دفترچه راهنمای سنسور تشخیص ضربه تحت شبکه مدل FDS۰۲۰۲-۲۱

شرح ـ نصب و راه اندازی ـ اطلاعات فنی

مشخصات فنی سنسور

عمومی	
مدل	FDS۰۲۰۲-۲۱
ابعاد	طول × ارتفاع × عمق ۹/۴cm ×۲/۴cm ×۱۴cm
وزن	۵۰۰ گرم
دمای کاری	۱۰- تا ۸۰ درجه سانتی‌گراد
دمای نگه‌داری	۲۰- تا ۸۰ درجه سانتی‌گراد
رطوبت کاری	۰ تا ۶۰ درصد
ولتاژ کاری	۲۴ تا ۱۰۰ولت
گیره نگه‌داری	۲ سوراخ برای نصب دیوار
گارانتی	۲ سال
ورودی/ خروجی	
نوع ورودی	ضربه به صورت افقی یا عمودی به سنسور
خروجی	شبکه

ملاحظات امنیتی

(قبل از استفاده از این محصول، اقدامات احتیاطی را بخوانید)

لطفاً قبل از استفاده از محصول، این دفترچه راهنما را به دقت مطالعه کرده و به نکات ذکر شده توجه کامل داشته باشید تا محصول را به‌درستی استفاده کنید.

در این راهنما، اقدامات ایمنی در دو سطح طبقه‌بندی‌شده است: ⚠ هشدار" و⚠ احتیاط"

⚠ **هشدار**	یعنی برخورد نادرست ممکن است به شرایط خطرناک منجر شود و موجب مرگ یا صدمات جدی شود.

⚠ **احتیاط**	یعنی برخورد نامناسب ممکن است به شرایط خطرناک منجر شود و موجب آسیب کم یا متوسط به اشخاص یا آسیب به اموال شود.

اقدامات ایمنی هر دو سطح را رعایت کنید زیرا برای ایمنی شخصی و سیستم بسیار مهم هستند.

اطمینان حاصل کنید که کاربران این راهنما را مطالعه کرده و سپس آن را در مکانی امن برای مراجعات بعدی نگهداری کنید.

(اقدامات احتیاطی در طراحی)

⚠ هشدار

- توجه به جزئیات کابل‌کشی و اتصال مناسب، یکی از مهم‌ترین بخش‌های نصب دستگاه‌هاست که تأثیر مستقیم بر عملکرد و کارایی شبکه دارد.

- لزوماً همیشه از یک استاندارد ثابت (T568A یا T568B) در هر دو انتهای کابل استفاده کنید تا از بروز مشکلات اتصال جلوگیری شود.

- اشتباه در چیدن سیم‌ها هنگام نصب سوکت، می‌تواند منجر به آسیب سخت‌افزاری محصول یا عملکرد نادرست شبکه شود.

- بعد از نصب سوکت‌ها، کابل را به سنسور تشخیص ضربه متصل کنید. در صورت شناسایی نشدن سنسور یا عدم عملکرد صحیح، موارد زیر را بررسی کنید:
  - اتصال کامل سوکت به کابل
  - صحت چیدمان سیم‌ها
  - استفاده از تستر شبکه برای شناسایی خطاهای احتمالی در کابل‌کشی
  - در صورت اطمینان از موارد فوق، محصول مربوطه را توسط یک عدد کابل شبکه‌ی سالم، تست کنید تا از عملکرد صحیح محصول مطمئن شوید.
- هنگام کار با کابل‌ها، از خم کردن بیش از حد یا کشیدن ناگهانی کابل خودداری کنید؛ زیرا این کار می‌تواند به سیم‌های داخلی آسیب بزند و کیفیت سیگنال را کاهش دهد.

⚠ حتیاط

- کابلRJ45 را با مدار اصلی و کابل‌های تغذیه دسته‌بندی نکنید و آن‌ها را نزدیک به یکدیگر نصب نکنید. فاصله‌ای حداقل ۱۰۰ میلی‌متر (۳.۹۴ اینچ) بین آن‌ها حفظ کنید. عدم رعایت این فاصله ممکن است منجر به ایجاد اختلال به علت نویز شود.

(اقدامات احتیاطی نصب)

⚠ شدار

- قبل از نصب سنسور تشخیص ضربه، حتماً از کیفیت کابل استفاده شده اطمینان حاصل کنید. کابل توصیه شده توسط سازنده، نوع RJ45 با CAT6 می باشد. عدم انجام این کار ممکن است باعث آسیب به محصول شود.
- به منظور حفظ کیفیت سیگنال ارتباطی، اتصال شیلد کابل RJ45 به سوکت‌های شیلددار الزامی است.
- از نصب سنسور تشخیص ضربه در محیط‌هایی با رطوبت یا دمای بسیار بالا یا پایین که خارج از محدوده کاری آن است خودداری کنید. این شرایط ممکن است باعث عملکرد نادرست محصول شود.
- از سنسور تشخیص ضربه تنها برای اهداف مشخص‌شده (ایجاد لرزش‌های ناگهانی در رک) استفاده کنید و از اتصال آن به دستگاه‌های ناسازگار خودداری نمایید.

⚠ احتیاط

● از سنسور تشخیص ضربه در محیطی استفاده کنید که مطابق با مشخصات عمومی موجود در این دفترچه باشد. استفاده از این محصول در هر محیط عملیاتی دیگری ممکن است منجر به شوک الکتریکی، آتش‌سوزی، نقص عملکرد یا آسیب و کاهش کیفیت ماژول شود.

● به هیچ وجه قسمت رسانا یا قطعه الکترونیکی سنسور تشخیص ضربه را مستقیماً لمس نکنید. انجام این کار ممکن است منجر به نقص عملکرد یا خرابی سنسور شود.

● در صورت نصب سنسور تشخیص ضربه به دیوار، پیچ‌های دیواری را با دقت محکم کنید. زیرا اگر پیچ‌ها شل باشند، ممکن است باعث سقوط سنسور شده و اتصال کوتاه اتفاق بیفتد.

● از ورود مواد خارجی مانند گردوغبار یا خرده‌های سیم به داخل سنسور ضربه جلوگیری کنید. این مواد خارجی ممکن است منجر به آتش‌سوزی، خرابی یا نقص عملکرد شوند.

(اقدامات احتیاطی سیم کشی)

⚠ هشدار

● قبل از سیم‌کشی، حتماً از سلامت و کیفیت تمامی کابل‌های ورودی و خروجی اطمینان حاصل کنید. عدم انجام این کار ممکن است باعث آسیب به محصول شود.

⚠ احتیاط

● قبل از اتصال کابل RJ45 اطمینان حاصل کنید که نوع رابطی که قرار است متصل شود، صحیح باشد. زیرا اتصال یک رابط نادرست یا سیم‌کشی اشتباه باعث خرابی سنسور می‌شود.

● در صورت نصب سنسور تشخیص ضربه به دیوار، گیره‌های نگه‌دارنده‌ی سنسور را توسط پیچ با دقت محکم کنید. زیرا اگر پیچ‌ها شل باشند، ممکن است باعث سقوط محصول شده و اتصال کوتاه اتفاق بیفتد.

● کابل RJ45 را به طور ایمن به سنسور تشخیص ضربه وصل کنید. عدم انجام این کار ممکن است باعث خرابی کابل‌ها شود و سنسور به درستی کار نکند.

● اطمینان حاصل کنید کابل‌های داده‌ی ورودی که به سنسور تشخیص ضربه متصل می‌شوند، در یک کانال قرار داده شده یا با استفاده از یک بست محکم شوند. اگر کابل‌ها در یک کانال قرار نگیرند یا با یک بست محکم نشوند، ممکن است به طور ناخواسته کشیده شوند. این کار به محصول و کابل‌ها آسیب می‌رساند یا باعث خطا در عملکرد ماژول به دلیل اتصالات نادرست کابل‌ها می‌شود.

● هنگام جدا کردن کابل RJ45 از سنسور تشخیص ضربه، آن‌ها را محکم نکشید. کشیدن کابل متصل به سنسور ممکن است باعث خطا در عملکرد محصول یا آسیب به آن یا کابل شود.

(اقدامات احتیاطی راه اندازی و نگهداری)

⚠ هشدار

● در هنگام فعال‌سازی سنسور تشخیص ضربه، قسمت رسانا یا الکترونیکی آن را لمس نکنید. انجام این کار ممکن است باعث شوک الکتریکی یا خرابی محصول شود.

⚠ احتیاط

● نصب و راه‌اندازی سنسور تشخیص ضربه باید توسط نیروهای تعمیرات مجرب با دانش مربوط به حفاظت در برابر شوک الکتریکی انجام شود.

● از Reset کردن سنسور تشخیص ضربه در مواقع غیرضروری، خودداری کنید. در صورت Reset کردن، تمامی تغییرات اعمال‌شده در صفحه‌ی وب سنسور، به تنظیمات کارخانه برمی‌گردد.

(اقدامات احتیاطی عملیاتی)

⚠ هشدار

● در حالی که سنسور تشخیص ضربه در حال ارسال داده است، هیچ قسمت رسانا، یا هیچ قطعه الکترونیکی از آن را به طور مستقیم لمس نکنید. انجام این کار ممکن است باعث نقص یا خرابی محصول شود.

⚠ احتیاط

● از هر دستگاه ارتباطی رادیویی مانند تلفن همراه در فاصله بیش از ۲۵ سانتی‌متر به ازای همه جهت از سنسور تشخیص ضربه استفاده کنید. انجام این کار ممکن است باعث ایجاد نویز شود.

(اقدامات احتیاطی دفع زباله)

⚠ احتیاط

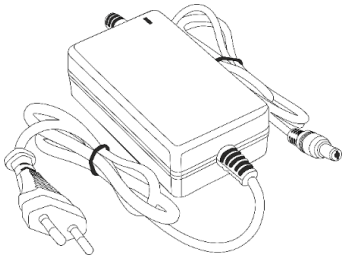
● سنسور تشخیص ضربه را به عنوان یک پسماند صنعتی دور بریزید.

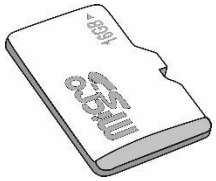
● هنگام دور انداختن سنسور، آن را بر اساس مقررات محلی از سایر پسماندها جدا کنید و به طور صحیح در مرکز جمع‌آوری/بازیافت پسماندهای محلی دور بریزید.

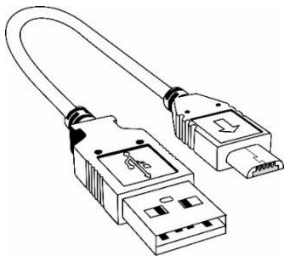
محتویات داخل جعبه

درون جعبه را از نظر کامل بودن طبق لیست بسته بندی بررسی کنید. موارد زیر باید گنجانده شود.

- سنسور تشخیص ضربه تحت شبکه مدل FDS۰۲۰۲-۲۱ [۱]
- آداپتور ۴۸ ولت [۲]
- کارت حافظه
- کابل OTG
- دفترچه راهنما







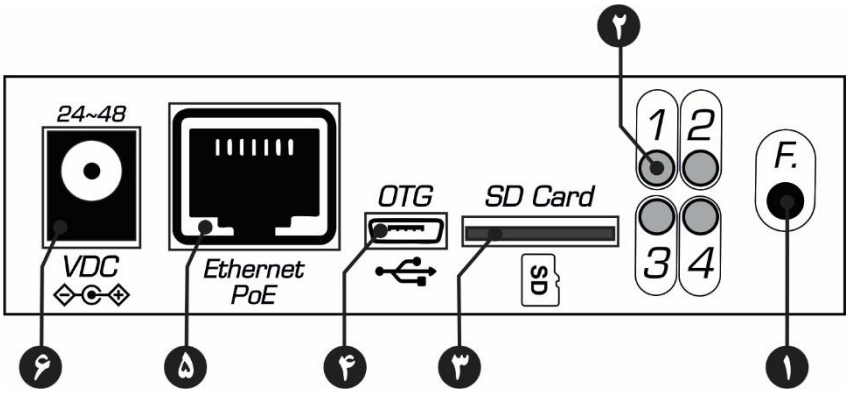
شکل ۱: محتویات داخل جعبه

[۱] اطلاعات دقیق در مورد ابعاد محصول در صفحه ۲۸ این دفترچه ارائه شده است.

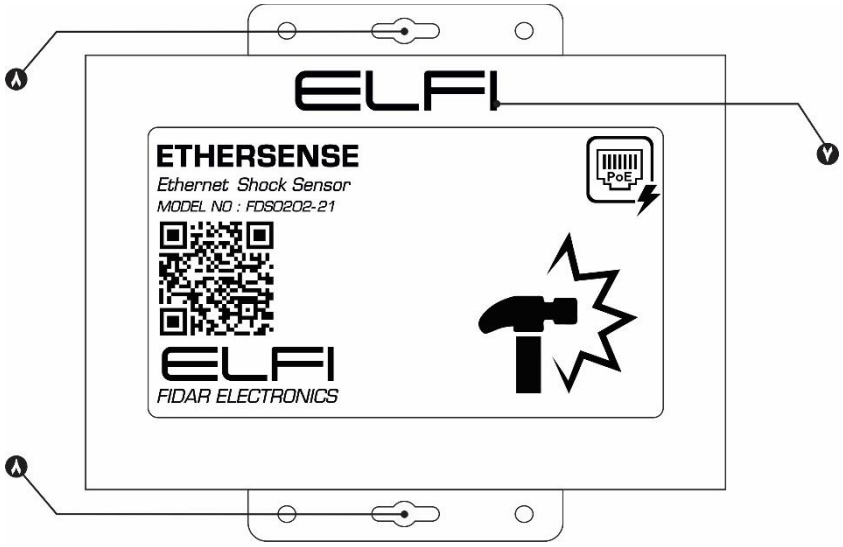
[۲] در صورت سفارش مشتری

فهرست

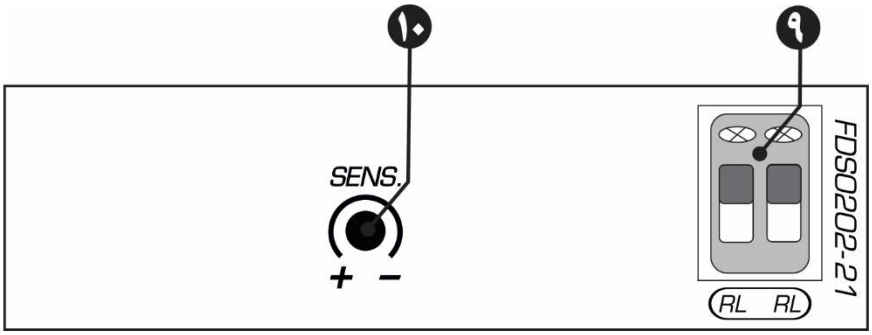
۱- نصب و راه‌اندازی سنسور



شکل ۲: نمای جانبی سنسور تشخیص ضربه



شکل ۳: نمای روبه‌روی سنسور تشخیص ضربه



شکل ۴: نمای جانبی سنسور تشخیص ضربه

جدول ۱: اطلاعات مربوط به رویه‌ی سنسور

شماره	نام	توضیح
۱	کلید F	برای Reset[1] کردن سنسور
۲	چراغ POWER	اتصال سنسور به برق را نشان می‌دهد.
۳	SD Card	ورودی کارت حافظه
۴	OTG	ورودی کابل OTG
۵	Ethernet PoE	ورودی کابل اترنت
۶	VDC	ورودی آداپتور
۷	نمایشگر اتصال پاور سنسور	در صورت متصل بودن پاور سنسور ،نماد ELFI به رنگ سبز نمایش داده می‌شود.
۸	محل نصب سنسور به دیوار	———
۹	RL	برای اتصال سنسور به تجهیزات هشدار (آژیر، لامپ) یا سیستم خنک‌کننده.
۱۰	SENS	تنظیم میزان حساسیت سنسور به ضربه[2]

[1] بازگشت به تنظیمات کارخانه

[2] توسط کاربر قابل تنظیم می‌باشد.

۲- اتصال سنسور به شبکه

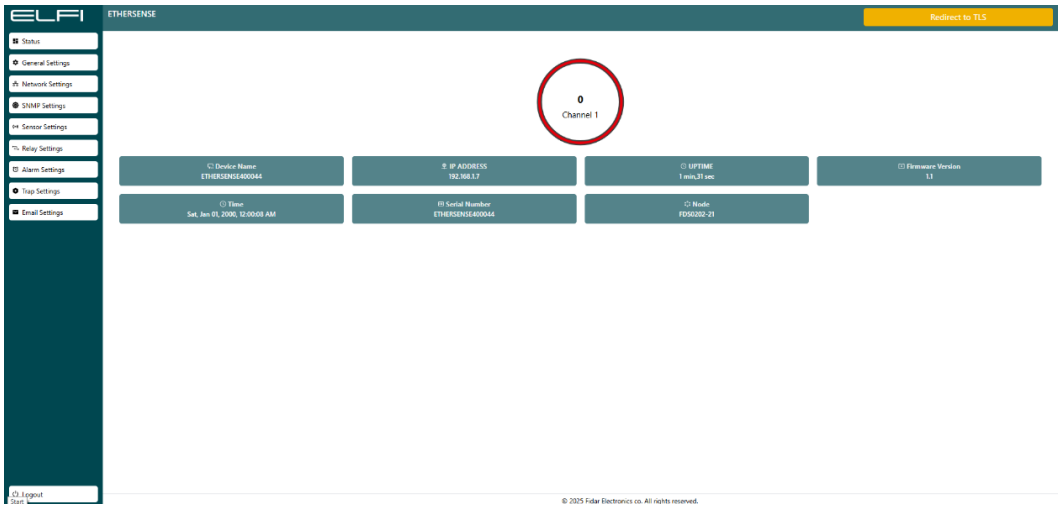
برای راه‌اندازی سنسور تشخیص ضربه، اگر از سوییچ POE استفاده می‌کنید فقط کافیست سنسور را با استفاده از یک کابل به سوییچ متصل کنید. در غیراین صورت از یک آداپتور ۴۸ ولتی برای راه‌اندازی آن استفاده کنید و سپس با استفاده از یک کابل شبکه، سنسور را به شبکه‌ی خود متصل نمایید.

توجه: به این نکته توجه داشته باشید که به هیچ عنوان از آداپتور و کابل شبکه به طور همزمان برای راه‌اندازی محصول استفاده نکنید.

توجه: در صورت Offline بودن سنسور تشخیص ضربه، ابتدا اتصال کابل شبکه یا RJ45 را تست کنید و در صورت اطمینان از صحت اتصال کابل، سنسور را Reset کنید. برای این منظور، کابل شبکه یا RJ45 را از محصول خارج کنید. کلید F را فشار داده و نگه‌دارید سپس کابل شبکه را وصل کرده و کلید F را تا زمان روشن شدن چراغ ELFI نگه دارید و سپس رها کنید.

۳- تنظیمات مربوط به نرم‌افزار سنسور

برای مشاهده رابط کاربری سنسور تشخیص ضربه، پس از روشن نمودن آن، IP (192.168.1.7) را با استفاده از یک مرورگر در یکی از رایانه‌های موجود در شبکه، وارد کنید. نام کاربری و رمز عبور را وارد کنید[۱] تا صفحه‌ی وب مربوط به محصول، نمایش داده شود (شکل ۵).



شکل ۵: صفحه وب مربوط به سنسور تشخیص ضربه

[۱] نام کاربری و رمز عبور اولیه مربوط به این محصول، هر دو admin می‌باشد.

۱-۳- منوی Status

صفحه وضعیت (Status) به طور خاص برای نمایش لحظه‌ای عملکرد سنسور تشخیص ضربه طراحی شده است. این سنسور دیجیتال تنها دو حالت دارد: فعال (۱) و غیرفعال (۰). از این صفحه می‌توان برای نظارت بر رویدادهای مهم و حیاتی در سیستم استفاده کرد (شکل ۶).

نمایش وضعیت سنسور

سنسور تشخیص ضربه به صورت یک ابزار دیجیتال عمل می‌کند که بسته به کاربرد می‌تواند به موارد زیر متصل باشد:

- فعال (۱):
  - شناسایی لرزش ناگهانی به رک یا خود سرورها
- **غیرفعال (۰):**
  - عدم تشخیص ضربه

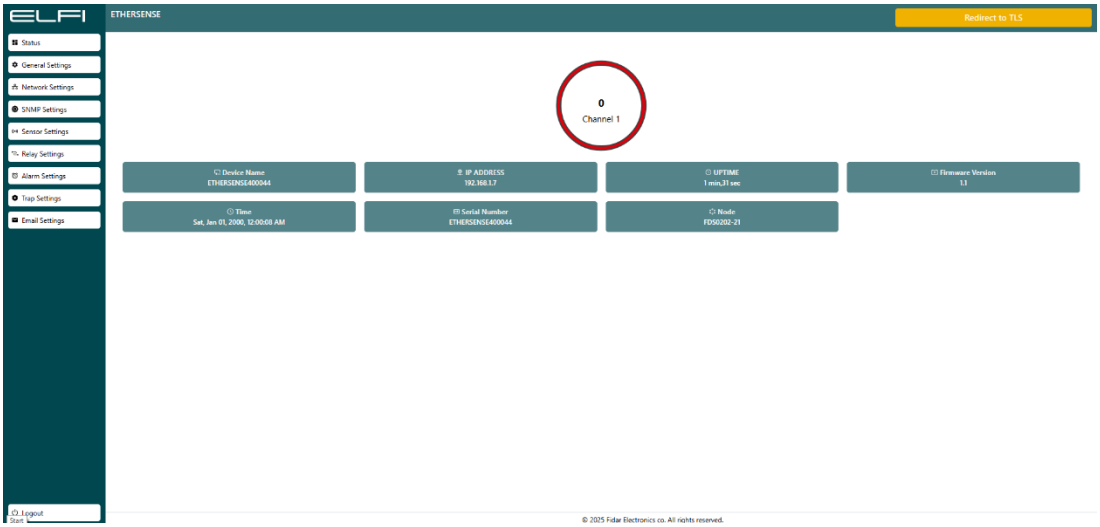
این صفحه به صورت زنده تغییرات وضعیت سنسور را نمایش می‌دهد و امکان تشخیص سریع رویدادها را فراهم می‌کند.

اطلاعات محصول

این بخش شامل جزئیات فنی سنسور است که به شرح زیر می‌باشد:

- نام محصول (Device Name): نام اختصاص داده‌شده به محصول برای شناسایی آسان در شبکه یا محیط کار.
- آدرس IP (IP Address): آدرس شبکه‌ای که سنسور از طریق آن به شبکه متصل است.
- مدت زمان روشن بودن سنسور تشخیص ضربه (Uptime): مدت زمانی که سنسور بدون وقفه کار کرده است. این مقدار از زمان آخرین روشن یا شروع مجدد سنسور محاسبه می‌شود.
- نسخه نرم‌افزار (Firmware Version): نسخه فعلی نرم‌افزار محصول که نشان‌دهنده قابلیت‌ها و به‌روزرسانی‌های آن است.

- زمان (Time): زمان و تاریخ فعلی تنظیم‌شده بر روی سنسور تشخیص ضربه. این اطلاعات برای بررسی همگام‌سازی زمانی و ثبت رخدادها اهمیت دارد.
- شماره سریال محصول (Serial Number): شماره یکتای محصول که برای ردیابی و مستندسازی استفاده می‌شود.
- پارت نامبر محصول: شماره قطعه مربوط به سنسور متصل به محصول که مشخصات فنی آن را تعیین می‌کند.



شکل ۶: منوی Status سنسور تشخیص ضربه

۳-۲- منوی General Settings

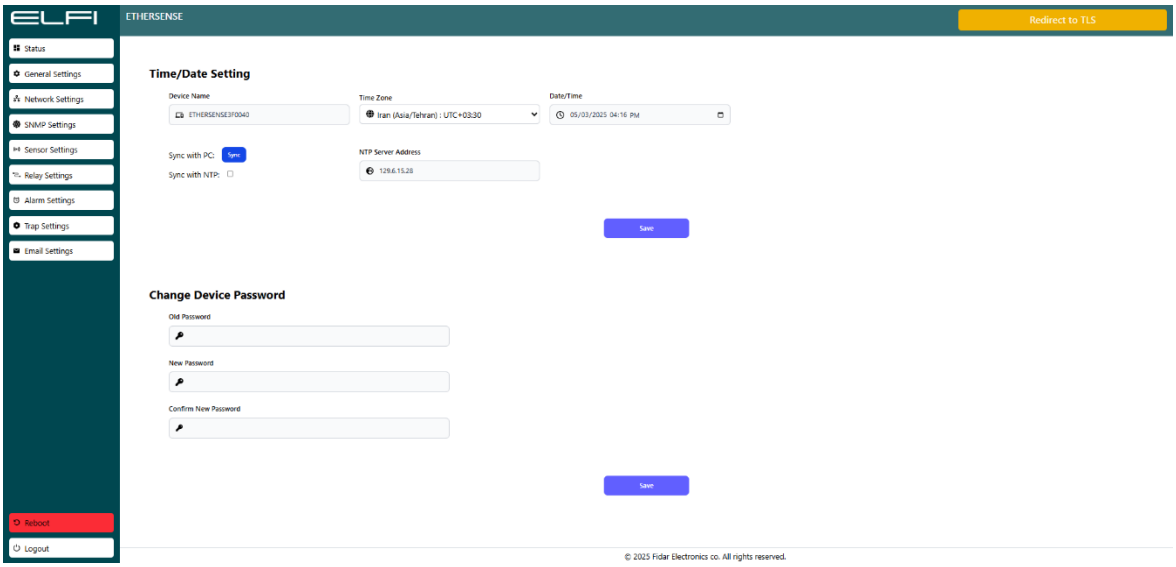
تنظیمات مربوط به زمان و همچنین تغییر رمز عبور در منوی General Settings، قابل انجام است (شکل ۷).

■ برای تنظیمات زمان، با انتخاب گزینه‌ی NTP، تنظیمات ساعت سنسور، به صورت خودکار و از طریق سرورهای ساعت اینترنتی صورت می‌گیرد. با غیرفعال کردن آن به صورت دستی می‌توانید تنظیمات روز و ساعت را به صورت دستی انجام دهید و یا می‌توانید با تنظیمات کامپیوتر خود هماهنگ کنید.

■ برای حفظ امنیت بیشتر، رمز عبور سنسور را تغییر دهید.

توجه: Device Name به صورت پیش‌فرض شماره سریال سنسور می‌باشد. پیشنهاد می‌شود بعد از راه‌اندازی محصول، نام آن را به صورت دلخواه تغییر دهید.

توجه: پس از اعمال تغییرات، ابتدا گزینه‌ی Save را انتخاب کرده و سپس Reboot را بزنید تا تغییرات به صورت کامل ذخیره گردد.



شکل ۷: منوی General Setting سنسور تشخیص ضربه

۳-۳- منوی Network Settings

این بخش به شما کمک می‌کند تا سنسورر خود را برای اتصال به شبکه پیکربندی کنید. بسته به نیاز شبکه، می‌توانید تنظیمات را به صورت خودکار از طریق DHCP یا به صورت دستی انجام دهید (شکل ۸).

۱- حالت DHCP فعال باشد، سنسور به طور خودکار اطلاعات موردنیاز شبکه را از سرور DHCP دریافت می‌کند. این اطلاعات شامل آدرس IP، Subnet، Gateway، DNS Server و سایر تنظیمات می‌باشد.

۲- حالت DHCP غیرفعال باشد: در صورتی که بخواهید تنظیمات را به صورت دستی وارد کنید، باید گزینه DHCP را غیرفعال کنید. پس از غیرفعال کردن، گزینه‌های زیر برای تنظیم دستی در دسترس خواهند بود:

- آدرس IP: آدرس یکتای محصول در شبکه (مثال: 192.168.1.100)
- Subnet: مشخص‌کننده محدوده شبکه محلی (مثال: 255.255.255.0)
- Gateway: آدرس گیت‌وی پیش‌فرض برای ارتباط با سایر شبکه‌ها (مثال: 192.168.1.1)
- DNS1 و DNS2: آدرس سرورهای DNS که برای ترجمه‌ی نام دامنه به آدرس IP استفاده می‌شوند.

- HTTP Port: پورت مورد استفاده برای دسترسی به رابط کاربری محصول از طریق پروتکل HTTP (پیش‌فرض: ۸۰)
- HTTPS Port: پورت مورد استفاده برای دسترسی به رابط کاربری محصول از طریق پروتکل HTTP (پیش‌فرض: ۴۴۳)
- Certificate (گواهینامه): یک فایل دیجیتال است که هویت سنسور شما را در ارتباطات امن HTTPS تأیید می‌کند.
- Private key (کلید خصوصی): بخشی از گواهینامه است که برای رمزگشایی اطلاعات در ارتباطات امن استفاده می‌شود.

در پایان روی گزینه‌ی Save کلیک کنید و برای اعمال تغییرات گزینه‌ی Reboot را بزنید تا تغییرات به صورت کامل ذخیره گردد.

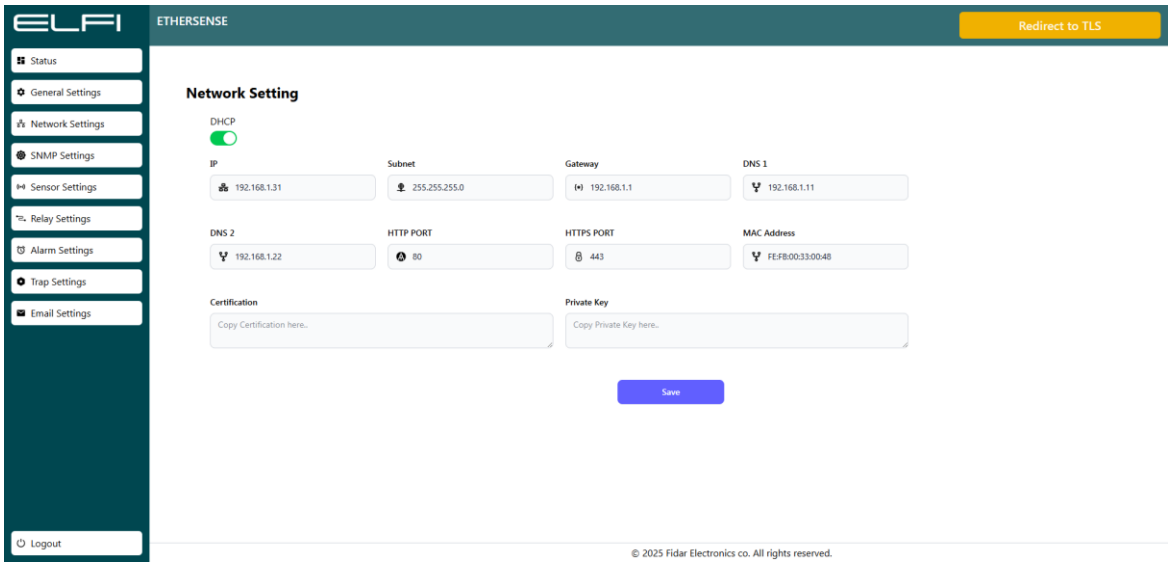
توجه: Private Key (کلید خصوصی) شما باید امن باقی بماند و نباید به اشتراک گذاشته شود.

توجه: برای افزایش امنیت، از HTTPS به جای HTTP استفاده کنید.

توجه: پورت‌های پیش‌فرض (مانند ۸۰ و ۴۴۳) را در صورت امکان تغییر دهید.

توجه: "کلید خصوصی" را در محلی امن نگهداری کنید و از دسترسی غیرمجاز جلوگیری کنید.

توجه: از رمزگذاری فایل "کلید خصوصی" استفاده کنید.



شکل ۸: منوی تنظیمات شبکه‌ی سنسور

۳-۴- منوی SNMP Settings

SNMP برای ارتباط بین مدیر شبکه و دستگاه‌ها (مانند سنسورها، سوئیچ‌ها و روترها) استفاده می‌شود. این بخش شامل گزینه‌هایی برای نسخه، تنظیمات Community، OIDها و Trapها است (شکل ۹).

- Current Version: نسخه فعلی پروتکل SNMP که سنسور تشخیص ضربه از آن پشتیبانی می‌کند. به طور معمول، این سنسور از نسخه‌های یک و دو پشتیبانی می‌کند.
- Community: Community در SNMP به عنوان رمز عبوری ساده برای کنترل دسترسی عمل می‌کند. این تنظیمات مشخص می‌کند که چه کسانی می‌توانند به اطلاعات سنسور دسترسی داشته باشند.

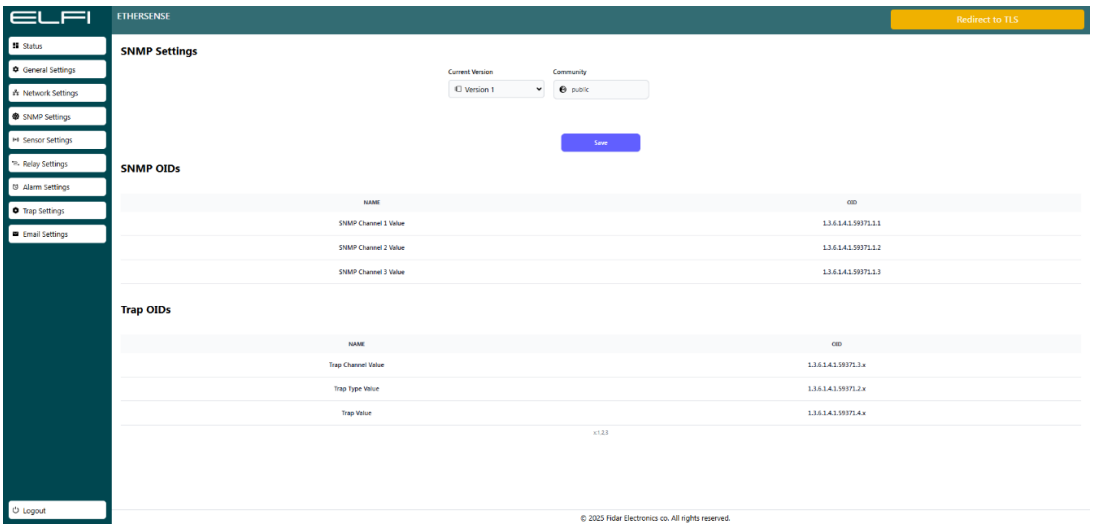
به صورت پیش‌فرض روی public تنظیم شده است، که به همه اجازه می‌دهد به اطلاعات عمومی سنسور دسترسی داشته باشند.

توجه: می‌توانید مقدار پیش‌فرض public را به یک نام اختصاصی و امن تغییر دهید.

توجه: از Community با نام‌هایی ساده و قابل حدس مانند public یا private اجتناب کنید.

در بخش SNMP OID و Trap OID، شناسه‌های موجود را مشاهده کنید.

توجه: Trap OIDها را با توجه به نیازهای نظارتی تنظیم کنید تا از ارسال اعلان‌های غیرضروری جلوگیری شود.



شکل ۹: منوی تنظیمات SNMP سنسور

۵-۳- منوی Sensor Setting

در صفحه تنظیمات سنسور، گزینه‌ای به نام **Reverse Mode** وجود دارد که به شما امکان می‌دهد عملکرد سنسور را معکوس کنید. این حالت برای شرایط خاصی که نیاز به تغییر نحوه تشخیص وضعیت سنسور دارید، طراحی شده است (شکل ۱۰).

عملکرد حالت معکوس

۱- **حالت عادی:**

در این حالت، سنسور وضعیت را به صورت پیش‌فرض تشخیص می‌دهد؛ به این معنا که:

- **حالت فعال (۱):** زمانی که سنسور، ضربات را شناسایی می‌کند.
- **حالت غیرفعال (صفر):** زمانی که سنسور، ضربه یا لرزشی را شناسایی نکند.

۲- **حالت معکوس (Reverse):**

در این حالت، تشخیص سنسور ضربه معکوس می‌شود؛ به این معنا که:

- **حالت فعال (۱):** زمانی که سنسور، ضربه یا لرزشی را شناسایی نکند.
- **حالت غیرفعال (صفر):** زمانی که سنسور، ضربات را شناسایی می‌کند.

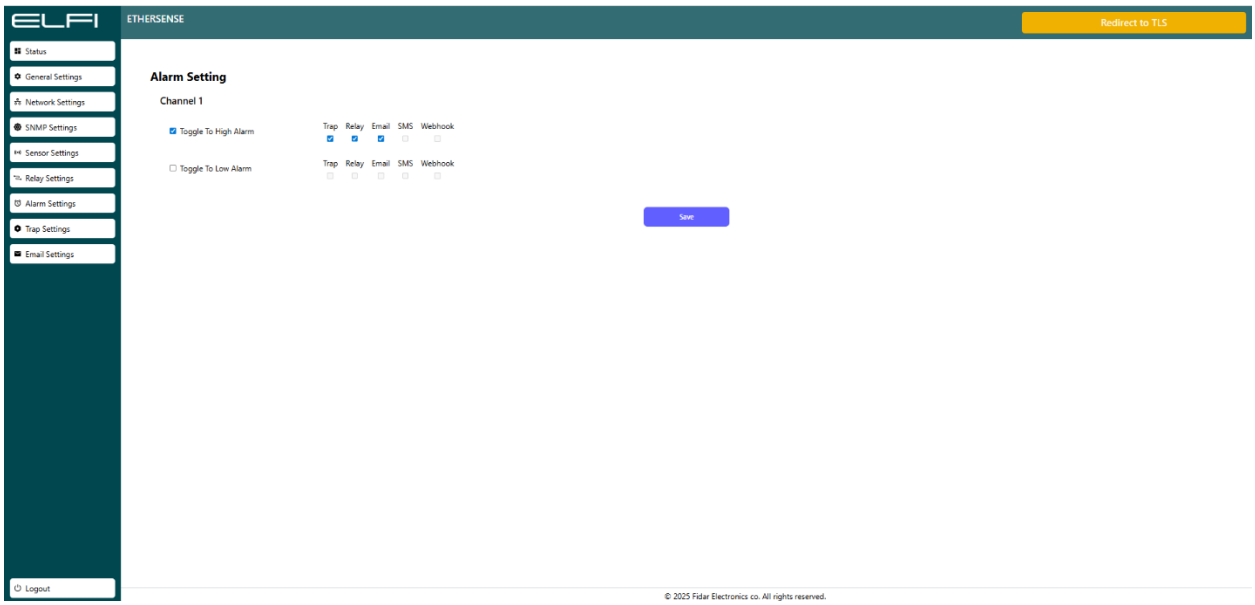
کاربردهای حالت معکوس:

- **هماهنگی با سنسورهای دیگر:**

در مواردی که سیستم‌های متصل به سنسور به تعریف متفاوتی از فعال یا غیرفعال بودن نیاز دارند.

- **تطبیق با محیط‌های خاص:**

در شرایطی که سیگنال ورودی سنسور برعکس تعریف شده است.



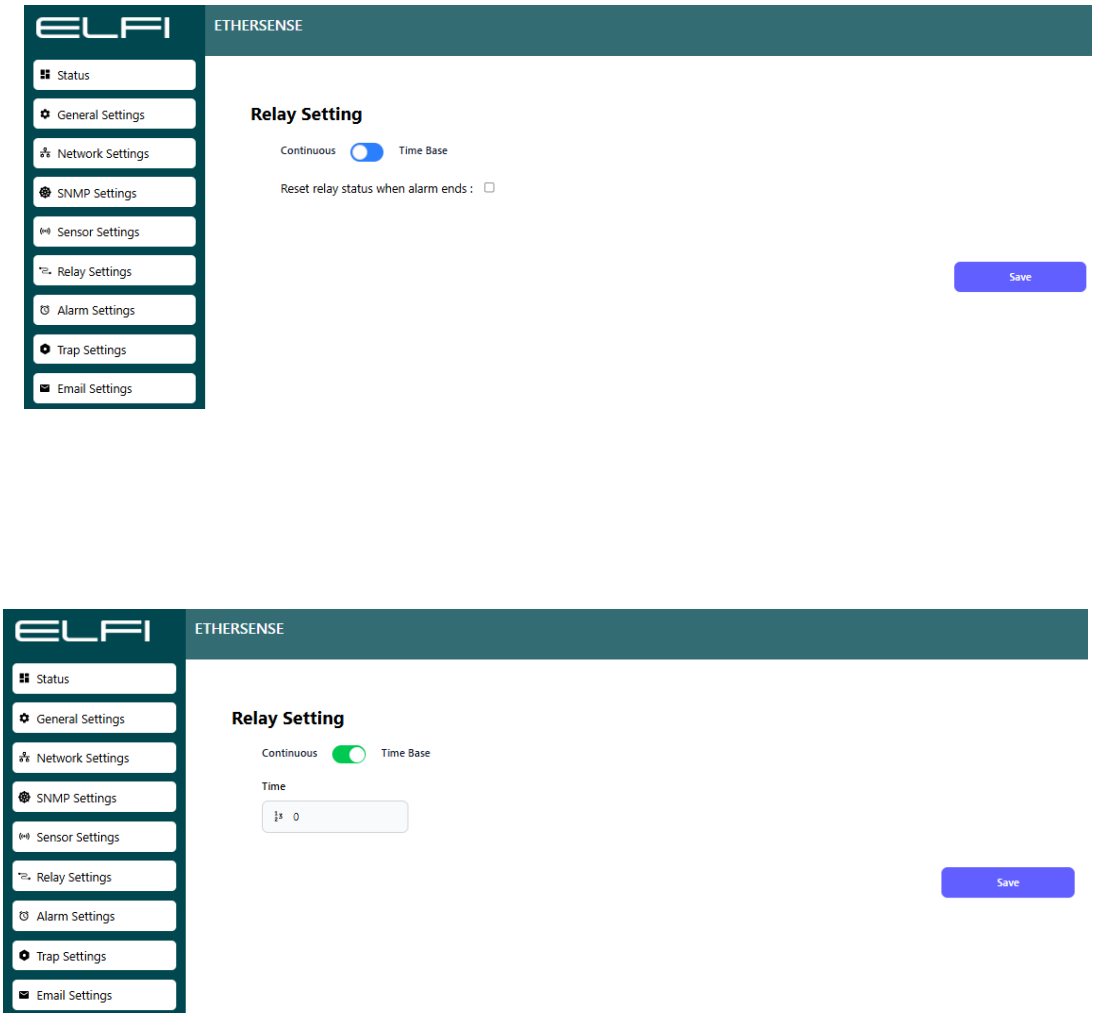
شکل ۱۰: صفحه‌ی تنظیمات سنسور

۳-۶- منوی Relay Setting

تنظیمات رله به دو صورت قابل انجام است:

■ اگر تنظیمات رله در حالت Time base باشد در صورت تعیین زمان (مثلاً ۱۰ ثانیه)، به محض تحریک شدن رله، تجهیزات متصل به آن از جمله آژیر، سیستم خنک‌کننده و ... به مدت ۱۰ ثانیه فعال شده و سپس قطع می‌شود.

■ اگر تنظیمات رله در حالت Continuous باشد به محض تحریک شدن رله، تا زمانی که سنسور از حالت آلارم خارج نشده باشد تجهیزات متصل به آن از جمله آژیر، سیستم خنک‌کننده و ... به فعالیت خود ادامه می‌دهند. همچنین در حالت Continuous، با فعال کردن گزینه‌ی Reset relay status when alarm ends پس از پایان هشدار، وضعیت رله به حالت قبلی باز می‌گردد یعنی آژیر خاموش می‌شود (شکل ۱۱).



شکل ۱۱: منوی تنظیمات رله‌ی سنسور تشخیص ضربه

۳-۷- منوی Alarm settings

صفحه تنظیمات آلارم به شما این امکان را می‌دهد تا نحوه عملکرد سنسور در هنگام شناسایی شرایط خاص را تعیین کنید. این آلارم‌ها می‌توانند برای نظارت و هشدار به کاربران در صورت تغییرات بحرانی یا وضعیت غیرعادی سنسور استفاده شوند (شکل ۱۲).

۱- Toggle To High Alarm:

- این حالت زمانی فعال می‌شود که مقدار سنسور به حالت **۱** تغییر کند.
- سنسور تشخیص ضربه با شناسایی این تغییر، آلارم را فعال کرده و هشدار ارسال می‌کند.
- مناسب برای شرایطی که نیاز به اطلاع از فعال‌شدن سنسور دارید (مانند شناسایی لرزش یا ضربه).

۲- Toggle To Low Alarm:

- این حالت زمانی فعال می‌شود که مقدار سنسور به حالت **صفر** تغییر کند.
- سنسور با شناسایی این تغییر، آلارم را فعال کرده و هشدار ارسال می‌کند.
- مناسب برای شرایطی که نیاز به اطلاع از غیرفعال‌شدن سنسور دارید (مانند عدم لزرش سنسور).

گزینه‌های ارسال و اعلام آلارم:

۱- ارسال آلارم از طریق ایمیل

- سنسور می‌تواند پس از فعال‌شدن آلارم، یک ایمیل هشدار به آدرس‌های تعریف‌شده ارسال کند.
- این ایمیل شامل جزئیاتی درباره وضعیت آلارم (مانند مشخصات محصول و نوع آلارم) خواهد بود.
- برای استفاده از این قابلیت، باید تنظیمات SMTP در بخش **تنظیمات ایمیل** به درستی پیکربندی شده باشد.

۲- ارسال SNMP Trap :

- سنسور می‌تواند یک **Trap** به مدیر شبکه ارسال کند تا وضعیت آلارم را اطلاع دهد.
- این قابلیت مناسب برای نظارت متمرکز در شبکه‌های مدیریتی است.
- تنظیمات مربوط به SNMP و Trap OID ها باید در بخش **تنظیمات SNMP** اعمال شوند.

۳- فعال‌سازی رله:

- سنسور تشخیص ضربه می‌تواند یک **رله** را فعال کند تا به صورت فیزیکی به آلارم پاسخ دهد.
- این پاسخ ممکن است شامل روشن‌شدن یک چراغ هشدار، فعال‌شدن آژیر یا کنترل یک دستگاه خارجی باشد.
- این گزینه برای محیط‌هایی با نیاز به اقدامات فوری و مکانیکی مفید است.

نحوه تنظیم آلارم:

الف) انتخاب حالت آلارم

۱. وارد صفحه **تنظیمات آلارم** شوید.
۲. یکی از دو حالت زیر را انتخاب کنید:
   - **Toggle To High Alarm**: فعال‌شدن آلارم در حالت **۱.**
   - **Toggle To Low Alarm**: فعال‌شدن آلارم در حالت **صفر**.

ب) انتخاب روش ارسال هشدار

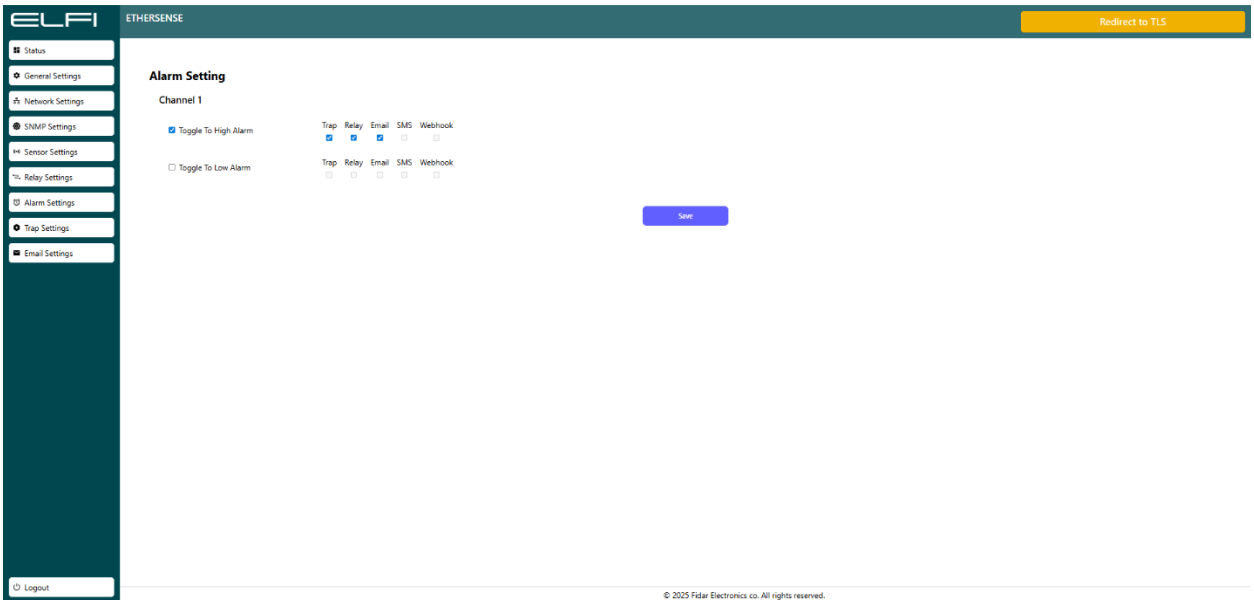
۱. در بخش **روش ارسال آلارم**، یکی یا چند گزینه زیر را انتخاب کنید:
   - **ایمیل:** ارسال هشدار به آدرس‌های ایمیل.
   - **SNMP Trap:** ارسال Trap به سرور مدیریت شبکه.
   - **فعال‌سازی رله:** ارسال فرمان به رله برای اقدامات فیزیکی.

ج) ذخیره و اعمال تنظیمات

۱. پس از انجام تنظیمات، روی گزینه Save و سپس Reboot را کلیک کنید.
۲. سنسور تنظیمات جدید را ذخیره کرده و آماده اجرای آن‌ها خواهد بود.

توجه: اگر از ایمیل برای هشدارها استفاده می‌کنید، حتماً آدرس گیرندگان و تنظیمات SMTP را بررسی کنید.

توجه: در محیط‌هایی که نیاز به پاسخ فیزیکی سریع دارند (مانند آژیر یا چراغ هشدار)، از قابلیت **فعال‌سازی رله** استفاده کنید.



شکل ۱۲: منوی تنظیمات آلارم

۸-۳- منوی Trap settings

SNMP Trap یک پیام هشدار ناهمگام است که توسط سنسور تشخیص ضربه به سرور SNMP ارسال می‌شود تا اطلاعاتی درباره وقوع یک رویداد خاص (مانند آلارم‌ها یا تغییرات وضعیت) ارائه دهد. این پیام به صورت خودکار و بدون نیاز به درخواست از طرف سنسور ارسال می‌شود (شکل ۱۳). نحوه پیکربندی تنظیمات Trap به این صورت است که:

۱. وارد بخش Trap Settings شوید.

۲. فیلدهای زیر را تکمیل کنید:

۱. **Trap Destination IP**: آدرس IP سرور مدیریت شبکه.

۲. **Trap Port**: شماره پورت مناسب (پیش‌فرض: ۱۶۲).

۳. **Trap Community**: مقدار مناسب (پیشنهاد می‌شود برای امنیت بیشتر مقدار پیش‌فرض را تغییر دهید).

در صفحه تنظیمات Trap Settings ، گزینه‌ای به نام **Send Delay Config** وجود دارد که برای تعریف تأخیر زمانی قبل از ارسال پیام‌های Trap به سرور مدیریت شبکه استفاده می‌شود. این قابلیت برای مدیریت بهتر ترافیک شبکه و کاهش بار سرور در شرایطی که رویدادهای مکرر رخ می‌دهند، بسیار مفید است.

اهمیت تنظیم Send Delay

- **مدیریت ترافیک شبکه:** جلوگیری از ارسال تعداد زیادی Trap در مدت زمان کوتاه که ممکن است باعث ازدحام شبکه شود.
- **کاهش بار سرور (سیستم مدیریت شبکه):** با ایجاد تأخیر در ارسال Trap، سرور زمان کافی برای پردازش پیام‌های قبلی را خواهد داشت.
- **پیشگیری از هشدارهای زائد**: در صورتی که تغییرات موقتی در سنسور رخ دهد، تأخیر می‌تواند از ارسالTrap های غیرضروری جلوگیری کند.

نحوه عملکرد Send Delay Config

تعریف زمان تأخیر

- شما می‌توانید زمان تأخیر را بر حسب **ثانیه** تنظیم کنید.
- **پیش‌فرض: صفر** (بدون تأخیر)
- **مثال**: ۱۰ (تأخیر ۱۰ ثانیه‌ای برای ارسال Trapها)
- Trapها تنها پس از گذشت زمان تعریف‌شده ارسال می‌شوند، حتی اگر چندین رویداد متوالی رخ دهد.

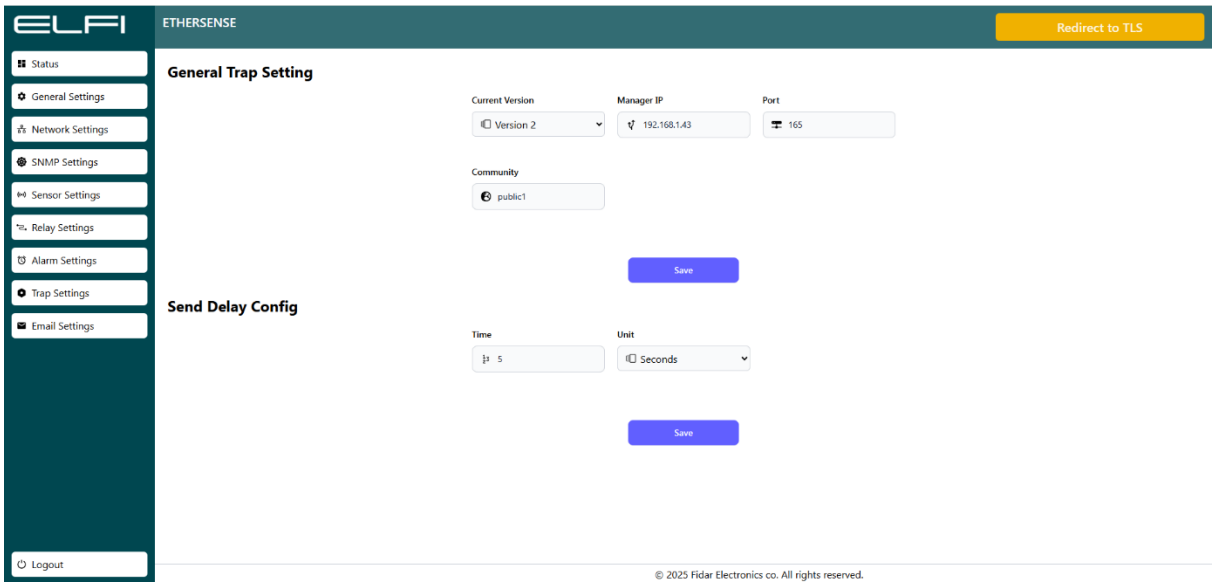
استفاده از تأخیر درTrap های مکرر

- اگر در طول زمان تأخیر چندین رویداد ثبت شود، سنسورتنها آخرین وضعیت را ارسال می‌کند.
- این ویژگی برای کاهش ترافیک در شبکه و جلوگیری از ارسال پیام‌های غیرضروری طراحی شده است.

توجه: مقدار تأخیر باید به گونه‌ای تنظیم شود که باعث از دست رفتن رویدادهای مهم نشود.

توجه: در شبکه‌هایی با نیاز به هشدارهای فوری، مقدار تأخیر را نزدیک به صفر تنظیم کنید.

توجه: پس از اعمال تنظیمات، عملکرد ارسال Trap را بررسی کنید تا اطمینان حاصل شود که پیام‌ها به موقع ارسال می‌شوند.



شکل ۱۳: منوی تنظیمات Trap سنسور

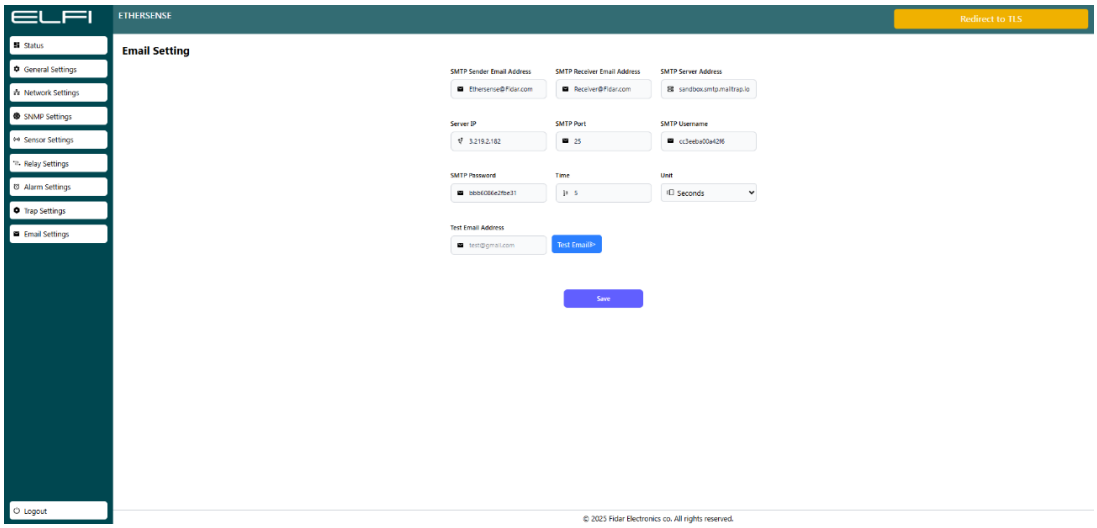
۹-۳- منوی Email Settings

این بخش به شما امکان می‌دهد تا تنظیمات مربوط به ارسال ایمیل از طریق پروتکل SMTP (Simple Mail Transfer Protocol) را پیکربندی کنید (شکل ۱۴). این قابلیت برای ارسال اعلان‌ها، هشدارها یا گزارش‌های سنسور به ایمیل‌های مشخص‌شده استفاده می‌شود.

- SMTP Sender Email Address: آدرس ایمیلی که به عنوان فرستنده در پیام‌های ارسال‌شده نمایش داده می‌شود. این آدرس باید معتبر باشد و معمولاً باید با تنظیمات سرور SMTP همخوانی داشته باشد. (مثال: Example@yourdomain.com)
- SMTP Receiver Email Address: آدرس ایمیلی که پیام‌ها به آن ارسال خواهند شد. (مثال: Example@yourdomain.com)
- SMTP Server Address: آدرس سرور SMTP که برای ارسال ایمیل استفاده می‌شود. این آدرس به ارائه‌دهنده سرویس ایمیل شما بستگی دارد.

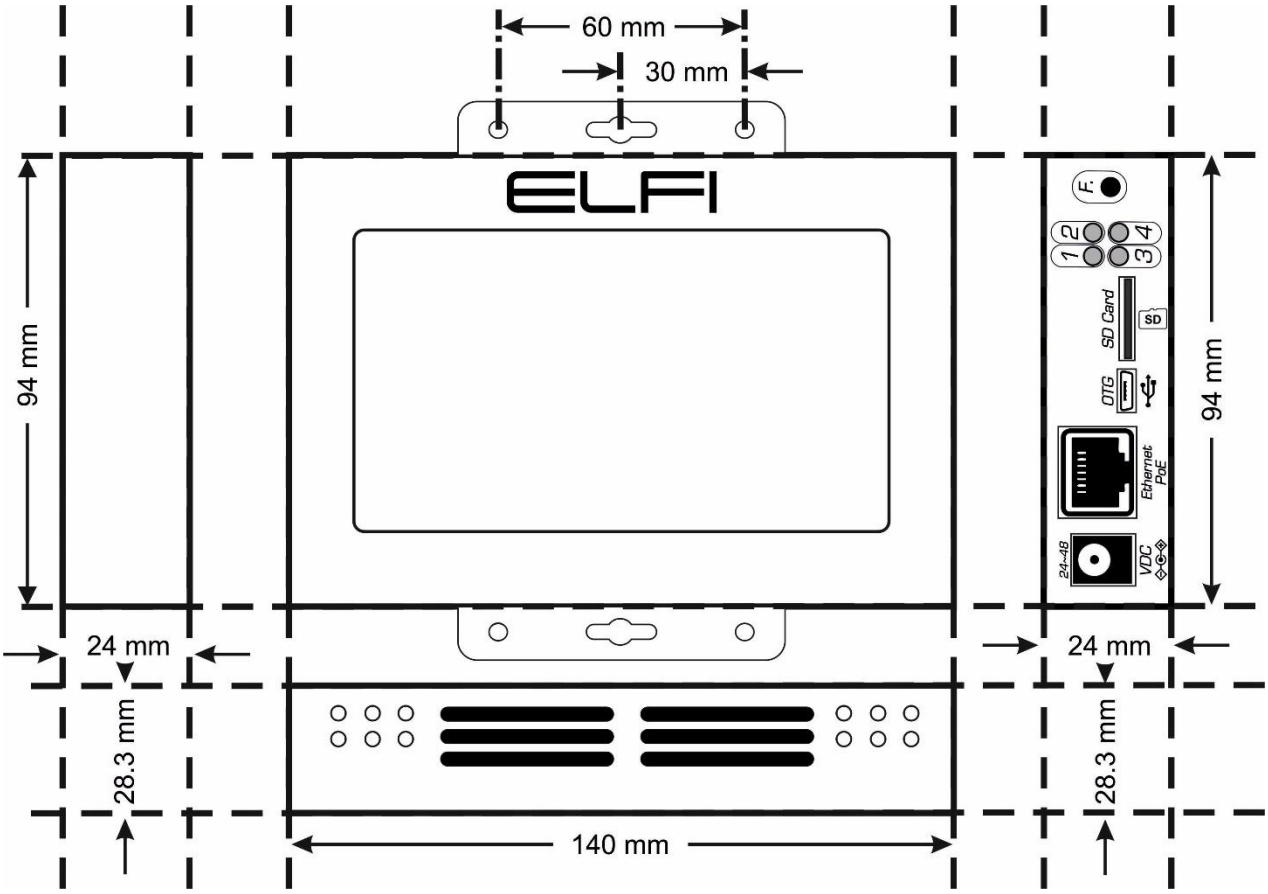
- **Server IP:** در صورت استفاده از سرور SMTP داخلی، می‌توانید آدرس IP سرور را وارد کنید.
- **SMTP Port:** شماره پورتی که سرور SMTP برای ارتباط استفاده می‌کند. پورت‌های رایج:
  - ۲۵: بدون رمزنگاری (اغلب قدیمی و کمتر استفاده می‌شود).
  - ۴۶۵: برای نظارت امن با SSL/TLS
  - ۵۸۷: برای ارتباطات امن با STARTTLS
- **SMTP Username:** نام کاربری مورد استفاده برای احراز هویت در سرورSMTP . معمولاً همان آدرس ایمیل فرستنده است.
- **SMTP Password:** رمز عبور مرتبط با نام کاربریSMTP . این رمز برای احراز هویت در سرور ایمیل استفاده می‌شود.
- **Time:** فاصله زمانی ارسال ایمیل‌ها یا زمان‌بندی ارسال خودکار پیام‌ها (بر حسب ثانیه).
- **Test Email Address:** آدرس ایمیلی که برای تست عملکرد تنظیمات ایمیل استفاده می‌شود. با وارد کردن این آدرس و استفاده از گزینه ارسال ایمیل تست، می‌توانید مطمئن شوید که تنظیمات به درستی پیکربندی شده‌اند.

در پایان روی گزینه‌ی Save کلیک کنید و برای اعمال تغییرات گزینه‌ی Reboot را بزنید تا تغییرات به صورت کامل ذخیره گردد.



شکل ۱۴: منوی تنظیمات ایمیل سنسور

۴- ابعاد سنسور



اطلاعات تماس

شرکت فنی و مهندسی بهینه فرآیند الکترونیک فیدار

تلفن: ۰۲۱-۹۱۳۰۸۵۱۵

نشانی: آذربایجان غربی - ارومیه، کیلومتر ۱۰ جاده سرو، پارک علم و فناوری استان، ساختمان ستادی، طبقه اول

پست الکترونیکی: info@fidarelectronics.com

نشانی سایت: www.fidarelectronics.com