



# User Manual for Network Based Ambient Temperature and Humidity Sensor Model FTA3070-21

---

Description – Initialization – Technical Information

## Sensor Technical Information

General	
Model	FTA3070-21
Dimension	Length × Height × Depth 14 cm × 2.4 cm × 9.4 cm
Weight	500 g
Working Temperature	-10 to 80 °C
Storage Temperature	-20 to 80 °C
Working Humidity	0 – 60%
Working Voltage	24 - 100 Volts
Mounting Brackets	2 holes at the top to be fixed on the wall
Guaranty	2 Years
Input/ Output	
Type of Input	Ambient Temperature and Humidity
Temperature Measurement Range	-30 to 70 °C
Humidity Measurement Range	0-100 percent
Output	Network

## Security Considerations

---

(Before using this product, please read the precautions)

Please carefully read this manual before using the product and pay full attention to the mentioned points to use the product correctly.

In this manual, safety measures are classified into two levels:

“Warning ⚠ ” and “Caution ⚠ ”.

---

Warning ⚠	Improper handling may lead to dangerous conditions and cause death or serious injury.
-----------	---

---

---

Caution ⚠	Improper handling may lead to dangerous conditions and cause minor or moderate injury to persons or damage to property.
-----------	---

---

Follow the safety measures of both levels as they are very important for personal and system safety. Ensure that users read this manual and then keep it in a safe place for future reference.

## Design Precautions

---

### Warning ⚠

---

- Paying attention to the details of cabling and proper connection is one of the most important parts of installing sensors, which directly affects the performance and efficiency of the network.
- Always use a consistent standard (T568A or T568B) at both ends of the cable to prevent connection issues.
- Mistakes in wiring during socket installation can lead to hardware damage to the Sensor or improper network performance.
- After installing the sockets, connect the cable to the Sensor. If the Sensor is not recognized or does not function properly, check the following:
  - Complete connection of the socket to the cable
  - Correct wiring arrangement
  - Use a network tester to identify potential cabling errors

- If the above points are confirmed, test the relevant sensor with a tested network cable at the sensor installation site to ensure the sensor's proper functioning.
- Avoid excessive bending or sudden pulling of cables while working with them, as this can damage the internal wires and reduce signal quality.

---

**Caution** 

---

- Do not bundle the RJ45 cable with the main circuit and power cables, and do not install them close to each other. Maintain a minimum distance of 100 mm (3.94 inches) between them. Failure to maintain this distance may cause interference due to noise.

## Installation Precautions

---

**Warning** 

---

- Before installing the sensor, ensure the quality of the cable being used. The manufacturer recommends using RJ45 with CAT6 specification. Failure to follow this guideline may result in damage to the device.
- To maintain signal integrity, it is essential to connect the shield of the RJ45 cable to properly shielded sockets.
- Avoid installing the sensor in environments with extremely high or low temperatures or humidity levels that exceed the sensor's operating range. Such conditions may lead to malfunction or incorrect performance.
- Use the sensor strictly for its intended purposes. Do not connect it to incompatible devices, as this may cause errors or permanent damage.

---

**Caution** 

---

- Use the sensor in an environment that complies with the general specifications in this manual. Using this sensor in any other operational environment may cause electric shock, fire, malfunction, or damage and reduce the quality of the module.
- Never directly touch the conductive part or electronic component of the sensor. Doing so may cause malfunction or damage to the data logger.
- When installing sensor on the wall, carefully tighten the wall screws. Loose screws may cause the sensor to fall and create a short circuit.
- Prevent external materials such as dust or wire fragments from entering the Sensor. These external materials may cause fire, malfunction, or damage.

## Wiring Precautions

---

### Warning ⚠

---

- Before wiring, ensure the health and quality of all input and output cables. Failure to do so may cause product damage.
- 

### Caution ⚠

---

- Before connecting the RJ45 cable, ensure that the type of connector to be connected is correct. Connecting an incorrect connector or incorrect wiring will cause Sensor damage.
- When wall-mounting the sensor, tighten the mounting bracket screws securely. Loose screws can cause the sensor to fall and short circuit.
- Securely connect the RJ45 cable to the sensor. Failure to do so may cause cable damage and improper device operation.
- Ensure that all incoming data cables connected to the sensor are routed through a cable channel or secured with a cable tie. Failure to do so may result in accidental cable pulling, which can damage the sensor and cables or cause module malfunction due to loosen connections.
- Handle RJ45 cables with care when disconnecting them from the sensor. Pulling on the cables can lead to device malfunctions or damage to the sensor or cable.

## Startup and maintenance precautions

---

### Warning ⚠

---

- Do not touch the conductive or electronic part of the sensor while it is activated. Doing so may cause an electric shock or damage the sensor.
- 

### Caution ⚠

---

- Sensor Installation and setup **must** only be done by qualified and expert repair personnel familiar with the knowledge related to protection against electric shock.
- Avoid resetting the sensor unnecessarily. Doing so will cause all changes made on the sensor's web page will be returned to factory settings.

## Operational safety measures

---

### Warning

---

- Do not touch any conductive parts or electronic components of the sensor while it is transmitting data. Doing so may cause the sensor to malfunction or fail.
- 

### Caution

---

- To avoid noise interference, keep all radio communication devices, including mobile phones, at least 25 centimeters away from the Sensor in all directions.
- 

## Waste disposal precautions

---

### Caution

---

- Dispose the sensor as an industrial waste.
- Ensure sensors are segregated from other waste in accordance with local regulations. Dispose of sensors correctly at your local waste collection/recycling facility.

## Contents of the box

---

Please verify that the box contents match the packing list. The following items should be included:

- Ambient Temperature and Humidity Sensor, model FTA3070-21 <sup>1</sup>
- 48-volt adaptor <sup>2</sup>
- SD Card
- OTG cable
- User manual.

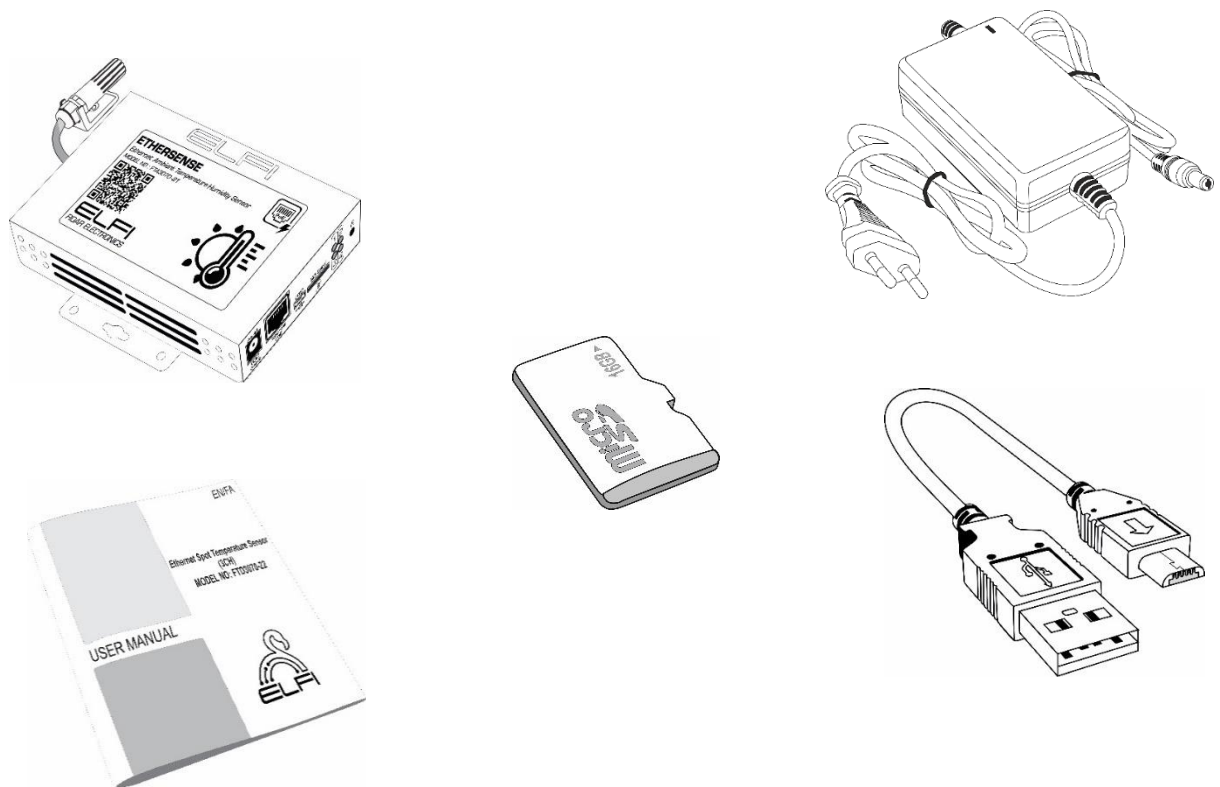


Figure 1: Contents of the box

---

1. Detailed dimensions of the device can be found on page 25 of the user manual.  
2. If requested by the customer

# Table of Contents

---

- 1. Initialization of the Sensor..... 9
- 2. Connecting Sensor to network..... 11
- 3. Sensor Software Configuration..... 11
  - 3.1. Status Menu ..... 12
  - 3.2. General Settings Menu..... 13
  - 3.3. Network Settings Menu..... 14
  - 3.4. SNMP Settings Menu ..... 16
  - 3.5. Relay Settings Menu..... 17
  - 3.6. Alarm Settings Menu ..... 18
  - 3.7. Trap Settings Menu..... 21
  - 3.8. Email Settings Menu ..... 23
- 4. Sensor Dimensions..... 25
- Contact Info ..... 26

# 1. Initialization of the Sensor

---

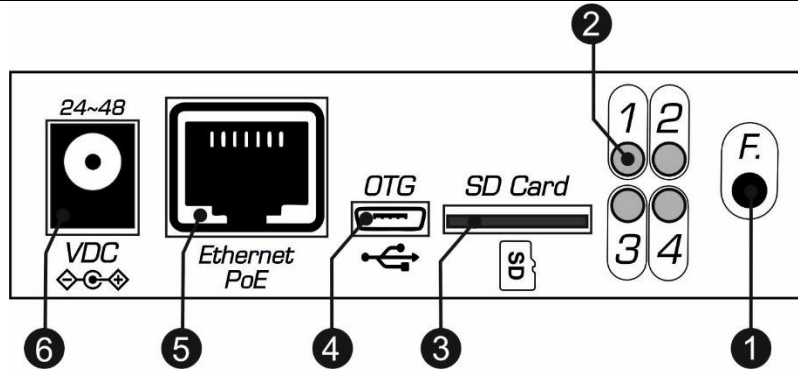


Figure 2: Side view of the sensor

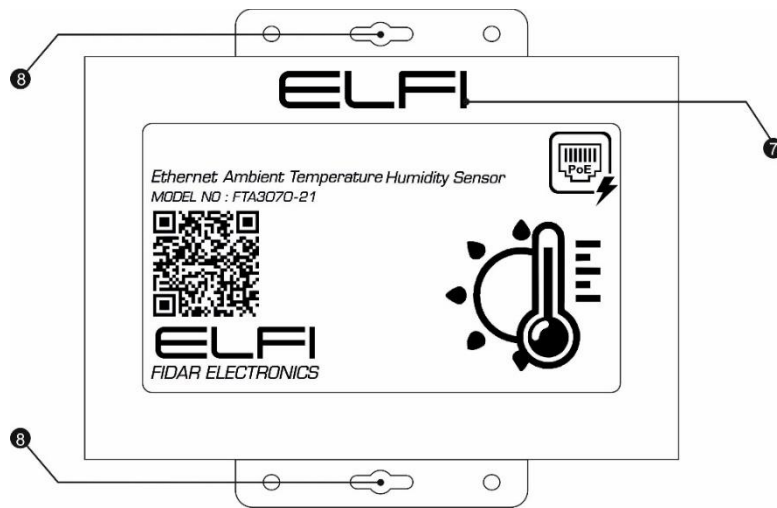


Figure 3: Front view of the sensor

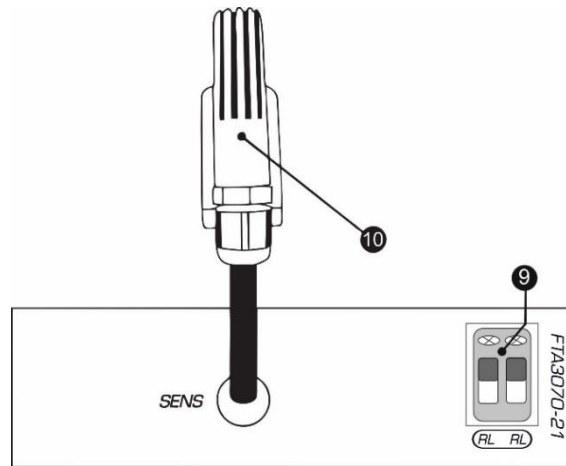



Figure 4: Side view the sensor

Table 1: Information related to Sensor cover

Number	Name	Description
1	F Key	To reset the sensor
2	POWER LED	Indicates Sensor's Power Connection
3	SD Card	SD Card input
4	OTG	OTG cable input
5	Ethernet PoE	Ethernet cable input
6	VDC	Adaptor input
7	Sensor Power Connection Display	If the Sensor's power is connected the  symbol will be displayed in green.
8	Wall Mounting Location	<hr/>
9	RL	To connect the sensor to alarm equipment (e.g. sirens, indicator lamps) or a cooling system
10	Ambient Temperature and Humidity measuring Sensor	<hr/>

## 2. Connecting Sensor to network

---

To set up the sensor, if you are using a PoE switch, simply connect the Sensor to the switch using a cable. Otherwise, use a 48V adapter to set up the sensor and then connect the Sensor to your network using a network cable.

**Note:** Please note that under no circumstances should you use the adapter and network cable at the same time to set up the Sensor.

**Note:** If the sensor is offline, first check the RJ45 or Ethernet cable connection. If the cable is properly connected and the sensor is still not responding, perform a reset as follows:

Disconnect the Ethernet (RJ45) cable from the sensor. Press and hold the F button. While holding the button, reconnect the Ethernet cable. Continue holding the F button until the **ELFI** indicator light turns on, then release the button.

## 3. Sensor Software Configuration

---

To access the sensor's user interface, after powering it on, enter the IP address 192.168.1.7 into a browser on a computer connected to the same network. Enter the username and password <sup>1</sup> to access the sensor's web interface (see Figure 5).



Figure 5: Sensor Web Page

---

1. The default username and password for this sensor are both "admin".

### 3.1. Status Menu

---

The Status page displays real-time and essential sensor information to the user. This page includes temperature and humidity charts as well as technical data related to the sensor, providing a convenient way to monitor system performance quickly and efficiently (see Figure 6).

#### Temperature and Humidity Chart

In this section, the temperature readings captured by the sensor are displayed graphically:

- The temperature and humidity curves are clearly identified on the chart using distinct colors and labels.
- Real-time data along with historical trends are visualized for both temperature and humidity.
- The chart is automatically updated to reflect accurate and up-to-date information.

#### Product Information

This section provides technical details about the sensor:

- **Device Name:** Custom name assigned to the sensor for easy identification on the network or in the field.
- **IP Address:** The network address through which the Sensor is connected.
- **Uptime:** The total time the Sensor has been running continuously since the last startup or reset.
- **Firmware Version:** Indicates the current software version of the Sensor, reflecting its features and updates.
- **Time:** The current date and time set on the Sensor, essential for event logging and time synchronization.
- **Serial Number:** The unique ID of the Sensor used for tracking and documentation.
- **Sensor (Node) part number:** Corresponding to the Sensor hardware, identifying its technical specifications.



Figure 6: Sensor “Status” Menu

### 3.2. General Settings Menu

This menu allows for time configuration and password changes (see Figure 7).

- To configure time settings, use the NTP option to automatically synchronize the Sensor’s clock with internet time servers. If disabled, you can manually adjust the date and time, or sync with your computer’s clock.
- For enhanced security, change the default Sensor password.

**Note:** The default Device Name is the Sensor's Serial Number. It is recommended to rename the device after setup for easier identification.

**Note:** After making any changes, first click Save and then select Reboot to apply the settings completely.

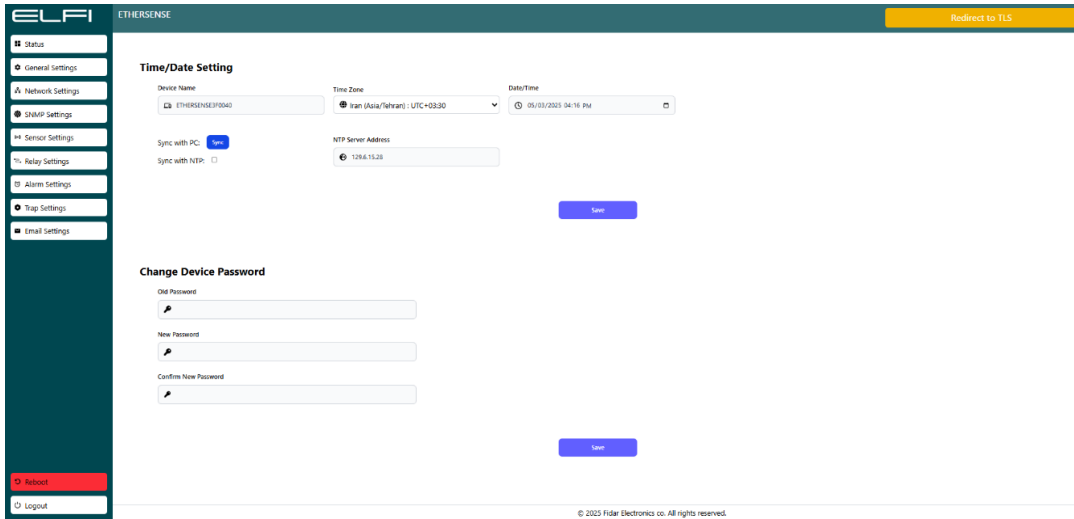


Figure 7: Sensor “General Settings” Menu

### 3.3. Network Settings Menu

This section helps configure the Sensor’s network connectivity. Depending on your network requirements, you can use either automatic configuration via DHCP or manual configuration (see Figure 8).

1. When DHCP is enabled, the Sensor automatically obtains required network information from the DHCP server. This includes the IP Address, Subnet, Gateway, DNS Server, and other relevant settings.
2. When DHCP is disabled, if you prefer to enter the settings manually, disable the DHCP option. Once disabled, the following fields will become available for manual configuration:
  - **IP Address:** The unique address of the Sensor on the network (e.g., 192.168.1.100)
  - **Subnet:** Defines the local network range (e.g., 255.255.255.0)
  - **Gateway:** The default gateway address for connecting to external networks (e.g., 192.168.1.1)
  - **DNS1 & DNS2:** Addresses of DNS servers used to resolve domain names to IP addresses
  - **HTTP Port:** Port used to access the Sensor's web interface via HTTP (Default: 80)

- **HTTPS Port:** Port used to access the Sensor's web interface via HTTPS (Default: 443)
- **Certificate:** A digital file that verifies the Sensor’s identity for secure HTTPS communication
- **Private Key:** A component of the certificate used to decrypt data in secure connections

After completing the settings, click Save, then click Reboot to apply the changes.

**Important Notes:**

**Note:** The Private Key must remain confidential and must not be shared.

**Note:** To enhance security, use HTTPS instead of HTTP.

**Note:** It is recommended to change default ports (e.g., 80 and 443) if possible.

**Note:** Store the Private Key in a secure location and prevent unauthorized access.

**Note:** Use encryption for the “Private Key” file.

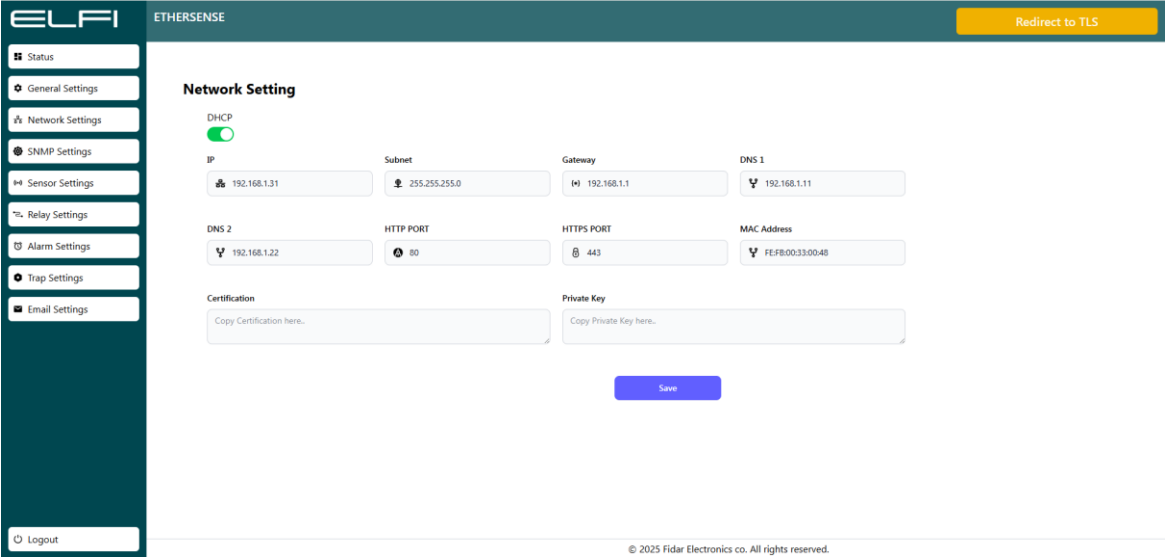


Figure 8: Sensor “Network Settings” Menu

### 3.4. SNMP Settings Menu

SNMP (Simple Network Management Protocol) enables communication between the network administrator and devices such as Sensors, switches, and routers. This section includes options for protocol version, Community settings, OIDs, and Traps (see Figure 9).

- **Current Version:** Indicates the SNMP version supported by the Sensor. Typically, versions 1 and 2 are supported.
- **Community:** Acts as a simple password controlling access to Sensor information.

**Default:** public, which allows general access to public Sensor data.

**Note:** Change the default public value to a secure and unique name.

**Note:** Avoid using easy-to-guess names like "public" or "private".

**Note:** In the SNMP OID and Trap OID sections, review available identifiers.

**Note:** Configure Trap OIDs based on your monitoring needs to avoid unnecessary notifications.

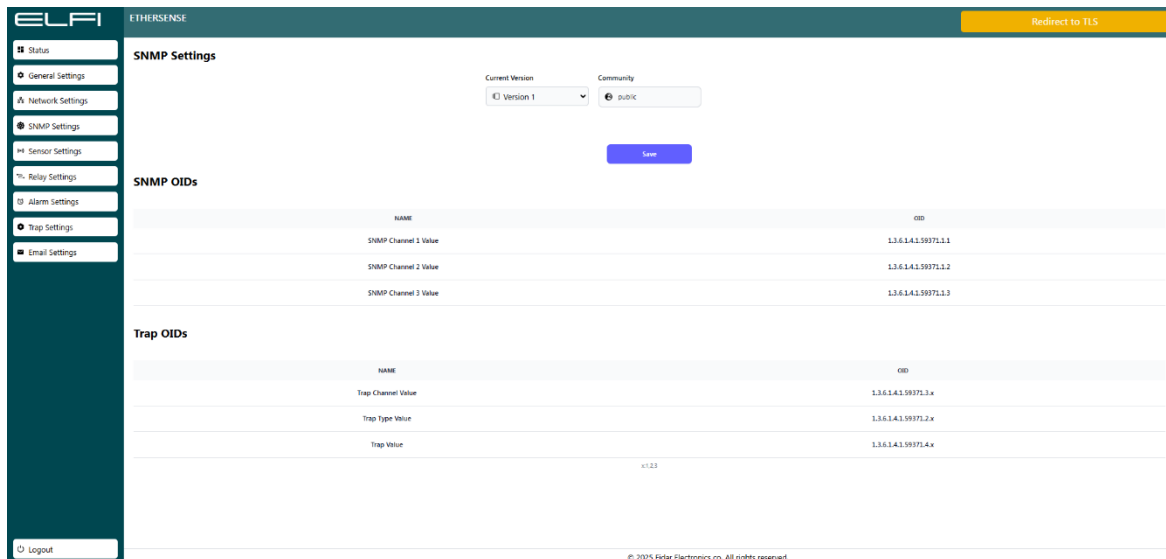


Figure 9: Sensor “SNMP Settings” Menu

### 3.5. Relay Settings Menu

---

Relay settings can be configured in two modes:

- **Time-Based Mode:** When this mode is enabled and a time value is set (e.g., 10 seconds), the relay will activate connected devices—such as sirens, cooling systems, etc.—for the specified time duration (10 seconds in this example) as soon as the relay is triggered, and will then automatically turn off.
- If Continuous mode is selected, once the relay is triggered, connected devices—such as alarms, cooling systems, etc.—will remain active until the Sensor exits the alarm state. Additionally, in Continuous mode, if the option “Reset relay status when alarm ends” is enabled, the relay will automatically return to its previous state when the alarm condition ends (e.g., the alarm will be turned off). (See Figure 10)

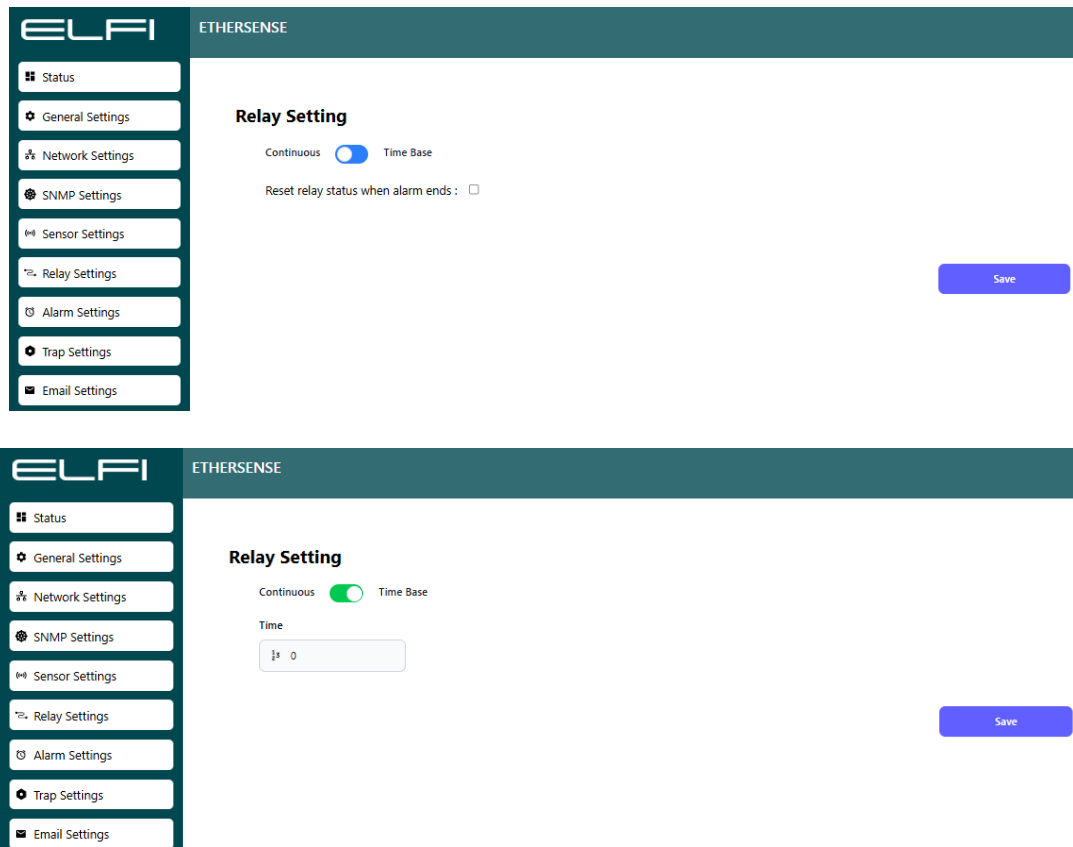


Figure 10: Sensor “Relay Settings” Menu

## 3.6. Alarm Settings Menu

---

The Sensor Alarm Settings page allows you to configure alarms for temperature and humidity monitoring independently. This feature helps you stay informed of environmental changes and take appropriate action in a timely manner. You can define separate thresholds for each parameter (temperature and humidity) for: **High Alarm, High Pre-Alarm, Low Alarm, Low Pre-Alarm** (See Figure 11).

### Types of Alarms

#### High Alarm

- Triggered when the temperature or humidity exceeds the defined high threshold.
- Suitable for warning users of critical increases in temperature or humidity.

#### High Pre-Alarm

- Activated when values approach the high threshold.
- Acts as an early warning before reaching critical levels.

#### Low Alarm

- Triggered when temperature or humidity falls below the defined low threshold.
- Useful for alerting users to critical drops in environmental conditions.

#### Low Pre-Alarm

- Activated when values approach the low threshold.
- Serves as an early alert to potential under-limit conditions.

#### Sensor Error Alarm

- Activated when the sensor is damaged or shows unusual values.

### How to Configure Alarms

For each channel, configure the following parameters:

- High Alarm: Critical upper limit for temperature or humidity.
- High Pre-Alarm: Near-critical upper limit.
- Low Alarm: Critical lower limit.
- Low Pre-Alarm: Near-critical lower limit.

## Possible problems and solutions:

- Alarm does not activate:
  - Check that the alarm values are entered correctly.
- Repeated alarms:
  - Recheck the pre-alarm and alarm ranges to avoid over-sensitivity.
- Sensor error:
  - Check the sensor connection.

These settings help you to closely monitor the system performance and react in time if problems occur.

### Alarm Notification Options

#### 1. Email Notification

- Once triggered, the Sensor can send an alarm email to predefined recipients.
- The email includes Sensor details and the type of alarm.
- Ensure that the SMTP settings are correctly configured in the Email Settings section.

#### 2. SNMP Trap

- The Sensor can send a trap to the network management server upon alarm activation.
- Suitable for centralized monitoring in managed network environments.
- Relevant SNMP and Trap OID settings must be properly configured.

#### 3. Relay Activation

- The Sensor can activate a relay in response to an alarm event.
- This may trigger a warning light, siren, or control an external device.
- Recommended for environments requiring immediate physical response.

### Selecting Alarm Notification Methods

In the Alarm Notification Method section, choose one or more of the following options:

- **Email:** Send an alarm notification via email.

- **SNMP Trap:** Send a trap to the network management server.
- **Relay Activation:** Trigger a relay to activate external hardware.

## **Saving Settings**

1. After configuring your thresholds, click **Save**, then select **Reboot** to apply the changes.
2. The Sensor will apply the new settings and will be ready to notify you when defined conditions are met.

## **Important Notes**

**Email Alerts:** Double-check recipient addresses and SMTP configurations.

**Fast Response Environments:** Use relay activation (e.g., for sirens or warning lights).

**Note:** To avoid false alarms, set Pre-Alarm thresholds slightly below or above the main alarm limits.

**Note:** For each channel, configure the temperature range based on the environmental conditions and the specifications of connected devices.

**Note:** Always test the alarm functionality after applying any changes to the settings.

## **Example Settings for One Channel**

**High Alarm:** 80°C

**High Pre-Alarm:** 65°C

**Low Alarm:** 10°C

**Low Pre-Alarm:** 15°C

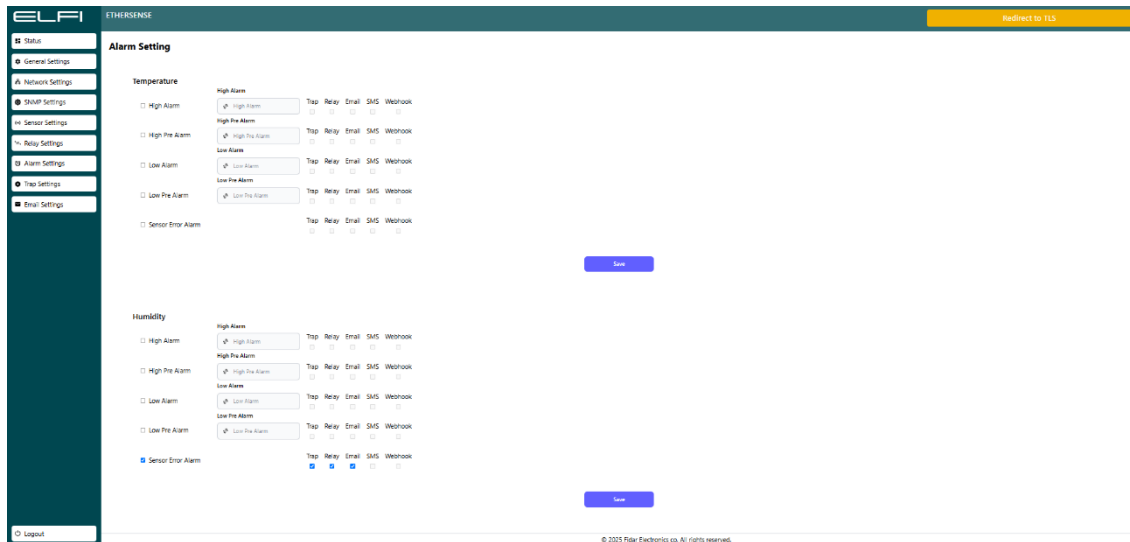


Figure 11: Sensor “Alarm Settings” Menu

### 3.7. Trap Settings Menu

A Trap is an asynchronous alert message sent by the Sensor to the SNMP server, providing information about specific events (such as alarms or status changes). These messages are automatically transmitted by the Sensor without any polling request from the server. (See Figure 12). To configure Trap Settings:

1. Go to the Trap Settings section.
2. Fill in the following fields:
  - 2.1. **Trap Destination IP:** The IP address of the network management server.
  - 2.2. **Trap Port:** The appropriate port number (default: 162).
  - 2.3. **Trap Community:** A community string used for SNMP access. (It is recommended to change the default value for improved security.)

Within the Trap Settings page, you will find the Send Delay Config option. This defines a delay before Trap messages are sent to the network management server. It is useful for optimizing network performance and reducing server load, especially in environments with frequent events.

#### Importance of Send Delay:

- **Network Traffic Management:** Prevents flooding the network with multiple Trap messages in a short time.
- **Reducing Server Load:** Allows the SNMP server enough time to process previous messages before receiving new ones.

- **Avoiding Redundant Alerts:** Temporary Sensor fluctuations won't immediately trigger a Trap, preventing unnecessary alerts.

### How Send Delay Config Works:

- Set Delay Time (in seconds):
- Default: 0 (no delay)
- Example: 10 means the Trap will be delayed for 10 seconds after the event occurs.
- Trap messages are only sent after the delay, even if multiple events happen.

### Using Delay in Repeated Traps:

- If several events occur within the delay period, only the latest status is sent.
- This helps reduce traffic and prevents repetitive messages.

**Note:** Choose a delay that does not risk missing critical events.

**Note:** For time-sensitive networks, set a very low or zero delay.

**Note:** After configuration, verify the Trap functionality to ensure messages are delivered properly.

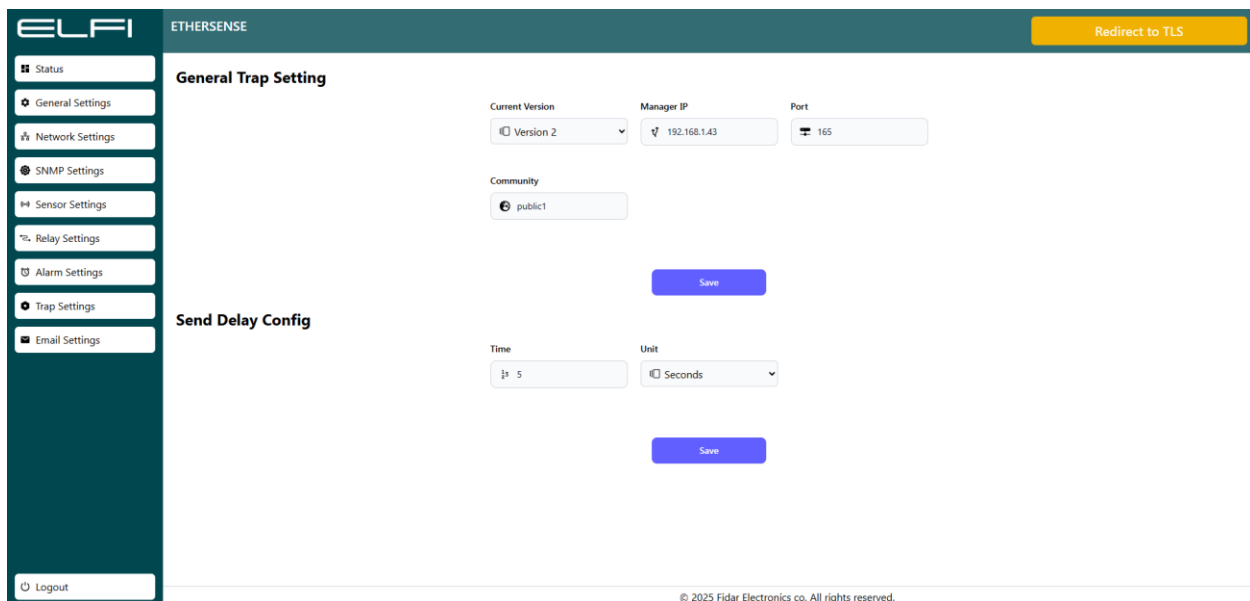


Figure 12: Sensor “Trap Settings” Menu

## 3.8. Email Settings Menu

---

This section allows you to configure settings for sending emails via the SMTP (Simple Mail Transfer Protocol). It is used for sending alerts, notifications, or reports to designated email addresses. (See Figure 13)

### Available Fields:

- **SMTP Sender Email Address:** The email address shown as the sender in the message. This must be valid and usually matches the credentials of the SMTP server. (Example: example@yourdomain.com)
- **SMTP Receiver Email Address:** The destination email address where alerts will be sent. (Example: example@yourdomain.com)
- **SMTP Server Address:** The address of the SMTP server used to send emails. (Depends on your email provider.)
- **Server IP:** If using a local SMTP server, enter its IP address here.
- **SMTP Port:** Port number used for communication with the SMTP server.  
Common values:
  - 25: No encryption (legacy, rarely used today)
  - 465: Secure connection using SSL/TLS
  - 587: Secure connection using STARTTLS
- **SMTP Username:** Username for authentication, typically the same as the sender's email address.
- **SMTP Password:** Password for the specified SMTP username (used for authentication).
- **Time:** Time interval (in seconds) for sending emails or scheduling automated messages.
- **Test Email Address:** An email address used for testing the configuration. Use the “Send Test Email” option to verify that the settings are correct.

After completing the configuration, click Save, then Reboot to ensure all settings are applied correctly.

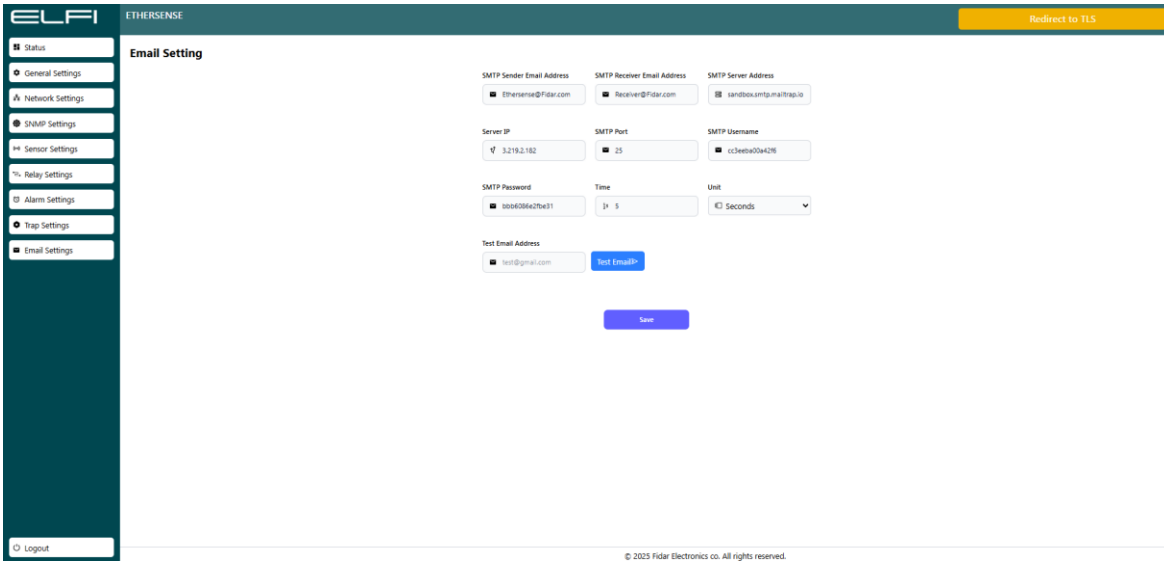
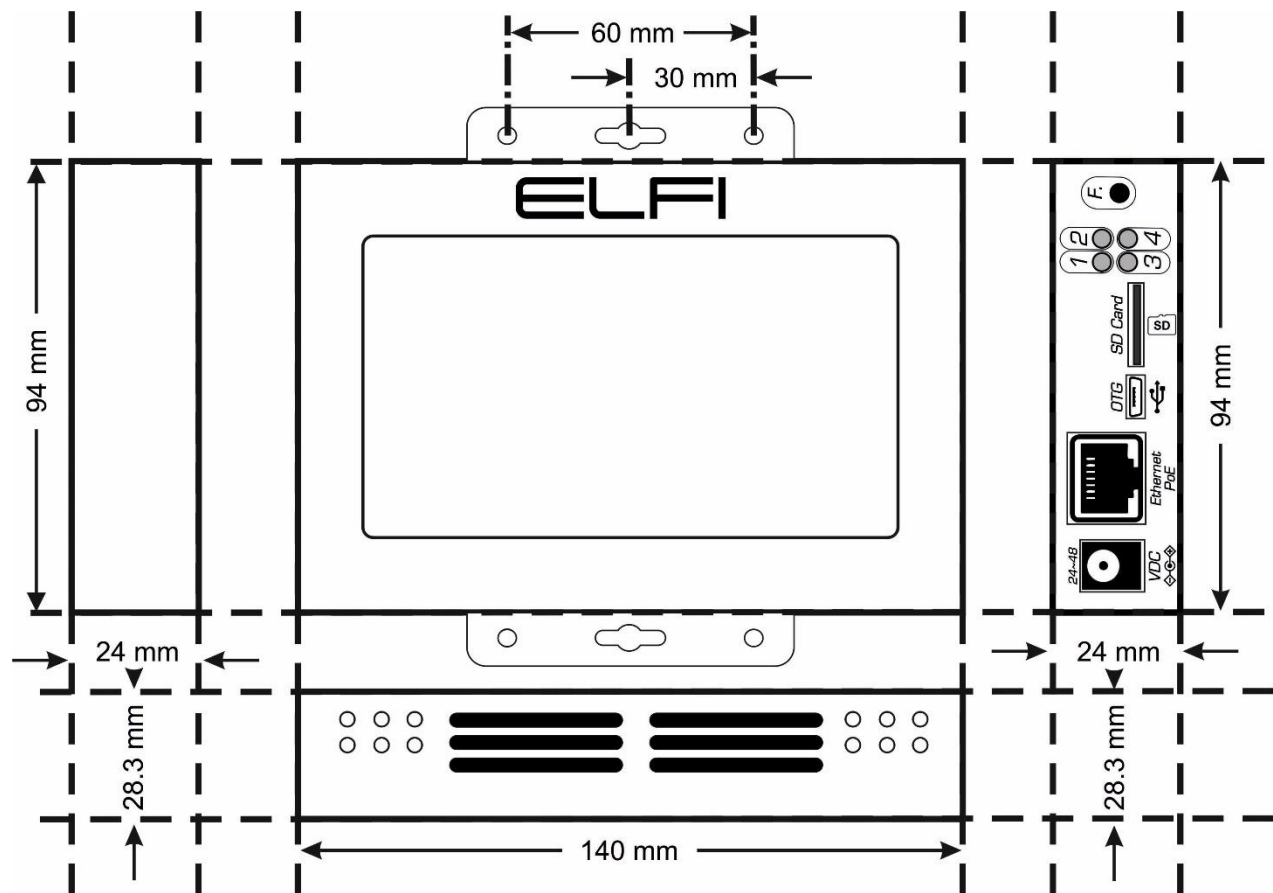


Figure 13: Sensor “Email Settings” Menu

## 4. Sensor Dimensions



## **Contact Info**

---

Behineh Farayand Electronic Fidar Company

Telephone: 021-91308515

Address: West Azerbaijan Province, Urmia, 10<sup>th</sup> KM Sero Road, Science and Technology Park

Email: [info@fidarelectronics.com](mailto:info@fidarelectronics.com)

Website: [www.fidarelectronics.com](http://www.fidarelectronics.com)