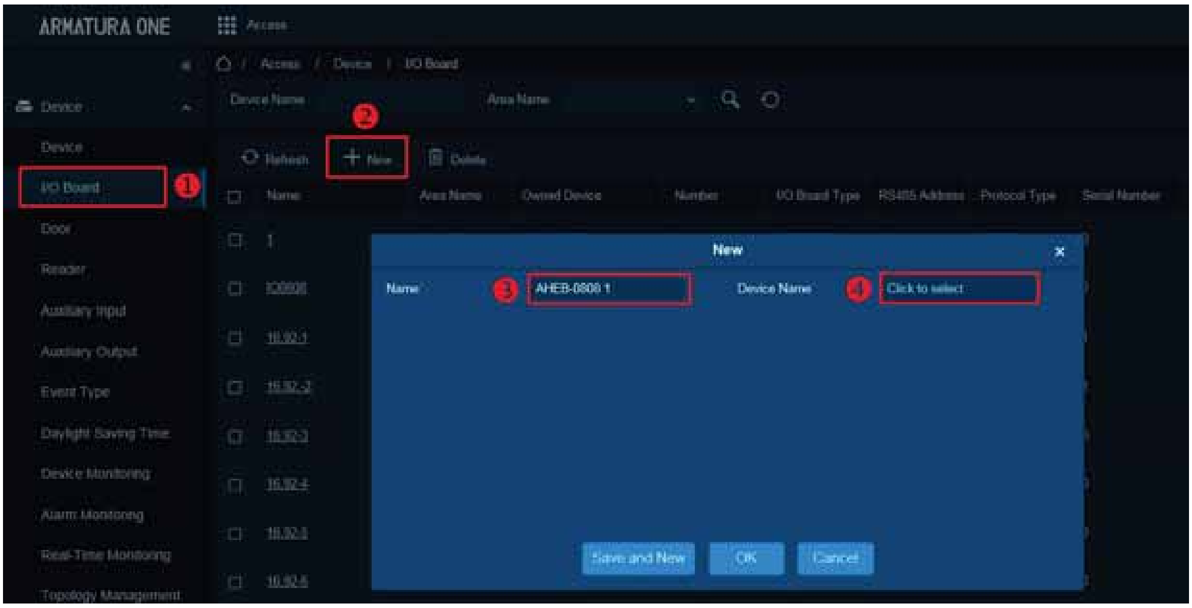


Figure 4-20 Aperio AH30 hub Wiring

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

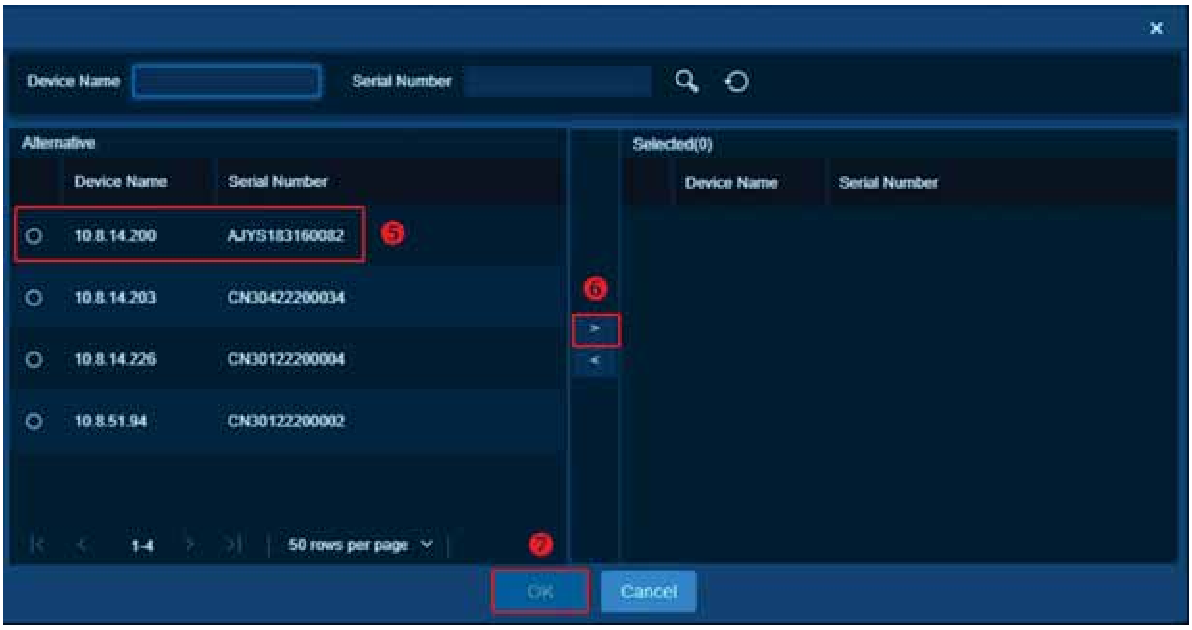
2. Enter **Name**.



Name: AHEB-0808 1

Device Name: Click to select

3. Click **Device Name** to pop-up a device select window. Select the added controller, click **OK** to save and exit.



Device Name | Serial Number

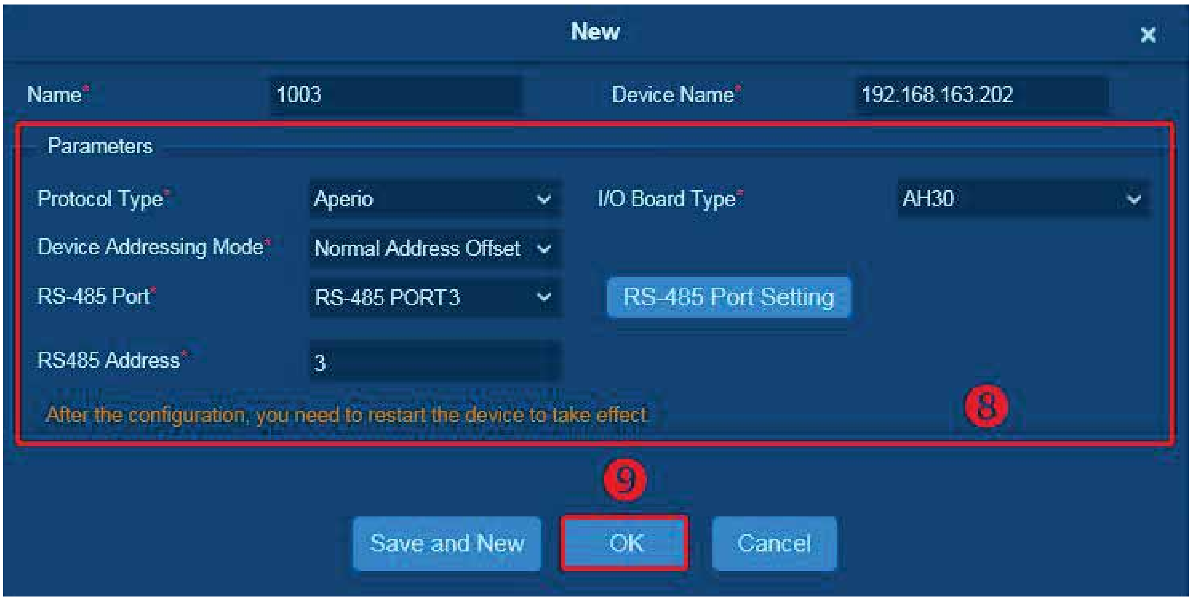
Alternative

	Device Name	Serial Number
○	10.8.14.200	AJYS183160082
○	10.8.14.203	CN30422200034
○	10.8.14.226	CN30122200004
○	10.8.51.94	CN30122200002

Selected(0)

Device Name	Serial Number

4. Enter each parameter.



New

Name*	1003	Device Name*	192.168.163.202

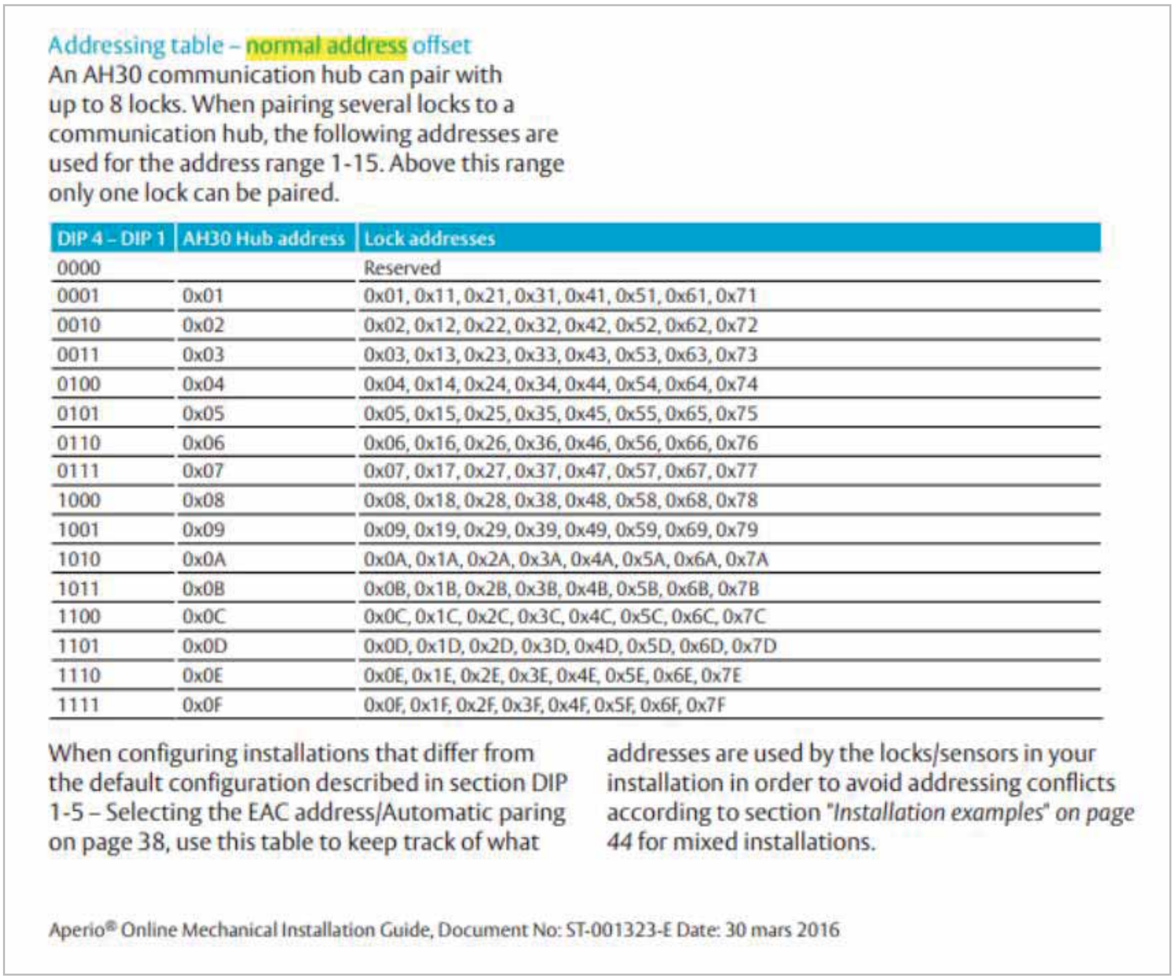
Parameters

Protocol Type*	Aperio	I/O Board Type*	AH30
Device Addressing Mode*	Normal Address Offset		
RS-485 Port*	RS-485 PORT3		
RS485 Address*	3		

After the configuration, you need to restart the device to take effect

- **Device Addressing Mode:**

➢ Normal Address Offset



Addressing table – normal address offset

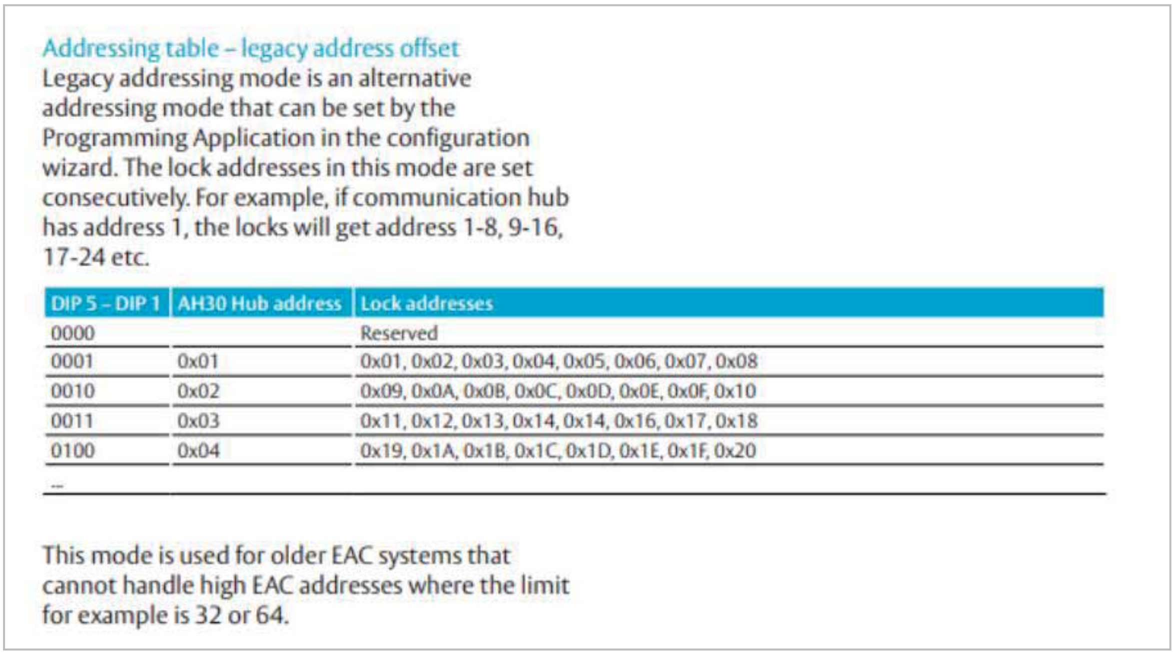
An AH30 communication hub can pair with up to 8 locks. When pairing several locks to a communication hub, the following addresses are used for the address range 1-15. Above this range only one lock can be paired.

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.

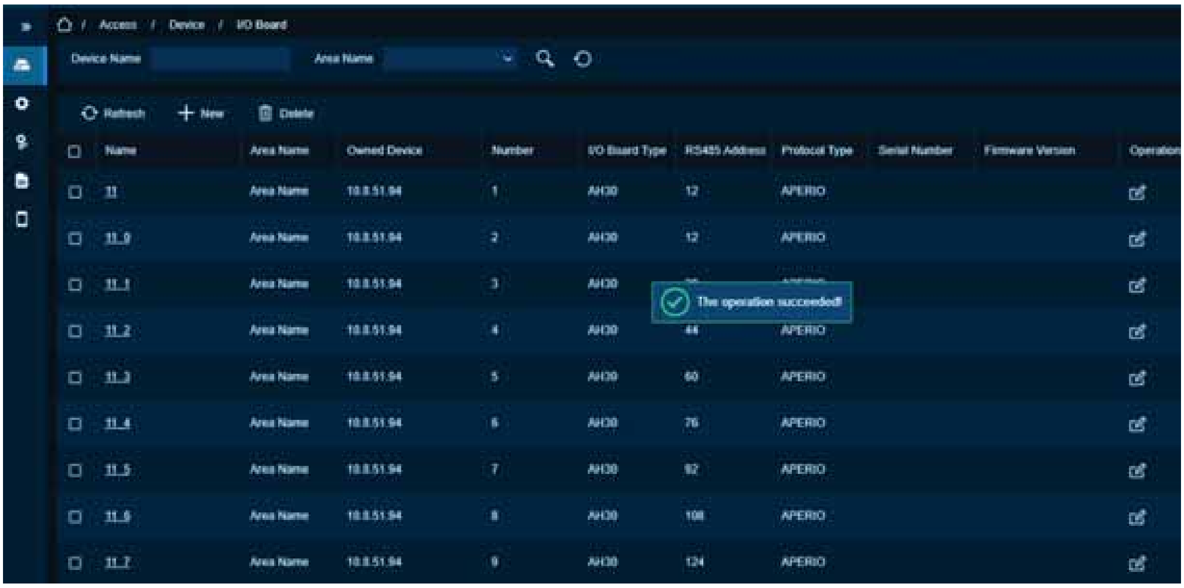
DIP 5 – DIP 1	AH30 Hub address	Lock addresses
0000		Reserved
0001	0x01	0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08
0010	0x02	0x09, 0x0A, 0x0B, 0x0C, 0x0D, 0x0E, 0x0F, 0x10
0011	0x03	0x11, 0x12, 0x13, 0x14, 0x14, 0x16, 0x17, 0x18
0100	0x04	0x19, 0x1A, 0x1B, 0x1C, 0x1D, 0x1E, 0x1F, 0x20
...		

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

Note: *Picture regards from ST-001323-Aperio Online Mechanical Installation Manual-E-US.pdf*

- **RS-485 Port:** System will filter via Protocol.
- **RS-485 Address:** The RS-485 address of Aperio AH30, range is from 1-15.

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



⌂ / Access / Device / I/O Board

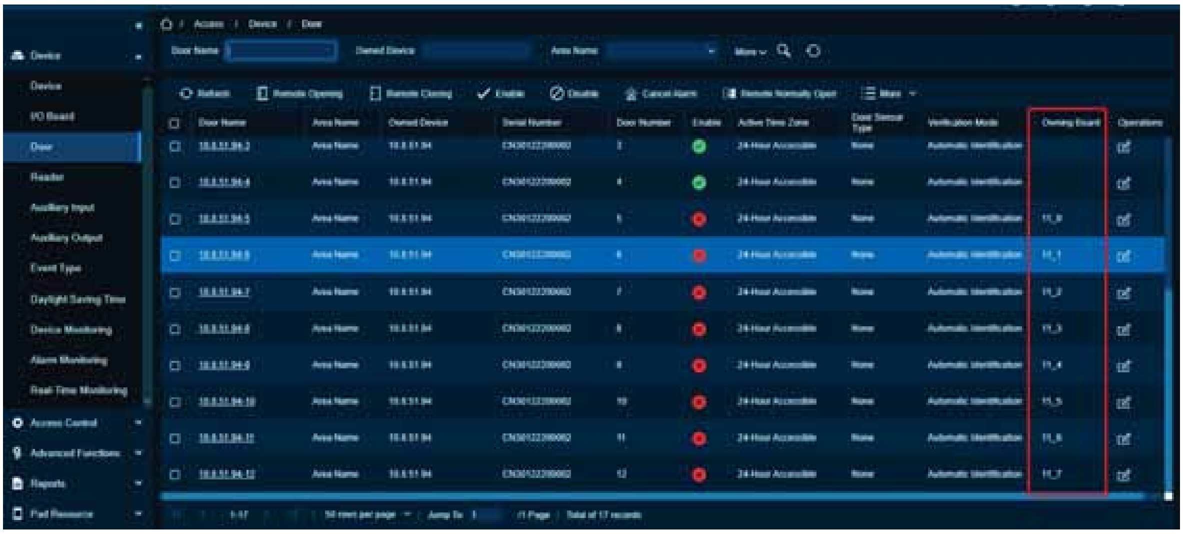
Device Name ______ Area Name ______

Refresh + New Delete

□	Name	Area Name	Owned Device	Number	I/O Board Type	RS485 Address	Protocol Type	Serial Number	Firmware Version	Operation
□	11	Area Name	10.8.51.94	1	AH30	12	APERIO			
□	11_0	Area Name	10.8.51.94	2	AH30	12	APERIO			
□	11_1	Area Name	10.8.51.94	3	AH30	[illegible]	[illegible]			
□	11_2	Area Name	10.8.51.94	4	AH30	44	APERIO			
□	11_3	Area Name	10.8.51.94	5	AH30	60	APERIO			
□	11_4	Area Name	10.8.51.94	6	AH30	76	APERIO			
□	11_5	Area Name	10.8.51.94	7	AH30	92	APERIO			
□	11_6	Area Name	10.8.51.94	8	AH30	108	APERIO			
□	11_7	Area Name	10.8.51.94	9	AH30	124	APERIO			

The operation succeeded!

6. System will generate several virtual devices in I/O Board.



⌂ / Access / Device / Door

Door Name ______ Owned Device ______ Area Name ______ More

Refresh Remote Opening Remote Closing Enable Disable Cancel Alarm Remote Normally Open More

□	Door Name	Area Name	Owned Device	Serial Number	Door Number	Enable	Active Time Zone	Door Sensor Type	Verification Mode	Owning Board	Operations
□	10.8.51.94-3	Area Name	10.8.51.94	CN30122200002	3	●	24-Hour Accessible	None	Automatic Identification		
□	10.8.51.94-4	Area Name	10.8.51.94	CN30122200002	4	●	24-Hour Accessible	None	Automatic Identification		
□	10.8.51.94-5	Area Name	10.8.51.94	CN30122200002	5	●	24-Hour Accessible	None	Automatic Identification	11_0	
□	10.8.51.94-6	Area Name	10.8.51.94	CN30122200002	6	●	24-Hour Accessible	None	Automatic Identification	11_1	
□	10.8.51.94-7	Area Name	10.8.51.94	CN30122200002	7	●	24-Hour Accessible	None	Automatic Identification	11_2	
□	10.8.51.94-8	Area Name	10.8.51.94	CN30122200002	8	●	24-Hour Accessible	None	Automatic Identification	11_3	
□	10.8.51.94-9	Area Name	10.8.51.94	CN30122200002	9	●	24-Hour Accessible	None	Automatic Identification	11_4	
□	10.8.51.94-10	Area Name	10.8.51.94	CN30122200002	10	●	24-Hour Accessible	None	Automatic Identification	11_5	
□	10.8.51.94-11	Area Name	10.8.51.94	CN30122200002	11	●	24-Hour Accessible	None	Automatic Identification	11_6	
□	10.8.51.94-12	Area Name	10.8.51.94	CN30122200002	12	●	24-Hour Accessible	None	Automatic Identification	11_7	

1-17 50 rows per page Jump To 1 /1 Page Total of 17 records

7. System will generate several doors which are bound to owning board which is auto generate in I/O Board Page.

Remarks:

1. Only AHSC-1000 supports connection Aperio AH30.
2. **Feature Trigger Result:** Will create several virtual I/O Boards in [I/O Board] and Virtual Doors in [Door].

4.3.11 Line Monitoring

This device supports monitoring the status of lines such as door sensor, exit button, and auxiliary input (such as alarm inputs). It includes four types of line status such as open, closed, short circuit and broken circuit. Open and closed are the normal switching states of the line.

As shown in the figure below, when short circuit, the lines in position 1 and 2 are connected; when broken circui, the line in position 1 or 2 is disconnected.

***Note*：**

The line monitoring feature requires two resistors on the door sensort, exit button and auxiliary input lines. Custom end of line (EOL) resistances may be configured via the host software. Support 1.2K, 2.2K, 4.7K, 10K resistors.

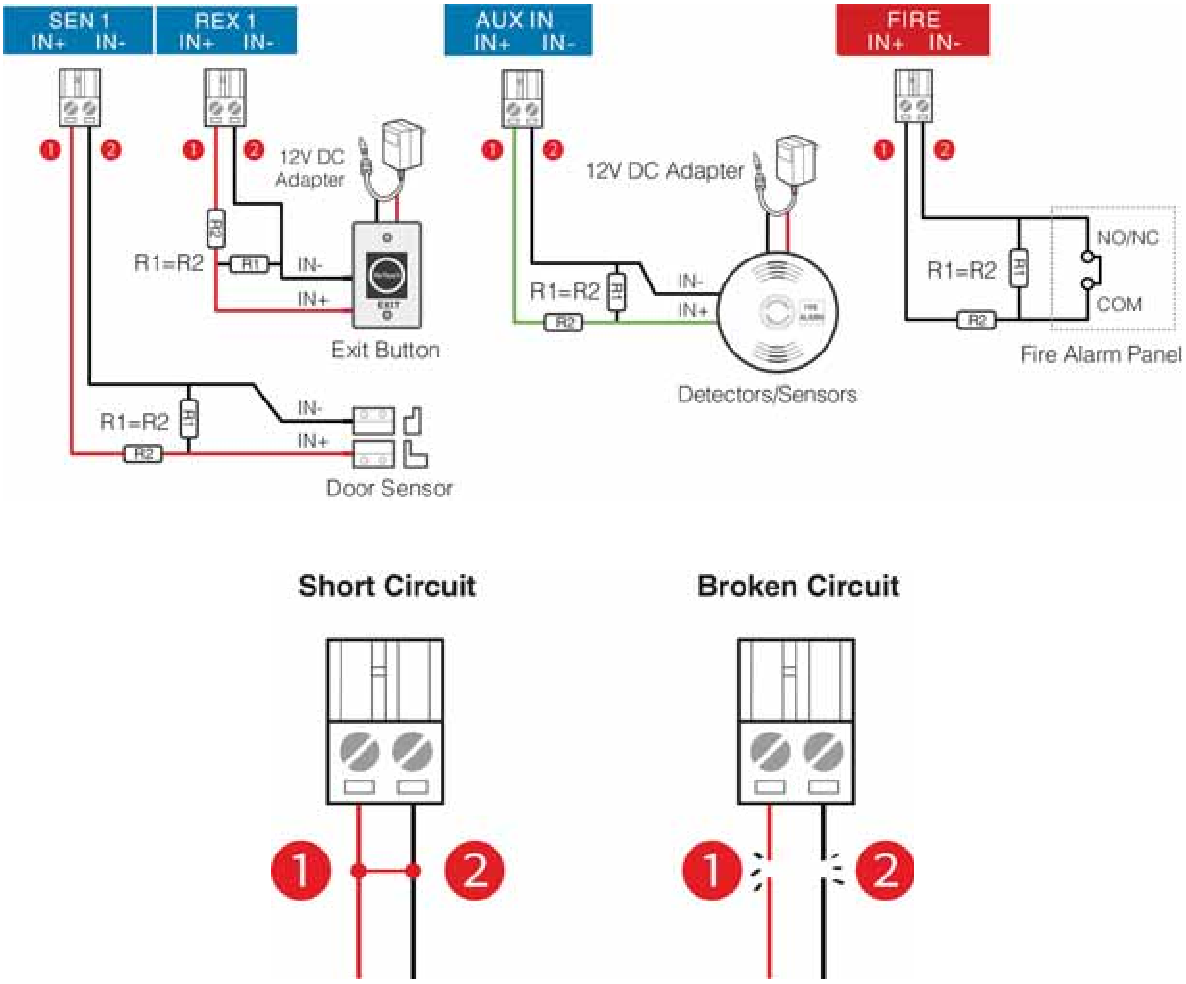


Figure 4-21 Line monitoring diagram

5. Equipment Communication

The background PC software is able to communicate with the system according to two protocols (TCP/IP and WiFi) for data exchange and remote management.

5.1 Access Control Networking Wires and Wiring

1. The power supply is 12V DC converted from 220V or PoE.

2. The Wiegand readers use 6-core communication shielded wires (RVVSP 6×0.5mm) (usually there are 6-core, 8-core, and 10-core available for users to select according to the ports) to reduce interference during transmission.

3. As an electronic lock has a big current, it generates strong interference signal while functioning. To reduce such an effect, 4-core wires (RVVP 4×0.75mm^2, two for a power supply and two for a door sensor) are recommended.

4. The RS-485 readers use 4-core communication shielded wires (RVVSP 4×0.5mm).

5. Other control cables (like exit switches) are all made of 2-core wires (RVVSP 2×0.5mm^2).

6. Notes for wiring:

   - Signal wires (like network cables) can neither run in parallel with nor share one casing pipe with large-power electric wires (like electronic lock wires and power cables). If parallel wiring is unavoidable for environmental reasons, the distance must be over 50cm.

   - Try to avoid using any conductor with a connector during distribution. When a connector is indispensable, it must be crimped or welded. No mechanical force can be applied to the joint or branch of conductors.

   - In a building, distribution lines must be installed horizontally or vertically. They should be protected in casing pipes (like plastic or iron water pipes, to be selected according to the technical requirements of indoor distribution). Metal hoses are applicable to ceiling wiring, but must be secure and good-looking.

   - Shielding measures and shielding connection: If the electromagnetic interference in the wiring environment is found strong in the survey before construction, it is necessary to consider shielding protection for data cables when designing a construction scheme. Overall shielding protection is required if there is a large radioactive interference source or wiring has to be parallel with a large-current power supply on the construction site. Generally, shielding measures include: keeping a maximum distance from any interference source, and using 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. Noted that a shielding enclosure can have a shielding effect only when it is grounded reliably.

   - Ground wire connection method: Reliable large-diameter ground wires in compliance with applicable national standards are needed on the wiring site, and should be connected in a tree form to avoid DC loop. These ground wires must be kept far away from lightning fields. No lightning conductor can serve as a ground wire, and ensure there is no lightning current through any ground wire when there is lightning. Metal wiring troughs and pipes must be connected continuously and reliably, and linked to ground wires through large-diameter wires. The impedance of this section of wire cannot exceed 2ohm. Also the shielding layer must be connected reliably, and grounded at one end to guarantee uniform current direction. The ground wire of the shielding layer must be connected through a large-diameter wire (not smaller than 2.5mm^2).

5.2 TCP/IP Communication

100BASE-TX: Twisted pair, use two unshielded twisted pair or two Category 1 shielded twisted pair connection, transmission distance of 328ft(100m). 256bit AES* symmetric encryption for Controller to Server and Inter-Controller communications.

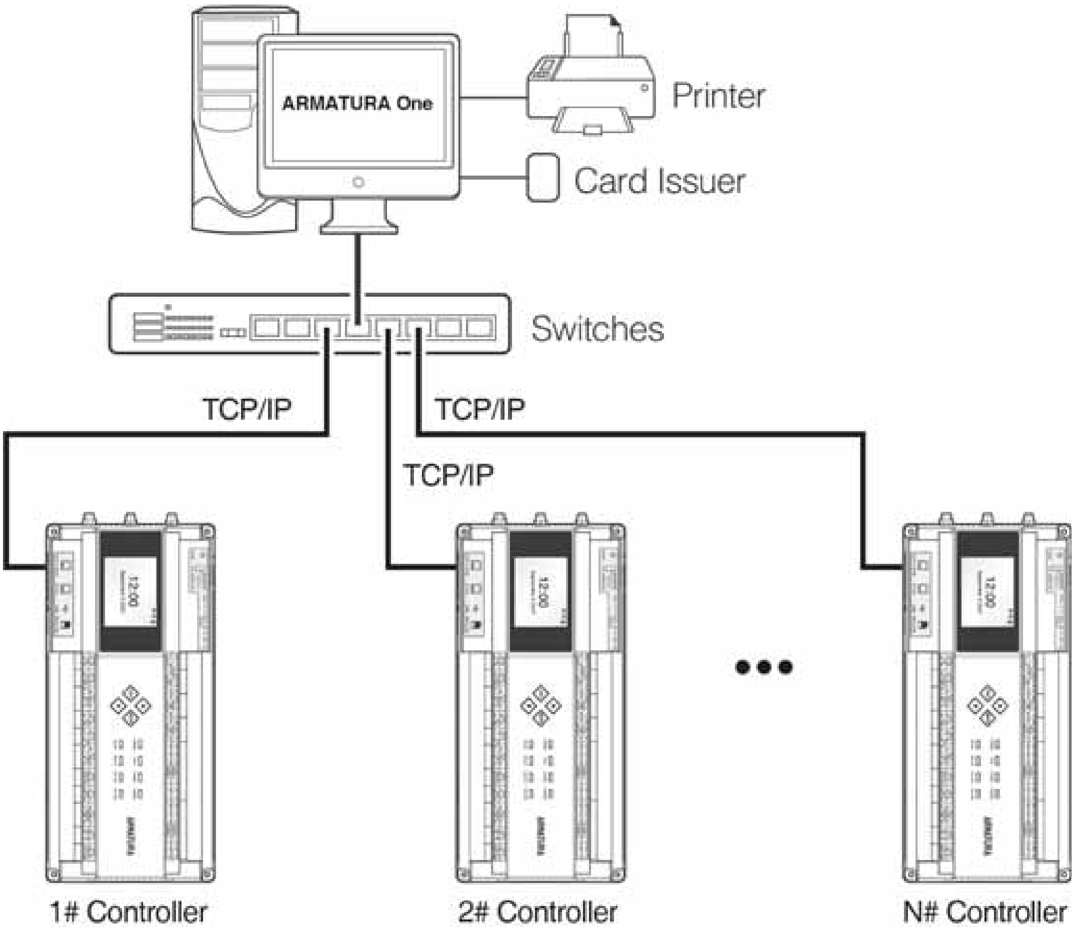


Figure 5-1 TCP/IP Communication System Networking

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

5.3 Configure network on the Webserver

Installation maintenance personnel or system maintenance personnel can do the following by accessing the device's webserver.

1) Configure the network and connect to the software server.

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

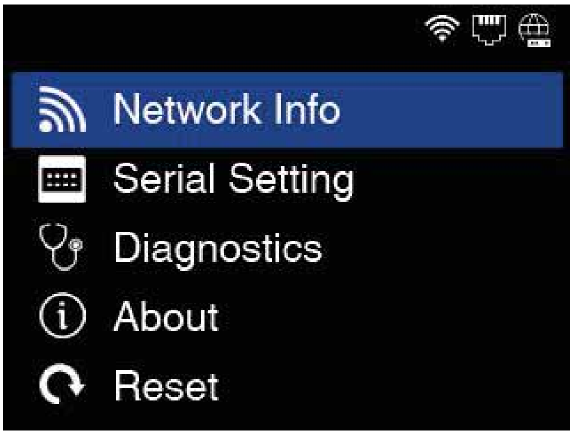
3) Carry out equipment maintenance, can pull debugging records, remotely initialize, reset parameters, restart equipment, etc.

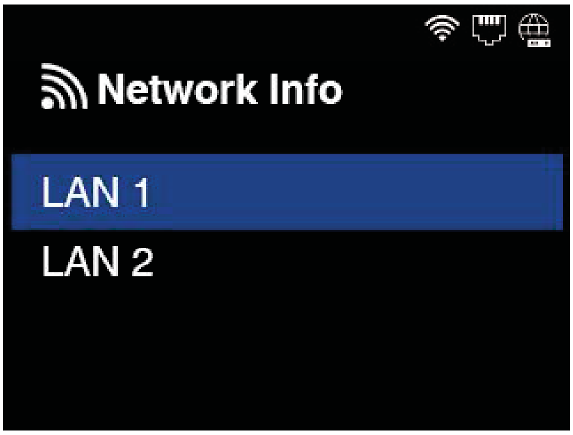
5.3.1 Opening the Webserver on the Browser

After the controller is powered on, connect the controller 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:

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

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



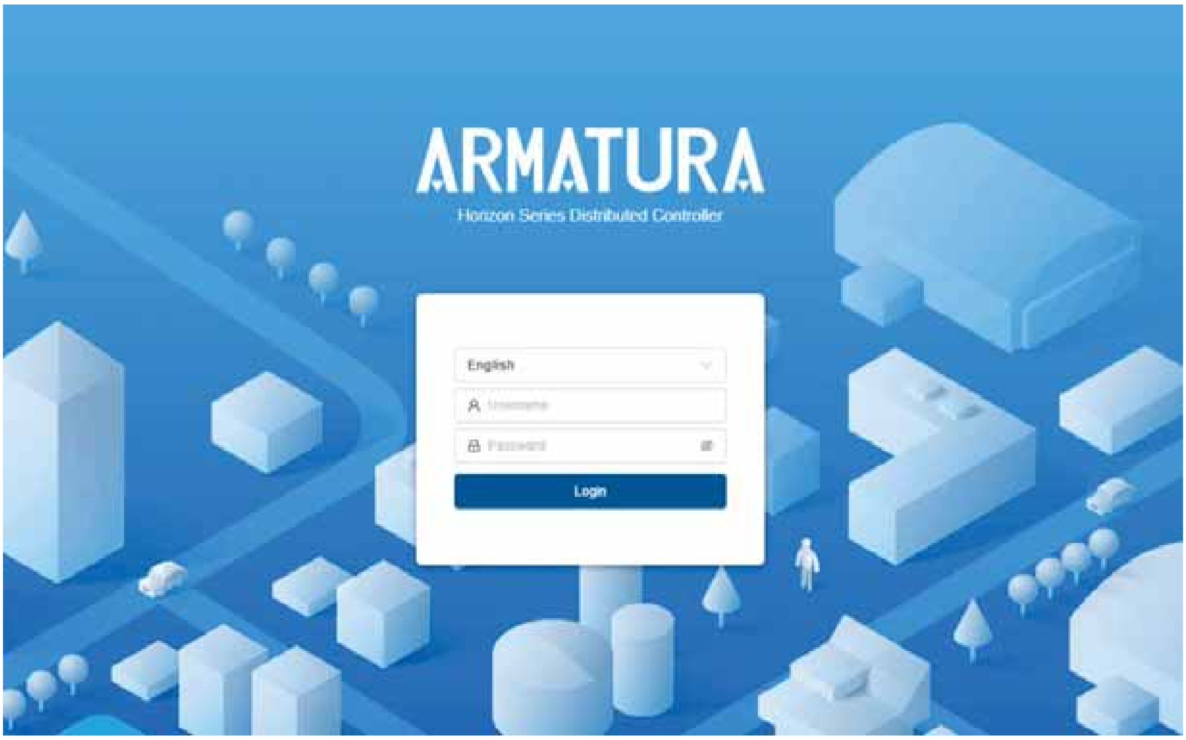


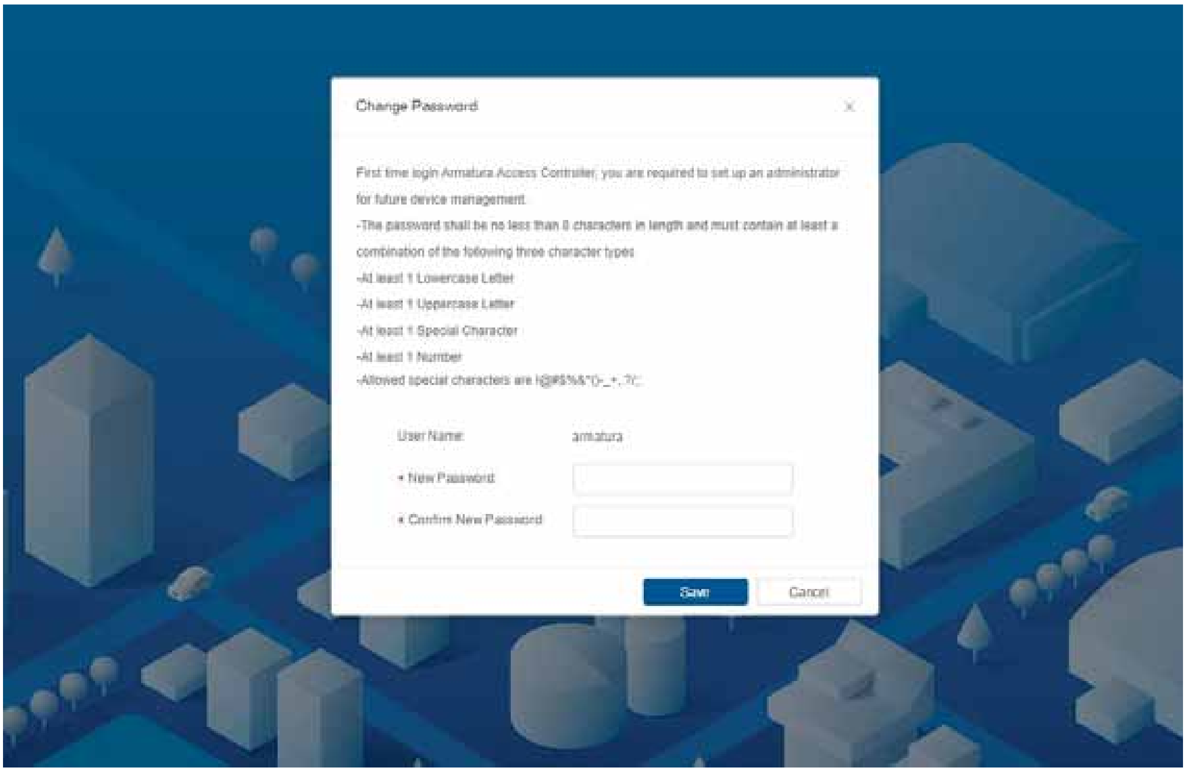
Status of Icons:

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.

5.3.2 Login to the Webserver

Open the login interface and enter the default administrator account and password (default is **armatura**), then click **Login**. First time login webserver, you are required to modify admin's password for future device management.





Change Password

First time login Armatura Access Controller, you are required to set up an administrator for future device management.

-The password shall be no less than 8 characters in length and must contain at least a combination of the following three character types

-At least 1 Lowercase Letter

-At least 1 Uppercase Letter

-At least 1 Special Character

-At least 1 Number

-Allowed special characters are !@#$%&*()-_+.,?/:

User Name: armatura

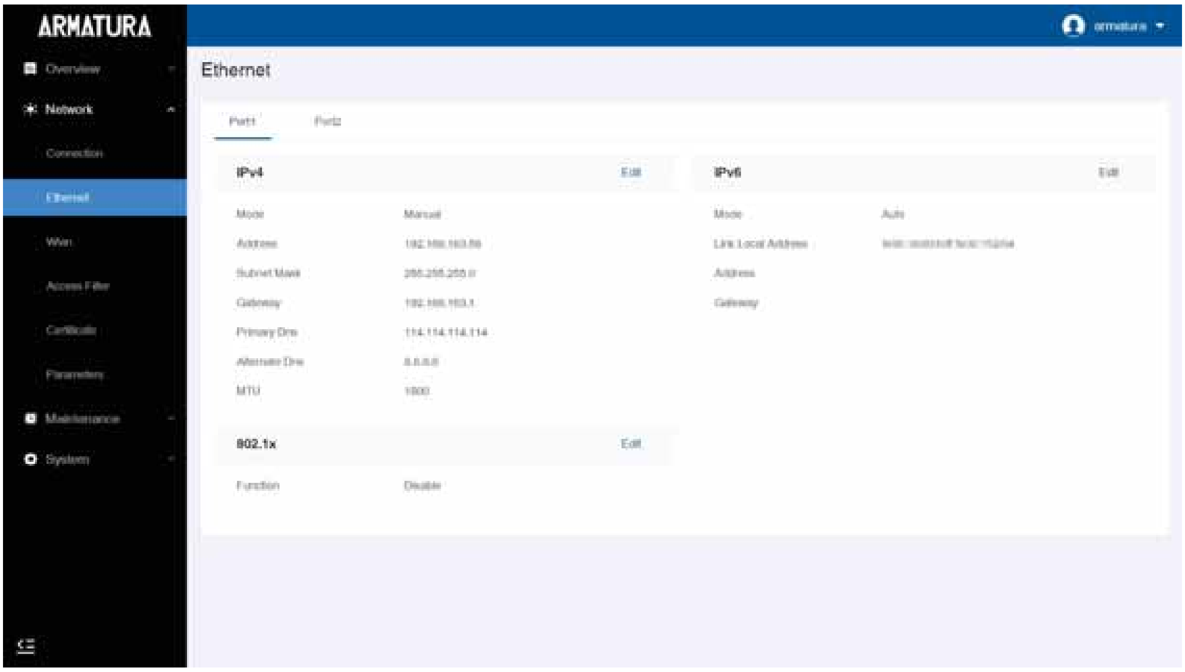
* New Password:

* Confirm New Password:

5.3.3 TCP/IP Settings

ARMATURA Horizon Controller has dual Ethernet interfaces, and IP addresses of Port 1 and Port 2 need to be configured. The gateways of Port 1 and Port 2 cannot be the same, and the IP addresses also need to be distinguished. When the controller is connected to a TCP/IP reader, the IP address of the expansion network card needs to be set.

Click **Network > Ethernet** to enter the setting interface. To modify the IP address and gateway address. As shown below.



Ethernet

IPv4

Mode Manual
Address 192.168.163.88
Subnet Mask 255.255.255.0
Gateway 192.168.163.1
Primary Dns 114.114.114.114
Alternate Dns 8.8.8.8
MTU 1500

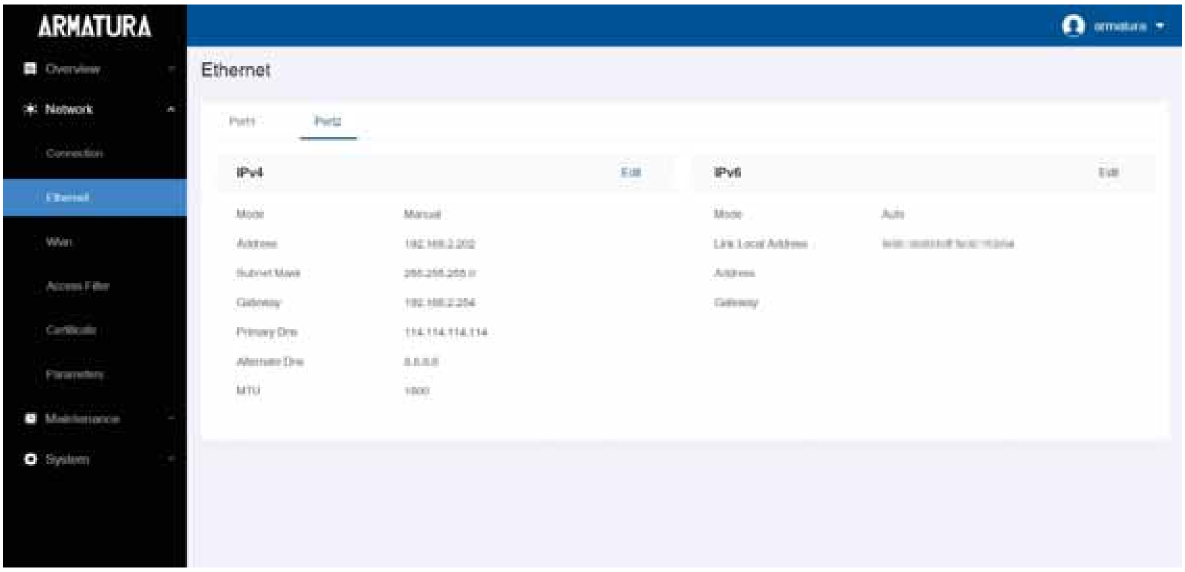
IPv6

Mode Auto
Link Local Address [illegible]
Address
Gateway

802.1x

Function Disable

The parameters of IPv4, IPv6, and 802.1x can be configured under the Port1 page.



Ethernet

IPv4

Mode Manual
Address 192.168.2.202
Subnet Mask 255.255.255.0
Gateway 192.168.2.254
Primary Dns 114.114.114.114
Alternate Dns 8.8.8.8
MTU 1500

IPv6

Mode Auto
Link Local Address [illegible]
Address
Gateway

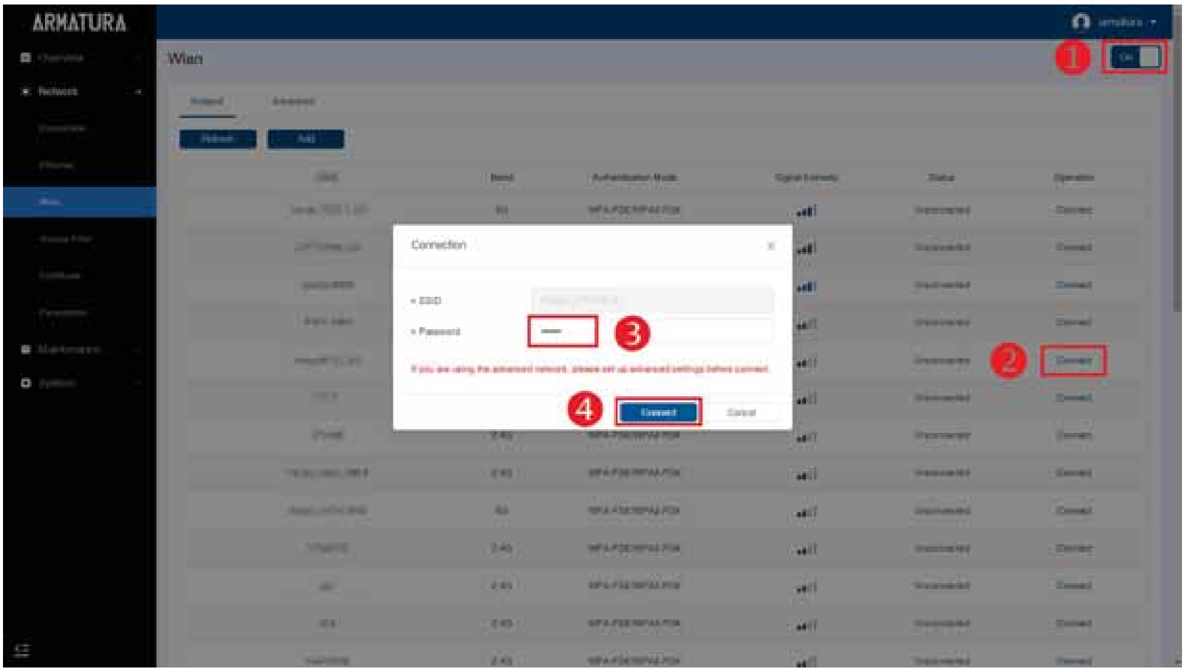
The parameters of IPv4 and IPv6 can be configured under the Port2 page.

5.3.4 Wireless Network Settings

The Wi-Fi module realizes data transmission through the Wi-Fi antenna and establishes a wireless network environment. Wi-Fi is enabled by default in the controller. If you don't need to use the Wi-Fi network, you can toggle the Wi-Fi to enable or disable the 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.
2. Once the Wi-Fi is turned on, the controller will automatically search for the available Wi-Fi within the network range.
3. Select the required Wi-Fi name from the available list and click **Connect**, and then input the correct password in the pop-up password interface, and click **Connect** when complete.

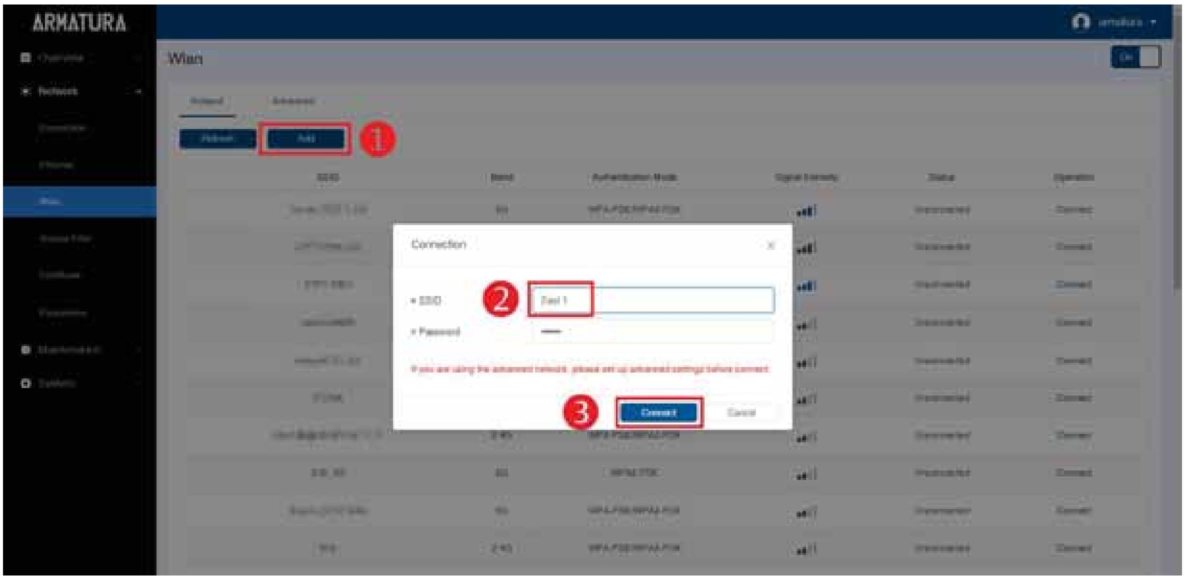


4. When the Wi-Fi is connected successfully, the Wi-Fi status shows as **Connected**.

Adding Wi-Fi Network Manually

The Wi-Fi can also be added manually if the required 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.)



Connection

- * SSID: Test 1
- * Password: ——

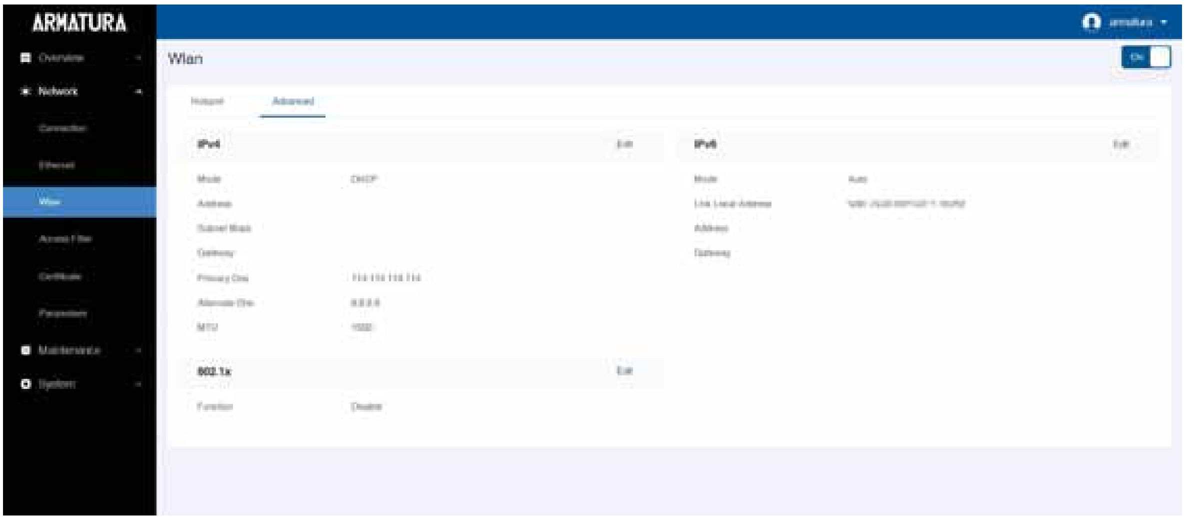
If you are using the advanced network, please set up advanced settings before connect

Connect

Note: *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 **Advanced** to set the relevant parameters as required. The parameters of IPv4, IPv6 and 802.1x can be configured in the advanced setting interface.



IPv4

- Mode: DHCP
- Address
- Subnet Mask
- Gateway
- Primary Dns: 114.114.114.114
- Alternate Dns: 8.8.8.8
- MTU: 1500

IPv6

- Mode: Auto
- Link Local Address: [illegible]
- Address
- Gateway

802.1x

- Function: Disable

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.*

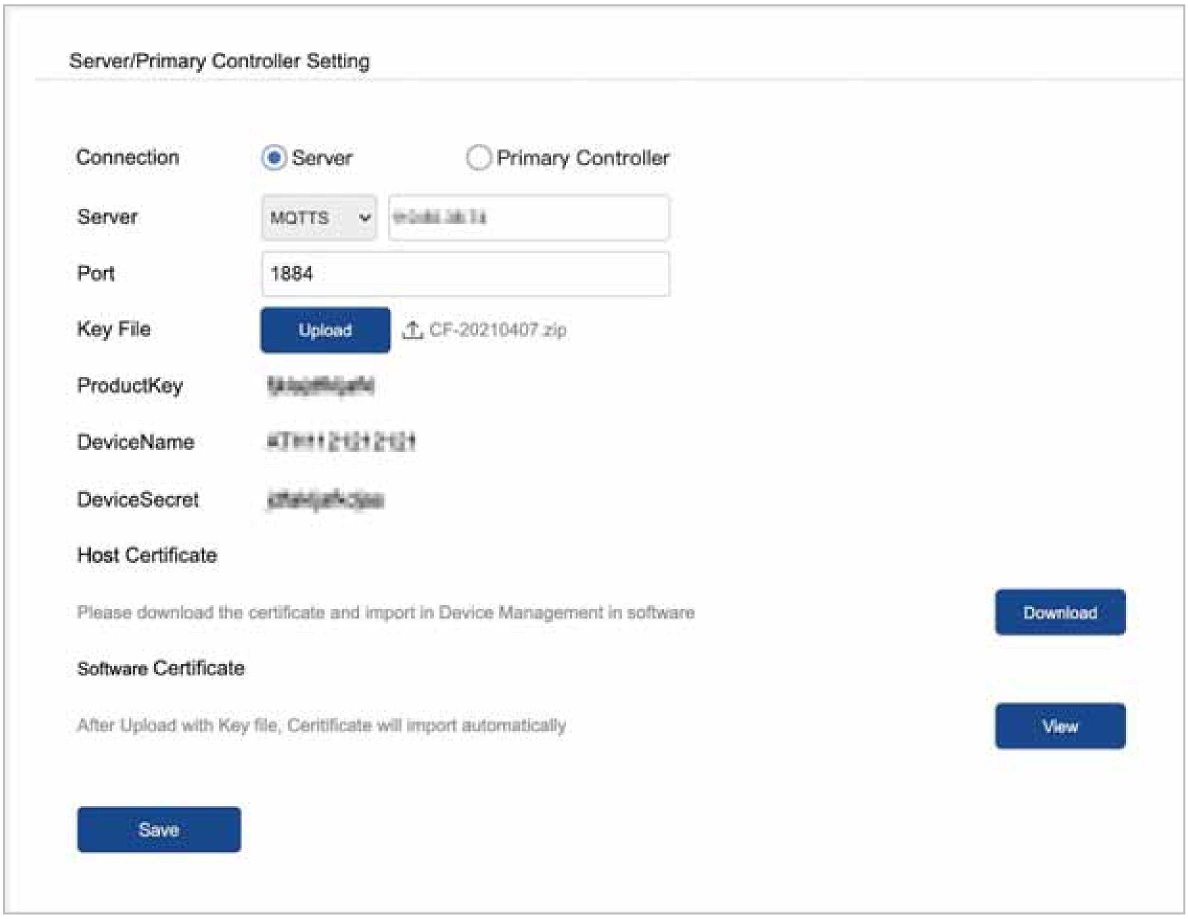
3. *Connect the PC with the software installed to the router and set the same network segment to allow the control panel to communicate with the PC and background software through Wi-Fi.*

5.3.5 Setting up the Server/Primary Controller

Armatura Horizon Controller can only be configured with either server/primary controller.

Click **Network > Connection** to enter the Server/Primary Controller Setting interface on the webserver.

Server Connection Configuration



Server/Primary Controller Setting

Connection ● Server ○ Primary Controller

Server MQTTS [redacted]

Port 1884

Key File CF-20210407.zip

ProductKey [redacted]

DeviceName [redacted]

DeviceSecret [redacted]

Host Certificate

Please download the certificate and import in Device Management in software

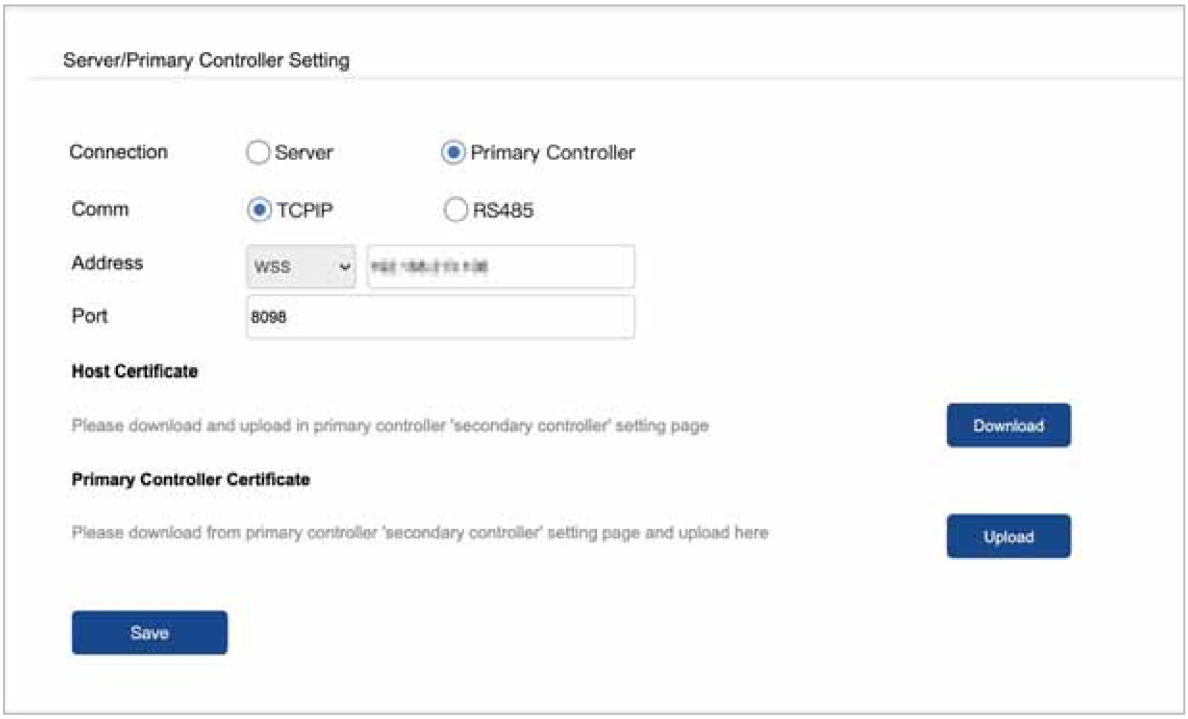
Software Certificate

After Upload with Key file, Ceritificate will import automatically

- **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. Other relevant information will be backfilled automatically.
- **Host Certificate:** For two-way authentication, you need to download the controller certificate and import it into the software, and the default is one-way authentication.
- **Software Certificate:** To view the software certificate.

Primary Controller Connection

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



Server/Primary Controller Setting

Connection ○ Server ● Primary Controller

Comm ● TCPIP ○ RS485

Address wss [redacted]

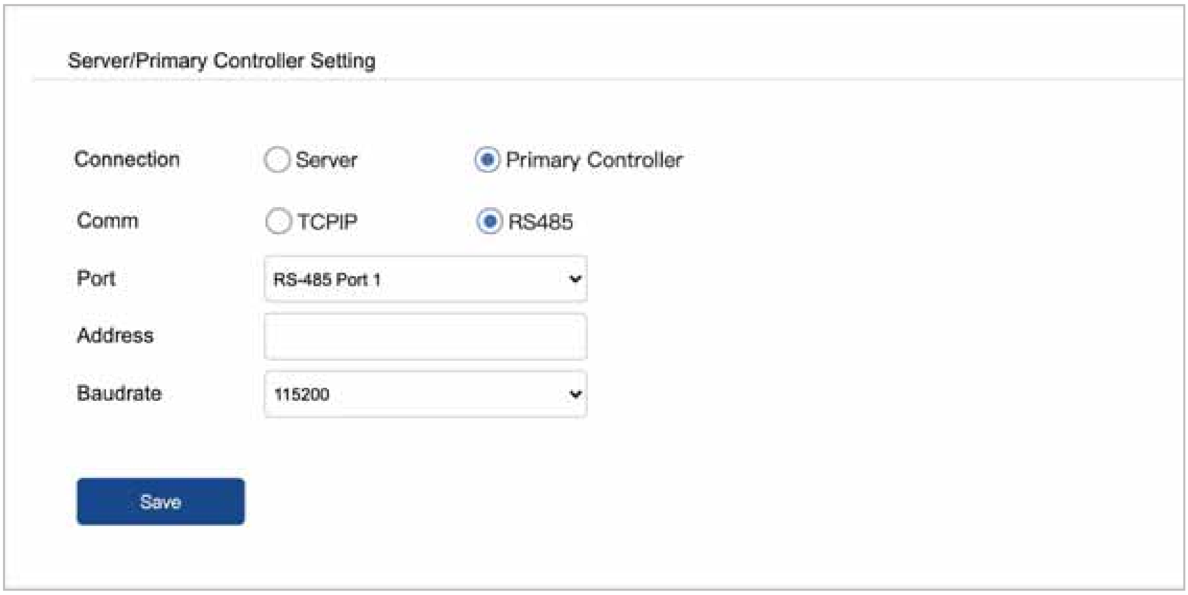
Port 8098

Host Certificate

Please download and upload in primary controller 'secondary controller' setting page

Primary Controller Certificate

Please download from primary controller 'secondary controller' setting page and upload here



Server/Primary Controller Setting

Connection ○ Server ● Primary Controller

Comm ○ TCPIP ● RS485

Port RS-485 Port 1

Address

Baudrate 115200

6. Connect to the ARMATURA One Software

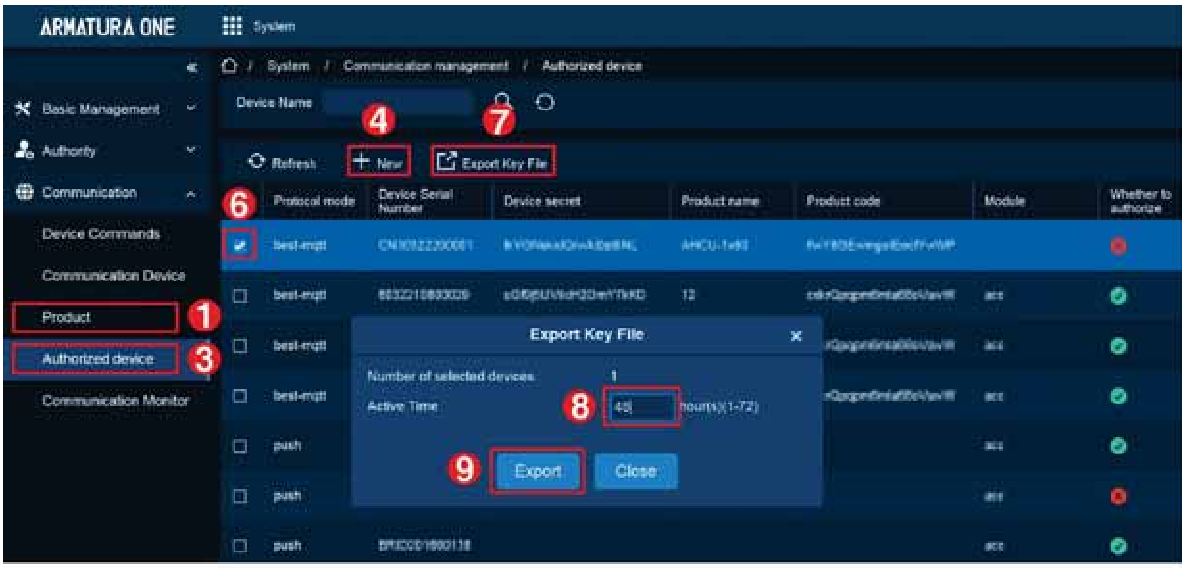
6.1 Export the Key File

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. Check the device key to be exported, click **Export Key File**, and fill in the active time, then click **Export**. You will get a key file.



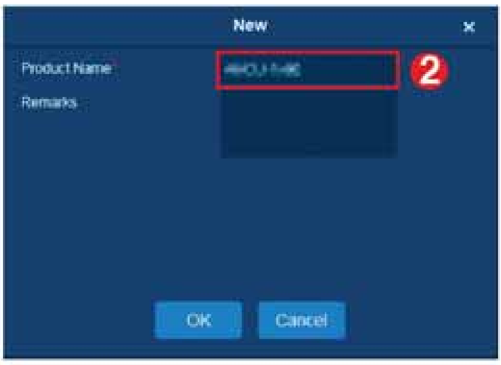
	Protocol mode	Device Serial Number	Device secret	Product name	Product code	Module	Whether to authorize
☑	best-mqtt	CN10322200001	[illegible]	AHCU-1x80	[illegible]		●
□	best-mqtt	6532210830029	[illegible]	12	[illegible]	acc	✓
□	best-mqtt				[illegible]	acc	✓
□	best-mqtt				[illegible]	acc	✓
□	push					acc	✓
□	push					acc	●
□	push	BRCC011800138				acc	✓

Export Key File

Number of selected devices 1

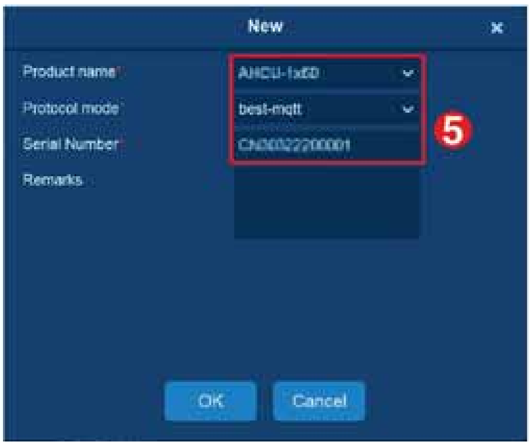
Active Time 48 hour(s)(1-72)

Export Close



Product Name AHCU-1x80

Remarks



Product name* AHCU-1xED

Protocol mode* best-mqtt

Serial Number* CN30322200001

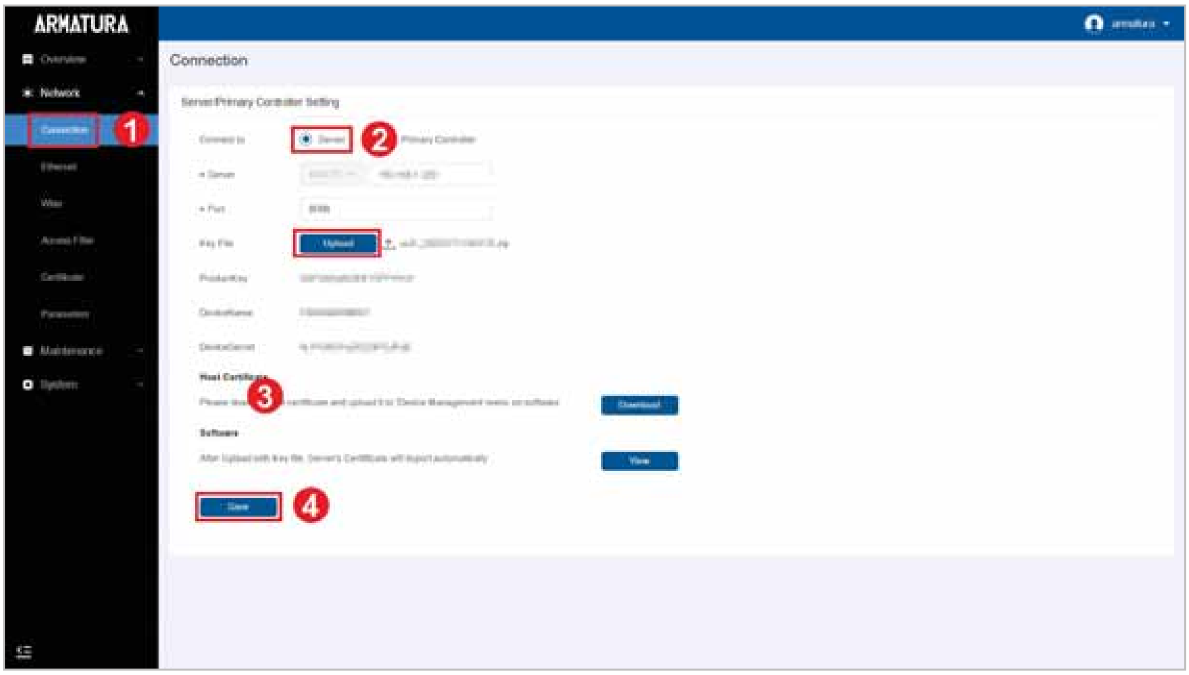
Remarks

6.2 Server Connection Configuration

1. Click **Network > Connection >** select **Server** to enter the Server/Primary 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**.



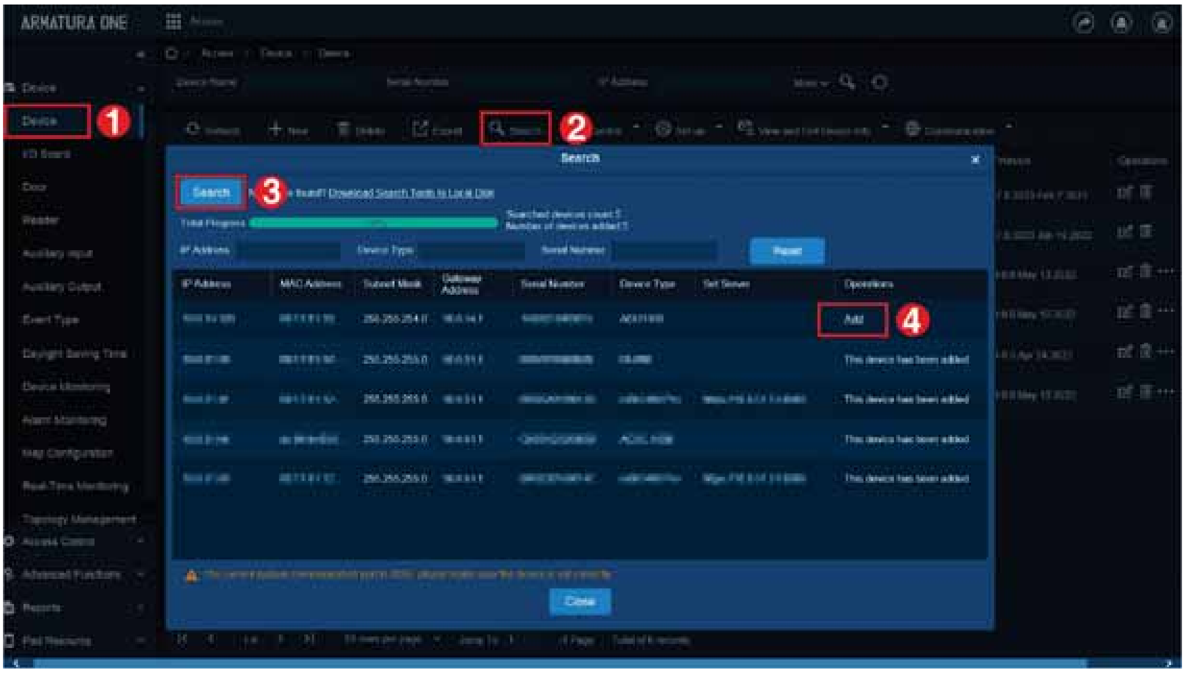
6.3 Add Device on the Software

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

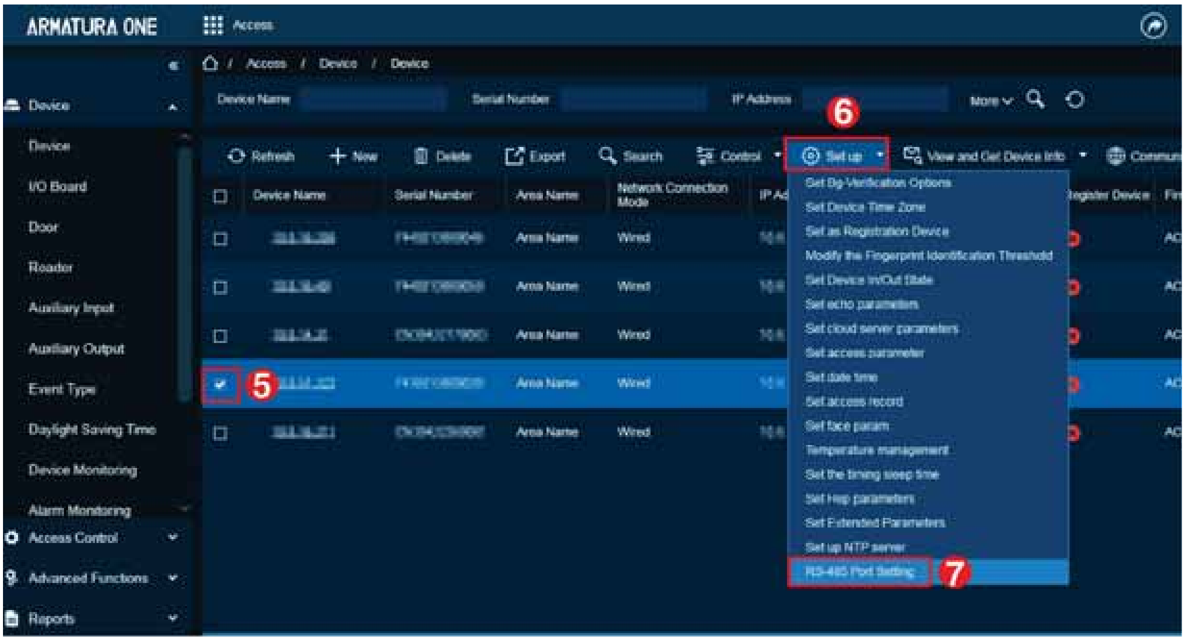
2. After clicking **Search**, the list and the total number of Access Control Devices will be displayed.

3. Click the **Add** button next to the Device to add the Device.

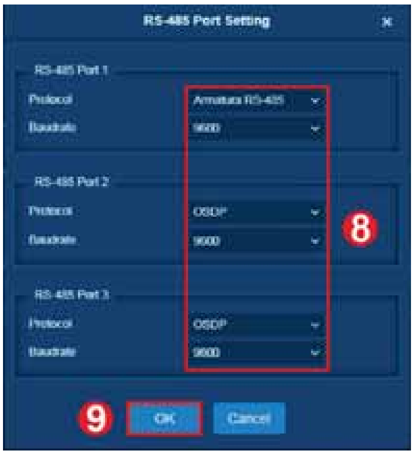
4. Click **Set up > RS-485 Port Setting** to configure the device's RS-485 port.



IP Address	MAC Address	Subnet Mask	Gateway Address	Serial Number	Device Type	Set Server	Operations
[illegible]	[illegible]	255.255.254.0	[illegible]	[illegible]	[illegible]		Add
[illegible]	[illegible]	255.255.255.0	[illegible]	[illegible]	[illegible]		This device has been added
[illegible]	[illegible]	255.255.255.0	[illegible]	[illegible]	[illegible]	[illegible]	This device has been added
[illegible]	[illegible]	255.255.255.0	[illegible]	[illegible]	[illegible]		This device has been added
[illegible]	[illegible]	255.255.255.0	[illegible]	[illegible]	[illegible]	[illegible]	This device has been added



☐	Device Name	Serial Number	Area Name	Network Connection Mode	IP Ad
☐	[illegible]	[illegible]	Area Name	Wired	[illegible]
☐	[illegible]	[illegible]	Area Name	Wired	[illegible]
☐	[illegible]	[illegible]	Area Name	Wired	[illegible]
☑	[illegible]	[illegible]	Area Name	Wired	[illegible]
☐	[illegible]	[illegible]	Area Name	Wired	[illegible]



RS-485 Port Setting

RS-485 Port 1
Protocol: Armatura RS-485
Baudrate: 9600

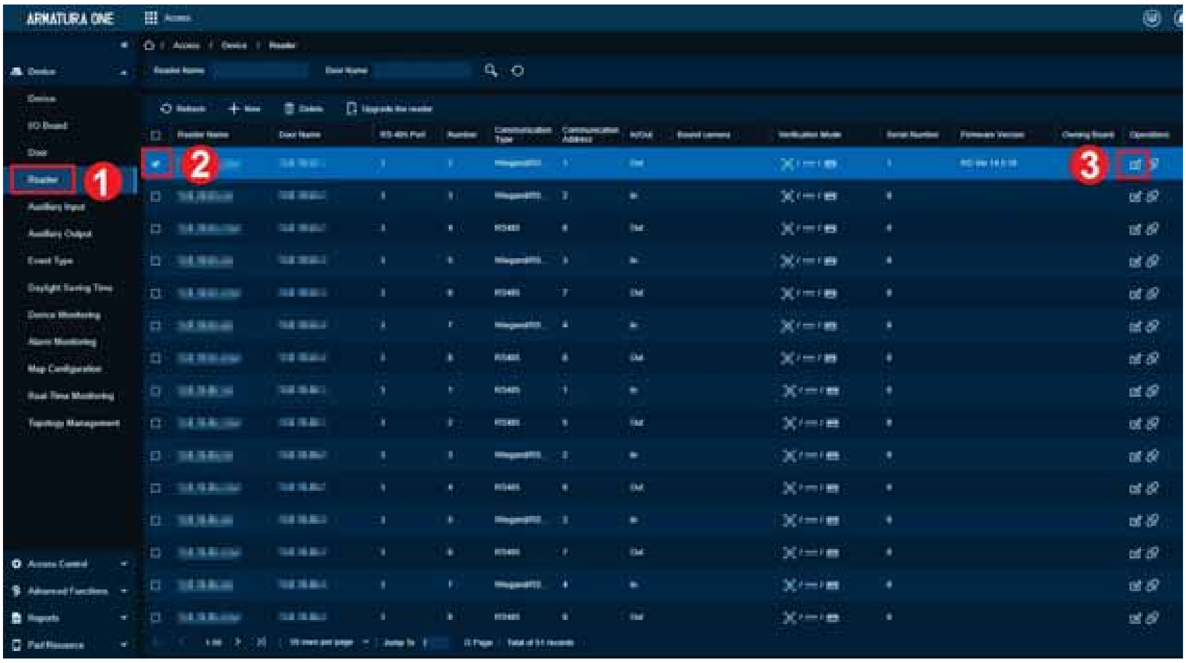
RS-485 Port 2
Protocol: OSDP
Baudrate: 9600

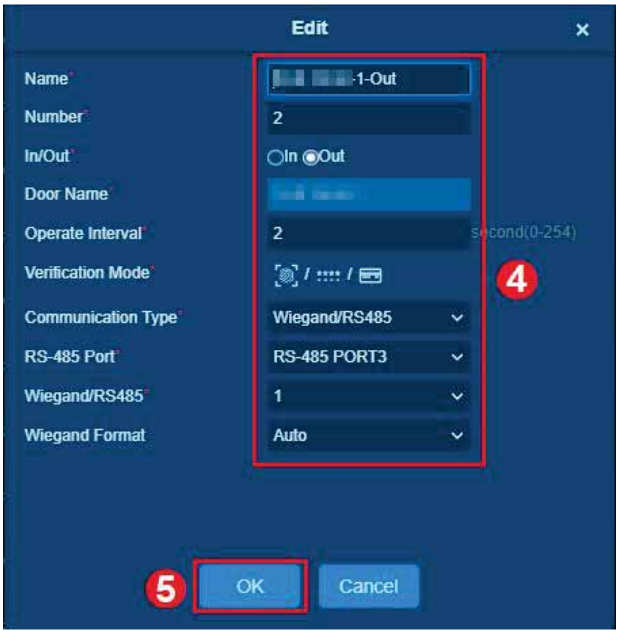
RS-485 Port 3
Protocol: OSDP
Baudrate: 9600

6.4 Configuring the Reader

1. When an RS-485 reader is connected. Refer to 4.2.7 RS-485 Reader Wiring to configure the EOL resistor for RS-485 port.

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




Edit

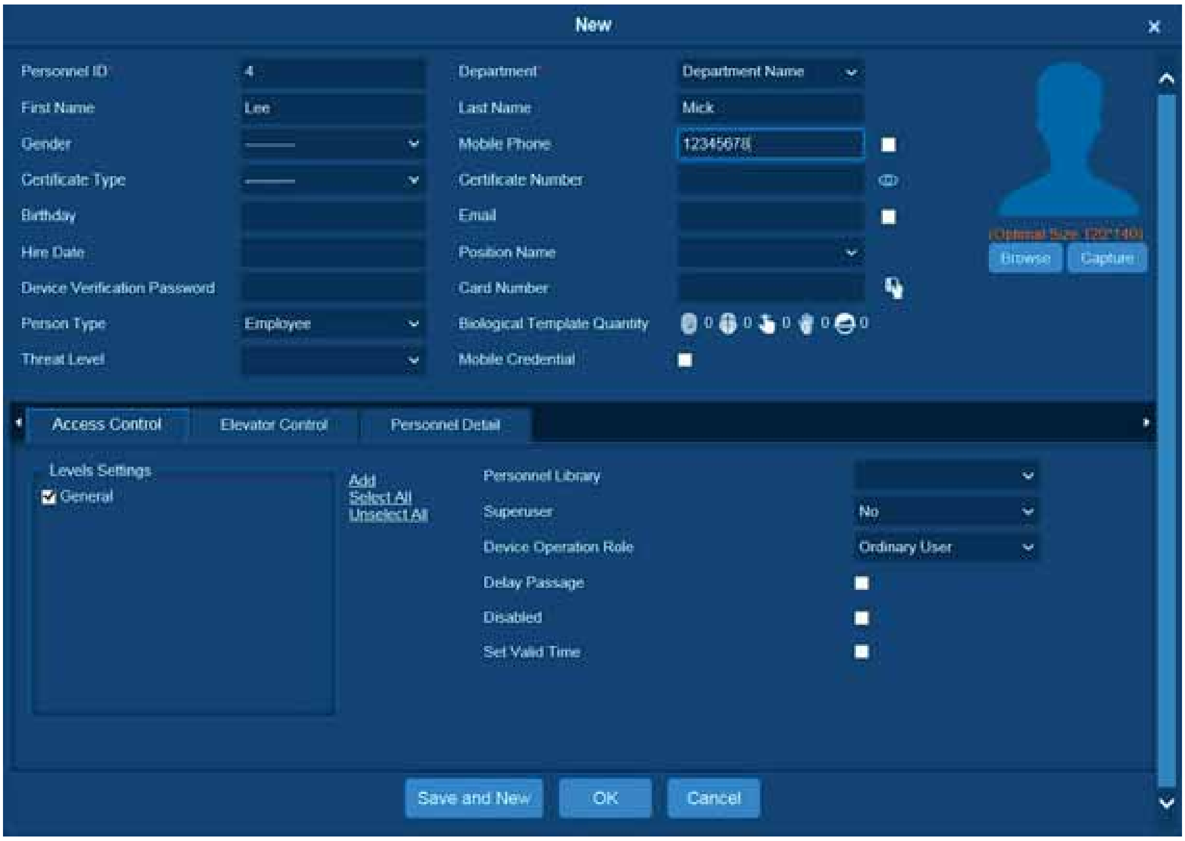
Name	[redacted]-1-Out
Number	2
In/Out	○In ●Out
Door Name	[redacted]
Operate Interval	2 second(0-254)
Verification Mode	/ ⠿ / 💳
Communication Type	Wiegand/RS485
RS-485 Port	RS-485 PORT3
Wiegand/RS485	1
Wiegand Format	Auto

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.



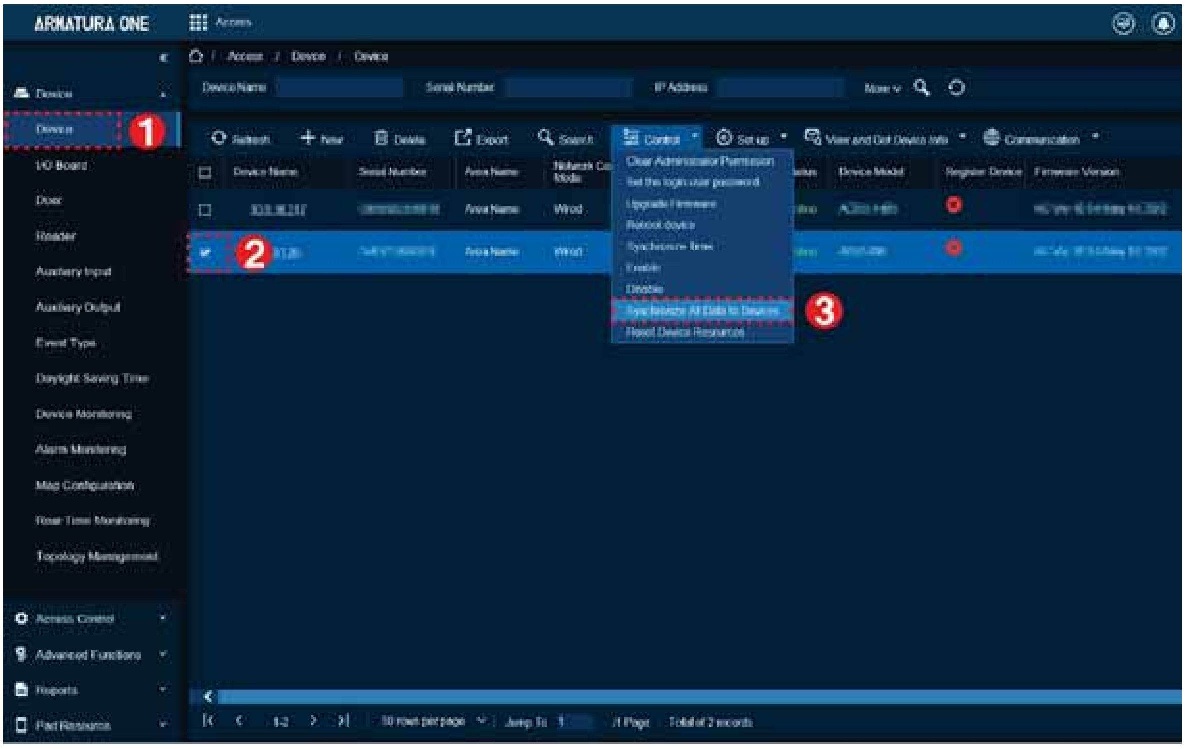
Personnel ID	4	Department	Department Name
First Name	Lee	Last Name	Mick
Gender	———	Mobile Phone	12345678 □
Certificate Type	———	Certificate Number	
Birthday		Email	□
Hire Date		Position Name	
Device Verification Password		Card Number	
Person Type	Employee	Biological Template Quantity	0 0 0 0 0
Threat Level		Mobile Credential	□

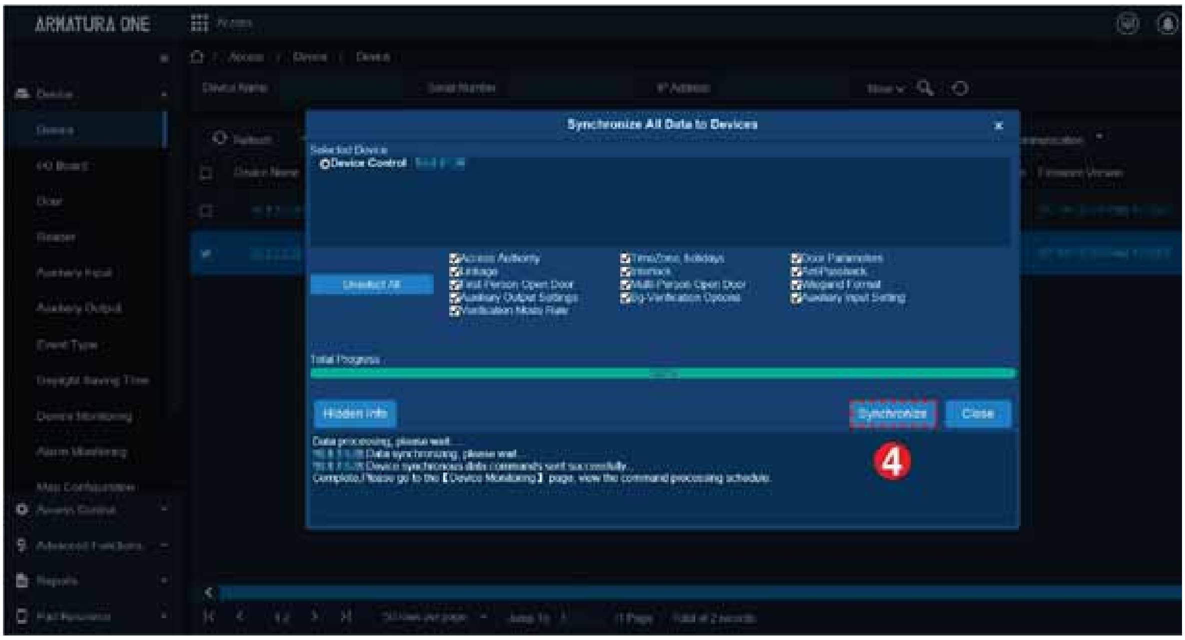
Levels Settings

☑ General

Personnel Library	
Superuser	No
Device Operation Role	Ordinary User
Delay Passage	□
Disabled	□
Set Valid Time	□

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



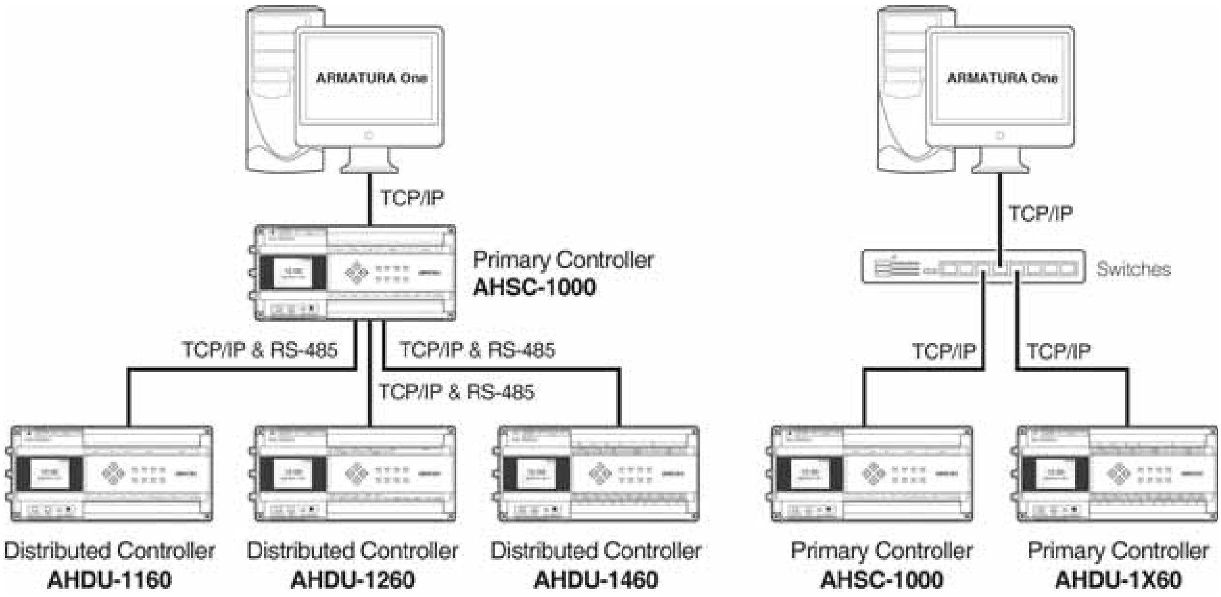


Data processing, please wait...
[illegible] Data synchronizing, please wait...
[illegible] Device synchronous data commands sent successfully...
Complete,Please go to the【Device Monitoring】 page, view the command processing schedule.

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

7. System Management Mode Connection

The system supports normal security levels to add Horizon Series controllers. And both Master-Slave Mode and Master Mode management modes are supported.



Master-Slave Mode **Master Mode**

Figure 7-1 Schematic Diagram of System Management Mode

Remarks:

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

7.1 Master-Slave Mode

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

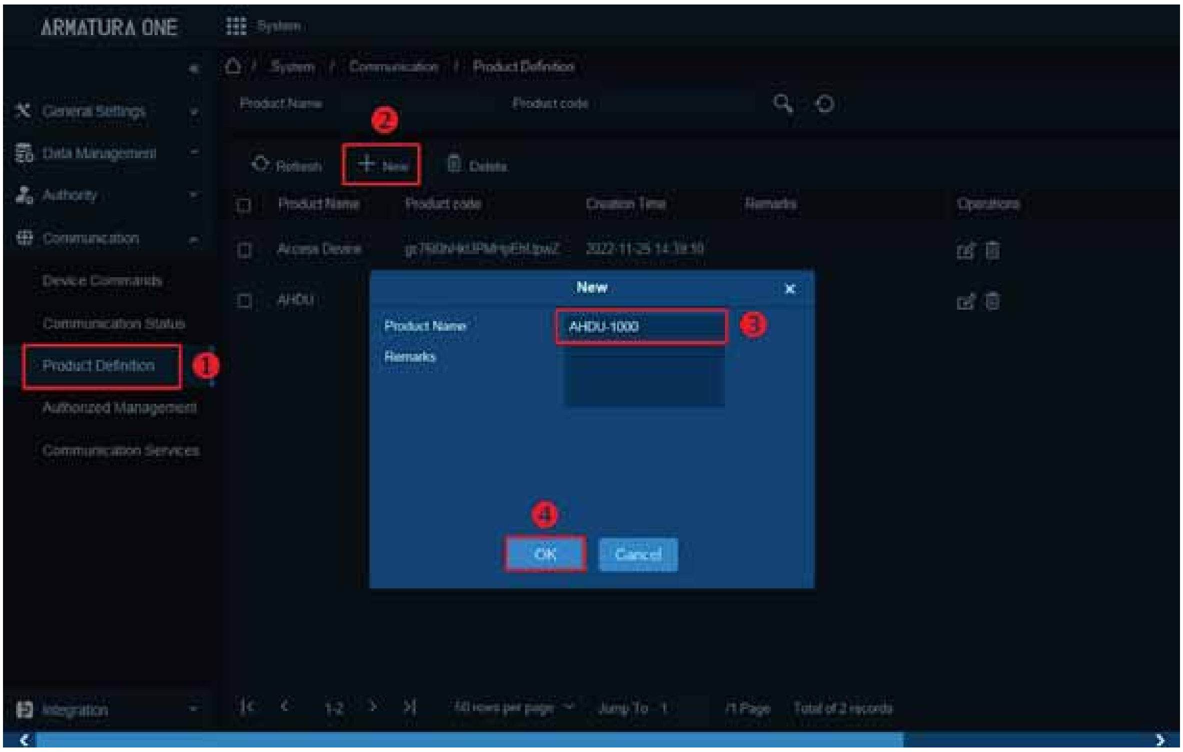
7.1.1 Connect AHDU-1X60 to AHSC-1000 via TCP/IP

7.1.1.1 Step 1 Add 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.



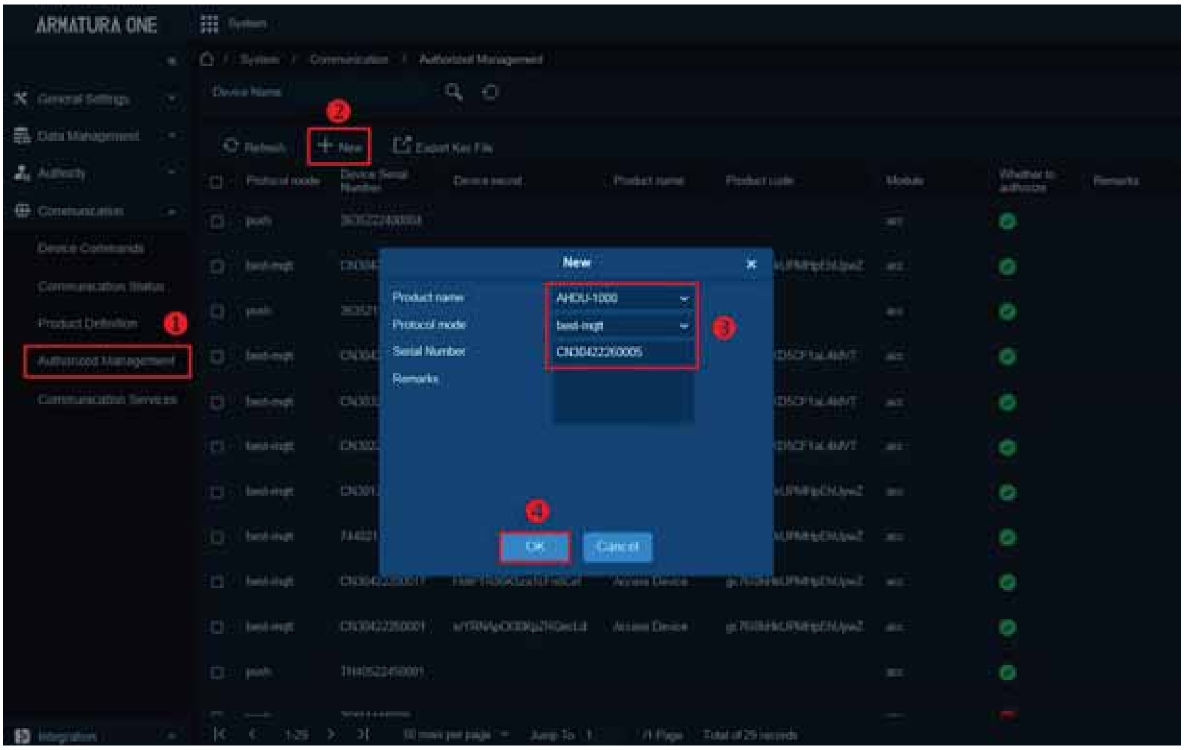
New

Product Name: AHDU-1000

Remarks:

2. Add a device

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



New

Product name: AHDU-1000

Protocol mode: best-mqtt

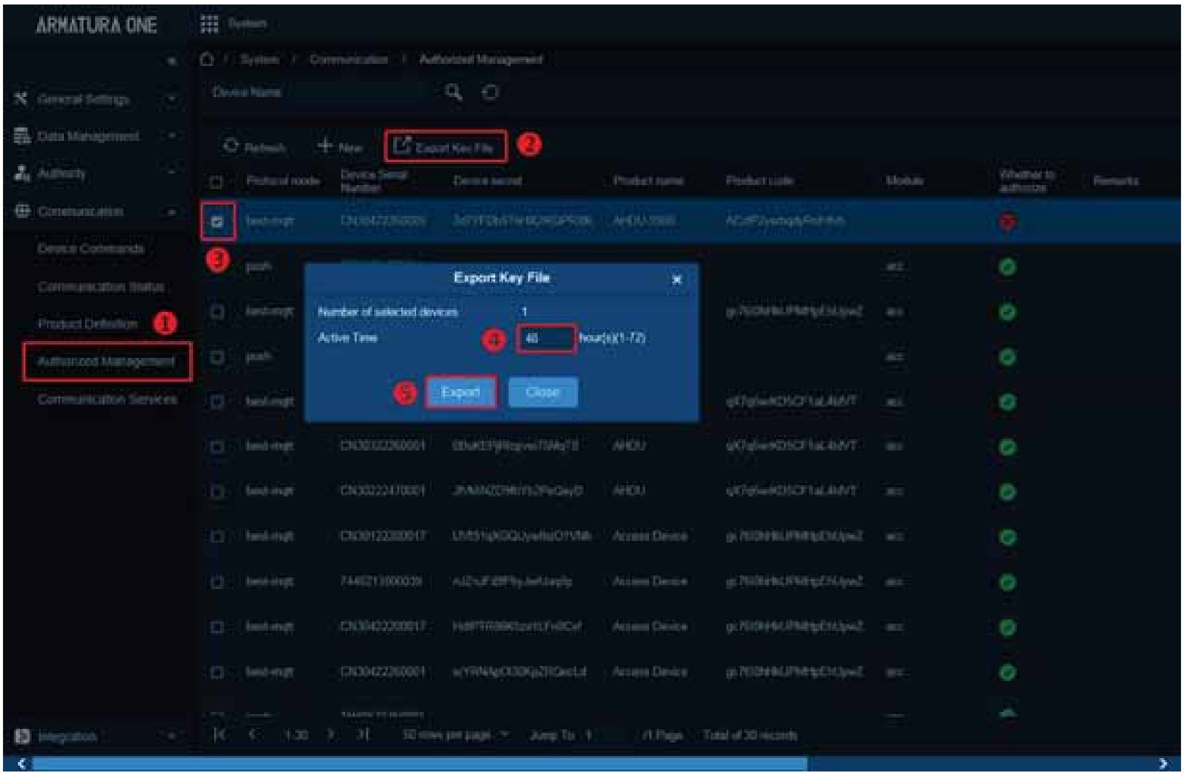
Serial Number: CN30422260005

Remarks:

Select Product just now created, then input serial number. Click **OK** to save and exit.

3. Export Key File

Click **System > Communication > Authorized Management** to check Device just now added and then click **Export Key File**.



Export Key File

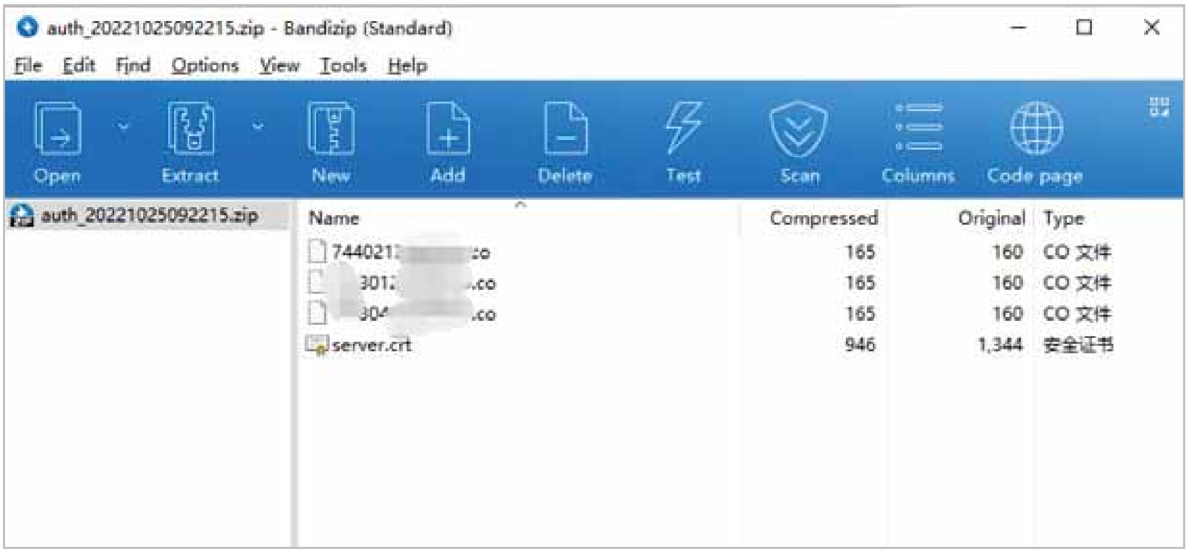
Number of selected devices 1

Active Time 48 hour(s)(1-72)

Export Close

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

After click **Export**, browser will download a .zip file.

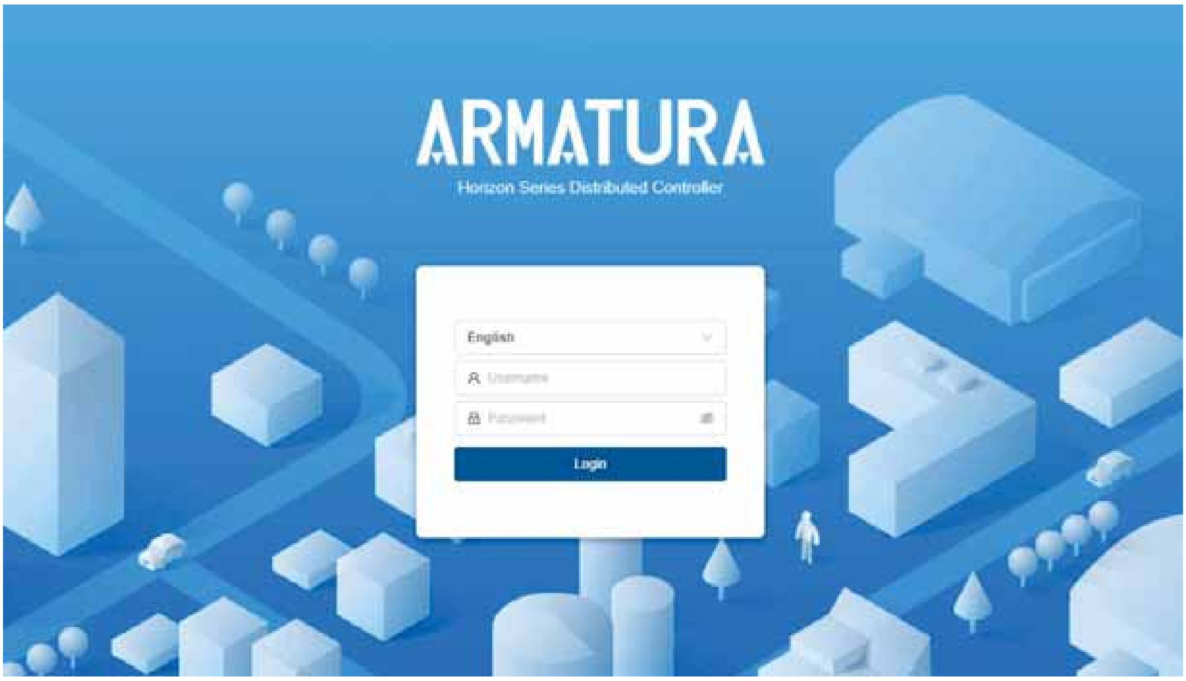

auth_20221025092215.zip - Bandizip (Standard)
File Edit Find Options View Tools Help
Open
Extract
New
Add
Delete
Test
Scan
Columns
Code page
auth_20221025092215.zip

Name	Compressed	Original	Type
744021[redacted].co	165	160	CO 文件
[redacted]301[redacted].co	165	160	CO 文件
[redacted]304[redacted].co	165	160	CO 文件
server.crt	946	1,344	安全证书

Note: *This function support selects multiple devices and click icon, it will generate all controllers .co file and server certificate in a .zip package, just upload this .zip package to controller webserver.*

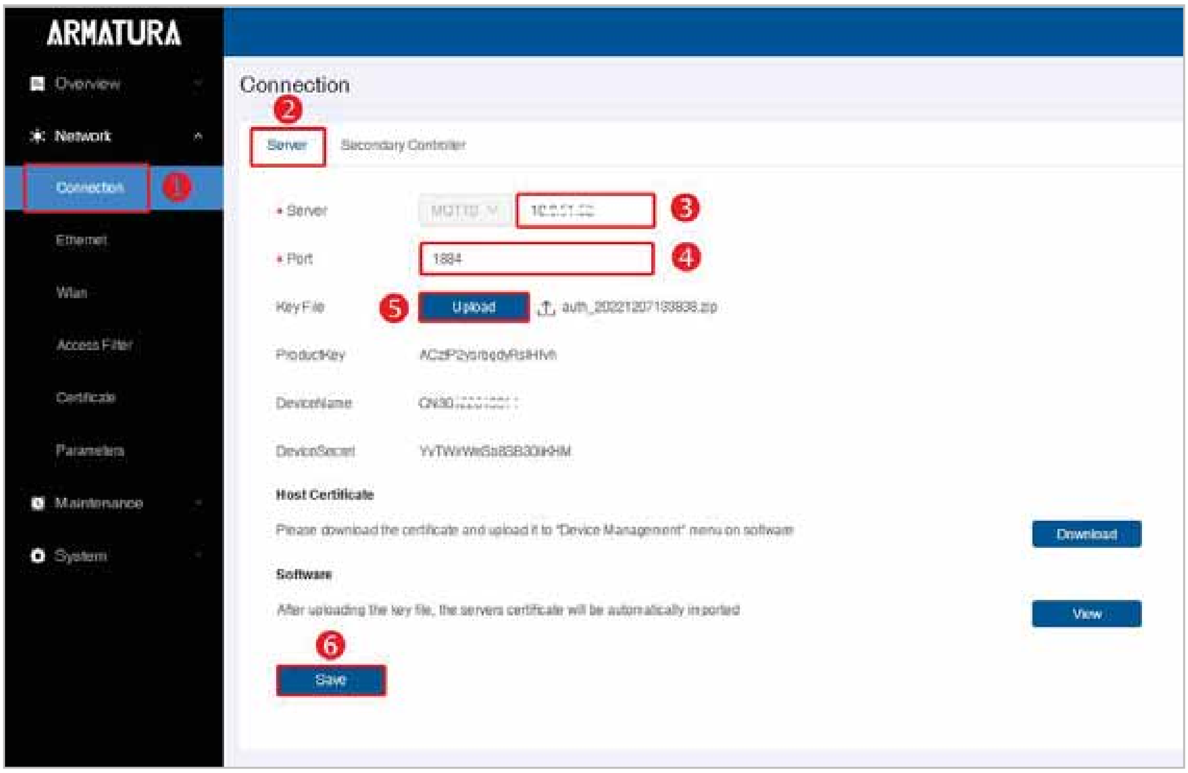
4. Import Key file to controller

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



First time login username and password are **armatura**. When login will require to change the password for admin.

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



Connection

Server Secondary Controller

* Server MQTT 10.[illegible]

* Port 1884

Key File auth_20221207193838.zip

ProductKey ACzIP2ysrbedyRsIHIvh

DeviceName CN30[illegible]

DeviceSecret YvTWrWeSa8SB30iKHM

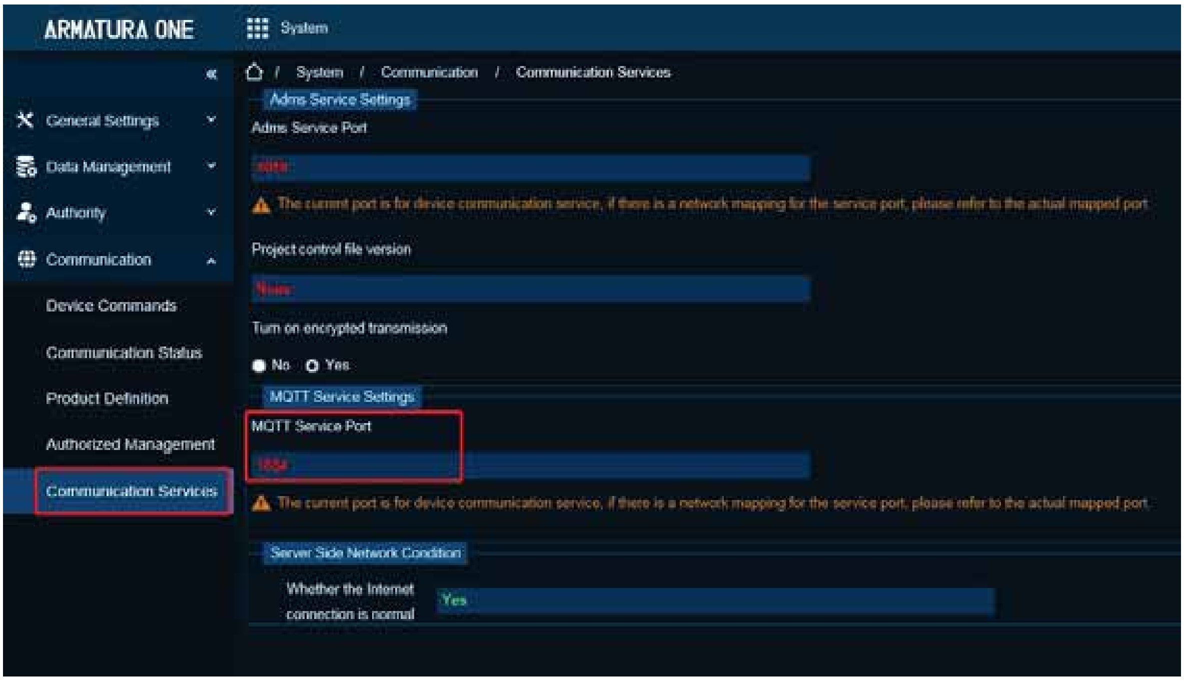
Host Certificate

Please download the certificate and upload it to "Device Management" menu on software

Software

After uploading the key file, the servers certificate will be automatically imported

- **Server:** Default is MQTTs protocol, address is the server address.
- **Port:** Default is 1884, this port can check by **System > Communication > Communication Services > MQTT Service Port**.



Adms Service Port: [illegible]

⚠ The current port is for device communication service, if there is a network mapping for the service port, please refer to the actual mapped port

Project control file version: None

Turn on encrypted transmission: ● No ○ Yes

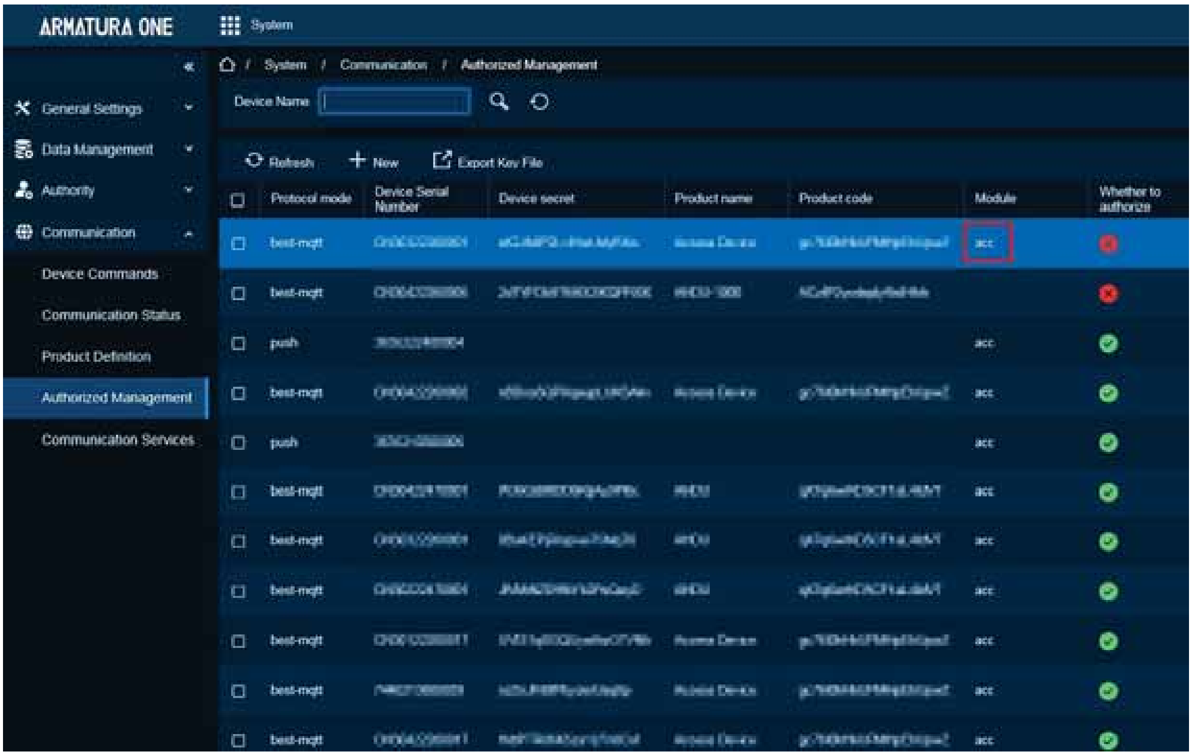
MQTT Service Port: 1884

⚠ The current port is for device communication service, if there is a network mapping for the service port, please refer to the actual mapped port

Whether the Internet connection is normal: Yes

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

After controller connect to MQTT successfully, Column Module will show ‘**acc**’. Because device has not authorized to Access Module, will show ☒.



□	Protocol mode	Device Serial Number	Device secret	Product name	Product code	Module	Whether to authorize
□	best-mqtt	[illegible]	[illegible]	[illegible]	[illegible]	acc	☒
□	best-mqtt	[illegible]	[illegible]	[illegible]	[illegible]		☒
□	push	[illegible]				acc	✓
□	best-mqtt	[illegible]	[illegible]	[illegible]	[illegible]	acc	✓
□	push	[illegible]				acc	✓
□	best-mqtt	[illegible]	[illegible]	[illegible]	[illegible]	acc	✓
□	best-mqtt	[illegible]	[illegible]	[illegible]	[illegible]	acc	✓
□	best-mqtt	[illegible]	[illegible]	[illegible]	[illegible]	acc	✓
□	best-mqtt	[illegible]	[illegible]	[illegible]	[illegible]	acc	✓
□	best-mqtt	[illegible]	[illegible]	[illegible]	[illegible]	acc	✓
□	best-mqtt	[illegible]	[illegible]	[illegible]	[illegible]	acc	✓

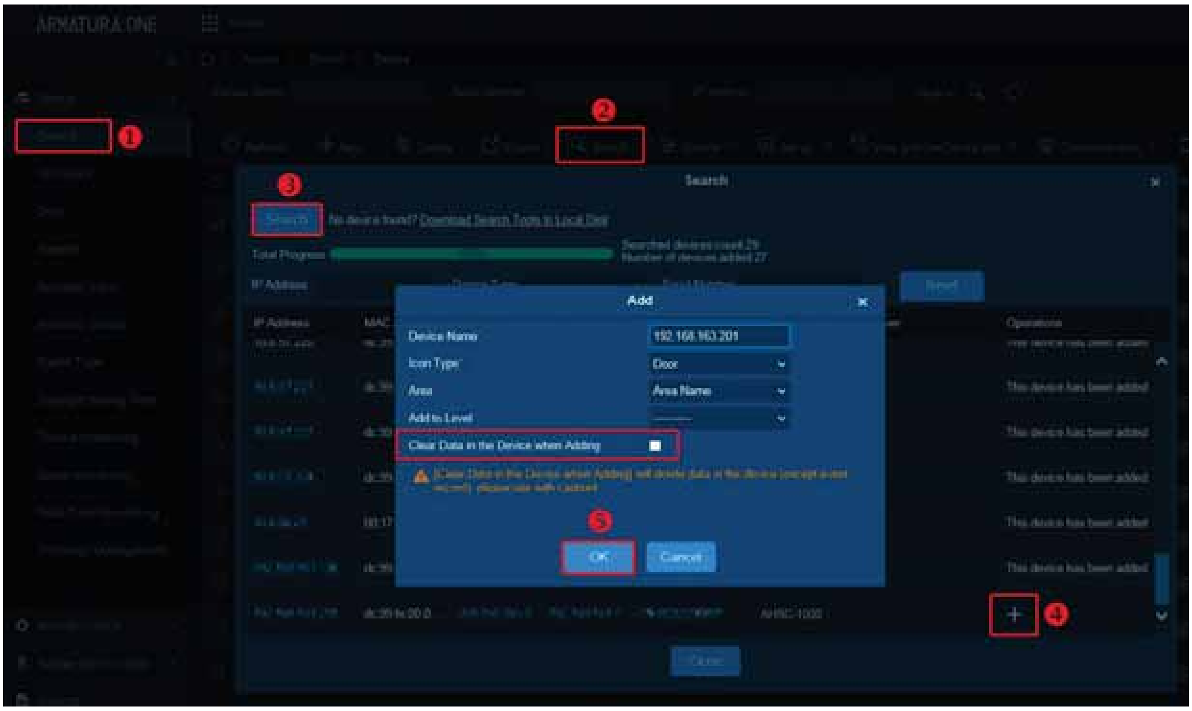
5. Add Controller on the Software

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 next to the Device to add the Device.

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



ARMATURA ONE
1
2
Search
3
Search
No device found? Download Search Tools to Local Disk
Total Progress
Searched devices count:29
Number of devices added:27
IP Address
Reset
IP Address
MAC
Operations
This device has been added
AHSC-1000
4
5
OK
Cancel
Close

Add

Device Name: 192.168.163.201

Icon Type: Door

Area: Area Name

Add to Level: --------

Clear Data in the Device when Adding □

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

7.1.1.2 Step 2 Set Secondary Controller Communication Port

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

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

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

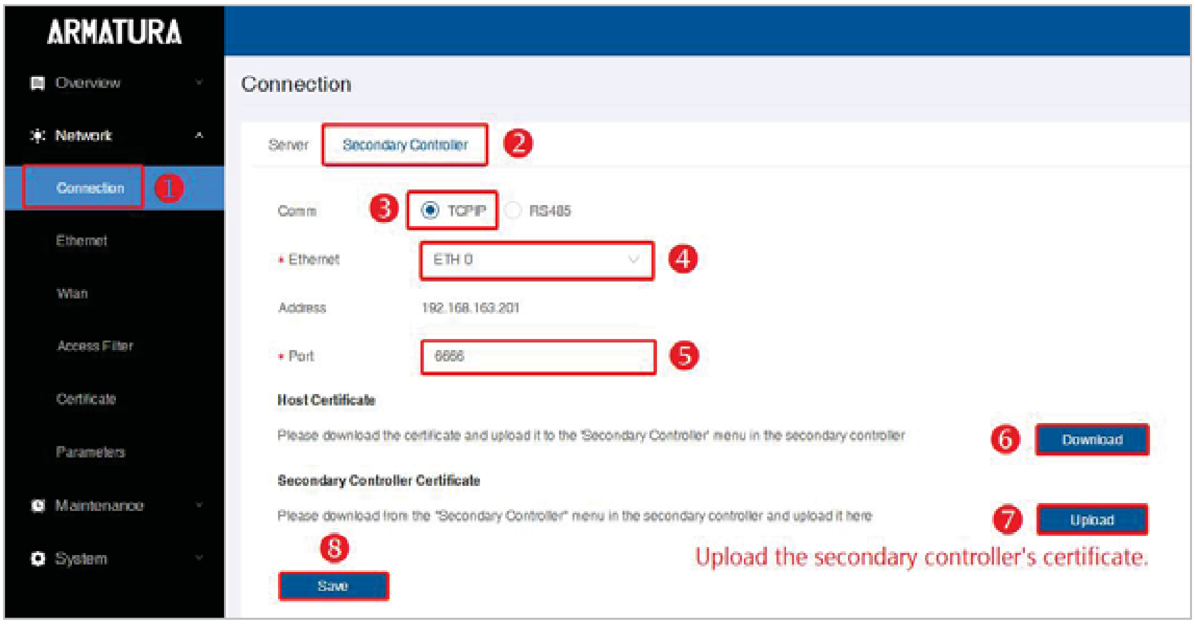
4. Click **Upload** to upload the secondary controller's certificate.

5. Click **Save** to exit.

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.



Connection

Server | Secondary Controller

Comm: ● TCP/IP ○ RS485

* Ethernet: ETH 0

Address: 192.168.163.201

* Port: 6666

Host Certificate

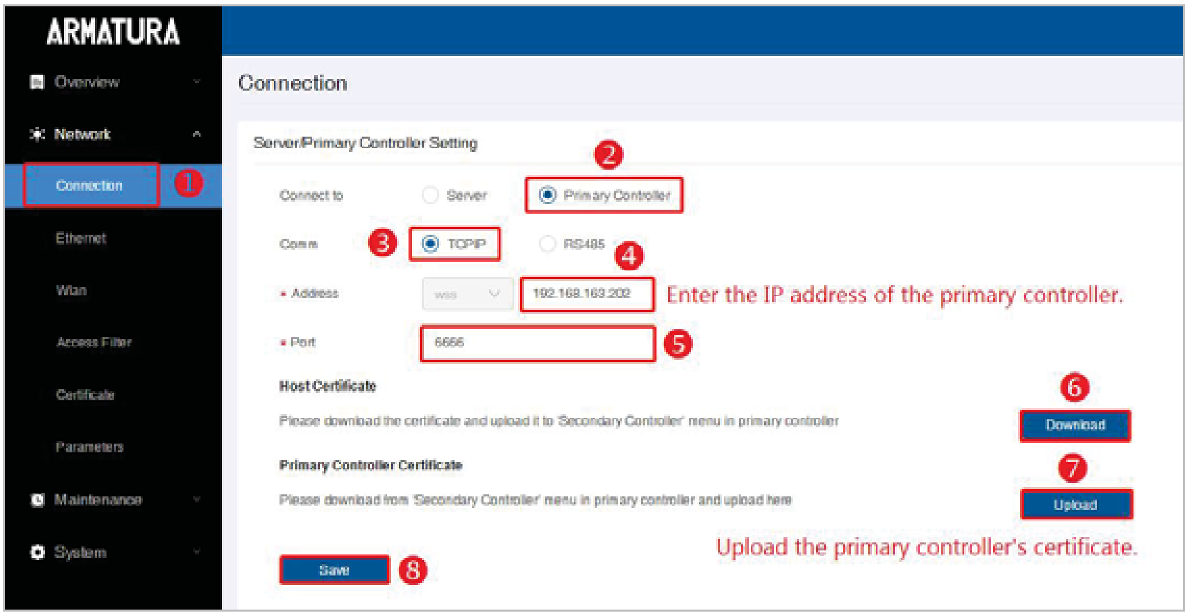
Please download the certificate and upload it to the 'Secondary Controller' menu in the secondary controller

Secondary Controller Certificate

Please download from the "Secondary Controller" menu in the secondary controller and upload it here

Upload the secondary controller's certificate.

- **Ethernet:** Select ‘Eth 0’ or ‘Eth 1’.
- **Address:** Will show IP address to confirm after select.
- **Port:** This is a port for secondary controller to use WSS protocol to connect.
- **Secondary Controller:** Download [Host Certificate] and Upload in Primary Controller Page [Secondary Controller Certificate].



Connection

Server/Primary Controller Setting

Connect to: ○ Server ● Primary Controller

Comm: ● TCP/IP ○ RS485

* Address: wss 192.168.163.202

Enter the IP address of the primary controller.

* Port: 6666

Host Certificate

Please download the certificate and upload it to 'Secondary Controller' menu in primary controller

Primary Controller Certificate

Please download from 'Secondary Controller' menu in primary controller and upload here

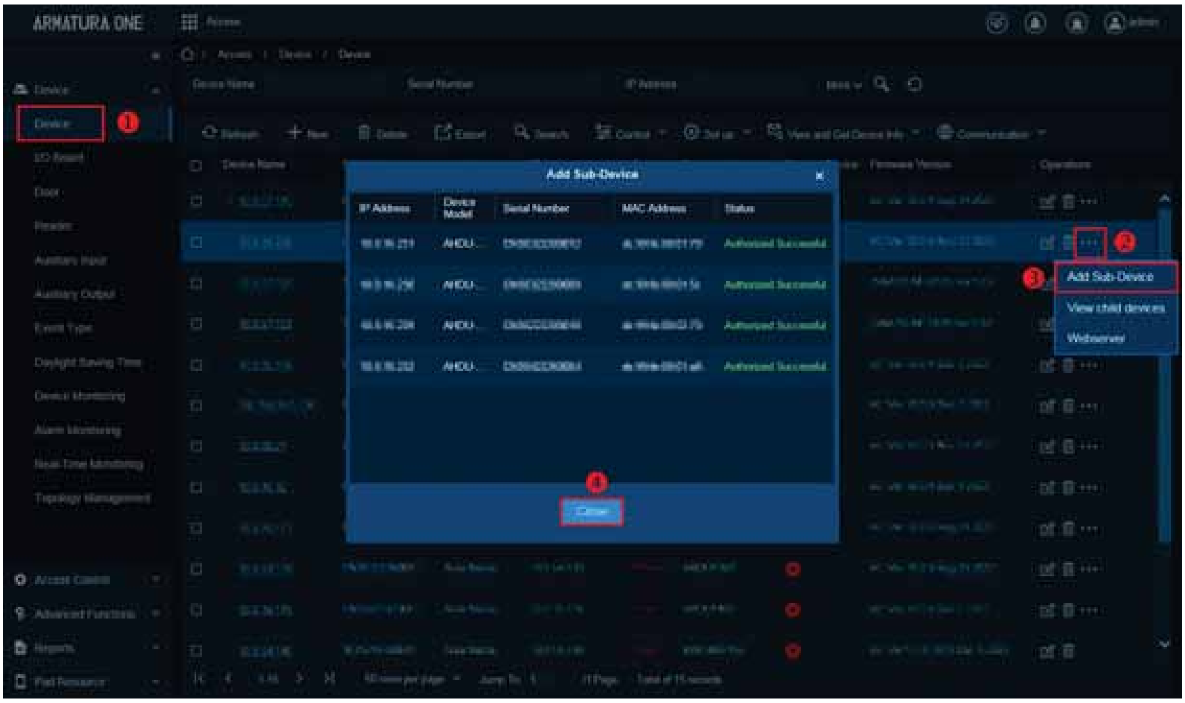
Upload the primary controller's certificate.

- **Address:** Enter the IP address of the primary controller.
- **Port:** This is a port for secondary controller to use WSS protocol to connect.
- **Primary Controller:** Download [Host Certificate] and Upload in Secondary Controller Page [Primary Controller Certificate].

9. After upload certificate each other, then add secondary controller.

7.1.1.3 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.



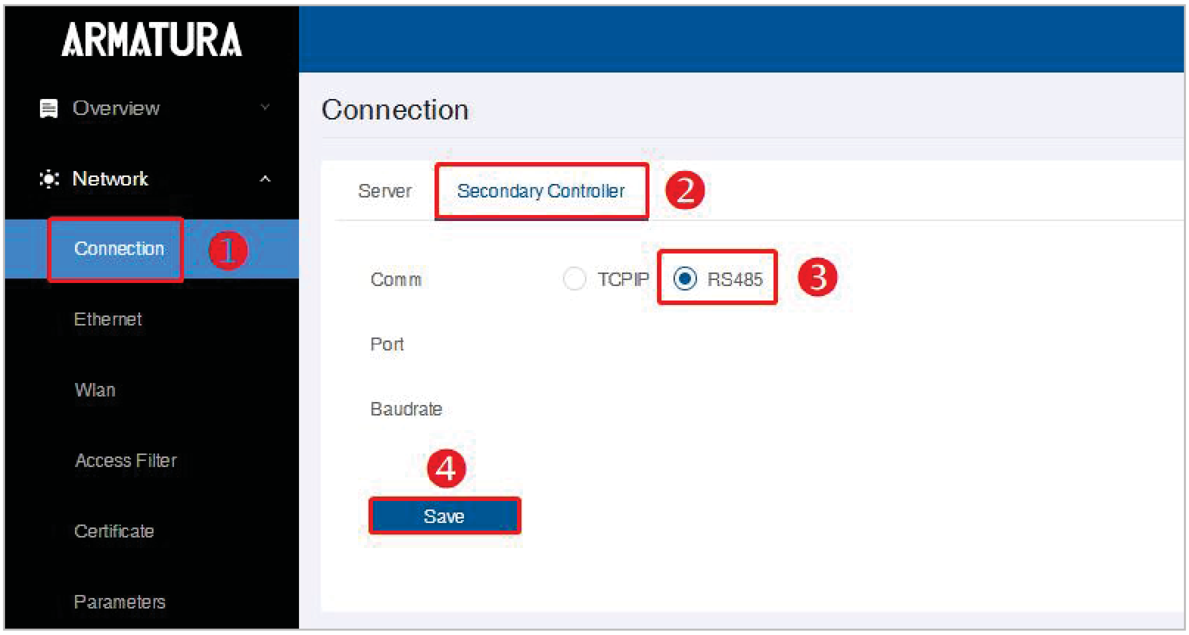
7.1.2 Connect AHDU-1X60 to AHSC1000 via RS-485

7.1.2.1 Step 1 Add Primary Controller

The method of adding a primary controller is the same as that of **7.1.1 Connect AHDU-1X60 to AHSC-1000 via TCP/IP**, please see 7.1.1.1 Step 1 Add Primary Controller for details on how to add it.

7.1.2.2 Step 2 Set Secondary Controller Communication Port

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



Connection

Server | Secondary Controller

Comm ○ TCPIP ● RS485

Port

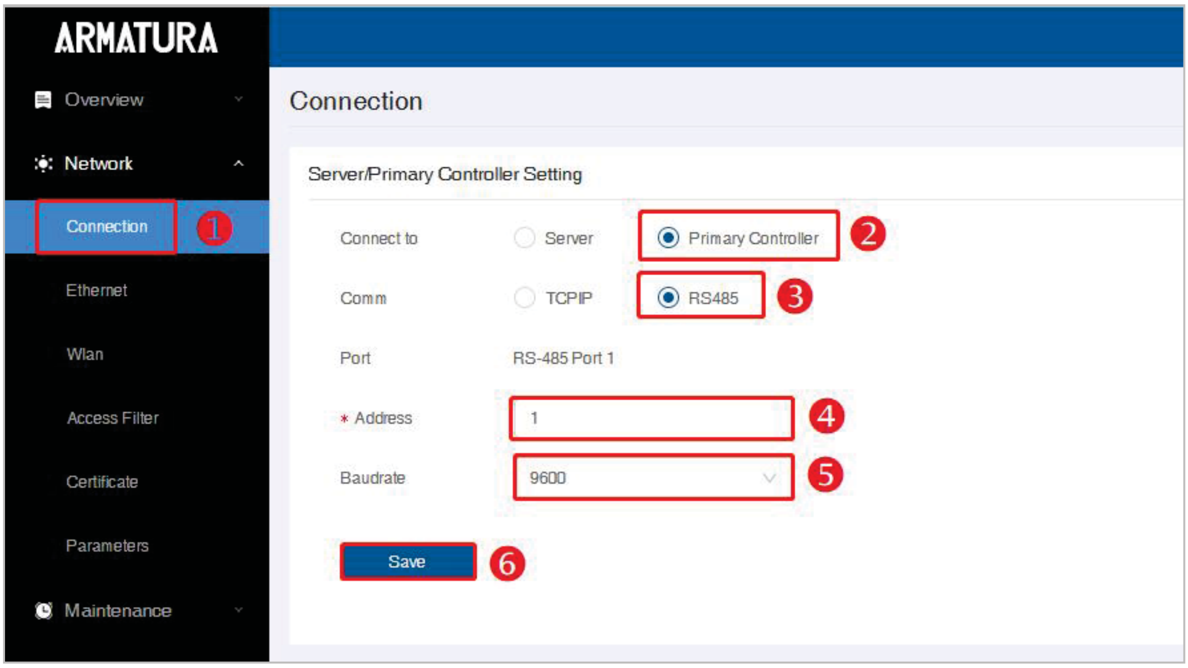
Baudrate

Save

Port: This is RS-485 port for secondary controller to connect. This depends on which port is set Armatura RS-485 in 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 RS-485 radio button in Comm.



Connection

Server/Primary Controller Setting

Connect to ○ Server ● Primary Controller

Comm ○ TCPIP ● RS485

Port RS-485 Port 1

* Address 1

Baudrate 9600

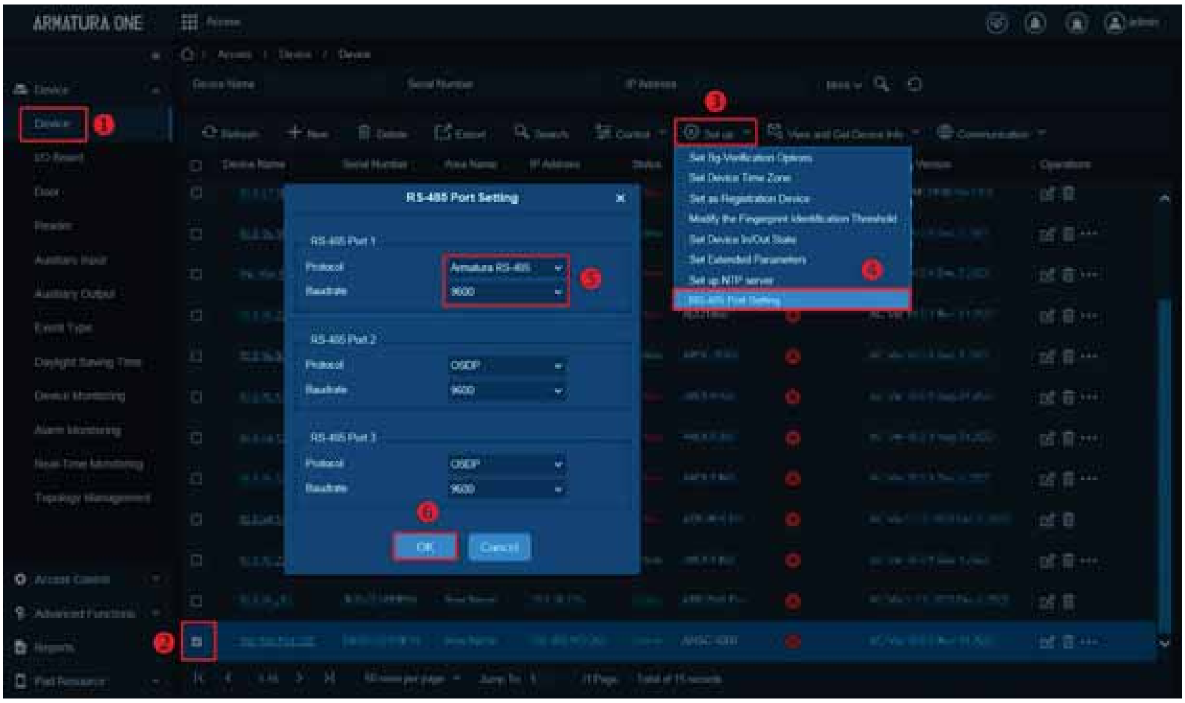
Save

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 in software.

5. In software **Access > Device > Device**, select a device and click **Set up** in operation bar, click **RS-485 Port Setting**.



RS-485 Port Setting

RS-485 Port 1
Protocol: Armatura RS-485
Baudrate: 9600

RS-485 Port 2
Protocol: OSDP
Baudrate: 9600

RS-485 Port 3
Protocol: OSDP
Baudrate: 9600

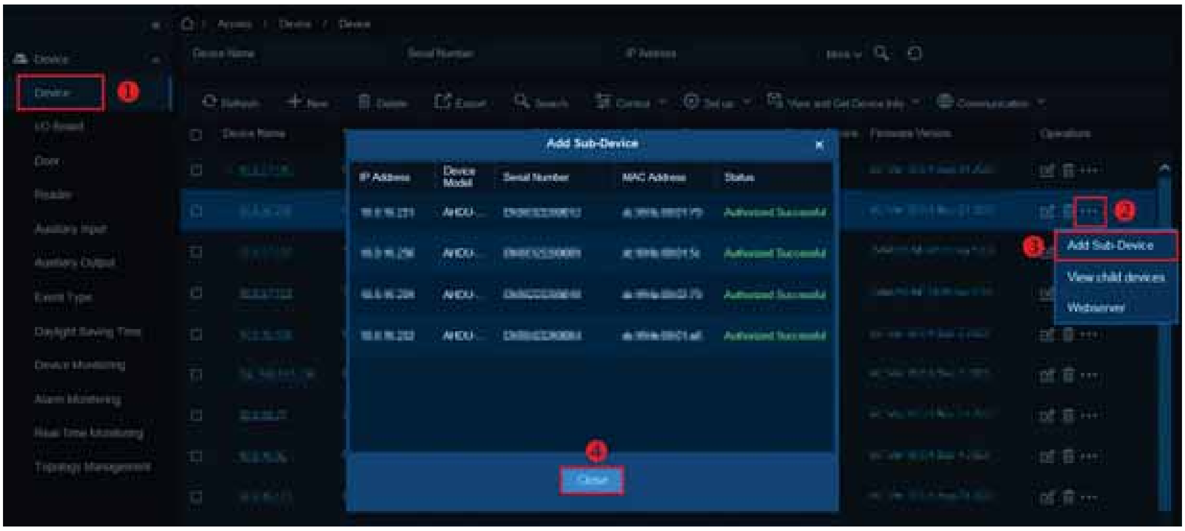
OK Cancel

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

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

7.1.2.3 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.



Add Sub-Device

IP Address	Device Model	Serial Number	MAC Address	Status
[illegible]	AHDU...	[illegible]	[illegible]	Authorized Successful
[illegible]	AHDU...	[illegible]	[illegible]	Authorized Successful
[illegible]	AHDU...	[illegible]	[illegible]	Authorized Successful
[illegible]	AHDU...	[illegible]	[illegible]	Authorized Successful

Close

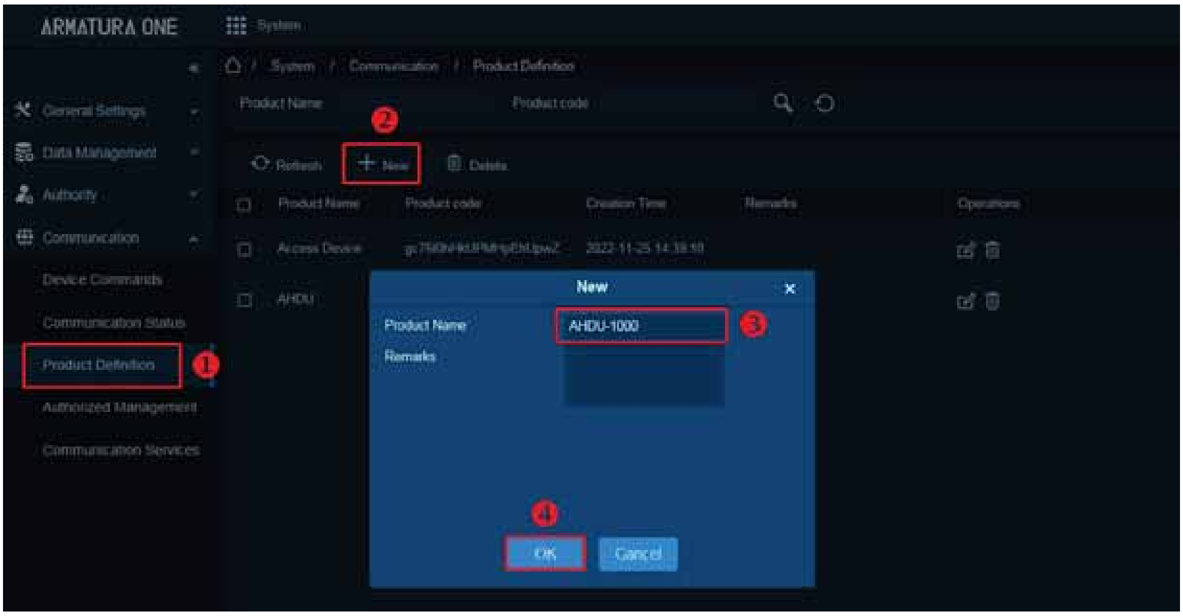
7.2 Master Mode

7.2.1 Add Primary Controller

1. Add a product

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

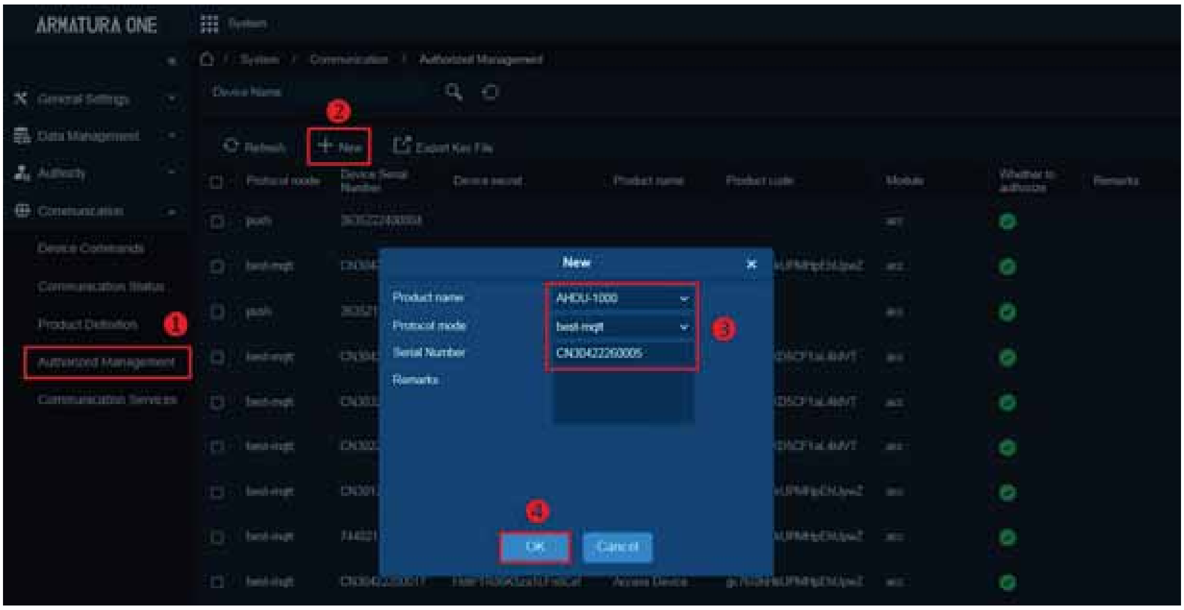
Enter the product name and click **OK** to save and exit.



Product Name: AHDU-1000

2. Add a device

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

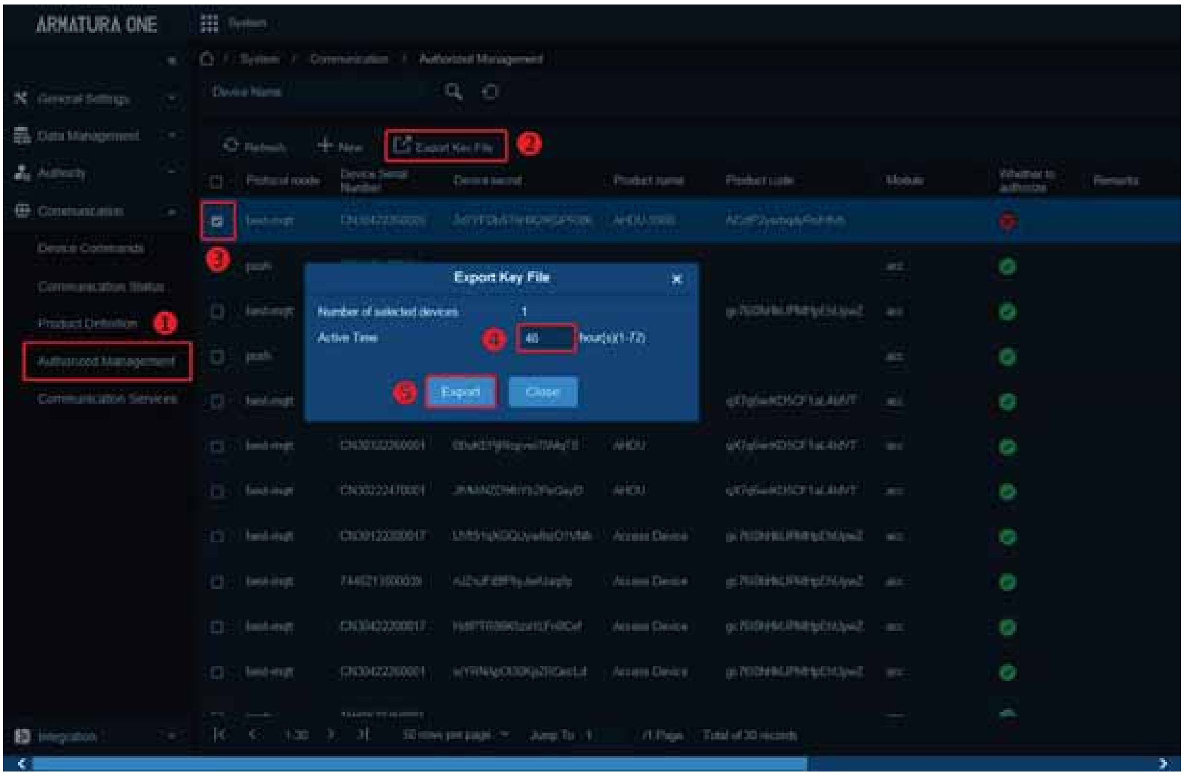


Product name: AHDU-1000
Protocol mode: best-mqtt
Serial Number: CN304222600005

Select Product just now created, then input serial number. Click **OK** to save and exit.

3. Export Key File

Click **System > Communication > Authorized Management** to check Device just now added and then click **Export Key File**.



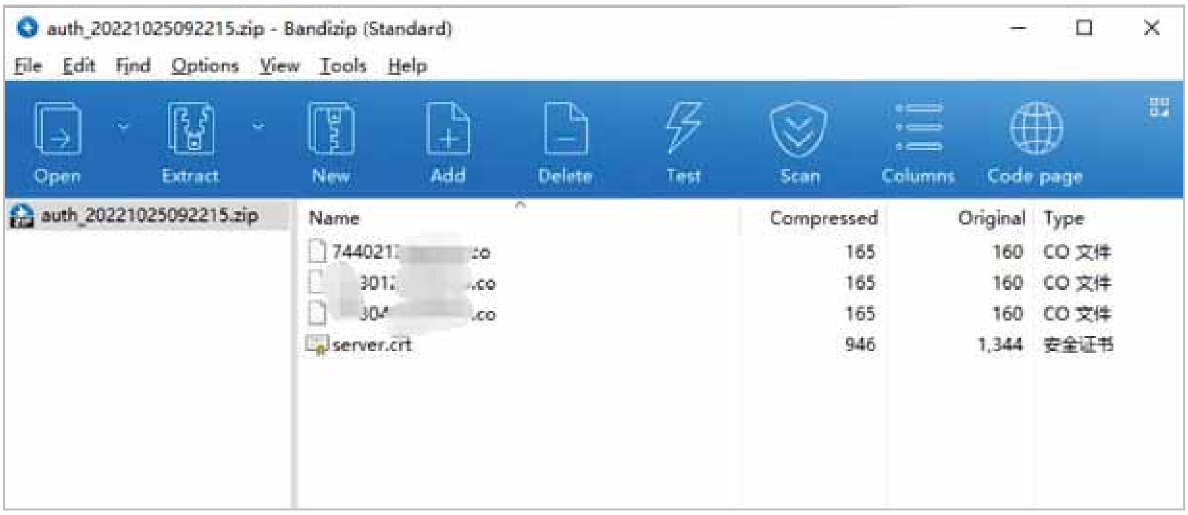
Export Key File

Number of selected devices 1

Active Time 40 hour(s)(1-72)

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

After click **Export**, browser will download a .zip file.

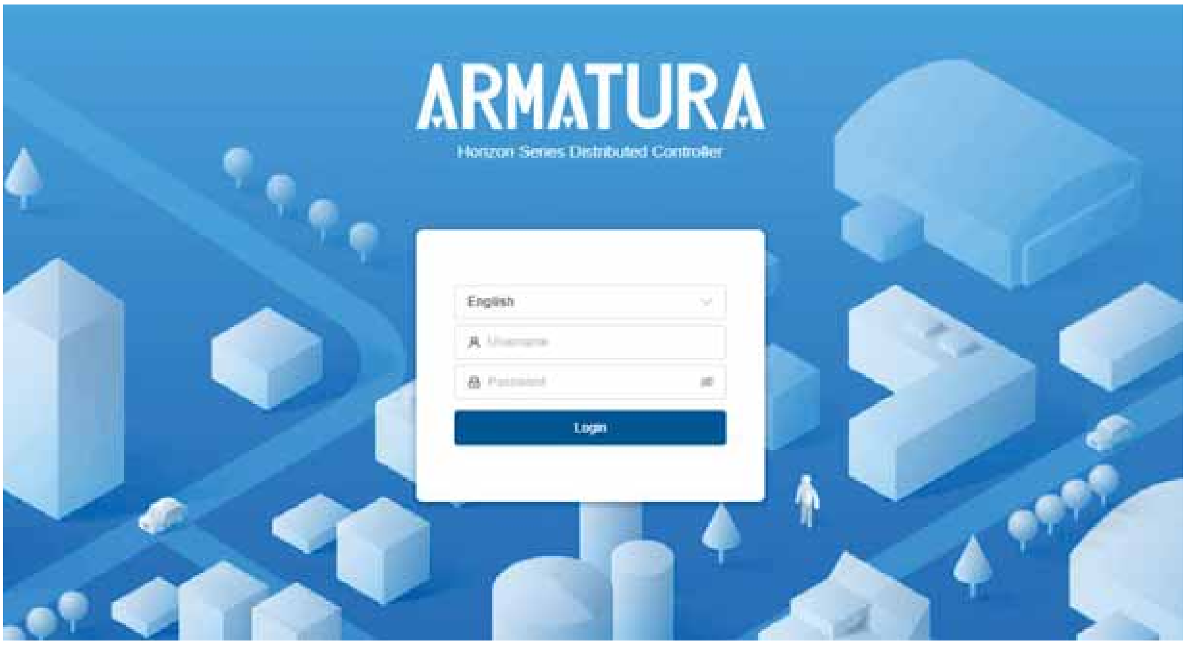

auth_20221025092215.zip - Bandizip (Standard)
File Edit Find Options View Tools Help
Open
Extract
New
Add
Delete
Test
Scan
Columns
Code page
auth_20221025092215.zip

Name	Compressed	Original	Type
744021[redacted].co	165	160	CO 文件
[redacted]301[redacted].co	165	160	CO 文件
[redacted]304[redacted].co	165	160	CO 文件
server.crt	946	1,344	安全证书

***Note:** This function support selects multiple devices and click icon, it will generate all controllers .co file and server certificate in a .zip package, just upload this .zip package to controller webserver.*

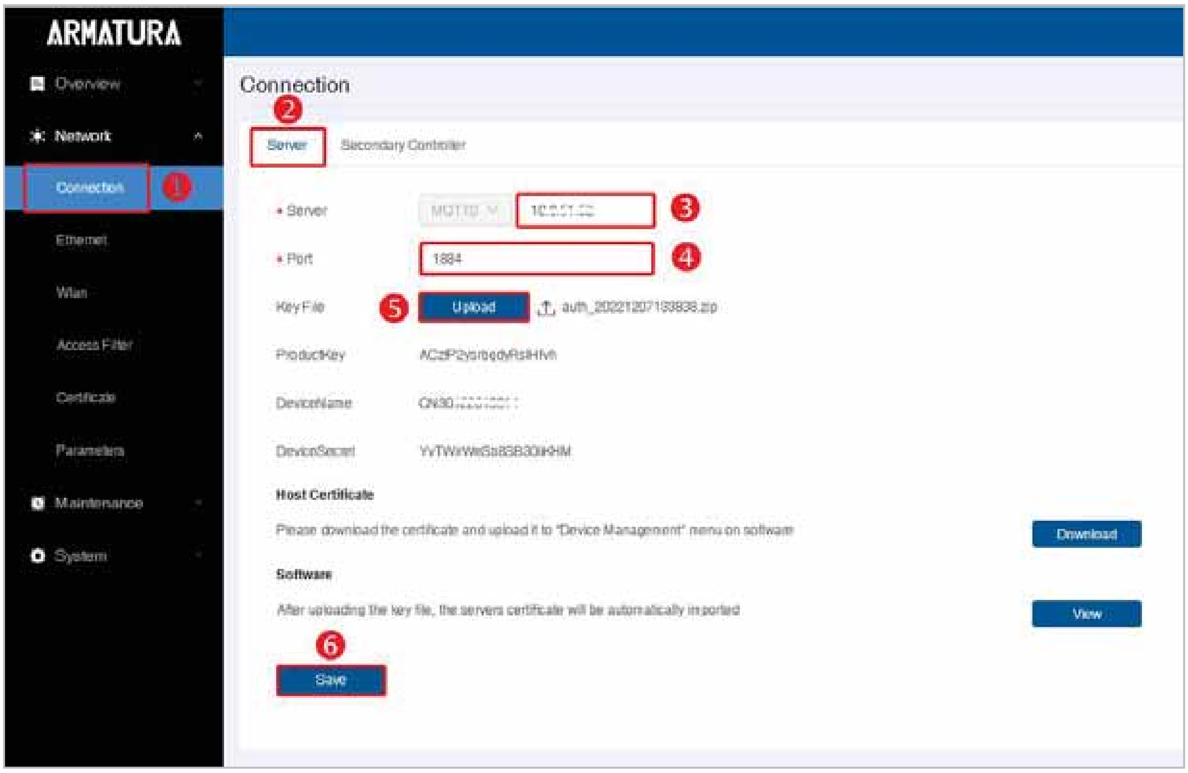
4. Import Key file to controller

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



First time login username and password are **armatura**. When login will require to change the password for admin.

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



Connection

Server | Secondary Controller

* Server MQTTS 1[illegible]

* Port 1884

Key File Upload auth_20221207133838.zip

ProductKey ACzlP2ysrbqdyRslHlvh

DeviceName CN30[illegible]

DeviceSecret YvTWrWeSs83B30iKHM

Host Certificate

Please download the certificate and upload it to "Device Management" menu on software Download

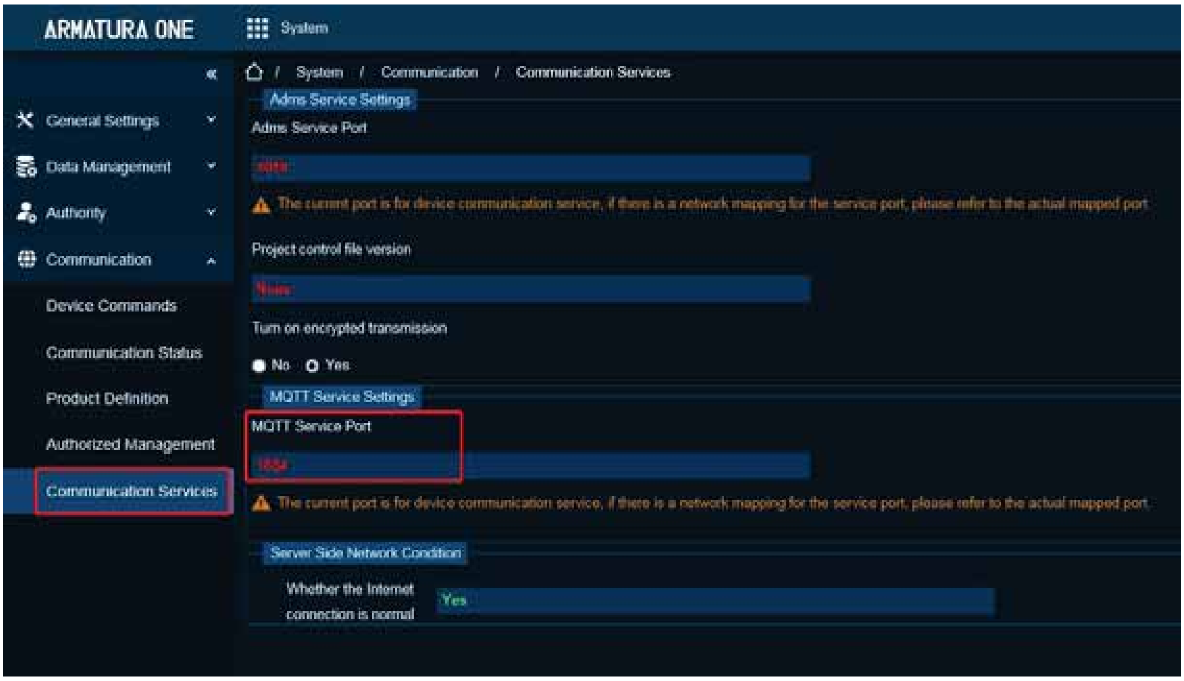
Software

After uploading the key file, the servers certificate will be automatically imported View

Save

- **Server:** Default is MQTTs protocol, address is the server address.

- **Port:** Default is 1884, this port can check by **System > Communication > Communication Services > MQTT Service Port**.



System / Communication / Communication Services

Adms Service Settings

Adms Service Port

[illegible]

⚠ The current port is for device communication service, if there is a network mapping for the service port, please refer to the actual mapped port

Project control file version

None

Turn on encrypted transmission

● No ○ Yes

MQTT Service Settings

MQTT Service Port

1884

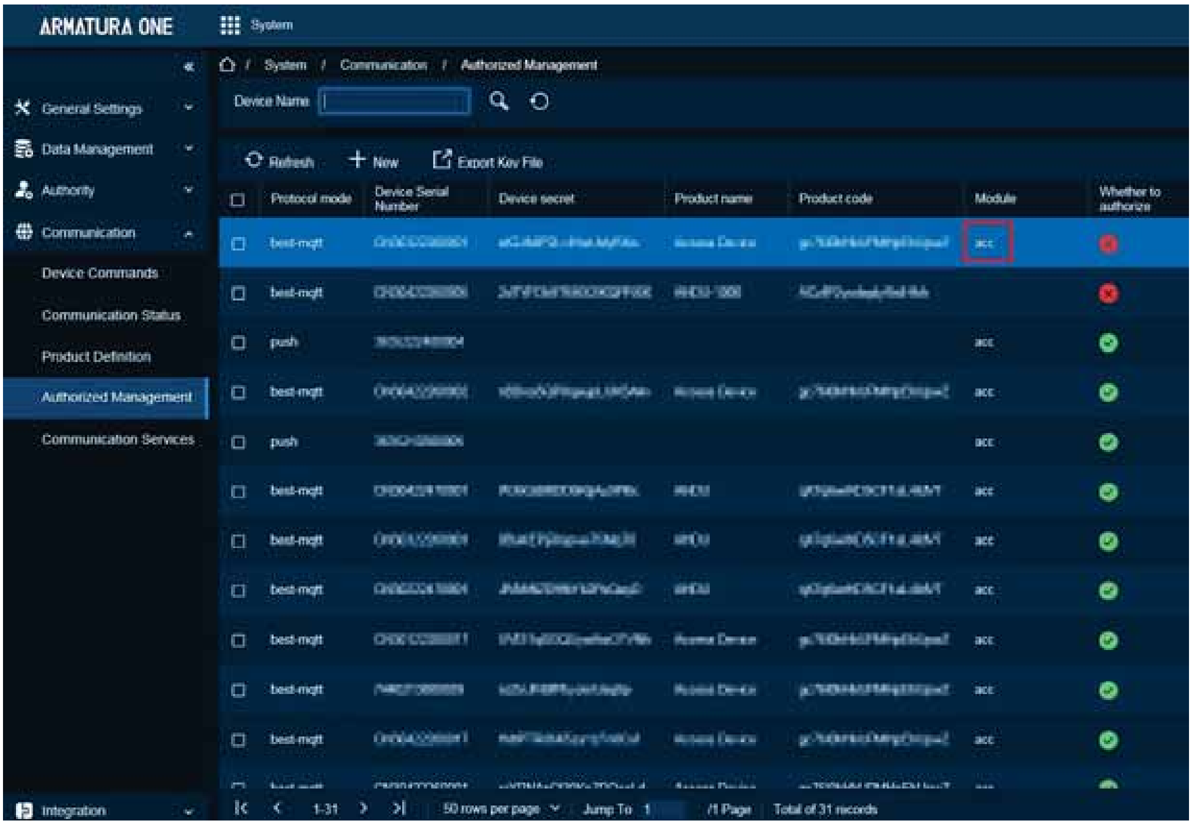
⚠ The current port is for device communication service, if there is a network mapping for the service port, please refer to the actual mapped port

Server Side Network Condition

Whether the Internet connection is normal: Yes

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

After controller connect to MQTT successfully, Column Module will show ‘**acc**’. Because device has not authorized to Access Module, will show ☒.



System / Communication / Authorized Management

Device Name

Refresh + New Export Key File

□	Protocol mode	Device Serial Number	Device secret	Product name	Product code	Module	Whether to authorize
□	best-mqtt	[illegible]	[illegible]	[illegible]	[illegible]	acc	☒
□	best-mqtt	[illegible]	[illegible]	[illegible]	[illegible]		☒
□	push	[illegible]				acc	✓
□	best-mqtt	[illegible]	[illegible]	[illegible]	[illegible]	acc	✓
□	push	[illegible]				acc	✓
□	best-mqtt	[illegible]	[illegible]	[illegible]	[illegible]	acc	✓
□	best-mqtt	[illegible]	[illegible]	[illegible]	[illegible]	acc	✓
□	best-mqtt	[illegible]	[illegible]	[illegible]	[illegible]	acc	✓
□	best-mqtt	[illegible]	[illegible]	[illegible]	[illegible]	acc	✓
□	best-mqtt	[illegible]	[illegible]	[illegible]	[illegible]	acc	✓
□	best-mqtt	[illegible]	[illegible]	[illegible]	[illegible]	acc	✓

|< < 1-31 > >| 50 rows per page Jump To 1 /1 Page Total of 31 records

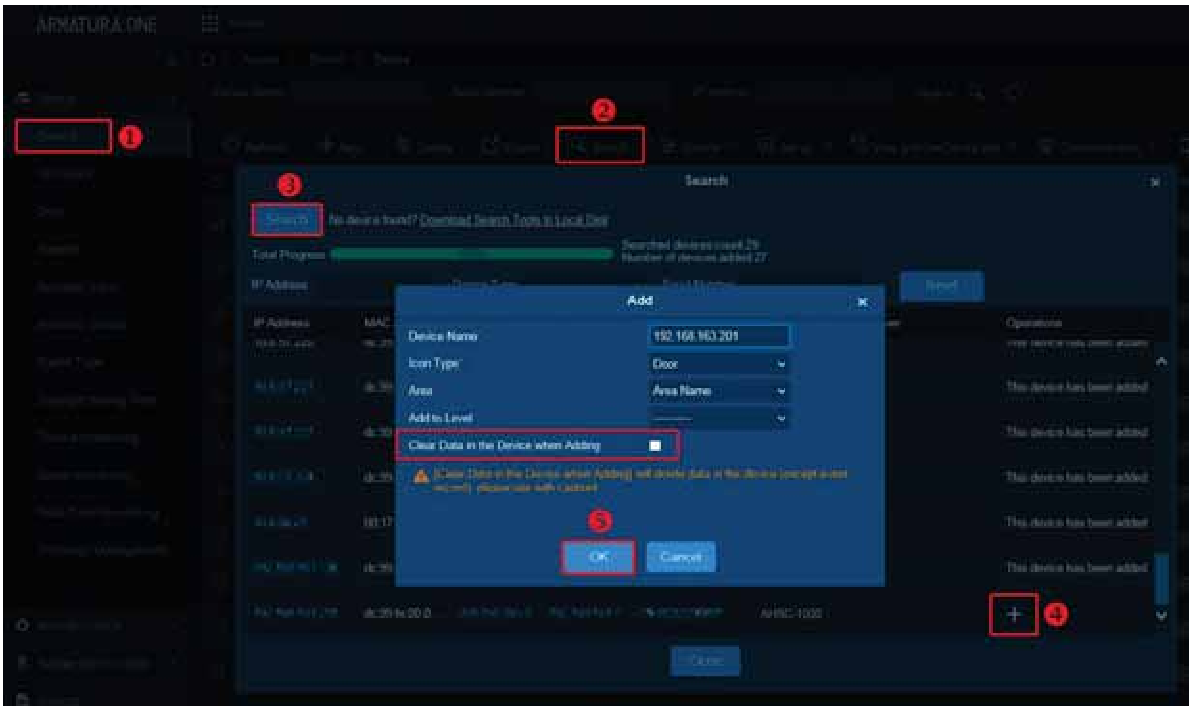
5. Add Controller on the Software

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 next to the Device to add the Device.

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



Searched devices count:29
Number of devices added:27

Device Name: 192.168.163.201
Icon Type: Door
Area: Area Name
Add to Level: --------
Clear Data in the Device when Adding □

[Clear Data in the Device when Adding] will delete data in the device (except event record), please use with caution!

AHSC-1000

This device has been added

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

8. Packing List

Make sure your box contains everything listed. If any pieces are missing, contact your dealer. Please save the original box and packing materials if you ever need to ship your equipment.

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

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

9. FAQ

Q1: How to check the IP address of the device when the user forgets it?

A: You can click the **M/OK** button > **Network Info** > **LAN1/LAN2/WLAN** to view the device IP address on the screen of the controller.

Q2: How to reset the network settings?

A: You can click the **M/OK** button on the controller screen > **Reset** > **Reset Network Settings** > **M/OK** to reset the network settings. Note that all the network settings will be reset. The default IP address of the main NIC is **192.168.1.201**, and the IP address of the extended NIC is **192.168.2.202**.

Q3: How to recover the administrator password of the webserver?

A: You can restore the device to factory settings by clicking the **M/OK** button > **Reset** > **Factory Reset** on the controller screen. You can also restore the factory settings by pressing and holding the **Reset button** for more than **5** seconds.

10. Appendix

10.1 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. <u>If you do not agree to the relevant agreement or any of its terms, you must stop using our products and services.</u>

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.

10.2 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.

10.3 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.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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

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

ARMATURA

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