User Manual for Network Based Impact Detection Sensor Model FDS0202-21

Description – Initialization – Technical Information

Sensor Technical Information

General	
Model	FDS0202-21
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	Impact along horizontal or vertical axis
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 (i.e. detecting abrupt vibrations in the rack). Do not connect it to incompatible or unsupported 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 sensor.
- 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:

- Network Based Impact Detection Sensor, model FDS0202-21 [1]
- 48-volt adaptor [2]
- SD Card
- OTG cable
- User manual.

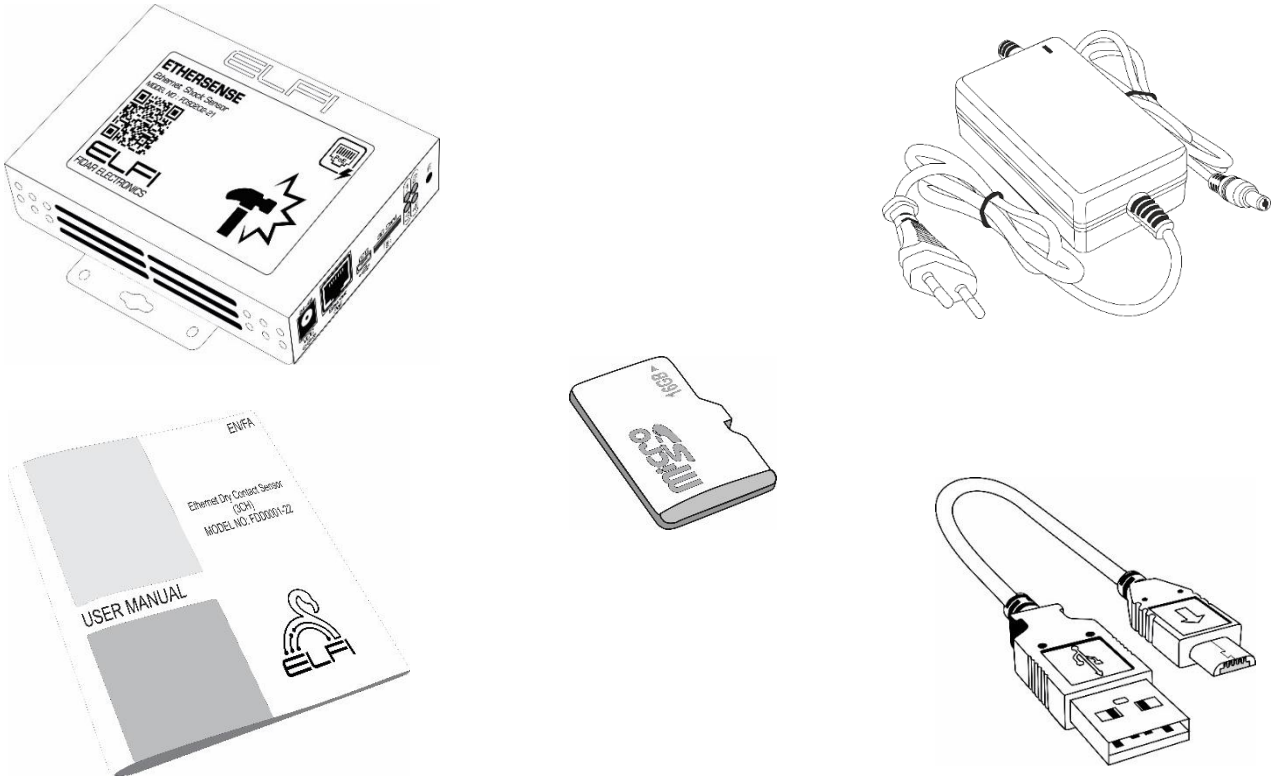


Figure 1: Contents of the box

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

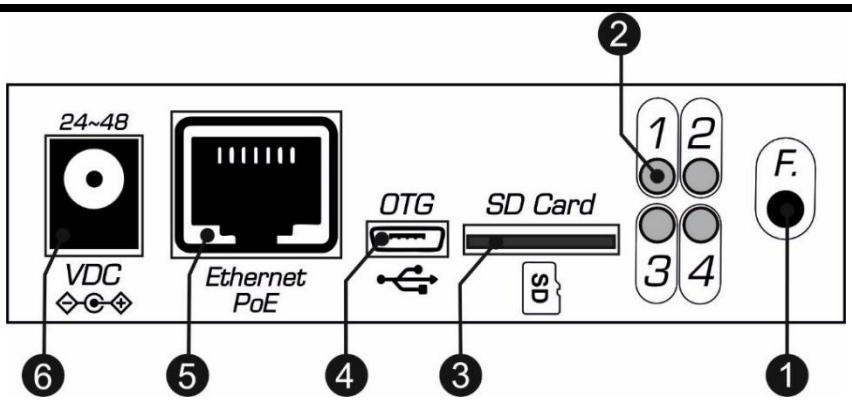


Figure 2: Side view of the sensor

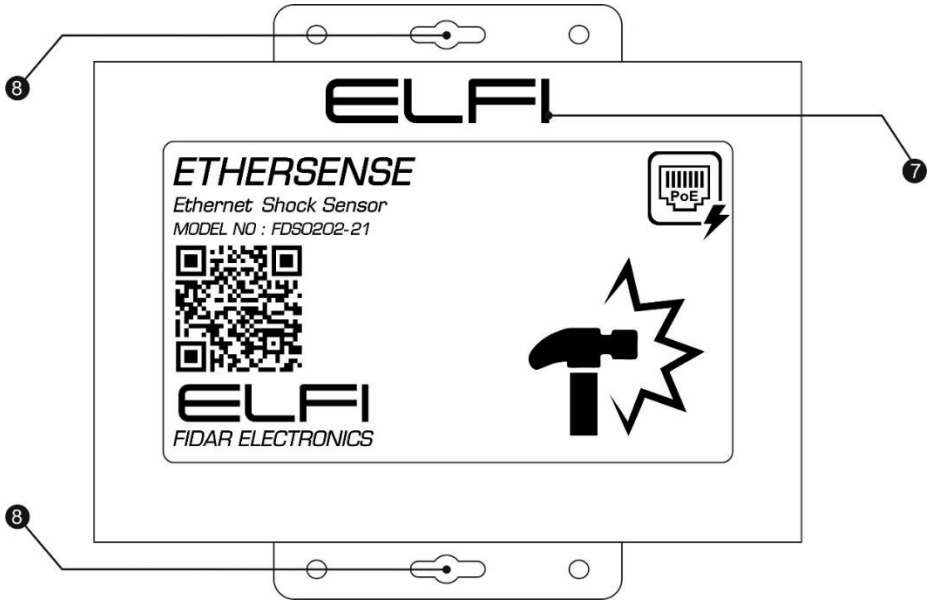


Figure 3: Front view of the sensor

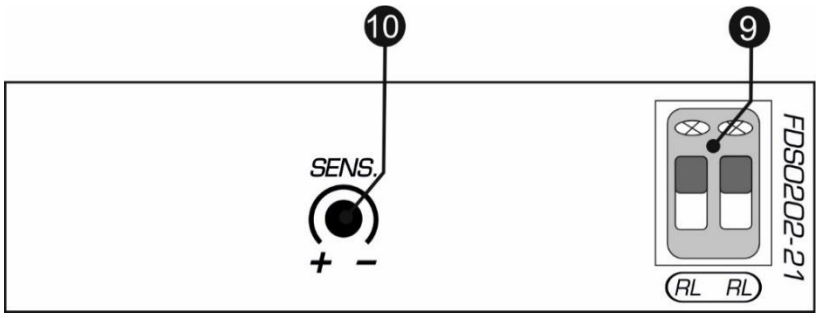


Figure 4: Side view of Sensor

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 ELFI symbol will be displayed in green.
8	Wall Mounting Location	
9	RL	To connect the sensor to alarm equipment (e.g. sirens, indicator lamps) or a cooling system
10	SENS	Configuration of Impact sensitivity level [1]

1. User-adjustable

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 [1] to access the sensor's web interface (see Figure 5).

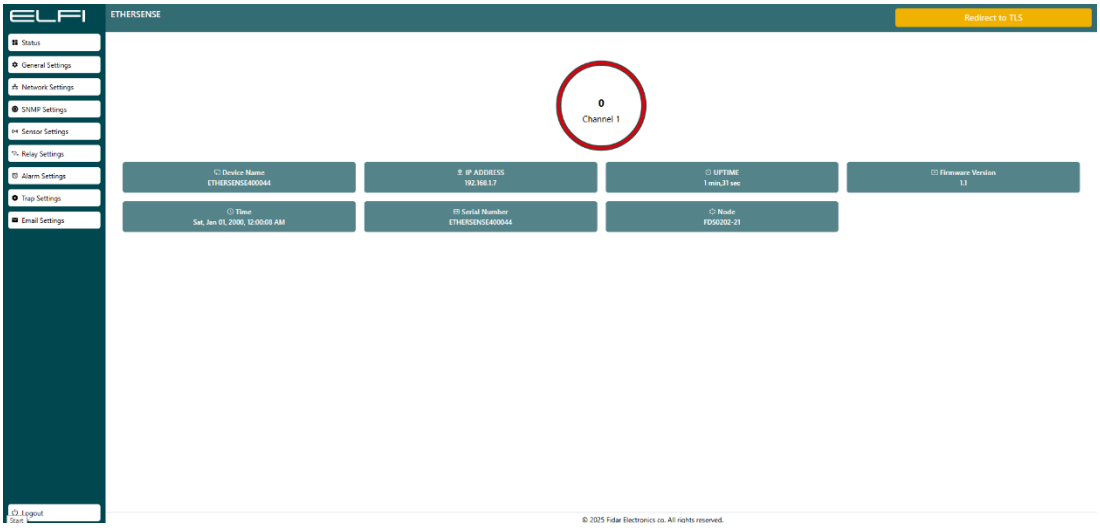


Figure 5: Sensor Web Page

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

3.1. Status Menu

The Status page is specifically designed to provide real-time monitoring of the Dry Contact Sensor's performance. This digital sensor operates in only two states: Active (1) and Inactive (0). This page can be used to observe critical events within the system (see Figure 6).

Sensor status display

The fry contact sensor functions as a digital device and, depending on the application, can be connected to various components:

- Active (1):
  - Sudden vibration applied to the rack or the servers themselves detected.
- Inactive (0):
  - No Impact detected

This page dynamically updates to reflect the sensor's status in real time, enabling quick identification of system events.

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 part number:** Corresponding to the Sensor hardware, identifying its technical specifications.

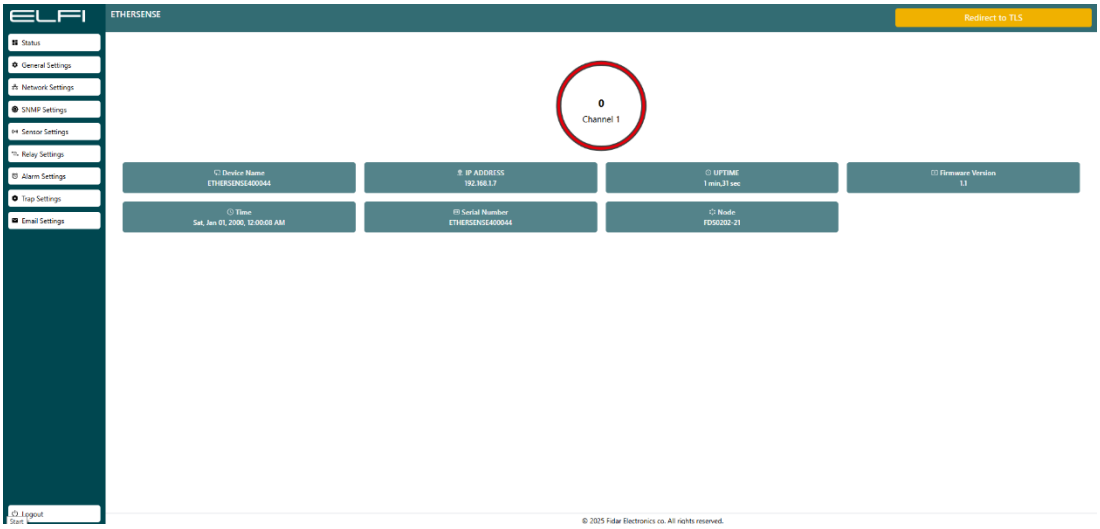


Figure 6: Sensor “Status” Menu

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.

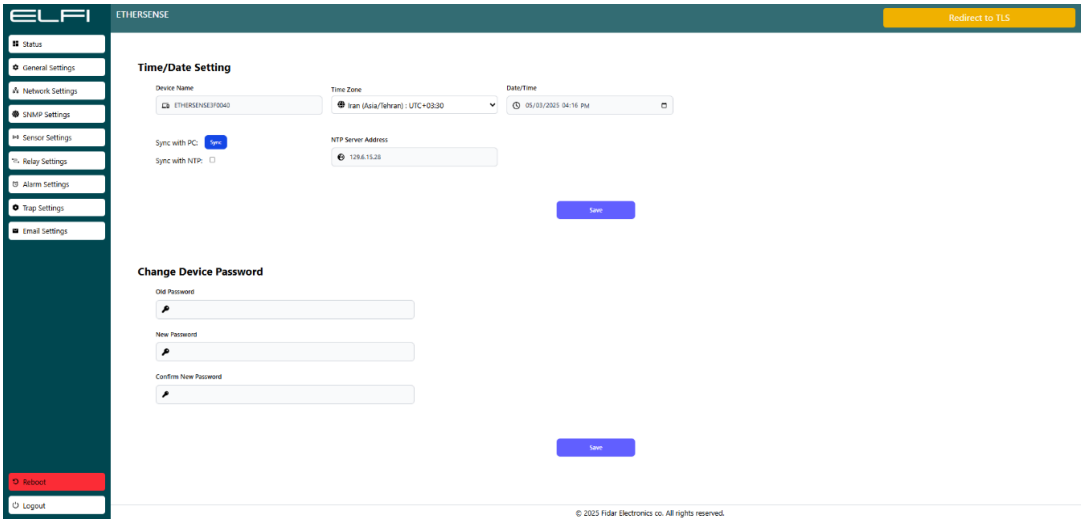


Figure 7: Sensor “General Settings” Menu

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.

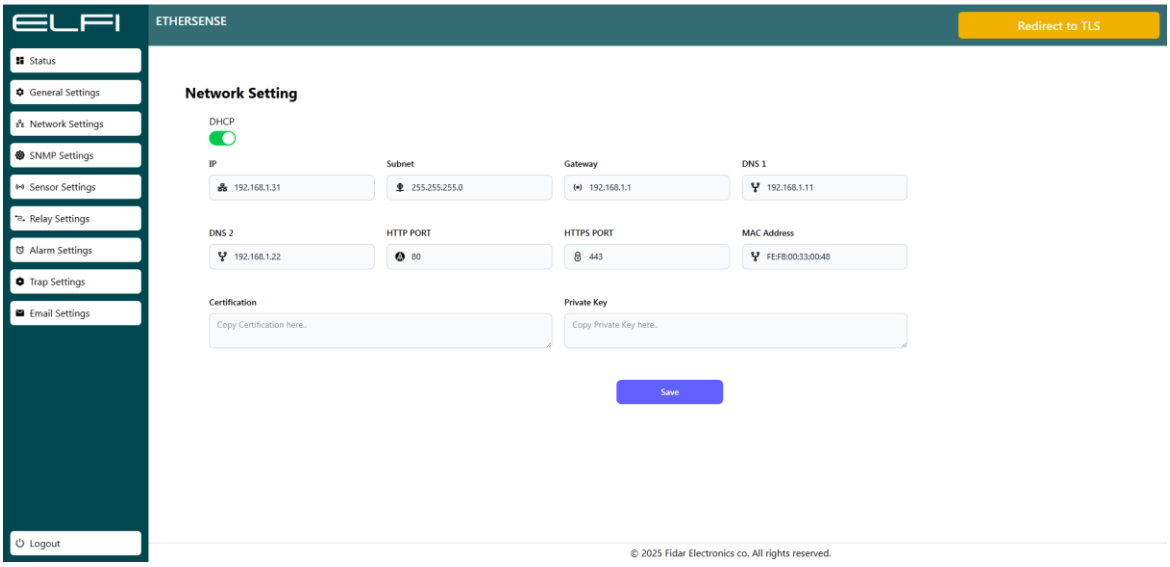


Figure 8: Sensor “Network Settings” Menu

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.

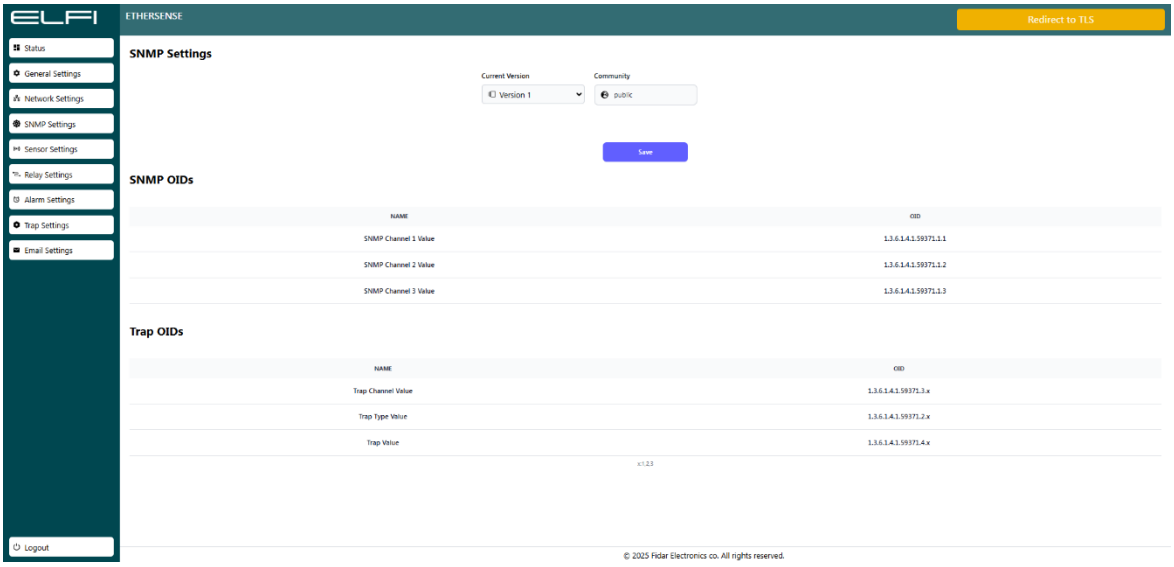


Figure 9: Sensor “SNMP Settings” Menu

3.5. Sensor Settings Menu

On the sensor settings page, there is an option called Reverse Mode, which allows you to invert the sensor's behavior. This mode is designed for special scenarios where you need to change the way the sensor interprets status signals (see Figure 10).

Reverse Mode Configuration

1. Normal Mode

In this default mode, the sensor interprets status signals as follows:

- **Active (1):** When the sensor detects an impact.
- **Inactive (0):** When the sensor detects no impact.

2. Reverse Mode

In this mode, the detection logic is inverted:

- **Active (1):** When the sensor detects no impact.
- **Inactive (0):** When the sensor detects an impact.

Use Cases for Reverse Mode

- **Integration with other sensors:**

Useful when connected systems interpret "active" and "inactive" states differently and require reverse logic.

- **Adaptation to specific environments:**

When the input signal of the sensor is defined in reverse due to environmental or system constraints.

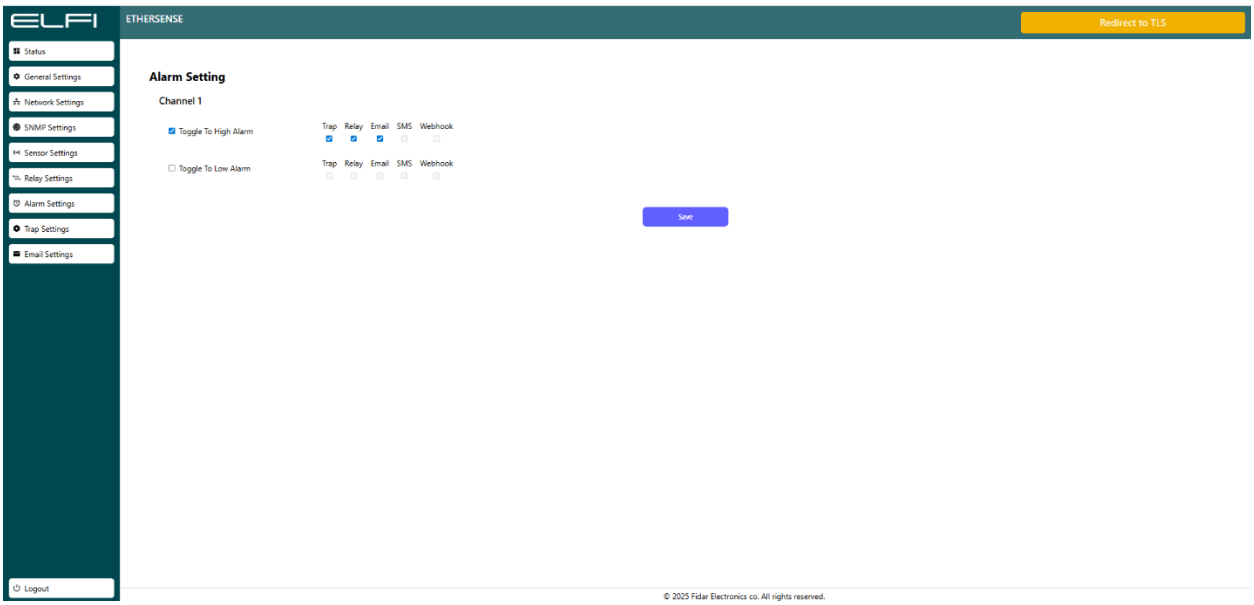


Figure 10: Sensor “Sensor Settings” Menu

3.6. 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 11)

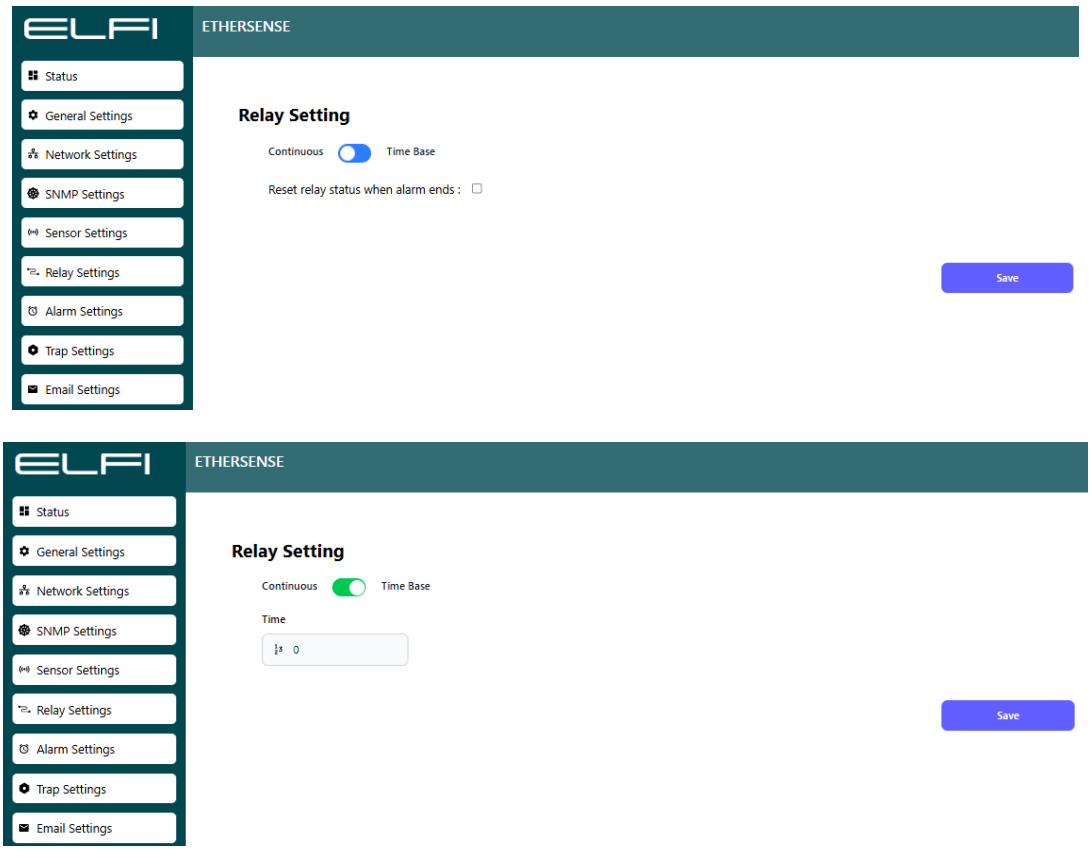


Figure 11: Sensor “Relay Settings” Menu

3.7. Alarm Settings Menu

The Sensor Alarm Settings page allows you to define how the sensor should behave when specific conditions are detected. These alarms can be used to monitor the system and notify users in case of critical changes or abnormal sensor status. (See Figure 12)

1. Toggle To High Alarm

- This alarm is triggered when the sensor’s value changes to 1.
- The sensor recognizes this transition and activates the alarm.
- Recommended for scenarios where it is important to be notified when the sensor becomes active (e.g., impact or vibration detection).

2. Toggle To Low Alarm

- This alarm is triggered when the sensor’s value changes to 0.
- The sensor detects this transition and activates the alarm.

- Suitable for situations where notification is required when the sensor becomes inactive (e.g., no vibration).

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.

How to Configure the Alarm

A) Select Alarm Trigger Mode

1. Go to the Alarm Settings page.
2. Choose one of the following modes:
   - **Toggle To High Alarm:** Alarm is triggered when the sensor switches to 1.
   - **Toggle To Low Alarm:** Alarm is triggered when the sensor switches to 0.

B) Selecting Alarm Notification Methods

1. 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.

C) 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).

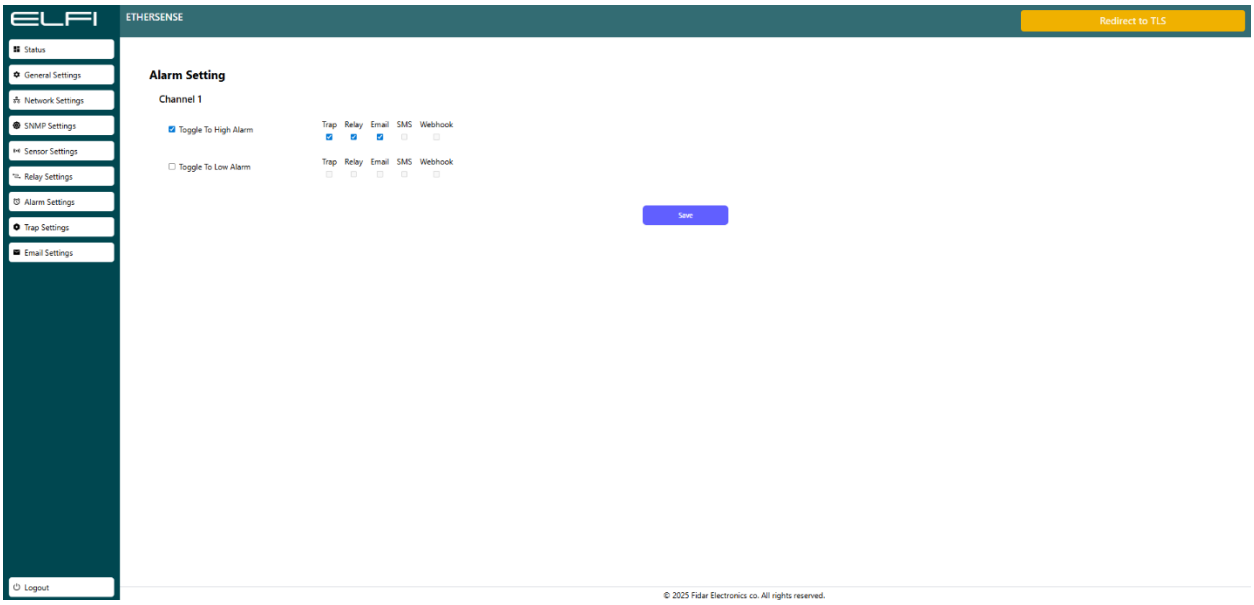


Figure 12: Sensor "Alarm Settings" Menu

3.8. 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 13). 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.

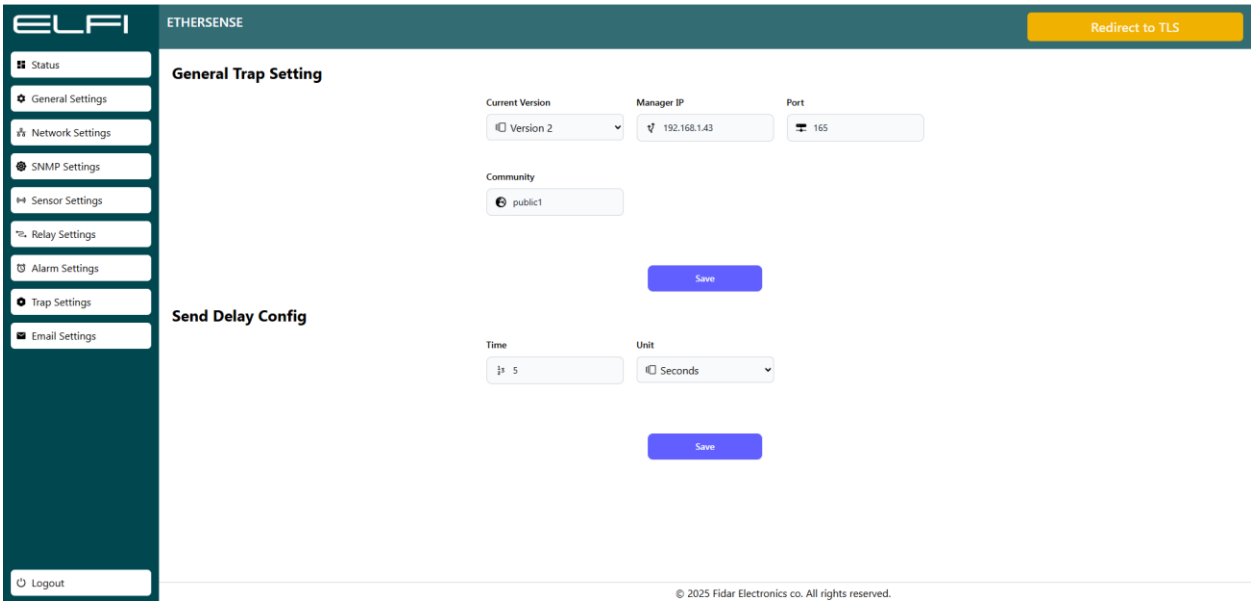


Figure 13: Sensor "Trap Settings" Menu

3.9. 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 14)

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.

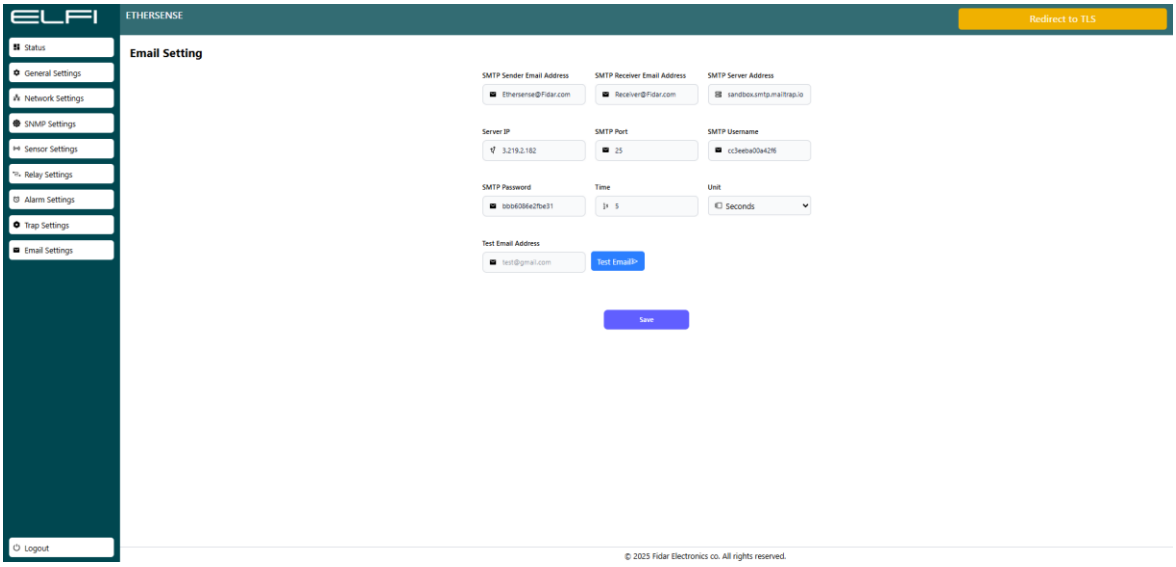
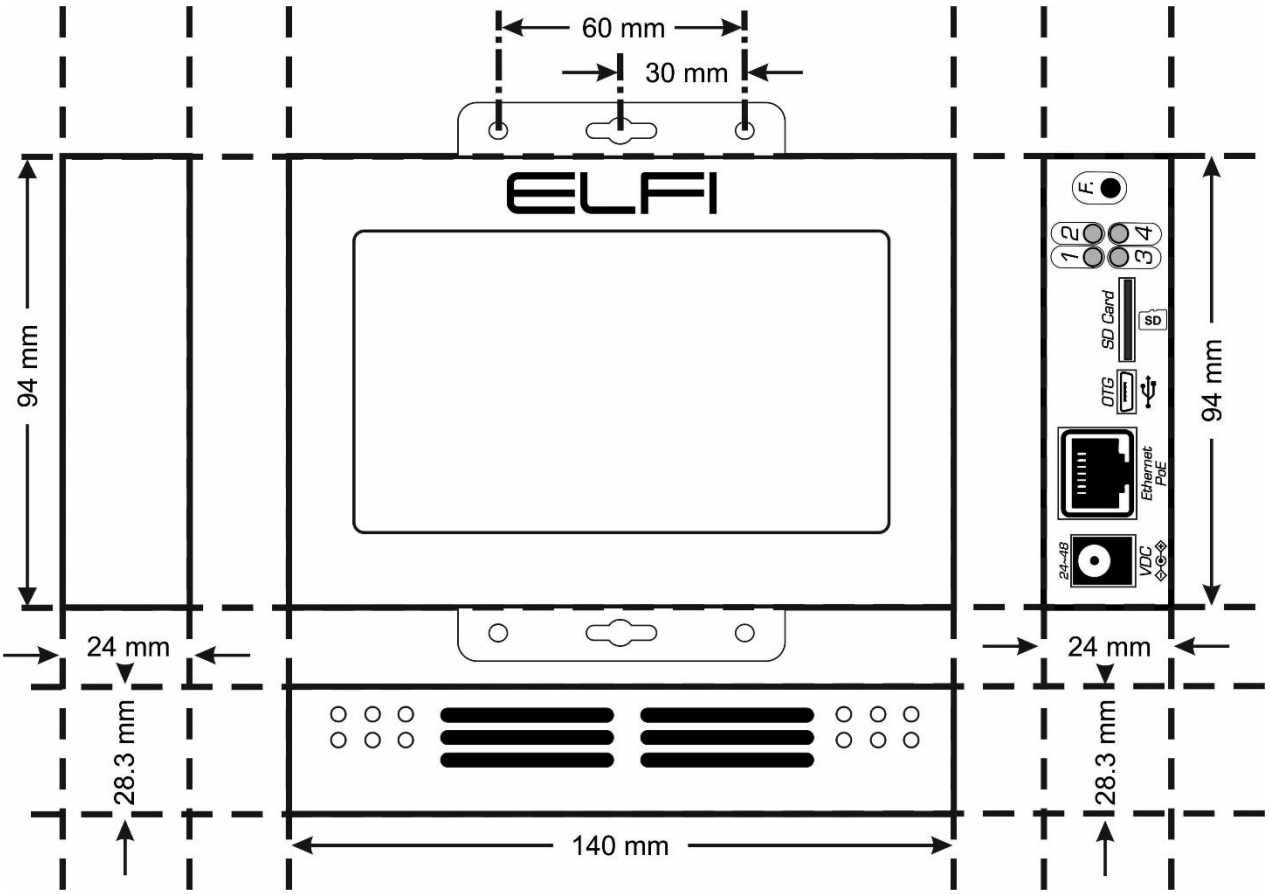


Figure 14: Sensor “Email Settings” Menu

4. Sensor Dimensions



Contact Info

Behineh Farayand Electronic Fidar Company

Telephone: 021-91308515

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

Email: info@fidarelectronics.com

Website: www.fidarelectronics.com