AHDU Series

IP-Based Biometric Door Unit

- Ultimate Authentication Performance
- PoE and 3rd Party Integration
- Threat Levels and Port Failover
- Advanced Access Control Functions
- Supervised and Programmable Inputs

Key Features

Ultimate authentication performance

Supports up to 400,000 (1:N) RFID card / mobile credential, 400,000 (1:1) & 50,000 (1:N) fingerprint, 100,000 (1:1) & 5,000 (1:N) facial, 5,000 (1:N) & 10,000 (1:1) palm authentication in one single controller.

PoE

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

Threat Levels

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

3rd Party Integration

Supports various reader protocols, including Armatura Explorer series readers, 3rd party biometric readers, along with 3rd party Wiegand and OSDP readers. Armatura One provides RESTful based API for 3rd Party software Integration.

Advanced Access Control Functions

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

Port Failover (TCP/IP coming soon) & Redundancy

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 redundancy 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 supervised inputs, which gradually avoids open or 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.

Dual System Rom Protection Design

To offer the best operation stability, durability, and safety and tackle different kinds of situations, such as an improper upgrade, cyber attack, and malware infections that completely render the ROM to inoperable status. Armatura's controllers are built with a dual ROM design, one of the ROMs acts as a primary ROM for the system startup, and the second layer ROM acts as a "Recover" ROM. When the primary ROM happens to fail or malfunction, the second layer ROM will automatically take over on your next controller board startup.

Scalable

Supports up to 384 inputs (when using AHEB-0216 IO expansion board) through OSDP V2.2 connection between boards. 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.

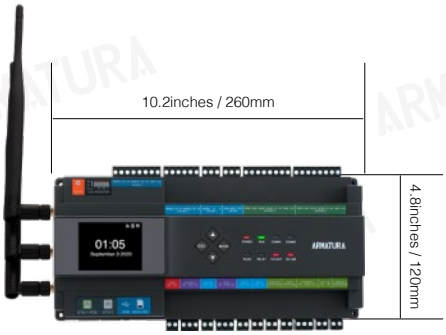
Advanced Communication

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.

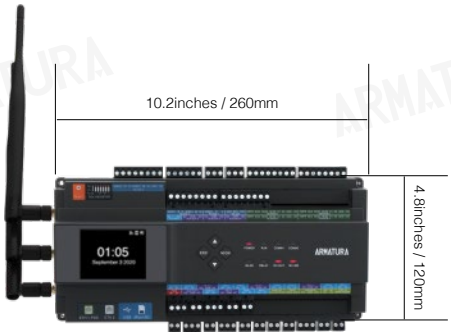
Cyber Security

Advanced Encryption Standard (AES) 256-bit algorithm for communication with Explorer series readers and I/O expansion boards through TCP/IP; AES 128 bit encryption to the readers and I/O expansion boards through OSDP V2.2 over RS-485.
AES128 / TLS 1.2 (with AES256) communication between Armatura One server and edge devices.
Communications between the Armatura One server and web-client are protected by HTTPS / TLS1.2 (AES256) or above
Enhanced cybersecurity level is provided by an additional crypto chip (Certified EAL6+ standard), providing dedicated storage and cryptographic functionality for the AHSC-1000 controller.
Supports IP/Mac address filtering functions, and VLAN isolation to enhance cybersecurity standard.

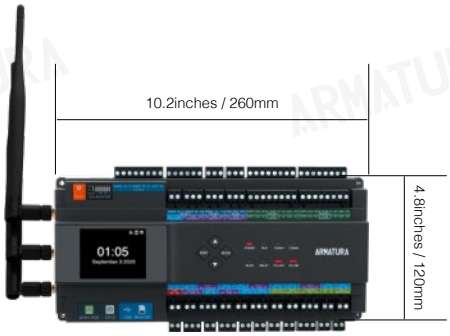
Dimensions of AHDU



AHDU-1160



AHDU-1260



AHDU-1460

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	BLE 5.2		
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: Armatura RS-485 / OSDP V2.2 Port 2: Armatura RS-485 / OSDP V2.2 Port 3: Armatura RS-485 / OSDP V2.2 (Configurable for Port Redundancy 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 Microchip Control Fire Alarm IO Input & REX Input for catastrophic situation		
Outputs	1 relay, 1* Form-C with dry contacts	2 relay, 2* Form-C with dry contacts	4 relay, 4* Form-C with dry contacts
Normally Open Contact Rating	5A @ 30Vdc resistive		
Normally Closed Contact Rating	5A @ 30Vdc resistive		
On-Board Monitor	Size: 2.4", Resolution: 320*240, TFT Monitor Quickly view status of board, connected doors and for configuration information display		

On-Board Webserver	Webserver for System Configuration and Management Dashboard for Controller Status Monitoring, Device Connection Status Monitoring & Configuration, Performance Status, server Primary Controller Setting, Network Status Monitoring & Setting, IP Access Filter, SSL / TLS Certificates Setting, Access Log Export, Controller Reset, Debug Status Monitoring, Operation Log Monitoring, User Management, Date & Time Setting, Daylight Saving Time Setting, NTP server Setting, General Status, Controller Information		
RFID Card Capacity	400,000 (1:N) / 800,000 (1:1)		
Maximum RFID Card Number Length	Supports up to 512bits card number length		
Mobile Credential Capacity	400,000 (1:N) (Bluetooth) 400,000 (1:N) (NFC) 400,000 (1:N) (Dynamic QR Code)		
Fingerprint Capacity	50,000 (1:N) / 100,000 (1:1)		
Face Capacity	5,000 (1:N) / 100,000 (1:1)		
Palm Capacity	3,000 (1:N) / 5,000 (1:1)		
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 1 (Wiegand) with on-board IO	3 (OSDP over RS-485) or 2 (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	384 (using Armatura AHEB-1602)		
Maximum Outputs	385 (using Armatura AHEB-0216)		
Maximum IO Board	24pcs (3*High Speed RS-485 communication)		

RFID / Biometrics Reader Interface	
Input Voltage	12 -24 Vdc +/- 10% regulated, 500 mA maximum each reader
Maximum Input Current	12 - 24 Vdc +/- 10% regulated, 500 mA maximum each reader
RS-485 Protocol	AES-128, OSDP Secure Channel
OSDP Mode	9600-115200 bps, OSDP V2.2, asynchronous, half-duplex, 1 start bit, 8 data bits, and1 stop bit. 3rd Party reader: support OSDP V2.2 or above
Wiegand	Read: support up to 128 bits / Write: Support 26 / 34 / 37 bit, and other customised card formats
Tamper Input (Wiegand)	TTL levels, high > 3 V, low < 0.5 V, 5 mA source/sink maximum
Buzzer Output (Wiegand)	TTL levels, high > 3 V, low < 0.5 V, 5 mA source/sink maximum
LED Output (Wiegand)	TTL levels, high > 3 V, low < 0.5 V, 5 mA source/sink maximum
Data Inputs	RS-485, OSDP and Wiegand standards supported. Maximum RS-485 /OSDP cable length: 3937ft. (1200m) Maximum Wiegand cable length: 328ft (100m)

IO Expansion Board Interface			
	AHDU-1160	AHDU-1260	AHDU-1460
RS-485 Protocol	AES-128, OSDP V2 Secure Channel		
OSDP Mode	9600-115200 bps, OSDP V2.2, asynchronous, half-duplex, 1 start bit, 8 data bits, and1 stop bit. Maximum cable length: 2,000 ft. (609.6m)		
Data Inputs	OSDP and Wiegand standards supported. Maximum cable length: 500 ft. (152m)		

Cable Requirement			
	AHDU-1160	AHDU-1260	AHDU-1460
Power & Relays	One twisted pair, 18 to 16 AWG		
Ethernet	CAT-5, minimum 330 ft. (100m)		
Ethernet Failover Port	CAT-5, minimum 330 ft. (100m)		
RS-485 Reader Port	9600-115200 bps, asynchronous, half-duplex, 1 start bit, 8 data bits, and1 stop bit. One twisted pair with drain wire and shield, 120 ohm resistance, 22-18 AWG, Maximum cable length: 3937ft (1200m)		
RS-485 I/O Device Port	9600-115200 bps, asynchronous, half-duplex, 1 start bit, 8 data bits, and1 stop bit. One twisted pair with drain wire and shield, 120 ohm resistance, 22-18 AWG, Maximum cable length: 3937ft (1200m)		
RS-485 Failover Port	9600-115200 bps, asynchronous, half-duplex, 1 start bit, 8 data bits, and1 stop bit. One twisted pair with drain wire and shield, 120 ohm resistance, 22-18 AWG, Maximum cable length: 3937ft (1200m)		
Wiegand Port	20 AWG shielded Wiegand wire, 328ft. (100m)		

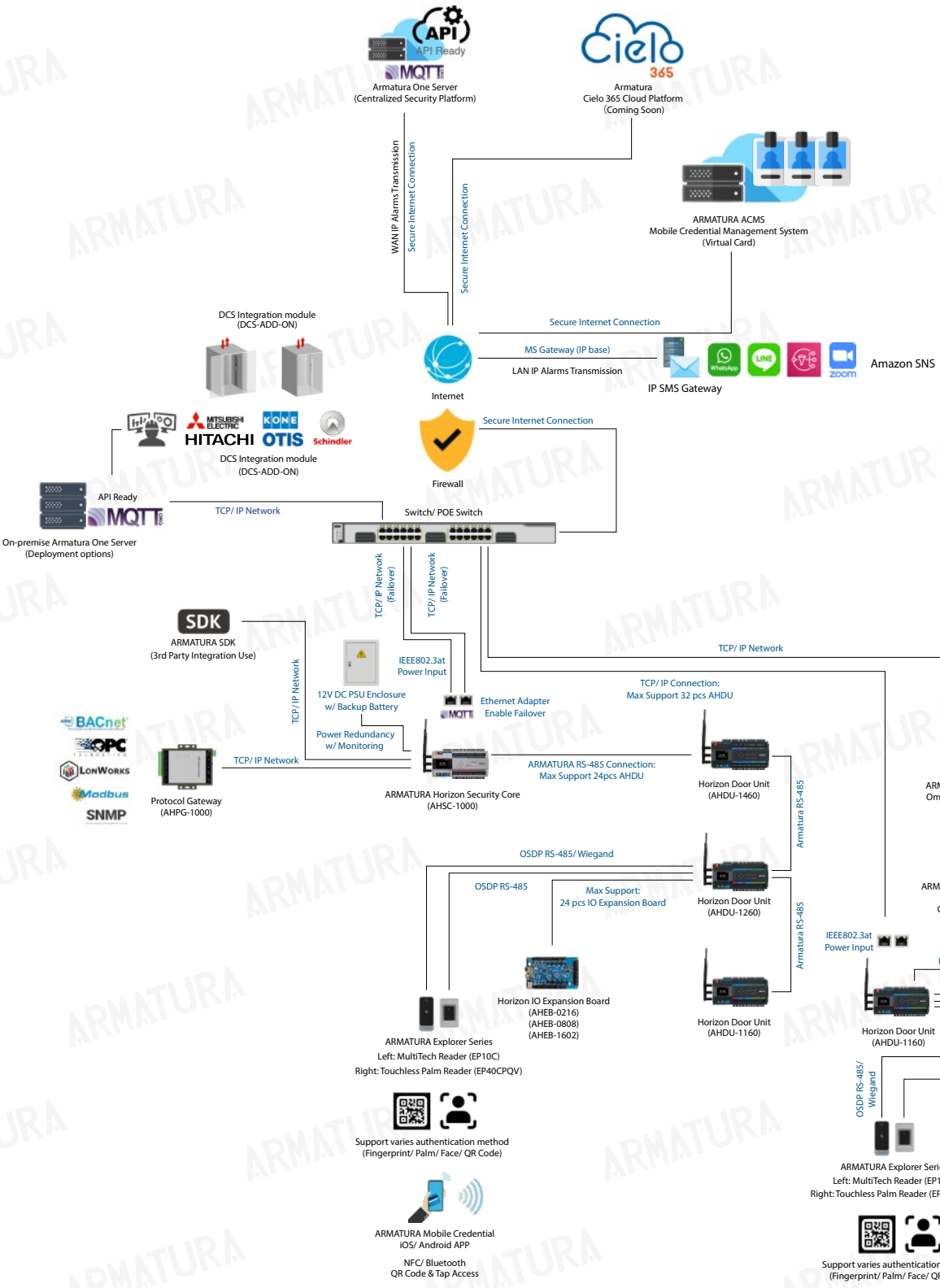
Mechanical			
	AHDU-1160	AHDU-1260	AHDU-1460
Dimensions	4.8” W x 10.2” L x 2.5” H (122 x 260 x 62.5mm)		
Weight	30oz (830g)	30oz (830g)	30oz (830g)
DIN Rail Mounting	Supported DIN35 Rail Compatible with UTA89 Din Rail Adapter for screwing on switchgear (Sold Separately) Wall mount		
Housing Material	ABS-PC UL-94 V2		

Environmental			
	AHDU-1160	AHDU-1260	AHDU-1460
Operating Temperature	-22°F ~ 158°F (-30°C~70°C), Operating & Storage		
Operating Humidity	0-95% RHNC		
Certification(s)*	CE, FCC, UL, RoHS, UL294		
Security Rating	Secure Data Storage in EAL 5+ Certified Crypto Chip		

Software Interface			
	AHDU-1160	AHDU-1260	AHDU-1460
TCP/IP Mode	Ethernet: 100Base-TX		
TCP/IP Protocol	NTP, SNMP V2 /V3, 802.1X, VLAN, SSH, MQTT, IPv4, IPv6, DNS, DDNS		
TCP/IP Encryption	Complies with TLS1.2, AES-256 end to end secure communication channel		
TCP/IP Communication	Spada Protocol over MQTT		
Supported Software	Armatura One Security System		

ARMATURA

Armatura System Diagram



ARMATURA

Address:190 Bluegrass Valley Parkway, Alpharetta, GA 30005
Phone: + 1 (470) 816-1970
Email: sales@armatura.us
Website: www.armatura.us