# **ARMATURA**

# **User** Manual

# Armatura Horizon Controller IP-Based Biometric Door Unit

Applicable Models: AHSC-1000, AHDU-Series, AHEB Series Date: December 2022 Version: 1.5

#### Copyright © 2022 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 <u>http://www.armatura.us</u>.

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: <u>sales@armatura.us</u>. To know more about our global branches, visit <u>www.armatura.us</u>.

#### 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  $\star$  are not available in all devices.

# **Table of Contents**

1. Safety Instructions	1
1.1 Important Security Instructions	1
1.2 Installation Instructions	2
2. Overview	4
2.1 Introduction	4
2.2 Features	4
2.3 Appearance	7
2.3.1 AHSC-1000 Primary Controller	7
2.3.2 AHDU-1X60 Secondary Controller	8
2.3.3 AHEB-0808 Expansion Board	9
2.3.4 ENC1 Enclosure (optional)	
2.4 General Information	10
3. Installation and Connection	13
3.1 Installation Procedure	13
3.1.1 Installation with screws	
3.1.2 Installation with original 35mm DIN rail	14
3.1.3 Installation with extended 35mm DIN rail adapter	15
3.2 Access Control System Installation	17
3.3 Controller System Installation	
3.4 Access Control System Power Supply Structure	19
4. Terminal and Wiring Description	
4.1 Controller Connection Terminals	21
4.2 Terminal Description	
4.2.1 AHSC-1000	22
4.2.2 AHDU-1160	23
4.2.3 AHDU-1260	24
4.2.4 AHDU-1460	25
4.2.5 AHEB-0808	
4.3 Wiring Description	
4.3.1 Power Wiring	27
4.3.2 Network Wiring	27
4.3.3 Auxiliary Output Wiring	

4.3.4 Auxiliary Input Wiring	
4.3.5 Door Sensor, Exit Button Wiring	
4.3.6 Wiegand Reader Wiring	
4.3.7 Lock Relay Wiring	31
4.3.8 Fire Alarm Monitoring Wiring	
4.3.9 RS-485 Reader Wiring	33
4.3.10 I/O Board Wiring	
4.3.11 Line Monitoring	44
5. Equipment Communication	
5.1 Access Control Networking Wires and Wiring	45
5.2 TCP/IP Communication	46
5.3 Configure network on the Webserver	47
5.3.1 Opening the Webserver on the Browser	
5.3.2 Login to the Webserver	48
5.3.3 TCP/IP Settings	
5.3.4 Wireless Network Settings	50
5.3.5 Setting up the Server/Primary Controller	52
6. Connect to the ARMATURA One Software	54
6.1 Export the Key File	54
6.2 Server Connection Configuration	55
6.3 Add Device on the Software	
6.4 Configuring the Reader	57
6.5 Add Personnel on the Software	
7. System Management Mode Connection	60
7.1 Master-Slave Mode	60
7.1.1 Connect AHDU-1X60 to AHSC-1000 via TCP/IP	60
7.1.2 Connect AHDU-1X60 to AHSC1000 via RS-485	67
7.2 Master Mode	70
7.2.1 Add Primary Controller	70
8. Packing List	75
9. FAQ	76
10. Appendix	77
10.1 Privacy Policy	77
10.2 Eco-friendly Operation	79

# 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.

i

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.

# 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 improve the 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.

#### ΡοΕ

 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, antipassback, 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

# 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)		
Primary Host Communication	Ethernet: 100Base-TX 256bit AES* symmetric encryption for Controller to Server and Inter-Controller communications		
Secondary Host Communication	Bluetooth 4.2+HS, BLE		
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,2 relay,4 relay,1* Form-C with dry contacts2* Form-C with dry contacts4* Form-C with contacts			
Normally Open Contact Rating		5A @ 30Vdc resistive		
Normally Closed Contact Rating		5A @ 30Vdc resistive		
On-Board Monitor	Size: 2.4 Quickly view status of	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	Support	s up to 512bits card numbe	er length	
Mobile Credentical Capacity	400,000 (1:N) (Bluetooth) 400,000 (1:N) (NFC) 400,000 (1:N) (Dynamic QR Code)			
Fingerprint Capacity	100,000 (1:N)			
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)			

# 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.



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



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 Access Control System Installation

Figure 3-6 Schematic Diagram of Access Control System Installation

#### Remarks:

- 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.

# 3.3 Controller System Installation



Figure 3-7 Schematic Diagram of AHDU-1X60 System Installation

# 3.4 Access Control System Power Supply Structure



Figure 3-8 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.



Figure 3-9 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:



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.







#### Default Supervision



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 <u>4.3.11 Line Monitoring</u>.

## 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<sup>2</sup>. 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<sup>2</sup> 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.



#### No Supervision



#### Default Supervision



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 <u>4.3.11 Line Monitoring</u>.

#### 4.3.6 Wiegand Reader Wiring



Figure 4-12 Wiegand Reader Wiring

#### 4.3.7 Lock Relay Wiring

- 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:




- **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 <u>4.3.11 Line Monitoring</u>.

### 4.3.9 RS-485 Reader Wiring





#### **Important Notes**

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

 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:

ARMATURA ONE	ĵ	A	ccess								
		合 /		Device /	Reader						
🚔 Device		Rea	ier Name			Door Name		Q 0	)		
Device		Ð	Refresh	+ New	🔟 Del	Namat				i i	
I/O Board			Reader N	ame	Door Nar	Number"		1			n In/Out
Door					-94.44.2	In/Out*		⊙In ⊖Out			In
Reader						Door Name*					
Auxiliary Input				-Out	-10.8.84.3	Operate Interval <sup>®</sup>		2		second(0-254)	Out
Auxiliary Output					184.84.3	Communication Type"		RS485			
Event Type				<u>-Out</u>		RS-485 Port		RS-485 PORT1			Out
						RS485 Address*		1			
Daylight Saving Time			50.005	<u>e -In</u>	-01013	Encrypt"		Default Password			
Device Monitoring				Out		Wiegand Format		Auto			Out
Alarm Monitoring				<b>₽</b> t-In	-	0.5					
Access Control						4	Ok	C Cancel			

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.

EOL-RESISTOR	DIP Number	DIP Switch Settings
RS-485 1 (A,B)	1	0FF 1 2 3 RS-485
RS-485 2 (1A,1B)	2	0FF 0N 1 2 3 RS-485
RS-485 2 (2A,2B)	3	0FF 0N 1 2 3 RS-485
RS-485 3 (1A,1B)	4	0FF 0N 1 2 3 RS-485
RS-485 3 (2A,2B)	5	1 2 3 RS-485
Reserve	6	1 2 3 RS-485

Table 1 - Configure EOL Resistor of 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 <u>6.3 Add Device on the Software</u> to add the controller on the software.
- 3. Then click Access > Device > I/O Board > New to display the new page.

ARMATURA ONE	Access		
«	☆ / Access / Device / I/O Board		
A Device ^	Device Name Q O		
Device	€ Refresh + New 🗇 Delete		
I/O Board			
Door	I 1 New X		
Reader	LO2828 Name' AHEB-0808 1 Device Name' Click to select		
Auxiliary Input			
Event Type			
Daylight Saving Time	<u>16923</u>		
Device Monitoring			
Alarm Monitoring			
Real-Time Monitoring	Save and New OK Cancel		
Topology Management		b)	Ľ

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

						×
Devi	ce Name	Serial Number		Q, Ð		
Alterr	native		Selec	ted(1)		
	Device Name	Serial Number		Device Name	Serial Number	
0	10.8.16.227	CN30422260002	۲	10.8.16.176	CN30422470001	
۲	10.8.54.140	3635210300005				
0	10.8.54.139	CN30322260001				
0	10.8.16.177	CN30222470001				
0	10.8.16.92	CN30122200017				
k	< 1-23 >	>  50 rows per page ~ 🛛 🐬				
		ок	Cance			

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

			New		×		
Name*	AHEB-0808 1		Device Name <sup>®</sup>	10.8.16.176			
Parameters							
Protocol Type"	OSDP	~	I/O Board Type*	AHEB-0808	~		
RS-485 Port*	RS-485 PORT2	~	RS-485 Port Setting				
RS485 Address*	1						
After the configurati	on, you need to restart t	ne device	e to take effect.				
				8			
			0				
	Save and New OK Cancel						

- **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	<u> </u>
RS-485 Port 3		
Protocol	OSDP	~
	9600	~

#### **Port Introduction**

Parame	eter	Introduction		
DS 495 Dort 1	Protocol	Armatura RS-485/OSDP/Aperio		
R5-485 Port 1	Baudrate	4800/9600/19200/38400/57600/115200		
DS 495 Dort 2	Protocol	Armatura RS-485/OSDP/Aperio		
K3-403 PUIL 2	Baudrate	4800/9600/19200/38400/57600/115200		
DC 495 Dort 2	Protocol	Armatura RS-485/OSDP/Aperio		
RS-485 Port 3	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.

ARMATURA ONE	- 111 /	Access								
«	☆ /			I/O Board						
A Device			2			~ Q	Ð			
Device	÷	Refresh	+ New	Delete						
I/O Board						Number	I/O Board Type	RS485 Address	Protocol Type	
Door						New			×	
Reader		1 <u>00808</u>	Na	me" 🧧	AHEB-0808 1	Devi	ice Name* 🛛 👩	Click to select		
Auxiliary Input Auxiliary Output		<u>16.92-1</u>								
Event Type										
Daylight Saving Time		<u>16.92-3</u>								
Device Monitoring		<u>16.92-4</u>								
Alarm Monitoring		<u>16.92-5</u>								
Real-Time Monitoring		<u>16.92-6</u>			Save an	d New OK	Cancel			

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

					×
Devi	ce Name	Serial Number		Q. Ð	
Alterr	native			Selected(0)	
	Device Name	Serial Number		Device Name Serial Number	
0	10.8.14.200	AJYS183160082 5			
0	10.8.14.203	CN30422200034	6		
0	10.8.14.226	CN30122200004			
0	10.8.51.94	CN30122200002			
	7 7 -				
15	< 1-4 >	50 rows per page V			
				Cancel	

4. Enter each parameter.

			New		×
Name*	1003		Device Name*	192.168.163.202	
Parameters					
Protocol Type*	Арегіо	~	I/O Board Type <sup>*</sup>	AH30	~
Device Addressing Mode*	Normal Address Offse	t 🗸			
RS-485 Port*	RS-485 PORT3	*	RS-485 Port Setting		
RS485 Address*	3				
After the configuration, ye	ou need to restart the device	e to ta	ake effect.	8	
			0		
	Save and Nev	V	OK Cancel		

- 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.

»	<u>۵</u> ,	Access / Dev	ice / I/C	) Board								
-	Devi	ce Name		Area	Name	~ q, .	0					
۰	Ð	Refresh +	- New	🗊 Delete								
8		Name		Area Name	Owned Device	Number	I/O Board Type	RS485 Address	Protocol Type	Serial Number	Firmware Version	Operation
	o	11		Area Name	10.8.51.94		AH30		APERIO			്
		<u>11_0</u>		Area Name	10.8.51.94		AH30		APERIO			ഭ
		11_1		Area Name	10.8.51.94		анзо	The operation	n succeeded!			Ċ
	0	<u>11_2</u>		Area Name	10.8.51.94		AH30	44	APERIO			്
		<u>11_3</u>		Area Name	10.8.51.94		AH30	60	APERIO			Ľ
		<u>11_4</u>		Area Name	10.8.51.94		AH30	76	APERIO			്
	0	<u>11_5</u>		Area Name	10.8.51.94		AH30	92	APERIO			Ľ
		<u>11_6</u>		Area Name	10.8.51.94		AH30	108	APERIO			ഭ
		<u>11_7</u>		Area Name	10.8.51.94	9	AH30	124	APERIO			്

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

		۵ י	Access / De	evice / Door									
🖴 Device		Do	or Name	Own	ned Device	Area N	ame		More 🗸 🍳 🕤				
Device			🕑 Refresh	Remote Opening	Remote Closing	🗸 Enable 🛛 🖉 Dis	able 🚊 Cancel /	Narm	Remote Normally Open	i∃ More ~			
I/O Board			Door Name	Area Name	Owned Device	Serial Number	Door Number	Enable	Active Time Zone	Door Sensor Type	Verification Mode	Owning Board	Operations
Door			<u>10.8.51.94-3</u>	Area Name	10.8.51.94	CN30122200002		0	24-Hour Accessible	None	Automatic Identification		ď
Reader		٥	<u>10.8.51.94-4</u>	Area Name	10.8.51.94	CN30122200002		0	24-Hour Accessible	None	Automatic Identification		C
Auxiliary Input			<u>10.8.51.94-5</u>	Area Name	10.8.51.94	CN30122200002		8	24-Hour Accessible	None	Automatic Identification	11_0	Ľ
Auxiliary Output		-	40.0 54.04.0	Area Mana	10.0 54.04	01/20(22200002			24 Hour Assessible	News	Automatic Identification		-
Event Type		U	10.6.51.94-0	Area Name	10.6.51.94	CN30122200002			24-nour Accessione	None	Automatic Identification	11_1	Ľ
Daylight Saving Time			<u>10.8.51.94-7</u>	Area Name	10.8.51.94	CN30122200002			24-Hour Accessible	None	Automatic Identification	11_2	٢ C
Device Monitoring		٥	<u>10.8.51.94-8</u>	Area Name	10.8.51.94	CN30122200002			24-Hour Accessible	None	Automatic Identification	11_3	Ľ
Alarm Monitoring			<u>10.8.51.94-9</u>	Area Name	10.8.51.94	CN30122200002			24-Hour Accessible	None	Automatic Identification	11_4	ď
Real-Time Monitoring	,		<u>10.8.51.94-10</u>	Area Name	10.8.51.94	CN30122200002		8	24-Hour Accessible	None	Automatic Identification	11_5	ď
Access Control			10 9 51 04 11	Aroa Nama	10 9 51 04	CN20122200002			24 Hour Accessible	None	Automatic Identification	11 6	-11
Se Advanced Functions		<u> </u>	10.0.31.54-11	Area Name	10.0.31.84	GN30122200002			241100 ACCESSION	NUIE	Automatic reentinearton	11_0	6
📄 Reports		٥	<u>10.8.51.94-12</u>	Area Name	10.8.51.94	CN30122200002	12	8	24-Hour Accessible	None	Automatic Identification	11_7	C
Pad Resource		K	< 1-17	> >    50 rows pe	r page 🖌 🕴 Jump To	1 /1 Page   Tota	al 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.



Short Circuit

**Broken Circuit** 



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<sup>2</sup>, 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<sup>2</sup>).
- 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 20hm. 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<sup>2</sup>).

## 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.

	÷ ۳	101
Metwork Info	ລີ Network Info	
📟 Serial Setting	LAN 1	
✤ Diagnostics	LAN 2	
(i) About		

#### Status of lcons:

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.

•		RMAT Horizon Series Distribu			
	•				
		English	×		
		A Usemame			
		B Password	ø		
		Login			
				ı.	

	First time login Armatura Access Co	ontroller, you are required to set up an administra	tor	
	for future device management.			
	-The password shall be no less tha	n 8 characters in length and must contain at leas	a	
Te	combination of the following three of	character types	1 1 1 1 1 1 1	
	-At least 1 Lowercase Letter		Constant of the	
	-At least 1 Uppercase Letter		10 301	
	-At least 1 Special Character			
	-At least 1 Number			
	User Name:	armatura		
	* New Password:			
	* Confirm New Password:			4
		Save Cance		

### 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.

ARMATURA						👥 armatura 🔻
■ Overview ×	Ethernet					
: Network	Port1 Port2					
Connection	IPv4		Edit	IPv6		Edit
Ethernet	Mode	Manual		Mode	Auto	
Wian	Address	192.168.163.58		Link Local Address	1000-350903083000-352054	
Access Filter	Subnet Mask	255.255.255.0		Address		
Certificate	Primary Dns	114.114.114.114		Galeway		
Parameters	Alternate Dns	8.8.8.8				
O Maintenance Y	MTU	1500				
	802.1x		Edit			
- Cystom	Function	Disable				
<u>&lt;</u>						

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

ARMATURA						👥 armatura 👻
Overview	Ethernet					
: Network	Port1 Port2					
Connection	IPv4		Edit	IPv6		Edit
Ethernet	Mode	Manual		Mode	Auto	
Wlan	Address	192.168.2.202		Link Local Address	1000-2000/08/1000-153004	
Access Filter	Subnet Mask Gateway	255.255.255.0 192.168.2.254		Address Gateway		
Certificate	Primary Dns	114.114.114.114				
Parameters	Alternate Dns MTU	8.8.8.8				
C Maintenance V						
System v						

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

- Click Network > Wlan to enter the wlan setting interface on the webserver. Then click the 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.

ARMATURA						armatura 👻
Overview Y	Wlan					
:e: Network	Hotspot Advanced					
Connection	Refresh Add					
Ethernet	104	Band	Authentication Mode	Signal Intensity	Status	Operation
Wlan	Texa.7071.00	5G	WPA-PSK/WPA2-PSK	at	Unconnected	Connect
Access Filter	20° tores de	Connection		× at	Unconnected	Connect
Certificate	Appropriate the second s			at	Unconnected	Connect
Parameters	PPLAN	* Password **		all	Unconnected	Connect
Maintenance	Notice Billion Bill	If you are using the advanced net	work, please set up advanced settings befor	are connect.	Unconnected	Connect
System ¥	1925			Cancel	Unconnected	Connect
	Poss	2.4G	WPA:PSK/WPA2-PSK		Unconnected	Connect
	1996 (1997 (	2.4G	WPA-PSK/WPA2-PSK	att	Unconnected	Connect
	Baser, 30757,0003	50	WPA-PSK/WPA2-PSK	att	Unconnected	Connect
	10410	2.4G	WPA-PSK/WPA2-PSK	att	Unconnected	Connect
		2.4G	WPA-PSK/WPA2-PSK	att	Unconnected	Connect
	**	2.4G	WPA-PSK/WPA2-PSK	att	Unconnected	Connect
<u>&lt;=</u>	TaxAN M	246	WPA-PSK/WPA2-PSK	- 11	Unconnected	Connect

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.)

ARMATURA	1									🚺 armatura 🗸
Overview	~	Wlan								On
:•: Network	^	Hotspot	Advanced							
		Refresh	Add 1							
			SSID		Band	Authentication Mode	Signal	Intensity	Status	Operation
Wlan			Term.7071.00		5G	WPA-PSK/WPA2-PSK		al	Unconnected	Connect
			24Phone.do	Connection			×	al	Unconnected	Connect
			1115.000	0010	6	h in a		al	Unconnected	Connect
			query state.	* SSID * Password		lest 1			Unconnected	Connect
Maintenance	×.		heleo#105.81	If you are usin	g the advanced n	network, please set up advanced settings befor	re connect.		Unconnected	Connect
System	~		Trank.			Counced	Canad		Unconnected	Connect
			In Address of the		2.4G	WPA-PSK/WPA2-PSK			Unconnected	Connect
			10,0		5G	WPA2-PSK			Unconnected	Connect
			Association		5G	WPA-PSK/WPA2-PSK			Unconnected	Connect
			**		2.4G	WPA-PSK/WPA2-PSK			Unconnected	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.

ARMATURA						💽 armatura 👻
Overview ~	Wlan					On
:•: Network	Hotspot Advanced	1				
Connection	IPv4	_	Edit	IPv6		Edit
Ethernet						
	Made	DHCP		Mode	Auto	
Wlan	Address			Link Local Address	WE AND STREET WAS	
Access Filter	Subnet Mask			Address		
	Gateway			Gateway		
Certificate	Primary Dns	114.114.114.114				
B	Alternate Dns	8.8.8.8				
Parameters	MTU	1500				
Maintenance v						
Svetem v	802.1x		Edit			
a oyuun	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

Connection	Server     OPrimary Controller	
Server	MQTTS V	
Port	1884	
Key File	Upload CF-20210407.zip	
ProductKey	Shothork	
DeviceName	ATM12121212131	
DeviceSecret	jathelijatholjen	
Host Certificate		
Please download th	e certificate and import in Device Management in software	Download
Software Certificat	e	
After Upload with K	ey file, Ceritificate will import automatically	View

- 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.

Connection	Server	Primary Controlle	r	
	0	0		
Comm	TCPIP	() RS485		
Address	wss 🗸	2.96(21).006		
Port	8098			
Host Certificate				
Please download a	and upload in primary co	ontroller 'secondary controller' s	etting page	Download
Primary Controlle	er Certificate			
Please download f	rom primary controller '	secondary controller' setting pa	je and upload here	Upload
Save				

2			
Comm		• 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.



## 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**.

ARMATURA		👤 armatura 👻
Overview ~	Connection	
: Network	Server/Primary Controller Setting	
Connection	Connect to Server 2 Primary Controller	
Ethernet	* Server MOTTS V	
Wlan	* Port 8088	
Access Filter	Key File zip	
Certificate	ProductKey	
Parameters	DeviceName	
G Maintenance v	DeviceSecret	
<ul> <li>System</li> </ul>	Host Certificate	
	Please dow Dicertificate and upload it to 'Device Management' menu on software Download	
	After Upload with Key file, Server's Ceritificate will import automatically View	
	Save	
<u>&lt;=</u>		

## 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.

## ARMATURA

ARMATURA ONE	Access								Ì	۲	۲
«											
📾 Device 🔷 🔺								, Q, Đ			
Device	🔿 Refresh 🕂 New 🗉 Delete 🖸 Export 🤍 Search 💋 Control 🔹 🕲 Set up 🍷 🖓 View and Get Device Info 🍷 🌐 Communication :										
I/O Board					Search				Version		
Door	Search	e found? Dowr	load Search Tools	to Local Disk			7.8.3033 Feb 7 2021				
Reader	Total Progress Searched devices count 5 Number of devices added:5										
Auxiliary Input	IP Address		Device Type		Serial Number		Reset				
Auxiliary Output	IP Address	MAC Address	Subnet Mask	Gateway Address	Serial Number	Device Type	Set Server	Operations	0.0.6 May 13 2022		
Event Type			255.255.254.0		10001080800	ADUTIO		Add 4	0.0.6 May 10 2022		
Daylight Saving Time					-	-		This device has been added	0.0.5 Apr 24 2022		
Device Monitoring			255.255.255.0		00000-000 E	Margan Pro	Negative 2.75 (1988)	This device has been added	0.0.6 May 18 2022		
Alarm Monitoring								This device has been added			
Map Configuration											
Real-Time Monitoring			255.255.255.0	NEW ALL	interest of the	100000000	Wpc.710.101.110.000	This device has been added			
Topology Management 🌱											
Advanced Functions ~											
🖥 Reports 🛛 👻					Close						
Pad Resource ~	K K 1-6	> >    5(	) rows per page	Ƴ │ Jump To	1 /1 Page	Total of 6 records					>

	ARMATURA ONE		Access										$\textcircled{\basis}$	
		«	🖒 / Access /	Device /	Device									
-	Device		Device Name		Se	rial Number		IP Address	6		More∨ Q	Ð		
	Device		🕂 Refresh	+ New	🗓 Delete	C Export	Q Search	≣ Control ▼	💮 Set up 🔻	℃ view	and Get Device	Info 🔻	① Commu	n
	I/O Board		Device Nar	ne	Serial Number	Area Name	Network Cor Mode	nnection IPAd	Set Bg-Verifica Set Device Tim	tion Options le Zone		tegist	ter Device F	ir
	Door		0 34.5	200	11-0210800-0	Area Name	Wired	90 B.	Set as Registra Modify the Find	ition Device perprint Identi	fication Thresho	ø	A	C
	Reader		0 34.34	-0	14401080040	Area Name	Wired	50.6	Set Device In/C	Out State		8	A	C
	Auxiliary Input		0 34.5	2	0000017000	Area Name	Wired	10.6	Set cloud serve	er parameters		3	A	c
	Event Type		· 5···	323		Area Name	Wired	10.6	Set date time			3	A	C
	Daylight Saving Time		0 34.5	ans	000003000	Area Name	Wired	52.6	Set access rec			2	A	c
	Device Monitoring								Set the timing s	anagement sleep time				
	Alarm Monitoring								Set Hep param	eters				
¢	Access Control								Set Extended F	arameters				
<b>8</b> .	Advanced Functions								RS-485 Port S	etting				
	Reports	~												

RS-48	5 Port Setting	×
RS-485 Port 1		
Protocol	Armatura RS-485	
Baudrate	9600	
RS-485 Port 2		
Protocol	OSDP	0
Baudrate	9600	0
RS-485 Port 3		
Protocol	OSDP	
Baudrate	9600	
9 ок	Cancel	

## 6.4 Configuring the Reader

- 1. When an RS-485 reader is connected. Refer to <u>4.2.7 RS-485 Reader Wiring</u> 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.

	ARMATURA ONE		A	cess												) ھ
		« {	<u>ن</u> د	Access / Device / I	Reader											
-	Device		Read	ler Name	Door Name			<b>Q</b> 0								
Device			e	Refresh + New	🗓 Dekete 📑 U	lpgrade the reader										
	I/O Board			Reader Name	Door Name	RS-485 Port	Number	Communication	Communication Address	In/Out	Bound camera	Verification Mode	Serial Number	Firmware Version	Owning Board	Operations
	Door	_1		2 -	10.0.000	3	2	Wiegand/RS	1	Out		[0] / / 📾	1	RD Ver 14.0.10	3	C 9
L	Reader Auxiliary Input			TR. BRID				Wiegand/RS				(a) / :::: / 🖂				Ľ (?),
	Auxiliary Output Event Type				100.0000			RS485		Out		[0] / / 📾				Ľ 8.
								Wiegand/RS				(a) / / E				Ľ 8
	Daylight Saving Time			10.000	100.0000			RS485		Out		[@] / / 📼				Ľ 8.
	Device Monitoring							Wiegand/RS				(a) / / Es				Ľ 8,
	Alarm Monitoring			THE OWNER.	10.000		8	RS485	8	Out		 `@`//■	ō			г <i>й. 12</i> .
	Map Configuration				100.00			D 9 496		In		~				-4 40
	Real-Time Monitoring							113403				_w, / / es				ш (X
	Topology Management			10.0.0	100.00.001			RS485		Out		(0) / :::: / 📼				Ľ (?)
				10.0.0	100.0000			Wiegand/RS				[0] / / 📼				Ľ 8
				10.0.0	100.000			RS485		Out		(@) / / 📾				Ľ 8
				-	100.00			Wiegand/RS				[0] / / EB				Ŀ 8.
ň	Access Control			10.0.0	100.000			RS485		Out		(8) / / 📾				Ľ 8
9	Advanced Functions			10.0.0	100.000			Wiegand/RS				[0] / / 📾				Ľ 8
6	Reports			-				RS485		Out		(a) / / 🖂				Ľ 8.
	Pad Resource				50 rows per page 🗸	/ Jump To 1	/2 Pa	ge Total of 51 re	cords							

	Edit		×
Name*	1-Out		
Number	2		
In/Out	Oln ⊚Out		
Door Name*			
Operate Interval	2		icond(0-254)
Verification Mode	[0] / :::: / 🗃		4
Communication Type	Wiegand/RS485	~	
RS-485 Port"	RS-485 PORT3	~	
Wiegand/RS485 <sup>®</sup>	1	~	
Wiegand Format	Auto	~	
	_		
<b>6</b>	Cancel		

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.

	New	×
Personnel ID 4	Department* Department Name V	
First Name Lee	Last Name Mick	
Gender	✓ Mobile Phone 12345678	
Certificate Type	Certificate Number	0
Birthday	Email	Charlenet Pire 4203440)
Hire Date	Position Name V	Browse Capture
Device Verification Password	Card Number	•
Person Type Employee	🗸 🛛 Biological Template Quantity 🛛 👰 0 🌐 0 🍟 0 🤿 0	
Threat Level	✓ Mobile Credential	
Access Control Elevator Control	Personnel Detail	
Levels Settings	Add Personnel Library	✓
General	Select All Unselect All Superuser No	×
	Device Operation Role Or	dinary User 🗸 🗸
	Delay Passage	
	Disabled	
	Set Valid Time	
	Save and New OK Cancel	

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

### **ARMATURA**

#### Armatura Horizon Controller User Manual



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.

ŝ	ARMATURA ONE	iii s	ystem				
		☆ /		nmunication / Product Definiti	ion		
×	General Settings			Product		9, Đ	
000	Data Management	÷	Refresh +	• New 🗒 Delete			
20			Product Name	Product code			Operations
				gc76I0hHkUPMHpEhUpwZ			
	Device Commands		AHDU		New	×	12 前
	Communication Statu			Product Name*	AHDU-1000		
	Product Definition			Remarks			
	Authorized Manageme						
	Communication Servio						
				OK	Cancel		
þ	Integration			> >   50 rows per page		/1 Page Total of 2 records	
<							>

#### 2. Add a device

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

ARMATURA ONE	System										
«	☆ / System / Communication / Authorized Management										
🗙 General Settings 🔹 👻	Device Name	vice Name Q, O									
😴 Data Management 🛛 👻	↔ Refresh + New C Export Key File										
🕹 Authority 🗸 🗸	Protocol mode Device Serial Device secret Product name Product code		Whether to Remarks authorize								
Communication											
Device Commands	best-mgtt CN3042     New X kUPMHpEhUpwZ		ø								
Communication Status	Product name* AHDU-1000 V										
Product Definition	Protocol mode" best-mątt v 🔒										
Authorized Management	best-mqtt CN3042 Serial Number' CN30422260005 O5CF1aL4Idv/T										
Communication Services	best-mgit CN303 CD5CF1aL4IdVT										
	Dest-matt CN302 CD5CF1aL4IdVT										
	L best-mqtt CN3012										
	best-mqtt 744021 VIC Cancel KUPMHpEhUpwZ										
	best-mqtt CN30422200017 HdtPTR86K5za1LFn8Cxf Access Device gc76l0hHkUPMHpEhUpwZ										
	best-mgtt     CN30422260001 srYRNApOl30KpZRQecLd     Access Device     gc76i0hHkUPMHpEhUpwZ										
Integration											

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**.

ARMATURA ONE	System									
«	1 System / Communication / Authorized Management									
🗙 General Settings 🛛 👻	Device Name Q 🕤									
🔓 Data Management 🛛 👻	Crefresh + New C Export Key File									
🤽 Authority 🗸 🗸	Protocol mode Device Serial Device secret Product name Product code	Module	Whether to Remark							
Communication ^	best-mqtt CN30422260005 2d7YFDb9T6HX2lKQPRXK AHDU-1000 ACzlP2ysrbqdyRslHivh									
Device Commands	B push Evont Kay File									
Communication Status	best-matt Number of selected devices 1 gc76I0hHkUPMHpEhUpwZ									
Authorized Management	Active Time									
Communication Services	best-mqtt     best-mqtt     Close     qX7q6wrKD5CF1aL4ldvT									
	best-mqtt CN30222470001 JI/MiNZD9/bYb2PeQeyD AHDU qX7q6wrKD5CF1aL4ldvT									
	best-mqtt 7440213800039 nJZnJFiBIPbyJerUaq8p Access Device gc76iDhHkUPMHpEhUpwZ									
	best-mqtt CN30422260001 srYRNApOl30KpZRQecLd Access Device gc76l0hHkUPMHpEhUpwZ									
Dintegration Y	K K 1-30 K 50 rows per page K Jump To 1 /1 Page Total of 30 records									

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

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

S auth_20221025092215.zip - Bandizip (Standard)     −     □     ×       File     Edit     Find     Options     View     Iools											
[→ Open		ြည် Extract		New	+ Add	 Delete	Test	Scan	Columns Co	de page	82
Auth_202	22102	5092215.4	zip	Name 744021: 301: 304 Server.co	20 ,.co .co t	^		Compressed 165 165 165 946	d Origir 16 16 18 18 1,34	al Type 0 CO文( 0 CO文( i0 CO文( 4 安全证 <sup>-</sup>	+ + +

**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.

	Horizon Series Distribut	UKA ted Controller		
9.0				
	English			
	A Username	ø		
	Login			
00			1	

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.

bad
v

- 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.

ARMATURA ONE	System
«	Arms Source Settings
🗙 General Settings 🛛 👻	Adms Service Port
😽 Data Management 🛛 👻	
🛃 Authority 🗸 🗸 🗸	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.
Communication	Project control file version
Device Commands	
Communication Status	Turn on encrypted transmission O No O Yes
Product Definition	MQTT Service Settings
Authorized Management	MQTT Service Port
Communication Services	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 Yes Connection is normal

• 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

	ARMATURA ONE			System							
		«	<u>۵</u> /	System / Cor	nmunication / Auth	orized Management					
×	General Settings		Dev	vice Name Q O							
0)2	Data Management		¢	Refresh +							
20	Authority			Protocol mode	Device Serial Number	Device secret	Product name	Product code	Module	Whether to authorize	
۲	Communication			best-mqtt	040000000000	accidents-analogistic	Rename Denise	g-700-to700-plicipal	acc	0	
	Device Commands			best-mqtt	040640348868	APPENDIX NO. KOTOK	HH31-1000	AC-POyeled/Sol No.		8	
	Communication Statu	IS	Π	push	3033340304				acc	0	
	Product Definition									×	
	Authorized Managem	ient		best-mqtt	040642296908	distriction (1954)	Arous Device	2/30/40/MgDrawl	acc	0	
	Communication Servi	ices	O	push	36562-0568005				acc	0	
				best-mqtt	0100403810001	косонскондьоты	eeu	47444000018.4MT	acc	0	
				best-mqtt	0.0003296804	ISASTRING-ISAGII	#00	9564000014.4MT	acc	0	
				best-mqtt	CHINESCOIL NEEDA	AAKDHINDVGqD	anos	4164655714-667	acc	0	
			o	best-mqtt	0400-00088841	Mitelizationhecity/We	Rooma Denter	p-NO+607409436pad	acc	0	
				best-mqtt	PARTONNES	NO. PRESIDENT	Pagent Device	Automation and an other	acc	0	
			Ω	best-mqtt	0406422988947	NETRORISIYETHICK	Arous Deko	2750/160/M1010-0-2	acc	0	

#### 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	Access				
«					
Device 🔨			nber IP Address		
Device 1			Export Search 🗄 Control 🗸 🗐		o 🖌 🌐 Communication 👻 🗖
I/O Board			Search		
Door	Search	No device found? Download Searc			
Reader			Searched devices count:29 Number of devices added:27		
Auxiliary Input			eo Sorial Number	Reset	
Auxiliary Output		MAC Device Name*	192 168 163 201	ver	
Event Type	10.0.57.220	lcon Type"	Door		This device has been added
Daylight Saving Time		dc:99: Area*	Area Name		
Device Monitoring		Add to Level			
Alarm Monitoring		dc:99: A [Clear Data in record) place	the Device when Adding] will delete data in the device		
Real-Time Monitoring		00:17:			
Topology Management		litter de:99:	OK Cancel		This device has been added
		dc:99.fe:00:0	IN THE REAL PROPERTY AND	HSC-1000	+ 0
🏟 Access Control 🛛 👻					¥* a
Advanced Functions *					
📑 Reports 🛛 👻					

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.

ARMATURA		٨	
11	Overview		Connection
	Network		Server: Secondary Controller
	Connection		Comm 3 0 TCPIP R5485
	Ethernet		* Ethernet ETH 0 V
	Wlan		Address 192.168.163.201
	Access Filter		* Port 6666 5
	Certificate		Host Certificate
	Parameters		Please download the certificate and upload it to the Secondary Controller' menu in the secondary controller 6 Download
	Maintonanco		Secondary Controller Certificate
	maintenance		Please download from the "Secondary Controller" menu in the secondary controller and upload it here 7 Upload
o	System		Image: Save   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].

ARMATURA						
Overview		Connection				
:•: Network	~	Server/Primary Co	ntroller Setting	2		
Connection	0	Connect to	O Server	Primary Contro	ller	
Ethernet		Comm		O RS485		
Wlan		* Address	wss 🗸	192.168.163.202	Enter the IP address of the p	rimary controller.
Access Filter		* Port	6666		6	
Certificate		Host Certificate				6
Parameters		Please download Primary Controll	the certificate and up er Certificate	load it to 'Secondary Con	troller' menu in primary controller	Download
🕑 Maintenance		Please download	from 'Secondary Con'	troller' menu in primary c	ontroller and upload here	Upload
System		Save	8		Upload the primary con	troller'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.

ARMATURA ONE	Access				admin
«	☆ / Access / Device				
🚔 Device 🔷				More 🗸 🔍 🕤	
Device 1	⊖ <sub>Refresh</sub> + <sub>Nev</sub>	n 🗓 Delete 📑 Export 🔍 Search	🗄 Control 🗡 🔇 Set up 🗡 🖓 View and		
I/O Board		Add	Sub-Device X	vice Firmware Version	
Door		IP Address Device Serial Number	MAC Address Status		
Reader		AHDU ENGLOCED	Authorized Successful		c û ··· 🧕
Auxiliary Input		19.5 19.2 AHDU DNB00215000	Authorized Successful		8 Add Sub-Device
Event Type		AHDU DARROCERRO	Authorized Successful		View child devices
Daylight Saving Time		AHDU DATECTION	H de Contract de Contra		
Device Monitoring					
Alarm Monitoring					
Real-Time Monitoring			0		
Access Control					
S Advanced Functions Y					
🖹 Reports 🛛 👻					
Pad Resource ×					

### 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 <u>7.1.1.1 Step 1 Add Primary Controller</u> 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.
| ARMATURA      |                               |
|---------------|-------------------------------|
| Overview ~    | Connection                    |
| 🔅 Network 🗠   | Server Secondary Controller 2 |
| Connection    |                               |
| Ethernet      | Port                          |
| Wlan          | Baudrate                      |
| Access Filter | 4                             |
| Certificate   | Save                          |
| Parameters    |                               |

**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.

ARMATURA			
🚔 Overview 🗸 🗸	Connection		
iș: Network ^	Server/Primary Co	ntroller Setting	
Connection	Connect to	O Server	Primary Controller
Ethernet	Comm		• RS485
Wlan	Port	RS-485 Port 1	
Access Filter	* Address	1	4
Certificate	Baudrate	9600	× 5
Parameters	Save	6	
🕒 Maintenance 🗸 🗸			

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.

ARMATURA ONE	Acces	55								(F)	admin	
×	🛆 / Aci											
🚔 Device 🖍							s –		ore 🗸 🔍	0		
Device 1	€ R			C Export	Q <sub>search</sub>		🙆 Set up 🗡					
I/O Board							Set Bg-Verifica	tion Options		Version		
Door		MARCH CO.	RS-	85 Port Setting	1		Set Device Tim Set as Registra	ie ∠one ition Device		MORE AND DE		
Reader			35 Port 1			nline	Modify the Fing Set Device In/C	erprint Identificati Out State	on Threshold	0.04 Dec 1 2021		
Auxiliary Input		Protoc Baudra	ol	Armatura RS-4 9600	485 🎽 🌀		Set Extended F Set up NTP set	Parameters rver	0	009 Dei 3 2003		
Event Type		MENO2					RS-485 Port Si ADU1460	etting	AC Ver	1000 Nord 1 2003		
Event Type Daylight Saving Time		RS-4	35 Port 2	OSDP		aline						
Device Monitoring		Baudra	ate	9600								
Alarm Monitoring		RS-4	35 Port 3									
Real-Time Monitoring		Protoc BILLEI Baudra	ol ate	OSDP 9600								
l opology Management		ILLIN L										
		-		Cance	1	nline						
Access Control     Advanced Functions												
E Reports												
Pad Resource												

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.

*	<u>ф</u> / А	ccess / Device / [	Device								
🚔 Device 🔷 🔨									~ <b>Q</b> , <del>O</del>		
Device 1	ۍ ا			🖸 Export	Q Search						
I/O Board					Add Sub-	-Device		vice			
Door			IP Address	Device Model	Serial Number	MAC Address	Status				
Reader			188 8.01	AHDU	CARGED BR U	AL 2018 10101/10	Authorized Successful				ŵ 🙆
Auxiliary Output			165.029	AHDU	04802150065	4.594.0015	Authorized Successful			3	Add Sub-Device
Event Type			-10.0 (0.00)	AHDU	Chillicological	419400379	Authorized Successful			Ľ	View child devices Webserver
Daylight Saving Time			184 8 20	AHDU	040102040004	4 10 a 10 0 al	Authorized Successful				ŵ····
Device Monitoring											
Alarm Monitoring											
Real-Time Monitoring											
ropology management											

# 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.

6	ARMATURA ONE		iii s	ystem						
			<u>∩</u> /	System / Cor	mmunication / Proc					
*	General Settings			luct Name	2	Product co		Q	Ð	
0)0	Data Management		Ð	Refresh	- New 🗓 Dele					
20				Product Name	Product code					Operations
					gc76l0hHkUPMI	HpEhUpwZ	2022-11-25 14:39:10			
	Device Commands			AHDU			New	×		
	Communication Statu				Product Name*		AHDU-1000			
	Product Definition	0			Remarks	1				
	Authorized Manageme									
	Communication Servio									
						ОК	Cancel			

## 2. Add a device

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

	ARMATURA ONE		s s	ystem										
			<u>۵</u> /			on / Autho	orized Managemer							
*					2		Q, O							
0)9			Ð	Refresh	- New									
20				Protocol mode	Device : Number							Module	Whether to authorize	
٢														
								New		×	kUPMHpEhUpwZ			
	Communication Status Product Definition	s 1				Product na Protocol m	me* ode*	AHDU-1 best-mq	1000 ~ įtt ~					
1	Authorized Manageme	ent				Serial Nurr	iber*	CN3042	22260005		0D5CF1aL4IdVT			
5						Remarks					CD5CF1aL4ldVT			
											CD5CF1aL4ldVT			
											kUPMHpEhUpwZ			
								ĸ	Cancel		kUPMHpEhUpwZ			
						2200017	HotPTR86K5za1	LFn8Cxf	Access Device	gc76l0h	HkUPMHpEhUpwZ			

**ARMATURA** 

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**.



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

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

<mark> </mark>	22102 Find	250922 <mark>1</mark> 5. <u>O</u> ptions	zip - B <u>V</u> iev	andizip (Sta v <u>T</u> ools <u>H</u>	ndard) <u>i</u> elp				_		×
[→ Open	¥	ि Extract	~	ि New	+ Add	L- Delete	Test	Scan	Columns Cod	e page	
A auth_202	22102	5092215.2	tip	Name 7440211 3012 304 Server.c	co .co .co	^		Compressed 165 165 165 946	d Original 5 160 5 160 5 160 5 1,344	Type CO 文件 CO 文件 CO 文件 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.

	Horizon Series Distribu			
19	English			
	A Usemame			
	A Password	ø		
	Login			
			1	

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.

ARMATURA			
Overview 🗸	Connection		
:•: Network ^	Server Second	lary Controller	
Connection	* Server		
Ethernet	* Port	1884	
Wlan	Key File	5 Upload 1. auth_20221207133838.zip	
Access Filter	ProductKey	ACzIP2ysrbqdyRsIHfvh	
Certificate	DeviceName	CN98(225):001 :	
Parameters	DeviceSecret	YvTWirWeSb8SB30IKHM	
🕒 Maintenance 🗸 🗸	Host Certificate		
R Custom V	Please download t	he certificate and upload it to "Device Management" menu on software	Download
System •	Software		
	After uploading the	key file, the servers certificate will be automatically imported	View
	6		
	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.

9	ARMATURA ONE		System
		«	Adms Service Settings
*	General Settings		Adms Service Port
0)8	Data Management		
2.	Authority		A 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.
۲	Communication		Project control file version
	Device Commands		
	Communication Statu	s	Turn on encrypted transmission O No O Yes
	Product Definition		MQTT Service Settings
	Authorized Manageme	ent	MQTT Service Port
	Communication Servio	ces	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 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

	ARMATURA ONE		s	ystem						
		«	<u>۵</u> /	System / Con	nmunication / Auth	orized Management				
*	General Settings		Devi	ice Name		Q, Ð				
0)0	Data Management		÷	Refresh +	- New 🖸 Expo	nt Key File				
20	Authority			Protocol mode	Device Serial Number	Device secret	Product name	Product code	Module	Whether to authorize
۲	Communication			best-mqtt	04000000000	actives and topics	Honora Danása	p.75046746pElisput	acc	0
	Device Commands	e	٥	best-mqtt	0406228808	2014/Del/NOCIKOPHOK	HED-100	AC-FOundation the		8
	Product Definition	2		push	30322940304				acc	0
	Authorized Managem	ent		best-mqtt	0406422968864	1011000PlangU00Atr	Arous Device	\$20000000000	acc	0
	Communication Servi	ces	٥	push	3650-056900				acc	0
				best-mqtt	010040313001	локовисковорьство		90904000114-0M	acc	0
				best-mqtt	010052298804	10#2701p=354(3)	ecu.	oliper(SCh4.4M	acc	0
				best-mqtt	04060043004	Masteringer	eros	47564606714-0AT	acc	0
				best-mqtt	0400-00388811	Mitgliczijehech/We	Rooma Denter	p-1044/949404pat	acc	0
				best-mqtt	P440310000008	schulled type/cepty	Room Device	presentation of the second	acc	0
				best-mqtt	048645398997	NOPTRONSprintfold	Rose Derix	2750150/042043a2	acc	0
				hoot matt	CNI20422260004					
þ	Integration	×	<	< 1-31	> >  50 rows	per page 🗡 🕴 Jump To 🧵	/1 Page T	otal 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.

ARMATURA ONE				
«				
🚔 Device 🖍			IP Address	
Device 1			🗣 🖓 Search 🛛 🚋 Control 🗸 🕲 Set up 🗸 🖏 V	fiew and Get Device Info 👻 🌐 Communication 👻 🗖
I/O Board	0 🚯		Search	
Door	Search	No device found? Download Search Tools to		
Reader			Searched devices count:29 Number of devices added:27	
Auxiliary Input			Sadal Number	
Auxiliary Output		MAC. Device Name*	192.168.163.201	ver Operations
Event Type		Icon Type*	Door 🗸	
Daylight Saving Time		dc:99: Area*	Area Name 🗸	
Device Monitoring		Add to Level dc:99. Clear Data in the Device whe	en Adding	
Alarm Monitoring		dc:99 [Clear Data in the Devic record), please use with	e when Adding] will delete data in the device (except event caution!	
Real-Time Monitoring		00:17:		
Topology Management		📧 dc:99:	OK Cancel	This device has been added
🌣 Access Control 💉			AHSC-1000	
Advanced Functions				
🖹 Deports 🗸 🗸				

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.

## <u>AHSC-1000</u>

- 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)

## <u>AHEB-0808</u>

- 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. If you do not agree to the relevant agreement or any of its terms, you must stop using our products and services.

#### I. Collected Information

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

- 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 <u>www.armatura.us</u> 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	×	0	0	0	0	0
Chip Capacitor	×	0	0	0	0	0
Chip Inductor	×	0	0	0	0	0
Diode	×	0	0	0	0	0
ESD component	×	0	0	0	0	0
Buzzer	×	0	0	0	0	0
Adapter	×	0	0	0	0	0
Screws	0	0	0	×	0	0

 $\circ$  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.



ARMATURA LLC www.armatura.us E-mail:sales@armatura.us Copyright © 2022 ARMATURA LLC. All rights reserved.