

Antenna Link ALD-200 High-Reliability Transmission Line Dehydrator

Includes Model Numbers:

ALD-200i – Indoor Rack Mount Model

ALD-200e – Outdoor Model

User Manual

*Antenna Link Products by
WIWORLD Co., LTD.*

Doc P/N: ALD-200-UM
Revision: 260930b

Contents

I. General Information	6
1. Introduction.....	6
2. Description.....	6
3. Theory of Operation.....	10
3.1. Overview.....	10
3.2. Main Components Related to Operation	10
3.3. Startup Sequence	11
3.4. Drying Operation	12
3.5. Purging (Regeneration) Operation.....	13
3.6. Pressure Control, Monitoring, and Alarms.....	13
3.7. Shutdown	13
3.8. Operating Sequence	15
4. Components	17
5. Drawing	20
5.1. Drawing of ALD-200i (Indoor model)	20
5.2. Drawing of ALD-200e (Outdoor model).....	21
II. ALD-200i (Indoor model).....	23
1. Front Panel Configuration	23
2. Back Panel Configuration.....	24
III. ALD-200e (Outdoor model)	26
1. Side Panel Configuration	26
1.1. External Port Connection and Usage Guidelines.....	26
2. Inner Panel Configuration.....	28
2.1. Power Connection and Wiring Instructions.....	29
IV. Indicator and Control.....	32
V. WEB Interface.....	39
1. Web access and accounts.....	39
1.1. First access and certificate trust.....	39
1.2. Initial administrator setup	40
2. Monitoring with the web interface.....	40
2.1. Status.....	40
2.2. Hardware.....	43
2.3. Log Graph.....	44
3. Operating settings and manual controls.....	46
3.1. Alarm settings and failure mode.....	46
3.2. Standby	46
3.3. Manual canister selection and output tests	46

4. Network, time and security settings.....	47
4.1. Network configuration.....	47
4.2. Device clock	48
4.3. RTC fine calibration	48
4.4. HTTPS certificates.....	49
5. Identity provider sign in.....	49
5.1. OpenID Connect	49
5.2. Supported login method.....	49
5.3. Certificate trust relationships	50
5.4. Information to obtain from the identity administrator	50
5.5. Role claim format	51
5.6. Commissioning procedure	52
5.7. Keycloak configuration example	52
5.8. Microsoft Entra ID configuration example.....	52
5.9. Okta configuration example	53
5.10. Auth0 configuration example	53
5.11. Other providers and unsupported profiles	54
5.12. Sessions logout and recovery.....	54
5.13. Diagnosing OIDC login failures.....	55
5.14. Verify your installation.....	55
6. Firmware updates and recovery	56
6.1. Updating firmware through the web interface	56
6.2. Reset choices	56
6.3. Physical account recovery	56
VI. REST API	58
1. Scope and connection model	58
1.1. Base URL.....	58
1.2. Model and option handling.....	58
2. Authentication and authorization.....	59
2.1. First read with curl.....	59
2.2. Request example conventions.....	60
3. Responses errors and request discipline	60
3.1. Polling and concurrency	61
4. Monitoring resources	61
4.1. Status fields and units	62
4.2. Canister state and condition fields	62
4.3. Heartbeat and diagnostics	63
5. Alarms and alarm history.....	63
5.1. History	64

5.2. Clearing an alarm.....	64
6. Alarm setpoints and failure mode.....	64
6.1. Failure mode resource.....	65
7. Hardware configuration.....	65
8. Manual control and maintenance.....	67
8.1. Pump runtime.....	68
9. Network accounts and time.....	68
9.1. Network	68
9.2. Passwords	69
9.3. Clock and time zone	69
9.4. RTC fine calibration	70
10. Certificate management.....	71
10.1. Generate a request.....	71
10.2. Upload a signed certificate	71
11. Firmware staging and application.....	72
11.1. Chunked upload	72
11.2. Verification and apply	72
12. Logs, resets and identity settings.....	73
12.1. CSV log download.....	73
12.2. System reset.....	73
12.3. OpenID Connect configuration.....	74
12.4. Discovery and signing key refresh	75
12.5. Provider connectivity and upgrade limits	76
12.6. Provider profile and claim interoperability.....	76
12.7. Token and client resource limits.....	77
12.8. Local session lifecycle.....	77
12.9. Provider acceptance tests	78
13. Compatibility notes and integration acceptance	78
13.1. Changes from the distributed manual	79
13.2. Integration acceptance checklist	79

Abbreviation

AC	Alternating Current
ALD	Antenna Link Dehydrator
API	Application Programming Interface
C	Celsius
CFM	Cubic Feet per Minute
CSR	Certificate Signing Request
DC	Direct Current
DHCP	Dynamic Host Configuration Protocol
DN	Down
DNS	Domain Name System
EMI	Electromagnetic Interference
ENT	Enter
EPDM	Ethylene Propylene Diene Monomer
GND	Ground
hex	Hexadecimal
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
JSON	JavaScript Object Notation
kg	Kilogram
L	Line
LAN	Local Area Network
lbs	Pounds
OLED	Organic Light Emitting Diode
LED	Light Emitting Diode
mm	Millimeter
N	Neutral
NPT	National Pipe Thread
OEM	Original Equipment Manufacturer
psi	Pounds per Square Inch
psig	Pounds per Square Inch Gauge
RBAC	Role-Based Access Control
REST	Representational State Transfer
RF	Radio Frequency
RJ45	Registered Jack 45

SD	Secure Digital
SMPS	Switched-Mode Power Supply
TLS	Transport Layer Security
U	Rack Unit
UI	User Interface
URL	Uniform Resource Locator
VAC	Volts Alternating Current
VDC	Volts Direct Current
W	Watt
Wh	Watt-hour
YAML	YAML Ain't Markup Language

I. General Information

1. Introduction

This document describes the ALD-200 Dehydrator manufactured by WIWORLD, including its product overview, operational methods, operating procedures, as well as the web-based interface and REST API for system monitoring and equipment control.

2. Description

ALD-200 High-Reliability Transmission Line Dehydrator

The ALD-200 is a high-reliability automatic transmission line dehydrator developed by WIWORLD, designed to remove moisture from RF transmission lines and antenna systems. By continuously supplying ultra-dry air with a dew point below -40°C , it effectively prevents condensation and moisture accumulation, ensuring stable system performance and long-term protection against corrosion.

The unit is specifically engineered for use in broadcast, telecommunications base stations, and satellite communication systems, where maintaining transmission quality and preventing internal corrosion are critical.

The ALD-200 supports Ethernet-based monitoring, a secure HTTPS web interface, REST API integration (OEM-supported), and features an integrated OLED display with intuitive front-panel control. This makes it suitable for a wide range of RF, telecom, and broadcast applications.

To accommodate different installation environments, the ALD-200 is available in two configurations:



Figure 1. ALD-200i (Indoor model)



Figure 2. ALD-200e (Outdoor model)

- Indoor model: 19-inch rack-mount type, ALD-200i
- Outdoor model: Extended temperature operation, waterproof, dustproof, ALD-200e

Key Features and Advantages

The ALD-200 Series is a high-performance dry air system designed to deliver ultra-low dew point air, ensure reliable operation in harsh environments, and provide advanced monitoring capabilities—offering a comprehensive solution for maintaining the stability and long-term reliability of RF transmission lines.

The key features and advantages of the ALD-200 Series are as follows:

1. Superior Dry Air Performance

- Continuous supply of ultra-dry air with dew point below -40°C
- Dry air flow rate:
 - Normal Operation: 2.0 L/min

- Purge Boost Operation at Low Output Pressure: During 80% of the operating cycle, the unit delivers dry air at 2.0 L/min.
 - Maintains low dew point continuously—even when system pressure is achieved (dew point remains in specification when output dry air flow rates are very low)
2. Continuous Operation using alternating desiccant canister technology
- Maintains pressure and supplies dry air continuously while purging humid canister
 - Ensures uninterrupted protection of RF transmission lines
3. Reliable Operation in Harsh Environments
- Fully operable during monsoon/rainy (high humidity) seasons
 - Capable of starting normal dry air supply within 20 minutes at -40°C ambient temperature.
 - Indoor model operates immediately under ambient temperature conditions
4. Compact and High-Performance Design
- Utilizes a compact desiccant canister
 - Achieves performance comparable to larger systems despite reduced size
 - Overcomes limitations of conventional systems that fail to sufficiently reduce dew point at very low temperatures
5. Advanced Monitoring and Sensor System
- Equipped with five temperature sensors:
 - One for each canister (A/B)
 - One at the humid air outlet (diffuser)
 - One at dry air output (with humidity/temperature sensor)
 - One at input air
 - Real-time monitoring of dry air conditioning (temperature & humidity)
 - Diffuser outlet reaching ~10°C indicates normal operation for ALD-200e (approximately 20 minutes after starting at -40°C)
6. Anti-Condensation Design
- Indoor model:
 - Evaporator maintains temperature above 80°C to prevent moisture formation
 - Outdoor model:
 - No evaporator (design optimized for external environment)
7. Enhanced Low-Temperature Durability

- Air pump diaphragm made of EPDM material, supporting operation down to -40°C
- Equipped with 15W heating pad to protect diaphragm under low-temperature conditions

8. Intelligent Sensor Calibration

- Internal temperature/humidity sensor integrated with proprietary calibration algorithm
- Achieves performance comparable to high-end sensors

9. Secure and Flexible System Integration

- Supports HTTPS-based secure web interface
- Provides REST API for system integration (OEM customization available)
- Ethernet-enabled remote monitoring and control

10. Safe and Stable Operation

- All solenoid valves automatically closed during power-off state, preventing ingress of humid air
- When the Dehydrator is powered on and the pressure in the transmission line reaches the user-configured pressure threshold (default: 0.5 psig), all valves are opened to rapidly release the pressure through the humid exhaust line.

11. Additional Functional Features

- Diffuser installed at humid air exhaust path
- Stable dry air supply regardless of pressure conditions
- Designed for long-term reliability and minimal maintenance

3. Theory of Operation

3.1. Overview

The ALD-200 is a dual-canister temperature swing adsorption (TSA) air dehydrator consisting of Canister A and Canister B. During normal operation, one canister performs the drying (adsorption) process while the other simultaneously undergoes purging (regeneration). The operating roles are automatically exchanged according to the control algorithm.

General product specifications and intended applications are described in Chapter 1 – General Information of this User Manual.

Unlike conventional dehydrators that utilize 3-way valves or resistive heater configurations, the ALD-200 employs seven independently controlled 2-way solenoid valves (SOL_1 through SOL_7) to precisely control each airflow path. The system also incorporates a feedback airflow circuit, which continuously re-circulates a small portion of the dried air back to the air pump inlet.

This chapter explains the operating principles of the valve-controlled airflow system, including:

- Startup sequence
- Drying operation
- Purging (regeneration) operation
- Overall operating sequence
- Valve operating matrix

3.2. Main Components Related to Operation

Detailed specifications of major components such as Canister A/B and the Air Pump are provided in Section 1.4 – Components.

The following components are directly related to the operating principles described in this chapter.

- SOL_1 to SOL_7
Seven independently controlled 2-way solenoid valves used to switch the internal airflow paths.
- Feedback Orifice
Recirculates a small portion of the dried air to the air pump inlet.

3.3. Startup Sequence

3.3.1. Power-Up and Valve Initialization

When AC power is applied, the unit automatically detects an input voltage between 100 and 240 VAC, eliminating the need for manual voltage selection.

All solenoid valves (SOL_1 through SOL_7) are designed to remain closed whenever power is removed. After power-up, the controller initializes the system and actuates each valve according to the programmed startup sequence.

Refer to Chapter 4 – Indicator and Control for LED indications during startup.

3.3.2. Canister Performance Evaluation (20 Minutes)

Before entering normal operation, the controller evaluates the drying performance of both canisters to determine their initial operating roles.

- 0 to 5min: Canister A operation (without dew point measurement)
- 5 to 15min: Canister B operation (with dew point measurement)
- 15min to 20min: Canister A operation (with dew point measurement)

After the 20-minute evaluation period, the controller assigns the initial operating mode according to the measured dew point.

Before entering normal operation, the controller evaluates the drying performance of both canisters to determine their initial operating roles.

- When Canister A reaches the user-configured dew point temperature (default: -40°C), Canister A begins purging, while Canister B begins drying.
- When Canister B reaches the user-configured dew point temperature (default: -40°C), Canister B begins purging, while Canister A begins drying.
- If both canisters fail to meet the target, the canister with better drying performance is assigned to drying, while the other begins purging.
- If both canisters satisfy the dew point requirement, the canister with the slightly lower performance begins drying, while the better-performing canister enters the READY state.

After the initial role assignment, the unit enters the normal operating cycle consisting of drying, purging, and READY modes.

3.4. Drying Operation

Example: Canister A is performing the drying process.

3.4.1. Air Compression and Supply

The air pump draws ambient air and compresses it while maintaining the system pressure below 0.3 psig.

The compressed air is directed through SOL_1 into the bottom of Canister A.

3.4.2. Moisture Adsorption

As the compressed air passes through the desiccant bed inside the canister, moisture is adsorbed by the desiccant.

By the time the air reaches the outlet, the dew point has been reduced to -40°C or lower.

3.4.3. Dry Air Distribution

The dry air exits the top of Canister A and flows through SOL_5 into the common dry-air manifold, where it is divided into two flow paths.

- **Feedback Path**
A small portion of the dry air passes through the Feedback Orifice and returns to the air pump inlet, forming a continuous recirculation loop.
- **Product Outlet Path**
The remaining dry air passes through the Humidity Sensor, SOL_7, and the Pressure Sensor before being delivered to the external dry-air outlet.

3.4.4. Continuous Air Delivery

During normal operation, the ALD-200 continuously supplies up to 2.0 L/min of dry air. The airflow control system is designed to maintain the specified dew point performance even under low-flow operating conditions.

3.5. Purging (Regeneration) Operation

The purging interval is automatically adjusted based on the humidity and flow rate of the incoming ambient air, with a maximum purging interval of 200 hours.

Example: Canister B is simultaneously undergoing regeneration.

3.5.1. Regeneration Air Supply

The dry air produced by Canister A is alternately directed to the external output and used for purging. The time ratio between supplying dry air to the external output and supplying dry air for purging is 4:1.

3.5.2. Heated Moisture Removal (Indoor Model Only)

Moist air leaving Canister B passes through SOL_4 into the Purge Block and Heater assembly. Any condensed moisture is reheated and vaporized before being discharged from the unit.

3.5.3. Exhaust

The warm, moisture-laden air is exhausted to the atmosphere through the Moist Air Exhaust port.

3.6. Pressure Control, Monitoring, and Alarms

System pressure is regulated through coordinated control of SOL_1, SOL_2, and the air pump.

Whenever system pressure deviates from the specified operating range, the controller automatically adjusts valve positions and pump operation to maintain positive internal pressure.

Additional information regarding alarms and pressure monitoring is provided in the corresponding sections of this manual.

3.7. Shutdown

When the main power is switched off, the air pump stops immediately and all solenoid valves (SOL_1 through SOL_7) automatically close.

For optimum performance, WIWORLD recommends allowing any canister currently undergoing regeneration to complete its regeneration cycle before disconnecting power. Regeneration status can be confirmed using either the web interface, the OLED display or the REST API (/status/canisters).

Interrupting power during regeneration may leave the canister only partially regenerated, resulting in reduced drying performance during the next startup.

3.7.1. Resuming Operation After a Brief Power Interruption

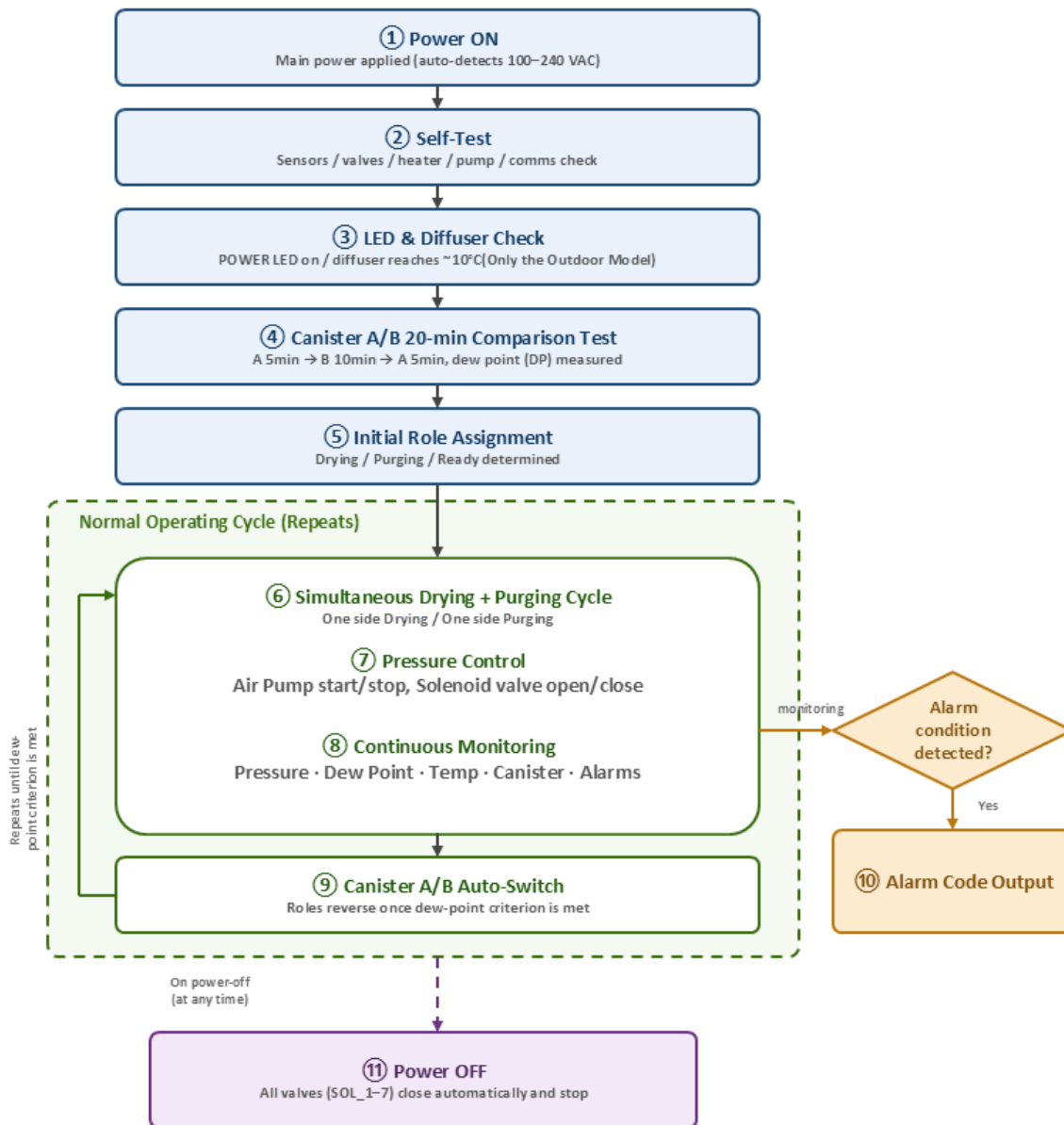
After power is restored, the controller may resume the previous canister operating states instead of completing the normal startup evaluation. This requires a valid saved operating record whose timestamp is within 10 minutes of the controller's boot time. The record must be processed while startup evaluation is still in progress. Time without power is not counted as active drying or purging time.

If the record shows that a canister was purging and that canister is at least 80°C when power returns, regeneration can resume immediately. On outdoor units, this can occur before the vapor block reaches its normal startup temperature; over-temperature protection remains active. If the saved record is missing, invalid, or too old, the unit follows the normal startup evaluation. Because the 10-minute limit is measured from the latest saved log entry—not the exact moment power was lost—restoration is not guaranteed solely because power is reapplied within 10 minutes.

3.8. Operating Sequence

ALD-200 Overall Operating Sequence

Theory of Operation



The overall operating sequence of the ALD-200 is illustrated in the operating flow diagram. The sequence consists of:

- Power On
- Startup Initialization
- Canister Performance Evaluation
- Normal Operating Cycle
 - Drying
 - Purging
 - Pressure Control
 - System Monitoring
 - Automatic Canister Switchover
- Alarm Indication (when applicable)
- Power Off

4. Components

The ALD-200 indoor (ALD-200i) and outdoor (ALD-200e) models share an identical internal component architecture. Both configurations utilize the same core components and control system to ensure consistent performance, reliability, and operational functionality regardless of the installation environment.

The primary components of the ALD-200 are described as follows.

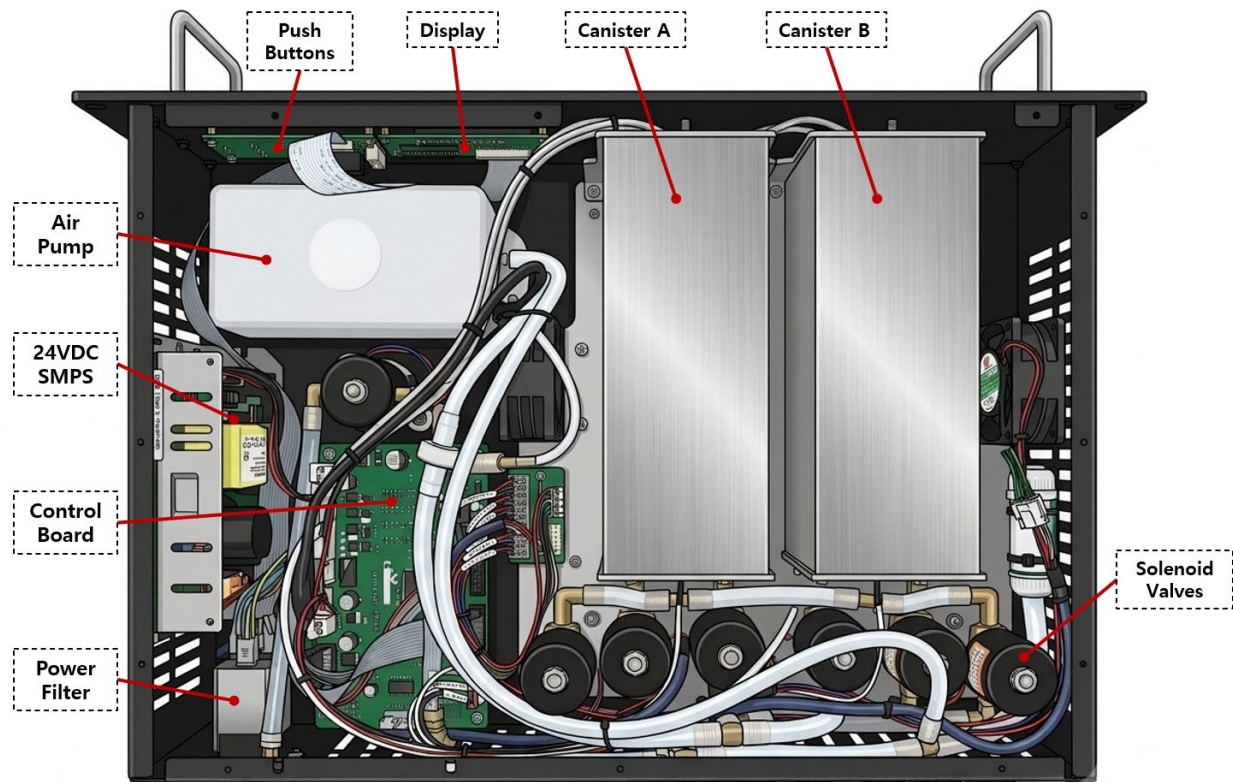


Figure 3. Components of ALD-200i (Indoor model)

- **Air Pump:**
This is an oilless diaphragm compressor that draws in ambient atmospheric air and pressures it. It generates the initial air flow that will be dried and sent to the transmission lines, operating under precise control to maintain the system's pressure limit of 0.3 psig.
- **Canister A & Canister B:**
These are the dual-bed adsorption units (desiccant towers) that serve as the core of the system's thermodynamic drying process. The dehydrator alternates between the two: while one canister is active (In-use) and adsorbing moisture to drop the air's dew point below -40°C , the other utilizes internal resistance heaters to vaporize trapped moisture and "regenerate" its drying capabilities for the next cycle.

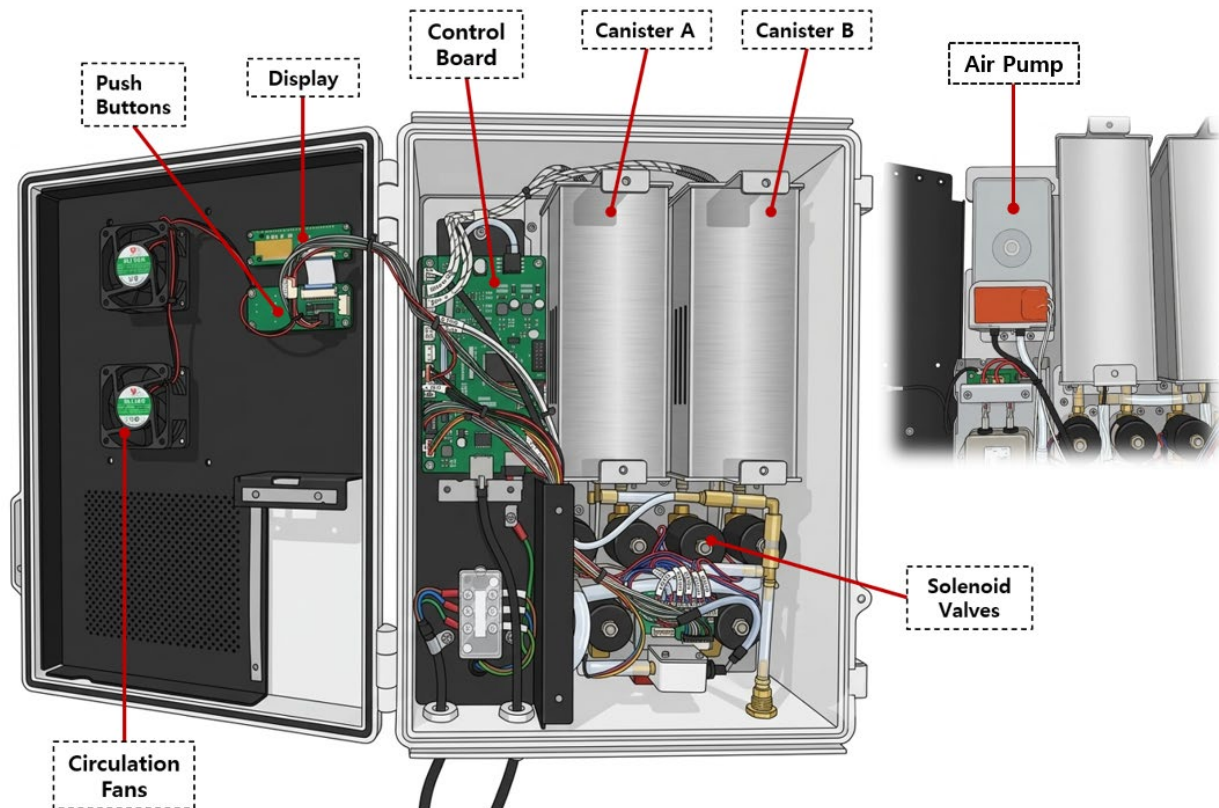


Figure 4. Components of ALD-200e (Outdoor model)

- **Solenoid Valve x7:**

Equipped with seven air flow control valves, the dehydrator dynamically configures optimal air flow paths, delivering reliable performance across a wider range of operating conditions than competing systems. These seven air flow control valves control air flow within the unit, directing moist air to the selected canister, delivering dry air to the output, and managing exhaust during regeneration.

- **Control Board:**

This printed circuit board is the central "brain" of the dehydrator. It processes data from onboard pressure, temperature, and humidity sensors, orchestrates the alternating canister cycles, and hosts the microprocessors responsible for the Ethernet-based Web UI and REST API remote monitoring systems.

- **24VDC SMPS (Switched-Mode Power Supply):**

This power module converts the incoming universal 100-240 VAC, 50/60 Hz line voltage into a stable 24 Volts DC. This regulated DC voltage is required to safely drive the electro-mechanical loads, specifically the air pump, the solenoid valves, and the internal canister heaters.

- **Power Filter:**

Positioned at the power entry point, this component suppresses electromagnetic interference (EMI) and electrical transients from the external power grid. It ensures that the sensitive digital components on the control board operate reliably without disruption from "dirty" power.

- Keypad & OLED:

Mounted to the front panel, this interface provides on-site technicians with direct access to the equipment. It displays real-time system parameters (such as operating status, air dew point, and active alarms) and allows for local diagnostic checks without requiring a network connection.

5. Drawing

5.1. Drawing of ALD-200i (Indoor model)

The indoor model, ALD-200i, is designed for seamless integration into standard 19-inch relay racks used in communication equipment rooms and data centers. The unit has a base width of 430 mm, a depth of 308 mm, and a height of 88 mm (approximately 2U rack space). When equipped with side extension brackets for rack mounting, the overall width conforms to the standard dimension of 482.6 mm.

The indoor unit weighs 9.4 kg (approximately 20.7 lbs), and it is recommended to install the equipment in the lower section of the rack in accordance with load distribution guidelines. In addition to securing the unit with front panel mounting screws, it is strongly recommended to use internal slide rails or support channels within the rack to ensure stable load support.

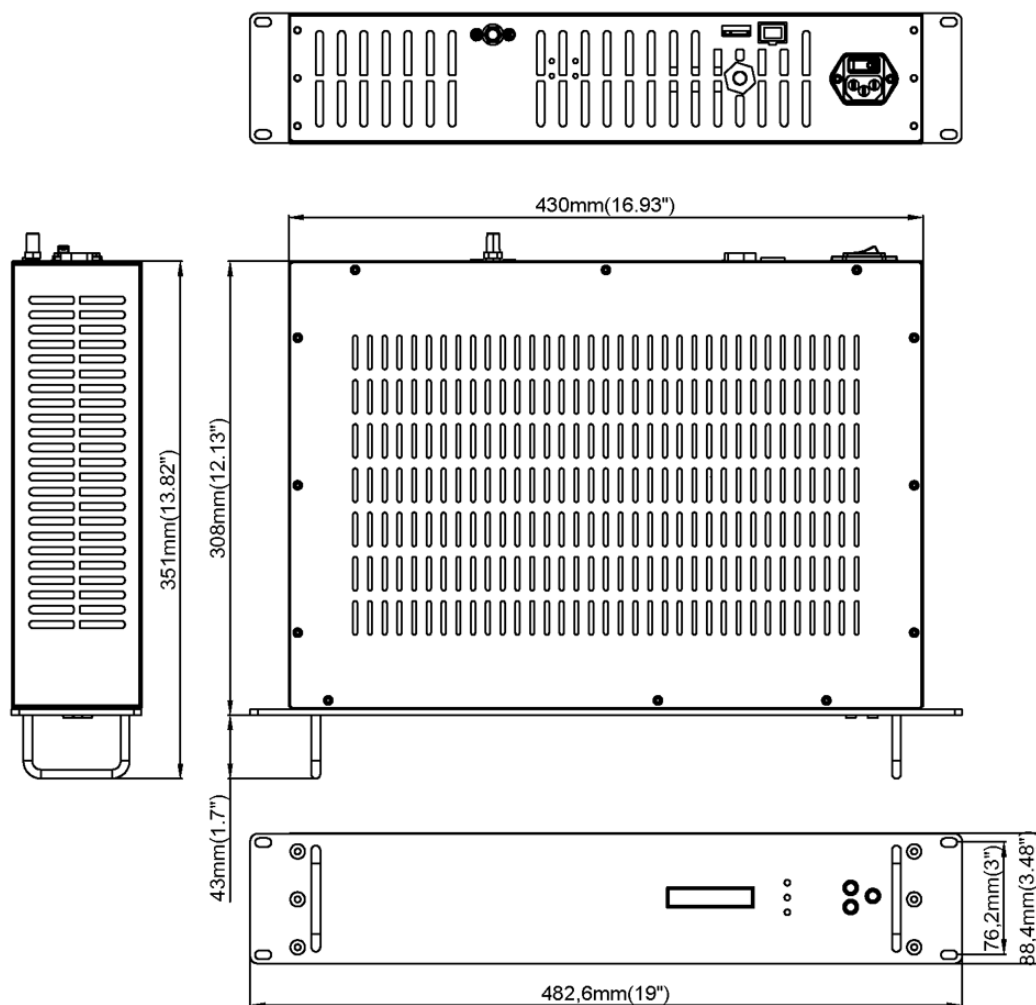


Figure 5. Drawing of ALD-200i (Indoor model)

5.2. Drawing of ALD-200e (Outdoor model)

The outdoor model, ALD-200e, is designed for installation in exposed environments such as the base of outdoor communication towers or the exterior walls of shelters in non-hazardous locations. It features a robust sealed enclosure structure capable of withstanding harsh environmental conditions. Compared to the indoor model, the outdoor unit has expanded dimensions to accommodate corrosion resistance and thermal insulation, measuring 324 mm in width, 408 mm in depth, and 150 mm in height, with a total weight of 10.4 kg (approximately 22.9 lbs).

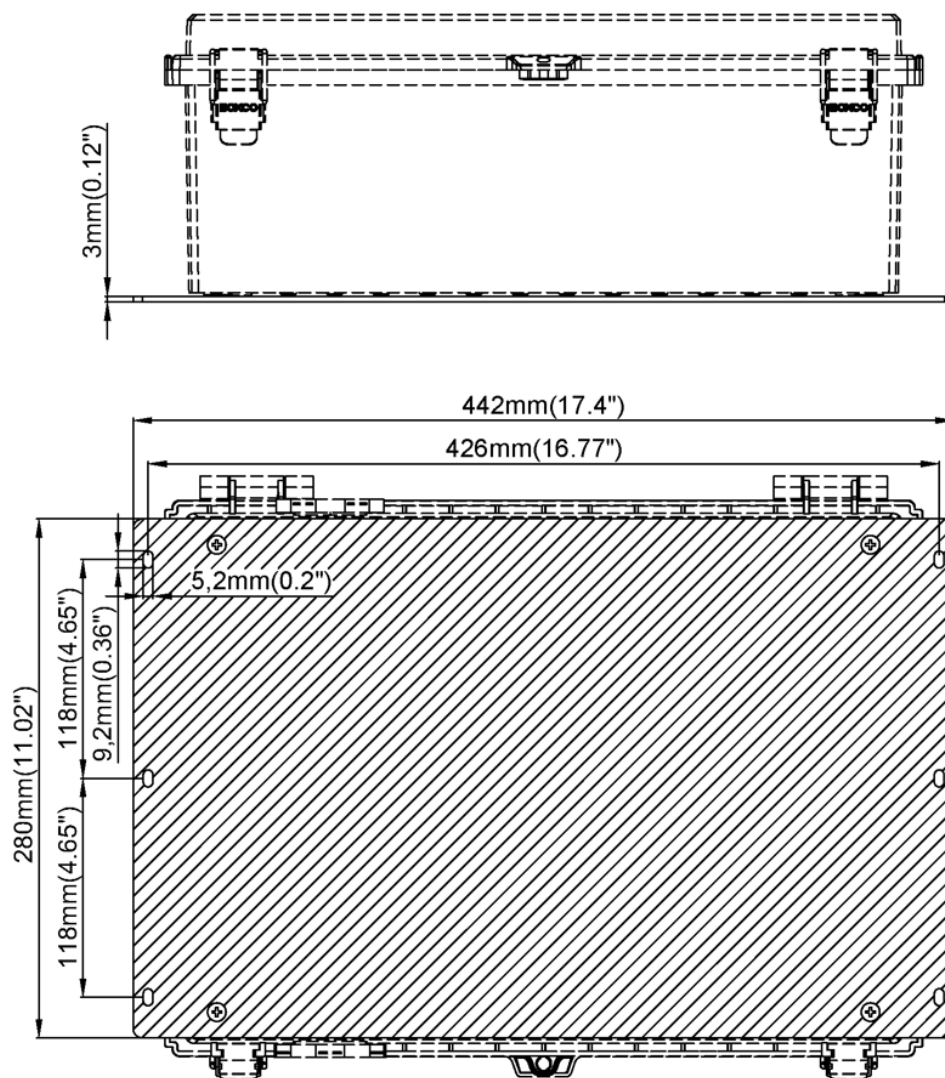


Figure 6. Drawing #1 of ALD-200e (Outdoor model)

The mounting bracket, attached to the rear or bottom of the outdoor unit, is engineered to withstand severe wind loads and mechanical vibrations. It provides a multi-anchor fastening

system with hole spacings of 426 mm and 118 mm, along with a total of six auxiliary mounting holes. Including the mounting bracket, the overall dimensions are 324 mm in width, 442 mm in depth, and 155 mm in height. This design provides the mechanical flexibility required for installation on both concrete walls and steel structures.

Since the fine vibrations generated by pump motors commonly found in communication equipment may lead to structural fatigue, it is essential to secure the unit firmly using anchor bolts capable of supporting a load of at least 30 kg (approximately 66 lbs).

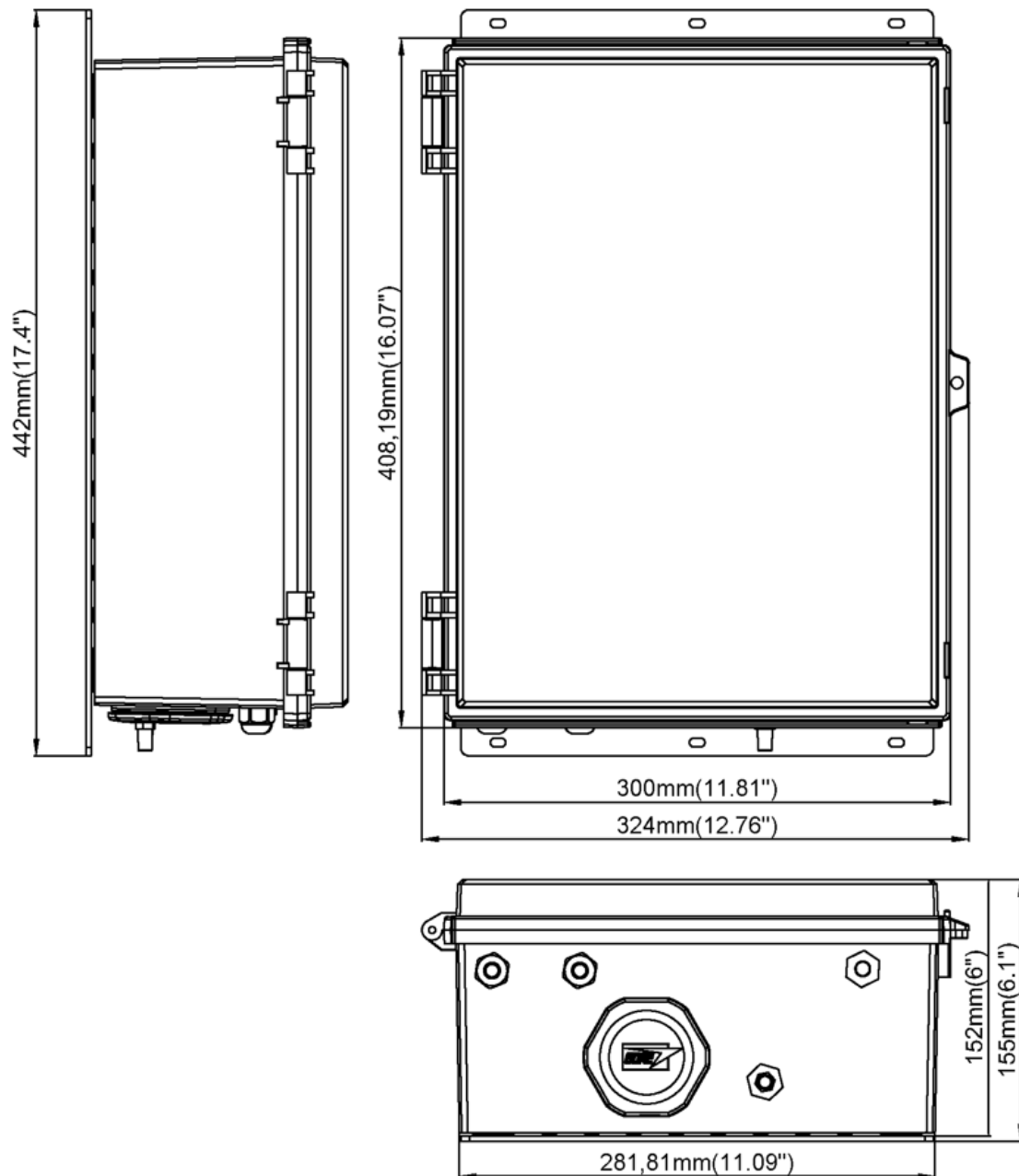


Figure 7. Drawing #2 of ALD-200e (Outdoor model)

II. ALD-200i (Indoor model)

1. Front Panel Configuration

The front panel of the ALD-200i is designed to provide real-time system monitoring and control. It consists of a display module, status LEDs, control buttons, and structural elements for rack mounting.



Figure 8. ALD-200i Front Panel

Mounting Holes

- Mounting holes are located on both sides of the front panel to enable installation in a standard 19-inch rack. The unit is designed with a compact size occupying approximately 2U rack space, allowing efficient use of limited rack capacity.

OLED Display

- The OLED screen provides real-time information on the overall system status. It allows operators to easily monitor key parameters such as current operating conditions, alarm status, and network information including the IP address.

Status LEDs

- The Status LEDs provide a quick and intuitive visual indication of the system condition, enabling easy monitoring even from a distance.
 - POWER (Green): Indicates that power is being supplied normally
 - OPERATING (Yellow): Indicates that the system is operating normally and maintaining the link
 - ALARM (Red): Indicates that a fault or alarm condition has occurred

Push Buttons

- Three push buttons are provided for menu navigation.
 - ENT (Enter) Button: Used to browse the alarm list and clear selected alarm.
 - UP / DN Buttons: Used to navigate menu screens and select menu items.

2. Back Panel Configuration

The back panel of the ALD-200i is designed to provide stable power input, network connectivity, data storage interfaces, and air flow connections required for system operation. It includes the AC power inlet, main power switch, Ethernet port, SD card slot, and air inlet/outlet ports, enabling stable power supply, remote monitoring, data logging, and controlled air circulation within the system.

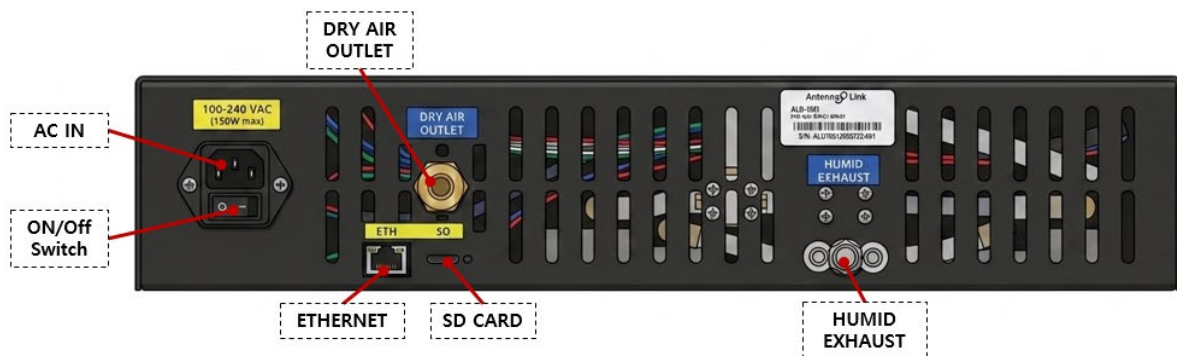


Figure 9. ALD-200i Back Panel

AC IN (Power Input)

- Supports a wide input voltage range of 100–240 VAC (free voltage).
- A standard AC power cable with an IEC C13 connector is used for the power input.

ON/OFF Switch (Main Power Switch)

- Located directly below the AC IN connector, this switch controls the main power supply for the entire system.

ETHERNET (LAN Port)

- Equipped with a 10/100 Mbps Ethernet (LAN) port for standard LAN cable connection, enabling remote device control and real-time status monitoring over a network.

SD CARD (SD Card Slot)

- Used for storing the system's operational history (log data) and for performing firmware updates.
- It allows users to monitor system status and perform detailed fault analysis and troubleshooting in case of abnormalities.

DRY AIR OUTLET

- A port for discharging dry air at a maximum pressure of 0.3 psig.
- It is designed with a default fitting compatible with Ø6 mm tubing, and can be replaced with other fitting specifications as required by the application.

HUMID EXHAUST (⚠ Hot Surface)

- This port exhausts humid air generated inside the unit.
- An internal heater is installed to prevent discharged moisture from condensing into droplets that could affect nearby equipment installed in the rack.
- ⚠ As the system evaporates moisture into vapor before discharge, the area around the exhaust port may become very hot during operation. Handle with care.

III. ALD-200e (Outdoor model)

1. Side Panel Configuration

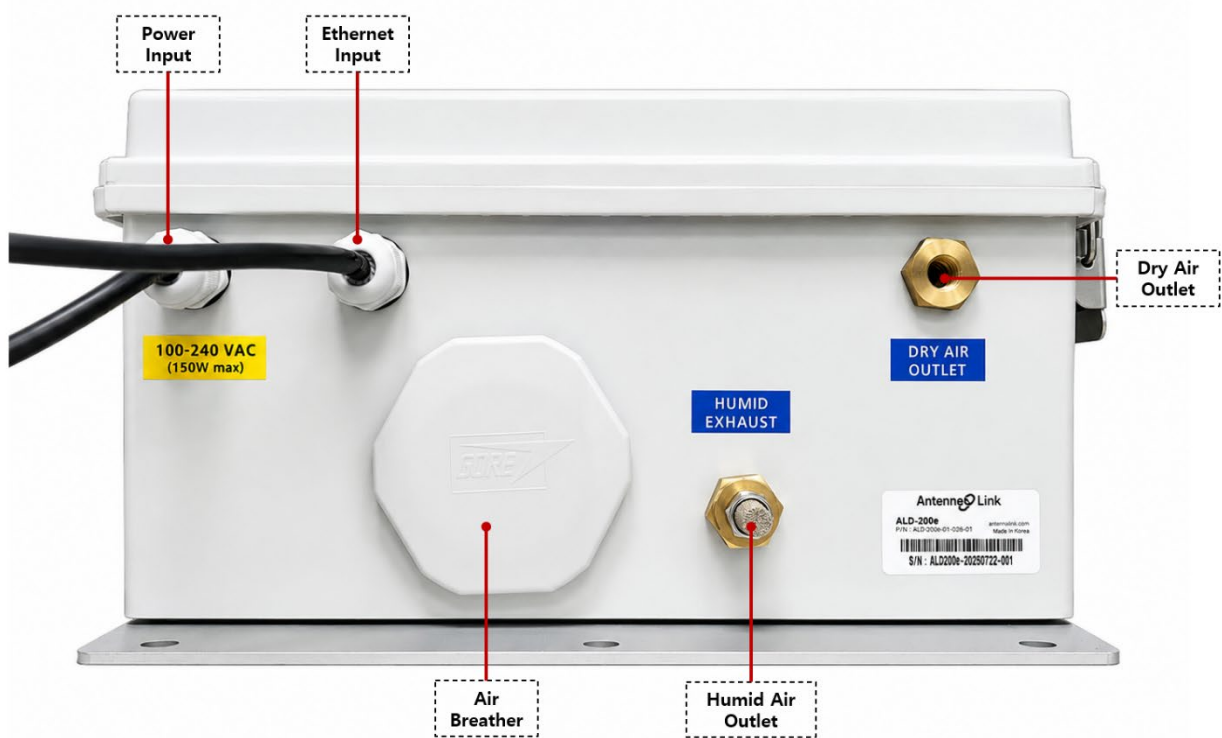


Figure 10. ALD-200e Side Panel

1.1. External Port Connection and Usage Guidelines

Two primary air circulation ports are located on the bottom (or side) of the unit, along with power and communication cable glands. To ensure proper operation and safe use of the equipment, please carefully review the characteristics and precautions for each port below.

1.1.1. DRY AIR OUTLET

Outlet Specification:

This port is compatible with NPT 1/8 inch nipple fittings. By using the supplied adapter, it can also accommodate NPT 1/4 inch nipple fittings.

Maximum Output Pressure:

The maximum output pressure of the dry air is 0.3 psig.

⚠ Caution:

Due to the low operating pressure, any bending, kinking, or compression of the connected tubing may restrict airflow, leading to reduced performance and possible internal pressure buildup.

Ensure that the tubing is routed smoothly with gentle curves in accordance with proper piping guidelines.

1.1.2. HUMID EXHAUST

Anti-Freeze Heater Equipped:

An internal anti-freeze heater is installed to prevent blockage caused by freezing of exhausted moisture under low ambient temperature conditions.

⚠ Caution (Hot Surface):

During operation, the exhaust port and surrounding area may experience elevated temperatures.

Use caution when handling components near the exhaust port.

Allow sufficient cooling time before maintenance.

Condensation Notice:

During operation at ambient temperatures, moisture generated during the internal purging process may condense into water droplets around the port and drip downward.

This is a normal phenomenon and not a product defect. If moisture management is required, appropriate drainage measures should be implemented beneath the unit.

2. Inner Panel Configuration

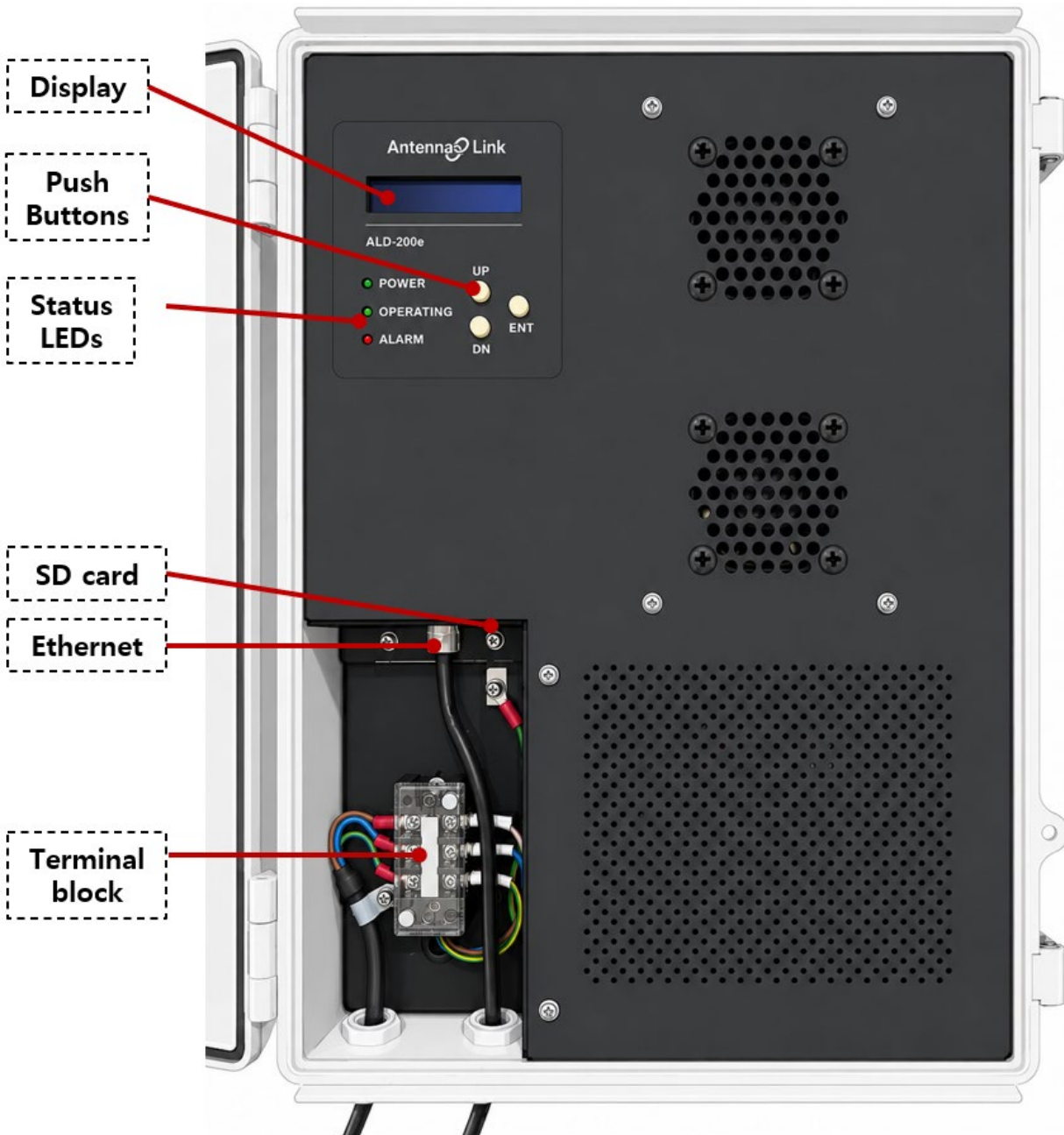


Figure 11. ALD-200e Inner Panel

OLED Display

- The OLED screen provides real-time information on the overall system status. It allows operators to easily monitor key parameters such as current operating conditions, alarm status, and network information including the IP address.

Status LEDs

- The Status LEDs provide a quick and intuitive visual indication of the system condition, enabling easy monitoring even from a distance.
 - POWER (Green): Indicates that power is being supplied normally
 - OPERATING (Yellow): Indicates that the system is operating normally and maintaining the link
 - ALARM (Red): Indicates that a fault or alarm condition has occurred

Push Buttons

- Three push buttons are provided for menu navigation.
 - ENT (Enter) Button: Used to browse the alarm list and clear selected alarm.
 - UP / DN Buttons: Used to navigate menu screens and select menu items.

SD CARD (SD Card Slot)

- Used for storing the system's operational history (log data) and for performing firmware updates.
- It allows users to monitor system status and perform detailed fault analysis and troubleshooting in case of abnormalities.

ETHERNET (LAN Port)

- Equipped with a 10/100 Mbps Ethernet (LAN) port for standard LAN cable connection, enabling remote device control and real-time status monitoring over a network.

Terminal Block

- The Terminal Block provides the main AC power input interface for the system. It is designed for secure connection of power cables to ensure stable operation.

2.1. Power Connection and Wiring Instructions

This equipment features a free-voltage design supporting a wide input voltage range, along with a terminal block structure for safe and stable power supply. Please follow the instructions below to ensure proper and safe installation.

2.1.1. Power Specifications

- Input Voltage Range: 100-240 VAC, 50/60 Hz (Power consumption: 20 W typical to 150 W maximum)

- Automatic Voltage Selection:
- The unit is equipped with an automatic voltage detection circuit, allowing operation within the 100–240 VAC range without the need for manual voltage selection.

2.1.2. Terminal Block Wiring (Left Terminal Block)

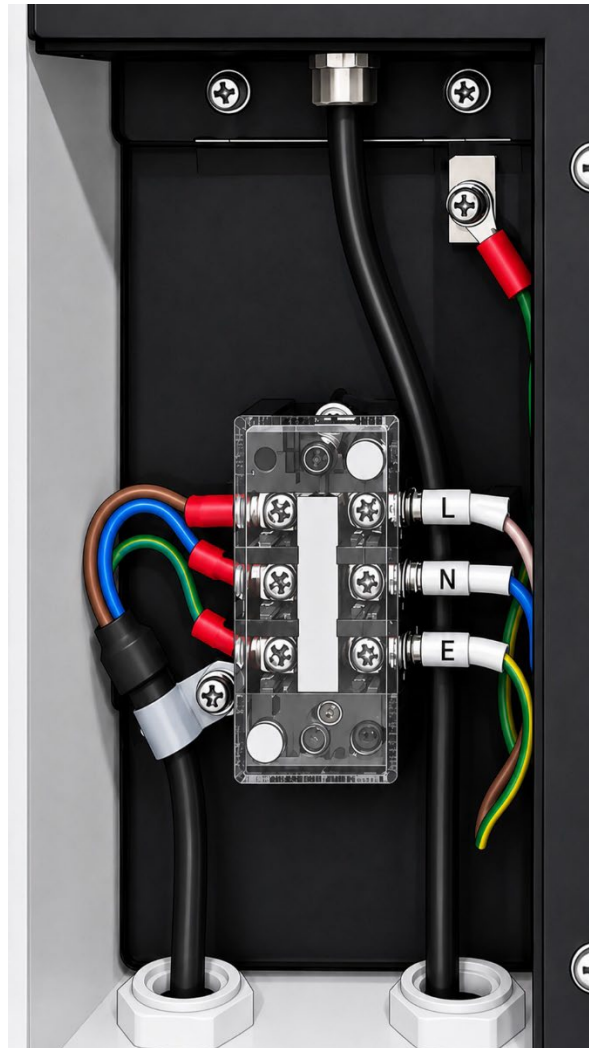


Figure 12. ALD-200e Terminal Block Wiring

Refer to the cable colors connected to the left-side terminal block in the image, and connect them in the following order from top to bottom:

- L (Line): Connect the brown cable to the first (top) terminal
- N (Neutral): Connect the blue cable to the second (middle) terminal

- GND (Ground): Connect the green/yellow cable to the third (bottom) terminal

 Important Safety Precautions

 Warning: Risk of Electric Shock and Fire

All wiring work must be performed with the main power completely turned OFF (circuit breaker switched off).

- **Proper Grounding (GND):**

Ground connection is essential to prevent electric shock due to leakage current and to reduce electromagnetic interference (EMI). Failure to properly connect grounding may result in equipment malfunction.

- **Terminal Screw Tightening:**

Loose connections due to vibration may cause overheating or fire. Ensure that all terminal screws are securely fastened so that crimped terminals are firmly fixed.

- **Cable Securing (Use of Clamp):**

To prevent cables from being pulled loose from the terminal block, ensure that cables are properly secured using the internal cable clamp (white fixture) and the bottom rubber gasket (gland nut), as shown in the image.

 Important Safety Precautions

 Warning: Risk of Electric Shock and Fire

All wiring work must be performed with the main power completely turned OFF (circuit breaker switched off).

 Important Precautions for Internal Interfaces (Ethernet / SD Card)

When installing the Ethernet cable and SD card on the internal main board, pay special attention to their insertion orientation:

IV. Indicator and Control

The ALD-200i (Indoor model) and ALD-200e (Outdoor model) models are designed with a user-friendly front panel interface that provides clear visibility into system status and enables straightforward control of key functions. Both models offer identical functionality, ensuring consistent operation regardless of installation environment.

The front panel is equipped with a set of LED indicators and control buttons that allow operators to easily monitor system conditions and respond to any operational events. The LED indicators—POWER, OPERATING, and ALARM—provide immediate visual feedback on the unit's power status, operational activity, and alarm conditions. These indicators enable quick diagnostics and help ensure reliable system performance.

In addition to the status indicators, the built-in OLED display presents detailed real-time information, including canister operation status, dew point, humidity, temperature, and pressure of the dry air. The interface also allows users to review active alarms, monitor purging conditions, and check system parameters such as IP address and software version.

Control of the system is simplified through three intuitive buttons (ENT, DN, and UP), which allow users to navigate menus, review alarm lists, and clear alarm entries efficiently. This design ensures that operators can manage the system with minimal training while maintaining full access to essential monitoring and control functions.

Overall, the front panel of the ALD-200i and ALD-200e provides a comprehensive and efficient interface for real-time monitoring, diagnostics, and control, contributing to stable and reliable operation of the dehydrator system.

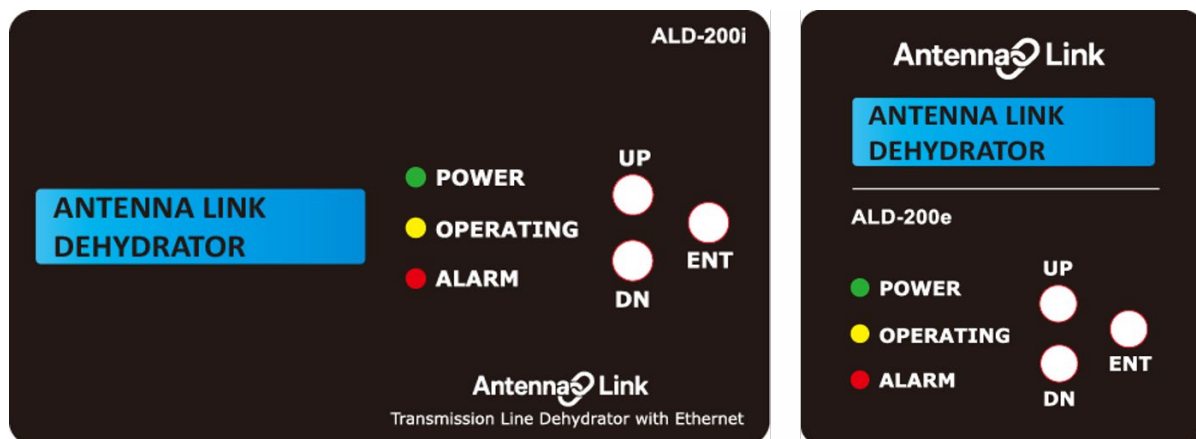


Figure 13. Indicators and Controls of ALD-200i (Left), ALD-200e(Right)

LED

- POWER LED
Indicates that the unit is powered ON.
- OPERATING LED

Indicates that the unit is in operation.

- For outdoor-type units (ALD-200e), the LED remains OFF after startup until the internal temperature reaches 10°C.
- Once the temperature reaches 10°C and the pump starts operating, the LED turns ON.
- The LED turns OFF if the unit stops due to a critical fault condition.
- **ALARM LED**
Indicates that one or more alarms are active.
 - The LED turns OFF when all alarms have been cleared.

Control Buttons

- **UP / DN Button**
Advances to the next OLED status menu page.
On the IP Address configuration screen, use the ENT button to move the cursor to the desired position, then use the UP and DN buttons to change the selected value.
- **ENT Button**
Deletes a selected alarm entry.
 - In the Alarm menu, use the ENT Button to select an alarm.
 - Press and hold the ENT button for 3 seconds to display the "DELETE?" confirmation message. Press the ENT button once more to confirm and clear the selected alarm.
 - On the IP Address configuration screen, press the ENT button to move the cursor to the value you want to change.

OLED Display

- **Startup Screen 1**



ALD-200i Rev2.21
S/N 20260716-001

- Displayed for 2.5 seconds after power is applied.
- Displays the product model, hardware revision number, and serial number.

- **Startup Screen 2**



B/L VER 1.0.3
S/W VER 1.0.12

- Displayed for 2.5 seconds after power is applied.

- Displays the bootloader version and software version.
- Main Screen

CAN B COOLING
DP:-58.1 3:28:10

- Displays the current operating status and the measured dew point.

- Dry Air Data Screen

T:40.96 RH:0.030
DP:-58.30 F:2.11

- Displays the temperature, humidity, and flow rate of the dry air.

- Temperature Sensor Screen

ExhTemp 55.87
A 48.12 B 129.4

- Displays the temperatures of the Exhaust Air Block and both canisters.

- IP Address Screen

IP DHCP ENT=SET
192.168.10.73

- Displays the current IP address.

- Entering the IP Address Configuration Menu

NET MODE
■HCP ENT=NEXT

- Press the ENT button to enter the IP address configuration menu.

- Selecting the Network Mode

NET MODE
STATIC ENT=NEXT

- Each press of the ENT button toggles between DHCP and STATIC mode.

- Configuring a Static IP Address



192.168.010.050
IP D01=1 ENT

- When STATIC mode is selected, press ENT to enter the IP address configuration mode.
- Use the UP and DN buttons to change the value of each digit, and press ENT to move to the next digit.
- To cancel the configuration at any time, press and hold the ENT button.

- Completing the IP Address



192.168.010.05
IP D12=9 ENT

- After entering the final digit of the IP address, press ENT to continue.

- Configuring the Subnet Prefix



SUBNET PREFIX
/ 4 UP/DN ENT

- Set the subnet prefix using CIDR notation.
- For example, a prefix length of 24 corresponds to a subnet mask of 255.255.255.0.
- Use the UP and DN buttons to adjust the value, then press ENT to proceed.

- Configuring the Gateway Address



192.168.010.00
GW D12=1 ENT

- Enter the gateway address.
- Only the host portion of the address can be configured. For example, when using a 24-bit subnet, only the last octet can be edited.
- Press ENT after completing the configuration.

- Saving the Network Settings



SAVE NETWORK?
ENT=SAVE LONG=X

- Press the ENT button to save the settings.

- To cancel the configuration, press and hold the ENT button for 3 seconds, as in the previous steps.

- Applying the New IP Address



NETWORK SAVED
Applying...

- Press ENT to save the configuration.
- The new IP address is applied immediately.

- Static IP Address Screen



IP STATIC ENT=SE
192.168.10.59

- Displays the configured Static IP address.

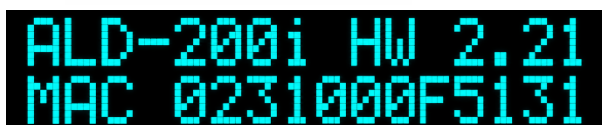
- Software Information Screen



SW VER: 1.0.12
BUILD:2026-07-16

- Displays the software version and firmware build date.

- Device Information Screen



ALD-200i HW 2.21
MAC 0231000F5131

- Displays the product model, hardware revision number, and MAC address.

- Alarm Display



106
PRESS LO WARN →

- When an alarm occurs, the alarm number and alarm name are displayed.
- If multiple alarms are active, press the ENT button to view the next alarm.

- Viewing the Next Alarm



- Press the ENT button to scroll through additional active alarms.

● Clearing an Alarm



- Press and hold the ENT button for 3 seconds.
- A confirmation message is displayed. Press ENT again to clear the selected alarm.

Alarm List

Alarm No.	Name	Description
101	Fault Humidity	Occurs when the humidity remains above the specified limit for six hours or longer. Dehydrator operation is stopped. The alarm threshold can be configured on the web page as either a dew point or relative humidity value.
102	Humidity High (warning)	Occurs when the humidity exceeds the specified warning threshold. The threshold can be configured as either a dew point or relative humidity value via the web page or REST API.
103	Humidity High (critical)	Occurs when the humidity exceeds the specified critical threshold. The threshold can be configured as either a dew point or relative humidity value via the web page or REST API.
104	Pressure High (warning)	Occurs when the pressure exceeds the specified warning threshold. The threshold can be configured via the web page or REST API.
105	Pressure High (critical)	Occurs when the pressure exceeds the specified critical threshold. The threshold can be configured via the web page or REST API.
106	Pressure low (warning)	Occurs when the pressure falls below the specified warning threshold. This alarm can be used to detect a minor leak. The threshold can be configured via the web page or REST API.
107	Pressure low (critical)	Occurs when the pressure falls below the specified critical threshold. This alarm can be used to detect a leak. The threshold can be configured via the web page or REST API.
201	Dry-air high temperature	Occurs when the dry-air temperature exceeds the specified limit. The threshold can be configured on the web page.
202	Regeneration canister low temperature	Occurs when the specified temperature is not reached by the end of the heating phase during regeneration. The threshold can be configured on the web page.
203	Canister A heater failure	Occurs during regeneration of Canister A when the temperature rise during the specified initial period is less than the specified value. The time and temperature-rise thresholds can be configured on the web page.
204	Canister B heater failure	Occurs during regeneration of Canister B when the temperature rise during the specified initial period is less than the specified value. The time and temperature-

		rise thresholds can be configured on the web page.
205	Canister A heater over-temperature	Occurs when the temperature of Canister A exceeds the specified limit. The threshold can be configured on the web page.
206	Canister B heater over-temperature	Occurs when the temperature of Canister B exceeds the specified limit. The threshold can be configured on the web page.
207	Exhaust block heater over-temperature	Occurs when the exhaust block temperature exceeds the specified limit. The threshold can be configured on the web page.
208	Pump failure	Occurs when the specified pressure is not reached within the specified time. The criteria can be configured on the web page.
301	Canister A temperature sensor failure	Occurs when the temperature reading cannot be obtained from the Canister A temperature sensor.
302	Canister B temperature sensor failure	Occurs when the temperature reading cannot be obtained from the Canister B temperature sensor.
303	Exhaust block temperature sensor failure	Occurs when the temperature reading cannot be obtained from the exhaust block temperature sensor.
304	Humidity/temperature sensor failure	Occurs when readings cannot be obtained from the dry-air outlet humidity/temperature sensor.
305	Pressure sensor failure	Occurs when a reading cannot be obtained from the pressure sensor.
306	MCU process failure	Occurs when the MCU sensing process does not operate normally.
307	SD card missing	Occurs when the system detects that no SD card is inserted.
308	SD card I/O failure	Occurs when an error is encountered while reading data from or writing data to files on the SD card.

V. WEB Interface

1. Web access and accounts

Connect a computer to a network that can reach the unit. Read the unit's current address from its local display and open `https://DEVICE_ADDRESS/`. DHCP is the default network mode; do not assume that every unit has the same address.

1.1. First access and certificate trust

A unit without an installed CA-issued certificate uses a self-signed HTTPS certificate. The browser can encrypt the connection but cannot establish device identity from its normal trust store. Confirm the device address and certificate with the administrator before accepting a commissioning exception.

HTTP on port 80 now shows an information page with an Open HTTPS link. It does not automatically redirect or process login, monitoring or settings API requests. Select the link to continue on HTTPS port 443. With the default certificate, the page explains the warnings below; when a CA-issued certificate is active, it gives certificate-check guidance instead.

Browser	Typical warning and commissioning action
Chrome and Edge	Your connection is not private, often <code>NET::ERR_CERT_AUTHORITY_INVALID</code> . After device verification, open Advanced and use the proceed option only if offered.
Firefox	Warning: Potential Security Risk Ahead. After device verification, use Advanced, then Accept the Risk and Continue if offered.
Safari	A privacy or certificate warning. Review Show Details and the certificate; use Visit Website only if offered after device verification.

Labels depend on browser version and language. If no exception is offered, ask the administrator to install a trusted certificate. Do not disable browser-wide security checks. A temporary exception can need renewal after a restart or certificate change. For lasting trust, generate a CSR in Settings > HTTPS Certificate, install the issued leaf and intermediate chain, and use an address covered by its subject alternative names. The browser or operating system must trust the issuing CA. An unexpected change on an established installation requires investigation.

Log in at the login page. The fixed local user IDs are viewer, operator and admin. Each has an independent password. Local user IDs cannot be renamed, and additional local accounts cannot be created.

Account	Typical access
viewer	View status, alarms, logs and hardware readings
operator	Viewer access plus operational settings, alarm clearing, Standby and manual controls
admin	Operator access plus network, accounts, clock, security, firmware, reset and pump runtime reset

Use viewer for routine monitoring. Use operator or admin only when the task requires changes. Log out after use, especially on a shared computer. Local sessions expire after eight hours without activity; the device supports up to four concurrent browser sessions.

1.2. Initial administrator setup

After a factory reset, enter and confirm a new administrator password on the setup page, then sign in as admin. There is no universal administrator password after this reset. The viewer and operator accounts remain disabled until the administrator assigns passwords to them.

In Settings, select the local account and enter the new password twice. Passwords must contain 4 to 31 characters; use a strong, unique password within that limit. Changing a password invalidates that account's browser sessions. Changing the administrator password therefore requires a new login.

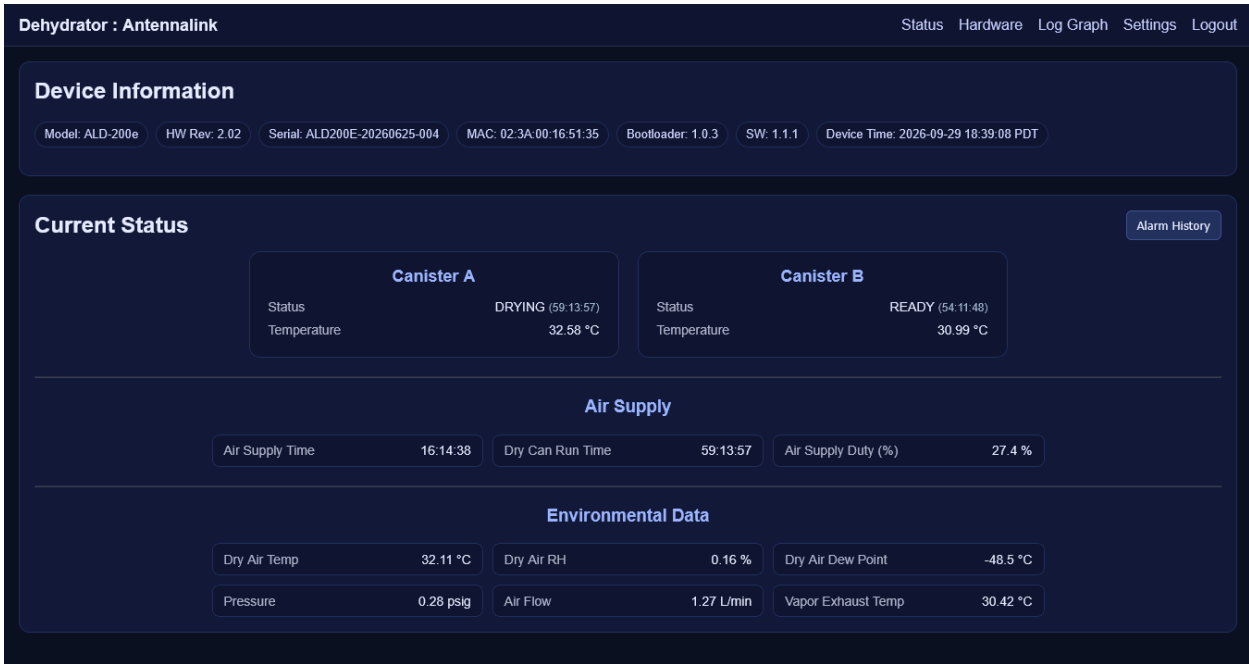
2. Monitoring with the web interface

The navigation contains Status, Hardware, Log Graph and, for administrators, Settings. Functions can be hidden when the signed-in account does not have permission or when the firmware omits an option.

2.1. Status

Use Status to check device identification, canisters A and B, air supply readings, environmental data, Active Alarms and Alarm History. Compare both the operating state and sensor values. An

operating state alone does not certify that the delivered air meets the connected system's requirements.



Alarm History helps distinguish a recurring condition from a single event. Note the timestamp, code, severity, event and available measurement context. Check the device clock when a timestamp appears incorrect. History availability depends on storage condition; missing history is not proof that no alarm occurred.

Dehydrator : Antennalink
Status Hardware Log Graph Settings Logout

Device Information
Model

Alarm History

Total 6 event(s) - Device time zone: America/Los_Angeles

Time	Code	Alarm	Severity	Event	Details	Source	Duration
2026-09-03 00:32:19 PDT	208	Pump failure	ERROR	CLEARED	Cleared by web user - Value 0.043 psig / Threshold 0.05 psig	WEB	02:53:01
2026-09-02 21:57:21 PDT	106	Low pressure warning	WARN	CLEARED	Pressure recovered above warning low limit - Value 0.115 psig / Threshold 0.1 psig	AUTO	00:00:00
2026-09-02 21:57:21 PDT	106	Low pressure warning	WARN	RAISED	Pressure fell below warning low limit - Value 0.003 psig / Threshold 0.1 psig	AUTO	-
2026-09-02 21:57:21 PDT	107	Low pressure critical	ERROR	CLEARED	Pressure recovered above critical low limit - Value 0.003 psig / Threshold 0 psig	AUTO	00:21:36
2026-09-02 21:39:18 PDT	208	Pump failure	ERROR	RAISED	Pump failed to reach target pressure within configured time - Value -0.04 psig / Threshold 0.05 psig	AUTO	-
2026-09-02 21:35:45 PDT	107	Low pressure critical	ERROR	RAISED	Pressure fell below critical low limit - Value -0.044 psig / Threshold 0 psig	AUTO	-

Environmental Data

Dry Air Temp32 °C

Dry Air RH0.18 %

Dry Air Dew Point-47.31 °C

Pressure0.26 psig

Air Flow0 L/min

Vapor Exhaust Temp30.42 °C

2.2. Hardware

Dehydrator - Antennalink

StatusHardwareLog GraphSettingsLogout

Hardware Status

Refresh period: 3 secondsUpdated 6:41:50 PM

Air Pump

Average Pump PWM Duty during refresh period: 0 %

Valves

Inlet A

ON

Inlet B

OFF

Purge A

OFF

Purge B

OFF

Dried A

ON

Dried B

OFF

Outlet

OFF

Fan / Heaters / SD Card

Fan

OFF

Canister A heater

OFF

Canister B heater

OFF

Pump heater

OFF

SD Card inserted

ON

Manual Canister Control

A Dry

B Dry

A Purge

B Purge

Standby On

Standby Off

Dry immediately selects that canister for drying and puts the other canister in READY. Purge starts the selected canister regeneration sequence. Standby closes valve #1 and preserves the canest dry as long until Standby Off.

Output Test (maximum 1 minute)

Output	Test control	Auto release
Valve 1 Inlet A	OpenCloseRelease	Automatic
Valve 2 Inlet B	OpenCloseRelease	Automatic
Valve 3 Purge A	OpenCloseRelease	Automatic
Valve 4 Purge B	OpenCloseRelease	Automatic
Valve 5 Dried A	OpenCloseRelease	Automatic
Valve 6 Dried B	OpenCloseRelease	Automatic
Valve 7 Outlet	OpenCloseRelease	Automatic
Fan	OnOffRelease	Automatic
Canister A heater	OnOffRelease	Automatic
Canister B heater	OnOffRelease	Automatic
Pump heater	OnOffRelease	Automatic
Air Pump	Off30%80%100%Release	Automatic

A test command takes priority over automatic control. At Pump 30% / 80% / 100% bypasses normal pressure-based pump duty control, but the configured Emergency pressure protection still opens all valves and stops the pump. Release returns the output to automatic control immediately.

Pump Maintenance

Accumulated pump runtime: 194.2 h

Last runtime reset (UTC): Never reset

Runtime before last reset: --

Runtime and the latest reset record are preserved during factory reset

Reset pump runtime after replacement

Sensor Refresh Control

Set the minimum Pump Operation Duty over the recent 10 minutes to keep the humidity sensor refreshed while maintaining pump usage.

Minimum Pump Operation Duty (for Sensor Refresh)

-

20%

+

Range: 10% - 100% Default: 20%

When valve #7 is closed and the recent Pump Operation Duty is below this target, the pump uses internal circulation at PWM duty 0.3. A 100% setting keeps internal circulation running whenever valve #7 is pressure closed.

Save Settings

Alarm Settings

Humidity

Setting	Value	Enable
Switching humidity	-10 °C DP	☐
Fail humidity	18 °C DP	☒ E101
High hum (warning)	20 °C DP	☒ F102
High hum (critical)	25 °C DP	☒ E103

Pressure

Setting	Value	Enable
High pressure (warning)	0.2200 pmp	☒ F104
High pressure (critical)	0.4800 pmp	☒ E105
High pressure decision time	3s	☐
Low pressure (warning)	0.1800 pmp	☒ E106
Low pressure (critical)	0.0600 pmp	☒ E107
Low pressure decision time	30s	☐
Emergency pressure	1.0000 pmp	☐

Temperature / Heater

Setting	Value	Enable
Dryer high temperature	100 °C	☒ F201
Regeneration canister low temperature	20 °C	☒ F202
Canister heater failure	300 sec	☒ F203 F204
Required heater temperature rise	5 °C	☐
Canister heater over-temperature	300 °C	☒ E205 E206
Purged fresh heater over-temperature	170 °C	☒ E207

Pump / Operation

Setting	Value	Enable
Pump failure pressure	0.0700 pmp	☒ F308
Pump failure decision time	50 min	☐
Failure mode	Pressure priority	

Units

Setting	Value
Temperature unit	°C
Pressure unit	pmp

Sensor / System alarms

☒ Canister A temperature sensor failure F301

☒ Canister B temperature sensor failure F302

☒ F filtered block temperature sensor failure F303

☒ Humidity/temperature sensor failure F304

☒ Pressure sensor failure F305

☒ MCU processor failure F306

☒ SD card missing F307

☒ SD card I/O failure F308

Save hardware settings

43

ALD-200 User Manual
Antenna Link - 990 Blue Mound E, Haslet, Texas 76052, USA

Hardware shows pump drive duty, valve states, fan and heater states, storage-card presence and pump maintenance information. Refresh selections are 1, 3 or 10 seconds; the normal selection is 3 seconds. Longer refresh periods reduce network and controller traffic.

ALD-200i labels its auxiliary heater as Vapor block heater. ALD-200e labels it as Pump heater. Some display and alarm labels use generic exhaust or block terminology; identify the model before arranging service.

2.2.1. Pump replacement record

Hardware > Pump Maintenance shows accumulated pump runtime, the most recent runtime reset time in UTC and runtime before that reset. Physical pump runtime includes internal circulation and test operation; it differs from air supply time.

After an authorized pump replacement, an administrator can select Reset pump runtime after replacement and confirm the action. Record the old reading, replacement date and part details first. Only the most recent reset record is retained on the device. If the device clock was unset, the reset date can appear as Time was not set.

Factory reset preserves pump runtime and the latest reset record, as well as canister lifetime information. Sudden power loss can lose the most recent uncheckpointed runtime; use the record for maintenance tracking rather than precision billing.

2.3. Log Graph

Log Graph displays a three-day trend view with temperature, dew point and, when enabled, pressure and dry-air flow. It also marks Standby periods. Use trends to investigate gradual changes, excessive cycling or the timing of alarms. A blank or incomplete graph can indicate unavailable storage, insufficient history or a communication problem.

For an exported CSV log, use the download procedure in the separate REST API Reference, or obtain the file through the site integration or service tool. Save it with the unit identity and download date. Availability depends on the storage card and retained log files. File age is not equivalent to a fixed number of calendar days.

3 Day Log Graph

points: 1440 / interval: 3 min / range: 3 days / auto refresh: 1 min



3. Operating settings and manual controls

Changes on Hardware require operator or admin access. Record the existing values before changing a setting. Select the intended units, enter the approved values, save and reload the page to verify the stored result. Display limits are input limits, not a statement of safe operating ratings.

3.1. Alarm settings and failure mode

The web Hardware page exposes the configurable alarm thresholds and decision times in Hardware > Alarm Settings. With operator or admin access, you can change nearly all threshold values used for humidity, high/low pressure, dry-air and regeneration temperatures, heater protection, and pump-failure detection; pressure alarm decision times are configurable there as well. The page also provides enable controls for supported alarm items. Use the displayed units and allowed ranges, save, then reload the page to verify the stored values. Some alarms are enable-only or derived, and paired A/B protection enables may be normalized together. These software input ranges are not equipment ratings. Keep protections enabled unless an approved service procedure requires a temporary change.

Zero pressure failure mode stops air delivery for the failure conditions governed by that mode. Maintain pressure with humid air permits continued supply under those conditions even when humidity control is degraded. Neither mode overrides every protective shutdown. Do not use the name Zero pressure as evidence that all downstream tubing has been depressurized.

3.2. Standby

Select Hardware > Manual Canister Control > Standby On to suspend normal external delivery. Standby closes the external shutdown valve and pauses the current dry-run timer. The setting is retained across reboot. Select Standby Off to resume normal operation and verify pressure and dryness afterward.

**WARNING: Standby does not isolate electricity, release all trapped pressure or guarantee that every heater and internal process has stopped. Use physical isolation for service.*

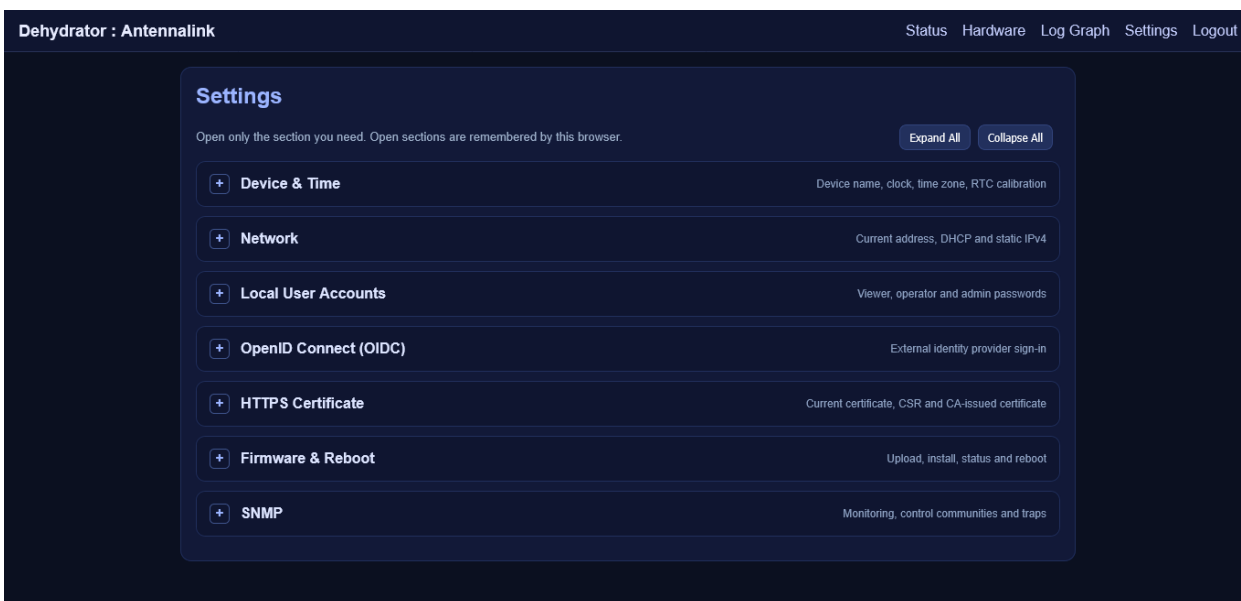
3.3. Manual canister selection and output tests

A Dry or B Dry immediately selects that canister for drying and puts the other canister in READY. A Purge or B Purge starts the selected canister's regeneration sequence. Use these controls only as part of an authorized service procedure.

Output Test can temporarily override valves, fan, heaters and pump. Tests last no more than one minute; Release returns the selected output to automatic control immediately. Pump test levels bypass normal pressure-based duty control, although configured emergency-pressure protection remains active. Observe the unit throughout the test.

Sensor Refresh Control sets minimum pump operation over the recent ten minutes. Its range is 10 to 100 percent, with a default of 20 percent. Internal circulation may run when external delivery is closed. Leave this setting at the approved site value.

4. Network, time and security settings



Settings uses collapsible groups: Device & Time, Network, Local User Accounts, OpenID Connect (OIDC), HTTPS Certificate, Firmware & Reboot, and SNMP when included. Select a group title to open it, or use Expand All and Collapse All. The browser remembers open groups; expanding or collapsing a group does not save its settings. Use the Save or action control inside the relevant group.

4.1. Network configuration

Administrators can select DHCP or enter a static IP address, subnet mask and gateway in Settings. Obtain the values from the network administrator. Record the new address before saving. Applying the change can end the current connection; reconnect using the new address and verify it against the local display.

If the unit cannot be reached, inspect the Ethernet connection and local IP page first. Use local network editing to correct addressing. Do not factory-reset the unit simply to discover its address.

4.2. Device clock

Select the installation's time-zone region and set or synchronize the device clock using the available Settings controls. The RTC stores UTC in 24-hour format; the local time is derived from the selected region and its supported daylight-saving rules. Check both the displayed local time and UTC time. Recheck the clock after an interruption or when records show an unexpected time.

A correct clock is needed for useful alarm records and identity-provider login. The controller validates RTC fields and reads the time/date pair coherently; if the clock is invalid or cannot be read, the time status is not valid. Do not treat an unset or invalid clock as a valid event timestamp. Time-zone configuration is separate from network addressing.

4.3. RTC fine calibration

In Settings > Device & Time, use Sync with PC / Phone to set the clock from an accurate reference computer or phone and establish a drift reference. An explicit clock set invalidates any previous drift reference; the sync operation establishes a new request/response midpoint reference after the clock write succeeds. This is separate from selecting the time zone.

For automatic fine adjustment, leave the clock running for at least 24 hours without setting it again, then select Measure & Auto Adjust. A measurement period of seven days or more is recommended by the interface. Use a reference computer with a reliable clock. The page takes five time samples, compares their device-to-PC offsets, keeps readings within 2 seconds of the sample median and uses the lowest-round-trip-time stable reading. If at least three readings are not consistent, or a PC clock change or invalid measurement is detected, the operation stops and must be retried. When accepted, the page measures accumulated drift, adjusts the RTC rate, synchronizes the clock and establishes a new reference. This is an operator-triggered procedure, not continuous synchronization with an NTP server.

Use Manual RTC Drift Input only for independently measured remaining drift at the current calibration: positive seconds per day means the device runs fast; negative means it runs slow. Do not repeatedly apply the same old measurement because adjustment is incremental. Synchronize and measure again after correction. If RTC time was lost or a time read is invalid, synchronize first; an unsynchronized clock is not a valid drift reference. A clock-setting failure must be corrected before starting a new measurement period.

Reset Calibration returns the rate correction to zero and clears the stored drift reference. It does not by itself set the calendar to the current time; synchronize again before a new measurement.

4.4. HTTPS certificates

1. Sign in as admin and open the certificate section in Settings.
 2. Review the current certificate source, subject, issuer, validity and fingerprint.
 3. Generate a CSR on the device using the hostname or IP address that clients will actually use. Include matching subject alternative names.
 4. Submit the CSR to the site's certificate authority. The private key stays on the device.
 5. Upload the returned leaf certificate and any required intermediate chain using the certificate rotation controls.
 6. Allow the requested restart, reconnect and verify certificate trust and device identity.
- Do not generate another CSR while waiting for a certificate issued for the previous CSR; it can replace the pending key. Certificate reset returns the unit to self-signed HTTPS and can restart it. It is different from a factory reset.

5. Identity provider sign in

5.1. OpenID Connect

OpenID Connect (OIDC) lets users sign in through an identity provider such as a corporate identity service. Both ALD-200i and ALD-200e use the same OIDC implementation. A local administrator configures Settings > OpenID Connect (OIDC). Keep a working local administrator account for recovery.

OIDC is a common standard, but providers differ in application registration, allowed redirect addresses, browser token exchange, role claims and signing keys. A provider offering OIDC is not automatically compatible with this embedded client. The provider examples below are configuration guidance, not certified interoperability results.

5.2. Supported login method

This unit uses Authorization Code with PKCE S256 as a public browser client. It does not store or send a client secret. The device retrieves Discovery metadata and JWKS signing keys over HTTPS. The browser visits the provider, receives an authorization code at `/oidc/callback`, exchanges that code at the provider's token endpoint, and submits the returned ID token to the device. After validation, the device creates a local browser session with the mapped role.

The provider must allow this browser token exchange from the device's HTTPS origin using CORS. Configure the authorization response to return code and state in the callback URL query. Implicit or hybrid tokens in a URL fragment, `form_post` callbacks, client-secret-only applications,

SAML and Device Authorization Grant are not implemented. MFA can be required by the provider during its login screen; the device does not configure or enroll MFA.

Use the same browser tab and device address throughout sign-in. JavaScript, WebCrypto and sessionStorage must be available. Pending device login flows last five minutes; restart sign-in after expiry. The device supports four pending flows, but a new attempt in the same tab replaces that tab's saved PKCE state.

5.3. Certificate trust relationships

Connection	Required trust
Browser to dehydrator	The browser trusts the device HTTPS certificate. Manage this in HTTPS Certificate.
Dehydrator to provider	The device trusts the CA for the provider's Discovery and JWKS HTTPS servers. Paste it in Provider HTTPS Trusted CA Certificate (PEM).
Browser to provider	The browser independently trusts the provider's login and token endpoints.

The provider CA is not a token signing public key, private key or the device's server certificate. This firmware has no general public CA store: configure a suitable CA even for a public cloud provider. Include the PEM BEGIN CERTIFICATE and END CERTIFICATE lines. The field holds at most 2047 characters in total; each supplied certificate must be a CA. The provider must serve required intermediate certificates. Token signing-key rotation normally does not require replacing this CA.

5.4. Information to obtain from the identity administrator

Setting	Required value
Issuer URL	Exact HTTPS issuer from Discovery and token iss, including any trailing slash. Do not enter the authorization endpoint.
Client ID	ID of the registered public or SPA application. No client secret.
Scope	Start with openid and add only scopes needed to deliver the role claim. The UI default is openid profile.
Role Claim	Exact top-level ID-token claim name, such as roles or groups.

Setting	Required value
Viewer / Operator / Admin Role	Three distinct, case-sensitive claim values; default examples are Dehydrator.Viewer, Dehydrator.Operator and Dehydrator.Admin.
Redirect URI	Copy the displayed value, for example https://ald.example.com/oidc/callback .
Allowed browser origin	For that example, https://ald.example.com with no callback path.
Provider trusted CA	CA PEM for the device's outbound HTTPS validation.

Use a stable device hostname or reserved address. If a provider does not accept a private IP redirect, use a registered hostname that the commissioning browser resolves to the unit and that the device certificate covers. Register each address actually used. Switching between an IP and a hostname changes the origin and invalidates browser state. Issuer names must also resolve from the device: a PC-only hosts-file entry does not configure device DNS.

5.5. Role claim format

The selected claim must be in the ID token itself as a string or an array of strings. The device does not query UserInfo, Microsoft Graph or an external group directory. It does not traverse nested objects: entering `realm_access.roles` will not read roles inside `realm_access`. Configure a mapper or claim rule at the provider to emit a top-level value.

For example, a role claim containing the configured operator value grants operator access. A claim containing both the viewer and operator values also grants operator access. The identity administrator should verify the actual ID-token contents; detailed claim examples and interface limits belong to the separate REST API Reference.

When more than one mapped role is present, admin takes precedence over operator, then viewer. Missing or unmatched roles reject login; there is no automatic viewer fallback. Restrict provider role assignment to the intended users. Map exact role values rather than human-readable display labels unless those labels are actually emitted in the token.

Keep claims small. The current decoded ID-token payload limit is 1151 bytes, including all claim names and values. Large group lists, profile claims or provider-specific claims can exceed it even when authentication succeeds at the provider. Scope reduction alone may not remove mandatory claims. The REST API Reference lists all size and transport limits.

5.6. Commissioning procedure

1. Confirm local admin access over HTTPS. Resolve device certificate trust before starting OIDC. Set an accurate device clock in Device & Time.
2. Obtain the provider application settings, role assignments and trusted CA. Confirm that both the browser and the device can reach the provider over the required network paths.
3. On the device, expand OpenID Connect (OIDC). Copy the displayed Redirect URI into the provider registration and configure the exact device origin for browser token exchange.
4. Configure Authorization Code with PKCE S256, no client secret, RS256 with an RSA-2048 signing key, and the top-level role claim in the ID token. Use one of the provider recipes below as a starting point.
5. Enter the matching Issuer, Client ID, Scope, role claim, role values and CA PEM on the device. Enable OIDC and save. A saved configuration is not proof of a successful connection.
6. Sign out locally and select Sign in with OIDC. Allow Discovery and JWKS loading, complete provider login and any MFA, and return in the same tab.
7. Test a viewer, operator and administrator separately. Confirm the resulting role and verify that viewer access cannot change settings. Also verify that a user without a mapped role is rejected.
8. Test local-account recovery, logout and a fresh login. Record firmware, provider version or tenant, origin, claim mapping and test results before deployment.

5.7. Keycloak configuration example

Create an OpenID Connect client with Client authentication Off and Standard flow enabled. Register the exact callback under Valid Redirect URIs and the device origin under Web Origins. Set the PKCE code challenge method to S256 where enforcement is available. Use the realm issuer, for example <https://idp.example.com/realms/dehydrator>.

Create and assign the three dehydrator roles. In the client's dedicated scope, configure an appropriate user realm role or user client role mapper to emit a top-level roles claim, with Add to ID token enabled and multivalued string output. Make the scope available to this client and include it in the request if it is optional. Default `realm_access.roles` or `resource_access` nesting is insufficient for this device. Verify the actual ID token and limit unrelated claims.

On the unit, use that issuer and client ID, Role Claim = roles and the three assigned role values. Check the active signing key and common transport limits before acceptance.

5.8. Microsoft Entra ID configuration example

Register an application for the intended tenant. Under Authentication, add the device callback as a Single-page application redirect URI. A Web-platform redirect intended for server-side code exchange does not provide the required SPA CORS behavior. No client secret is needed for this unit.

Use the exact tenant-specific v2 issuer from Discovery, normally <https://login.microsoftonline.com/TENANT-ID/v2.0>, and the Application client ID. Do not substitute common or organizations: this device requires literal issuer equality and does not expand tenant placeholders.

Define user app roles with values Dehydrator.Viewer, Dehydrator.Operator and Dehydrator.Admin. Assign users or groups through Enterprise applications, and verify the roles array in the ID token issued for this application. Set Role Claim = roles on the device.

The recipe still requires device testing. Cloud token payloads or the Discovery/JWKS response can exceed this firmware's limits; a valid Entra registration alone does not establish compatibility.

5.9. Okta configuration example

Create an OIDC Single-Page Application integration and enable Authorization Code with PKCE without a client secret. Register the exact Sign-in redirect URI and verify token-endpoint CORS from the device origin. Do not confuse general Trusted Origins settings with the application's OAuth registration.

Use the issuer of the authorization server actually assigned to the application. The org issuer, such as <https://example.okta.com>, and a custom authorization-server issuer, such as <https://example.okta.com/oauth2/default>, are different; do not mix their metadata or keys.

Configure a filtered groups claim in the ID token containing only the required device groups. Set Role Claim = groups and map the exact group names. For a custom authorization server, configure claim inclusion and scopes so that the authorization-code response includes the claim in its ID token, not only in UserInfo or the access token. Avoid an unrestricted all-groups list.

Verify actual token size, signing key, CA trust and browser login on the unit before accepting the configuration.

5.10. Auth0 configuration example

Create a Single Page Application. Register the device callback in Allowed Callback URLs and the exact origin in applicable Allowed Web Origins and Allowed Origins (CORS) settings. Use Authorization Code with PKCE, no client secret and RS256 signing. Copy the exact issuer from Discovery; Auth0 issuers commonly end in a slash, which must be retained on the unit.

Use a deployed Post Login Action to add assigned application roles to the ID token with `api.idToken.setCustomClaim`. Access-token permissions alone do not satisfy this device. One suitable custom claim name is `https://ald.example/roles`; set that entire literal name as Role Claim on the device and map the three role values. Keep the name within 47 characters and verify a string-array value in the issued token. Use an organization-controlled namespace in deployment.

Adding an API audience is not required by this device's login flow. Confirm the returned ID token, CA chain and embedded-client limits before acceptance.

5.11. Other providers and unsupported profiles

For another provider, use the same commissioning checklist. Ask whether it can issue a compact RS256 ID token with an RSA-2048 key, a top-level mapped role, exact issuer and client audience, nonce and expiry through a public PKCE browser flow. If it requires a client secret, a special authorization parameter, an unsupported callback mode or a separate UserInfo request for roles, changing the device's nine settings is insufficient. Plan an integration change or an identity broker that presents the supported profile, then test it on the device. There is no universal per-provider compatibility switch.

5.12. Sessions logout and recovery

OIDC login creates the same local role-based browser session as local login. The device does not retain provider refresh tokens or revalidate the provider role on every request. Provider logout, account disablement or a role change does not automatically terminate an existing device session. Device Logout ends the local session; it does not sign out of the provider. A fresh OIDC login may therefore reuse an existing provider session. Follow the site's provider sign-out procedure when changing users on a shared browser.

Local browser sessions have an eight-hour inactivity timeout. Do not equate that timeout with the ID-token expiry. For urgent access removal, coordinate termination of existing device sessions; disabling OIDC prevents new OIDC sign-ins but is not a global session-revocation command.

Saving OIDC settings clears metadata, keys and pending login flows. Disabling preserves the supplied configuration. Keys are cached for up to one hour and reloaded after restart. A new kid triggers JWKS refresh; if login fails during the 30-second refresh rate limit, wait at least 30 seconds and start again.

When upgrading from the earlier manual-signing-key format, OIDC starts disabled and must be configured again. Local accounts and installed device HTTPS credentials remain. Device certificate rotation or certificate reset preserves OIDC settings; factory reset clears them.

5.13. Diagnosing OIDC login failures

Stage or symptom	Check
Settings save rejected	Required fields, lengths, HTTPS issuer, openid scope, distinct roles and valid CA PEM. configured means local validity only.
Loading provider or keys fails	Device DNS, IPv4 routing, device time, provider CA/host match, exact discovered issuer and response/TLS size limits.
Provider rejects callback	Exact registered HTTPS callback, SPA/public application type and the origin used to begin login.
invalid OIDC state	Same tab and origin, sessionStorage enabled, no competing login in that tab; restart the five-minute flow.
token endpoint error or browser CORS error	Public PKCE client, token-endpoint CORS, exact redirect, query callback and an unused authorization code.
ID token missing or device rejected ID token	Role in ID token, exact claim/value, RS256/RSA-2048/kid, issuer, audience, nonce, expiry and decoded token size.
public key refresh timed out	Provider reachability and JWKS contents; wait 30 seconds before a new login.

Use browser developer tools to distinguish a CORS failure from the device's token rejection. Do not paste live tokens, authorization codes or session cookies into public diagnostic sites. Retain only sanitized failure details for support.

5.14. Verify your installation

Provider examples describe configuration requirements and do not guarantee compatibility with every tenant, browser or provider version. Confirm sign-in, role permissions, logout, recovery and key renewal using the actual device and browser before deployment.

Provider references were reviewed on 14 September 2026. Console labels and policies can change; apply the protocol requirements above when labels differ.

6. Firmware updates and recovery

6.1. Updating firmware through the web interface

1. Obtain the approved AntennaLink firmware ZIP package for the exact hardware. Do not unpack, modify or substitute files in the package.
 2. Record current settings and versions, save relevant logs and schedule interruption of the air supply. Ensure a stable supply and working storage card.
 3. Sign in as admin and open Settings > Upload Firmware. Select the package and start the upload.
 4. Wait for upload and validation to finish. Review Firmware Status and Update Log. Do not proceed if package validation fails.
 5. Select Install & Reboot and confirm the action to install the staged update.
 6. Do not interrupt power or remove storage during installation. After the unit returns, reconnect and verify firmware version, network access, settings, alarms and normal air delivery.
- Uploading and validating a package is separate from applying it. A completed upload alone does not mean that the running firmware has changed. If the unit does not return, follow the supplier's recovery procedure; do not improvise a bootloader reflash.

6.2. Reset choices

A soft reset restarts the control task. A hard reset restarts the controller. A factory reset restores user configuration defaults and restarts the unit. Each can affect air delivery; coordinate the action with the site owner.

Factory reset clears local passwords and OIDC configuration, removes uploaded TLS credentials and requires new administrator setup. It restores ordinary settings, including network defaults. It preserves canister lifetime information, accumulated pump runtime and the latest pump runtime reset record. It is not a secure erasure procedure for all stored logs.

6.3. Physical account recovery

1. Power off. Hold UP, ENTER and DOWN together while powering on.
2. Keep all three pressed for 20 seconds, then release when requested.
3. Enter the last six numeric digits of the factory serial number. For 20260824-017, enter 824017. UP increases the digit, DOWN decreases it and ENTER accepts it.
4. After successful serial confirmation, release all buttons.

5. At ALL SETTINGS LOST, hold ENTER continuously for 10 seconds to confirm factory reset. Complete admin setup after reboot.

Releasing the initial hold early, failing the serial check or releasing the final ENTER hold early cancels recovery. Serial entry times out after 120 seconds of inactivity. This procedure is available only during boot.

VI. REST API

1. Scope and connection model

This reference describes the device-hosted REST interface for ALD-200i and ALD-200e monitoring and administration. It accompanies the User Manual. Read the User Manual before using operations that change air delivery, heater operation, security settings or firmware.

This reference describes the requests and responses available from the device. Check the installed firmware version before integration. The device-provided OpenAPI metadata is a compact route index and may not include every endpoint or all request and authorization details.

This edition replaces the REST material embedded in the distributed Rev.260818a User Manual and reconciles the later reference with firmware 1.1.1 build 40 source. Check the installed version before relying on a route or field. Examples are illustrative and do not constitute a record of device or provider acceptance testing.

1.1. Base URL

Use `https://DEVICE_ADDRESS/api/v1`. Replace `DEVICE_ADDRESS` with the actual device IP address or hostname covered by its certificate. HTTPS uses port 443. Validate the certificate with the site's trusted CA chain. Port 80 serves an HTML HTTPS guidance page for ordinary GET/POST requests, including API paths, before authentication or operation handling. It does not execute the requested API operation or automatically redirect. Never send credentials to HTTP; use HTTPS directly and validate status, Content-Type and the expected response body.

Paths in the following sections are relative to `/api/v1` unless explicitly shown as absolute. Path names and string values are case-sensitive. Send JSON requests with Content-Type: `application/json`. Send upload chunks as raw bytes with Content-Type: `application/octet-stream` and a known Content-Length. Configuration writes documented here use POST. Do not substitute PUT or PATCH.

1.2. Model and option handling

Read `/system/info` to identify the unit. In hardware responses, `model_id` 0 identifies ALD-200i and 1 identifies ALD-200e. Use `aux_heater_label` for presentation rather than renaming the shared `vapor_block_heater` JSON field. The shared field represents the model's auxiliary heater.

Configure and enable OIDC before using identity-provider sign-in. Confirm that the service is available and reachable on the installed device.

Examples use illustrative addresses and values. They are not recorded measurements, factory credentials or installation recommendations.

2. Authentication and authorization

Local REST clients use HTTP Basic authentication with the fixed IDs viewer, operator or admin and the account's current password. Passwords are case-sensitive. Use a secret store or an interactive prompt; do not place passwords in URLs or logs.

Browser requests can use the DEHYDRATOR_SESSION cookie established by browser login. An OIDC browser login creates that same type of session. Arbitrary OAuth bearer-token authentication is not supported for local REST requests. If a session cookie is present, it is evaluated before Basic authentication; use a separate cookie-free client for Basic integration.

Access	Minimum role
GET /heartbeat and GET /metadata/openapi.json or .yaml	Public
Most other GET requests, including status, alarms, logs and diagnostics	viewer
GET /system/certificates and all certificate subpaths	admin
GET /firmware/jobs and job subpaths	admin
GET or POST /system/oidc	admin
POST alarm settings, clear, hardware settings, manual outputs and Standby	operator
POST system, password, certificate, time, firmware and reset operations	admin
POST /hardware/pump-maintenance/reset	admin
GET or POST /system/snmp	admin

Higher roles include lower-role access. GET /firmware and GET /hardware/pump-maintenance are readable by viewer; do not apply the firmware-job or runtime-reset restriction to these reads.

After factory reset, provision admin through the browser before using authenticated integration. viewer and operator are disabled until passwords are assigned. Changing a local password invalidates browser sessions for that account. New Basic requests must use the changed password.

2.1. First read with curl

```
curl --cacert site-ca.pem --user viewer \  
https://DEVICE_ADDRESS/api/v1/system/info
```

This shell example prompts for the password. On Windows, call curl.exe to avoid a shell alias. Use the equivalent line-continuation syntax for your shell, or enter the command on one line.

2.2. Request example conventions

JSON examples are request bodies unless described as responses. Replace example hosts, addresses and secrets before use. The curl examples use POSIX line continuation; on PowerShell use curl.exe and put the command on one line or use the native shell continuation syntax. Never use a disabled certificate check as a permanent integration setting.

3. Responses errors and request discipline

Successful reads return resource-specific JSON. Many writes return an object containing ok and message; others return the updated resource without an ok property. Firmware validation uses is_valid. Always inspect the expected response shape, not just the HTTP status.

Result	Client action
HTTP 200 with expected resource	Parse and verify the required values.
HTTP 200 with ok equal to 0	Treat the operation as failed. Record message or error.
HTTP 400	Invalid request or operation rejected; inspect the response.
HTTP 401	Authenticate again or correct credentials.
HTTP 403	Use an account with the required role.
HTTP 404 or non-JSON response	Check route, identifier, feature availability and returned Content-Type.
HTTP 500 or 503 from log service	Inspect storage state or retry later with backoff.
Connection closed during reset or apply	Reconnect and verify resulting state before deciding whether to retry.

Some operations return HTTP 200 for application errors, and an unrecognized or malformed request can return an HTML error page. Preserve the status, Content-Type and a bounded response body for diagnosis. Do not attempt to decode every response as JSON.

3.1. Polling and concurrency

Use a modest polling interval, such as 3 to 10 seconds as an integration starting point, and increase it if the unit is busy. This is client guidance, not a throughput guarantee. Serialize configuration writes and upload operations. Avoid unnecessary repeated saves to nonvolatile storage.

GET /action-result is a shared latest-action buffer, not a per-client job or audit resource. Another request can replace its content. Use the direct POST response and a subsequent resource GET to verify a change. Do not use /action-result to correlate concurrent commands.

Most commands do not provide an idempotency key. After an ambiguous failure, read the current state. Do not blindly repeat reset, firmware apply, pump runtime reset, manual purge or certificate rotation. Read requests may be retried with bounded backoff.

4. Monitoring resources

Method and path	Response or purpose
GET /heartbeat	Public controller heartbeat
GET /system/info	Model, serial and device information
GET /firmware	firmware_version, build_number, bootloader_version and update information
GET /status	Object containing input, output and canisters
GET /status/input	Input or ambient temperature object
GET /status/output	Pressure, humidity, temperature, dew_point and legacy air_volume objects
GET /status/canisters	Object wrapping the canisters array
GET /status/canisters/A or /B	Individual canister status
GET /hardware	Hardware states and alarm configuration
GET /hardware/status	Hardware status view
GET /hardware/alarms	Hardware configuration view; can include additional hardware data

Method and path	Response or purpose
GET /diagnostics	Diagnostic information for service
GET /system/stacks	Controller stack and memory diagnostic information
GET /auth/me	Current authenticated user and role

4.1. Status fields and units

Output.pressure.value is gauge pressure and output.pressure.unit is psi. Output temperature and dew_point use C. output.humidity.unit can be C, F or %RH according to the selected humidity setting. Read the unit returned with each value; do not assume a web display-unit change converts all API resources.

Canister entries include canister_id, mode, drying_time_seconds, run_time_seconds, cycle_count, temperature, purge_power_wh and health. A and B are uppercase. Treat state strings as extensible and retain unknown values in logs instead of mapping them to a healthy state.

IMPORTANT: output.air_volume.value and relative are derived from pump duty although the object labels its unit CFM. They are not a calibrated volumetric-flow measurement. Do not use this field for flow calculations or acceptance testing.

Collection endpoints can reduce the number of monitoring requests. Do not infer successful installation from a firmware job state alone; read the running firmware version after reboot.

4.2. Canister state and condition fields

mode value	Current controller state
standby	Idle canister state; not proof of the global Standby setting
drying	Canister selected for drying
regenerating	Canister purge or regeneration state
cooling	Cooling state
supply	READY state; not proof of current external delivery
pending	Pending state

The health string is a temperature-derived indicator: good below 95 C, degraded from 95 C to below 110 C, and replaceSoon at or above 110 C in this implementation. These thresholds can be

crossed during regeneration. This field is not an estimate of remaining desiccant life and must not, by itself, trigger automatic canister replacement.

4.3. Heartbeat and diagnostics

GET /heartbeat returns status, timestamp and uptime_seconds. status is healthy, degraded when alarms are active, or unhealthy in the controller error phase. It is a controller summary, not a calibrated assurance of air quality. Check the operating readings and alarm set as well.

GET /diagnostics returns status (ok, warning or fault), fault_flags, warning_flags, last_fault_code, last_fault_text, watchdog_enabled, pump_on_seconds, hex_data, generated_at, device_serial and firmware_version. hex_data is 32 uppercase hexadecimal characters representing four 32-bit words. It is encoded diagnostic data, not encrypted data; do not use it to protect sensitive information.

Word	Meaning
0	Fault flags
1	Warning flags
2	Last fault code
3	Bits 31–24: format version (1); 23–16: state (0 ok, 1 warning, 2 fault); 15–8: watchdog enabled; 7–0: storage card present

5. Alarms and alarm history

GET /alarms returns the active-alarm collection. An empty response is {"alarms":[]}. Entries use the following compact schema.

Field	Type and meaning
code	Integer alarm code, for example 102
msg	Short human-readable message
sev	Numeric severity: 0 information, 1 warning, 2 error
first	First occurrence in seconds of controller tick time
last	Latest occurrence in seconds of controller tick time

first and last are not Unix timestamps and should not be used as calendar time. Alarm messages can be abbreviated. Use the numeric code as the stable identifier.

GET /alarms/{alarmId} accepts a numeric alarm ID as text. Its response differs from the collection: id, type, severity, message, active, triggered_at and cleared_at. triggered_at is a fixed epoch placeholder, not the real alarm time. Use alarm history for event timestamps.

5.1. History

GET /alarms/history?page=1 returns available, page, page_size, total, pages, pending, dropped, timezone, timezone_code, utc_offset_minutes and items. Page numbering starts at 1. Check available before reading items; storage contention can return available:false and error:storage_busy.

Items can include seq, timestamp, uptime_s, code, name, severity, event, value, threshold, unit, source, duration_s and reason. value and threshold can be null. pending and dropped indicate limitations in the event recording pipeline. Do not assume a complete history when events were dropped or storage was unavailable.

5.2. Clearing an alarm

POST /alarms/{alarmId}/clear requires operator or admin. Send an empty JSON object. The response can contain ok:1, message:alarm_cleared and alarm_id. Read /alarms afterward to confirm the active set. Acceptance does not establish that the underlying physical fault was corrected or that the code had been active.

For canister-heater faults, manual clearing suppresses that fault for the remainder of the current purge cycle. Design operator workflows so clearing does not hide an unresolved service problem.

6. Alarm setpoints and failure mode

GET /alarms/setpoints returns nested pressure and humidity objects. POST to the same path requires operator or admin and returns the saved representation on success. Read before editing and read again after saving.

```

{
  "pressure": {
    "low_warning": 0.15,
    "low_critical": 0.10,
    "high_warning": 0.35,
    "high_critical": 0.40,
    "unit": "psi"
  },
  "humidity": {
    "warning": -35.0,
    "critical": -25.0,
    "unit": "C"
  }
}

```

These values illustrate example defaults, not universally appropriate site settings. Pressure units are psi, bar or kPa. Humidity units are C or F for dew point, or %RH. A higher dew-point threshold represents wetter air. The ordering must be `low_critical <= low_warning <= high_warning <= high_critical`; humidity critical must be at least warning. Values must also satisfy the related device setting limits.

Do not interchange this schema with the Hardware schema. Hardware uses different unit strings and flat field names. For RH versus dew point, select explicit approved thresholds in the new unit; a single temperature-independent conversion is not appropriate.

6.1. Failure mode resource

GET `/alarms/failure-mode` returns mode and description. POST accepts one of the following strings.

```

{"mode": "zero_pressure"}
{"mode": "maintain_pressure_humid"}

```

`zero_pressure` shuts down air output for affected failures. `maintain_pressure_humid` permits continued supply with potentially degraded humidity control. This selection does not replace protective shutdowns or safe maintenance isolation. Record the approved site choice and verify the response after changing it.

7. Hardware configuration

GET `/hardware`, `/hardware/status` and `/hardware/alarms` can return overlapping information. Parse the fields needed rather than requiring a minimal response. Hardware includes model

information, pump, valves, outputs and an alarm object with enable_mask, setpoints and alarm items.

pump.pwm_duty and pump.avg_pwm_duty are fractions from 0 to 1. Reading this resource returns and resets the average, so multiple polling clients affect the sampling interval. It is not a fixed-window statistic shared independently with every client. Valve array IDs are 0 through 6; manual paths are valve-1 through valve-7.

POST /hardware or /hardware/alarms accepts flat fields. The web Hardware page's Alarm Settings area is an operator/admin control surface for nearly all alarm thresholds and decision times. It exposes humidity warning/critical values, high/low pressure warning/critical values and decision times, dry-air and regeneration temperature limits, heater protection limits, and pump-failure pressure/time limits, together with supported alarm enable controls. Values are entered in the selected units; use the displayed range, save, then use GET /hardware or GET /hardware/alarms to verify the stored result. Some alarms are enable-only or derived, and paired A/B enable bits can be normalized together. These are software input limits, not equipment ratings. Do not echo the entire GET envelope back as an update. Example of a targeted sensor-refresh change:

```
{"pump_operation_duty_target_pct":20}
```

Field or group	Accepted range or values for this interface
pressure_unit	psig, bar, kpa
temperature_unit	c, f
switch_humidity_unit, fault_humidity_unit, high_humidity_unit	dp_c, dp_f, rh
switch_humidity, fault_humidity, humidity_warning, humidity_critical	-40 to 20 C dew point; -40 to 68 F dew point; 0 to 20 %RH
pressure_high_warning, pressure_high_critical, pressure_low_warning, pressure_low_critical	0 to 1 psig equivalent
pressure_high_delay_sec, pressure_low_delay_sec	1 to 3600 seconds
emergency_pressure	0 to 5 psig equivalent

Field or group	Accepted range or values for this interface
dry_air_high_temp, regen_can_low_temp, wet_block_overtemp	55 to 200 C equivalent
heater_fault_time_sec	60 to 3600 seconds
heater_rise_temp	1 to 50 C temperature rise; see compatibility notes
heater_overtemp	100 to 400 C equivalent
pump_fail_pressure	0 to 0.5 psig equivalent
pump_fail_time_min	1 to 600 minutes
failure_mode	Integer 0 for zero pressure, 1 for maintain pressure with humid air
pump_operation_duty_target_pct	10 to 100 percent

Ranges are software input limits, not equipment ratings. Use integer values for counts, times and selectors. Return data may reflect rounding to stored precision. Paired A/B heater-fault enable bits and paired overtemperature bits are normalized together. Read the alarm items' bit values instead of guessing a bit position.

8. Manual control and maintenance

The following POST requests require operator or admin except for pump runtime reset, which requires admin. Send {} for commands without parameters. These actions can change air delivery immediately.

Path	Action
/control/standby/enable	Save and queue Standby On
/control/standby/disable	Save and queue Standby Off
/hardware/manual/dry-a	Select A for drying and mark B ready
/hardware/manual/dry-b	Select B for drying and mark A ready
/hardware/manual/purge-a	Request A regeneration
/hardware/manual/purge-b	Request B regeneration

Path	Action
/hardware/output/{target}/{command}	Temporary output override
/hardware/pump-maintenance/reset	Reset pump runtime and replace the latest reset record

Output targets are valve-1 through valve-7, fan, heater-a, heater-b, aux-heater and air-pump. For valves use open, close or release. For fan and heaters use on, off or release. For air-pump use off, 30, 80, 100 or release.

Output overrides expire after at most one minute. release returns the selected output to automatic control immediately. Pump test levels bypass ordinary pressure-based duty selection. Emergency pressure protection still opens valves and stops the pump. Perform such tests only with the physical system supervised and prepared for the consequences.

Standby saves persistently before queuing the control request. A success message such as standby_queued indicates acceptance, not that the pneumatic state has already settled. The ordinary /status response does not expose a dedicated Standby field in this interface. The browser's absolute /api/status.json resource exposes additional operating data, but is a separate interface that must be version-checked before integration.

8.1. Pump runtime

GET /hardware/pump-maintenance is available to viewer and higher roles. Read and archive the current runtime and reset record before resetting after replacement. Do not retry an uncertain reset blindly: it can overwrite the record of the pre-replacement runtime. Factory reset preserves this information. An unset clock can leave the reset timestamp unavailable.

9. Network accounts and time

System writes in this section require admin. A successful write can change the address or credentials used by subsequent requests.

9.1. Network

GET /system/network reads configuration. POST accepts mode dhcp or static. Static mode requires all three address fields.

```
{"mode":"static","ip_address":"192.0.2.20",  
  "subnet_mask":"255.255.255.0","gateway":"192.0.2.1"}
```

The address above is illustrative. Supply values assigned for the real network. DHCP uses {"mode":"dhcp"}. The device saves the configuration and requests network reapplication. Reconnect at the resulting address; use the local display if the connection is lost.

9.2. Passwords

POST /system/password accepts user and new_password. user must be viewer, operator or admin. Always provide it explicitly; omission defaults to admin. The supported length is 4 to 31 characters. Verify success without echoing the password in application logs.

```
{"user":"operator","new_password":"REPLACE_WITH_A_UNIQUE_SECRET"}
```

9.3. Clock and time zone

GET /system/time returns timestamp in UTC with a trailing Z, local_timestamp, timezone, timezone_code, utc_offset_minutes, dst_active, unix_time, subsecond_ms, valid, source and uptime_seconds. The controller validates the RTC fields and reads a coherent time/date pair; treat valid:false or source:unknown as an unusable clock. GET /system/timezones returns the supported time-zone names in a timezones array.

POST /system/time accepts unix_time or timestamp and can also accept timezone. Specify a single time representation. With both supplied, unix_time takes precedence. A trailing Z provides an unambiguous UTC timestamp. A successful explicit clock write invalidates the stored RTC drift reference; a timezone-only update does not change the clock.

```
{"timestamp":"2026-09-10T03:00:00Z","timezone":"Asia/Seoul"}
```

Sending only timezone changes the region. Do not send utc_offset_minutes; it is derived from the region and daylight-saving rule and is rejected as a writable setting. A numeric timestamp offset must agree with the selected region for that instant. Inspect valid and read back both UTC and local time. If the RTC write cannot be completed, the response is {"ok":0,"message":"time_set_failed"}; do not assume that the requested time was applied.

9.4. RTC fine calibration

GET /system/time/calibration reports correction_steps, correction_ppm, correction_seconds_per_day, step_ppm, step_seconds_per_day, drift_min_milliseconds_per_day, drift_max_milliseconds_per_day, reference_valid, reference_unix_time, reference_offset_ms, rtc_clock_source, time_valid, time_source and auto_adjust_ready. Ordinary authenticated read permissions apply. POST requires admin. auto_adjust_ready is true only when a reference exists and the RTC time is valid and synchronized from a trusted recovered or manual source.

POST action	Required additional fields
set_reference	reference_unix_time and reference_offset_ms; requires synchronized device time.
apply_drift	drift_milliseconds_per_day, a signed integer from -120000 to 120000.
apply_auto_drift	drift_milliseconds_per_day; also requires a valid reference and at least 86400 seconds of elapsed device time.
reset	No additional fields; clears correction and the stored reference.

Positive measured drift means the device runs fast. The correction is added to the existing calibration with the opposite sign; this is not an absolute calibration setting and is not safe to replay blindly. A successful drift adjustment invalidates the old reference. Set the time and establish a fresh measured reference afterward, as the supplied browser does. An explicit calendar time write also invalidates the reference. Merely reading auto_adjust_ready does not prove that the required 24-hour measurement period has elapsed; the server enforces that minimum for apply_auto_drift.

The accepted actions are set_reference, apply_drift, apply_auto_drift and reset. set_reference accepts a reference Unix time of at least 946684800 and a reference offset within +/-3600000 ms. Record the offset as device clock minus reference clock, using a request/response midpoint measurement. apply_auto_drift receives the measured daily drift from the client; it does not contact an NTP server or independently measure drift. The supplied Settings page obtains five GET /system/time samples, rejects a PC clock change or non-finite measurement, and selects the lowest-round-trip-time sample within 2 seconds of the sample median; at least three stable samples are required. Inspect ok and message, including measurement_period_too_short, rtc_time_not_synchronized, rtc_reference_not_set, rtc_reference_time_invalid and calibration_range_exceeded, then read back the result.

Illustrative manual correction for a device independently measured to run 1.5 seconds per day fast:

```
{ "action": "apply_drift", "drift_milliseconds_per_day": 1500 }
```

10. Certificate management

All certificate reads and writes require admin. GET /system/certificates reports HTTPS availability, certificate source, subject, issuer, subject alternative name, validity, SHA-256 fingerprint, csr_pending and server status. Verify identity independently when first establishing trust.

10.1. Generate a request

POST /system/certificates/csr generates an on-device EC P-256 key and CSR. common_name is required. Optional fields include organization, country and subject_alt_names. Use the actual hostname or IP clients will connect to.

```
{ "common_name": "dehydrator.example.net",  
  "subject_alt_names": [ "dehydrator.example.net", "192.0.2.20" ] }
```

Save the returned CSR and submit it to the site's CA. GET on this path returns guidance and pending-key state, not a previously generated CSR. Private keys are not exported. Avoid generating a second CSR before installing the certificate for the first one.

10.2. Upload a signed certificate

Use the chunked interface for predictable payload sizes. The device allows up to 16382 bytes total for leaf plus chain, with a maximum chunk size of 2048 bytes. Use exact PEM byte lengths, not character counts after text transformations.

1. POST /system/certificates/upload/start with certificate_size and chain_size. Inspect ok and chunk_max.
2. POST raw leaf PEM bytes to /system/certificates/upload/leaf/chunk/{offset}, starting at offset 0 and increasing by the bytes accepted.
3. If a chain is supplied, POST its bytes to /system/certificates/upload/chain/chunk/{offset}. Chain offsets start independently at 0.
4. POST {} to /system/certificates/upload/finish. Confirm the returned result and allow any requested reboot.
5. Reconnect with certificate verification and compare the installed certificate information with the intended certificate.

POST /system/certificates/rotate is the direct JSON alternative using certificate and optional certificate_chain, both PEM strings with escaped newlines. Chunked upload is preferable for larger chains. Do not upload a private key with these requests.

POST {} to /system/certificates/reset removes the installed credentials and returns to self-signed HTTPS after restart. This is distinct from factory reset. Certificate rotation and certificate reset preserve OIDC configuration; factory reset clears it.

11. Firmware staging and application

Firmware writes and job reads require admin. Use an approved ZIP package for the exact hardware. The workflow is upload, validate, inspect, apply, reconnect and verify. A staged package is not yet the running firmware.

11.1. Chunked upload

Read /firmware and record current firmware, bootloader and build information.

2. POST {} to /firmware/upload/start/{totalSize}. totalSize is the ZIP package byte length.

3. POST sequential raw chunks to /firmware/upload/chunk/{offset}. Begin at byte 0. Use 2048-byte chunks or smaller; the supplied HTTPS client uses 512 to 2048 bytes. Wait for and inspect each reply before advancing.

4. POST {} to /firmware/upload/finish. Inspect the result and retain the returned job_id when available.

5. POST {} to /firmware/validate and require is_valid:true and is_compatible_with_device:true. Review checksums, signature results, validation_errors and validation_warnings.

POST /firmware/upload is a direct raw ZIP upload alternative. Do not send browser multipart form data unless explicitly supported by the installed firmware. Serialize uploads: there is a shared staging area, not an independent upload slot per client.

11.2. Verification and apply

Validation reports firmware_version, file_size_bytes, crc32, checksum, checksum_verified, sha256_verified, signature_required and signature_verified. These refer to the staged image; file_size_bytes is not necessarily the ZIP size. If a verification step is reported as skipped, do not treat it as a successful cryptographic check. Confirm that validation meets the update requirements for the supplied equipment.

POST /firmware/apply requires {"confirm":true}. This revalidates the current staged package and requests installation and reboot. Additional version, size and crc32 request fields are not checked for a match. Prevent another administrator from replacing staging between validation and apply.

After the connection returns, read /firmware and /system/info, compare the installed version and device identity, and verify operation. GET /firmware/jobs reports the current job collection; GET /firmware/jobs/{jobId} reads the current job by its returned identifier. This is not an unlimited historical job database. Collection or upload status completed can refer to completed staging and must not alone be treated as installed firmware.

12. Logs, resets and identity settings

12.1. CSV log download

GET /logdown or GET /logdown/1 downloads a snapshot of the current log. GET /logdown/{ageIndex} downloads an older log by age, with 2 representing the next older available file. Indices must be positive decimal integers. They identify relative file age, not a stable filename or a number of days.

The response is a file stream. Save it as CSV after checking the HTTP status and Content-Type; an error response may be JSON instead. Log availability depends on the storage card and retained files. POST /logdown is not supported for downloading and returns a message directing the client to GET.

```
curl --cacert site-ca.pem --user viewer \
  https://DEVICE_ADDRESS/api/v1/logdown/1 --output log.csv
```

12.2. System reset

POST /system/reset requires admin and a reset_type string: soft, hard or factory. soft restarts the control task; hard restarts the controller; factory resets configuration and restarts. Read the User Manual's reset effects before using factory. It clears local passwords, OIDC settings and uploaded TLS credentials, restores ordinary defaults and requires admin provisioning. It preserves canister lifetime data and pump runtime/reset records.

```
{"reset_type":"hard"}
```

Coordinate interrupted air delivery and verify the result after reconnection. A factory reset can also change addressing and invalidate the previous HTTPS trust relationship. It is not a complete storage-media erasure operation.

12.3. OpenID Connect configuration

GET and POST /system/oidc require admin. POST replaces the OIDC configuration and requires all nine writable fields below. enabled is the number 0 or 1; all other writable values are strings. Unknown or duplicate fields are rejected. GET also returns configured; omit this read-only field when writing. configured indicates an enabled, locally validated configuration, not successful provider connectivity.

Field	Meaning and limit
enabled	0 disables sign-in; 1 enables it. Disabling preserves supplied values.
issuer	HTTPS Issuer URL, at most 191 characters. Must exactly match the discovered issuer and token iss.
client_id	Provider-issued public-client ID, at most 127 characters.
scope	At most 95 characters; must contain the space-delimited openid scope when enabled.
role_claim	Top-level token claim used for role mapping, at most 47 characters.
viewer_role	Viewer claim value, at most 63 characters.
operator_role	Operator claim value, at most 63 characters.
admin_role	Admin claim value, at most 63 characters. All three role values must differ.
trusted_ca_pem	IdP HTTPS CA certificate PEM, at most 2047 characters. A parsable CA certificate is required when enabled.
configured	GET only. Enabled configuration state; not a live connection test.

The CA is the trust anchor for outbound HTTPS, not the ID-token signing key or the device's HTTPS server certificate. This firmware does not ship a general public CA store, so a suitable CA is required for public and private providers. The provider must serve the intermediate certificates needed to build a valid chain. Changing the provider's token signing key normally does not require a CA update.

POST example follows. Replace the illustrative certificate body with the complete CA PEM supplied by the site's identity administrator; the placeholder is not a valid certificate. Encode PEM newlines as JSON escapes.

```
{
  "enabled": 1,
  "issuer": "https://idp.example.com/realms/dehydrator",
  "client_id": "dehydrator",
  "scope": "openid profile",
  "role_claim": "roles",
  "viewer_role": "Dehydrator.Viewer",
  "operator_role": "Dehydrator.Operator",
  "admin_role": "Dehydrator.Admin",
  "trusted_ca_pem":
    "-----BEGIN CERTIFICATE-----\nCA_BASE64\n-----END CERTIFICATE-----\n"
}
```

A successful save returns `{"ok":1,"enabled":1}`, or `enabled:0` when disabled. Invalid settings are rejected without replacing the stored configuration. Saving clears provider metadata, keys and pending OIDC sign-in flows. Incomplete values may be stored while disabled, but the same nine fields and their size limits still apply.

12.4. Discovery and signing key refresh

The device retrieves `/.well-known/openid-configuration` under the configured Issuer, checks exact issuer equality, and reads `authorization_endpoint`, `token_endpoint` and `jwt_uri`. These endpoints must use HTTPS. `authorization_endpoint`, `token_endpoint` and `signing_public_key_pem` are no longer writable configuration fields; legacy POST bodies containing them are rejected.

The device downloads JWKS directly and selects an RSA-2048 RS256 signing key by the token's required kid. It validates the signature, issuer, audience, stored nonce, expiry and role. A role claim may be a string or string array; when several mapped roles are present, admin takes precedence over operator and viewer. Keys supplied by the browser or token `jku/x5u` URLs are not trusted.

Keys are cached in RAM for up to one hour. Restart clears the cache. An unknown kid requests a JWKS refresh, with a minimum 30-second interval between refresh starts. Unexpired known keys remain usable during a JWKS network outage; unknown or expired keys are not substituted or accepted. A replacement set containing duplicate kid values or invalid RSA signing keys is rejected.

The browser callback uses the absolute path POST /api/oidc/login with application/x-www-form-urlencoded state and id_token fields. HTTP 202 means key refresh is pending; the supplied callback retries at one-second intervals up to 30 times. HTTP 200 issues the local session cookie, while HTTP 401 rejects the token or flow. This is an internal browser sign-in exchange, not a general bearer-token REST authentication interface. If a new key appears during the refresh rate-limit interval, wait 30 seconds and start a new login.

The flow remains Authorization Code with PKCE S256 and browser-side token exchange. Register the exact device HTTPS origin plus /oidc/callback, and enable the corresponding public-client/SPA and CORS behavior at the provider. No client secret is stored on the device.

12.5. Provider connectivity and upgrade limits

Outbound HTTPS verifies CA trust, host identity and certificate dates using the device RTC. IPv4 URLs require an exact IP-address SAN; DNS names must match the server certificate. An uninitialized device time earlier than 2020 is rejected. Device and browser must both reach the provider; the PC's localhost or hosts-file entry does not configure device networking. DNS comes from DHCP or, when unset, the static network gateway's DNS service.

Supported profile: IPv4; TLS 1.2 with ECDHE-RSA or ECDHE-ECDSA and AES-128-GCM-SHA256; RSA-2048 RS256; up to eight signing keys with kid values of at most 127 characters. Discovery/JWKS URLs are limited to 255 characters. HTTP responses including headers are limited to 16 KiB and TLS records to 4096 bytes. Each fetch has a 15-second DNS/connect/receive deadline. Basic Content-Length, connection-close and chunked framing are accepted; redirects, compression, IPv6 and chunk extensions/trailers are not supported. Confirm actual provider interoperability against this profile.

The new OIDC storage format does not activate older manual-signing-key settings. After upgrade, OIDC is disabled and must be configured again. Local accounts and installed device HTTPS credentials remain available. HTTPS certificate rotation/reset preserves OIDC settings; factory reset clears them.

12.6. Provider profile and claim interoperability

The User Manual supplies commissioning recipes for Keycloak, Microsoft Entra ID, Okta and Auth0. They are configuration examples, not a list of certified providers. All providers must meet the device requirements described below.

The callback reads code and state from the URL query. Browser token exchange uses grant_type=authorization_code, client_id, code, redirect_uri and code_verifier without a client secret. The provider must accept this public PKCE S256 exchange and allow CORS from the exact

device HTTPS origin. form_post, implicit and hybrid responses, required custom authorization parameters, client-secret authentication and SAML are not handled. No UserInfo, group-directory or bearer-token REST integration is provided.

role_claim is a literal, top-level ID-token key, not a dotted path or JSONPath. A string or string array is accepted. A namespaced key such as https://ald.example/roles works when its complete name is within 47 characters. Nested realm_access.roles and resource_access objects require a provider mapper. Roles supplied only in an access token, UserInfo or a group-coverage reference cannot authorize this client. Missing/unmapped roles reject sign-in; precedence is admin, operator, viewer.

For a literal role_claim value of roles, either {"roles":"Dehydrator.Operator"} or {"roles":["Dehydrator.Viewer","Dehydrator.Operator"]} grants the mapped operator role. These are claim excerpts, not complete or usable tokens.

12.7. Token and client resource limits

Item	Current limit or behavior
Decoded JWT header	511 bytes of JSON plus terminator storage.
Decoded JWT payload	1151 bytes of JSON; includes every claim, not just mapped roles.
Submitted ID token	At most 4095 characters; decoded limits usually constrain it first.
Signing profile	RS256 with RSA-2048 and a required kid. ES256, PS256 and HS256 are not accepted.
Pending flows	Four device slots, five-minute lifetime. Browser state is per tab and origin.
Claim names and mappings	Exact case-sensitive comparison; no directory lookup or nested traversal.

Large default cloud ID tokens can fail before role mapping. Request only required scopes and filter optional claims and groups, then measure the actual returned token without logging it. If unavoidable provider claims exceed the decoded payload limit, settings changes cannot establish compatibility; a firmware or broker integration change is required. Do not confuse token-signing RSA with the separate algorithm used by the provider's HTTPS certificate.

12.8. Local session lifecycle

Successful ID-token validation creates a local role session. Token expiry is checked at sign-in, but does not become the local session expiry. Local sessions use the eight-hour inactivity timeout

and four-session limit. The device does not preserve refresh tokens, poll provider revocation or re-check role assignments for every request.

Device logout clears the local session only. Provider logout or role removal does not automatically invalidate an existing device session. Saving or disabling OIDC clears pending flows and provider caches but is not a global local-session revocation action. Plan session termination separately for urgent access removal. A local admin account remains the recovery path over HTTPS.

12.9. Provider acceptance tests

1. Verify device HTTPS trust, browser WebCrypto/sessionStorage, device time and outbound IPv4/DNS/CA connectivity.
2. Verify Discovery issuer equality, reachable HTTPS endpoints, JWKS key size/count and the documented HTTP/TLS limits using the device itself.
3. Complete the real browser PKCE exchange from the registered origin. A Python or server-side token exchange does not test browser CORS.
4. Verify all three mapped roles, rejection of an unmapped user, decoded token sizes and local /api/v1/auth/me results over HTTPS.
5. Test logout, a new user session, local recovery, key rotation, concurrent logins and cache expiry in a planned test environment.

Record the provider or tenant, browser and device firmware with each acceptance result. Complete testing with the actual device and browser; configuration examples alone do not establish interoperability. Consult the provider recipes in the User Manual.

13. Compatibility notes and integration acceptance

The following limits are material to clients using this interface. Recheck them whenever firmware changes. They describe interface behavior, not recommended client assumptions for future releases.

Topic	Integration consequence
Embedded OpenAPI metadata	A route index with limited schemas; optional and newer routes may be absent.
GET /status/output air_volume	Pump-duty-derived value labeled CFM; unsuitable as measured flow.
Active alarm first and last	Controller tick seconds, not UTC.

Topic	Integration consequence
Single alarm triggered_at	Epoch placeholder; use available history records for real event timing.
Hardware average pump duty	Reading the response resets the average; other readers affect the interval.
Firmware apply identity	confirm is checked and staging is revalidated, but request version/size/CRC are not matched. Serialize staging and apply.
heater_rise_temp	The API stores a Celsius temperature rise without converting according to temperature_unit. Submit the rise in C and validate the read-back; do not use it as an absolute Fahrenheit value.
OIDC and OAuth declarations	Browser OIDC is implemented; generic REST bearer authentication is not.

13.1. Changes from the distributed manual

Earlier assumption	Current integration requirement
HTTP API base address	Use HTTPS on port 443 and validate the device certificate
Single account or universal default password	Provision admin and assign independent viewer/operator passwords
PUT for settings changes	Use the POST routes and exact schemas documented here
Upload a raw BIN then reboot	Upload the approved ZIP, validate, apply with confirm:true and verify after reboot
Upload the server private key	Generate a CSR on the unit; install the issued certificate and chain
Log index identifies a day	Log index is relative retained-file age
Diagnostic hex is encrypted	It is an encoded diagnostic summary
Canister health or air_volume is a calibrated measurement	Health is temperature-derived; air_volume is derived from pump duty

13.2. Integration acceptance checklist

1. Confirm the model, firmware version, build and enabled options on the real device.

2. Verify HTTPS trust and role enforcement with viewer, operator and admin accounts.
3. Compare status units and alarm responses with observed operation. Test unavailable storage and invalid clock handling.
4. Perform one approved reversible settings change, check the direct response and GET read-back, then restore the original value.
5. Test timeouts and lost responses without blindly replaying physical actions.
6. Stage and validate an approved firmware package. Apply only in a scheduled maintenance window and verify the installed version after reboot.
7. Archive the tested response samples and configuration with the integration version.