SENSORS PLATFORM USER MANUAL



Copyright:

Copyright © 2025 InfraSensing BV All rights reserved. Reproduction without permission is prohibited.

Software:

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Trademarks:

ServersCheck and InfraSensing are registered trademarks of InfraSensing BV. All other trademarks or registered marks in this manual belong to their respective manufacturers.

Disclaimer:

Information in this document is subject to change without notice and does not represent a commitment on the part of InfraSensing BV.

Revision # 103 - Sensors Platform

InfraSensing BV provides this document "as is," without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. InfraSensing BV reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

InfraSensing BV has made this document to the best of its abilities. However InfraSensing BV assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

For UL compliant use we refer to the UL compliancy guide available on <u>http://manuals.infrasensing.com/UL Compliancy Guide v1.pdf</u>

Warranty: For the warranty on this product please visit <u>https://infrasensing.com/</u>

OPENING BASE UNIT, ADDON, EXPANSION HUB, SENSOR OR ANY OTHER HARDWARE VOIDS THE WARRANTY

Certifications:



The InfraSensing sensors are FCC (Class A) & CE (Class B) certified. Certificates can be downloaded from <u>https://infrasensing.com/sensors</u>

Commissioning Requirements

Testing and Verification: Before deploying any InfraSensing sensors into production, it is the responsibility of the customer to rigorously test each sensor during the commissioning phase. This is to ascertain and confirm the proper and accurate operation of the sensors, to ensure the integrity of data communication pathways, and to verify that alert mechanisms are configured and functioning correctly.

Gas Sensor Bump Testing: For all gas sensors provided by InfraSensing, a mandatory bump test shall be conducted during the commissioning phase. Bump testing is a quick check to confirm the sensor's responsiveness. It involves exposing the sensor to a known concentration of test gas and verifying the sensor's response.

Annual Review: In accordance with applicable code requirements, gas sensors shall be subjected to periodic bump testing at a minimum frequency of once annually. The customer is responsible for scheduling and ensuring this testing takes place and for maintaining accurate records of each test conducted.

Safety precautions

Caution

For safety reasons, the Base Units (base units), add-ons, expansion hubs and sensor probes may never be moved, disconnected, connected fully or partially covered while operating. Disconnect any power supply before performing installation or maintenance work.

Danger

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH FOR POWER SENSORS OR SENSORS IN ELECTRICAL ENVIRONMENTS

Apply appropriate personal protective equipment (PPE) and follow safe electrical work practices. In the USA, see NFPA 70E.

Only qualified electrical workers should install electrical equipment like our power sensors. Such work should be performed only after reading this entire set of instructions. NEVER install if something is not clear.

NEVER work alone.

Before performing visual inspections, tests, or maintenance on this equipment, disconnect all sources of electric power. Assume that all circuits are live until they have been completely de- energized, tested, and tagged.

Turn off all power supplying the power sensors and the equipment (such as base units) in which it is installed before working on it.

Always use a properly rated voltage sensing device to confirm that all power is off. The successful operation of this equipment depends upon proper handling, installation, and operation. Neglecting fundamental installation requirements may lead to personal injury as

well as damage to electrical equipment or other property.

NEVER bypass external fusing.

Before performing testing on any equipment in which the power sensors are installed, disconnect all input and output wires to the power meter. High voltage testing may damage electronic components contained in the electronics.

The power sensors should be installed in a suitable electrical enclosure.

Failure to follow the above instructions may result in damage of the equipment, serious personal injury or death.

Table of Contents

1	InfraSe	ensing Sensors Overview	11
	1.1	Unboxing video of the InfraSensing sensors	11
	1.2	Base Unit Overview	12
		1.2.1 ServersCheck – Base Unit	13
		1.2.2 SwitchMon – Base Unit	14
		1.2.3 Prevent-iON – Base Unit	15
	1.3	Base Unit Hardware Overview	16
	1.4	Base Unit's LED table	17
	1.5	OLED display subscripts	18
	1.6	Rack mounting	18
	1.7	DIN rail mounting	19
	1.8	Magnetic mounting	19
	1.9	Base Unit interface overview	20
	1.10	Configuring the Base Unit to the network	21
	1.11	Base Unit discovery tool	21
	1.12	Set your PC in the same network segment as the Base Unit	22
	1.13	Connecting to the Base Unit via the default IP	24
	1.14	Updating the firmware of the Base Unit	27
	1.15	Configuring the Base Unit's access security	28
2	Base L	Jnit Security Feature	29
	2.1	Username and Password configuration	29
	2.2	Firewall settings	30
	2.3	Enabling and Disabling Web Server	31
3	Base L	Jnit features and configuration	33
	3.1	Int. ping	33
	3.2	Configuring the Fahrenheit / Celsius readings	34
	3.3	ICMP server	35
	3.4	Sensor polling/refresh time	35
	3.5	Configuring internal clock of the Base Unit	36
	3.6	Setting threshold values in the Base Unit for alerting	40
	3.7	Alarm and Ambient VOC	41
4	Base L	Jnit alerting feature	42
	4.1	Email alerting	42
	4.2	Email alerts using the ADDON-LTE	43
		4.2.1 Gmail as e-mail server (https://mail.google.com)	44
		4.2.2 Outlook mail as e-mail server (https://outlook.live.com)	48
	4.3	Slack channel integration via e-mail alerts	50
	4.4	Tunneling an SSL connection	51
	4.5	Mail service like AuthSMTP.com	56

	4.6	SMS alerting from Base Unit	57
		4.6.1 SMS alerts via ADDON-LTE	57
		4.6.2 SMS alerts via my.infrasensing premium credits	59
		4.6.3 Sending SMS alerts and JSON Push data using the Microservice feature	61
	4.7	Voice call alerts	65
	4.8	Retest before alarm	67
	4.9	Maintenance Mode	68
	4.10	Fault Sensor	69
5	Histor	у	70
	5.1	Alert history	70
	5.2	Fault history	71
6	Config	uring the Base Unit for SNMP	72
	6.1	SNMP get requests	73
	6.2	SNMP traps	
	6.3	JSON (PULL)	80
	6.4	JSON (PUSH) with ADDON-LTE	82
	6.5	JSON (PUSH) with ADDON-LTE - Adding Webhook Endpoint	83
	6.6	XML output	85
	6.7	ModBus TCP / RTU	85
7	Senso	r calibration	86
	7.1	Reference Sensors	87
	7.2	Tolerance level	87
	7.3	Threshold change and additional calibration functions	
8	Factor	y resetting of Base Unit	90
	8.1	Base Units v1 and v2	
	8.2	Base Unit v3 and v4	91
	8.3	Base Unit v5	92
9	Add-O	ns for the Base Unit	93
	9.1	Wifi Add-On	93
		9.1.1 Features	94
		9.1.2 View of the Wifi Add-On connected to the Base Unit	94
		9.1.3 Hardware interface	95
		9.1.4 Getting started	96
		9.1.5 How to access the Graphical User Interface (GUI)	97
		9.1.6 Username and password settings	99
		9.1.7 Configuration modes	100
	9.2	Satellite Communication Add-On (ADDON-SATELLITE)	105
	9.3	Industrial PoE+ Injectors +24 or -48v (ADDON-POE-24 / ADDON-POE-48	3) 106
	9.4	LTE/2G/3G Communication Add-On (ADDON-LTE)	107
		9.4.1 GUI of the ADDON-LTE	
		9.4.2 ADDON-LTF modes	110

		9.4.3 Setting up data connection	
		9.4.4 SIM section	
		9.4.5 Email section	
		9.4.6 GPS section	
		9.4.7 Inserting the SIM card into the LTE Add-	On
10	InfraS	ensing sensor probes	117
	10.1	External sensor probes	117
	10.2	General instructions	117
11	THER	IOGRAPHY SENSORS	119
	11.1	Thermography Sensor (THIMG-XX)	119
		11.1.1 Installation of Thermal Image	
		11.1.2 Adding Zones to the Thermography Se	ensor Camera 120
		11.1.3 Delete Zones from the Thermal Imagin	g Sensor Camera120
	11.2	Thermography Sensor – Cylindrical Series	(C-THIMG-SM) 121
	11.3	Industrial Infrared Spot Sensor (THIMG-IR	SPOT) 122
	11.4	Industrial Infrared Spot Sensor – Cylindrica	al Series (C-THIMG-IRSPOT) 122
12	Gas So	nsors	123
	12.1	VOC, Temperature and Humidity Sensor (G	GAS-VOC) 123
	12.2	Flammable Gas Sensor (R-GAS-FLAMMABI	_E) 124
	12.1	Panel Sensor (R-EGD-PANEL)	
	12.2	Ozone (O3) Gas Sensor (EGD-O3)	
	12.3	Sulfur Hexafluoride (SF6) Gas Sensor (EGE	0-SF6) 128
	12.4	Refrigerant A1 (R-410A) Gas Sensor (GAS-	A1) 128
	12.5	Refrigerant A2L (R-32, R-454B, and R454C) Gas Sensor (GAS-A2L) 129
	12.6	Refrigerant A3 (R-290) Gas Sensor (GAS-A	3) 129
	12.7	Gas Sensor Bump Test	130
13	Enviro	nmental Sensors	131
	13.1	Temperature Sensor (ENV-TEMP)	
	13.2	Temperature & Humidity Sensor (ENV-THU	M) 131
	13.3	ISO17025 Calibrated Cylindrical Temperat 132	ure & Humidity Sensor (C-ENV-THUM)
	13.4	Magnetic Surface Temperature Sensor (EN	IV-TEMP-MAGNETIC) 132
	13.5	Digital Sound and Noise level Sensor(dbA)	(ENV-NOISE) 133
	13.6	Atmospheric Corrosion Sensor (ENV-CORF	ROSION) 133
	13.7	Differential Air Pressure and Temperature	Sensor (ENV-AIRPRESSURE) 134
	13.8	Linear Heat Detection Sensor (ENV-LHD)	
	13.9	Optical Dust Sensor Probe (ENV-DUST)	
	13.10	Particle Sensor (ENV-PARTICLE)	
	13.11	Water Leak Sensor (ENV-WLEAK-COMBO	5M) 136
	13.12	Optical Oil & Hydrocarbon Leak Sensor (E	NV-LEAK-OPTICAL) 137
	13.13	Stainless Steel Temperature Probe (ENV-	TSTAIN) 137

	13.14	Extreme Low Temperature Sensor (ENV-TULTRA)	138
	13.15	Industrial Surface Temperature Sensor (ENV-TSURFACE)	138
	13.16	IP rated sensor assembly (leak, industrial probes, etc.)	139
	13.17	Water Spot Detection Sensor (monitors a specific spot) (ENV-WSPOT)	141
	13.18	View of the Airflow Sensor (ENV-AIRFLW)	142
14	Daisy	Chain	143
	14.1	Daisy Chain Temperature Sensor (DAISY-TEMP)	143
	14.2	Daisy Chain Temperature and Humidity Sensor (DAISY-THUM)	143
	14.3	Daisy Chain Infrared Spot Sensor (DAISY-THIMG-IRSPOT)	144
	14.4	Daisy Chain Temperature Magnet Sensor (DAISY-TEMP-MAGNET)	144
	14.5 (C-DA	ISO 17025 Calibrated Cylindrical Daisy Chained Temperature & Humidit ISY-THUM)	
	14.6	Daisy Chain Start (DAISY-STARTER)	145
		14.6.1 Connecting Daisy Chain Sensor	146
	14.7	Daisy Booster	152
15	Power	r Sensors	153
	15.1	View of DC Voltage Sensor Sensor (12-80V) (PWR-DC-VOLT)	153
	15.2	View of Current Sensor (PWR-AC-CUR)	153
	15.3	View of AC power failure (PWR-AC-FAIL)	154
		15.3.1 Main sensor unit (PWR-BAT-STRING)	156
	15.4	Power Quality Sensor (PWR-AC-QUAL)	157
		15.4.1 Initial set up for the power quality sensor using BASE-XX	158
		15.4.2 Initial set up for the power quality sensor using SD card .ini file	159
		15.4.3 Ground (Earthing) Monitoring Sensor (PWR-GROUND)	160
	15.5	IP68 Ultrasonic Fuel Level Sensor (PWR-FUEL)	162
		15.5.1 Features	162
		15.5.2 Maximum Tank Depths	162
		15.5.3 Dimensions	162
		15.5.4 Mounting and installation	163
		15.5.5 Tips and example installations	164
16	Indust	rial sensor	167
	16.1	Industrial 0-10V (IND-0-10V)	167
	16.2	Industrial 4-20mA (IND-4-20mA)	167
	16.3	The IO Sensor Probe – 16 Dry Contacts IN & 4 OUT (IND-IO)	168
	16.4	General description	168
	16.5	Applications	168
	16.6	Terminal description	168
	16.7	Basic wiring diagram	169
	16.8	Base Unit IO sensor probe interface	172
	16.9	Wiring configuration and settings (anti tampering)	173
	16.10	Output triggering	176

17	Securi	ty Sensors	177
	17.1	General description	177
	17.2	Door Sensor (SEC-DOOR)	177
	17.3	Motion Sensor (SEC-MOTION)	178
	17.4	Smoke Sensor (SEC-SMOKE)	180
		17.4.1 Installation guide for Security Smoke Sensor	. 181
	17.5	Sound Sensor (SEC-SOUND)	182
	17.6	Digital Luminosity Sensor (LUX) (SEC-LUX)	182
	17.7	Shock / Vibration Sensor (SEC-SHOCK)	183
	17.8	Tilt Sensor (SEC-TILT)	183
18	The Se	nsor Hub (EXP-8HUB)	184
	18.1	General description	184
	18.2	Probe restrictions	185
	18.3	Connecting the SensorHub to the Base Unit	185
	18.4	Terminal connections	186
	18.5	Basic wiring	187
	18.6	Basic wiring diagram	188
	18.7	SensorHub web interface	190
19	LoRa V	Vireless Hub and Node	191
	19.1	Connecting and Pairing	192
20	Autom	atic & remote control of equipment	196
	20.1	Triggering outputs through the web interface	197
	20.2	Wiring for a control output	198
	20.3	Geomapping sensors	199
21	Power	rating	200
22	Produc	et Registration	202
	22.1	How to Register your Hardware:	202
	22.2	Managing your Registered Device	206
		22.2.1 RMA Request	206
		22.2.2 Firmware Updates	207
23	RMA / I	Repair	209

Note:

For technical support kindly visit https://infrasensing.com/support

In June 2018 we did rebrand our sensor platform from ServersCheck to **InfraSensing.** This document may still include references to ServersCheck in graphics and images while the InfraSensing name is now being used.

1 InfraSensing Sensors Overview

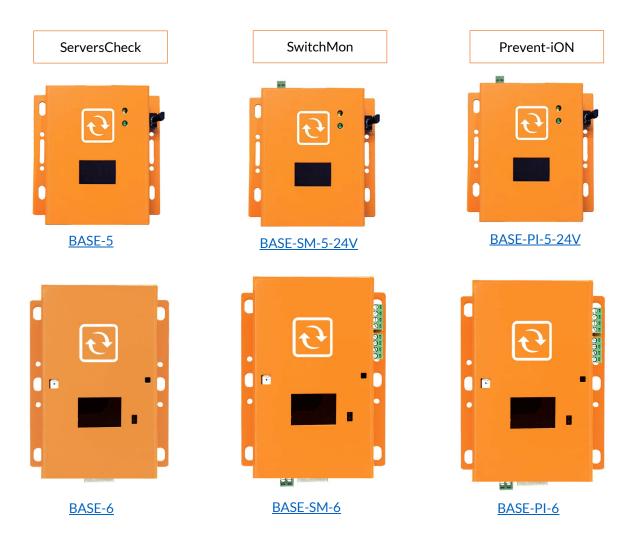
1.1 Unboxing video of the InfraSensing sensors

We invite you to watch following unboxing video before unpacking, installing and configuring your InfraSensing sensors: https://infrasensing.com/sensors/



1.2 Base Unit Overview

The Base Unit is the heart of the InfraSensing sensors. This Base Unit is where all the smart logic resides : from connection to monitoring, reporting and alerting.



The Base Unit is connected to the network via a standard network cable over a 10/100Mbps network. It supports PoE too. This allows for powering the sensors without having to rely on external power adapters. If you don't have a PoE network then a power adapter is optionally available. Each Base unit is specifically designed to support a unique set of sensors, ensuring compatibility and functionality tailored to their applications. This means that the sensors supported by each Base Unit are carefully selected to match its specific capabilities, enabling optimized performance for different use cases.

Note : If a power adapter (BASE-PWR) and PoE is plugged into the Base Unit to supply power at the same time the Base Unit will automatically switch to the power adapter and use the PoE as backup. Also the Base Unit will not shutdown or restart if either one is unplugged.

In the following sections of this user manual, we are going to describe in detail the configuration and operation of the Base Unit.

The maximum tested length between a PoE switch and the Base Unit is 330ft or 100meters (using Cat6 shielded cables). Actuals may vary depending on cable quality, switch and environmental factors.

BASE-5

The Base Unit is a stand-alone, IP-based monitoring device with built-in alerting features, serving as the foundational unit for our entire ServersCheck sensor solution lineup.

The BASE-5 version incorporates various built-in features, including an onboard temperature sensor, a secure HTTPS-enabled web server, and a fully responsive web interface accessible on desktops, tablets, or smartphones.

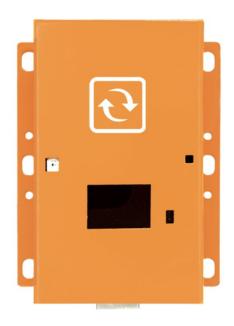
This Base Unit seamlessly supports all ServersCheck sensors except for Gas and Thermography sensors, enabling real-time environmental and infrastructure monitoring for comprehensive facility management.



BASE-6

The BASE-6 is an updated version of the Base Unit that includes newbuilt-in features, such as RS485 on a terminal block. It boost a data memory of QSPI 256Mbit and allow for the insertion of and SD Card. Additionally, it has two status LEDs on the PCB.

This Base Unit seamlessly supports all ServersCheck sensors except for Gas and Thermography sensors, enabling real-time environmental and infrastructure monitoring for comprehensive facility management.



BASE-SM-5-24V

Compared to the regular base unit, the BASE-SM-5-24V is equipped with a terminal block for power connections, offering a more secure and industrial-grade alternative to the traditional barrel jack.

This design enhances its suitability for industrial environments where reliability and robustness are essential.

This Base Unit seamlessly supports all SwitchMon-compatible sensors, except for Gas sensors, enabling real-time environmental and infrastructure monitoring for comprehensive facility management.



BASE-SM-6

The BASE-SM-6 is an updated version of the Base Unit that includes new built-in features, such as RS485 on a terminal block with 1 relay output.

This base unit serves as the foundational unit for our entire SwitchMon sensor. It boosts a data memory of QSPI 256Mbit and allows for the insertion of an SD Card. Additionally, it has two status LEDs on the PCB.

This Base Unit seamlessly supports all SwitchMon-compatible sensors, except for Gas sensors, enabling real-time environmental and infrastructure monitoring for comprehensive facility management.



BASE-PI-5

The BASE-IP-5 is a stand-alone, IP-based monitoring device with built-in alerting features, serving as the foundational unit for our Prevent-iON solution lineup.

This Base Unit seamlessly supports all sensors, enabling real-time environmental and infrastructure monitoring for comprehensive facility management.

BASE-PI-5-24V

Compared to the regular base unit, the BASE-PI-5-24V is equipped with a terminal block for power connections, offering a more secure and industrial-grade alternative to the traditional barrel jack.

This design enhances its suitability for industrial environments where reliability and robustness are essential.

This Base Unit seamlessly supports all sensors, enabling real-time environmental and infrastructure monitoring for comprehensive facility management.

BASE-PI-6

The BASE-PI-6 is an updated version of the Base Unit that includes new built-in features, such as RS485 on a terminal block with 3 relay output. It boasts a data memory of QSPI 256Mbit and allows for the insertion of an SD Card. Additionally, it has two status LEDs on the PCB.

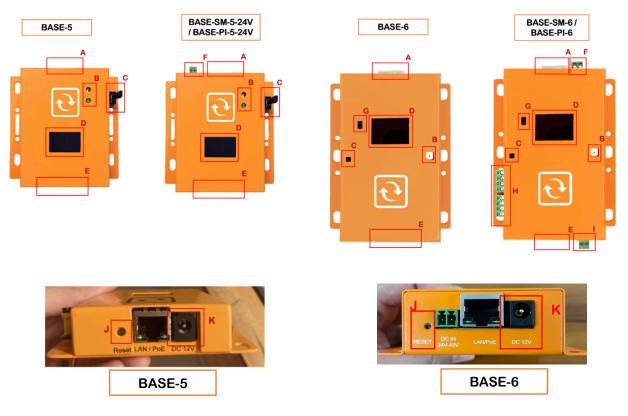
This Base Unit seamlessly supports all sensors, enabling real-time environmental and infrastructure monitoring for comprehensive facility management.







1.3 Base Unit Hardware Overview



- A. Ethernet/PoE Port for network and PoE connection via RJ45
- B. Status LED
 - a. Yellow (Network) Stable = Network established, No Light = No Network
 - b. Green (Sensor) Stable =External Probe detected, No Light = No External Probe
- C. Int. Temp. Base Unit's built in Temperature Sensor
- D. OLED Screen
 - a. OLED displays a rolling banner that has the following information:
 - i. Base Unit IP Address
 - ii. Date
 - iii. Time
 - iv. Internal Temperature of Base Unit
- E. Sensor Probe Ports where sensor probes connect via RJ45
- F. Power supply input another option to power up the base unit with 12v DC to 24v DC input via the terminal block
- G. Proximity sensor this feature activates when motion is detected or when you hover your hand above it, causing the OLED display to light up, this can also be disabled.
- H. RS485 port
- I. Relay output
- J. Reset Button Pressing the Reset button will present you with three options: 'Start Webserver', 'Reboot', and 'Load Defaults'. To perform any of the options, hold the reset button until the desired option appears on the OLED display. Once the desired option is displayed, release the reset button.



K. Power Adapter DC Jack – where optional Power Adaptor connects to provide power when PoE is unavailable.

1.4 Base Unit's LED table



The following table details the different led indication combinations. Each combination allows you to visually get the nature of the state/issue

Yellow LED (Network/Online)	Green LED (Sensor)	Description
Flashing (fast, ~1/10 sec)	On	Updating firmware after reboot. Reboot time is about 5 seconds before Base Unit is ready.
Flashing (slow, ~1 sec)	Any	Can't sync with NTP (time) server
On	Any	Synchronized with NTP (time) server
Any	Flashing	Can't communicate with external sensor probe
Any	On	Connected with external sensor probe

Normal Power on Reset, No New Firmware Uploaded

Power ON state: Yellow & Green LED are ON for 2 seconds and start flashing

Run state: Yellow & Green LED are both flashing Green LED is ON if able to connect with external sensor probe Yellow LED is ON if able to sync with NTP (time) server

Reboot, New Firmware Uploaded

Power ON state: Yellow & Green LEDs are ON for 1 second and Yellow LED starts flashing

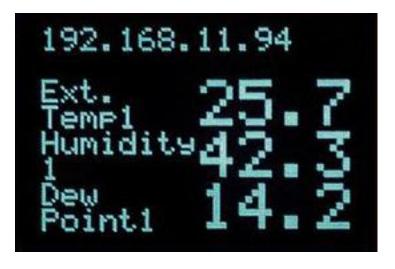
Updating firmware state: takes around 20 seconds Green LED stays ON Yellow LED will flash very fast (about 1/10 seconds)

Ready state: Yellow & Green LED are both flashing Green LED is ON if able to connect with external sensor probe Yellow LED is ON if able to sync with NTP (time) server

Note:

Various options will appear including Start, Webserver, Reboot, and Load Default, depending on the duration of pressing the reset button.

1.5 OLED display subscripts

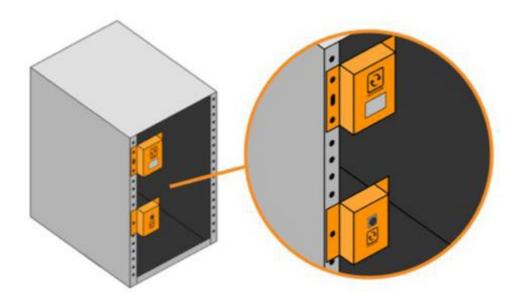


The OLED display gives one a quick view of the values the Base Unit reading. The reference for the order of the subscript numbering is completely dependent on how the web page is showing it.

1.6 Rack mounting

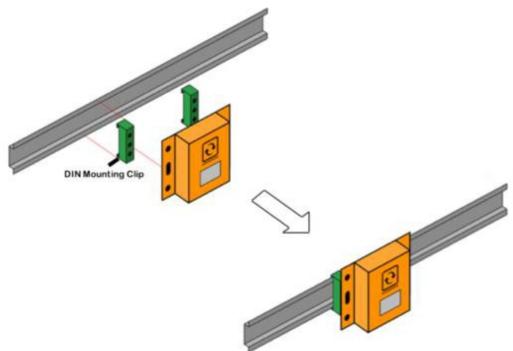
The Base Unit and most of our sensors are OU devices that can be easily and securely mounted in a rack using standard rack mount screws with a head of at least 0.65cm / 0.26 inch. Although one screw is sufficient to hold the whole equipment in place, a second one improves stability.

Typically, the sensors are mounted at the rear of the rack where ample place is available so that it doesn't use any space reserved for server and other network rack mounted equipment.



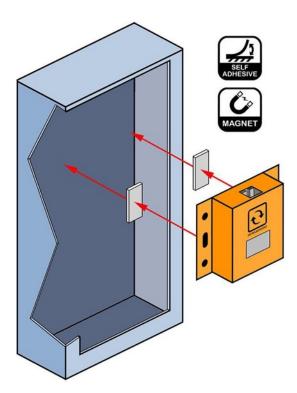
1.7 DIN rail mounting

The base unit has DIN mounting provisions that can be easily attached on DIN mounting clips using standard screws with a head of at least 0.6 cm / 0.24 inch. The clips are then mounted on DIN rails as shown on the image below.



1.8 Magnetic mounting

As our base unit, add-ons, expansion hubs, and most sensors feature a metal steel enclosure, the devices can also be mounted using simple magnets.



1.9 Base Unit interface overview

Connect to the InfraSensing Base Unit using your browser and on the IP address defined in the next section.

Status	Type	Name	Value	Warning Range	Down Rang
	Temperature	Int. Temp1	29.98 °C	<18 OR >37	<15 OR >41

Image of the left side of the main page.

(1) This is the Home Button which will bring you to the sensor information page whenever it is clicked.

(2) The sensors will be shown on this portion of the page

(3) Additional options will appear on this area depending on the sensor connected (Wireless Hub, Thermal Image, etc.)

Image of the right side of the main page.

						4. 🔳
						5. 🧰
D	Repeat Alarm	Email	SMS	SNMP Trap	Set Output To	
18			2		DISABLE	

(4) The Menu Button, when clicked will show the options on the image below.

[ਦੇ	
	Sensor Status	
	Alert History	
	Settings	
	Buy new sensors	
	myServersCheck & Support	

(5) Edit button to configure the thresholds and alerting features for each of your sensor

1.10 Configuring the Base Unit to the network

The Base Unit can have 2 types of IPv4 addresses: Fixed or Dynamic (using DHCP). By

default, the gateway will try to get an IP address via DHCP to connect to your network. If this fails, then the default IP address from factory of the Base Unit is **192.168.11.160**

To change the IP address to a different fixed one, proceed as follows.

We highly recommend not using DCHP but instead to use fixed IP addresses.

Make sure the Base Unit is plugged with a network cable into the network.

1.11 Base Unit discovery tool

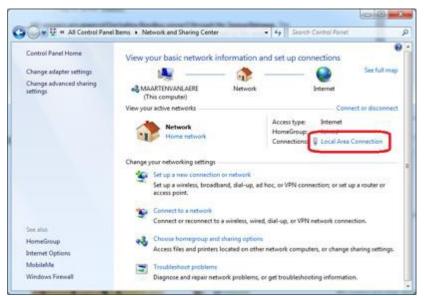
If you have connected multiple gateways and wanted to check their IP/MAC address you can use our tool to immediately show all the Base Unit connected within your network. All you have to do is run the software, which can be downloaded, from <u>https://infrasensing.com/support/downloads.asp</u>

Works with Windows(Discoverer.exe) and Mac OS(Discoverer.jar).

		Microchip TCPI	P Discoverer		
Help					
Discover	Devices			Exit	
IP Address	Host Name	MAC Address	Other Info		
192.168.9.14	SENSORGATEW	00-03-64-03-5A			
192.168.9.31	SENSORGATEW	00-03-64-03-56			
192.168.9.33	SENSORGATEW	00-03-64-03-5E			
192.168.9.19	SENSORGATEW	00-03-64-03-56			
I					

1.12 Set your PC in the same network segment as the Base Unit

The steps below apply to a Windows 7 system. For other systems (Windows, Mac, Linux) steps are similar. You may skip the instructions entirely, provided your gateway received an IP address from your DHCP server (you can check via our Network Discovery Tool) or your network segment is already the same as the gateways default IP and that the IP 192.168.11.160 is not being used/leased.



Go to Network Panel > Network & Sharing Center

Click on Local Area Connection and then click on Properties. In the new window select Internet Protocol Version 4 and click on the Properties button.

General		Networking
Connection JPv4 Connectivity: JPv6 Connectivity: Media State: Duration: Speed: Dgtals	Internet No Internet access Enabled 2 days 12:01:59 1.0 Gbps	Connect using: Proadcom NetLink (TM) Gigabit Ethemet Configure This connection uses the following items: Graphic Configure for Microsoft Networks Graphic Configure for Microsoft Networks Graphic File and Printer Sharing for Microsoft Networks Graphic Configure for Microsoft Networks
Activity Sent	Received	Internet Protocol Version 4 (TCP/IPv4) Image: a protocol Version 4 (TCP/IPv4) <
Bytes: 883,787,938	9,051,371,850	Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
	Close	OK Cancel

Now you need to set in the Properties window your PC in the same IP range as the sensor. Remember the current settings of your PC before changing any value!

We recommend setting it to 192.168.11.159 as shown below. When done, click on the **OK** button.

You can now plug your Base Unit directly to your PC

Seneral	
	automatically if your network supports sed to ask your network administrator
🗇 Obtain an IP address autom	atically
Q Use the following IP address	
(P address:	192 . 168 . 11 . 159
Sybriet mask:	. 255 . 255 . 0
Default gateway:	-
O Ogtan DNS server address	automatically
Use the following DNS serve	r addresses:
Breferred DNS server:	 a) b) b)
Alternate DNS server:	12 11 12
Vajdate settings upon exit	Adganced

Note: the gateway needs a Power Adapter so you can directly connect it via the PC's Ethernet port unless the port supports PoE.

1.13 Connecting to the Base Unit via the default IP

Once you have completed **Section 2.9**, Open your browser and surf to <u>http://192.168.11.160</u> A connection will be made to the web server on board of the Base Unit and you will be prompted for a username & password. Default username and password is: **admin / admin**

6	To view this 192,168,11,1	page, you must log in to area "Protected" or 60-80.
Ø	Tour passwo	nd will be sent unencrypted.
-	Name	admin
	Password	
	Rememi	ber this password

When logged in you will be shown the main screen of the Base Unit with the first sensor reading being the built-in temperature probe.

In the main window, click on the **Menu button** located on the upper right corner of the page. Then click on settings, and once the page loads click on "**Change IP**"

3												
Sensors												
Satus	Type	Name	Value	Warning Range	Down Range	Repeat Alarm	Enal	5545	Shift Trap		Set Output To	
	Temperature	int. Tempf	28.90 °C	<18-OR >37	+15 OR 141			- 2		DISABLE	•	•
PING Sensor												
ਿ												
Sensor Status												
Alert History												
Settings												
Buy new sensors												
myServersCheck &												

Settings & Info

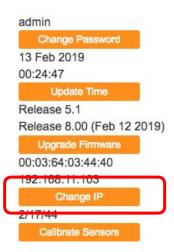
Device information Account name

Current System Date Current System Time

Hardware Version Firmware Version

Mac Address IP Address

Node Status (online/used/max)



You can now change the Base Unit's IP address to any value you like: either to DHCP or to a fixed IP that would fit your local network. We will now set it to 10.0.0.36 with its default gateway to 10.0.0.1 respectively. As for the DNS server feel free to use any, in this set up, we will use 4.2.2.2 and 8.8.8.8. You can also see the MAC address of the gateway and set the Net BIOS Name.

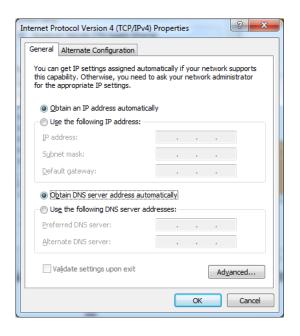
Note: If you want to make a device accessible via DNS please make sure that the Net BIOS Name is 15 or more characters if not, then it will be appended with a blank space because of the padding process of Microsoft please see link. <u>https://technet.microsoft.com/en-us/library/cc958811.aspx</u>

Once the value has been changed, the Base Unit will reboot itself and will then be accessible through the newly defined IP.

Fixed IP	
DHCP	()
CMP Server	
P Address	10.0.0.36
Subnet Mask	255.255.255.0
Sateway	10.0.0.1
Primary DNS	4.2.2.2
Secondary DNS	8.8.8.8
Net BIOS Name	SENSORGATEWAY
Mac Address (HEX)	00:03:64:03:03:E8

Network Settings

Now reset your system to its normal IP address. In our case we reset it to DHCP.



We will now check the Base Unit and connect to its new IP address by connecting to it using a browser.

Sensor	s			
Status	Туре	Name	Value	Warning Range
	Temperature	Int. Temp1	28.98 °C	<18 OR >37

As seen on the image above, We were able to access the gateway via its new IP address since our network segment is set at 10.0.0.X and we set our computer back to DHCP the gateway is now connected and can be accessed through our network.

1.14 Updating the firmware of the Base Unit

InfraSensing may release from time to time new firmware versions for its Base Units.

You can check your currently installed firmware version by going to your Base Unit, and then click on the menu option then settings.

Settings & Info

Devile a lafe marking

Device information	
Account name	admin
	Change Password
Current System Date	14 Feb 2019
Current System Time	03:57:16
	Update Time
Hardware Version	Release 5.1
Firmware Version	Release 8.00 (Feb 12 2019)
	Upgrade Firmware
Mac Address	00:03:64:03:44:40
IP Address	192.168.11.104
	Change IP
Node Status (online/used/max)	3/43/44
	Calibrate Sensors

Go to your https://my.infrasensing.com/ account to check for new firmware releases.

You must be on firmware version 8.5 or above before uploading the latest firmware.

Download the firmware to your PC and then go with your browser to the Base Unit you wish to upgrade.

Click on the **Upgrade Firmware** option and then click on the **Browse** button to locate the downloaded firmware file. Only then click on the **Upload** button.

Your Base Unit will now start loading the new firmware. Your Base Unit will be available on <u>http://192.168.11.160 (Default)</u> or via the IP address shown on its OLED after the firmware update has been completed

Note: Should the upgrade fail and should the Base Unit be unresponsive then perform a factory reset as described in section 8.

1.15 Configuring the Base Unit's access security

The Base Units can be username and password secured. Default factory values are admin/admin

To change the values, click on the Settings menu option

ਦ	
Sensor Status	
Alert History	
Settings Buy new sensors	
myServersCheck & Support	

Click on "Change Password" and enter the new username and password

Settings & Info

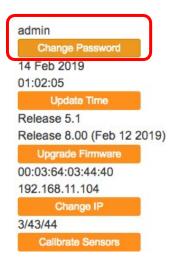
Device information Account name

Current System Date Current System Time

Hardware Version Firmware Version

Mac Address IP Address

Node Status (online/used/max)



2 Base Unit Security Feature

2.1 Username and Password configuration

Every time you access your base unit, a pop-up message will appear prompting you to enter your username and password.

Username	
Password	
	Sign In

You can configure or edit the username and password for your device by accessing the settings of your base unit and click on the change password.

Settings & Info	
Device information	
Account name	admin
	Change Password

On this page, you can configure the username for your base unit and update your password. Please note that the password must be between 5 and 20 characters in length. Once you have updated it, simply click on the "Update" button.

ਦ	
User Account	
Username	admin
New Password	
Retype Password	
Update Reset	

2.2 Firewall settings

Firewall can be accessed through your gateway's settings by clicking on the button on the upper right,



With this feature you may configure your gateway to allow access to specific IP/MAC or a range of IP/MAC addresses.

Firewall	Settings
----------	----------

This firewall feature enables to disable access to the web interface, SNMP agent or Modbus TCP based on the IP address AND MAC address filters.				
You can use wildcards (*) to allow multiple addresses from a sa	me subnet to access the device			
Your IP: 192.168.11.45 Your MAC address: C0:56:27:39:6E:24				
IP address #1				
IP address #2				
IP address #3				
IP address #4				
IP address #5				
MAC #1	*******			
MAC #2				
MAC #3				
MAC #4				
MAC #5				
Update Reset				

Note that both fields cannot be left blank. The input "*.*.*" will allow all IP and as for allowing all MAC address we need to input "*:*:*:*", they are already typed in by default.

Note: MAC address letters should always be in upper case.

2.3 Enabling and Disabling Web Server

Web Server is one of the newest features included in the latest firmware version. Disabling the web server option restricts the ability to send commands or configure settings. To disable it, simply select "Disable" from the dropdown menu and click "Update".

Web Server	Disable ✓ Enable	
Update	Reboot	Legal Info

Once you click on "Disable", a pop-up message will appear asking if you want to disable the web server. After you click "Ok" and then "Update", the web server is disabled. You will not be able to load the web server, send commands or configure it.

Ĭ			\smile	
е	Are you sure you want to disable the webserver?			
eway		Cancel	ОК	-
r				

After you disable the web server, your base unit will automatically reboot, and you will see this reflected in your base unit's OLED.



After the base unit reboots, a message will appear to inform you that the Web server is Disabled.

Please note that a common mistake users make when unable to access the base unit is that the web server is turned off. To verify, reboot the base unit and check the OLED display for the message indicating that the web server is Disabled or off.

To enable it back, you will need to be near the device as you need <u>to press the reset button 4</u> <u>times within 2 seconds</u>. This is an additional security measure added to the Web Server feature, as you will need to be physically present with the device to manually re-enable it.



After you enable the web server again, a message will appear on the Base Unit's OLED display indicating that the Web server is Enabled, and you may now access your web server again.



3 Base Unit features and configuration

3.1 Int. ping

Once you have updated to firmware 8.0 and above an internal ping check is added on our sensor list where in you can check the status of your connection to a specific URL or IP address in which a great example is trying to ping another gateway (BASE-XX).

How to set it up

1. Access your gateway and click on the "PING" option.

Sensors				
Status	Туре	Name	Value	Warning Range
	Temperature	Int. Temp1	28.98 °C	<18 OR >37

2. Make sure to click on "Enable Ping"

Ping Setting

This optional PING sensor enables you to monito to the internet, then you can also use a public IP.		You can check ag	ainst an internal IP address to see	If the internal network is still operation	al. If the device can connect
Enable Ping sensor					-
Domain name OR IP address	www.serversche	ck.com.			
Ping timeout	60	8	Lec		
Uptein Reset					

3. Input the URL / IP address you wanted you check and then click on UPDATE.

I the IP network link is still reachable. You can check egainst an internal IP address to see if t	the internal network is still operational. If the device can connect
www.serverscheck.com.	
60 ÷ sec	
	www.serverscheck.com.

3.2 Configuring the Fahrenheit / Celsius readings

The default setup is readings in Celsius. However, through a simple switch, the sensor readings can be set to Fahrenheit. Simply connect to the Base Unit, go to the menu option and click on settings.

રુ	
Sensor Status	
Alert History Settings	
Buy new sensors	
myServersCheck & Support	

Change the value from Celsius to Fahrenheit under general settings.

General settings Device Name	SensorGateway
Device Location	Data Center
Sensor Polling	every 1
Temperature Unit	Celsius
OLED Screen	Enable
Repeat Alarm Time	every 5

3.3 ICMP server

The Internet Control Message Protocol (ICMP) is widely used for diagnostic purposes

Network Settings	
Fixed IP	-
DHCP	0
ICMP Server	

By Default your ICMP Server is enabled, you may disable it through your network settings page.

3.4 Sensor polling/refresh time

Can also be found under general settings, the unit dictates the time the gateway polls/gets the data from any of the sensors connected to it. Recommended setting is from 1-5 seconds.

General settings	
Device Name	SensorGateway
Device Location	Data Center
Sensor Polling	every 1
Temperature Unit	Celsius
OLED Screen	Enable
Repeat Alarm Time	every 5

3.5 Configuring internal clock of the Base Unit

To modify the internal clock, click on the menu option and then go to settings and then click on "Update Time". You can either set it manually or have it synchronized with a timeserver as shown in the picture below. Click on **Update** when done

SNTP Settings	
Use SNTP Time Server	
Current Device Date & Time	14 Feb 2019 01:12:03
Update date time to	14 • February • 2019 • - 1 •: 10 •
IP Address SNTP Time Server	us.pool.ntp.org
Time Zone	+8 (configured)
SNTP Sync Frequency	every 1
Update Reset	

Following table provides a list of time zones in UTC offset per country.

CountryUTC time offsetCountryAMAfghanistan+04Albania*+01Algeria+01Malawi	UTC time offset +01 +03 +02 +08 +05		
AMAfghanistan+04Macedonia *Albania *+01MadagascarAlgeria+01Malawi	+01 +03 +02 +08		
Afghanistan+04Macedonia *Albania *+01MadagascarAlgeria+01Malawi	+03 +02 +08		
Albania*+01MadagascarAlgeria+01Malawi	+03 +02 +08		
Algeria +01 Malawi	+02 +08		
	+08		
Andorra* +01 Malaysia	+05		
Angola +01 Maldives			
Antigua and Barbuda –04 Mali	±00		
Arg'entina –03 Malta*	+01		
'Ar'enia '04 Marshall Islands	+12		
Australia – 5 time zones Mauritania	±00		
Western Australia'08 Northern Territory +09 Mauritius	+04		
South 'Australia * +09 Austra'lian C'apital Mexico * – 3 time zones	Mexico * - 3 time zones		
Territory * +10 New South Wale's * +10 The state o'Baja California	The state o'Baja California –08 The states of		
	Baja California Sur, Chihuahua, Nayarit,		
Howe Island [*] +10 M'c'uraei Is'and +11 Sinaloa and Sonora -07 M	Sinaloa and Sonora -07 Most of Mexico -06		
Australian Overseas Territories – 6 time Micronesia – 2 time zones	Micronesia – 2 time zones		
Zones The states of Chuuk and Y	The states of Chuuk and Yap +10 The states		
Heard Island and McDonald Islands +05 of Kosrae and Pohnpei +1:			
Cocos (Keeling) Islands +06 Christmas Island Moldova *	+02		
+07 Ashmore and Cartier Islands +08 Coral Monaco*	+01		
Sea Islands +10 Norfolk Island +11 Mongolia * – 2 time zones			
Austria* +01 Provinces of Khovd, Uvs, E	Bavan-Olgii +07		
Azerbaijan * +04 Ulaanbaatar and most of t	· •		
B Montenegro *	+01		
Bahamas* –'5 Morocco [*]	±00		
Bahrain +03 Mozambique	+02		
Bangladesh +06 Myanmar (Burma)	+06::		
Barbados –04 N			
Belarus +03 Namibia	+01		
Belgium* +01 Nauru	+12		
Belize -06 Nepal	+05:45		
Benin +01 Netherlands *	+01		
Bhutan +06 Netherlands Overseas Ter	rritories - 1 time		

Delivie	-04	70700				
Bolivia Bospia and Horzogovina *	-04 +01	zones	landa 04			
Bosnia and Herzegovina * Botswana	+01	Aruba –04 Caribbean Netherlands –04 Curaçao –04 Sint Maarten –04				
	+02	3				
Brazil – 4 time zones		New Zealand * +12 New-Zealand's Dependent Territories – 4				
Acre and Southwestern Amaz		-	erritories – 4			
part of the Amazonas State, N		time zones				
Mato Grosso do Sul, Rondôni		Niue – 11 Cook Islands – 10 C	hatham Islands			
The Southeast, the South, the		+12:45 Tokelau +13	<u>0</u> (
Regions (except some islands		Nicaragua	-06			
Federal, Tocantins, Pará, Ama		Niger	+01			
on the east coast of Brazil (Fe		Nigeria	+01			
Noronha, Trindade, Martin V	,	North Korea	+09			
Rocas, Saint Peter and Paul R		Norway*	+01			
Brunei	+08	0	.04			
Bulgaria*	+02	Oman	+04			
Burkina Faso	±00	P	.05			
Burundi	+02	Pakistan	+05			
C Caba) (anda	01	Palau Palaatina *	+09			
Cabo Verde	-01	Palestine *	-06			
Cambodia	+07	Panama Danua Naur Cuinas	-05			
Cameroon	+01	Papua New Guinea	+10			
Canada - 6 time zones		Paraguay	-04			
Larger western part of British		Peru	-05			
Tungsten and the associated	-	Philippines	+08			
in Northwest Territories, Yuk		Poland *	+01			
some eastern parts of British		Portugal *	±00			
Northwest Territories, Nunav		Portugal - Azores *	+01			
102°W and all communities in		Q	100			
Region), Lloydminster – 07 Ma		Qatar	+03			
Nunavut (between 85°W and		R Demonia *	102			
western Southampton Island (Northwestern Ontario west		Romania * Russia – 9 time zones	+02			
		Kaliningrad Oblast +03 Most	ofFurancan			
some exceptions and Big Trou		Russia and all railroads throu				
east of 90°W), Saskatchewan Lloydminster -06 Nunavut ea		+04 Bashkortostan, Chelyabi	-			
entire Southampton Island, O		Khanty–Mansia, Kurgan Obla				
90°W (except Big Trout Lake		Oblast, Perm Krai, Sverdlovs	-			
part of Quebec –05 Labrador		Tyumen Oblast, and Yamalia				
southeastern tip), New Bruns		Altai Republic, Kemerovo Ob				
Scotia, Prince Edward Island,		Novosibirsk Oblast, Omsk Ol	,			
Quebec –04 Labrador (south	•	Oblast +07 Khakassia, Krasn				
Newfoundland -03	castern),	Tuva +08 Buryatia and Irkuts	,			
Central African Republic	+01	Amur Oblast, western Sakha				
Chad	+01	Zabaykalsky Krai +10 The Je				
Chile	-04	Autonomous Oblast, Khabar				
Chile - Easter Island	-06	Primorsky Krai, central Sakha				
China	+08	Sakhalin Island +11 Magadar				
Colombia	-05	Sakha, Kuril Islands, Chukotk				
Comoros	+03	Kamchatka Krai +12				
Congo, Republic of the	+01	Rwanda	+02			
Congo, Dem. Rep Kinshasa	+01	S				
Congo, Dem. Rep		St. Kitts and Nevis	-04			
Lubumbashi	+02	St. Lucia	-04			
Costa Rica	-06	St. Vincent and The				
Cote d'Ivoire	±00	Grenadines	-04			
Croatia*	+01	Samoa	+13			
Cuba*	-05	San Marino *	+01			
Cyprus *	+02	Sao Tome and Principe	±00			
Czech Republic	+'1	Saudi Arabia	+03			
D		Senegal	±00			
L						

Denmark*	+01	Serbia*	+01	
Denmark's Dependent Territ	ories * – 4 time	Seychelles	+04	
zones		Sierra Leone	±00	
The most of Greenland, includ		Singapore	+08	
south coast and west coast -0		Slovakia *	+01	
Thule Air Base -04 Greenland		Slovenia *	+01	
Ittoqqortoormiit –01 Faroe Is		Solomon Islands	+11	
Djibouti	+03	Somalia	+03	
Dominic	-04	South Africa	+02	
Dominican Republic	-04	South Korea	+09	
E		South Sudan	+03	
Ecuador	-05	Spain *	+01	
Ecuador - Galapagos Province	e -06	Spain - Canary Islands *	±00	
Egypt	+02	Sri Lanka	+05	
El Salvador	-06	Sudan	+03	
Equatorial Guinea	+01	Suriname	-03	
Eritrea	+03	Swaziland	+02	
Estonia *	+02	Sweden*	+01	
Ethiopia	+03	Switzerland *	+01	
F		Syria *	+02	
Fiji	+12	Т		
Finland *	+02	Taiwan	+08	
France *	+01	Tajikistan	+05	
French Overseas Territories	- 10 time zones	Tanzania	+03	
French Polynesia - Tahiti Islar	nd –10 French	Thailand	+07	
Polynesia - Marquesas Island	s – 09 French	Timor-Leste	+09	
Polynesia - Gambier Islands -	09 Clipperton	Тодо	±00	
Island -07 Guadeloupe -04 N	1artinique –04	Tonga	+13	
Saint Barthelemy -04 Saint №	•	Trinidad and Tobago	-04	
French Guiana –03 Saint Pier	re and	Tunisia	+01	
Miquelon * -03 Mayotte +03	Réunion +04	Turkey*	+02	
Kerguelen Islands +05 New C		Turkmenistan	+05	
Wallis and Futuna +12		Tuvalu	+12	
G		U		
Gabon	+01	Uganda	+03	
Gambia	±00	Ukraine	+02	
Georgia	+04	United Arab Emirates	+04	
Germany*	+01	United Kingdom *	±00	
Ghana	±00	British Overseas Territories -	9 time zones	
Greece*	+02	Pitcairn Islands –08 Cayman I		
Grenada	-04	Anguilla –04 Bermuda –04 Br		
Guatemala	-06	Islands –04 Montserrat –04 T	-	
Guinea	±00	Caicos Islands –04 Falkland Is		
Guinea-Bissau	±00	South Georgia and the South S		
Guyana	-04	Islands -02 Saint Helena ± 00 Ascension and		
H		Tristan da Cunha ±00 Guerns		
Hait'i *	-05	Man * ±00 Jersey * ±00 Gibral	•	
Honduras	-06	Akrotiri and Dhekelia * +02 Bi		
Hungary *	+01	Ocean Territory +06		
	-	United States of America * – 6	time zones	
Iceland	±00	Hawaii, most of the Aleutian Is		
India	+05	Most of the state of Alaska –09 The states on		
Indonesia – 3 time zones		the Pacific coast plus Nevada, parts of Idaho		
Islands of Sumatra, Java, prov	inces of West	-08 Arizona, Colorado, Monta		
Kalimantan and Central Kalim		Mexico, Utah, parts of Idaho, I		
Islands of Sulawesi, Bali, prov		Oregon, North Dakota, South		
Nusa Tenggara, West Nusa Te		-07 Gulf Coast, Tennessee Va		
Kalimantan and South Kalima		Interior Highlands, Great Plai		
Provinces of Maluku, North M		Texas –06 The states on the A		
and West Papua +09	and and a second	the eastern two-thirds of the	,	
			erne vancy,	

Iran*	+03	most of Michigan –05	
Iraq	+03	US Dependent Territories -	7 time zones
Ireland *	±00	Baker Island –12 Howland Is	land –12
Israel *	+02	American Samoa –11 Kingm	an Reef –11
Italy*	+01	Midway Islands –11 Palmyra	Atoll – 11 Jarvis
J		Island – 10 Johnston Atoll – 1	.0 Navassa
Jamaica	-05	Island -05 Puerto Rico -04 l	JS Virgin Islands
Japan	+09	-04 Guam +10 Northern Ma	riana Islands
Jordan*	+02	+10 Wake Island +12	
К		Uruguay	-03
Kazakhstan - Oral, Aktobe	+05	Uzbekistan	+05
Kazakhstan 'Almaty, Astana	+06	V	
Kenya	+03	Vanuatu	+11
Kiribati - 3 time zones		Vatican City (Holy See) *	+01
Gilbert Islands +12 Phoenix Is	slands +13 Line	Venezuela	-04
Islands +14		Vietnam	+07
Kosovo*	+01	Y	
Kuwait	+03	Yemen	+03
Kyrgyzstan	+06	Z	
L		Zambia	+02
Laos	+07	Zimbabwe	+02
Latvia *	+02		
Lebanon *	+02		
Lesotho	+02		
Liberia	±00		
Libya	+01		
Liechtenstein *	+01		
Lithuania *	+02		
Luxembourg *	+01		

3.6 Setting threshold values in the Base Unit for alerting

Connect to the Base Unit and click on "EDIT" located on the upper right corner just below the menu button. You will now see the button change into "Updated and Reset"

Sensors

Status	Туре	Name	Value
	Temperature	Int. Temp1	29.61 °C
	Zigbee 1	WT-0221	25.93 °C

I lood as here	Danat
COLORED D	PV05/01
Contraction of the second s	

Warning Range				Down Range		Repeat Alarm	Email	SMS	SNMP Trap	Se	t Output To	
<	18	0	<	15	8	0	0	۵	0	DISABLE	•	•
>	37	ŝ	>	41	0							
<	18	8	<	15	8	0	0	0	0	DISABLE	•	•
>	30	\$	>	29								

Status: this shows if the internal sensor or the external sensor probe is working or not **Type:** type of reading for the sensor

Name this is the name of the sensor and will be used in alerting

Value: this is the latest reading for both the internal sensor and the external sensor probe Warning range: below the minimum value and above the maximum value a WARNING alert will be sent. Current value color will change to orange

Down range: below the minimum value and above the maximum value a DOWN alert will be sent. Current value color will change to red. DOWN overrules WARNING

Repeat alarm: when set then this will trigger an alert to be sent every 5 minutes <u>Only if the</u> status is on a DOWN state.

Email: when checked then email alerts will be sent for this sensor value

SMS: When checked then SMS or Voice call alerts will be sent for this sensor value **SNMP trap:** when checked then a SNMP Trap will be sent for this sensor value

Note that the repeat alarm is customizable from the settings menu under General Settings.

3.7 Alarm and Ambient VOC

Ambient VOC refers to the calculated average of the last 10 readings from each individual VOC sensor. This means that if you have multiple sensors, each one maintains is own rolling averaged based on lasts 10 readings. This value provides a more stable indication of VOC levels over time, helping to smooth out sudden spikes.

VOC Alarm is a separate feature that triggers when a sensor detects VOC levels above a predefined threshold. This threshold is typically set to alert users of potentially harmful concentrations in real time. While the **Ambient VOC** provides a trend, the **VOC Alarm** highlights urgent conditions that may require immediate attention.

Both the **Warning Range** and **Down Range** thresholds for Ambient VOC can be configured based on user requirements by click the **"Edit"** button at the upper right side of the sensor homepage.

In the example shown in the screenshot below:

- The Warning Range is set to >200, meaning if the Ambient VOC value reaches 201 or higher, the VOC Alarm status will change to "Alarm", indicating that the VOC level has entered the warning stage.
- The **Down Range** is set to >400, meaning if the Ambient VOC value reaches 401 or higher, the status will be considered as "**Down**", and the VOC Alarm status will again change to "Alarm", this time indicating that the VOC level has crossed into the down range.

Sens	ors						Enable	e Mainten	ance Mode		E
Status	Туре	Name	Value	Warning Range	Down Range	Repeat Alarm	Email	Alert+	SNMP Trap	Set Output T	ō
	Temperature	Int. Temp1	32.3 °C	<18 OR >37	<15 OR >41					DISABLE \$	
	Fault	Int. Fault1	ОК	-	SET					DISABLE \$	- +
	Ambient VOC	Ambient VOC1	483.67	>200	>400					DISABLE \$	
	VOC Alarm	Alarm VOC1	Alarm	-	SET					DISABLE \$	- +
	VOC Index	VOC Sensor5	487	>100	>400					DISABLE \$	- 4
	Pure H2	Pure H2 Sensor2	0 %LEL	>25	>50					DISABLE \$	- 4

4 Base Unit alerting feature

4.1 Email alerting

The InfraSensing sensors can generate autonomous alerts via SNMP Traps and also via email. Make sure that the email checked as one of the alerting options for any of your sensors.

Repeat Alarm	Email	SMS	SNMP Trap
	\checkmark		

To setup email alerting, Go to the menu option, then settings and then click on the **Email** option under Industrial and external use.

Industrial & external co	mmunications			
SNMP		Cloud	Email	
Modbus	-		SMS	0

This screen consists of 3 main parts: Mail server settings

Mail heading settings (from, to, subject ...) Mail content (body)

NOTE : Please make sure you have whitelisted us in your system so that these emails can be delivered without delay or disruption. Also, we don't currently support gmail as of the moment, only outlook and yahoo.

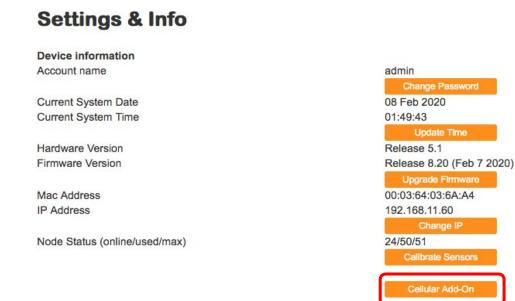
Email Alert	
Enable Email Alerts))))
SMTP Server	mail.serverscheck.email
SMTP Port	465
SSL (v3)	
Use SMTP Authentication	
SMTP Username	Test
SMTP Password	
From Email	Manual@serverscheck.com
To Email	Customer@gmail.com
сс	

Note: Sending to multiple recipients can be separated by a comma however in respect to the "To" and "Cc" fields, To is limited to 90 characters and Cc is limited to 70, So if you need to send an email to multiple addresses then it is advised that you create a "group mail" and use that instead.

For email alerting, InfraSensing supports standard outgoing mail servers like the ones used by ISP's (SMTP relay servers) or corporate SMTP mail servers requiring standard username & password authentication. SSL mail servers are not supported. For use of SSL, web-based emails are recommended.

In some cases, it may happen that you don't have a non-SSL server available in your network or from your ISP. In such situations, we have 4 alternative solutions that may fix the issue.

4.2 Email alerts using the ADDON-LTE



Access the base unit and go to settings, under settings click on the Cellular Add-On button and then scroll down to access the email configuration.

Note: (see section for the ADDON-LTE) The built-in email feature of the Base Unit will be disabled upon using the ADDON-LTE

-Lie Comg	
SMTP Server	
dimit denvoi	
SMTP Port	
non Para an anna da	
Secure connection	✓ None
Rea	SSL/TLS
Use SMTP Authentication	STARTTLS
	() III
SMTP Username	
SMTP Password	
and the second se	
0.50% Peakod	
From Email	
To Email(s)	
to Entan(s)	
Email Subject	ServersCheck Sensor Alert
netter	
Append to Email this text	
100 M	
. 📕	
	Send test Email
	avend leps chrain
Linal Ro And	
	A.
	Rev kardina
tas	No fa
Fault	0 4.0000
	4 - SMB

Input your email settings and perform a test mail, the ADDON-LTE is tested to work on our free email server, Gmail and yahoo mail. (Continue reading for sample email set up).

4.2.1 Gmail as e-mail server (<u>https://mail.google.com</u>)

To use Gmail as a mail server, you need to have a Gmail account. You may sign up for one at https://mail.google.com and port 25 should not be blocked by your ISP.

THINGS TO SET UP FOR GMAIL

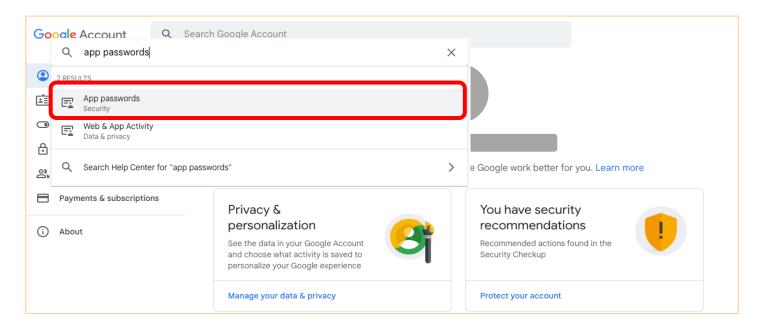
Below are the instructions on how to set it up.

1. Log in to your Gmail Account and access "Manage your Google Account."

🔰 Gmail	Q Search in mail 프	0 \$ III e
Compose	□· ɑ :	This account is managed by infrasensing team.
Inbox 57		
☆ Starred ① Snoozed		Manage your Google Account
⊳ Sent		C Recommended actions
Drafts 1 V More		음 Add another account
Labels +		[→ Sign out
LUDUS		Privacy Policy • Terms of Service

2. On the search bar type in "App Passwords."

Note : Make sure that your 2-factor authenticator is enabled so that you can access the "App Passwords"



3. Once you click **"App Passwords"** you will see this pop up message. Just click **"Select App"** and choose **"Other"**

	App pa	sswords		
		you sign in to your Google Account from apps on devices that d only need to enter it once so you don't need to remember it. Lea		
	You don't have any app passwords. Select the app and device you want to generate the app password for.			
	Select app	▼ Select device ▼		
Selec Mail	t app		GENERATE	
Calen	dar			
Conta	acts			
YouT	ube			
Other	(Custom name)			

- 4. After you choose "Other" you may type in the name of your device or any name you desire.
- 5. Once you put in the name of your device, you may now click "Generate" so that it will generate you a password that you need to save for later.

← /	App passwords
	asswords let you sign in to your Google Account from apps on devices that don't support 2-Step ation. You'll only need to enter it once so you don't need to remember it. Learn more
You	don't have any app passwords.
Sele	ect the app and device you want to generate the app password for.
	Base Unit X
	GENERATE

6. After you click "Generate" a pop message will appear. This is now your app password for your device.

Important: Make sure to copy and securely store this password in your notes for future reference. Once you close this pop-up message, the password will not be retrievable. In case you lose it, you will need to follow the same steps again to generate a new password.

Generated app password				
	Your app password for your device			
	tezy gpyj eohp aauc			
	How to use it			
Email securesally@gmail.com	Go to the settings for your Google Account in the application or device you are trying to set			
Password	up. Replace your password with the 16- character password shown above. Just like your normal password, this app			
•••••	password grants complete access to your Google Account. You won't need to remember it, so don't write it down or share it with			
	anyone.			
	DONE			

Non-Secure Settings SMTP Server: aspmx.l.google.com SMTP Port: **25** SMTP Authentication: **Off / Unchecked** From address: <u>yourgmailname@gmail.com</u> To address: same as from address

The emails will arrive in your SPAM filter unless you whitelist the IP address on Gmail from which you are sending the alerts.

For SSL, the settings will be: SMTP Server: smtp.gmail.com SMTP Port: **465** SMTP Use SSL: **Checked** SMTP Authentication: **Checked** SMTP Username/Password: **Filled out** From/To address: Filled out. Not required to be the same.

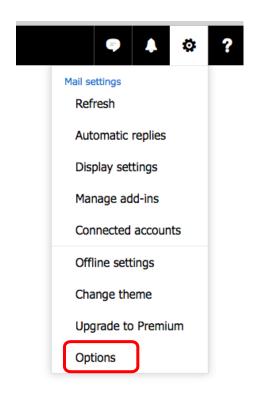
For TLS, the settings will be: SMTP Server: smtp.gmail.com SMTP Port: **587** SMTP Use SSL: **UnChecked** SMTP Authentication: **Checked** SMTP Username/Password: **Filled out** From/To address: Filled out. Not required to be the same.

Note: Only version 5 Base Units are supported with Gmail's SSL ever since they offered RSA 2048-bit encryption.

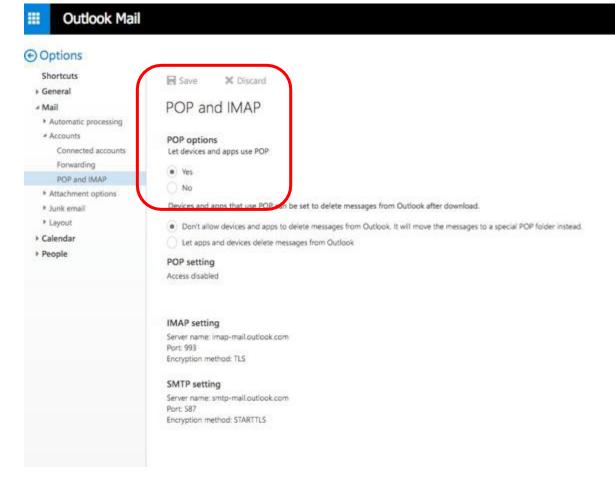
Outlook mail is another example of an SMTP server, which can be used on the gateway

However, you have to turn the option for "Let devices and apps use POP" to YES and then make sure you save it.

To do so just log in onto your account and click on the settings lcon beside your log-in name. Then choose options.



Then Click on "Mail" on the left panel to expand it then expand "Accounts" then click on "POP and IMAP"



Now choose YES under "let device and app use POP" and save it.

You can now set the gateway using the SMTP settings of outlook mail.

For TLS, the settings will be: SMTP Server: smtp-mail.outlook.com SMTP Port: **587** SMTP Use SSL: Un**Checked** SMTP Authentication: **Checked** SMTP Username/Password: **Filled out** From/To address: Filled out. Not required to be the same.

Note:

Check if your account allows User Consent to apps:

- 1. In the admin center, go to Settings>OrgSettings>Services page, and select User Consent to apps.
- 2. On the User consent to apps page, select the option to turn user consent on or off.

4.3 Slack channel integration via e-mail alerts

To receive alerts via slack we first need to have the email app integrated into our slack account

	Email
	App Info Settings
	This app was made by Slack.
	This app was made by a member of the Slack team to help connect Slack with a third-party service; these apps may not be tested, documented, or supported by Slack in the way we support our core offerings, like Slack Enterprise Grid and Slack for Teams. You may provide
Add to Slack	feedback about these apps at feedback@slack.com.
	It only uses data Slack already has access to (view our Privacy Policy to learn more). By
kpp help	enabling and/or using this app, you may be connecting with a service that is not part of
ferms	Slack.

As shown on the image above we need to add the email app into our slack account.

Email Send emails directly to a channel in	Slack.
	tress that you can use to subscribe to important notifications from any service. Emails sent to choice. This integration is available to workspaces on the Slack Standard Plan and above.
Example uses include:	
	vebsite into your company's #support channels instantly. vents, traffic closures, domain name renewals) can be pointed at your company's #general
Each integration has its own email address ar	nd a customizable name and icon, and you can create as many of them as you like.
Please note that the following limits apply to	emails sent to this integration:
The combined headers and body of an ema When combined with attachments, an ema There is a maximum of 20 attachments per You can address each email to one integrat	iil cannot be larger than 30 MB. • email.
Post to Channel	
Start by choosing a channel where email will be posted.	• Email alerts v
	Add Email Integration

Once we add the app you will be prompt to choose a channel where the alerts will be received

Email Address	
Emails sent to this address will be imported into Slack.	2 http://www.com/actional.com/
	 Hide this address Anyone in your workspace can view this email address and send email to it.
Post to Channel	
Emails will be posted here. They will be kept private if posted to a private group or direct message.	o Email alerts v
Descriptive Label	
Use this label to provide extra context in your list of integrations (optional).	Optional description of this integration
Customize Name	
Choose the username that this integration will post as.	email

Once done you will then see the email address that you can use to receive alerts, you can place the email address on the "To" or "Cc" field see **section 4.1.**

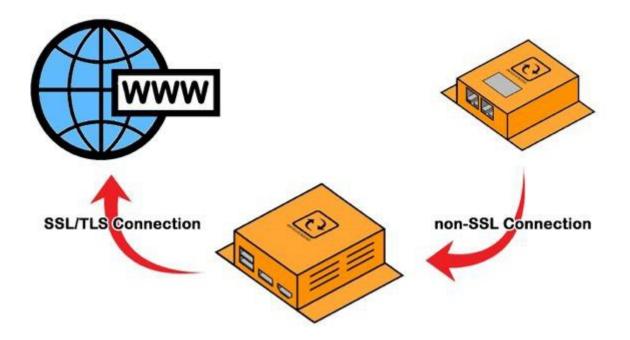
4.4 Tunneling an SSL connection

In this guide we will be using the STunnel software installed on our InfraSensing Monitoring Appliance.

You can use STunnel to allow non-SSL devices such as the Base Unit to connect to a secure mail server in which the Base Unit will connect to STunnel using non-SSL SMTP then STunnel will bridge the connection to for example Google Mail using an SSL connection.

Network Diagram

The Image below will show that the gateway sends via Non-SSL smtp connection going to the monitoring appliance, the data is then relayed using an SSL/TLS connection going to Gmail's smtp server.



How to do it:

- Download and Install the STunnel Software (can be downloaded from: <u>http://www.stunnel.org/</u>)
- 2. During the installation you will be prompt to input details, which will be needed to created certificates.

> Access the config folder as shown in the image below and open stunnel.conf using a text editor.

Ex. Notepad, Notepad++

This PC > Windows (C:) > Program Files (x86) > stunnel > config				
□ Name	Date modified	Туре	Size	
a-certs.pem	07/06/2017 4:22 A	PEM File	254 KB	
] openssl.cnf	17/01/2017 4:12 A	CNF File	2 KB	
📕 stunnel.conf	28/01/2017 5:04 PM	CONF File	5 KB	
stunnel.conf.old2	30/08/2017 5:55 PM	OLD2 File	1 KB	
stunnel.pem	31/08/2017 5:20 PM	PEM File	4 KB	

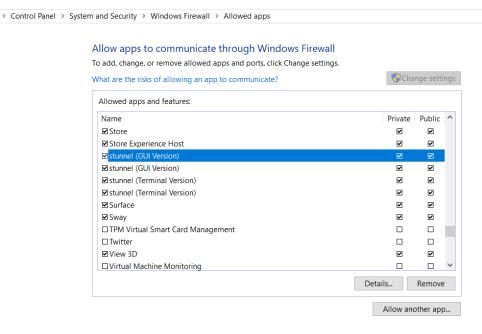
4. You should be able to see sample configuration commands. You can either edit the current or add the configuration below. Then save the file.

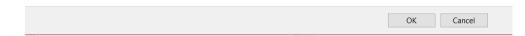
[gmail-pop3] client = yes accept = 110 connect = pop.gmail.com:995 verifyChain = yes CAfile = ca-certs.pem checkHost = pop.gmail.com OCSPaia = yes

```
[gmail-imap]
client = yes
accept = 143
connect = imap.gmail.com:993
verifyChain = yes
CAfile = ca-certs.pem
checkHost = imap.gmail.com
OCSPaia = yes
```

```
[gmail-smtp]
client = yes
accept = 25
connect = smtp.gmail.com:465
verifyChain = yes
CAfile = ca-certs.pem
checkHost = smtp.gmail.com
OCSPaia = yes
```

5. Make sure STunnel is added on your allowed application in the firewall list





6. Click on the desktop icon of the STunnel. You can also see and choose options on the Icon created on the system tray.



7. You should see a result like the image below once successful.

Stunnel 5.42 on Win32 File Configuration Save Peer Certificate Help 2017.08.31 17:59:14 LOG5[main]: stunnel 5.42 on x86-pc-msvc-1500 platform 2017.08.31 17:59:14 LOG5[main]: Compiled∕running with OpenSSL 1.0.21-fips 25 May 2017 2017.08.31 17:59:14 LOG5[main]: Threading: WIN32 Sockets:SELECT, IPv6 TLS:ENGINE, FIPS, OCSP, PSK, SNI 2017.08.31 17:59:14 LOG5[main]: Reading configuration from file stunnel.conf 2017.08.31 17:59:14 LOG5[main]: UTF-8 byte order mark detected 2017.08.31 17:59:14 LOG5[main]: FIPS mode disabled 2017.08.31 17:59:15 LOG5[main]: Configuration successful]

8. Check the IP address of the Appliance/Computer. In this example our Monitoring Appliance is at 192.168.9.16. (Note: One method to get the IP address of the Monitoring appliance is by opening a command prompt and typing in the command "ipconfig")

an Administrator: Command Prompt
Microsoft Windows [Version 10.0.15063] (c) 2017 Microsoft Corporation. All rights reserved.
C:\WINDOWS\system32>ipconfig
Windows IP Configuration
Wireless LAN adapter Local Area Connection* 2:
Media State Media disconnected Connection-specific DNS Suffix . :
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix .: domain.name Link-local IPv6 Address : fe80::4411:48b:d06c:a5a8%2 IPv4 Address : 192.168.9.16 Subnet Mask : 255.255.255.0 Default Gateway : fe80::213:33ff:fef3:569c%2 192.168.9.1
Tunnel adapter Local Area Connection* 11:
Media State Media disconnected Connection-specific DNS Suffix . :
C:\WINDOWS\system32>

9. Access your gateway and go to email alerts. Then configure as shown in the image. (**192.168.9.16** is the IP of the Monitoring Appliance where STunnel is installed)

Email Alert	
Enable Email Alerts	
SMTP Server	192.168.9.16
SMTP Port	25
SSL (v3)	
Use SMTP Authentication	
SMTP Username	test
SMTP Password	
From Email	Manual@serverscheck.com
To Email	Customer@gmail.com
СС	
	We recommend the use of distribution group
Email Subject	
Email Body	

10. Then click on submit and check if the email was sent successfully.

4.5 Mail service like AuthSMTP.com

If you don't have a non-SSL mail server on your network and you don't want to use STunnel and you can't use Gmail because your operator blocks it, then we could recommend AuthSMTP.com which provides a solid SMTP relay service.

With AuthSMTP.com you can subscribe to use their relay servers on a port such as 2525 while using standard authentication (non-SSL).

More information on http://www.authsmtp.com

Note:

If you need to send alerts to multiple recipients, then the best option is to create a group in your mail server to send out the email alerts to multiple people.

In the email body we suggest to put in the location of the sensor. When you have multiple sensors, a user easily knows where to look for when receiving the alert.

When done click on the **Submit** button. It will now try to send a test message to the mail account.

Below is the test email as received in Outlook 2010.



4.6 SMS alerting from Base Unit

4.6.1 SMS alerts via ADDON-LTE

SMTP Server		
SMTP Port		
Secure connection	✓ None SSL/TLS	
Use SMTP Authentication SMTP Usemame	STARTTLS	
SMTP Password		
From Email		
To Email(s)		
Email Subject	ServersCheck Sensor Alert	
Append to Email this text		
	Send test Email	

Access the base unit and go to settings, under settings click on the Cellular Add-On button to access the configuration.

Note: The built in Premium SMS feature of the Base Unit will be disabled upon using the SMS functionality of the LTE addon

ADDON-LTE Config	
Primary male	0
Backup made	•
SMIPN	
SAFI APN	
SMI Usemane	
SIM1 P	IN
Attor lists Lating	
SIM1 A	PN
Active SM Network Name	
	sername
SINTO	sentance
SVS Respects	
Append to 2010 market	assword
Children	
SVIP Server	
Skille Pon Secure connection	8
Becce comedian	Nes
Use SNTP Autoritization	Cm
SVTP Generality SVTP Persent	
and Fallent	
From Email	
To Email (s)	
Email Balged	Seneral Deck Senar Ref.
Appared to Detail Headed	
	Bert half frai
SPS Status Fix	No fa
Saletties Pound Latitude	
Longitude	5.889
Lines	

Enter the SIM information, if the SIM does not have a security PIN then leave it blank.

ADDON-LTE Config					
Primary mode		0			
Babup male					
SMIPN			SAG PN		
DMI APK			BAD AM		
SMI Usename			BNG Overane BNG Passeriel		
SMI Passachi			DAG Passacra		
Add on Status Law Entry		Connected			
Network Dates Actus M Network Netwo Signal Revi Real MS		9A41 20A40 SANKET 128 16 467/0800421022114			
SVS Recparts					
Appoint to SMS this foot	SMS Recipients Append to SMS this text				
	•				
SM19 Server	•				
SUTP Post	•				
Becure connection	•		Send test SMS		
Use SVTP Automication SVTP Usename					
\$41P Passent					
Per Enai					
To Email(s)					
Email Bulged		ServersCheck Server Ref.			
Append to Email this level					
				A	
		Sami test Emai			
0PS Status Pa Edulities Flucid Laffold Laffold		No. 15 0 0.00000 0.00000			
Uptime Reset					

A maximum of 5 recipients can be added separated by a comma.

					Update
	Repeat Alarm	Email	SMS	SNMP Trap	Set Output To
	0	0	۵		DISABLE -
٢	0	0			DISABLE

Make sure that the SMS checkbox is ticked to receive alerts via SMS for the sensors you are monitoring.

4.6.2 SMS alerts via my.infrasensing premium credits

Requirements for SMS alerting: An active account created on <u>https://my.infrasensing.com</u> Firmware 2.10 or higher on Base Units Outbound communication on port 80 from Base Unit to Internet

For SMS alerting, SMS messages are sent by InfraSensing's SMS Gateway. Base Units make a connection over TCP/IP with the SMS Gateway servers for delivering SMS messages.

As per above requirements you need to create an account first on https://my.infrasensing.com

https://my.serverscheck.com		😇 🏠 🔤 Q. Search
6 🔲 Pokemon Sun / Moo		
	Email address	
	Parasword	
	Sign in	
	Forgot Plateword? Create an Account	
	You can login here with your Premium account details. All Premium accounts	
	have been transferred to this new	
	oustomer portal.	

When you have completed above steps to create your account, then you will receive an email with your username and temporary password to login.

Sensor Cloud	News		Care		Products	
Sensor Cloud login	> latest news from ServersCheck	,	Gare: support & warranty	,	3 sensors & no software registered	>
Alerts	Calibrations		Orders	la l	Account	
325 SMS credita & mail alerta	> 0 active calibrations	>	3 orders found	,	nys.emiguezilitervenscheck.com	0

Note: Premium Credits are required for the SMS & Voice feature, Credits can be purchased through your account.

To check for the configuration and remaining SMS/Voice Call Credit we need to click on the "Alerts" Icon and then "SMS" in the middle of your Home page.

	Purchase Cre		
		odits	
Alert	s UID: ' PIN:		
generate new alert uid			>

You need to note down the following configuration info: the **UID** and **PIN** codes. These have to be entered in the Base Unit in order to have the SMS alerting work. You may also Generate a new alert UID, should you wish to do so.

From the above personal page, you can check your SMS credits status, Upgrade into New Plans or check your SMS alerting history. You can also add additional SMS recipients if you want SMS alerts to be send to multiple mobile numbers.

Now connect to your Base Unit, click on the Menu button and go to settings then click on SMS

Enable SMS & Voice Call	
UID	
PIN	
Update Reset	

Activate the **Enable SMS& Voice Call** option. Then enter the **UID** and **PIN** from your account page. Click on the **Submit** button and wait for an SMS test alert to be sent on your cell phone.

Didn't you receive the SMS test alert? Verify your network settings especially if the DNS server has been configured correctly in the **Network** menu settings. If the DNS server has been correctly defined then make sure that no firewall is blocking outgoing HTTP calls from the Base Unit to the InfraSensing SMS Gateway.

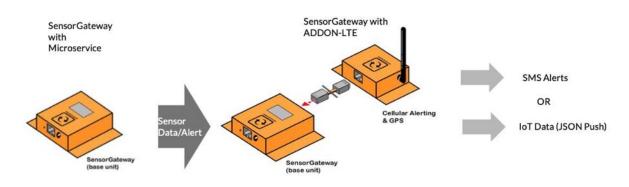
					Update Rese
	Repeat Alarm	Email	SMS	SNMP Trap	Set Output To
0	0	0	۵		DISABLE
0	0	0			DISABLE

Now click on the SMS checkbox to receive alerts via SMS for the item you are monitoring.

4.6.3 Sending SMS alerts and JSON Push data using the Microservice feature

Starting from Base Unit firmware 8.7, the Microservice feature of the Base Unit lets you send SMS alerts and JSON Push data through the ADDON-LTE of another Base Unit that is within the same network.

How the Microservice works

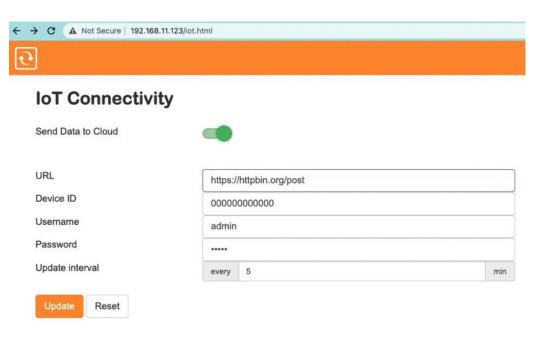


Requirements:

- Base Unit to use the feature
- Base Unit with connected ADDON-LTE(with attached SIM card) to host the Microservice
- Both Base Units must be on the same network

Setting up the host Base Unit

1. On the Web Interface of the Base Unit, go to the Menu > Settings > IoT. You should be able to see a window like this:



- 2. Turn on Send Data to Cloud.
- 3. Fill in the following data:
 - URL that will receive JSON Push data
 - Device ID of the Base Unit (alphanumeric)
 - Username and Password
 - Update interval of the Base Unit to send data over the Microservice
- 4. After the details are entered, click **Update**.

Setting up the Base Unit that will use the Microservice

1. On the Web Interface of the Base Unit, go to Menu > Settings > Microservice.

Take note that the Microservice Settings button will only appear on Base Unit with firmware version 8.7 and up.

You should be able to see a window like this:



Microservice Settings

Send Alerts Through Microservice	••			
Microservice Gateway IP Address	192.168.11.123			
IOT				
Device ID	00000000000			
Username	admin			
Password				
Update interval	every 5	min		
	IOT URL should be configured on the Microservice G	ateway		

Test SMS Recipients	+639991234444	
Test SMS Text	SMS recipients should be configured on the Microservice Gateway test message	
	Send Test SMS	
Update Reset		

- 2. Turn on the Send Alerts Through Microservice.
- 3. Fill in the following data:
 - The Microservice Gateway IP Address (host IP Address)
 - Device ID of the host Base Unit
 - Username and Password of the host
 - Update interval
- 4. Click Update.

Disclaimer:

If you experience issues while using the microservice, they may be due to network-related factors. Please consult your network engineer for support, as connectivity or configuration problems are beyond the scope of the microservice.

Sending Test SMS for Microservice

→ C ▲ Not Secure 192.168.11.	ZZ/microservice.html				
Microservice Setting	IS				
Send Alerts Through Microservice	-				
Microservice Gateway IP Address	192.168.11.123				
Device ID	00000000000				
Username	admin				
Password					
Update interval	every 5	m			
	IOT URL should be configured on the Microservice Gateway				
Test SMS Recipients	IOT URL should be configured on the Microservice Gateway				
	+639991234444				
Test SMS Text	SMS recipients should be configured on the Microservice Gate	way			
	test message				

- 1. On the Microservice Settings, fill in the mobile numbers for the Test SMS Recipients.
- 2. Input the Test SMS Text that the recipients should receive.
- 3. Click Send Text SMS.

4.7 Voice call alerts

Aside from SMS messages, InfraSensing also offers voice calls as an alert by using text-tospeech technology. This feature could be utilized to monitor your mission-critical environments and/or devices. It works by dialing the recipient's number then informing him/her of the error message.

Voice call alerts are configured on the SMS portal and can be used by purchasing the same credits used for your SMS alerts.

To get started, add a new recipient by proceeding to the "Manage Numbers" page of the SMS portal. From there, as seen on the screenshot below, you'll have to choose the alert type for the new recipient which can be for SMS, voice call, or both.

9								
Alert+ / Registered Recipient								ወ
Add Recipient								
The number was deleted from the datab	ase.							
Show 10 v entries							Search:	
Contact 13	Alert Type	Ļ∲	Description	↓∲	Status	Ļ∲	Actions	Ļ∲
+639176203877	SMS		Anj		Active		C 🖻	
Showing 1 to 1 of 1 entries							Previous	1 Next

Fill in the required fields

A Mark / Desidered Desideres / Adductive Marker	
Alert+ / Registered Recipients / Add Mobile Number	
dd a new recipient	
tification type	
Select a notification type	
SMS Alerts	
Voice Call Alerts	
WhatsApp Alerts (Beta)	
Email Alerts (Beta)	
escription	
Example: Mike Phone	
Submit	
pricing:	
credit per SMS sent	
predits per voice call 3 credits per Whatsapp message	

Then select "Voice" or "SMS and Voice"

After which, you'll have to verify the added number by clicking the "Activation Pending" link as seen below.

Number	Alert Type	Description	Status	Actions
	SHSVOICE		Activation Pending	edit/a> delete
	VOICE		Active	edit/an delete

Once activated, we'll have to go the Base Unit's web page to specify the sensors where you want the voice call alert to be used. In order to do so, make sure the SMS and Voice Call alert option on the Settings page is ticked.

					Update
	Repeat Alarm	Email	SMS	SNMP Trap	Set Output To
•			۵		DISABLE
0	0				DISABLE

Depending on the active recipients on the SMS portal, each time the specified sensor sends an alert, you will receive an SMS and/or voice call alert(s). If the active recipient(s) is only enabled for SMS, then you'll only be receiving an SMS alert. Other options are voice only, or both SMS and voice.

4.8 Retest before alarm

Retest before alarm is one of the newest features that verifies alerts to prevent false alarms before triggering a genuine one. This feature also empowers you to specify the number of checks before initiating a real alarm.

To adjust how times the alarm will be checked, navigate to 'Settings' and under 'General Settings', locate 'Retest Before Alarm'. By default, it is set to zero (0), but you can modify it by typing the desired number or using the up and down arrow buttons.

Device Name	SensorGateway	
Device Location	Data Center	
Sensor Polling	every 1	sec
Temperature Unit	Celsius	\$
OLED Screen	Enable	\$
Repeat Alarm Time	everv 5	min
Retest Before Alarm	3	times
Web Server	Enable	\$
	Reboot	Legal Info

Once you input your desired number you may now click on update to apply the changes.

4.9 Maintenance Mode

Maintenance Mode is one of the newest features that can be found in the latest firmware version 9.1.

Enabling the Maintenance Mode allows you to configure the sensors without triggering any alerts, even when the alerting is enabled. In order to enable this feature, just click on the button "Enable Maintenance mode". Please see image below for reference.

Sen	sors						l	Enable N	laintenance Mo	de			Edit
Status	Туре	Name	Value	Warning Range	arning Range Down Range Repeat Alarm		Alarm Email S		SNMP Trap	Set Output To			
	Temperature	Int. Temp1	30.58 °C	<18 OR >29	<15 OR >30		V		1	Output1	\$	ON	×

Once you click "Enable Maintenance Mode," it will change to "Disable Maintenance Mode." To deactivate it, simply click again.

	Edit
Set Output To	o
out1 🗘 ON	N \$
ABLE 💠 -	\$

4.10 Fault Sensor

Fault Sensor is one of the newest features that can also be found in the latest firmware version 9.1. Whenever this feature is enabled, by default it will trigger an alert when a sensor gets disconnected. Also, it will send an alert if a sensor sends a zero value. In order to configure this feature, click on the Fault Sensor button at the bottom of the page, please refer to the image below.

Relay1	OFF	OFF \$	CYCLE
Relay2	OFF	OFF \$	CYCLE
Mixus Sensor			

6	9				
	Fault Config				
А	Enable Fault Sensor				
	Sensor Type	Min Threshold		Max Threshold	
	CO2	400.00	٢	5000.00	٢
	VOC	0.00	۲	500.00	0
В	Trigger Internal Fault If Sensor Sends Zero Value				
С	Reset Missing Sensors Fault	Reset			
	Update				

- A. Enable Fault Sensor When this feature is enabled, it will send out an alert whenever a sensor gets disconnected.
- B. Trigger internal Fault if Sensor Sends Zero Value Enabling this feature will generate an alert whenever a sensor transmit a zero value.
- C. Reset Missing Sensors Fault This option enables you to reset Fault alerts triggered by missing sensors.

5 History

5.1 Alert history

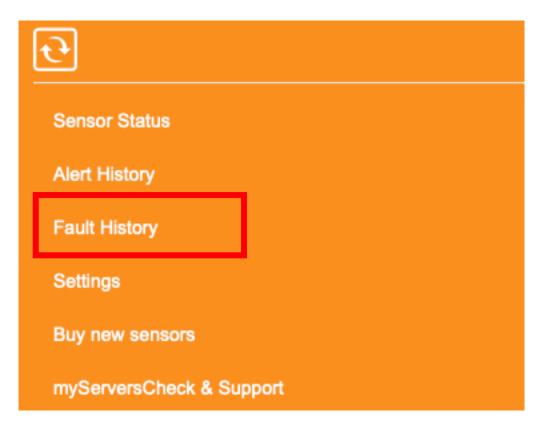
ર
Sensor Status
Alert History
Fault History
Settings
Buy new sensors
myServersCheck & Support

Each time a threshold is hit, an entry is automatically recorded on the log. And as seen on the screenshot, recovery alerts are also included. The Base Unit is able to store up to 2048 entries and are downloadable in CSV format. On column F of the CSV file, the following legend is used for the alerts - 0:Recovery; 1:Warning; 2:Down.

Alert History

2019/02/13 05:30:10	Recover	WT-0221	28.68
2019/02/13 05:29:09	Down	WT-0221	29.06
2019/02/13 05:24:08	Recover	WT-0221	28.87
2019/02/13 05:23:08	Down	WT-0221	29.12
2019/02/13 05:20:06	Recover	WT-0221	28.93
2019/02/13 05:18:06	Down	WT-0221	29.12
2019/02/13 05:16:05	Placover	WT-0221	28.87
2019/02/13 05:15:05	Down	WT-0221	29.18
2019/02/13 05:14:05	Recover	WT-0221	29.00
2019/02/13 05:05:01	Down	WT-0221	29.12
2019/02/13 03:01:40	Warring	WT-0221	26.00
2019/02/13 02:52:55	Pacover.	Ext. Temp2	24.82
2019/02/13 02:52:53	Warring	Ext. Temp2	25.60
2019/02/13 02:12:53	Recover	Ext. Temp2	22.74
2019/02/13 02:12:52	Wanting	Ext. Temp2	25.64
2019/02/13 02:11:53	Recover	Ext. Temp2	23.07
2019/02/13 02:11:50	Warring	Ext. Temp2	27.75
2019/02/13 02:06:50	Recover	Ext. Temp2	24.82
2019/02/13 02:05:35	Warring	Ext. Temp2	27.15
2019/02/13 02:04:50	Recover	Ext. Temp2	24.78
2019/02/13 02:03:30	Down	Ext. Temp2	32.16

5.2 Fault history



Each there's a Fault triggered; an entry is automatically recorded on the log. This can also be downloaded as cvs.

				l
Fault Alert History				
rault Alert History				
Download as csv				
2024/02/21 19:40:42	Fault	Hub Port 7	Probe Missing	Triggered
2024/02/21 19:40:37	Fault	Hub Port 8	Probe Missing	Triggered
2024/02/21 19:39:12	ОК	Particle1	CO2/VOC Limit	Recovered
2024/02/21 17:59:40	Fault	Hub Port 4	Probe Missing	Recovered
2024/02/21 17:50:26	Fault	Hub Port 4	Probe Missing	Triggered
2024/02/21 16:49:37	Fault	VOC Sensor1	CO2/VOC Limit	Triggered
2024/02/21 16:48:21	Fault	VOC Sensor1	CO2/VOC Limit	Triggered
2024/02/21 15:11:20	Fault	VOC Sensor1	CO2/VOC Limit	Triggered
2024/02/21 15:09:08	Fault	VOC Sensor1	CO2/VOC Limit	Triggered
2024/02/21 14:34:11	Fault	Hub Port 3	Probe Missing	Triggered
2024/02/21 14:33:20	Fault	VOC Sensor1	CO2/VOC Limit	Triggered
2024/02/21 14:33:16	Fault	Hub Port 7	Probe Missing	Triggered
2024/02/21 13:24:07	Fault	Port 2	Probe Missing	Triggered
2024/02/21 13:21:13	Fault	Port 2	Probe Missing	Triggered
2024/02/21 13:21:11	Fault	Port 1	Probe Missing	Triggered
2024/02/21 12:44:32	Fault	Port 2	Probe Missing	Triggered
2024/02/21 12:39:01	Fault	Hub Port 7	Probe Missing	Triggered
2024/02/21 12:39:01	Fault	Hub Port 6	Probe Missing	Triggered
2024/02/21 12:39:01	Fault	Hub Port 5	Probe Missing	Triggered
2024/02/21 12:39:01	Fault	Hub Port 3	Probe Missing	Triggered
2024/02/21 12:39:01	Fault	Hub Port 1	Probe Missing	Triggered
2024/02/21 12:39:01	Fault	Hub Port 4	Probe Missing	Triggered

6 Configuring the Base Unit for SNMP

In this section we are going to explain how the InfraSensing sensors can interact with SNMP enabled management systems.

The Base Unit supports 2 kinds of SNMP messages:

- **Pulling:** a network management system's requests status for the sensors through SNMP get requests
- **Pushing:** the Base Unit pushing SNMP notifications (called SNMP Traps) to network or building management systems

To illustrate SNMP, we will use the free (for personal use) SNMP Browser from iReasoning which is available from the following URL: <u>http://ireasoning.com/mibbrowser.shtml</u>

6.1 SNMP get requests

In the Base Unit the built-in SNMP agent needs to be enabled to allow for querying of the sensor by external applications using the SNMP GET protocol.

The Base Unit has its own MIB file, which can be downloaded here: <u>http://downloads.infrasensing.com/sensors/Base Unit.mib</u>

1. To enable SNMP, connect to the Base Unit, Click on the menu button and go to settings and then under industrial and external communications *toggle on "SNMP"* and click *Update*.

SensorGateway	
Data Center	
every 1	
Celsius	
Enable	
every 5	

Community string is limited to 16 characters.

2. You need now to enable the **SNMP Agent**. Click on *SNMP* to proceed to the SNMP settings.



3. On the SNMP Settings, click on the *SNMP Agent* toggle and enter the *Port* number to be used(default port for this UDP is 161 for Windows OS and 5555 for MAC OS). If you want to use a different community string, then you can change the value up to 16 characters. Default value for a read community is typically *public*, and *private* for write community.

4. Select the SNMP Version (SNMPv2 or SNMPv3). Refer to the illustration for settings of each version:

SNMP Agent	
SNMP Agent	
Port	161
Version	SNMPv2
SNMP Read Community	public
SNMP Write Community	private
SNMP s	ettings for v2
SNMP Agent	
SNMP Agent	
SNMP Agent Port	161
	161 SNMPv3
Port	
Port Version	SNMPv3
Port Version SNMP Read Community SNMP Write Community	SNMPv3 public
Port Version SNMP Read Community SNMP Write Community Username	SNMPv3 public
Port Version SNMP Read Community SNMP Write Community	SNMPv3 public private
Port Version SNMP Read Community SNMP Write Community Username	SNMPv3 public private Serverscheck
Port Version SNMP Read Community SNMP Write Community Username Auth Key	SNMPv3 public private Serverscheck auth12345

SNMP settings for v3

Note. On v3, additional settings will appear. Select a username, then select MD5 and AES for the 1^{st} and 2^{nd} Protocol respectively, and enter an Auth Key and Privacy Key.

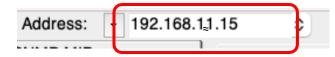
5. After all the SNMP settings are done, click Update.

6. Now let's proceed to opening the iReasoning MIB Browser.

000	iReasoning M	IB Browser	
Address: - 192.168.11	.15:5555 C Advanced OID	: .1. Operations: Wa	alk 🗘 🍙 Go
SNMP MIBs	Result Table		
MIB Tree	Name/OID	Value	Type IP:Port
Name DID			
MIB			

iReasoning MIB Browser main screen

7. Set the Address field to the IP address of your Base Unit.



- 8. Next, click Advanced to go to the advanced properties of the SNMP agent.
- 9. In the Advanced Properties window, enter the following details:
 - IP Address of the Base Unit
 - Copy details from the SNMP settings of the Base Unit such as Read and Write Community string, and Port number
- 10. Select the SNMP version (2 or 3)

Note. When SNMP Version 3 is selected, there will be additional settings to fill out. For the *Security Level*, select *auth*, *priv* then for the rest, copy from the SNMP settings of the Base Unit.

Sens	sorGateway	<u>iReasoning</u>	MIB Browser
		SNMPv3	
Username	Serverscheck -	USM User	Serverscheck
Auth Key	auth12345	Security Level	auth, priv
Protocol	MD5	Auth Algorithm	MD5
Privacy Key	priv12345	Auth Password	*****
Protocol	AES	Privacy Algorithm Privacy Password	AES

For the remaining settings of SNMPv3, leave it blank and it will later have values after it has undergone the SNMP Walk operation.

- 11. After the SNMP v2 or v3 settings are entered, click OK.
- 12. Go to the main screen and perform SNMP walk by selecting *Walk* on Operations and then click *Go*.

Operations:	Walk	~ 🜔	n 🔁 😭

13. The image below shows the example output of the SNMP walk.

Address: 1	92.168.11.15 - Adva	anced OID: .1.3.6.1.4.1	. 17095.3. 10.0 👻	Operations: Walk	- <i>e</i>	Go
SNMP MIBs		Result Table				
MIB Tre		Name/OID	V	alue	Туре	
	1213-MIB.iso.org.dod.internet.mgmt.mib-	sysDescr.0	Temperature & Sensor Gateway		OctetString	6
	ST-RESOURCES-MIB.iso.org.dod.internet.n	sysObjectID.0	serverscheck		OID	2
Serv	verscheck.iso.org.dod.internet.private.ent	sysUpTime.0	36 minutes 49 seconds (220907)		TimeTicks	1 4
		sysContact.0	http://www.serverscheck.com		OctetString	
		sysName.0	Sensor Gateway: SC-TS01		OctetString	
	I	sysLocation.0	Europe Data Center		OctetString	15
		productname.0	Temperature & SensorGateway		OctetString	1 -
	I	productversion.0	Release 1.0		OctetString	1
		productdate.0	Apr 2010		OctetString	1 *
		productusername.0	SensorGateway		OctetString	1 0
		productuserloc.0	Europe Data Center		OctetString	1 7
		productnetip.0	10.0.36		IpAddress	1
1	111 +	productnetgateway.0	10.0.0.99		IpAddress	1
	1.4.4	productnetpridns.0	10.0.0.99		IpAddress	1
ame	mib-2	productnetsecdns.0	0.0.0.0		IpAddress	1
ID	.1.3.6.1.2.1	trapReceiverNumber.0	0		Integer	1
IB	RFC1213-MIB	trapEnabled.0	Yes (1)		Integer	1
yntax		trapReceiverIPAddress.0	192.168.11.64		IpAddress	1
ccess		trapCommunity.0			OctetString	1
tatus		sensor Iname.0	Undefined1		OctetString	1
efVal		sensor 1Value.0	34.31		OctetString	1
dexes		sensor 1LastErrMsg.0	DOWN		OctetString	1
escr		sensor 1LastErrTime.0	04/07/2010, 12:29:20		OctetString	1
		sensor2name.0	Undefined2		OctetString	1
		sensor2Value.0	23.38		OctetString	1
		sensor2LastErrMsg.0	DOWN		OctetString	1
		sensor2LastErrTime.0	04/07/2010, 12:29:20		OctetString	1
		sensor3name.0	Undefined3		OctetString	1
		sensor3Value.0	47.99		OctetString	
		sensor3LastErrMsg.0	DOWN		OctetString	1
		sensor3LastErrTime.0	04/07/2010, 12:29:20		OctetString	1

In the above screen copy you see all the SNMP parameters as made available by the InfraSensing Base Unit.

At the bottom you will see the values of the internal temperature sensor connected to the appliance (**sensor1Value.O**) and then of the values returned by external sensor probes connected to it.

In this example we added an external temperature & humidity probe to it. By clicking on a field, you can see the matching OID for that field at the top. In above example the OID for the humidity reading is **.1.3.6.1.4.1.17095.3.10.0**

Note: for Firmware 7.5 and above a new OID structure is implemented which would have sensor values as String and Integer. The update will not affect the OLD OID structure and can still be used.

Below is an Example of the new structure added on top of our current structure.

1.3.6.1.4.1.17095.1010.10.3.0	25.62	OctetString	192.168.11
1.3.6.1.4.1.17095.1010.10.4.0	25	Integer	192.168.11
1.3.6.1.4.1.17095.1010.10.5.0	WARNING	OctetString	192.168.11
1.3.6.1.4.1.17095.1010.10.6.0	1	Integer	192.168.11
1.3.6.1.4.1.17095.1010.10.7.0	WARNING	OctetString	192.168.11
1.3.6.1.4.1.17095.1010.10.8.0	05 July 2018, 14: 49: 47	OctetString	192.168.11

Note. After the walk operation, the SNMPv3 advanced properties (Engine ID, Localized Auth Key and Localized Priv Key) will have values. The engine ID is composed of the initial default value and followed by the MAC Address of the Base Unit. It can be seen by looking into the Main Settings of the gateway.

Se	nsorGateway	iReasor	ning MIB Browser	
		● ◎ ●	Advanced Properties of SNMP Agent	
		Address	192.168.11.15	
		Port	5555	
Settings & Info		Read Community	*****	
9		Write Community		
Device information		SNMP Version	3	0
Account name	admin	SNMPv3		
	Change Password	USM User	Serverscheck	
Current System Date	01 Jan 2021	Security Level	auth, priv	0
Current System Time	00:00:18	Auth Algorithm	MD5	0
	Update Time	Auth Password		
Hardware Version	Release 2.0	Privacy Algorithm	AES	0
Firmware Version	Release 8.7 (Jan 12 2022 Upgrade Firmware	Privacy Password		-
Mac Address	54:10:EC:DB:EB:AB	Context Name		
110071001000	01.10.20.00.20.00	Engine ID	0x 80 00 42 C7 03 54 10 EC DB EB AB	

IMPORTANT NOTE:

In any cases you encounter or experience where the OID changes whenever a sensor is unplugged please note that this is because you are using an OLD SNMP structure.

With the introduction of the new structure, the SNMP OIDs will remain fixed and will not change whenever a sensor is unplugged.

The OID for the new structure starts with .1.3.6.1.4.1.17095.8.50.9.0.

If you have recently updated your firmware to version 9.2, please perform an SNMP WALK to check the OIDs for the Sound Meter and Pressure sensor on the new structure.

6.2 SNMP traps

When threshold values are exceeded or on failure (water detection or power failure), the Base Unit can send out SNMP Traps to network management systems.

1. On our system we have installed the iReasoning MIB Browser. Go to **Tools > Trap Receiver**

ions	Tools	Bookmar	ks	Expressions	Help
	Trap Re	eceiver		96 1	1
Ac	Trap So Ping Trace F				

2. In the Trap Receiver, click on the Tools button for SNMP Trap settings. Set the Trap Receiver Port. This is the UDP port used by the SNMP Trap Receiver to receive incoming messages. In our example we set it to 5555.

	Result Table Tra	p Receiver ×		
	Operations Tools Da	atabase		
	0 🚳 🚻 🚺 🔏			
• • •		Trap Receiver Settings		
		General SMTP SNMPv3 Trap Receive	r	
		_		
Trap Port:	5555	Bind IP: All	😌 Transport:	UDP 😒
Forward traps to		Port: 5555	Community:	*****

For SNMPv3, additional settings should be added by going to the *SNMPv3 Trap Receiver* tab and then click *Add*, the Add SNMPv3 Parameters will show, thencopy the SNMPv3 settings from the Base Unit to the iReasoning MIB Add SNMPv3 Parameters. After that, click *Ok*.

	General SMTP	SNMPv3 Trap Red	elver
Auth Protocol	Auth Password	Priv Protoc	ol Pr
	Add SNMPv3	Parameters	
	Username	Serverscheck	
	Authentication Protocol	MD5	0
	Authentication Password	****	
	Privacy Protocol	AES	0
	Privacy Password	•••••	
	Security Level	auth, priv	•
		Ok Cano	el

The iReasoning is now ready to receive SNMP Trap alerts from the Base Unit.

Go back to the Base Unit to set the SNMP Trap Alerts by:
 3.1. Click on the Enable 1st Trap Receiver

Note: With the firmware version 7.40 and above you can have up to 2 trap receivers meaning you can install iReasoning or any trap receiver on any two computers and have the gateway send trap alerts on both.

3.2. Define the IP address of the system on which the SNMP Trap Receiver runs.

- 3.3. Selecting the Trap Receivers SNMP Version.
- 3.4. Set the Trap Receiver Port.

Enable 1st Trap Receiver	
Trap Receiver 1 IP Address	192.168.11.159
Enable 2nd Trap Receiver	
Trap Receiver 2 IP Address	192.168.11.23
Frap Receivers SNMP Version	SNMPv3
Trap Receiver Port	5555

4. Click on the **Update** button when done. Once you click the update button, the Base Unit will reboot and will start sending SMS trap alerts.

• • •	iReasoning MIB Browse			
Address: • 192.168.11.15:5555 Advanced	OID: .1.3.6.1.4.1.17095.1000.1.5.0		Operations: Walk	🕒 🋛 🌈 Go
SNMP MIBs	Result Table Trap Receiver ×			
MIB Tree Tee iso.org.dod.internet	Operations Tools Database			
	0 3 2 3 3			
	Description	Source	Time	Severity
	sysObjectID	192.168.11.15	2022-03-18 13:03:32	
Name				
חור				

Above shows the SNMP Trap as received by iReasoning MIB Browser

6.3 JSON (PULL)

To integrate using JSON, We just have to type in the URL the following extensions along with the IP address of your gateway.

http://IP ADDRESS/probe list.json

This call returns the list of sensor probes connected to the Base Unit and their settings.

Example:

http://192.168.1.1/probe_list.json

JSON	Raw Data	Headers	
Save Cop	У		
probe_n	10:	9	
<pre>> probe_l</pre>	ist:		
- 0:			
pr	obe_id:	1	
pr	obe_type:	0	
🔻 se	nsor_name:		
	0:	"Int. Te	mp1"
	1:	"Int. Pi	ng1"
▶ un	it_type:	[2]	
🕨 🕨 al	ert_type:	[2]	
🕨 wa	rn_range:	[2]	
▶ do	wn_range:	[2]	
🕨 🕨 al	ert_setting:	[2]	
▶ ou	tput:	[2]	
🕨 ou	tput_state:	[2]	
🕨 🕨 de	fault_state:	[2]	
▶ 1:		Object	
▼ 2:			
pr	obe_id:	3	
pr	obe_type:	1	
🔻 se	nsor_name:		
	0:	"Ext. Te	mp2"
	1:	"Humidit	y2"
	2:	"Dew Poi	nt2"
🕨 un	it_type:	[3]	
🕨 🕨 al	ert_type:	[3]	
🔻 wa	rn_range:		
-	0:		

http://IP ADDRESS/probe update.json

And this call returns the latest values of all the sensor probes.

Example:

http://192.168.1.1/probe update.json

JSON	Raw Data	Headers
Save Cop	у	
<pre> probe_</pre>	update:	
v 0:		
p	robe_id:	1
p	robe_type:	0
	tatus:	
	0:	1
	1:	1
▼ va	alue:	
	0:	30.65
	1:	30
▼ 1:		
p	robe_id:	2
p	robe_type:	19
▶ st	tatus:	[6]
▶ va	alue:	[6]
▼ 2:		
p	robe_id:	3
p	robe_type:	1
▶ st	tatus:	[3]
▼ va	alue:	
	0:	29.01
	1:	51
	2:	19.2
▶ 3:		0bject
▶ 4:		0bject

6.4 JSON (PUSH) with ADDON-LTE

With the use of our ADDON-LTE, we are now enabled to integrate into your IoT platforms.

Once we connect the LTE add-on into our base unit, we will have a new option for IoT under the settings menu.

Settings & I	nfo				Free	wal
Device information						
Account name		edmin				
		Change Password				
Current System Date		01 Jan 2019				
Current System Time		00:49:58	-			
Hardware Version		Release 5.1	-			
Firmware Version		Release 8.30 (Feb.)	21 2020)			
		Upgrade Pirmware				
Mac Address		00:03:64:03:44:40	_			
IP Address		192.168.11.25				
		Change IP				
Node Status (online/used	s/max)	2/11/61				
		Califrate Barrens				
		Cellular Add. Cri	-			
Industrial & external co	mmunications	1.00				
SNMP		AuT .	()B)	Email		
Modbus	~					
MOODUR	0					
General settings						
Device Name						
Device Location						
Sensor Polling	IoT			100		880
Temperature Unit				, 1		
OLED Screen						-
2 - C - C - C - C - C - C - C - C - C -						
Repeat Alarm Tin					4	min
1.00						
					-	-
Update					Legal	a teste

Click on the IoT option and it will bring us to the set up page for our IoT integration.

IoT Connectivity		
Send Data to Cloud	•	
URL		
Device ID		
Username		
Password		_
Update interval	every 0	1 min
Updane Reset		

You can now input the URL where the data should go, the Device ID that will identify the gateway sending the data, Username and password for security and the update interval.

Note: Update interval has a minimum of 5 minutes

JSON structure is as follows:

{"t":"2020-02-21T05:20:332","d":"000364037961","u":"user","p":"pass","lo":"27.674","la":"53.874","nsg":"14","nty":"36","nsi":"sim1"}
{"t":"2020-02-21T05:20:332","d":"000364037961","u":"user","p":"pass","sensors":[{"si":"1","sn":"Int. Temp1","st":"Int. Temp","sv":"24.40"}]]}
{"t":"2020-02-21T05:20:332","d":"000364037961","u":"user","p":"pass","sensors":[{"si":"2","sn":"Int. Temp1","st":"Int. Ping1","sv":"1.00"}]]}
...
{"t":"2020-02-21T05:21:362","d":"000364037961","u":"user","p":"pass","Ios::[{"si":"9","sn":"UndefineIO 1","st":"Dry Contact","sv":"0"}]}

t = is the timestamp in UTC d = is the device ID u = is the username p = is the password

The first call is the connectivity details: lo: longitude from GPS la: latitude from GPS nsg: network signal strength nty: network type 4G/3G/2G nsi: sim used

"sensors":[{"si":"1","sn":"Int. Temp1","st":"Int. Temp","sv":"24.40"}]}

This is the sensors structure: si: sensor sequential identifier sn: sensor name st: sensor type sv: sensor value

6.5 JSON (PUSH) with ADDON-LTE - Adding Webhook Endpoint

First, visit webhook.site and click on 'Your unique URL' then copy the URL.

••• • • • >	0	🗎 webhook.site	Ċ	ů + C
U Webhook.site Docs & API	Custom Actions WebhookScript Terms & Privacy	Support	.🗳 Copy 👻 🖸	Edit + New → DLogin ★ Upgrade
Password Alias Schedule CSV		XHR Redirect Settings Redirect Now	ORS Headers 🛛 🗖 Auto Navigate 📄 Hide Det	alis More -
REQUESTS (0/500) Newest First Search Query	Webhook.site lets you easily inspect, test and These addresses were generated for you just n			
Waiting for first request	Your unique URL https://webhook.site/bb8ad62	2–1cd4–47f2–8c6f–2b759bc39a8	d 🕸 Copy 🖸 Open in new tab 🕻 Examples	
	Your unique email address bb8ad622-1cd4-47f2-8c6f-2b75	9bc39a8d@email.webhook.site	Ĵg Copy 🖾 Send mail	
	To change the response (status code, body cor With Webhook.site Pro, you get more features use them to send push notifications and real custom scripts using WebhookScript, and more Star on GitHub	ike Schedules, that lets you create a periodica s, convert and forward the request to another l		s that lets you extract JSON or Regex values and databases like MySQL, PostgreSQL and write
	Request Details	Permalink Raw content	Headers	
	Date Size 0 bytes ID			
	Query strings		Form values	
	(empty) No content		(empty)	Copied URL to clipboard.

After copying the URL, let's return to our IoT settings to input the credentials.

e		
IoT Connectivity		
Send Data to Cloud		
URL	https://webhook.site/bb8ad622-1cd4-47f2-8c6f-2b759bc39a8d]
Device ID	00036403EA7D	
Username	admin	
Password		
Update interval	every 5 💿 min	
Update Reset		

Above is an example input using the newly generated endpoint. The device ID, username, password and interval are all customizable.

••• • • < >				C	ů + ©
🐌 (30) Webhoo	ok.site - Test, process and transform emails and HTTP requ	ests		1 InfraSensing	
Webhook.site Docs & API	I Custom Actions WebhookScript Terms & Privac	y Support		📲 Copy 🗸 🖸 Edit 🕂 Ne	w Dogin 🛨 Upgrade
Password Alias Schedule CS		XHR Redirect Settings Redirect Now	DRS Headers 📔 🗖 Auto	Navigate Hide Details More -	
REQUESTS (49/500) Newest First	Request Details	Permalink Raw content Copy as 🗸	Headers		
Search Query	POST https://webhook.site/bb8ad622-10	d4-47f2-8c6f-2b759bc39a8d	content-type	application/json	
	Host 209.35.167.229 Whois Shodan N	etify Censys	connection	close	
POST #a8ccc	Date 11/07/2023 6:52:53 PM (5 minutes	ago)	content-length	139	
209.35.167.229	Size 139 bytes		host	webhook.site	
11/07/2023 6:57:41 PM	ID 57a08313-cd1d-4467-bc28-5884f	cd02eea			
POST #b05d9	Files				
209.35.167.229	Query strings		Form values		
11/07/2023 6:57:39 PM	(empty)		(empty)		
			(
POST #8e000	Raw Content			.	Format JSON Vord-Wrap Copy
209.35.167.229 11/07/2023 6:57:32 PM	{				
11/01/2023 0.37.32 PM	"t": "2023-11-07T10:51:29Z", "d": "00036403EA7D",				
POST #36888	"u": "admin",				
209.35.167.229	"p": "admin",				
11/07/2023 6:57:30 PM	"IOs": [{				
	"si": "20",				
POST #842a3	"sn": "UndefineIO 4", "st": "Dry Contact",				
209.35.167.229 11/07/2023 6:57:28 PM	"sv": "0"				
11/01/2023 0.31.20 PM	}				
POST #c8de6	}				
209.35.167.229					
11/07/2023 6:57:26 PM					

Go back to your browser where your endpoint is opened and results will start to populate.

6.6 XML output

← → C 🗋 192.168.11.80/xmlOutput.xml

This XML file does not appear to have any style information associated with it. The document tree is shown below

```
v<note>
 v<status>
    <from>192.168.11.80</from>
    <from>sgw17</from>
    <ssname0>temp1</ssname0>
    <ssvalue0>21.74</ssvalue0>
    <ssname1>Ext. Temp</ssname1>
    <ssvalue1>20.87</ssvalue1>
  </status>
 v<alerts>
    <alert1>temp1,21.86,NORMAL,26 November 2013,13:54:37</alert1>
    <alert2>temp1,71.80,DOWN,26 November 2013,13:54:13</alert2>
    <alert3>temp1,24.34,NORMAL,25 November 2013,20:10:24</alert3>
    <alert4>temp1,44.14,DOWN,25 November 2013,20:07:41</alert4>
    <alert5>Ext. Temp,25.00,NORMAL,24 November 2013,19:17:44</alert5>
    <alert6>Ext. Temp,25.06,WARNING,24 November 2013,19:17:43</alert6>
    <alert7>Ext. Temp,25.00,NORMAL,24 November 2013,19:15:52</alert7>
    <alert8>Ext. Temp,25.06,WARNING,24 November 2013,19:15:50</alert8>
    <alert9>Ext. Temp,25.00,NORMAL,24 November 2013,19:14:49</alert9>
    <alert10>Ext. Temp,25.06,WARNING,24 November 2013,19:14:48</alert10>
    <alert11>Ext. Temp,25.00,NORMAL,24 November 2013,19:14:16</alert11>
    <alert12>Ext. Temp,25.06,WARNING,24 November 2013,19:14:14</alert12>
    <alert13>Ext. Temp, 25.00, NORMAL, 24 November 2013, 19:13:29</alert13>
    <alert14>Ext. Temp,25.06,WARNING,24 November 2013,19:13:28</alert14>
    <alert15>Ext. Temp,25.00,NORMAL,24 November 2013,19:13:11</alert15>
```

The log can be accessed by appending *xmlOutput.xml* at the end of the Base Unit's IP address/FQDN as seen on the screenshot. More than the alerts, it also gives you the current status of the device. This option shows the latest 500 alert entries.

6.7 ModBus TCP / RTU

With the firmware 9.2 and above, Base Unit Modbus TCP can now be polled by 4 Modbus masters. For detailed instructions on Modbus usage, please refer to the dedicated manual available on our website or you may access it through the provided link below: Modbus Manual.

7 Sensor calibration

A unique feature of the InfraSensing Base Unit and external probes is that the Base Unit has a calibration feature available from the web interface. This feature allows to correct temperature and humidity readings based upon, for example a NIST Traceable measurement system.

To recalibrate the built-in or external probes, Go to Menu and then Settings.

Settings & Info Device information Account name admin Current System Date 14 Feb 2019 Current System Time 01:02:05 Hardware Version Release 5.1 Release 8.00 (Feb 12 2019) Firmware Version 00:03:64:03:44:40 Mac Address IP Address 192.168.11.104 Node Status (online/used/max) 3/43/44

Adjust your sensor readings by modifying the offset value (either + or -) and click on Update.

Note : Our sensors are pre calibrated by our manufacturer However we do offer our very own Calibration Certificate more information can be found here https://infrasensing.com/lab/**

Sensor Type	Example Value	Operator		Offset value	
InternalTemp	28.58 °C	+	\$	0.00	
ExternalTemp	2° °C	+	\$	0.00	
ExternalHumd	? %RH	+	\$	0.00	
Fuel Level Max	?	=	\$	1023.00	
Fuel Level Min	?	=	\$	0.00	
Flow Rate Period (min)	5	-		5	
Air Flow Threshold	?	>	\$	20.00	
Shock Threshold	?	>	\$	765.00	
Temp Threshold	0.00	-		0.00	
Humidity Threshold	0.00	-		0.00	
AC Voltage Type	220/240	110/120			
AC Voltage Offset	?	+	\$	0.00	
Sync Internal Temp Sensor with External					
Thermal Emissivity (0.01-1)	0.95				
Power Quality	230 Volts / 60 Hz				
Reset 3-Phase Power Meter Counter	Reset Counter				
Reset Power Meter Total kWh Reading	Reset Reading				
Reset Tilt Sensor Values	Set to Zero Reset to Defa	ult			
Tum Panel Fan	On Off				
DC Power Control Sensor:					
Minimum(7-89) / Maximum(10-90) Voltage	-	7.00	0	48.00	0
Minimum(0-89) / Maximum(0.1-90) Current		1.00	0	50.00	0
Minimum Time to detect error (0-120s)	-	-		10.00	\$
Reset Counter	Reset Counter				

With the introduction of firmware version 9.1, a new feature has been incorporated, allowing users to designate CO2/VOC sensors as reference points. For more information, refer to section 7.1.

7.1 Reference Sensors

Reference Sensor Selection" is a feature that offers the ability to designate a sensor as the reference point. Whether a CO2/VOC regular or daisy sensor is connected, a dropdown menu will appear to facilitate the selection of the reference sensor.

Cpdate		Lindete Report	
		Update Reset	
Reference Sensor Selection	Reference	e Sensor Selection	
		e Sensor Selection	¢
CO2 Reference	CO2 Reference		¢ ¢
Reference Sensor Selection CO2 Reference VOC Reference VOC Reference CO2 Offgas Enable	CO2 Reference		

7.2 Tolerance level

Flow Rate Period(min)	5	÷.	5
Air Flow Threshold	?	>	• 20.00
Shock Threshold	?	>	• 765.00
Temp Threshold	0.00	*	0.00
Humidity Threshold	0.00	*	0.00
AC Voltage Type	220/240	110/120	
AC Voltage Tolerance	?	+	• •
AC Voltage Value	•		220.00
Sync Internal Temp Sensor with External	0.00		

As you can see in the image above, you can also set the tolerance level (threshold) which is a parameter where in a trigger won't go off immediately if its within tolerance levels.

An example on how it is used is if you have an alert that would trigger at 30 degree Celsius and a tolerance set at "5" what happens is, if your actual temperature goes on to 30 degrees an alert would trigger and you would only receive a recovery alert or an "OK" status once the value goes down to 25 degrees as set on the tolerance level. That way, if in case the temperature goes down between

25.1 – 29.99 then goes back to 30 or above you won't get spammed with alerts or recovery emails or in a case where a device is set to turn on when the threshold is met and would turn off if not, you would avoid having that device to turn on and off countless times.

Note. Starting from firmware version 8.8 and above, there will be additional calibration options for SEC-TILT(Reset Counter) and ENV-THIMG(Thermal Emissivity) sensors.

Warning. For Thermal Emissivity calibration, it is recommended to be set to 0.95 or depending on the surface to be scanned with ENV-THIMG.Failure to calibrate may give off incorrect values for the ENV-THIMG sensor.

7.3 Threshold change and additional calibration functions

With the latest firmware update, you can now modify or configure the thresholds, you can access it using the following link format below:

(Base Unit's IP Address)/calibration2.html

Q IP ADDRESS/calibration2.html	6
--------------------------------	---

Once you access the link, you will be prompted with this window which it will ask you for your username and password. By default the username and password is admin/admin

Sign in to Your password v	IP Address vill be sent unencrypted.			
User Name				
Password				
Remember t	nis password			
		Canaal	Cian In	
		Cancel	Sign In	

Upon logging in, you will be routed to the special calibration page. At the very bottom of the page you will be able to see the option for ENV-LHD.

SAS-X	x
Gas ID:	00 (C2H4) +
Set ID	
Calibration:	•
Calibrate	Set 0
Sensitivity:	
Set Sensitivi	
	-
LED Warning:	Thresholds:
Down:	•
Set Thresho	
Set Thresho	
IND-0t	o10
Min Value:	0
Max Value:	
Set Value	Reset
ENV-T	HUM
	Temperature:
Slope:	•
Intercept:	٦
Calibrate	
For	Humidity:
Slope:	•
Intercept:	•
Calibrate	

RS485	i-GAS-V	OC-H
Thr	esholds:	
Relay 1:	0	٢
Relay 2:	0	٥
_		•
Set Thresh	olds	
Mo	dbus Config:	
Baudrate:	1200	\$
Parity:	None	\$
Stop Bits:	1.5	\$
Set Config		
	•	
ENV-L	HD	
	istance per	
Resistance		٢
Set		
Res	istance Offs	et
Line 1		٢
Line 2		٢
		•
Set		

This is where you can set or adjust threshold to each sensor provided on this page.

8 Factory resetting of Base Unit

8.1 Base Units v1 and v2

Following only applies to Base Units v1 & v2 - the matching models are shown below



You can always hard reset the Base Unit to its default factory settings as follows. Resetting

the device to factory default will result in all settings to be lost



- 1. Plug in power adapter or PoE cable
- 2. Within 2 seconds from plugging the power adapter or PoE cable, push the **Reset** button with a pen or similar and hold it for 5 seconds before releasing it.
- 3. Wait until the yellow LED doesn't blink anymore
- 4. Reconnect to the Base Unit's web interface at http://192.168.11.160

8.2 Base Unit v3 and v4

Following only applies to Base Units v3 and v4 - matching the picture below Kindly

note that due to a mistake in the boot loader of v3 units, the internal system specifications show it as a v2 unit. However, those are v3 units (or v4 for dual sensor probes) when they match the picture below.

You can always hard reset the Base Unit to its default factory settings as follows. Resetting

the device to factory default will result in all settings to be lost



Remove the external sensor probe Remove the power adapter or PoE cable Push the **Reset** button While the **Reset** button is pushed, plug in the power adapter or PoE Cable After 10 seconds the Green & Yellow LED's will be on steady (not blinking) Remove power adapter or PoE cable Wait 3 seconds Plug in power adapter or PoE cable After a few seconds both Green & Yellow LED's are blinking Reconnect to the Base Unit's web interface at <u>http://192.168.11.160</u>

8.3 Base Unit v5

Following only applies to Base Units v5

Resetting the device to factory default will result in all settings to be lost



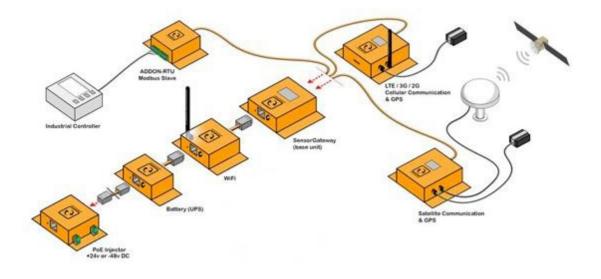
- 1. Remove the external sensor probe.
- 2. Remove the power adapter or PoE powered network cable.
- 3. Push the **Reset** button.
- 4. While the **Reset** button is pushed, plug in the power adapter or PoE powered network cable .
- 5. Hold it for 15 seconds before releasing it. The yellow LED should be blinking fast.
- 6. Wait until the yellow LED is not blinking fast anymore.
- 7. On the LED display, the Base Unit will reboot. After a few seconds both Green & Yellow LED's should be flashing slowly.
- 8. While the PoE or power adapter is plugged in, push the **Reset** button.
- 9. Hold it for 15 seconds before releasing it.
- 10. On the LED display, the Base Unit will reboot. After a few seconds both Green & Yellow LED's should be flashing slowly.
- 11. The base unit will reset and it will go back to the default home page where they will upload the latest firmware they have.

Dutside Temperature 32.31 C / 90.16 F P Address 192.168.9.40 subnet Mask 255.255.255.0	Dutside Temperature 32.31 C / 90.16 F P Address 192.168.9.40 subnet Mask 255.255.255.0	lardware Info		
P Address 192.168.9.40 Subnet Mask 255.255.255.0	P Address 192.168.9.40 Subnet Mask 255.255.255.0	nternal Temperature	35.06 C / 95.11 F	
Subnet Mask 255.255.25	Subnet Mask 255.255.0	Dutside Temperature	32.31 C / 90.16 F	
		P Address	192.168.9.40	
efault Gateway 192.168.9.1	efault Gateway 192.168.9.1	ubnet Mask	255.255.255.0	
		efault Gateway	192.168.9.1	
his is the default firmware - Please update the firmware to start using the device.	his is the default firmware - Please update the firmware to start using the device.	his is the default firmware - F	lease update the firmware to start using the device.	

12. Reconnect to the Base Unit's web interface at **http://192.168.11.160** If you are unable to connect on that IP address then lookup the IP address of the device either from your DHCP server or using the Sensor Discovery Tool - <u>https://infrasensing.com/support/downloads.asp</u>

9 Add-Ons for the Base Unit

The Base Unit, the base unit, requires by default a network cable and 12v DC or POE power input. With the optional add-on modules, customers can add other network and power connectivity options to the base units.



9.1 Wifi Add-On

The InfraSensing Add on Wifi module is an expansion unit to the Base Unit which enables wired and wireless networking application. The Add on Wifi module supports 802.11n standards, and provides backward compatibility with older 802.11b/g standards as well. The up-to-150Mbps wireless speed makes it ideal for handling multiple data streams at the same time that ensures your network is stability and reliability



9.1.1 Features

Portable design Connects directly to the Base Unit Directly powers the Base Unit via the 12v DC adapter output GUI accessible using any browser USB support for 3G and LTE dongles Pre-encryption that prevents unauthorized access from users outside of the network

It enables you to:

Add a Standard Wireless Router mode that creates an instant private wireless network to access and configure the Base Unit

Add an Access Point mode that creates a wireless network for Wi-Fi devices to access and configure the Base Unit

Add a client mode functionality that works as a wireless adapter for any Ethernet enabled devices to access and configure the Base Unit

Add an 3G and LTE USB data connection to your network when there is no ISP available

9.1.2 View of the Wifi Add-On connected to the Base Unit



9.1.3 Hardware interface

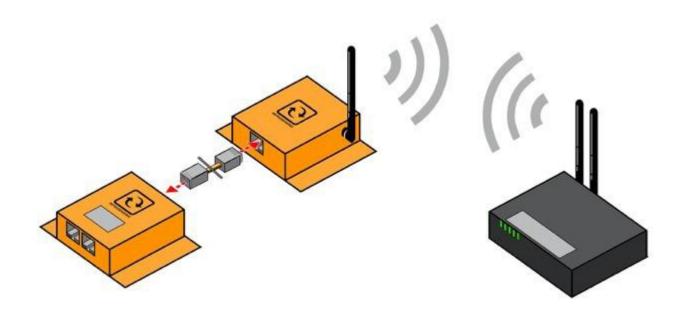


Interface	Description
ANT	Wireless antenna
ETH1	WAN/LAN port
ETHO	LAN port to Base Unit
DC IN	12-volt DC adapter socket
USB1	USB for 3G and LTE dongle

9.1.4 Getting started

Powering the Add-On Wifi module with Base Unit

- 1. Connect the 12-volt DC adapter to the DC IN socket
- 2. Wait for the RED LED to turn solid
- 3. Connect the Base Unit to the Add on Wifi module via ETH0 and DC OUT



System requirements

PC with working LAN/WLAN interface TCP/IP protocol installed on the PC Web browser (Chrome, Firefox, IE, Safari etc.) LAN cables (RJ 45) RJ 45 male to female adapter for configuration via ETHO

9.1.5 How to access the Graphical User Interface (GUI)

We can access the GUI via WLAN and/or LAN connection. Configurations will be done on the GUI $\,$

As an access point (WLAN)

Power on the Add on Wifi module Connect via Wifi to the unsecured SSID "ServersCheck" Launch a web browser and type the default IP 192.168.1.1 to the address bar By default there is no password that has been set Username must always be "root" Click LOGIN to access main menu page Base Unit GUI will be available from the IP address on the OLED screen Make sure that the Add on Wifi module and Base Unit has the correct IP range Setting the Base Unit to DHCP is recommended

LAN connection to PC (LAN)

The steps below apply to a Windows 7 system. For other systems (Windows, Mac, *Nix) steps are similar

Power on the Add on Wifi module Connect ETH1 to the LAN port of your PC Go to Network Panel > Network & Sharing Center Click on Local Area Connection and then click on Properties. In the new window select Internet Protocol Version 4 and click on the Properties button.

Local Area Connection Properties	x
Networking	
Connect using:	
Broadcom NetLink (TM) Gigabit Ethernet	
Configure	
This connection uses the following items:	
Client for Microsoft Networks	
🗹 📮 Kaspersky Anti-Virus NDIS 6 Filter	
🗹 💂 QoS Packet Scheduler	
File and Printer Sharing for Microsoft Networks	
Internet Protocol Version 4 (TCP/IPv4)	
✓ Link-Layer Topology Discovery Responder	
Install Uninstall Properties	
Description	
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication	t
across diverse interconnected networks.	
	— II
ОК Са	ncel

Set the corressponding IP ranges

We recommend setting it to 192.168.1.15 as shown below. When done, click on the **OK** button.

General	
	tomatically if your network supports d to ask your network administrator
Obtain an IP address automat	ically
• Use the following IP address:	
IP address:	192.168.1.15
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	
Obtain DNS server address au	tomatically
Use the following DNS server a	addresses:
Preferred DNS server:	
Alternate DNS server:	
Validate settings upon exit	Ad <u>v</u> anced

Launch a web browser and type the default IP 192.168.1.1 to the address bar. By default there is no password that has been set. Username must always be "root". Click LOGIN to access main menu page.

9		
Status	Status	
Overview	Status	
Firewall		
Routes	System	
System Log		ServersCheck
Kernel Log	Hostname	
Processes	Local Time	Wed Sep 6 14:28:59 2017
Realtime Graphs	Uptime	0h 36m 5s
System	Load Average	0.00, 0.01, 0.05
Network		
	Memory	
Logout	Total Available	33800 kB / 60520 kB (5
	Free	30336 kB / 60520 kB (50
	Buffered	3464 kB / 60520 kB (5/

Base Unit GUI will be available from the IP address on the OLED screen. Make sure that the Add on Wifi module and Base Unit has the correct IP range. Setting the Base Unit to DHCP is recommended 9.1.6 Username and password settings

Access the GUI. By default there is no password that has been set. Username must always be "root". Click LOGIN to access main menu page.

No password set! There is no password set on this router. F	Please configure a root password to protect the web interface and enable SSH.
Go to password configuration	
Authorization Requir	red
Please enter your username and password.	

Username	root
Password	



Desined by ServersCheck 2017 (

Go to System > Administration Set and confirm password Click SAVE and APPLY

ē				
Status System System Administration Software	No password set! There is no password set on this router Go to password configuration		to protect the web interface and enable SSR	
Startup Scheduled Tasks Backup / Flash Firmware Reboot	Router Password	ccessing the device		
Network Logout	Fashero		e e	

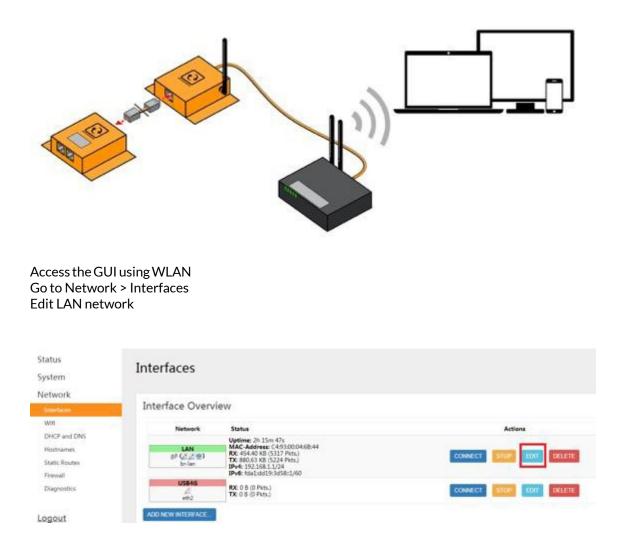
There will be a notification that the password was successfully set

Ð		
Status		
System		
System		
Software	Router Password	
Startup	Changes the administrator paraword for accessing the device	
Scheduled Tasks		
Backup / Flash Firmware		
Reboot	Password	
Network	Confirmation	
Logout		

9.1.7 Configuration modes

Adding Internet connection to the Base Unit via ETH0 can be done with the following modes.

As wireless router



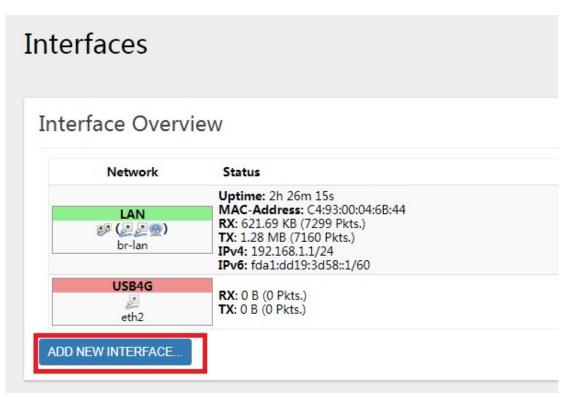
Go to Physical Settings tab and uncheck Ethernet adapter: eth1 (LAN)

Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by tickin interfaces separated by spaces. You can also use <u>VLAN</u> notation INTERFACE.VLANNR (e.g.: eth0.1).

Common (Configuration		
General Setup	Advanced Settings	Physical Settings	Firewall Settings
	Bridge interfaces		er specified interface(s)
	Enable <u>STP</u>		ng Tree Protocol on this bridge
	Interface	 Ethernet Adapter: "eth0" (lan) Ethernet Adapter: "eth1" (lan) 	
		Ethernet Adapte Mireless Netwo Custom Interface	rk: Master "ServersCheck" (lan)

Click SAVE and APPLY Go to Network > Interfaces ADD NEW interface

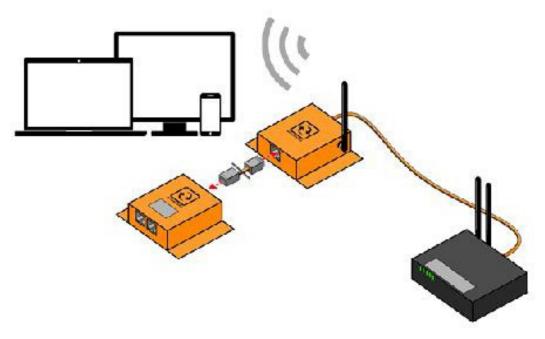


Name the new interface and select Ethernet adapter: eth1 (LAN)

Choose between DHCP Client or Static protocol Click SUBMIT On the Firewall setting Tab chose WAN

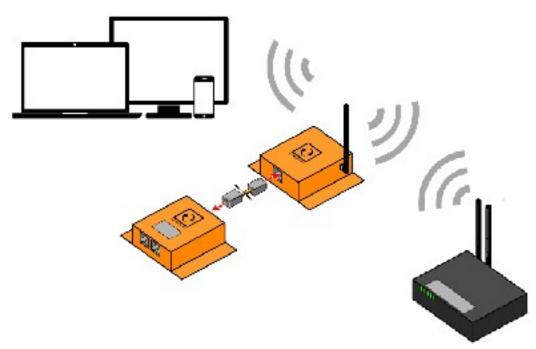
Click SAVE and APPLY Connect ETH1 to WAN port Internet connection will be available on ETH0

As an access point



Do steps 1 to 12 from Wireless Router configuration (section 9.1.7) Connect ETH1 to any of the LAN port of the Router Internet connection will be available on ETH0

As a WIFI client



Access the GUI using WLAN or LAN Go to Network > Wifi Do a SCAN for available Wireless networks

e		
Status System Network	Wireless Overview	
Interfaces with	Generic MAC60211 802.11bgn (radio0) Channet 11 (2462 Gira) Bitrate: 52 MbrUs	SCAN ADD
DHCP and DNS Hostnames Static Routes	SSID: ServersCheck Mode: Master BSSID: C4/93/00/04/68/43 Encryption: None	DISARLE EDIT REMOVE

Join the desired Wifi network

oin Network: Wireless Scan	
Neighborhood Neighborhood Master BSSID: 94:46:96:16:97:EC Encryption: mixed WPA/WPA2 - PSK	JOIN NETWORK
ServersCheck_IOT 100% Channel: 2 Mode: Master BSSID: 90:61:0C:0C:4B:A8 Encryption: <u>WPA2 - PSK</u>	JOIN NETWORK
PLDTHOMEDSLLINEARLINK Mode: Master BSSID: 00:13:33:F3:56:9C Encryption: mixed WPA/WPA2 - PSK	JOIN NETWORK
PLDTHOMEDSL_0 100% Channel: 1 Mode: Master BSSID: 94:46:96:16:97:ED Encryption: mixed WPA/WPA2 - PSK	JOIN NETWORK
AYALA_GLOBE 57% Channel: 5 Mode: Master BSSID: FC:3F:7C:6B:41:5F Encryption: mixed WPA/WPA2 - PSK	JOIN NETWORK
Globe-Telcomcall-10L 328 Channel: 4 Mode: Master BSSID: 64:66:B3:29:5B:BE Encryption: mixed WPA/WPA2 - PSK	JOIN NETWORK

Type the password for the Wifi network and uncheck the "replace wireless configuration"

Join Network: Settir	ngs	
Replace wireless configuration	✔ ● An additional network will be created if you leave this	unchecked.
WPA passphrase		2 2
Name of the new network	Specify the secret encountion key here wwan	
Create / Assign firewall-zone	The allowed characters are: A-Z, a-Z, a-Z, 0-9 and _ Ian: Ian: Ian: Ian: Ian: Ian: Ian: I	
	• wan: usb4g: 🖉 eth1: 🖉	
	unspecified -or- create:	

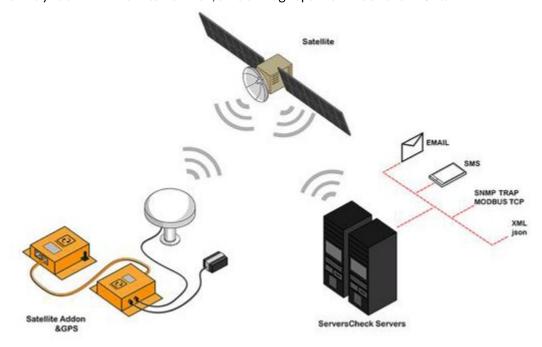
Click SUBMIT Internet connection will be available on ETH0

NOTE: The WIFI add-on serves as a router and designed for you to connect directly to the device, In the event that you want to integrate the device into your network it is indeed possible by having a network engineer configure the routing tables or protocols to be used for the connection.

9.2 Satellite Communication Add-On (ADDON-SATELLITE)



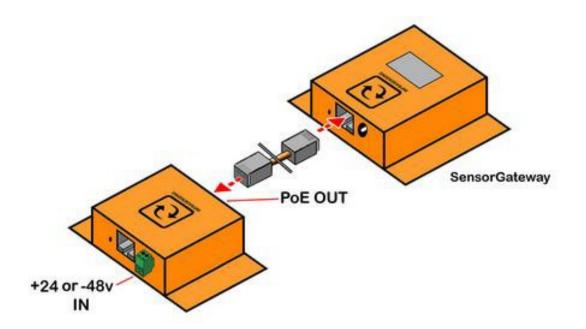
The addon is used to send alerts via Satellite connection, it has global satellite coverage from pole to pole. Can be used as primary or back up connection enables you to receive alerts via email, SMS through space and has built-in GPS.



In order to use the add-on a monthly subscription through InfraSensing is required to connect the device onto the satellite network. Credits are required per message sent or received by the Base Unit



Designed to support the deployment of our sensor platform in industrial environments operating on +24v DC and for the telecom industry, the telecom version PoE addon supports negative -48v DC as power input. This second generation of our DC Power Add-On has been modified so that we not just support our base units, but any PoE 802.3at enabled device. Up to 22 Watts.



9.4 LTE/2G/3G Communication Add-On (ADDON-LTE)

Designed to send alerts even when your IP network is down. Supports Global LTE/3G/2G connection and can send SMS alerts using your local micro SIM card. (Micro SIM + Data Plan required)



The addon features support for two(2) micro SIM cards. When the network on SIM1 fails, then automatically it will use the network of the backup SIM to send out the alerts and data.

The Cellular alerting addon has the Quectel wireless module embedded. This module has international carrier and regulatory approval as follows:

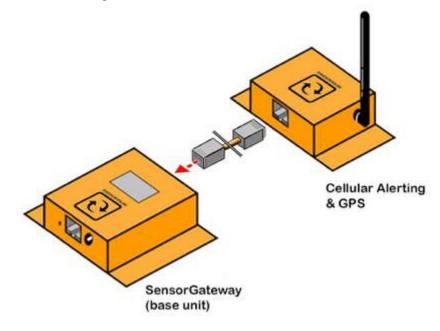
Carrier approvals: Deutsche Telekom(Europe), Rogers (Canada)

Regulatory approvals: GCF (Global), CE(Europe), FCC/PTCRB (North America), IC (Canada), Anatel (Brazil), IFETEL (Mexico), SRRC/CCC/NAL (China), KC (South Korea), NCC (Taiwan, China), JATE/TELEC (Japan), RCM (Australia & New Zealand), FAC (Russia), NBTC (Thailand), IMDA (Singapore), ICASA (South Africa)

Note:

The LTE add-on currently does not support cloud data upload and will automatically disable the cloud option when connected.

The LTE add-on is always in offline mode, and it only goes online when data is being sent. It will also disable the default SMS option of the base unit that uses premium credits. Also the add-on LTE,



The LTE addon can connect to the Base Unit or Sensorhubs (EXP-4HUB/ EXP-8HUB) in the same convention as our regular sensors.

9.4.1 GUI of the ADDON-LTE

To access the ADDON set up, login to your base unit and go to settings, under settings click Cellular Add-On

Settings & Info

Device information Account name

Current System Date Current System Time

Hardware Version Firmware Version

Mac Address IP Address

Node Status (online/used/max)

admin
Change Password
08 Feb 2020
01:49:43
Update Time
Release 5.1
Release 8.20 (Feb 7 2020)
Upgrade Firmware
00:03:64:03:6A:A4
192.168.11.60
Change IP
24/50/51
Calibrate Sensors
Cellular Add-On

ADDON-LTE Config	g
Primary mode	
Backup mode	
SIM1 PIN	SIM2 PIN
SIM1 APN	SIM2 APN
SIM1 APN Username SIM1 APN Password	SIM2 APN Username SIM2 APN Password
Add-on Status Last Error	Connected
Network Status Active SIM Network Name Signal Band RSSI IMEI	SIM2 GOMO GOMO LTE 14 867698040182514
SMS Recipients	
Append to SMS this text	
	Send test SMS
SMTP Server	
SMTP Port Secure connection	25
	None ~
Use SMTP Authentication SMTP Username SMTP Password	
From Email	
To Email(s)	
Email Subject Append to Email this text	ServersCheck Sensor Alert
	Send test Email
GPS Status Fix Satellites Found Latitude	No fix 0 0.00000
Longitude	0.00000

The Image above is the configuration page of the LTE addon and each section will be discussed further.

9.4.2 ADDON-LTE modes

There are two modes you can set your addon into, the Primary mode and the Backup mode. When set in "**Primary mode**" the add-on will primarily use the SIM's data connection to send alerts.

ADDON-LTE Config						
Primary mode						
Babu) mate						
SAT PK			SAC PN			
SMI Usemane			BMI Osemane			
SMI Passent			SNG Passaint			
Add on Shihas Last Error		Connected				
Natural Status	ADDON-LTE	Config				
Active SM Network Name	ADDON-LIE	coning				
Signal Band MSD	Discussion of the	6				
MD	Primary mode					
SVS Recparts	Backup mode		0			
Appoint to 3MS this last						
	SIM1 PIN			SIM2 PIN		
	SIM1 APN			SIM2 APN		
SMIP Sever						
SMIP For Secure connection	SIM1 Usemame			SIM2 Usemame		
3401 C 01 - 8001	SIM1 Password			SIM2 Password		
Use SHTP Automication SATP Generate						
With Passatri						
	Add-on Status		Connected			
From Email To Email(s)	Last Error		Data connection failed			
Email Bulget						
Append to Small Res lead		Seneral/hox Sensor Ret				
					. Ale	
		Sensi kest Email				
GPS Status						
Fix Balantines Proved		to fix				
Latitude						
Langhula		0-004000				
Lines Real						

When set in "**Backup mode**" the addon uses the SIM's data connection to send alerts only when your network connection is unavailable. The LTE addon checks for the internal PING parameter to identify if your local Internet is down.

ADDON-LTE Config					
Primary mode	0				
Backup mode					
SM PN			SAG PN		
EAT AND			ENG APR		
SMI Usename			BM3 Usemane		
BMI Passerri			SNG Passante		
And on Status Landborn	ADDON-LTE C	onfig			
Active SM					
Network Name Dignal Band		-			
ND NO	Primary mode	ſ	0		
SVS Recents					
Append to SMS this test	Backup mode				
	SIM1 PIN			5IM2 PIN	
SVTP Server	SIM1 APN			SIM2 APN	
SATE For	SIM1 Username			SIM2 Username	
Becure connection				and become	
Use SVTP Automication	SIM1 Password			SIM2 Password	
SATP General					
\$MTP Passaged					
Prot Enai	Add-on Status Last Error		Connected		
To Email(s)	Lass Little		-		
Erral Bayest	2	mencheck benear met			
Append to Email this lead					
					A.
		ni test Emai			
0P3 Solve Px Saddiss Pand Latitus Latitus Latitus	No.1 0.0 0.00 0.00				

As shown on the image below the Internal ping is down, this will then signal the LTE add-on that the local network is down and will now use the SIM's data connection to send alerts.

Sensors

Status	Туре	Name	Value	
	Temperature	Int. Temp1	32.3 °C	
	Ping	Int. Ping1	2000 ms	



In Backup mode, the internal Ping is required to be enabled and ideally input an IP address or website outside of your local network with at least 60sec on the timeout counter like the example below.

Ping Setting

pdate Reset

This optional PING sensor enables you to monitor if to the internet, then you can also use a public IP.	the IP network link is still reachable.	You can check ag	gainst an inte	mal IP address to see if the internal ne	twork is still operational. If the device can connect
Enable Ping sensor					
Domain name OR IP address	www.serversche	ck.com.			
Ping timeout	60	1	sec		

Note: The LTE add-on does not provide Internet connection for your base unit and that data connection will only be used for sending alerts via the LTE addon configuration. With that in mind the Ping parameter will still be down until your local Internet is restored.

9.4.3 Setting up data connection

Data settings for your SIM include the APN, PIN, Username and Password. If any of the given are not applicable then we can just leave it blank.

We suggest performing a test mail to make sure you have data connection and that your APN is correct.

9.4.4 SIM section

Following the data settings is the SIM information and SMS settings

ADDON-LTE Config	Network Status			
-	Active SIM		SIM1	
	Network Name		T-Mobile	
Primary mode	Signal Band		LTE	
Baltup male	RSSI		16	
SAT PN	IMEI		857803040H5D5H	
SAT APN	Child Development			
BMI Username	SMS Recipients			
SMI Passent	Append to SMS this text			
Add or Status Last Error				
Network Balas Active SM Network Notes Signar Band RSB Net			Send test SMS	
SVS Recparts				
Augured to SMS this test				
			A	
		Sand And SMS		
SMTP Server				
SATIR Put		15		
Secure connection		Nere	•	
Use SVTP Authentication				
BATTP Demane				
UATP Passant				
Frontimul				
To Email (s)				
Email Bulgert		SeneroCheck Sensor Reft		
Append to Dinal this last			A	
		Serviced Errol		
0PS Status Fix Bahrlites Found Laffulte LangeLote		No.1a 0 0.0000 0.0000		
Liphon Read				

See section 9.4.7 on how to insert a SIM card and for alerting, see section 4.6

9.4.5 Email section

Next is the Email configuration field (Go to section 4.1 for setting up Email Alerts)

ADDON-LIE Comig					
Primary mode	()#				
Bachup mode					
SMI PN		SAG PN			
SMI AN		SING APN			
BMI Usersame		BM3 Overname			
SMI Passer4		BM2 Passecret			
Add-on Batus Last Error	Convertex				
Network Distus					
Active SM Network Name					
Signal Band KSS	SMTP Server				
ND					
SVS Recents	SMTP Port		25		
Appoint to SMS this test	Secure connection				mi.
			None		-
SMTP Sever	Use SMTP Authentication				
SMIP Pot	SMTP Username				
Secure connection					
Use SNTP Automouton	SMTP Password				
SVIIP Usename					
SUTP Passaint	From Email				
From Email	Tron Chan				
Te Email(s)	To Email(s)				
Email Bulged Append to Email this lead	En 1 E Mart				_
	Email Subject		ServersCheck Sense	or Alert	
	Append to Email this text				-1
SPS Status Fix					A
Exhibits Paula Latitude					
Longikula			Send test Email		
Upters Reset					

9.4.6 GPS section

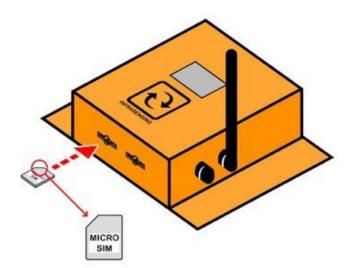
When you avail of the optional GPS feature you will have the information on the OLED screen of the LTE add-on as well as on the GPS section.

At the bottom most part of the Add-on settings we would see the optional GPS information as well as the update and reset buttons.

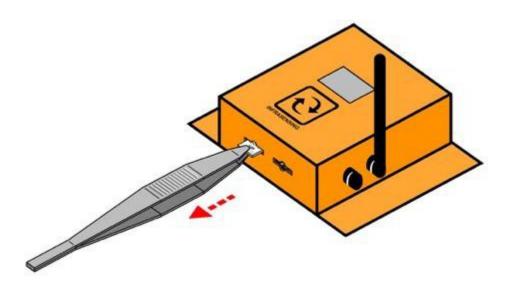
ADDON-LTE Config					
Primary mode		()#			
Backup mode					
SMT PN SMT APN BMT Usersere BMT Persent			SAG PA SAG AN SAG Username SAG Passacril		
Add on Status Last Error		Connected			
Network Eleks Actus SA Metuson Nume Daywe Band Nati NG		BAH SHARKI SHARKI LTE N BETERRHIFTER HETERRHIFTER			
SVS Recipents Append to SVS this test					
SHIP Server SHIP For Manya annatatin SHIP Autoretastan SHIP Feasare SHIP Feasare SHIP Feasare SHIP Feasare SHIP Server) Smil Salpet	GPS Status Fix Satellites Found Latitude Longitude			No fix 0 0.00000 0.00000	
Append to Email this lead	Update Reset				
Fx Ballies Fund Lathur Longton		No. 14 G 0-80880 0-90880			
Upters Reset					

9.4.7 Inserting the SIM card into the LTE Add-On

1. Insert the SIM card(s) as shown in the image below(SIM card should be inserted all the way to the back).



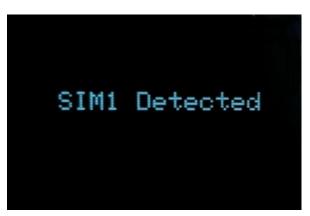
Note: that for security reasons the only way to remove the SIM card is by using tweezers as shown on the illustration below.



2. Connect your ADDON-LTE into your base unit, initialization will start.



3. If SIM is inserted correctly the device will show that it has been detected and will start to register into your mobile network.



Note: That if it keeps on initializing and does not go to "Registering to network" then it means that the SIM card is not well inserted.



4. After the device successfully registers, it will have the default screen below showing the status of your ADDON-LTE.



5. If you have the optional GPS feature then please allow 5-10 minutes before the GPS signal is established.

6. Your ADDON-LTE will be ready for use, for SMS set up please go to section 3.9 and for email set-up go to section 3.2.

10 InfraSensing sensor probes

10.1 External sensor probes



InfraSensing uses external sensor probes for its environmental monitoring solution.

Only the power sensor requires a power adapter plugged into it; the power adapter's current sent to the sensor will be used to analyze the power state.

You can replace the shipped RJ45 cable with a custom standard RJ45 for a length of up to 10 meters or 33 ft between the Base Unit and an external probe. And can go longer with the use of CAT6/ CAT7 cables for up to 100m or 330 ft.

10.2 General instructions

The sensor should be connected as shown in the picture below. The RJ45-to-RJ45 cable goes from the external sensor probe into the bottom of the Base Unit using the RJ45 connector labeled **Serial** (for Base Unit v1, v2 & v3) Base Unit v4 or higher have 2 connectors for external probes labeled **Probe1** and **Probe2**



On the top you plug in your network cable connected to a switch and this into the RJ45 connector labeled **LAN/PoE** If you don't have a PoE enabled network, then you will need the optional 12DC power adapter and plug it into the connector on top labeled **DC 12V**

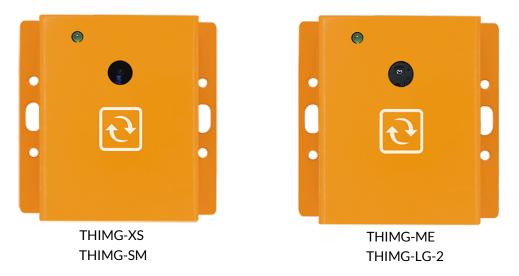


Important note: It is highly recommended to reboot the Base Unit after adding or removing any sensor probes for stability. Also, using incorrect power supplies or wrong PoE source may permanently damage the equipment and void the warranty.

11 THERMOGRAPHY SENSORS

11.1 Thermography Sensor (THIMG-XX)

The world's first SNMP & Modbus temperature monitoring sensor that tells you what it actually sees. 192(XS), 768(S), 4800(M), or 19200(L) temperature measurement points in one image, analyzed every 2 seconds.



11.1.1 Installation of Thermal Image

Once the Thermal Sensor is plugged in, you should see a button on the gateway's GUI named "Thermal Camera" (firmware 8.0 and above). Once you click the option you will see the live feed of your thermal camera.



With firmware version 9, the Base Unit can connect up to 5 Thermal Imaging Sensors provided that they are connected to the high-speed ports (1, 2, 3, 4, and 7) of the SensorHub.

With the latest firmware version 9.1, the device is now capable of measuring thermal imbalances, which represent the difference between the highest maximum and lowest maximum temperatures.

Senso	rs					
Status	Туре	Name	Value	Warning Range	Down Range	R
	Temperature	Int. Temp1	26.69 °C	<18 OR >30	<15 OR >37	
	Ping	Int. Ping1	46 ms	>50	>60	
	Fault	Int. Fault1	FAULT	-	SET	
	Temperature	Ext. Temp2	13.49 °C	<18 OR >25	<15 OR >29	
	Temperature	Ext. Temp3	15.18 °C	<18 OR >25	<15 OR >29	
	Thermal Temp	Temp Min1	38.3 °C	<18 OR >25	<15 OR >29	
	Thermal Temp	Temp Max5	38.72 °C	<18 OR >25	<15 OR >29	
	Thermal Temp	Temp Min2	38.18 °C	<18 OR >25	<15 OR >29	
	Thermal Temp	Temp Max2	38.7 °C	<18 OR >25	<15 OR >29	
	Thermal Temp	Temp Min3	38.2 °C	<18 OR >25	<15 OR >29	
	Thermal Temp	Temp Max3	38.78 °C	<18 OR >25	<15 OR >29	
	Thermal Temp	Temp Min4	38.34 °C	<18 OR >25	<15 OR >29	
	Thermal Temp	Temp Max4	38.78 °C	<18 OR >25	<15 OR >29	
	Thermal Imbalance	Thermal Imbalance1	0.08 °C	>5	>10	

Thermal Imbalances = highest maximum - lowest maximum Based on the image above the thermal imbalance is 0.08°C

NOTE: Due to transit or unforeseen events, in rare occasions the values of thermal camera sizes M and L are not displayed. This is possibly due to the sensor getting slightly loose. This is remedied by pressing down on the lens assembly in front of the case to reseat it in its socket.

Link : <u>https://infrasensing.com/sensors/sensor-thermal-image-temperature.asp</u>

11.1.2 Adding Zones to the Thermography Sensor Camera

From firmware version 8.8, you can add zones within the thermal view page to specifically pinpoint the highest temperature recorded in each zone.

To add a zone, please follow these steps :

- 1. On the main screen, click Thermal Camera and you will be redirected to the thermal view page.
- 2. You can add up to 4 zone. To add a zone, simply highlight an area within the camera vie w.
- 3. Once done, click "Updated Selected Zones"

11.1.3 Delete Zones from the Thermal Imaging Sensor Camera

- 1. On the Thermal View, press middle-click (scroll button) on your mouse to delete a zone.
- 2. Once done, click "Updated Selected Zones"



The C-THIMG-SM is a compact thermal image sensor designed for switchgear, offering a comprehensive solution to monitor all bus bars with its 768 discrete temperature measurement points and 4 reporting zones. It's mountable inside switchgear or onto existing IR windows.

It's mountable inside switchgear or onto existing IR windows, UL 61010 recognized, and integrates seamlessly via Modbus TCP or SNMP. Optionally available as an RS-485 sensor for direct integration with PLC and other systems, it provides flexible deployment options for efficient monitoring.

11.3 Industrial Infrared Spot Sensor (THIMG-IRSPOT)



Works by capturing the emitted infrared radiation within a wide field of view (90°)



11.4 Industrial Infrared Spot Sensor – Cylindrical Series (C-THIMG-IRSPOT)



The C-THIMG-IRSPOT is an industrial digital SNMP & Modbus TCP sensor designed for contactless temperature monitoring inside enclosures. It offers a flexible and scalable solution with an optional daisy chain configuration, supporting up to 20 IR Spot sensors per Base Unit. This makes it ideal for comprehensive temperature management, whether monitoring individual components or entire systems within industrial enclosures

12 Gas Sensors

12.1 VOC, Temperature and Humidity Sensor (GAS-VOC)



Designed for monitoring off-gas in battery systems. Measures Volatile Organic Compound(VOC), Temperature and Humidity.

12.2 Flammable Gas Sensor (R-GAS-FLAMMABLE)



Calibration free flammable RS485 version gas sensor that is specifically designed to detect the presence and measure the concentration of specific gases in nonhazardous critical facilities. User settable address (RS485) out of 256 possibilities

The relay from the R-GAS-FLAMMABLE sensor can also be used with the Base Unit. To enable this, follow these steps.

1. Access the settings by navigating to [IP_ADDRESS]/calibration2.html in your browser.



2. Scroll down until you find the **R-GAS-FLAMMABLE** section.

AS-F		ABLE		7
	r Sources:			
F	Relay1:	Direct Control	\$	
F	Relay2:	Direct Control	\$	
F	Relay3:	Direct Control	\$	
l	Set Sources			
Thresh	olds:			
F	Relay 1:	0	٢	
F	Relay 2:	0	٢	
F	Relay 3:	0	٢	
	Set Threshold	ds		
	is Config:			
E	Baudrate:	9600	\$	
F	Parity:	None	\$	
S	Stop Bits:	2	\$	
1	Set Config			

3. Under Trigger Sources, ensure that all three relays are set to "Direct Control".

Trigger Sources	:			H2
Relay1:	Direct Control	¢	R-GAS-FLAMM	Temperature
Relay2:	Direct Control	\$		Humidity
Relay3:	Direct Control	•	Trigger Sources:	VOC
Set Sources			00	CH4
Set Sources			Relay1:	✓ Direct Control
Thresholds:				Fault
Relay 1:	0	•	Relay2:	Other Flammable Gas
Relay 2:			51.0	
rioldy 2.	0	٢	Relay3:	Direct Control

4. Once configured, return to the **Sensor Home Page** and reload the page.

Status	Туре	Type Name Value			Down Range	Repeat Alarm	Email	Alert+	SNMP Trap	Set Output To		
	Temperature	Int. Temp1	27.34 °C	<18 OR >37	<15 OR >41					DISABLE	\$	- 4
	Ping	Int. Ping1	203 ms	>50	>60					DISABLE	\$	- +
	Ambient VOC	Ambient VOC1	19	>200	>400					DISABLE	•	- \$
	VOC Alarm	Alarm VOC1	ок	-	SET					DISABLE	\$	- +
	VOC Index	VOC Sensor1	19	>100	>400					DISABLE	\$	- +
	H2	H2 Sensor1	0 %LEL	>25	>50					DISABLE	\$	- ‡
	Temperature	Ext. Temp1	30.04 °C	<18 OR >25	<15 OR >29					DISABLE	\$	- +
	Humidity	Humidity1	44.01 %RH	<45 OR >65	<40 OR >70					DISABLE	\$	- +
	Flammable Gas	Flammable Gas1	0 %LEL	>25	>50					DISABLE	\$	+
Control Outputs				Current Value		Default State				Edi Control Output		
Relay1				OFF		OFF			¢	CYCLE		
Relay2			OFF		OFF			¢	CYCLE			
Relay3			OFF		OFF \$			\$	CYCLE			

5. You should now see the three relays listed under **Control Outputs.**

The relay from the R-GAS-FLAMMABLE sensor can also be used with the Base Unit. To enable this, follow these steps

12.1 Panel Sensor (R-EGD-PANEL)



Our Panel Sensor has been designed for early detection of anomalies inside automation and electrical panels. By monitoring factors like VOCs, NOx, CO, smoke, temperature, and humidity—which are signs of overheating, insulation breakdown, or component failure—it can potentially alert you before minor issues escalate into catastrophic failures.

12.2 Ozone (O3) Gas Sensor (EGD-O3)



Digital sensor designed for monitoring and measuring the level of Ozone (O3) in the ambient air.

12.3 Sulfur Hexafluoride (SF6) Gas Sensor (EGD-SF6)



Measures SF6 concentrations up to 1,000ppm (parts per million)

12.4 Refrigerant A1 (R-410A) Gas Sensor (GAS-A1)



Digital sensor designed to monitor refrigerant gas leaks and can measures ASHRAE A1 class refrigerant gas sensor.

12.5 Refrigerant A2L (R-32, R-454B, and R454C) Gas Sensor (GAS-A2L)



Measures Refrigerant gas concentrations up to 10,000ppm (parts per million)

12.6 Refrigerant A3 (R-290) Gas Sensor (GAS-A3)



Measures Refrigerant gas concentrations up to 10,000ppm (parts per million)

12.7 Gas Sensor Bump Test

We recommend to periodically test the operation of the gas sensor in critical environments. OSHA defines a bump test as "a qualitative function check in which a challenge gas is passed over the sensor(s) at a concentration and exposure time sufficient to activate all alarm settings."

Required equipment:

- 1. Base Unit (BASE-XX)
- Gas sensor
 Bump test adapter (SPARE-GAS-GEN-BUMP)
- 4. Gas canister (from your local gas supplier)
- 5. Gas tubing (from your local gas supplier)

Note: For the amount of pressure, we can only apply up to 1000 PSIG.

Procedure:

- 1. Connect the Gas sensor to the Base Unit.
- 2. Next, connect the bump test adaptor to the gas sensor.
- 3. Attach one end of the tube to the adaptor.
- 4. Attach the other end of the tube to the gas cylinder source
- 5. Open the cylinder valve to apply gas until detected.
- 6. Stop applying gas by closing the cylinder valve.

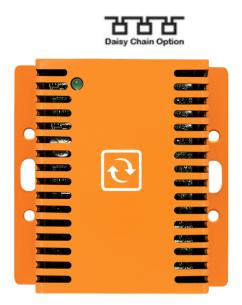
13 Environmental Sensors

13.1 Temperature Sensor (ENV-TEMP)



Designed for indoor use inside data centers, server rooms and cabinets. Optional calibration certificates available.

13.2 Temperature & Humidity Sensor (ENV-THUM)

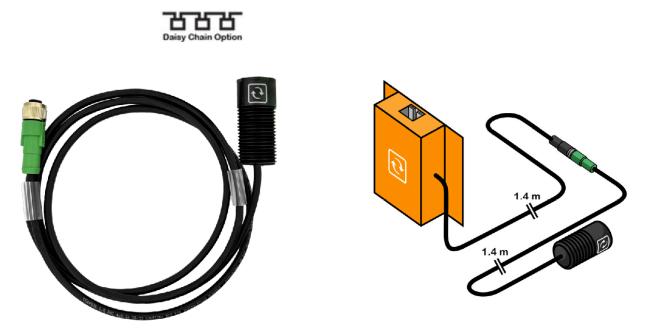


Designed for monitoring temperature and humidity levels inside data centers, server rooms, cabinets and other critical facilities. Humidity probe made in Switzerland.

Considerations for humidity sensor:

- Very dependent on air flow
- For rooms with different levels of air flows which is usually those in front of AC units and those that aren't, you can calibrate accordingly for more accurate results of ambient level and rack or other specific point levels of humidity

13.3 ISO17025 Calibrated Cylindrical Temperature & Humidity Sensor (C-ENV-THUM)



The C-ENV-THUM is a cylindrical version of plug & play sensor designed for monitoring temperature & humidity inside racks and hot/cold aisles in data center white spaces by hanging from ceiling.

13.4 Magnetic Surface Temperature Sensor (ENV-TEMP-MAGNETIC)



The magnetic probe can be attached to any metal surface and measure its temperature.



13.5 Digital Sound and Noise level Sensor(dbA) (ENV-NOISE)



Designed for indoor use, this monitoring system ensures compliance with OSHA regulations and HCAHPS standards by accurately tracking and managing sound and noise levels.

Note: Detection for ENV-NOISE Takes up to 30 seconds before appearing on your interface.



13.6 Atmospheric Corrosion Sensor (ENV-CORROSION)

This non-intrusive plug & play corrosion sensor empowers users in mission-critical industries to effectively monitor atmospheric corrosion levels in real time and to compute the G level classification of the monitored infrastructure.

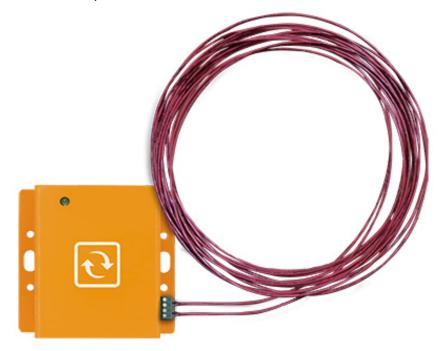
13.7 Differential Air Pressure and Temperature Sensor (ENV-AIRPRESSURE)



Designed in the USA for monitoring differential air pressure and air temperature in data centers, server rooms, healthcare facilities and other critical facilities. Pressure and temperature sensors are made in Switzerland.

13.8 Linear Heat Detection Sensor (ENV-LHD)

Digital sensor that uses the linear heat cable. This sensor is capable of sensing heat anywhere along the cable and initiate an alarm once it's fixed activation temperature is reached. Unlike the linear heat cables, the senso device is not a fire safety device. It is a temperature limit detection device.



13.9 Optical Dust Sensor Probe (ENV-DUST)

Air Quality (dust) is an invisible threat to Data Centers, server rooms, equipment rooms, telecom shelters, also Haze due to forest fires or fossil fuels is a common source of dust particles. Typically air-conditioning units can purify the air but when high peaks of pollution are reached, then they may no longer cope. Dust deposits on circuit boards can damage it. This may result in permanent loss of IT equipment such as servers, network and storage systems.

Our sensor is designed to monitor dust particles in data centers, server rooms & cabinets.



13.10 Particle Sensor (ENV-PARTICLE)

Designed to provide added value to applications in several industries, including air quality monitoring air purifiers and HVAC.



13.11 Water Leak Sensor (ENV-WLEAK-COMBO5M)

*Fuel and battery cables are also available and all cables can be expanded up to 200m or 660ft (ENV-FLEAK-COMBO and ENV-BLEAK-COMBO)





IMPORTANT NOTICE FOR WATER / FLOODING SENSORS

The flooding / water detection sensor consists of 2 parts: the sensor (gray box with InfraSensing label on it) and the yellow water sensing cable (shown left). **Only the yellow cable may be submerged** – this is the water sensitive part of the sensors! The sensor probe (gray box) has to be kept at all times above the water level.

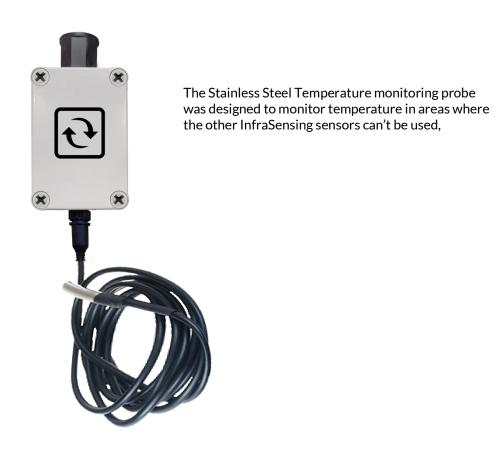
Should you need to pinpoint the exact location of the leak, then we also have a Water leak location module. (ENV-WLEAK-LOC-COMBO5)

13.12 Optical Oil & Hydrocarbon Leak Sensor (ENV-LEAK-OPTICAL)



A reusable, contactless sensor designed to detect liquid hydrocarbon presence on surfaces. Utilized optical sensing to monitor hydrocarbon leaks with the option for calibration to detect surface area.

13.13 Stainless Steel Temperature Probe (ENV-TSTAIN)



13.14 Extreme Low Temperature Sensor (ENV-TULTRA)



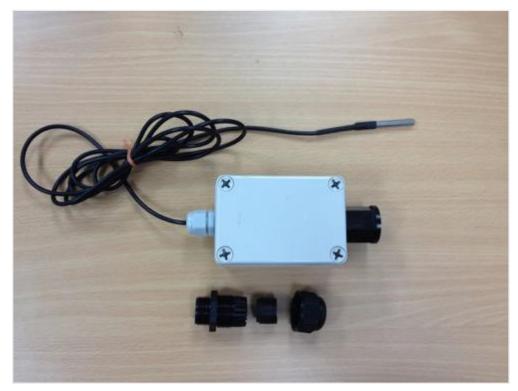
This sensor was designed to monitor temperature in applications where our traditional temperature sensors can't be used. With its IP 66 rated enclosure and stainless steel protected platinum sensor head, this sensor can be used in extreme low temperature environments of up to -200°C(-328°F)

13.15 Industrial Surface Temperature Sensor (ENV-TSURFACE)

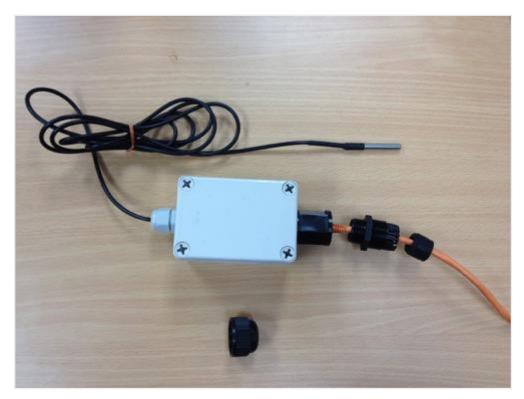


13.16IP rated sensor assembly (leak, industrial probes, etc.)

Out from the box, for the Ethernet connector, you should have the 3 parts that are yet to be assembled: the over-nut, rubber gasket, and contracting gland (from left to right).



To get started, insert the over-nut and rubber gasket in your LAN cable then plug it in on the protruding RJ 45 connector from the sensor probe.



Once that's done, insert the rubber gasket all the way inside the over-nut.



After that, connect them both on the RJ 45 connector of the sensor.



Now that we have that, we just need to insert the contracting gland to seal the Ethernet passthrough. Your stainless steel temperature sensor should now look similar to the following image.



13.17 Water Spot Detection Sensor (monitors a specific spot) (ENV-WSPOT)



The water spot sensor is used in applications where the water leak sensor can't be deployed. Detects water from the location where it is placed wherein water makes contact to the 2 rods.

Note: Once an alert is triggered using our water spot detection sensor, make sure the metal prongs are dried before reusing.

13.18 View of the Airflow Sensor (ENV-AIRFLW)



The displayed side will be the one where the air should be allowed to flow. As an example, on an environment where floor cooling is utilized, the implementation would be similar to the ff. figure:



As we're utilizing floor cooling on this example, the side where the air should flow is placed facing downwards to detect the airflow it should have.

14 Daisy Chain



This icon represents sensors with the optional Daisy Chain Version.

Please upload the special firmware to your Base Unit (BASE-XX) for the daisy chain sensors to work. You may download the firmware here <u>Daisy Chain Firmware</u>

Please refer to section 2.11 on how to properly upload the firmware.

14.1 Daisy Chain Temperature Sensor (DAISY-TEMP)



Designed for monitoring temperature and humidity levels inside data centers, server rooms, cabinets and other critical facilities. Offers optional calibration certificates. With a streamlined setup requiring only one IP address for every daisy chain, it can seamlessly connect up to 15 DAISY-TEMP sensors.

14.2 Daisy Chain Temperature and Humidity Sensor (DAISY-THUM)



Designed for monitoring temperature and humidity levels within critical facilities such as data centers, server rooms, and cabinets. Also, has the capacity to connect up to 15 DAISY-THUM sensors.

14.3 Daisy Chain Infrared Spot Sensor (DAISY-THIMG-IRSPOT)



Industrial digital SNMP & Modbus TCP sensor designed for contactless temperature monitoring inside enclosures. The sensor returns the average temperature of everything within its field of view. Can connect up to 20 THIMG-DAISY-IRSPOT sensors per daisy chain and only 1 IP address required for every daisy chain.

14.4 Daisy Chain Temperature Magnet Sensor (DAISY-TEMP-MAGNET)



This sensor was designed to monitor temperature in applications where our traditional temperature sensors can't be used. The magnetic probe can be attached to any metal surface and measure its temperature and has a high temperature silver plated shielded wire with strong magnetism and strong absorption.

14.5 ISO 17025 Calibrated Cylindrical Daisy Chained Temperature & Humidity Sensor (C-DAISY-THUM)



Plug & play sensor designed for monitoring temperature & humidity inside racks and hot/cold aisles in data center white spaces. Also, has the capacity to connect up to 20 C-DAISY-THUM sensors. With an optional RS-485 (Modbus RTU) output.



14.6 Daisy Chain Start (DAISY-STARTER)

The DAISY-STARTER serves as the controller for the daisy-chained sensors. It is required for all our daisy chain sensors.

Note:

The DAISY-STARTER cannot be connected to Sensorhub (EXP-8HUB) and Multi-Sensor & Hub (EXP-4HUB)

Only one DAISY-STARTER can be connected to one Base Unit (BASE-XX).

14.6.1 Connecting Daisy Chain Sensor

The ports on DAISY-STARTER and DAISY SENSORS are labeled "**IN**" and "**OUT**". This is to ensure that you are connecting each device accordingly. See images below for reference.



DAISY-STARTER



DAISY-THUM

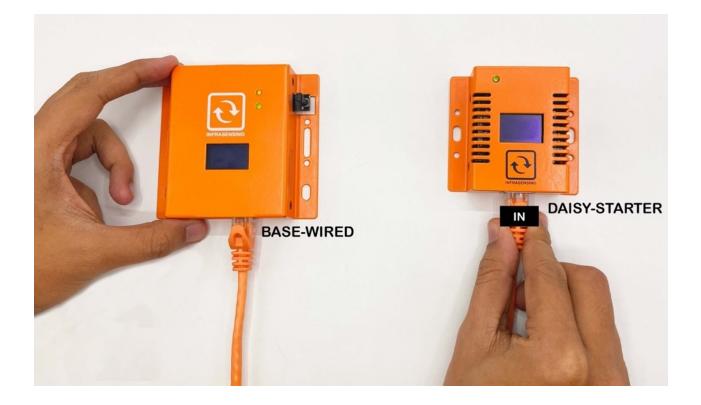


Images above shows the IN and OUT ports labeled on your sensors.

Before proceeding, it's important to prepare all the necessary devices. Ensure that you have both the BASE-XX and DAISY-STARTER devices on hand. Keep in mind that each BASE-XX can only connect to one DAISY-STARTER. In the example below, we used DAISY-THUM SENSOR.



First, connect your BASE-XX to your DAISY-STARTER using a regular RJ45 cable. Refer to the image below for reference :

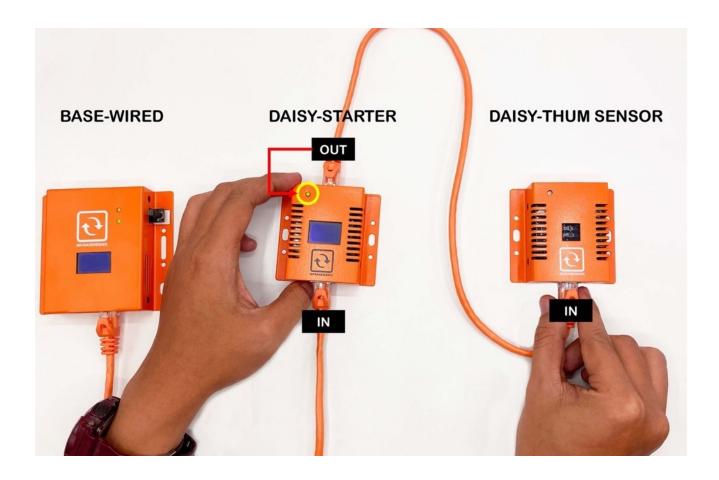


Once you have connected the BASE-XX and DAISY-STARTER, it's time to connect the DAISY-THUM sensor. Begin by locating the OUT port on the DAISY-STARTER and the IN port on the DAISY-THUM sensor. These ports are typically labeled for easy identification.

Next, take a regular RJ45 cable and connect one end to the OUT port on the DAISY-STARTER and the other end to the IN port on the DAISY-THUM sensor. Ensure that the cable is securely plugged in on both ends to establish a stable connection. Please refer to the image below for reference.

Take care not to force the cable into the ports, and avoid pulling on the cable once it is connected. Once the connection is established, you're ready to move on to the next step.

NOTE: The port near the led indicator is always the OUT port. Even you have a label that would say IN, but it's near the led indicator, that would basically be the OUT port.

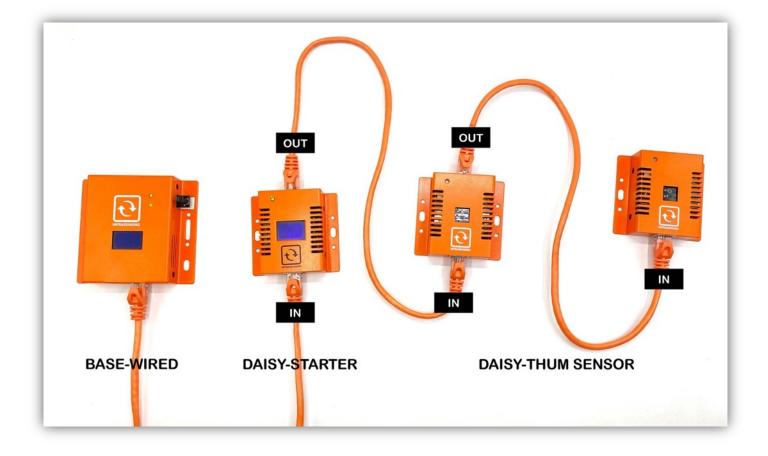


Now that you've successfully connected the first DAISY-THUM sensor, you can repeat the same process for any additional sensors you have. Remember to locate the OUT and IN ports labeled on each sensor.

Using a regular RJ45 cable, connect the OUT port of the first sensor to the IN port of the next sensor. Keep repeating this process until all of your sensors are connected.

Make sure to refer to the diagram below for guidance. It's important to ensure that all sensors are securely connected and that the cables are not tangled or stretched too far.

NOTE: Up to 15 daisy sensors per base unit within 100m/330ft of total length Longer distances possible with optional DAISY-BOOSTER



Now that all of your sensors are connected, it's time to power up your Base Unit. You have several options for powering your device:

- 1. POE (Power over Ethernet): You can power your Base Unit directly through the Ethernet cable.
- 2. BASE-PWR: You can also use power adapter to plug your Base Unit directly into an electrical outlet.
- 3. BASE-PWR-USB: If you don't have access to an electrical outlet, you can power your Base Unit using a USB cable connected to a computer or other USB-enabled device.



Note:

The Base Unit and Daisy Chain Start connecting cable should not be more than 2 meters (6.6 ft.) in length. Additionally, the total length of the daisy chain, including the Daisy Start and Gateway, should not exceed 100 meters. However, if you require a longer distance, you may extend the daisy chain with the use of Daisy Booster.

Now that you have everything set up and your Base Unit is powered on, you can access it by obtaining the IP address displayed on the device. To do this, check the device manual or packaging for instructions on how to find the IP address.

Once you have the IP address, enter it into your web browser to access the Base Unit's user interface. From there, you can view and manage your sensors and configure settings for your system.



If you have daisy-chained sensors, you may see a new menu that displays all of your connected sensors. Refer to the image below for an example of what this menu might look like.

Status	Туре	Name	Value	Warning Range	Down Range
	Temperature	Int. Temp1	17.99 °C	<18 OR >37	<15 OR >41
	Temperature	Daisy Sensor1	18.65 °C	<18 OR >25	<15 OR >29
	Humidity	Daisy Sensor2	51.29 %RH	<45 OR >65	<40 OR >70
	Temperature	Daisy Sensor3	18.49 °C	<18 OR >25	<15 OR >29
	Humidity	Daisy Sensor4	51.95 %RH	<45 OR >65	<40 OR >70

To identify the chained sensors in your Daisy chain, simply click on the "Scan for connected Daisy Chain Sensors" option. This will prompt your Gateway to perform a scan, which typically takes less than a minute. If you need to scan again, you may click on the same button after one minute.

Ð **Daisy Chain Sensor Config** No. Status Serial Name Туре Temperature DSS-TH004587 Daisy Sensor1 1 DSS-TH004587 Daisy Sensor2 2 Humidity 3 DSS-TH004046 Daisy Sensor3 Temperature DSS-TH004046 4 Daisy Sensor4 Humidity Scan for Connected Daisy Chain Sensors

14.7 Daisy Booster



The DAISY-BOOSTER extends the operating length of the daisy chain sensors from 100 meters up to 200 meters. It is connected between 2 sensors on the daisy chain for those applications where the standard total length of 100m/300ft for a daisy chain is too short.

You can add a DAISY-BOOSTER anywhere on your daisy chain. When adding a booster, be sure to pay attention to the color indications to ensure that it is properly connected. It has a led to show optimal placement of DAISY-BOOSTER.

Color Indicator :

Red 📃	The placement of the Daisy Booster is not optimal
Yellow	The placement of the Daisy Booster is fairly good
Green	The placement of the Daisy Booster is optimal

15 Power Sensors

15.1 View of DC Voltage Sensor Sensor (12-80V) (PWR-DC-VOLT)

DC voltage measurement & failure monitoring sensor. Designed for industrial +24v environments and -48v telecom infrastructure..



15.2 View of Current Sensor (PWR-AC-CUR)

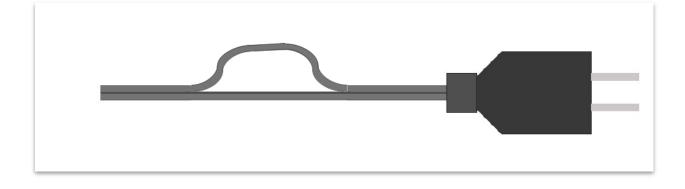


- 1. Just plug the sensor to your gateway via Ethernet cable.
- 2. Make sure you place the current clamp correctly as shown below.

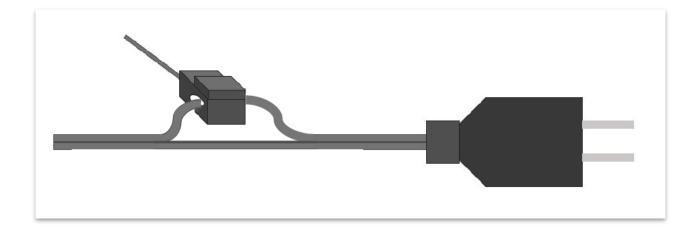
Example Plug going to the wall outlet



Make sure you separate the wire as shown on the image below You do not have to peel the protective rubber covering the wire but make sure that the two wires are separate.



Clamp the transducer on either of the wires and check if you have reading over the gateway GUI.



15.3 View of AC power failure (PWR-AC-FAIL)

The power failure sensors enable you to get alerts when the main power goes out.



Almost any server room is equipped with UPS systems (batteries) that kick in when the main power supply goes out. However knowing when this occurs is a different thing. While the more expensive UPS systems have some kind of management and alerting system, the most popular ones don't have it.

The power failure sensors from enable you to get alerts when the main power goes out as well as measure the actual voltage.

In combination with our PWR-AC-CUR, you can measure power more accurately.

15.3.1 Main sensor unit (PWR-BAT-STRING)



Main unit for the battery monitoring system where the battery cell sensors as well as the string current sensor are connected.

Sensor Units (PWR-BAT-CELL)



Note:- for Li-Ion batteries monitor for following toxic gasses: Hydrogen Fluoride (HF), Carbon Monoxide (CO) or Carbon Dioxide (CO2)

- For lead acid batteries the primary gas to monitor is the Hydrogen gas (H2). Monitoring up to 100% Lower Explosive Limit (LEL).

The gas detectors can be optionally mounted onto the PWR-BAT-STRING module or can be purchased as separate gas sensors.

You can chain connect up to 15 PWR-BAT-CELL for every PWR-BAT-STRING.

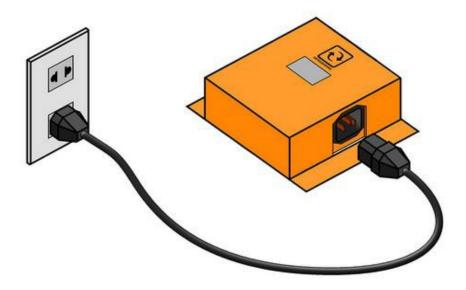
15.4 Power Quality Sensor (PWR-AC-QUAL)



Using industry standards, it will analyze and translate your power quality in simple and actionable information.

Plug and play. Simply connect an IEC C13-C14 cable to the unit and into the power wall outlet you want to monitor. As soon as it is powered, it starts monitoring. It is that simple.

It is designed to monitor single-phase power quality in your critical facilities and edge infrastructure sites.



- 15.4.1 Initial set up for the power quality sensor using BASE-XX
- 1. Connect your power quality sensor into your power outlet using an IEC C13-C14 cable, then via Ethernet cable going into your Base Unit.

Vot	Volt Meter1	198.4 V	445 OR >250	+44 OR >300			DISABLE	•	+	٠
Voltage Status	Voltage Status1	BROWNOUT		SET			DISABLE		(e	
THD	THD1	1.1%	>5	>10			DISABLE	-	(e) -	
Prequency	AC Frequency1	eo os Hz	<50 OR >50	<40 OR >70			DISABLE	-		•

2. Access your Base Unit, the above image should be visible from your homepage, now we have to set up the correct reference voltage, to do this we have to go to Settings>Calibrate Sensors

Temp Threshold	0.00		0.00
Humidity Threshold	0.00	•	0.00
AC Votage Type	220/240	110/120	
AC Voltage Offset	7	•	0.00
Sync Internal Temp Sensor with External			
Power Quality	230 Volts / 60 Hz		3

```
Update Reset
```

3. Under the Calibration option, just scroll down until you see the option for Power Quality, then apply the correct Voltage reference. The power quality sensor would also sync its time with Base Unit upon updating the calibration option.

Although you can fully customize the alerting parameters, we recommend the table below as your guide.

State	Description	Actual V	Voltage Threshold	Duration
OK		Within +/-6%	+/-6% from reference	
Warning	SAG	Low voltage	- 6% from reference Voltage	0 to 1min
Down	BROWNOUT	Low voltage	- 6% from reference Voltage	> 1min
Warning	SWELL	High voltage	+6% from reference Voltage	0 to 1min
Down	LONG SWELL	High voltage	+6% from reference Voltage	> 1min
Down	INTERRUPTIO N	Zero Voltage	Voltage is zero	< 5 sec
Down	FAILURE	Zero Voltage	Voltage is zero	>= 5 sec
Down	TRANCIENT	Sudden Spike	>30%	Few milliseconds (lightning, etc.)

15.4.2 Initial set up for the power quality sensor using SD card .ini file

- 1. Connect your power quality sensor into the power outlet using an IEC C13-C14 cable, then connect it to the PC using the USB Type-B to USB cable.
- 2. Access then SD Card using your PC's file explorer, then open the .ini file. The .ini file contains the parameters that are used by the PWR-AC-QUAL.
- 3. In the .ini text file, change the following:

Parameter	Value
"VOLT_DEFAULT"	230
"F_DEFAULT"	60
"SET_TIME" • After you have enabled this option, set the YEAR, MONTH, DAY, HOUR, MIN, and SEC according to the current timestamp.	YES

Sample file:

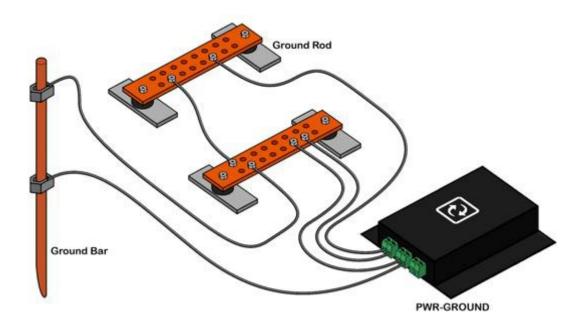
"RELEASE"		3.00	
"DATE"		Sep_25	_2019
"VOLT_DEFAUI	_T"		230
"F_DEFAULT"		60	
"CALIBRATED"		YES	
"VOLT_OFFSET	-11		1
"VOLT_CODE1	00"		455300
"VOLT_CODE2	00"		912400
"SET_TIME"		YES	
"YEAR"	2022		
"MONTH"	02		
"DAY"	03		
"HOUR"	17		
"MIN"	24		
"SEC"	00		
}			

4. After the parameters are changed, save the file.

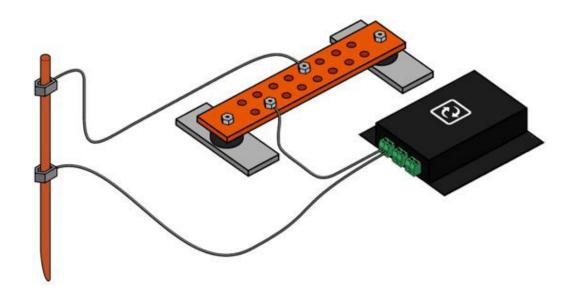
15.4.3 Ground (Earthing) Monitoring Sensor (PWR-GROUND)



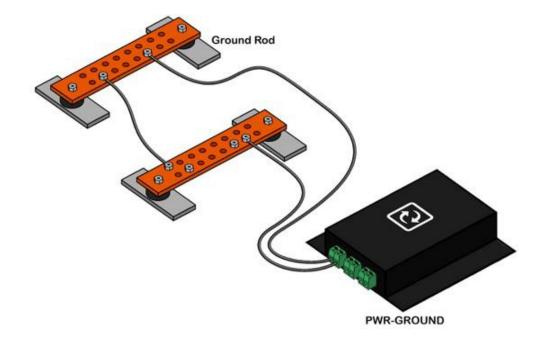
The InfraSensing Grounding Monitoring system connects to your facilities or sites electrical ground system. It checks non-stop the grounding's resistance. This allows you to get early warning on your grounding system.



The above image shows our grounding sensor which checks the ground bar connected to the ground rod as well as the connectivity of 2 ground rods.



Ground bar connected to your Ground Rod



Ground rod connected to another ground rod

The above applications show that our sensor would continuously check if there are changes in your grounding system such as:

- accidental disconnected grounding systems
- corrosion of copper ground bars due to environmental conditions
- copper ground theft

Use solid/stranded wires with sizes 26-16 AWG to connect to the terminal blocks of the sensor.

15.5 IP68 Ultrasonic Fuel Level Sensor (PWR-FUEL)

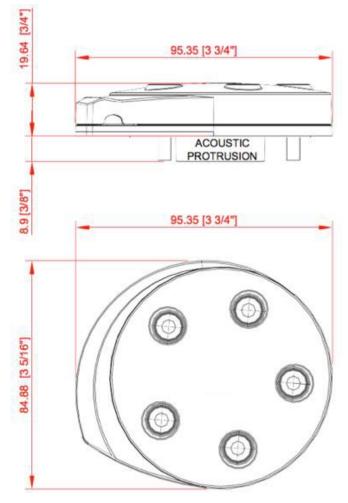
15.5.1 Features

- Plug & Play
- Contactless (ultrasonic) fuel level measurement
- Operating distance of 0mm to 2000mm maximum
- Measures fuel level inside tanks with depths of up to 2m (6.5ft) with wall thickness of up to 6mm.
- Supports metal and plastic tanks
- Extremely low profile only 20mm high once mounted
- IP68 rates for outdoor use
- Calibrated in factory based on specs of your tank
- In operating temperatures of 4°C to 65°C (39F to 148F)
- ISO 884 6ignition protected
- Fire Resistance tested to ABYC, US Coast guard and ISO 10088Industry standard SAE-5 stud mounting pattern with gasket seal and washers. Resistant to Petrol and Diesel

15.5.2 Maximum Tank Depths

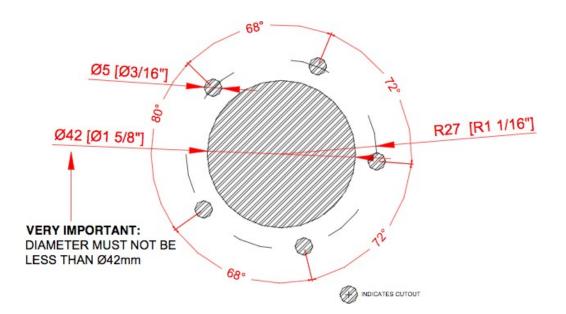
- Operating distance of 0mm to 1100mm for Petrol tanks
- Operating distance of 0mm to 2000mm for Diesel tanks
- Operating distance of 0mm to 1500mm at 55°c
- •

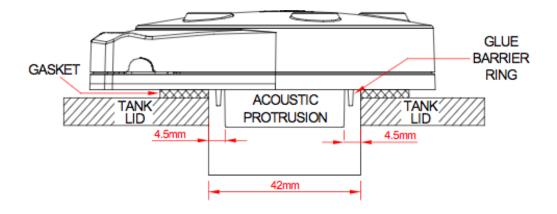






15.5.4 Mounting and installation





IMPORTANT SIDE WALLS OF ACOUSTIC PROTRUSION MUST BE NO CLOSER THAN 4.5mm TO THE TANK SIDES OF THE CUTOUT HOLE

- The acoustic protrusion should be positioned in the tank aperture in the center of the hole. The protrusion should ideally be protruding into the tank and not be recessed in the hole. See drawing above.
- For tightening screws ensure base and washers are sitting flat. Tighten screw until screw head makes contact with the washer, and then tighten another 2 full turns.

Maximum torque for the mounting screws is 0.5 Newton meter.

Note: Drawing is not to scale. Please use the tank gasket as a template and make sure the tank hole is 42mm.

15.5.5 Tips and example installations

- The sensor must not be mounted closer than 150mm from the center to the sides of the tank, baffles or other intrusions.
- Only use on tanks greater than 200mm in depth.
- Sensor must be mounted parallel to the surface of the liquid.
- Make sure that sensor protrusion is NOT in contact with any object including Sealan ts when mounted.
- Use gasket and fittings as provided.
- Mount above deepest point of the tank.

Case 2

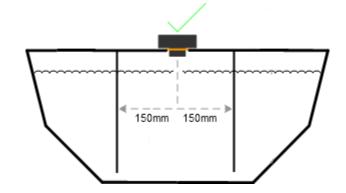
Case 1

The sensor must be mounted at least 150mm from a vertical tank baffle, tank walls and piping.

The sensor must be mounted at the deepest tank point!

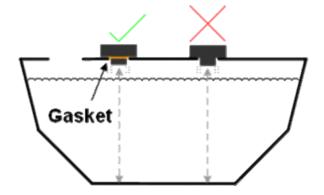
correct level when the depth is varying due to wave slop.

It is recommended the sensor is mounted in the middle of the tank, this is particularly important on low or no baffled tanks that are mounted in moving vehicles or vessels. This allows the sensor to average waves of fuel to the



Case 3

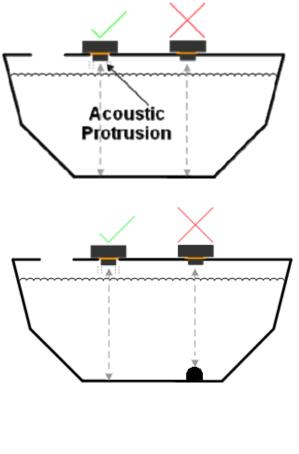
Use 5 washers provided, washers must be placed under screw heads to prevent rubber lid damage.



Case 4 Acoustic protrusion must not touch the tank frame.

The sensor must be mounted so it can see the bottom of the

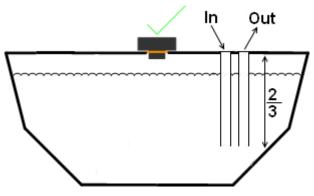
tank if the fuel is to be measured to the bottom.

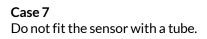


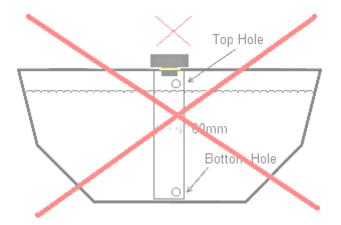
Case 6

Case 5

Inlet and Outlet piping must go in at least 2/3rds of the way in to the tank to stop turbulence when filling.

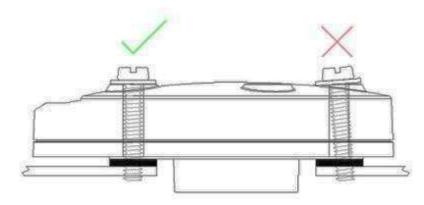






Case 8

Ensure bolts and mounting holes are aligned properly to keep plastic body isolated acoustically from tank. Do not over tighten the screws.



16 Industrial sensor

16.1 Industrial 0-10V (IND-0-10V)



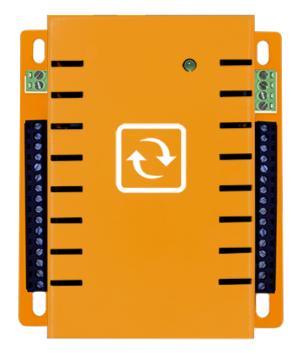
Designed to read ay 3^{rd} party sensors that has output of 0-10V. Can power up sensors with auxiliary 12V DC supply.

16.2 Industrial 4-20mA (IND-4-20mA)



Designed to read any 3^{rd} party sensors that has output of 4-20mA. Can power up sensors with auxiliary 12V DC supply.

16.3 The IO Sensor Probe – 16 Dry Contacts IN & 4 OUT (IND-IO)



16.4 General description

The IO sensor probe is a 16-zone expander for the Base Unit that adds up to 16 dry contacts for sensor alarm detection and indication. It has 4 output lines that can drive sirens and strobe lights. It is also capable of giving a 12-volt power supply and a maximum of 700 mA current capacity, enough to power several sensors and output devices.

Note: Only one IO Sensor Probe per Base Unit with no other sensors connected, It needs to be directly plugged in one of the ports (does not work with expansion hubs)

16.5 Applications

- SNMP interface sensor trigger and status
- SNMP traps sent when a change of state occurred
- SNMP polling for zone/sensor status
- SNMP set capability for OUTPUT purposes
- 12-VDC power source for sensors

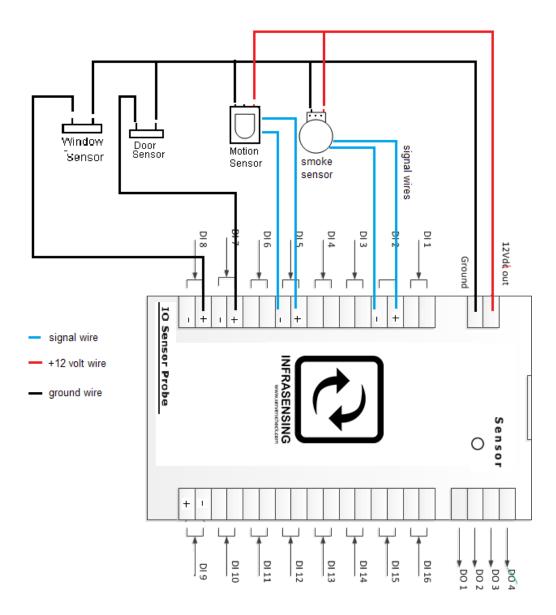
16.6 Terminal description

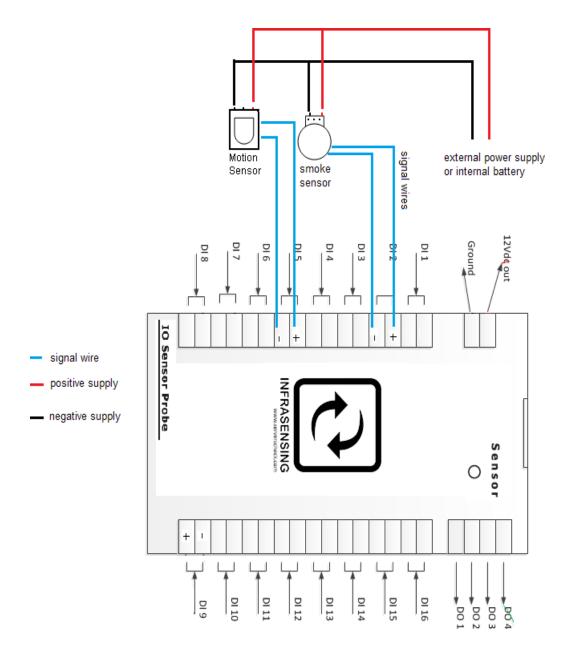
TERMINAL BLOCKS

DI1 to DI16 : 16 digital inputs DO1 to DO4 : 4 digital outputs +12V : 12 VDC supply GND : supply ground

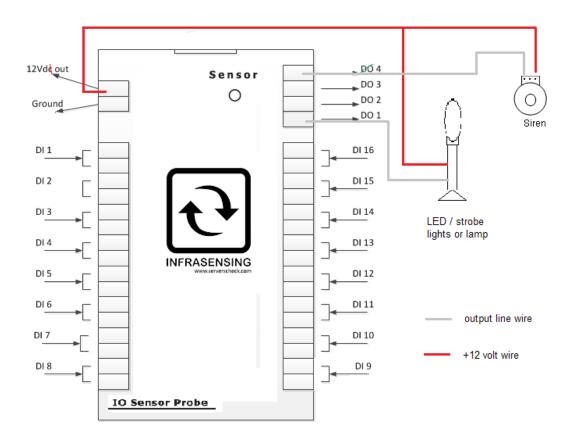
16.7 Basic wiring diagram

Inputs: if sensors are getting their power supply from the IO sensor probe





Inputs: if sensors are getting their power supply from an external source or internal battery



16.8 Base Unit IO sensor probe interface

Status	Туре	Name	Value	Warning Range				Down Range				
	Temperature	Int. Temp1	29.42 °C	< 18		8		<	15			
				>	37	٢	1	>	41			
	Input 1	UndefineIO 1	ок	C	Open	alert if contact state is not		50	for more than			
	Input 2	UndefineIO 2	ок		Open	alert if contact state is not		50	for more than			

Control Outputs

Name	Current Value	Default State	Control Output
Outputt	Ota	OFF	GYOLE
Output2	0##	OFF .	CYCLE
Output	0##	077	CYCLE
Outputi	Ott	OFF	CYCLE

Name

- Is used to assign a name to a zone or sensor (i.e. motion1, smoke1, door1)
- Due to memory limitations, make sure that the maximum number of characters on this field doesn't exceed 31.

Value

- Shows the status of a zone. OK = normal condition, Trig = a zone/sensor has been triggered

Time (milliseconds)

- A time period that can be set which serves as a "wait period" before the IO sensor probe considers a change of state of a zone/sensor as an alert or a trigger

Normal State

- This will set the "logic" of the Input on how to define a trigger /change of state coming from the sensors
- It can be set as "open" for normally open (NO) logic or "closed" for normally closed (NC) logic.

ALWAYS CLICK "UPDATE" AFTER EVERY CHANGE IN VALUES/PARAMETERS for changes to take effect

OUTPUT1 TO OUTPUT4

- The default state can be set to either ON or OFF and is used in conjunction with triggers (ex. siren or strobe /lamp)
- CYCLE button is used to switch the button on and then off or vice versa depending on the default state.

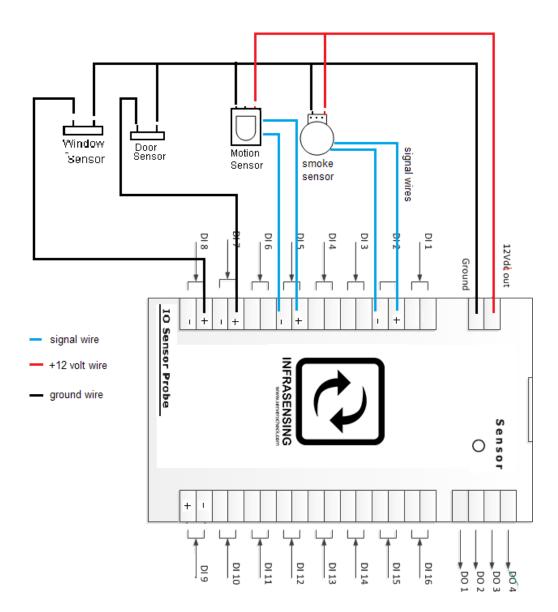
16.9 Wiring configuration and settings (anti tampering)

The IO sensor probe does not have the ability to give out specifically a "tamper" alert. But it can be wired and set to give out a "normal" alert.

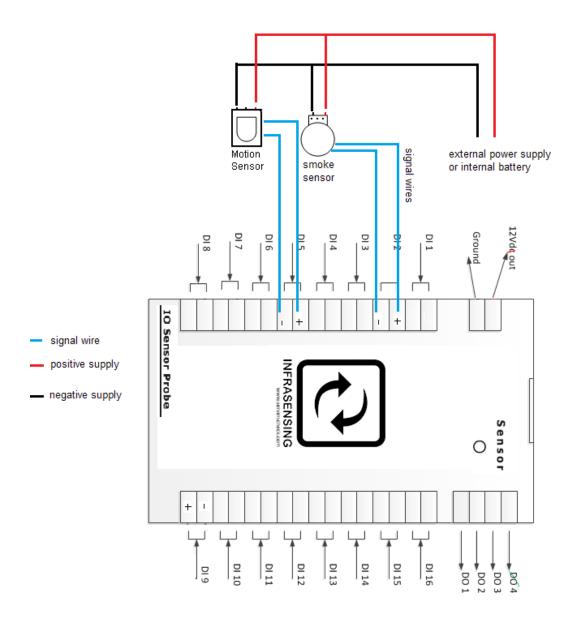
If ever a power supply wire or a signal wire was cut off in which case the monitoring team must still attend to.

Basic wiring diagram for Inputs still applies

Inputs: if sensors are getting their power supply from the IO sensor probe

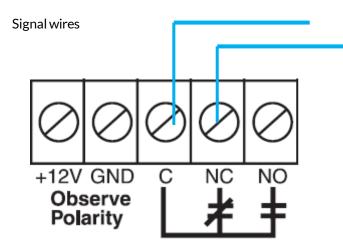


Inputs: if sensors are getting their power supply from an external source or internal battery



A typical sensor (motion, smoke, CO, etc.) has dry contacts as its signal output to a control panel (usually located inside of the sensor, at the back or already exposed via 3 wires and a terminal connector)

Connect the signal wires from the IO sensor probe (can be interchanged) to NC and C terminals of the sensor



DRY CONTACT TERMINALS

NO: normally open (open circuit if not triggered / short circuit when triggered)

- NC: normally closed (short circuit if not triggered / open circuit when triggered)
- **C** : common (common terminal)

Set the all Normal State to "Closed" (setting the trigger logic to normally closed)

IMPORTANT NOTICE WHEN MONITORING VIA SNMP

When monitoring the IO Sensor via SNMP then one should use the SNMP traps feature instead of using the SNMP Get requests. Through SNMP GET one only receives the status of the contact at the time when the request is made. With the SNMP Traps it will trigger an alert as soon as the condition is met

16.10 Output triggering

The output triggering can toggle between automatic / assigned or manual/direct using the corresponding buttons on the sensor page. This requires firmware 6.00 or higher for the new Logic architecture.

Control Outputs

Name	Current Value	Default State	Control Output
Ougutt	0##	011	CYCLE
Output2	0##	017	CYOLE
Output)	0##	•	CYCLE
Output4	0##	OFF .	CYCLE

Automatic/Assigned Output on Sensor Thresholds

The output triggering (digital and relay) can be set using the assigned threshold on a particular sensor. Simply assign an output from the drop down menu and its state you want it to do. Several sensors can share and be assigned to a particular output.

Status	Type	Name	Value		Warning Range		Down Range		Repeat Alarm	Errel	SWS	SMMP Trap	Set Output To				
	Temperature	Int. Temp1	29.79 °C	<	18	\$	<	15	8	0	0	0	0	Output1	٠	ON	•
			2		> 37		> 41										
	Input 1	UndefineIO 1	ок	0	alert if contact state Open	i k nd	5	00	for more than	0	0	0	0	Output2	•	OFF	·
	Input 2	UndefinelO 2	ок		alert if contact state Open	i a nat	5	00	for more than	D	0	D	0	Output3	•	CYCLE	·

so to say after meeting a threshold, it can direct a device to either turn on or off

Edt

17 Security Sensors

17.1 General description

InfraSensing's security solution allows detection of doors, motion, and smoke. Underneath all of these security probes is a simple logic that's adjustable to be close or open. Upon setting a given value, the sensor will instantly be triggered once the opposite is detected which will end up sending you an alert on the event that currently occurred. Being adjustable however, means there's room for changes whenever the situation requires you. This allows for maximum flexibility of what defines an alert.

In this figure, the actual probe that's attached is the door sensor with the logic defaulting to *CLOSE*. Upon opening, we see how it is triggered and thus will eventually send alerts depending on the alerting options chosen.

It is important to note that all security probes have the same web interface so it is advisable to attach one at a time and immediately rename it according to your naming conventions.



17.2 Door Sensor (SEC-DOOR)

The door contact sensor can be mounted inside racks, cabinets, or server room doors. It triggers an alert when the door is opened.



17.3 Motion Sensor (SEC-MOTION)



Industrial grade motion sensor feature digital signal analysis ensures consistent detection across its coverage pattern. With digital temperature compensation, it enhance catch performance at critical temperature levels, providing accurate detection of human IR energy over a wide temperature range.

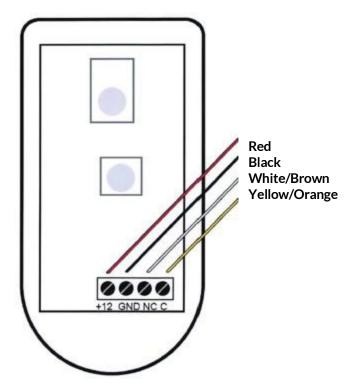
Installation guide for motion sensor



As shown on the image, to remove the cover the lock should be pressed.



Once opened you should see 4 screws where you can connect the wires.



Red Wire: Connect to the Positive terminal (+12) of the Motion Sensor.

Black Wire: Connect to the Negative terminal or GND of the Motion Sensor.

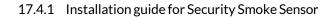
Yellow or Orange Wire: Connect to the Common terminal (C) of the Motion Sensor.

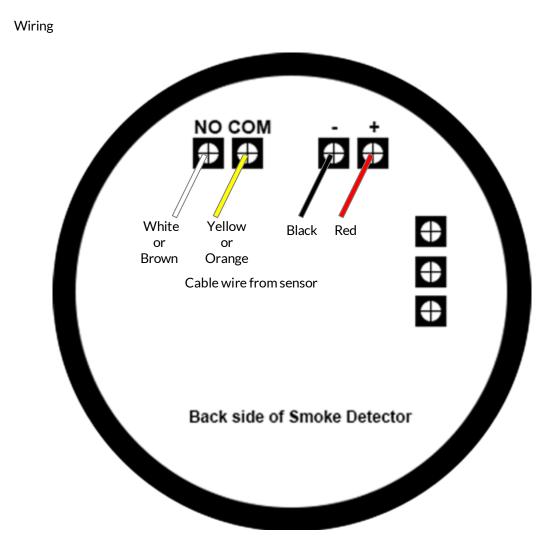
White or Brown Wire: Connect to the Normally Closed (NC) Terminal of the Motion Sensor.

17.4 Smoke Sensor (SEC-SMOKE)



This sensor is a photoelectric smoke sensor that is designed to monitor smoke within facilities, complementing but not replacing mandatory building fire detection systems. It incorporates self-diagnostics and meets NFPA 72 Sensitivity testing requirements without external meters. Equipped with in-built dust compensation, sounder, and a patented CleanMe® feature, it ensures easy maintenance with a replaceable optical chamber. This sensor provides superior protection against false alarms from dust, RF, and ambient light through built-in drift compensation, enhancing its reliability.





There are 4 wires from the Security Sensor

- 1. Red Wire: Connect to the Positive terminal of the Smoke Detector.
- 2. Black Wire: Connect to the Negative terminal of the Smoke Detector.
- 3. Yellow or Orange Wire: Connect to the Common terminal of the Smoke Detector.
- 4. White or Brown Wire: Connect to the Normally Open Terminal of the Smoke Detector.

How to turn off alarm after smoke detection.

Disconnect the RJ45 cable connecting the smoke sensor from the Base Unit or SensorHub

17.5 Sound Sensor (SEC-SOUND)

With the data center demanding a very conducive environment for the services it provides, we know that the people making all those possible needs to be safeguarded as well from any anomaly-producing situations.

This sensor probe measures sound levels in decibels (dB) which allows you to be notified from a number of noise-producing deviations within your data center. Maximum level allowed is up to 100 dB.



17.6 Digital Luminosity Sensor (LUX) (SEC-LUX)



Industrial grade digital luminosity sensor measuring the ambient light in lux (lx).

17.7 Shock / Vibration Sensor (SEC-SHOCK)



This sensor can effectively detect and record tampering, movement, removal, or installation of equipment within racks, as well as monitor vibrations or shocks in rooms, particularly for sensitive equipment like traditional hard disks.

17.8 Tilt Sensor (SEC-TILT)

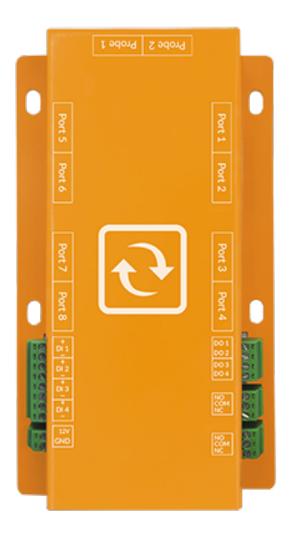


Digital SNMP & Modbus TCP sensor designed for monitoring and measuring tilt and levels in structures. The sensor is versatile, allowing installation, allowing installation in any orientation and presents values in degrees for precise monitoring.

18 The Sensor Hub (EXP-8HUB)

18.1 General description

The sensor hub is a port expander attachment / peripheral for the Base Unit that allows it to accommodate up to 8 sensor probes. It has 4 input dry contacts for sensor alarm detection and indication, 4 output lines that can drive sirens and strobe lights, 2 relay outputs for contact control requirements. It is also capable of giving a 9 to 12-volt power supply and a maximum of 500 mA current capacity, enough to power several sensors and output devices.



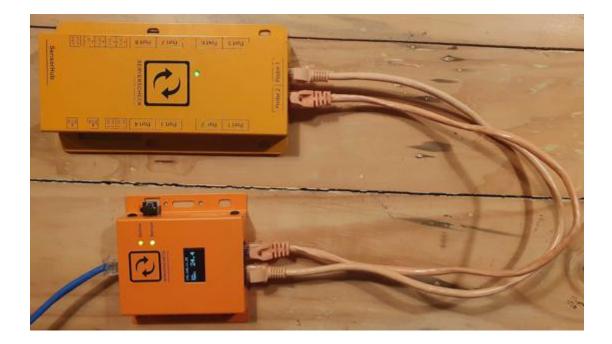


18.2 Probe restrictions

- must not be connected with IO sensor probe
- must not be connected with wireless probe
- must not be connected with QoS probe
- Thermal camera and other sensors indicated should be connected to High-speed ports

Ports 1 to 4: High speed ports Ports 5 to 8: Regular ports

18.3 Connecting the SensorHub to the Base Unit



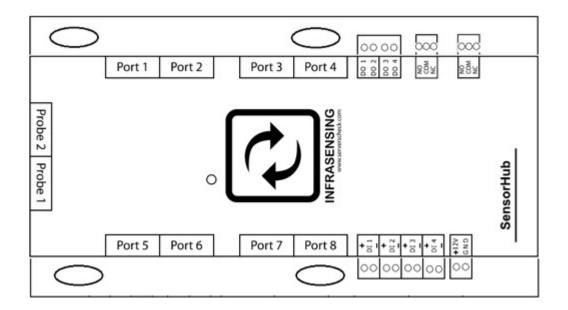
The sensor hub connects through regular RJ45 cables to the Base Unit. The connection from the base unit going to the SensorHub should not exceed 1 meter / 3.3 ft.

Plug the 2 RJ45 cables in the 2 ports of the Base Unit and the other end going to the 2 ports of the SensorHub.

Do note that port label can be disregarded as long as 2 cables are connected, any combination would work, please refer to the image below.

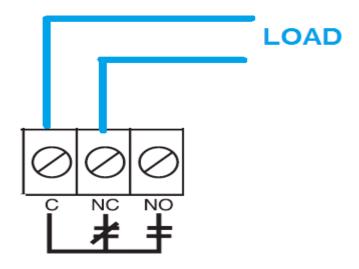


18.4 Terminal connections



PROBE 1 AND PROBE 2: connect to Base Unit using two RJ 45 cables PORT 1 TO PORT 8 : connect sensor probes

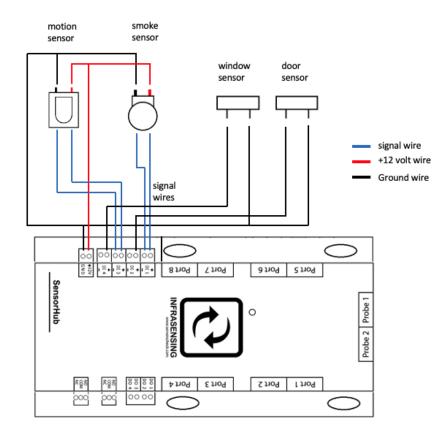
DI 1 to DI 4 DO 1 to DO4 NO, COM and NC :connect to 4 dry contact inputs :connect to 4 digital outputs :relay outputs INPUTS (dry contact): same wiring diagram as the IO sensor probe for inputsOUTPUTS (digital): same wiring diagram as the IO sensor probe for outputsOUTPUTS (relay): connection to a load will depend on the wiring convention



relay terminals

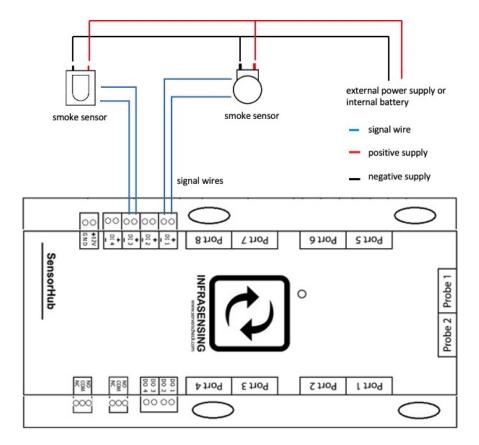
- NO: normally open(always open contact/not connected)
- NC: normally closed(always shorted contact/connected)
- C : common(common terminal)

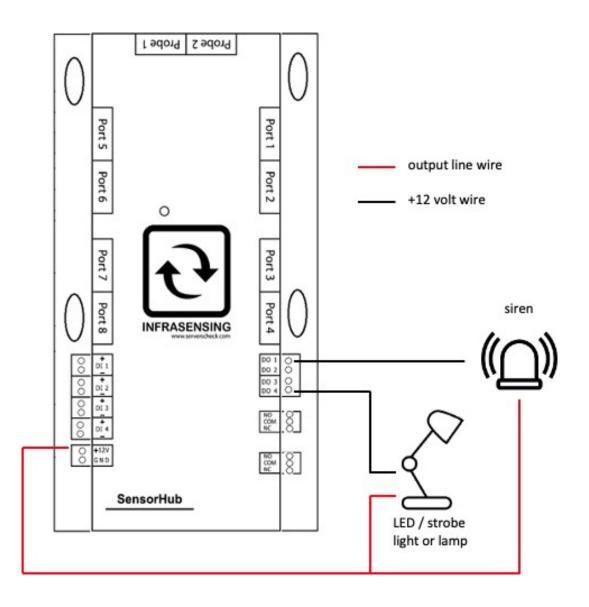
18.6 Basic wiring diagram



INPUTS: If sensors are getting their supply from the EXP-8HUB

INPUTS: If sensors are getting their power supply from an external source or internal battery





18.7 SensorHub web interface

When you access the Base Unit with the SensorHub Connected you can see the images below.

Expansion of probes along with Inputs along with a new option for outputs.

latus	1 ₀ e	Name	Value	Warning Range	Down Range	Replat Aarm	Eral	5945	Stater Trap		et Output To	
	Temperature	Int. Tamp1	31.10	<18 DR H37	<16.08.HI1					DISABLE		-
	Temperature	Ext. Temp1	20.00.10	~18-DR +25	+15-04-+29					DIMANE		-
	Security	Security1	the .	Sera	or Triggered					DISABLE	•	-
	Temperature	Ext. famp1	27.68.6L	<18 DR H25	+10 OR +28					DIMABLE		
	Temperature	Ext. Temp2	27.00.00	+18-DR +28	<10 OK>28					DISABLE		
	Shock.	(Prock)	6.97 G	=0.75-QR =1.25	+0.8 GR+5.8					DISABLE	•	-
	input 1	Undefine®D 1	OK.	Cose	for more than 500ma					DISABLE		-
	19pul 2	Undefine® 2	OK	Close	for more than \$20ms.					DISABLE		
	Figur 3	UndefineIO 3	OK	Cites	for more than 500ms					DISABLE		-
	Input 4	UndefinelO 4	04	Cose	for more than 500ms					DISABLE		-

Outputs

Control Outputs

Name	Current Value	Default State	Control Output
Output	044	0//	GYOLE
Cuput	0**	017	CYCLE
Cuput	0**	017 .	CYCLE
Output	0**	017	CYCLE
Relay1	ON	977	CYCLE
Relay2	011	017	CYOLE

We will discuss triggering outputs in the in section 19.1.

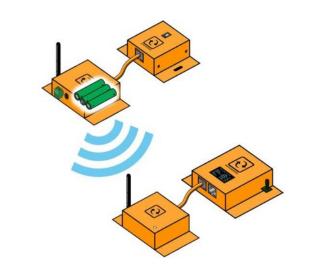
100

19 LoRa Wireless Hub and Node

By default our InfraSensing sensors are connected with an RJ45 cable to the base unit, But with the Wireless hub (EXP-LWHUB) and Node (NODE-LW-1P), any sensor can be connected wirelessly.

It works when we connect our wireless hub to our base unit (BASE-XX) then any of our sensor to one of the nodes, The node then transmits sensor data over a wireless communication protocol to the Wireless Hub.

The wireless protocol used is called LoRa, a long range and low power communication protocol in the free spectrum. What you need:





EXP-LWHUB

NODE-LW-1P

BASE-XX

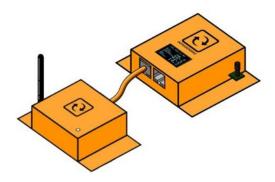
Ethernet Cable

Sensors

19.1 Connecting and Pairing

Connect the Wireless Hub to the Base Unit via ethernet cable.

The Base Unit should be running firmware version 8.9.



Wireless LoRa should appear in the Base Unit GUI.

Sensors										Edit
Statue T	ype Name	Value	Warning Range	Down Range	Repeat Alarm	Email	SMS	SNMP Trap	Set Output To)
Тетр	perature Int. Temp1	30.17 °C	<18 OR >37	<15 OR >41				2	DISABLE ¥	· v

On the Base Unit GUI, click on Wireless LoRa and you will be taken to the Wireless LoRa Configuration page.

Node No.	Status	Sensor Name	RSSI, dB	SNR	TX Power, dBm	
Node No.	Status	Selisor Name	R551, 05	SHK	TX Fower, doin	
Pairing Status:		Not Pairing				
Start Pairing		~				
LoRa Band		AU/AS (915-928 MHz)		~		
LoRa Channel			~			

Setup your Band and Channel prior to connecting nodes. After choosing your desired band and channel, click on "Update". Changing the band and channel will disconnect any previously connected nodes and re-pairing them would be required.

It is a good practice to keep adjacent hubs in different channels to avoid wireless congestion. Also, avoid using same LoRa channel to avoid any interference.

Node No.	Status	Sensor Name	RSSI, dB	SNR	TX Power, dBm	
Pairing Status:		Not Pairing	EU (863-870 MHz)			
Start Pairing			US (902-928 MHz)			
			✓ AU/AS (915-928 MHz)			
LoRa Band		AU/AS (915-928 MHz)		~		
LoRa Channel		1	~			
Update Reset			0			
Opdate			v 1			
Note						
Chainging LoRa Band	and/or Channel will delete Pairin	g and would need to re-pair the sensors.	4			

NOTE:

When adding a new node to an existing group of paired nodes, please note that all previously connected nodes will also be unpaired and have to be repaired again. This is done by design.

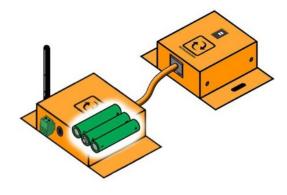
To start the pairing process, on the Wireless LoRa Configuration page, click on "Start Pairing". The LED on the LoRa hub will blink red and green which indicates pairing mode is active.

NOTE : The pairing status will also show "Pairing" when in pairing mode.

Node No.	Status	Se	nsor Name	RSSI, dB	SNR	TX Power, dBm	
Pairing Status: Start Pairing			Not Pairing				
LoRa Band			AU/AS (915-928 MHz)		~		
LoRa Channel			1	~			

To pair a node, you would need to power it up and you will see the LED will blink red and green, it should stop before 5 seconds, that means that the node is paired successfully. If the LED stays ON for more than 10 seconds it would mean that the pairing failed and we would need to start over. To avoid a pairing miss we need to power and pair each node one at a time.

The node can be powered via 12v DC with a terminal block, 12v DC with a barrel jack for an AC/DC adapter, - 5v DC with a USB-C connector or 3x AAA batteries.



NOTE:

-You can pair the node even without a sensor connected.

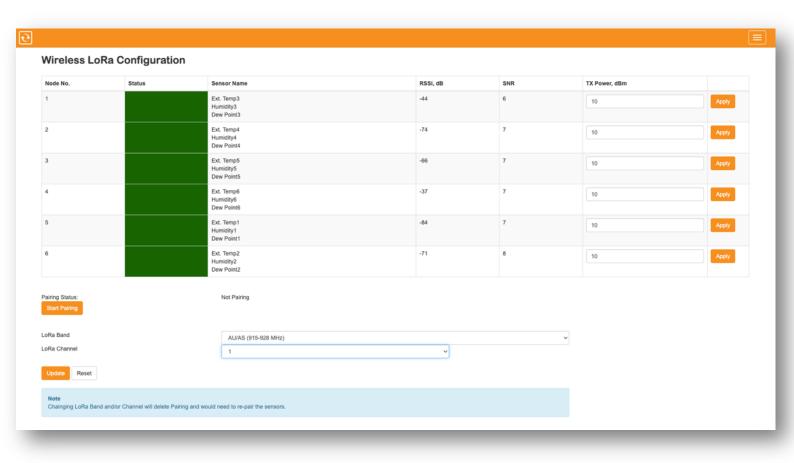
-Up to 16 nodes can be connected

Click on "Stop Pairing" when done. Refresh the page and the list will populate with the connected nodes.

Node No.	Status	Sensor Name	RSSI, dB	SNR	TX Power, dBm	
1			0	0	0	Apply
2			0	0	0	Apply
3			0	0	0	Apply
4			0	0	0	Apply
5			0	0	0	Apply
6			0	0	0	Apply
Pairing Status: Start Pairing		Not Pairing				
LoRa Band		AU/AS (915-928 MHz)			~	
LoRa Channel		1	~			

After pairing, the sensor connected to the wireless node should be ready to go.

To ensure no data is lost when transmitting, The minimum Polling Time for the Base Unit is 5 seconds when connected to a Wireless Hub.



Unpairing Nodes

To unpair connected nodes, click on "Start Pairing" then click "Stop Pairing", this will disconnect all previously connected nodes on the hub. To start the pairing process again, please proceed to "Step 3" of this document.

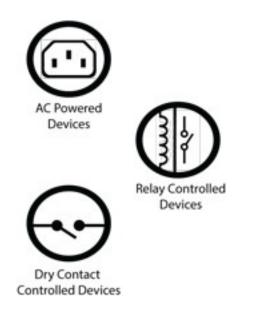
20 Automatic & remote control of equipment

The built-in alerting enables you to be informed when a sensor exceeds defined thresholds or when an incident occurs. Some of these incidents could require an immediate action. For example, when the temperature is too high one may want to start a backup cooling unit; or when water is detected then start a pump.

With InfraSensing's infrastructure monitoring solution you can now also control devices: AC, relay or Dry Contact based. Devices can be controlled either by the Base Unit in an automatic way (condition based). In this section we will cover the automatic (condition based) control.

Requirement:

To use the control features you need a Base Unit with firmware 6 or higher and with an IO sensor or a SensorHub.



Both the IO sensor and the SensorHub feature dry contact outputs. However only the SensorHub feature relay outputs. AC powered devices can be controlled through an **external relay** which connects to a dry contact port on the SensorHub.

Important Notice:

The maximum capacity for the SensorHub's relay is 400VAC/150VDC and 200VA/192W. If an output device is to be used that exceeds those specifications, an external relay, i.e. solid-state relay, will have to be used.

20.1 Triggering outputs through the web interface

The output triggering can toggle between automatic / assigned or manual/direct using the corresponding buttons on the sensor page. This requires firmware 6.00 or higher for the new Logic architecture.

Control Outputs			60
Name	Current Value	Default State	Control Output
0ugurt	011	0#	CYCLE
Output	OFF	0//	CYCLE
Outpuß	OFF	0#	CYCLE
Culpun	CA14	0//	CYCLE
Ratay1	CMA	017	CYCLE
Raing2	OFF	017	GYOLE

Automatic/Assigned Output on Sensor Thresholds

The output triggering (digital and relay) can be set using the assigned threshold on a particular sensor. Simply assign an output from the drop-down menu and its state you want it to do. Several sensors can share and be assigned to a particular output.

Sata	Type	Name	Value	Warning Range			Down Range		Repeat Alarm	Enal	345	SWP Inp		Ser Out	put To	
	Tenpesture	ist, Tempt	29.79.70	18	ŝ.	<	15	\$	0	0	0	0	Output	•	ON	•
				37	÷.	>	41	\$								
	ingut 1	UndefineIO 1	ок	alen i formad state is not Open	•		for more than	ms	0	0	0	0	Output2	•	OFF	3
	Input 2	Undefinal0.2	OK	alest if control rates is not			for more than		0	0	0	Ö	Outputs	8	CIQLE	2
				Open	•	. 5	00	ms								

so to say after meeting a threshold, it can direct a device to either turn on or off

Let's for example configure a scenario where we want to trigger a backup air conditioning unit when the thresholds are exceeded.

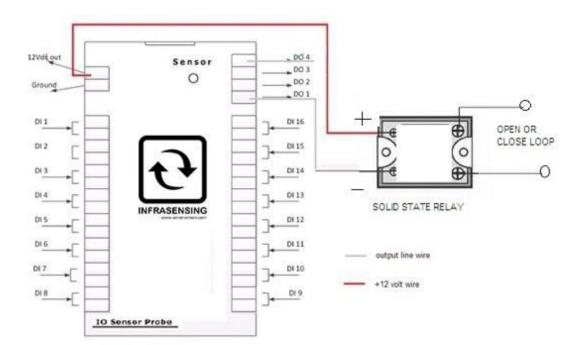
Go to your temperature sensor and select the correct output and the state it should be in, as shown below

Satus	1ge	Xare	Value	Vaning Range	Covn Range	Repeat Aam	Stal	98	SMP Top	Set Cutput To	
	Terperature	it. Terpi	25%	<0.00	<0Rx0					No 🖯 Itado	·

- Based on the image, the temp threshold danger levels is when it reaches 40 or above and 10 or less thus will trigger the device connected to the "Output1" to turn ON Thus if an Air-condition unit is connected to "Output1" if the temperature rises above 40 it will
- turn ON automatically

20.2 Wiring for a control output

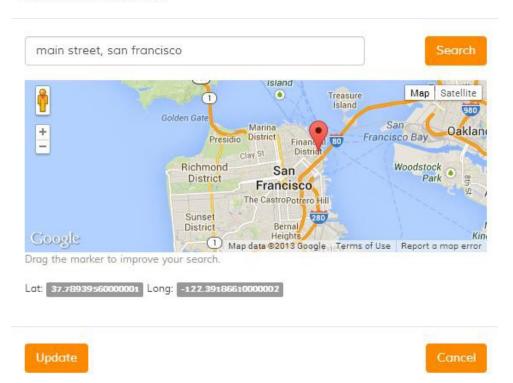
Now that we have those configured, for the output wiring, kindly refer to **section 20.1**. If an external relay will be used, refer to the following diagram:



20.3 Geomapping sensors

For a more organized view of your over-all monitoring infrastructure, you could setup the location of each of your Base Units.

From the "Devices" tab, click "Location" to set it up.



Edit Device Location

After updating it, you could now navigate to the "Map" tab and view the configured devices.



21 Power rating

A Base Unit can be provided with up to 12 watts of power from a PoE source. Because of this, careful power budgeting should be done especially when probes like the IO, QoS, and fuel sensors are to be utilized. Below shows the power ratings of InfraSensing sensor modules:

MODULE	POWER RATING
BASE-5 Base Unit	552 mW
BASE-6 Base Unit	876 mW
BASE-SM-5-24V Base Unit	684 mW
BASE-SM-6 Base Unit	900-1752 mW
BASE-PI-5-24 Base Unit	684 mW
BASE-PI-6 Base Unit	684 mW
ADDON-LTE LTE/3G/2G Cellular Add-On	2800 mW
ADDON-WIFI Wifi Add-On	720 mW
ADDON-POE 24v/-48v DC Power Add-On (PoE injector)	48v DC via POE; max 22W
EXP-8HUB SensorHub for Base Unit	235 mW
EXP-LWHUB Wireless Hub	720 mW
NODE-LW-1P Wireless Node	720 mW
THIMG-XS Thermal Imaging Sensor (extra small)	492 mW
THIMG-SM Thermal Imaging Sensor (small)	492 mW
THIMG-ME Thermal Imaging Sensor (medium)	492 mW
THIMG-LG-2 Thermal Imaging Sensor (Large)	492 mW
C-THIMG-SM Thermal Imaging Sensor (CS)	492 mW
THIMG-IRSPOT Infrared Spot Temperature Sensor	60 mW
C-THIMG-SM-IRSPOT Infrared Spot Temperature Sensor (CS)	60 mW
ENV-THUM Temperature and Humidity Sensor	60 mW
ENV-TEMP Temperature Sensor	60 mW
C-ENV-THUM Temperature and Humidity Sensor (CS)	120 mW
ENV-TSURFACE Industrial Surface Temperature Sensor	60 mW
ENV-TSTAIN Steel Temperature Sensor	60 mW
ENV-TULTRA Ultra Low Temperature Sensor	60 mW
ENV-TEMP-MAGNET Temperature Magnet Sensor	120 mW
ENV-LHD Linear Heat Trace Sensor	468 mW
DAISY-STARTER Daisy Chain Sensor Start Unit	288 mW
DAISY-BOOSTER Daisy Chain Booster	300 mW
DAISY-THUM Daisy Chain Temp & Humidity Unit	120 mW
DAISY-TEMP Daisy Chain Temperature Sensor Unit	120 mW
DAISY-IRSPOT Daisy Chain IR Spot Temperature Sensor	60 mW
DAISY-TEMP-MAGNET Daisy Chain Temperature Magnet Sensor	120 mW
C-DAISY-THUM Daisy Chain Temp & Humidity Unit (CS)	120 mW
ENV-NOISE Digital sound & noise level (dbA) sensor	312 mW
ENV-AIRFLW Digital Airflow Sensor	84 mW
ENV-AIRPRESSURE Differential Air Pressure Sensor	96 mW
ENV-PARTICLE Particle Sensor	156 mW
ENV-CORROSION Atmospheric Corrosion (ACM) Sensor	260 mW
ENV-DUST Optical Dust Particle Sensor	156 mW
ENV-LEAK OPTICAL Optical Oil & Hydrocarbon Leak Sensor	2.1 W
ENV-WLEAK-COMBO Water Detection & Flooding Sensor	264 mW
ENV-WSPOT Water Spot Sensor	288 mW

MODULE	POWER RATING
GAS-VOC	120 mW
GAS-A1 Refrigerant A1 Gas Sensor	600 mW
GAS-A2L Refrigerant A2L Gas Sensor	600 mW
GAS-A3 Refrigerant A3 Gas Sensor	600 mW
EGD-O3 Ozone Gas Sensor	216 mW
EGD-SF6 Sulfur Hexafluoride Gas Sensor	1240mW
R-EGD-PANEL	0.4-4.4W
R-GAS-FLAMMABLE	672mW
PWR-AC-FAIL AC Power Failure Sensor	216 mW
PWR-DC-VOLT DC Voltage Sensor	530 mW
PWR-AC-QUAL AC Power Quality Sensor	460 mW
PWR-AC-CUR AC Current (Power Usage) Sensor	384 mW
PWR-FUEL Ultrasonic Fuel Level Sensor	1008 mW
PWR-GROUND Grounding Sensor	456mW
PWR-BAT-STRING Battery Monitoring - Control Module	500 mW
PWR-BAT-CELL Battery Monitoring - Battery Module	500 mW
SEC-DOOR Door Contact Sensor	240mW
SEC-SHOCK Digital Shock / Vibration Sensor	156mW
SEC-LUX Light Sensor	83mW
SEC-SMOKE Smoke Sensor	240mW
SEC-TILT Tilt Sensor	240mW
SEC-MOTION Motion Sensor	252mW
SEC-SOUND Noise triggered security sensor	144mW
IND-IO IO-Dry Contact Sensor	516mW
IND-0-10V Industrial 0-10V	660 mW
IND-4-20mA Industrial 4-20mA	660 mW

With the given power ratings, for best practices, the fuel sensor, power meter sensor probes, QoS probe and the wireless hub should be connected to a dedicated Base Unit as they are more resource intensive in power and memory than the other ones. Know, however, that in the mentioned list, it would be completely fine to use 2 of them in combination on a single Base Unit (i.e. Base Unit with IO and QoS probes).

22 Product Registration

The main purpose of **Product Registration** is to help you keep track of your device, including its warranty status, purchase date, help you file an RMA request and for firmware updates. While registration is not mandatory, we highly encourage users to register their devices to stay informed and ensure timely updates.

22.1 How to Register your Hardware:

1. Log in to your my.infrasensing.com account. User your credentials to access your account

	 my.infrasensing.com		5	Û +
<u> </u>				
	Email address	° ~		
	Password			
	🕑 Sign in			
	Forgot Password? Create an Account			

2. Once logged in, go to Registered Products section.

ਦ			
News	Registered Products	Support	Repair
latest news from InfraSensing	no products registered	Technical support options	Warranty & out-of-warranty repairs
Alert+	Purchase History	Account	
108.0 remaining credits for alerting	3 orders found	angelie.tuazon@infrasensing.team	

Here, you can view all the products you have registered. In the sample image below, no products have been registered yet.

3. To register a new device, click on Add Your Purchase.

Ì										
A / Products /	Regi	stered Hardware								ወ
Show 10 🗘 entr	ies							Search:		
Product	↓ ≣	Serial Number	1\$	Purchase Date	LØ	Warranty Until	1\$	Firmware Updates Until		1\$
				No da	ata available ir	n table				
Showing 0 to 0 of 0 en	ries								Previous	Next
Missing produ ts? Add	l you	r purchases								

4. You will be prompted to select your purchase method. Choose how you purchased the product.

. ર		
1 Products / Hardware / Register Hard	ware	ტ
How did you purchase	the products?	
	Direct from InfraSensing	
		1
	From a reseller	

- 4.1. Direct Purchase from InfraSensing
 - Click "Direct From InfraSensing"
 - Make sure you have your InfraSensing order number ready.
 - Only orders that have been shipped will be listed here. However if you have an order number click on the **"here"** button to enter the order number.

· €	
↑ / Products / Register Hardware & Software	ڻ ٺ
Direct orders from ServersCheck Only orders that have been shipped will be listed here. Software only order? Add it here.	
Submit	
Do you have another order number? Click here to enter the order number and link the products to your account.	

Once you click the "here" button, you will be redirected to a page where you can enter your InfraSensing order number in the designated field, then click Submit to complete the step.

Order from InfraSensing InfraSensing order number The InfraSensing order number is an alphanumeric number that you should find on your invoice or shipping paperwork Submit	♠ / Products / Products / Register Hardware	
The InfraSensing order number is an alphanumeric number that you should find on your invoice or shipping paperwork	Order from InfraSensing	
Submit	The intraSensing order number is an alphanumeric number that you should lind on your inv	voice or snipping paperwork
	Submit	

4.2. Direct Purchase From a Reseller

- Click "From a reseller"
- You'll be asked whether you have an InfraSensing Order number.

ି ପ	
1 / Products / Products / Register Hardware	ტ
Do you have an InfraSensing order number?	
I have an InfraSensing order number from my reseller	
I don't have an InfraSensing order number	
An InfraSensing order number enables us to automatically link an order in our systems to your account. When you don't have such an order number then we will ask you to upload your invoice from the reseller. Upon verification we will add the products to your	account.

• If **YES**, select "*I* have an InfraSensing order number from my reseller", and input it on the next screen.

• If **NO**, select the option to continue without an order number. You'll be redirected to a form where you can enter the necessary details and submit your registration.

Please note that in order to add your purchase to your account you will need to send a copy of your invoice from the reseller and allow 1-2 business days to review the information you sent and to process it.

der from a reseller				
order to add your purchase to your account kindly ow 1-2 business days to review the information yo der date		he reseller.		
elect day	Select month	\$	Select year	\$
py of your invoice				
Choose File no file selected				
IG, JPG or PDF format accepted (max 4MB)				
Submit				
ou have an InfraSensing order number? Click here	to continue.			

5. Once your device is registered, it will appear in your dashboard with the following information.

Show 10 🗘 entrie	8			Search:
Product	Serial Number	Purchase Date	Warranty Until	Firmware Updates Until
EXP-8HUB		2022-11-25	2023-11-25 🔎	2023-11-25 🛓
ENV-TSURFACE		2021-07-16	2022-07-16 🔎	2022-07-16
ENV-THUM		2022-11-25	2023-11-25 🔎	2023-11-25 🛃
ENV-TEMP		2022-11-25	2023-11-25 🔎	2023-11-25 🛓
BASE-5		2017-10-24	2018-10-24 🔎	2018-10-24
BASE-5		2017-07-27	2018-07-27 🔎	2018-07-27
BASE-5		2017-07-27	2018-07-27	2018-07-27
BASE-5		2020-02-10	2021-10-06	2021-02-09
BASE-5		2022-09-07	2023-09-07 🔎	2023-09-07
BASE-5		2020-10-06	2021-10-06	2021-10-06

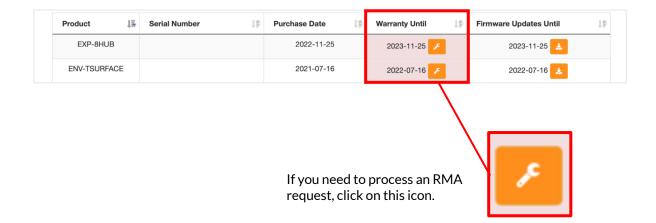
22.2 Managing your Registered Device

On this page, you can easily view your device's **purchase date**, check its **warranty status**, **submit an RMA request**, and access the latest **firmware updates** available for your device

now 10 💠 entries				Search:
Product	Serial Number	Purchase Date	Warranty Until	Firmware Updates Until
EXP-8HUB		2022-11-25	2023-11-25 🔎	2023-11-25 🛃
ENV-TSURFACE		2021-07-16	2022-07-16	2022-07-16 🛓
ENV-THUM		2022-11-25	2023-11-25 🔎	2023-11-25 🛃
ENV-TEMP		2022-11-25	2023-11-25 🔎	2023-11-25
BASE-5		2017-10-24	2018-10-24 🔎	2018-10-24
BASE-5		2017-07-27	2018-07-27 🔎	2018-07-27 🛃
BASE-5		2017-07-27	2018-07-27 🔎	2018-07-27 🛃
BASE-5		2020-02-10	2021-10-06 🔎	2021-02-09 👱
BASE-5		2022-09-07	2023-09-07 🔎	2023-09-07 👱
BASE-5		2020-10-06	2021-10-06	2021-10-06
howing 1 to 10 of 12 ent	tries			Previous 1 2 Ne

22.2.1 RMA Request

If you encounter any issues with your sensor and require an RMA, you can easily initiate the process on this page. Simply click on the Warranty section for the device you wish to process an RMA for, and you will be directed to the RMA Wizard. Here, you can request and RMA, select the device needing repair, and describe the issue.



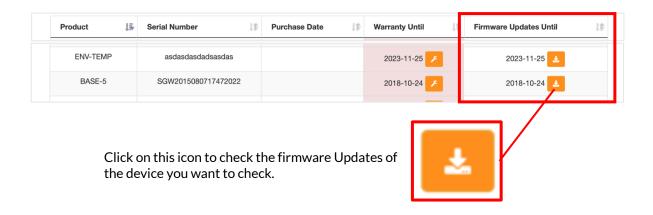
• If you encounter any issues with your sensor and require an RMA, you can easily initiate the process on this page. Simply click on the **Warranty** section for the device you wish to process an RMA for, and you will be directed to the RMA **Wizard**. Here, you can request and RMA, select the device needing repair, and describe the issue.

↑ RMA / Request RMA / RMA Product Selection	ტ
This RMA wizard enables you to request a ServersCheck Retunumber of the product(s). Product missing? Click here to add missing products to your	urn Merchandise Authorization (RMA) to return the defective product for repair. You will need the serial hardware list.
Product Selection & Issue De	escription
Product 1	Problem Description
Product Type Select a product type Serial Number	 ↓ ↓
Select a product type	Ť

22.2.2 Firmware Updates

You can also view and download the latest release notes for firmware update.

• To check for the latest firmware available for your device, click on the **Firmware Updates Until** section for your device.



• Based on the image below, for example if you check the Firmware updates under BASE-5, you will see details such as the **Firmware Version**, **Release Date**, **Eligible Serial Numbers**, and a **Download Link** for the firmware.

🛉 / Produc	ts / Firmware Downloa	d for BASE-5		
A The firmwa	re may only be download	ded onto the registered units r	natching the serial numbers. For units not listed a firmware update must be pu	irchased.
	Delesse Notes			
	Release Notes			
now 25 🗧	entries		Search:	
Product 🕼	Firmware Version	Firmware Release Date	Eligible Serial Numbers	Downloa Link
BASE-5	9.2	2024-03-15		Unavaila
BASE-5	9.1	2023-11-15		Downloa
BASE-5	9.0	2023-03-17		Downloa
BASE-5	8.10	2022-10-21		Downloa
BASE-5	8.9	2022-07-26		Downloa
BASE-5	8.8	2022-05-18		Downloa
BASE-5	8.7	2022-01-12		Downloa
BASE-5	8.6	2021-01-06		Downloa
BASE-5	8.5	2020-08-26		Downloa
BASE-5	8.4	2020-04-06		Downloa
BASE-5	8.3	2020-02-24		Downloa
BASE-5	8.2	2020-02-10		Downloa
BASE-5	8.1	2019-07-01		Downloa
BASE-5	8.0	2019-02-12		Downloa
BASE-5	7.5	2018-07-05		Downloa
BASE-5	7.4	2017-11-23		Downloa

23 RMA / Repair

Defective InfraSensing hardware can be returned to one of our repair centers through our Return Merchandise Authorization (RMA) program.

RMA requests have to be submitted through your <u>order page</u> or from your <u>my.infrasensing.com</u> account.

If purchased from a reseller, add your products to your <u>my.infrasensing.com</u> account.

Warranty covered repairs:

All InfraSensing products are covered by a limited 1 year world-wide warranty as detailed <u>here</u>. If the defect to your product(s) is covered by the warranty, then the product(s) will be diagnosed, repaired or replaced and finally tested before returning the product(s) to you. If the defect is found to be not warranty covered, then an inspection fee of \$75 per product will be invoiced. After payment reception of the inspection fee you have 3 options: receive the defective product(s) back, have it repaired (if repairable) or purchase of a new product(s). In the event of a repair or purchase of new product(s), the cost will be discounted with the paid inspection fee.

Out of warranty repairs:

Do you have a defective device outside of its warranty period or is the defect not covered by warranty? It might still be possible to repair it. In such an event, you can also apply for an out of warranty repair. This incurs an inspection fee of \$75. After receiving payment for the inspection fee, the RMA will be issued to you. If the device can be repaired, then you will receive a quote for repair with a discount for the paid inspection fee. You may also opt for the purchase of a new unit with a discount for the paid inspection fee.

Depending on the complexity of the defects and availability of parts, you should expect a turn- around time of 2 to 5 weeks. We appreciate your patience while we try to repair the defective units.