SENSORS PLATFORM USER MANUAL

INFRASENSING

Copyright:

Software:

Trademarks:

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

Revision # 99- 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 http://manuals.infrasensing.com/UL_Compliancy_Guide_v1.pdf

Warranty:
For the warranty on this product please visit
https://infrasensing.com/
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 https://infrasensing.com/sensors

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

Note:

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

In June 2018 we did rebranded 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

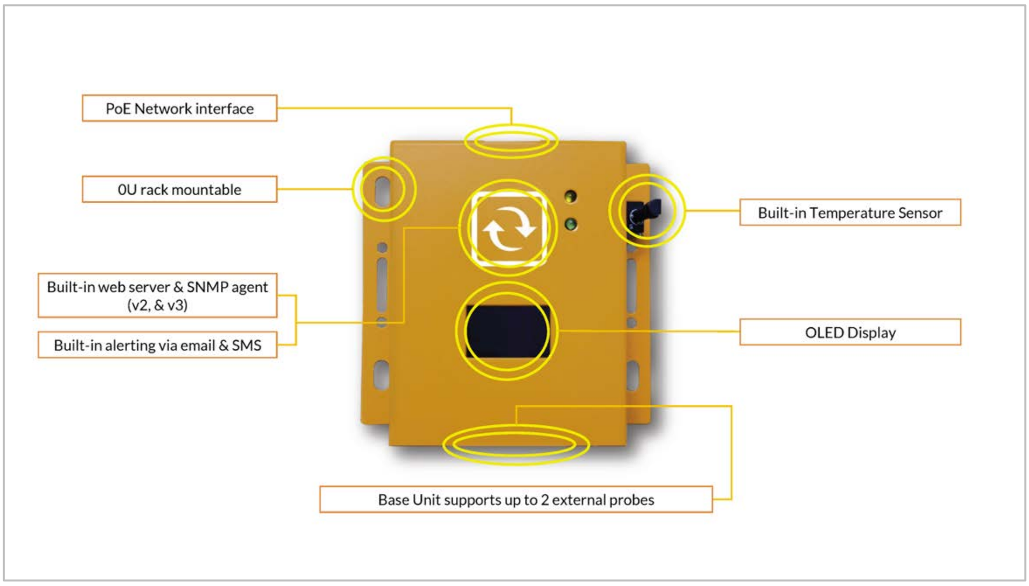
1 InfraSensing Sensors Overview

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 quick 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.


PoE Network interface
0U rack mountable
Built-in Temperature Sensor
Built-in web server & SNMP agent (v2, & v3)
Built-in alerting via email & SMS
OLED Display
Base Unit supports up to 2 external probes

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.

Note: If a power adapter (BASE-PWR) and POE is plugged into the gateway to supply power at the same time the gateway will automatically switch to the power adapter and use POE as backup, Also the gateway 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.

It is recommended to verify the calibration of the temperature probe in your environment and if an offset is noticed, to recalibrate the sensor as explained in **section 6** of this document.

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.

1.3 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

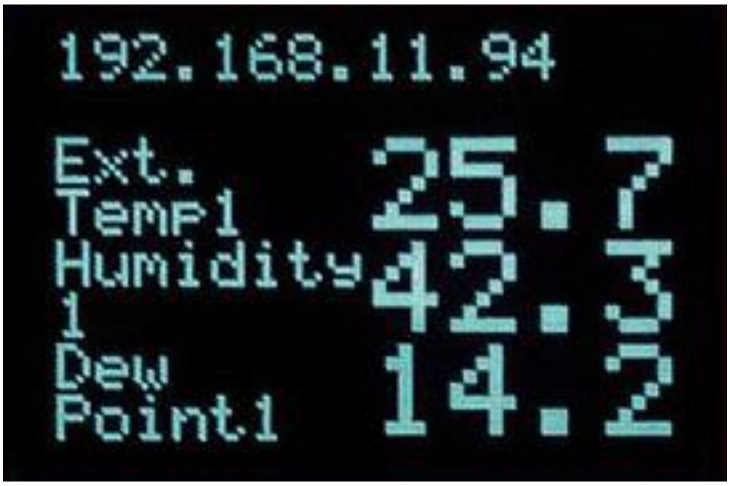
Reboot, New Firmware Uploaded

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

1.4 OLED display subscripts



192.168.11.94

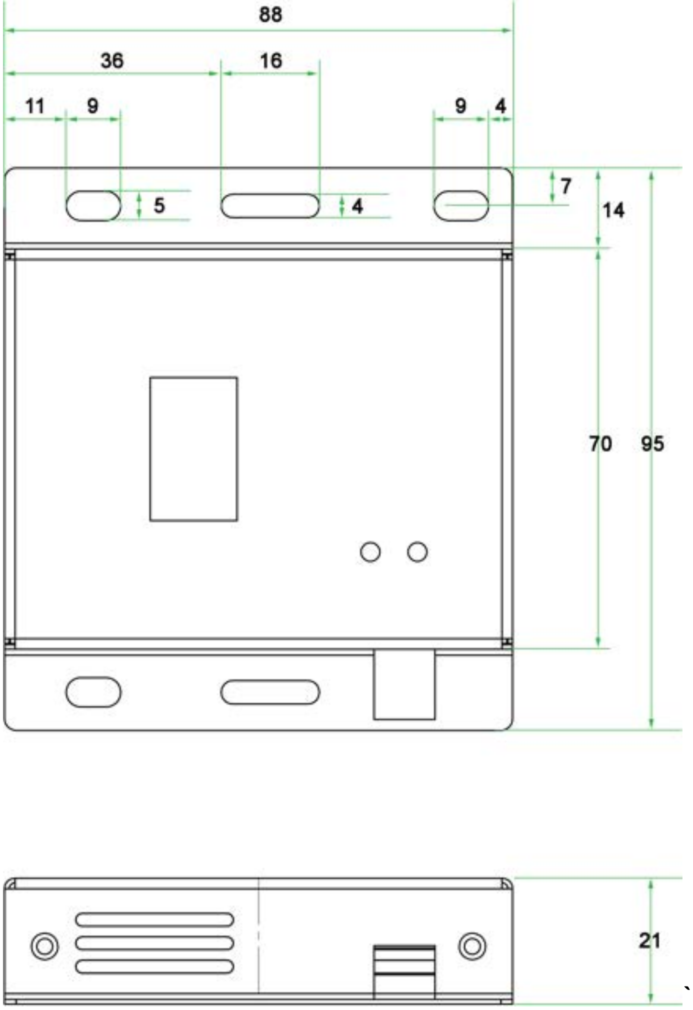
Ext. Temp1 25.7

Humidity1 42.3

Dew Point1 14.2

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.

1.5 Dimensions of the sensor gateway

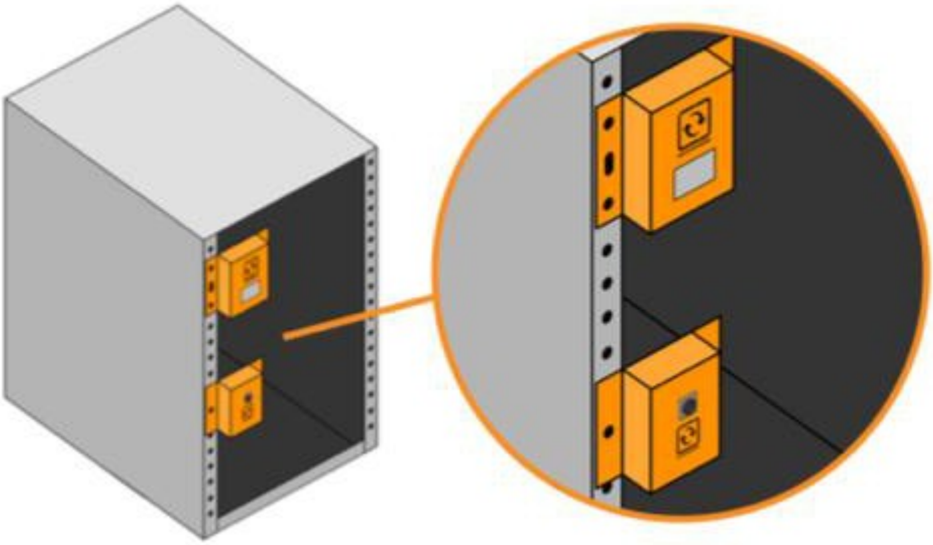


Measurement unit in millimeter (mm)

1.6 **Rack mounting**

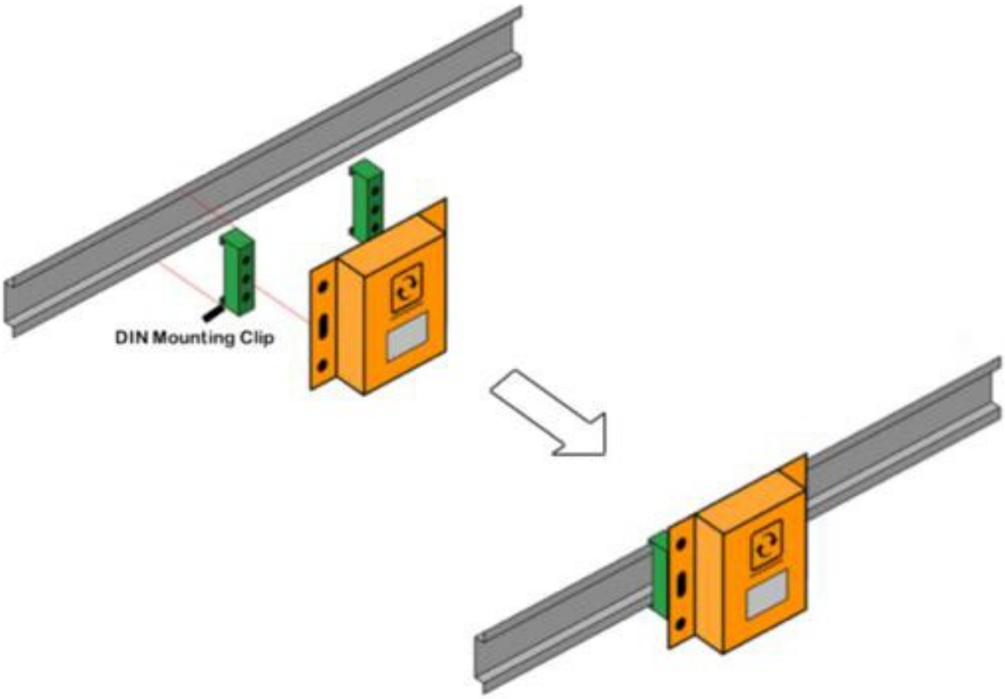
The Base Unit and most of our sensors are 0U devices that can be easily and securely mounted in a rack using standard rack mount screws with a head of at least 0.65cm / 0.26 inch. Although one screw is sufficient to hold the whole equipment in place, a second one improves stability.

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.



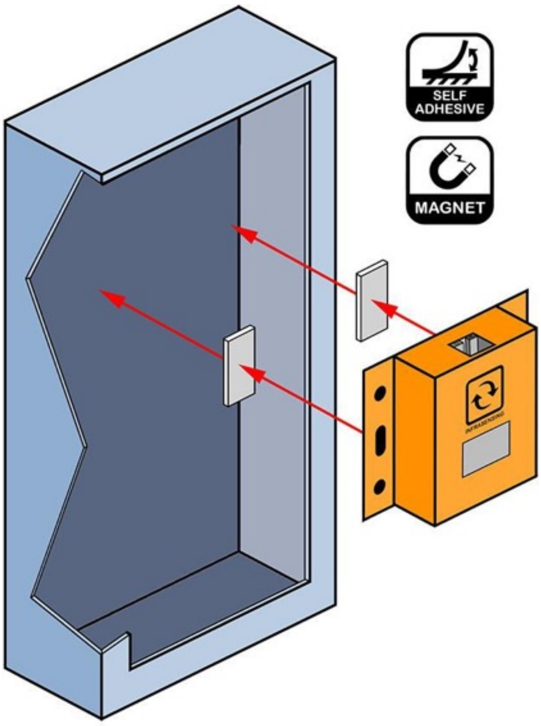
1.7 **DIN rail mounting**

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 0.6cm / 0.24 inch. The clips are then mounted on DIN rails as shown on the image below.



1.8 Magnetic mounting

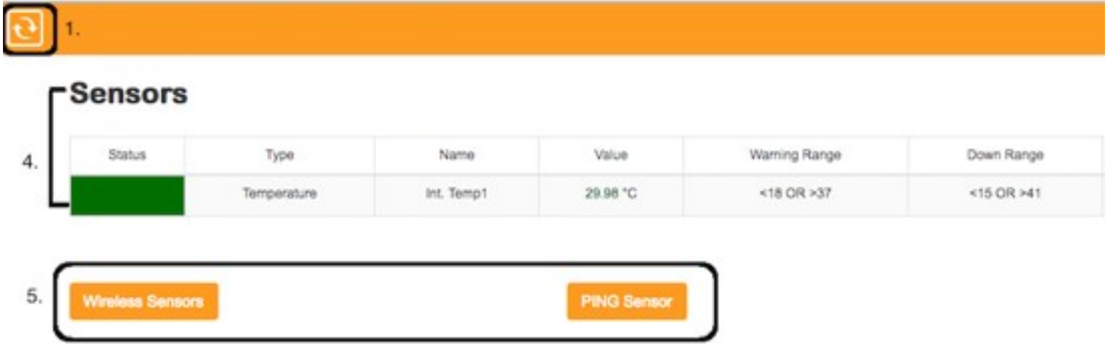
As our base unit, add-ons, expansion hubs, and most sensors feature a metal steel enclosure, the devices can also be mounted using simple magnets.



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.

Image of the left side of the main page.



Sensors

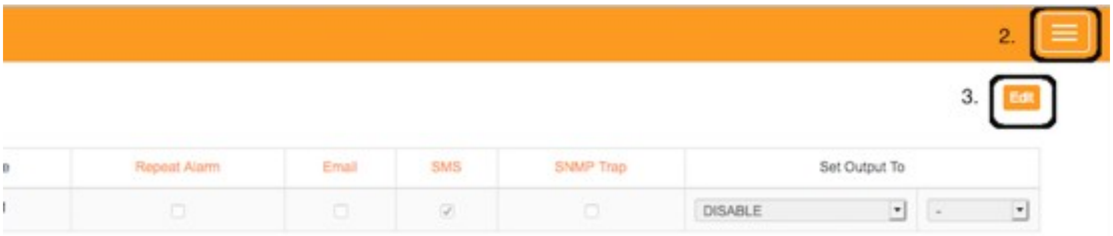
Status	Type	Name	Value	Warning Range	Down Range
🟩	Temperature	Int. Temp1	29.98 °C	<18 OR >37	<15 OR >41

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

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

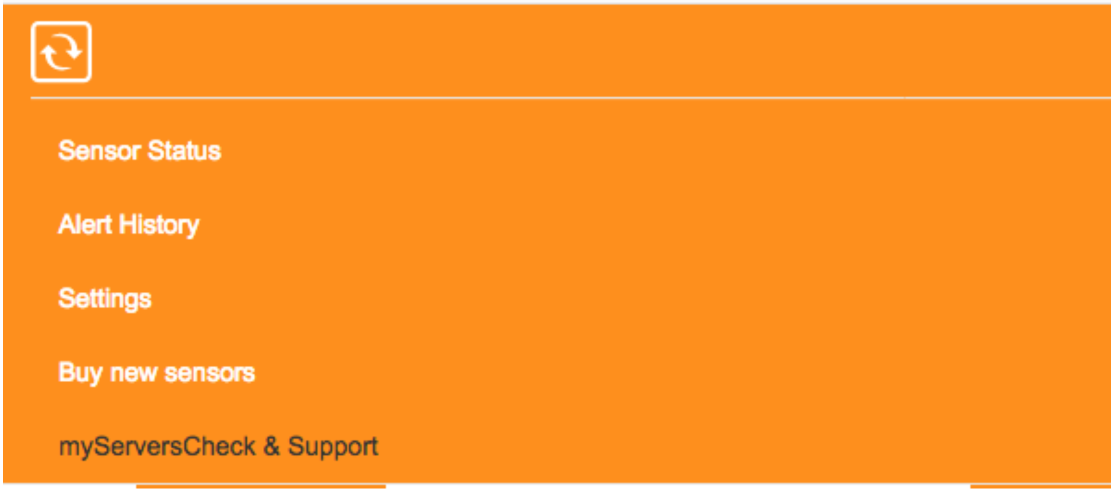
(5) Additional options will appear on this area depending on the sensor connected (Wireless Hub, Thermal Image, etc.)

Image of the right side of the main page.



Repeat Alarm	Email	SMS	SNMP Trap	Set Output To	
□	□	☑	□	DISABLE	-

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



(3) 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.

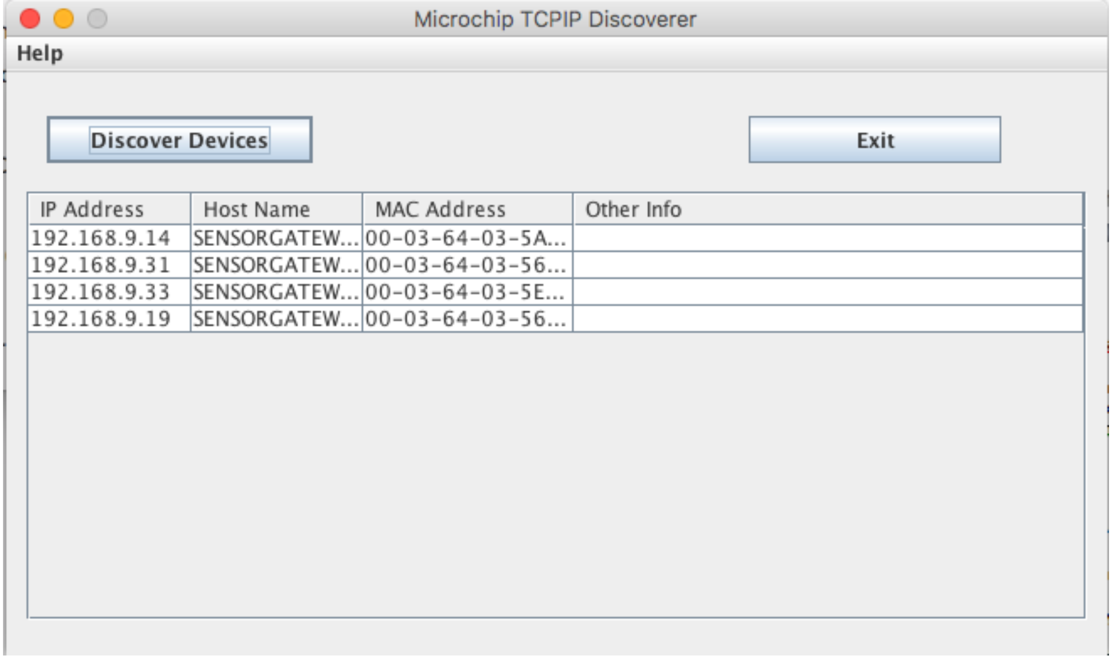
We highly recommend not using DCHP but instead to use fixed IP addresses.

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 https://infrasensing.com/support/downloads.asp

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

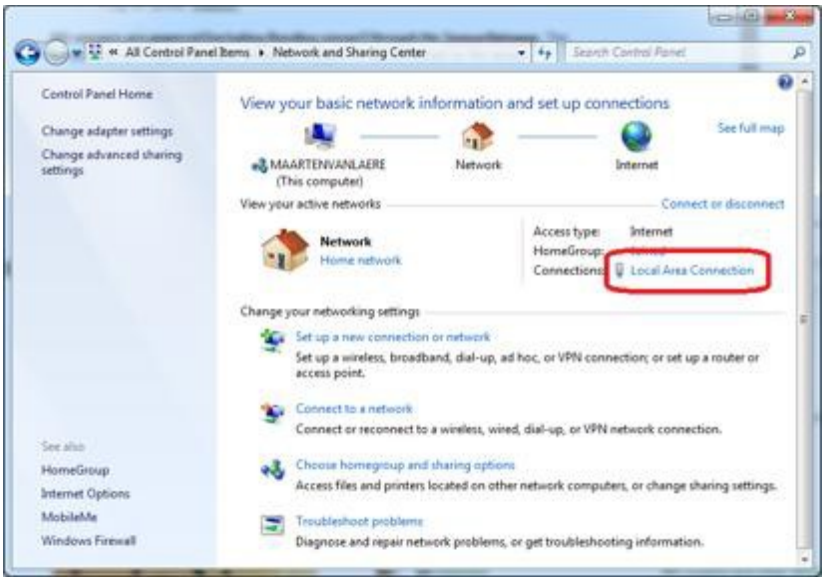


IP Address	Host Name	MAC Address	Other Info
192.168.9.14	SENSORGATEW...	00-03-64-03-5A...	
192.168.9.31	SENSORGATEW...	00-03-64-03-56...	
192.168.9.33	SENSORGATEW...	00-03-64-03-5E...	
192.168.9.19	SENSORGATEW...	00-03-64-03-56...	

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



View your basic network information and set up connections

View your active networks

Access type: Internet
HomeGroup:
Connections: Local Area Connection

Change your networking settings

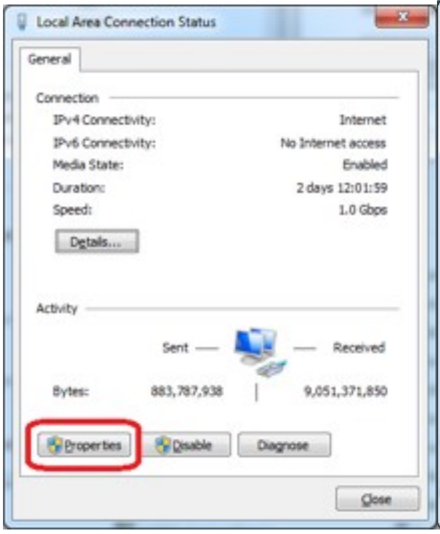
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

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 Status

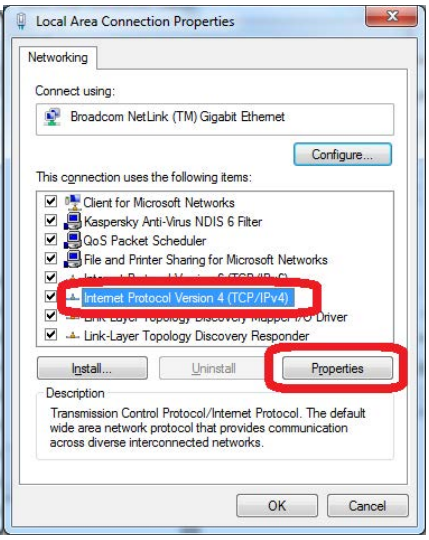
General

Connection

IPv4 Connectivity:	Internet
IPv6 Connectivity:	No Internet access
Media State:	Enabled
Duration:	2 days 12:01:59
Speed:	1.0 Gbps

Activity

	Sent	Received
Bytes:	883,787,938	9,051,371,850



Local Area Connection Properties

Networking

Connect using:

Broadcom NetLink (TM) Gigabit Ethernet

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 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

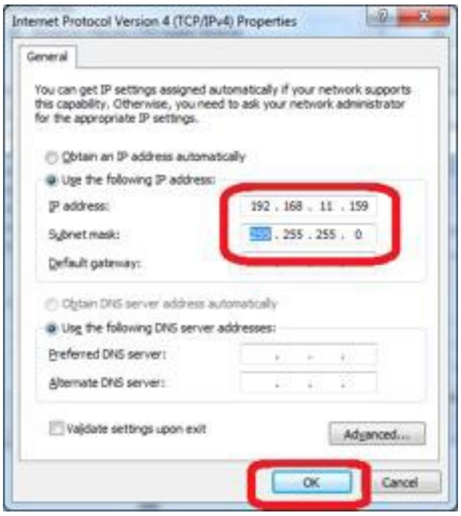
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 11 . 159
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

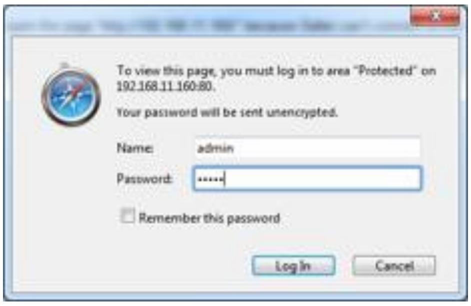
Preferred DNS server:	. . .
Alternate DNS server:	. . .

□ Validate settings upon exit

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 http://192.168.11.160
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**



To view this page, you must log in to area "Protected" on 192.168.11.160:80.

Your password will be sent unencrypted.

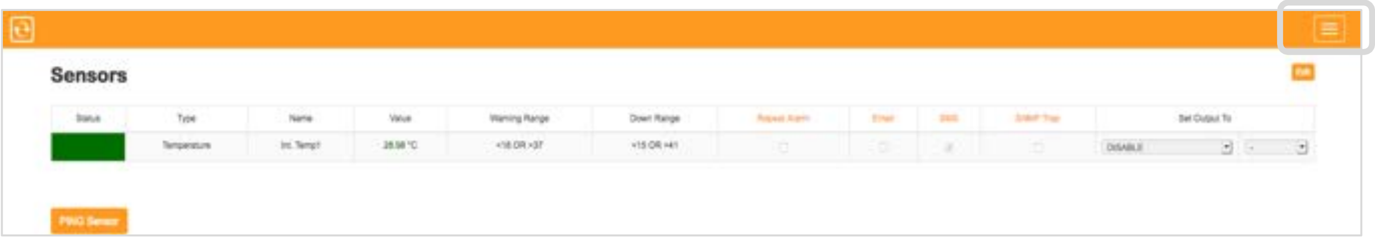
Name: admin

Password: •••••

□ Remember this password

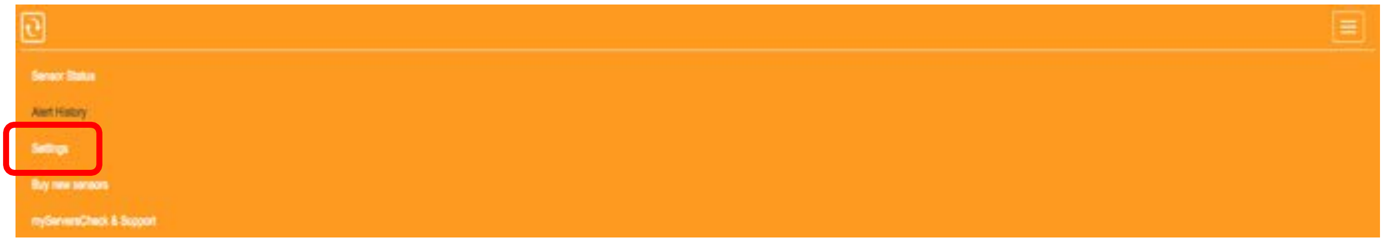
When logged in you will be shown the main screen of the Base Unit with the first sensor reading being the built-in temperature probe.

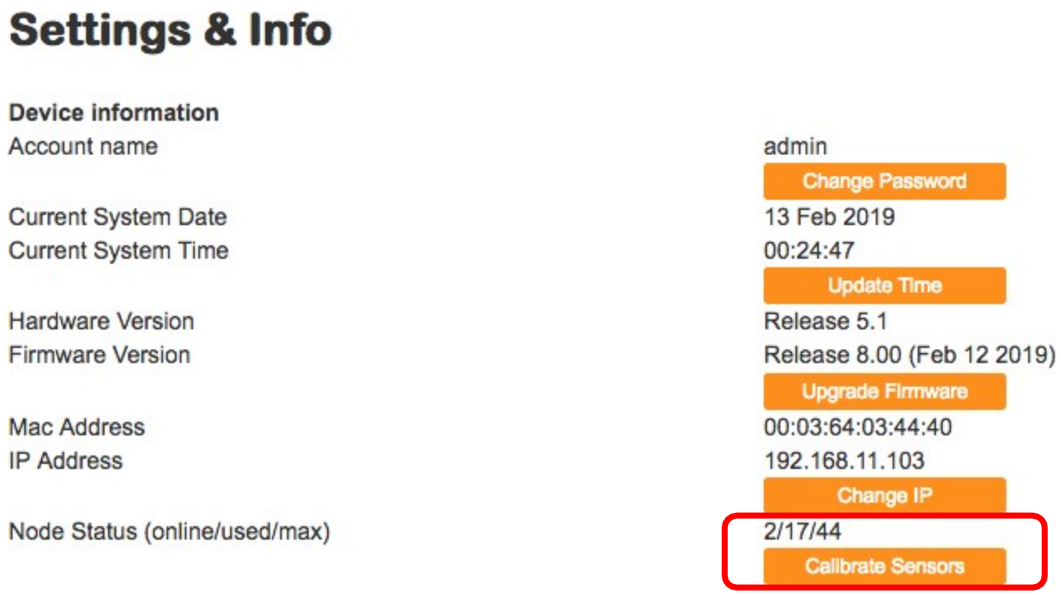
In the main window, click on the **Menu button** located on the upper right corner of the page. Then click on settings, and once the page loads click on "**Change IP**"



Sensors

Status	Type	Name	Value	Warning Range	Down Range	Repeat Alarm	Email	SMS	SNMP Trap	Set Output To	
🟩	Temperature	Int. Temp1	28.98 °C	<16 OR >37	<15 OR >41	□	□	☑	□	DISABLE	-





Settings & Info

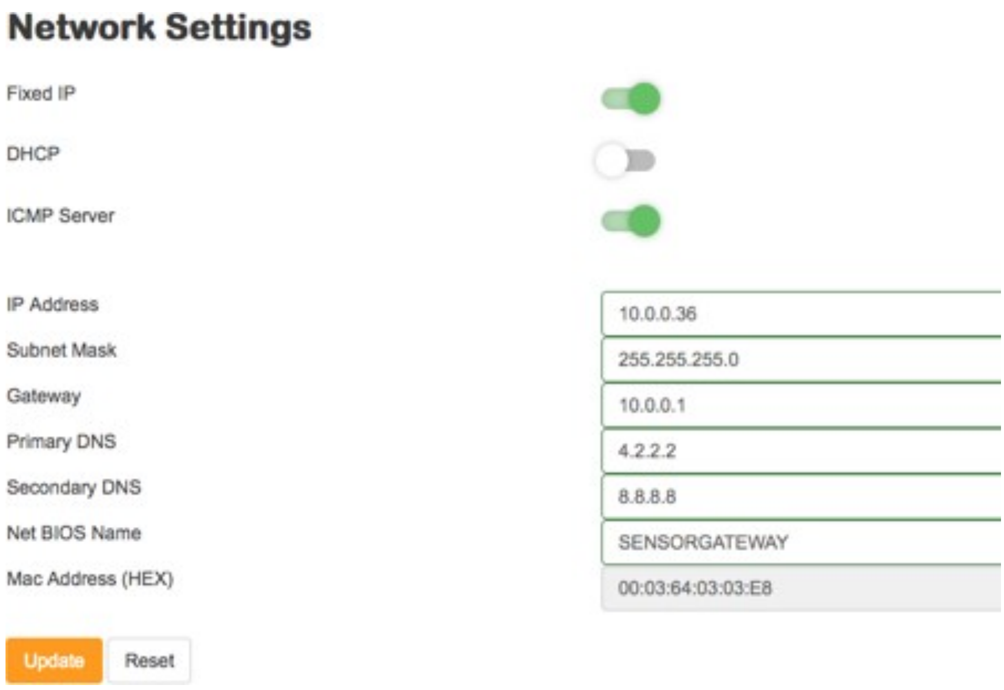
Device information

Account name	admin
Current System Date	13 Feb 2019
Current System Time	00:24:47
Hardware Version	Release 5.1
Firmware Version	Release 8.00 (Feb 12 2019)
Mac Address	00:03:64:03:44:40
IP Address	192.168.11.103
Node Status (online/used/max)	2/17/44

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. https://technet.microsoft.com/en-us/library/cc958811.aspx

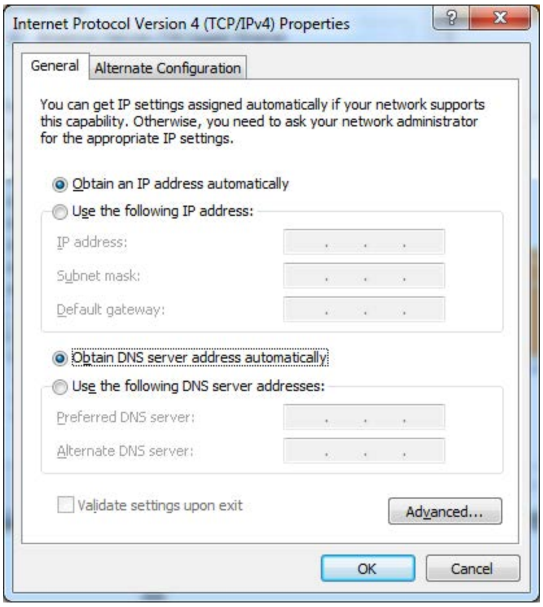
Once the value has been changed, the Base Unit will reboot itself and will then be accessible through the newly defined IP.



Network Settings

Fixed IP	●
DHCP	○
ICMP Server	●
IP Address	10.0.0.36
Subnet Mask	255.255.255.0
Gateway	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

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



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

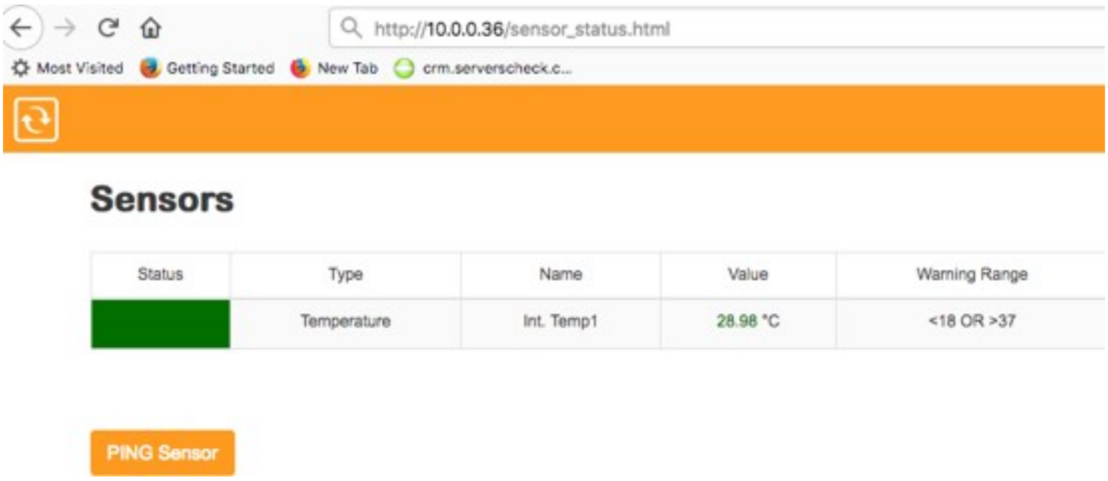
○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

☐ Validate settings upon exit

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



http://10.0.0.36/sensor_status.html

Sensors

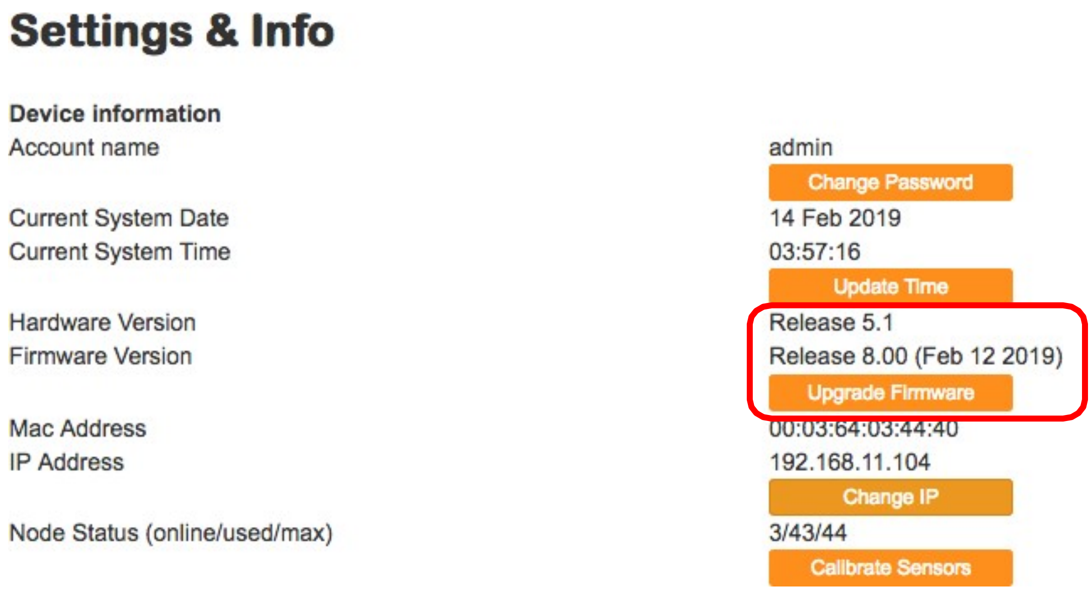
Status	Type	Name	Value	Warning Range
🟩	Temperature	Int. Temp1	28.98 °C	<18 OR >37

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

Device information

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

Go to http://www.infrasensing.com/sensors/firmware.asp to check for new firmware releases. Simply check on that page the latest firmware version available for your Base Unit

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.

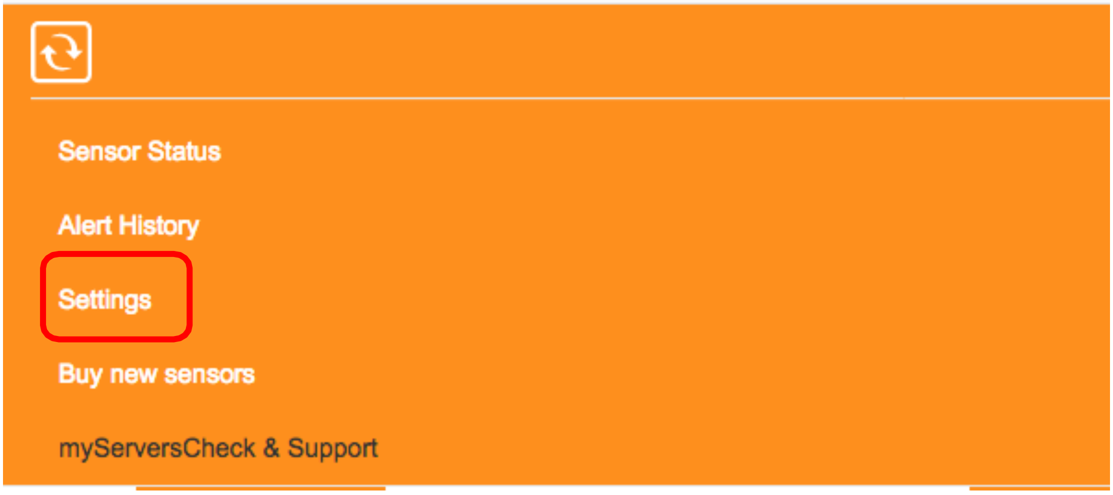
Your Base Unit will now start loading the new firmware. Your Base Unit will be available on http://192.168.11.160 (Default) or via the IP address shown on its OLED after the firmware update has been completed

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

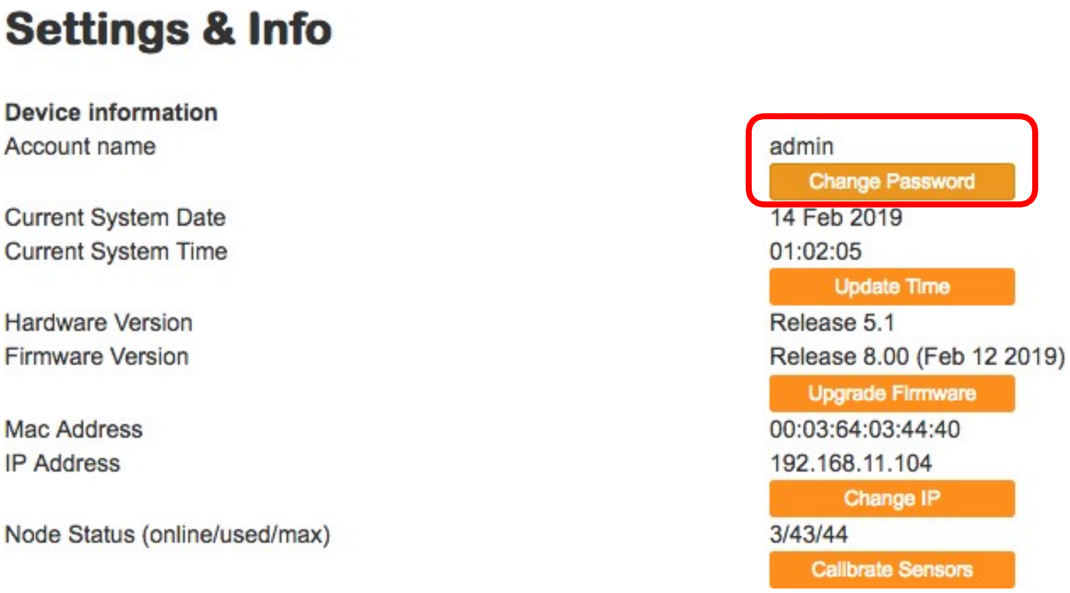
1.15 Configuring the Base Unit's access security

The Base Unit's can be username and password secured. Default factory values are **admin/admin**

To change the values, click on the **Settings** menu option



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



Settings & Info

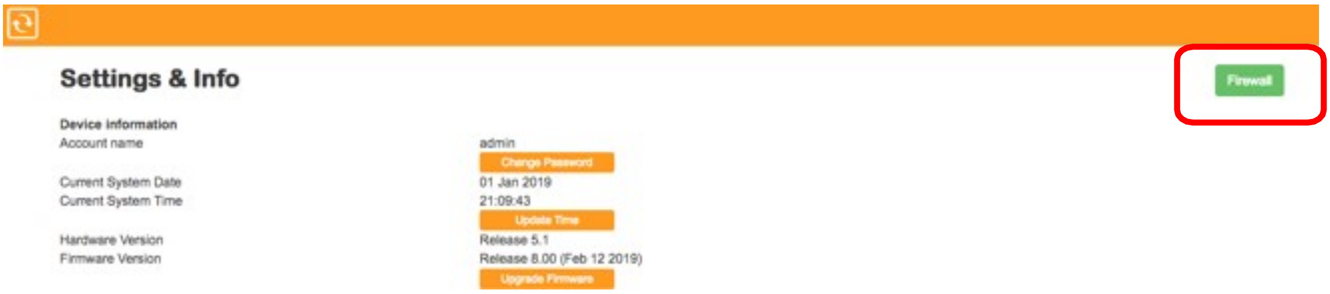
Device information

Account name	admin
	Change Password
Current System Date	14 Feb 2019
Current System Time	01:02:05
	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

2 Base Unit features and configuration

2.1 Firewall settings

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

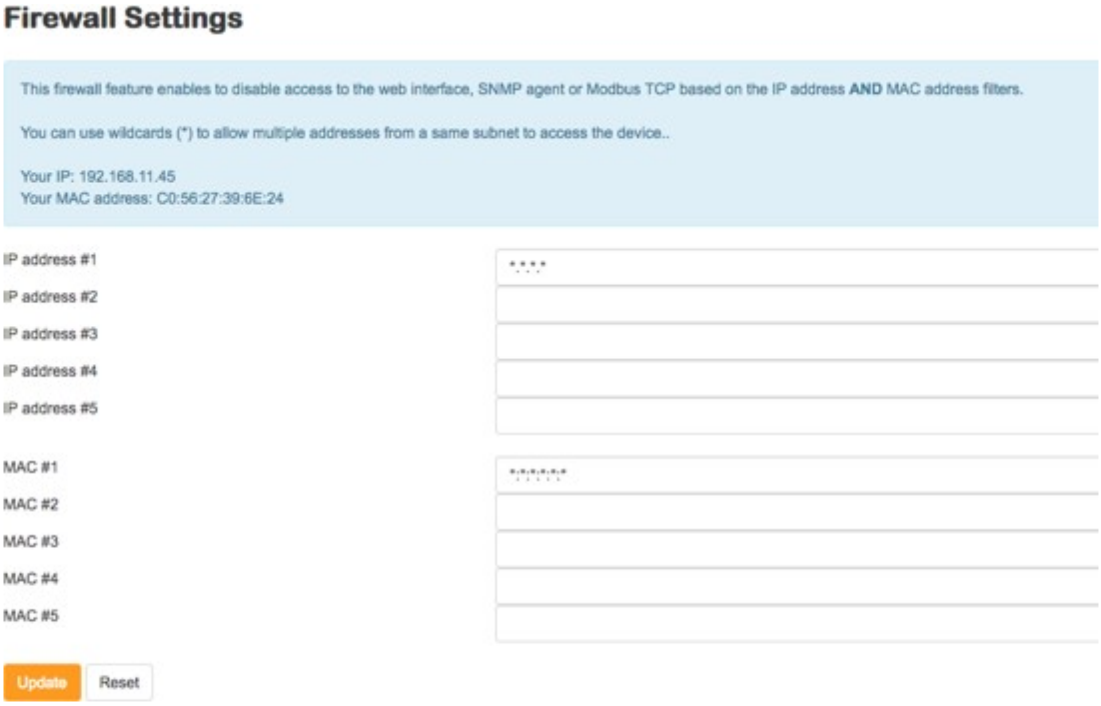


Settings & Info

Device information

Account name	admin Change Password
Current System Date	01 Jan 2019
Current System Time	21:09:43 Update Time
Hardware Version	Release 5.1
Firmware Version	Release 8.00 (Feb 12 2019) Upgrade Firmware

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 same 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	

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.

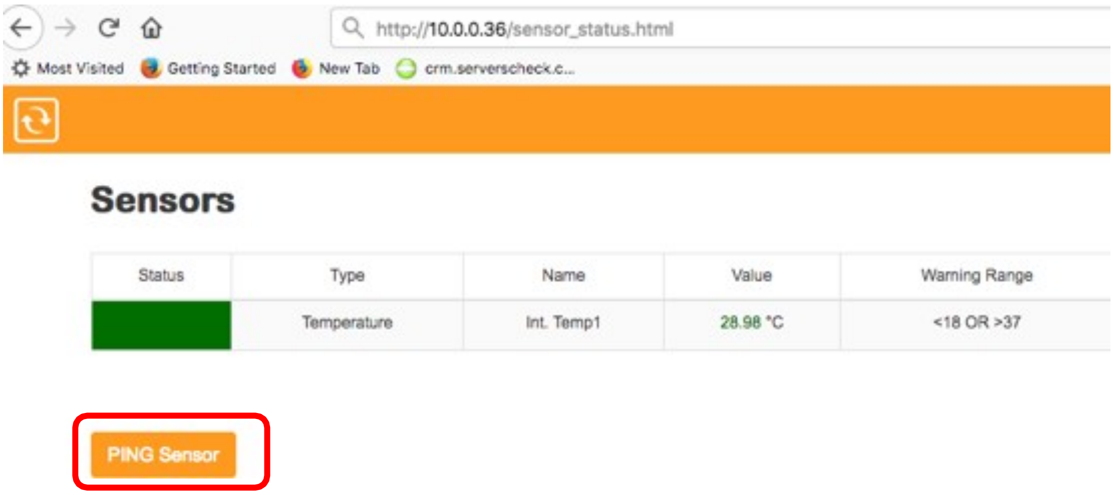
Note: MAC address letters should always be in upper case.

2.2 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.

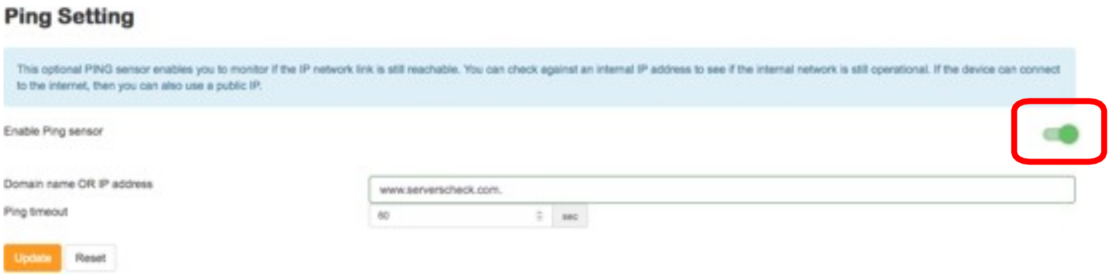


http://10.0.0.36/sensor_status.html

Sensors

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

2. Make sure to click on "Enable Ping"



Ping Setting

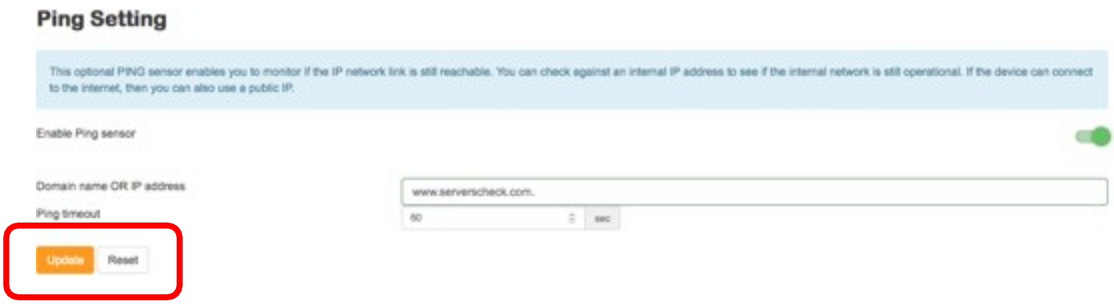
This optional PING sensor enables you to monitor if the IP network link is still reachable. You can check against an internal IP address to see if the internal network is still operational. If the device can connect to the internet, then you can also use a public IP.

Enable Ping sensor

Domain name OR IP address: www.serverscheck.com.

Ping timeout: 60 sec

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



Ping Setting

This optional PING sensor enables you to monitor if the IP network link is still reachable. You can check against an internal IP address to see if the internal network is still operational. If the device can connect to the internet, then you can also use a public IP.

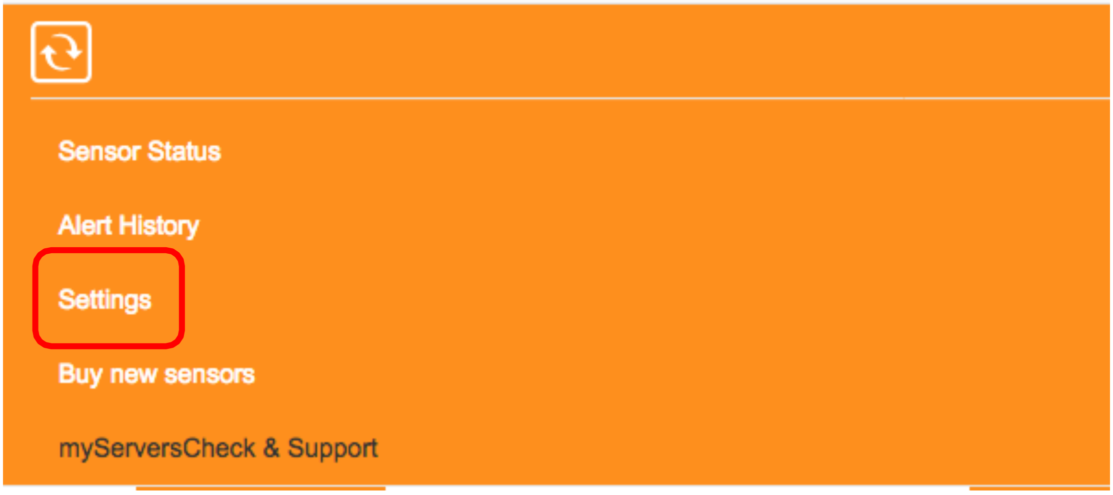
Enable Ping sensor

Domain name OR IP address: www.serverscheck.com.

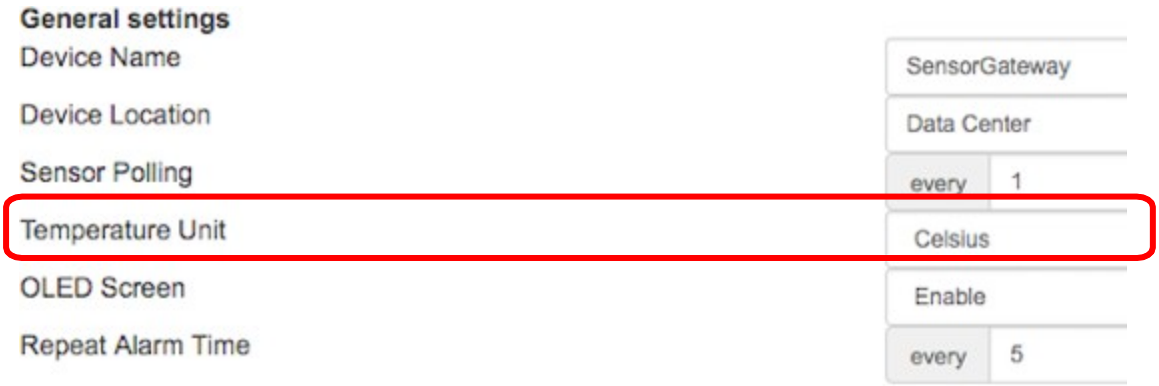
Ping timeout: 60 sec

2.3 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.



Change the value from Celsius to Fahrenheit under general settings.

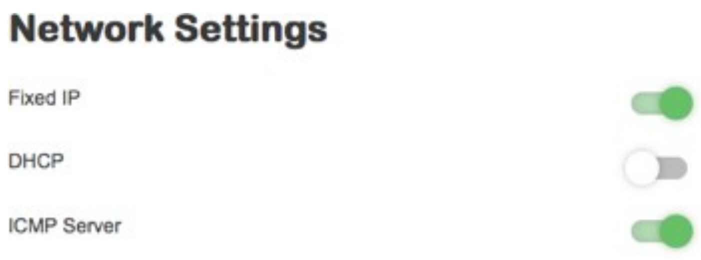


General settings

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

2.4 ICMP server

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



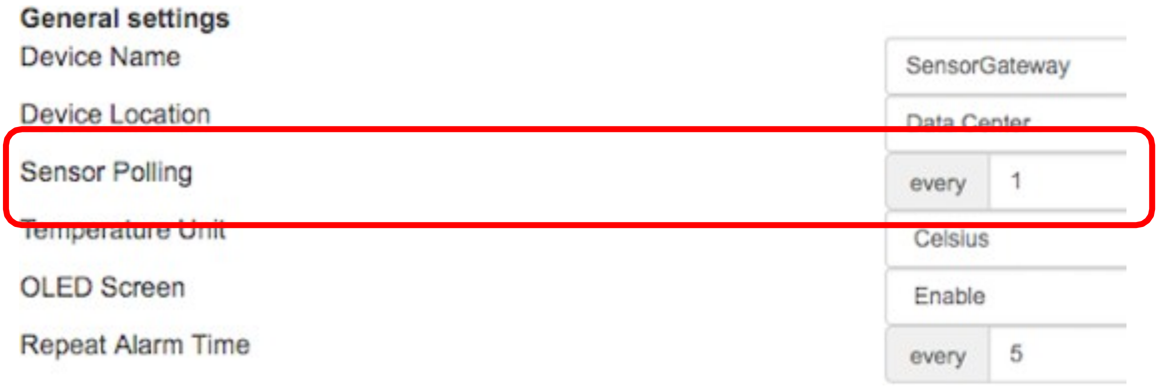
Network Settings

Fixed IP	●
DHCP	○
ICMP Server	●

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

2.5 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.

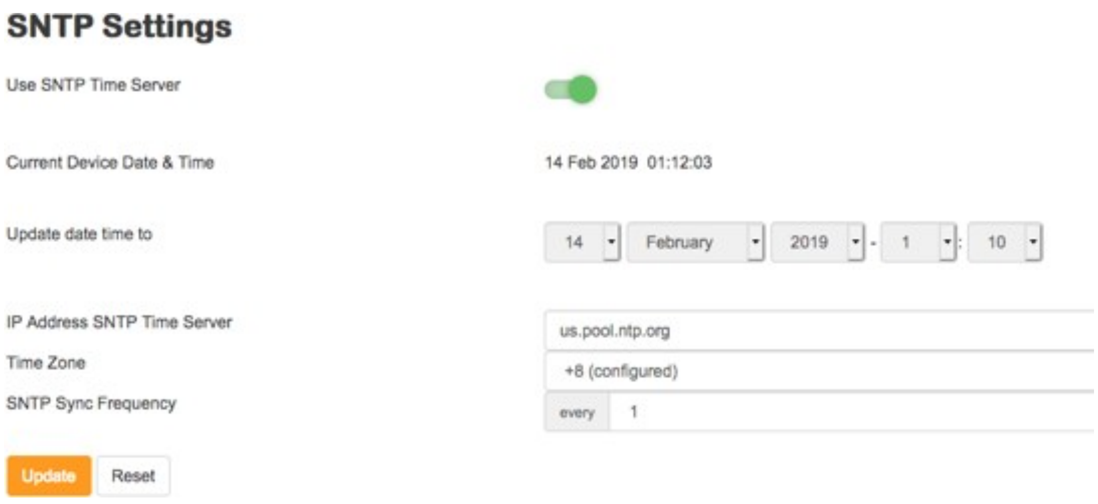


General settings

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

2.6 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

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

Country	UTC time offset
A	
Afghanistan	+04
Albania *	+01
Algeria	+01
Andorra *	+01
Angola	+01
Antigua and Barbuda	–04
Arg'entina	–03
'Ar'enia	'04
Australia – 5 time zones	
Western Australia'08 Northern Territory +09 South 'Australia * +09 Austra'lian C'apital Territory * +10 New South Wale's * +10 Queens'a'+10 Tasmania * '10 Victoria * +'0 Lor' Howe Island'* +10 M'c'uraei Is'and +11	
Australian Overseas Territories – 6 time Zones	
Heard Island and McDonald Islands +05 Cocos (Keeling) Islands +06 Christmas Island +07 Ashmore and Cartier Islands +08 Coral Sea Islands +10 Norfolk Island +11	
Austria *	+01
Azerbaijan *	+04
B	
Bahamas *	–'5
Bahrain	+03
Bangladesh	+06
Barbados	–04
Belarus	+03
Belgium *	+01
Belize	–06
Benin	+01
Bhutan	+06
M	
Macedonia *	+01
Madagascar	+03
Malawi	+02
Malaysia	+08
Maldives	+05
Mali	±00
Malta *	+01
Marshall Islands	+12
Mauritania	±00
Mauritius	+04
Mexico * – 3 time zones	
The state o'Baja California –08 The states of Baja California Sur, Chihuahua, Nayarit, Sinaloa and Sonora –07 Most of Mexico –06	
Micronesia – 2 time zones	
The states of Chuuk and Yap +10 The states of Kosrae and Pohnpei +11	
Moldova *	+02
Monaco *	+01
Mongolia * – 2 time zones	
Provinces of Khovd, Uvs, Bayan-Olgii +07	
Ulaanbaatar and most of the country +08	
Montenegro *	+01
Morocco *	±00
Mozambique	+02
Myanmar (Burma)	+06::
N	
Namibia	+01
Nauru	+12
Nepal	+05:45
Netherlands *	+01
Netherlands Overseas Territories – 1 time	

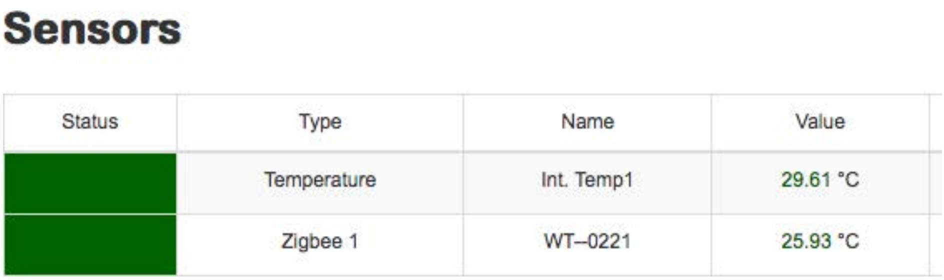
Bolivia	−04
Bosnia and Herzegovina *	+01
Botswana	+02
Brazil – 4 time zones	
Acre and Southwestern Amazonas −05 Most part of the Amazonas State, Mato Grosso, Mato Grosso do Sul, Rondônia, Roraima −04 The Southeast, the South, the Northeast Regions (except some islands), Goias, Distrito Federal, Tocantins, Pará, Amapa −03 Islands on the east coast of Brazil (Fernando de Noronha, Trindade, Martin Vaz, Atol das Rocas, Saint Peter and Paul Rocks) −02	
Brunei	+08
Bulgaria *	+02
Burkina Faso	±00
Burundi	+02
C	
Cabo Verde	−01
Cambodia	+07
Cameroon	+01
Canada – 6 time zones	
Larger western part of British Columbia, Tungsten and the associated Cantung Mine in Northwest Territories, Yukon −08 Alberta, some eastern parts of British Columbia, the Northwest Territories, Nunavut (west of 102°W and all communities in the Kitikmeot Region), Lloydminster −07 Manitoba, Nunavut (between 85°W and 102°W except western Southampton Island), Ontario (Northwestern Ontario west of 90°W with some exceptions and Big Trout Lake area east of 90°W), Saskatchewan except Lloydminster −06 Nunavut east of 85°W and entire Southampton Island, Ontario east of 90°W (except Big Trout Lake area), the most part of Quebec −05 Labrador (all but southeastern tip), New Brunswick, Nova Scotia, Prince Edward Island, eastern part of Quebec −04 Labrador (southeastern), Newfoundland −03	
Central African Republic	+01
Chad	+01
Chile	−04
Chile - Easter Island	−06
China	+08
Colombia	−05
Comoros	+03
Congo, Republic of the	+01
Congo, Dem. Rep. - Kinshasa	+01
Congo, Dem. Rep. - Lubumbashi	+02
Costa Rica	−06
Cote d'Ivoire	±00
Croatia *	+01
Cuba *	−05
Cyprus *	+02
Czech Republic	+'1
D	
zones	
Aruba −04 Caribbean Netherlands −04 Curaçao −04 Sint Maarten −04	
New Zealand *	+12
New-Zealand's Dependent Territories – 4 time zones	
Niue −11 Cook Islands −10 Chatham Islands +12:45 Tokelau +13	
Nicaragua	−06
Niger	+01
Nigeria	+01
North Korea	+09
Norway *	+01
O	
Oman	+04
P	
Pakistan	+05
Palau	+09
Palestine *	−06
Panama	−05
Papua New Guinea	+10
Paraguay	−04
Peru	−05
Philippines	+08
Poland *	+01
Portugal *	±00
Portugal - Azores *	+01
Q	
Qatar	+03
R	
Romania *	+02
Russia – 9 time zones	
Kaliningrad Oblast +03 Most of European Russia and all railroads throughout Russia +04 Bashkortostan, Chelyabinsk Oblast, Khanty–Mansia, Kurgan Oblast, Orenburg Oblast, Perm Krai, Sverdlovsk Oblast, Tyumen Oblast, and Yamalia +06 Altai Krai, Altai Republic, Kemerovo Oblast, Novosibirsk Oblast, Omsk Oblast and Tomsk Oblast +07 Khakassia, Krasnoyarsk Krai and Tuva +08 Buryatia and Irkutsk Oblast +09 Amur Oblast, western Sakha Republic and Zabaykalsky Krai +10 The Jewish Autonomous Oblast, Khabarovsk Krai, Primorsky Krai, central Sakha Republic and Sakhalin Island +11 Magadan Oblast, eastern Sakha, Kuril Islands, Chukotka and Kamchatka Krai +12	
Rwanda	+02
S	
St. Kitts and Nevis	−04
St. Lucia	−04
St. Vincent and The Grenadines	−04
Samoa	+13
San Marino *	+01
Sao Tome and Principe	±00
Saudi Arabia	+03
Senegal	±00

Denmark *	+01
Denmark's Dependent Territories * – 4 time zones	
The most of Greenland, including inhabited south coast and west coast −03 Greenland - Thule Air Base −04 Greenland - Ittoqqortoormiit −01 Faroe Islands ±00	
Djibouti	+03
Dominic	−04
Dominican Republic	−04
E	
Ecuador	−05
Ecuador - Galapagos Province	−06
Egypt	+02
El Salvador	−06
Equatorial Guinea	+01
Eritrea	+03
Estonia *	+02
Ethiopia	+03
F	
Fiji	+12
Finland *	+02
France *	+01
French Overseas Territories – 10 time zones	
French Polynesia - Tahiti Island −10 French Polynesia - Marquesas Islands −09 French Polynesia - Gambier Islands −09 Clipperton Island −07 Guadeloupe −04 Martinique −04 Saint Barthelemy −04 Saint Martin −04 French Guiana −03 Saint Pierre and Miquelon * −03 Mayotte +03 Réunion +04 Kerguelen Islands +05 New Caledonia +11 Wallis and Futuna +12	
G	
Gabon	+01
Gambia	±00
Georgia	+04
Germany *	+01
Ghana	±00
Greece *	+02
Grenada	−04
Guatemala	−06
Guinea	±00
Guinea-Bissau	±00
Guyana	−04
H	
Hait'i *	−05
Honduras	−06
Hungary *	+01
I	
Iceland	±00
India	+05
Indonesia – 3 time zones	
Islands of Sumatra, Java, provinces of West Kalimantan and Central Kalimantan +07 Islands of Sulawesi, Bali, provinces of East Nusa Tenggara, West Nusa Tenggara, E'st Kalimantan and South Kalimantan +08 Provinces of Maluku, North Maluku, Papua and West Papua +09	
Serbia *	+01
Seychelles	+04
Sierra Leone	±00
Singapore	+08
Slovakia *	+01
Slovenia *	+01
Solomon Islands	+11
Somalia	+03
South Africa	+02
South Korea	+09
South Sudan	+03
Spain *	+01
Spain - Canary Islands *	±00
Sri Lanka	+05
Sudan	+03
Suriname	−03
Swaziland	+02
Sweden *	+01
Switzerland *	+01
Syria *	+02
T	
Taiwan	+08
Tajikistan	+05
Tanzania	+03
Thailand	+07
Timor-Leste	+09
Togo	±00
Tonga	+13
Trinidad and Tobago	−04
Tunisia	+01
Turkey *	+02
Turkmenistan	+05
Tuvalu	+12
U	
Uganda	+03
Ukraine	+02
United Arab Emirates	+04
United Kingdom *	±00
British Overseas Territories – 9 time zones	
Pitcairn Islands −08 Cayman Islands −05 Anguilla −04 Bermuda −04 British Virgin Islands −04 Montserrat −04 Turks and Caicos Islands −04 Falkland Islands −03 South Georgia and the South Sandwich Islands −02 Saint Helena ±00 Ascension and Tristan da Cunha ±00 Guernsey * ±00 Isle of Man * ±00 Jersey * ±00 Gibraltar * +01 Akrotiri and Dhekelia * +02 British Indian Ocean Territory +06	
United States of America * – 6 time zones	
Hawaii, most of the Aleutian Islands −10 Most of the state of Alaska −09 The states on the Pacific coast plus Nevada, parts of Idaho −08 Arizona, Colorado, Montana, New Mexico, Utah, parts of Idaho, Kansas, Oregon, North Dakota, South Dakota, Texas −07 Gulf Coast, Tennessee Valley, U.S. Interior Highlands, Great Plains, most of Texas −06 The states on the Atlantic coast, the eastern two-thirds of the Ohio Valley,	

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

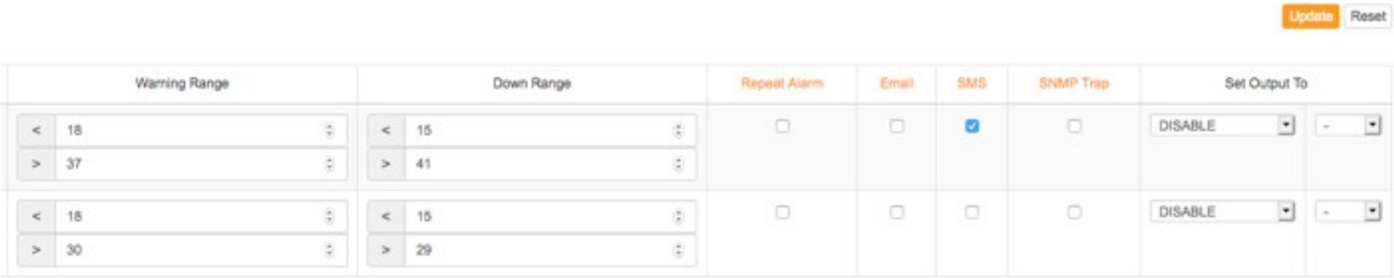
2.7 Setting threshold values in the Base Unit for alerting

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	Type	Name	Value
🟩	Temperature	Int. Temp1	29.61 °C
🟩	Zigbee 1	WT–0221	25.93 °C



Warning Range	Down Range	Repeat Alarm	Email	SMS	SNMP Trap	Set Output To	
< 18 > 37	< 15 > 41	☐	☐	☑	☐	DISABLE	-
< 18 > 30	< 15 > 29	☐	☐	☐	☐	DISABLE	-

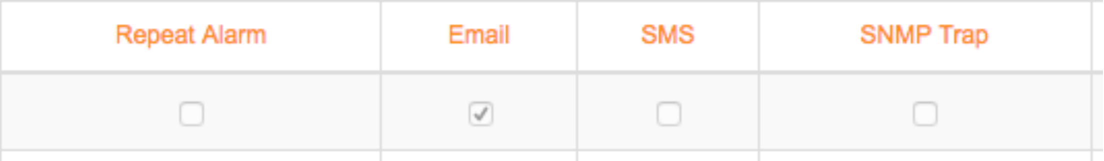
Status: this shows if the internal sensor or the external sensor probe is working or not
Type: type of reading for the sensor
Name this is the name of the sensor and will be used in alerting
Value: this is the latest reading for both the internal sensor and the external sensor probe
Warning range: below 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 Only if the 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 Base Unit alerting feature

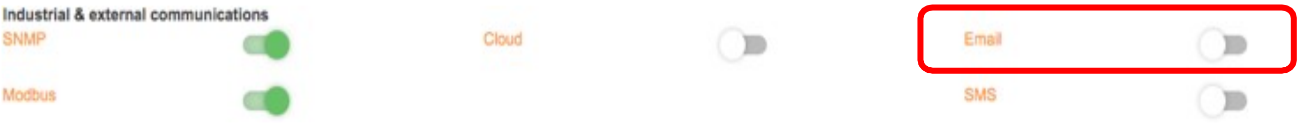
3.1 Email alerting

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
□	☑	□	□

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 communications

SNMP ●

Modbus ●

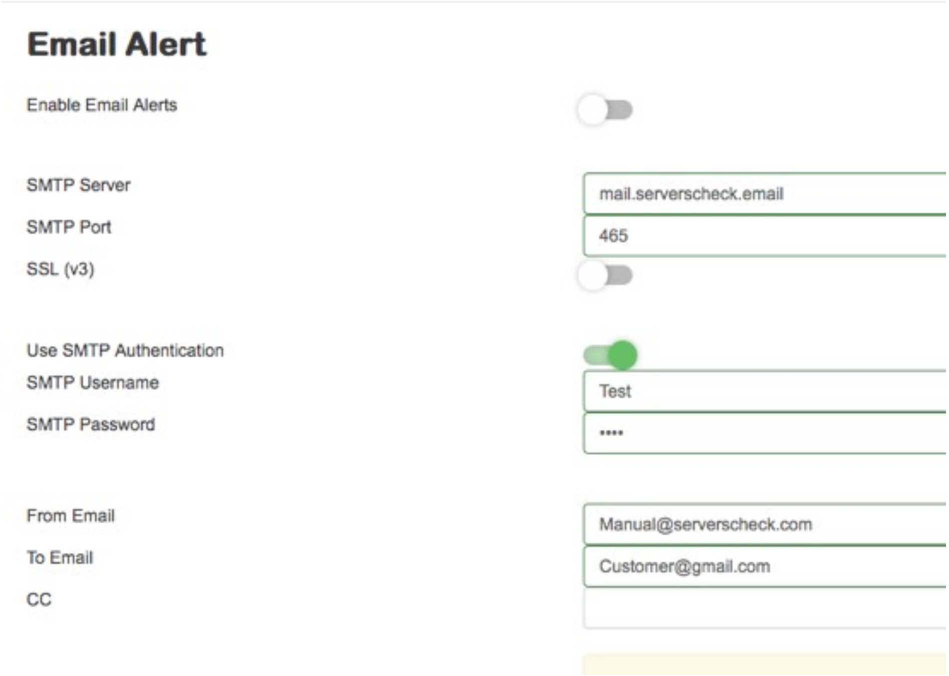
Cloud ○

Email ○

SMS ○

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: ••••

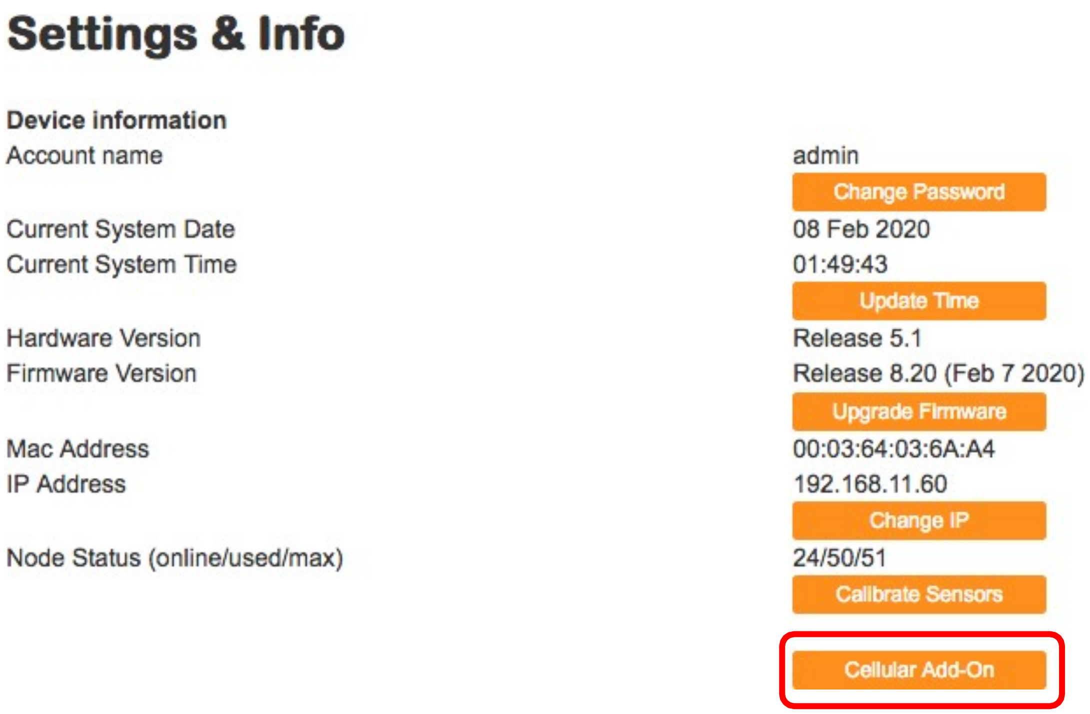
From Email: Manual@serverscheck.com
To Email: Customer@gmail.com
CC:

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.

3.2 Email alerts using the ADDON-LTE



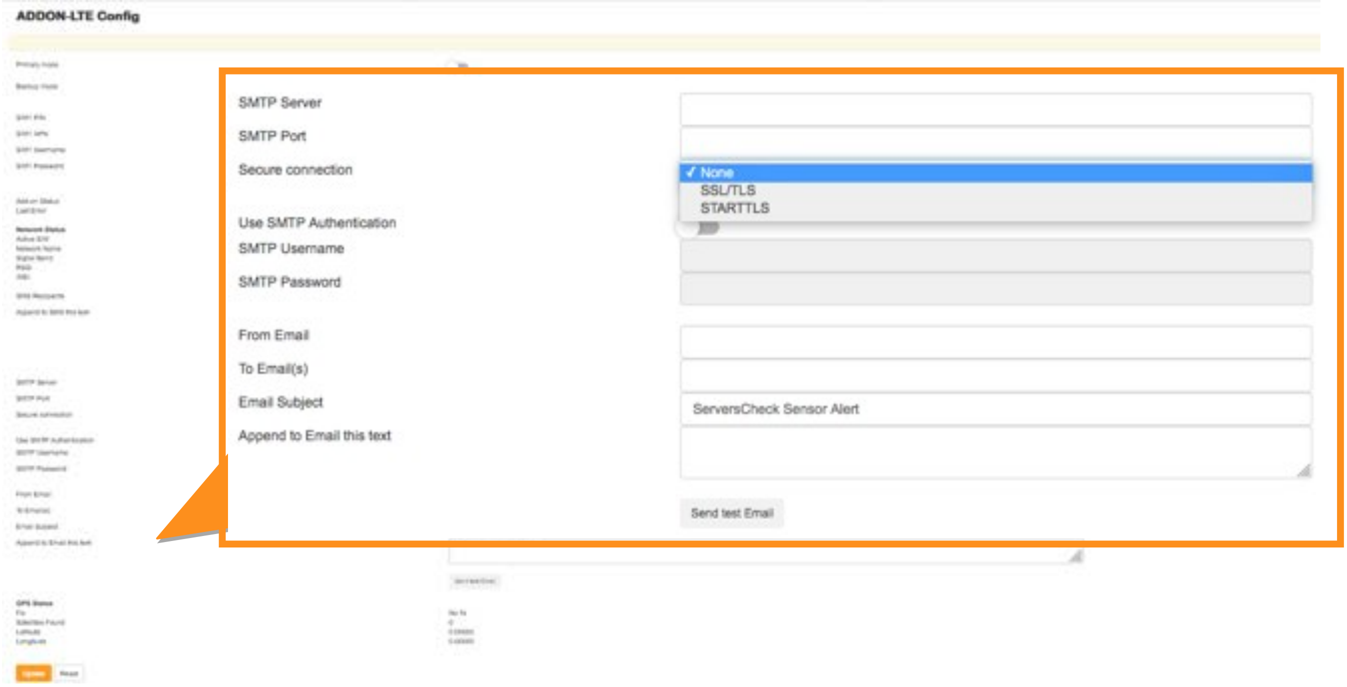
Settings & Info

Device information

Account name	admin
	Change Password
Current System Date	08 Feb 2020
Current System Time	01:49:43
	Update Time
Hardware Version	Release 5.1
Firmware Version	Release 8.20 (Feb 7 2020)
	Upgrade Firmware
Mac Address	00:03:64:03:6A:A4
IP Address	192.168.11.60
	Change IP
Node Status (online/used/max)	24/50/51
	Calibrate Sensors
	Cellular Add-On

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



ADDON-LTE Config

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

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).

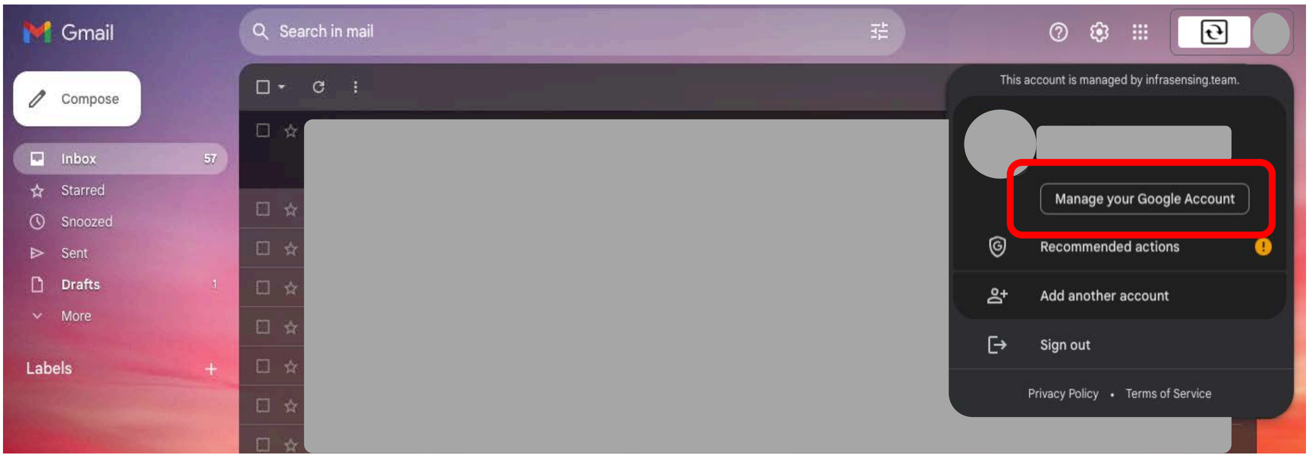
3.2.1 Gmail as e-mail server (https://mail.google.com)

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

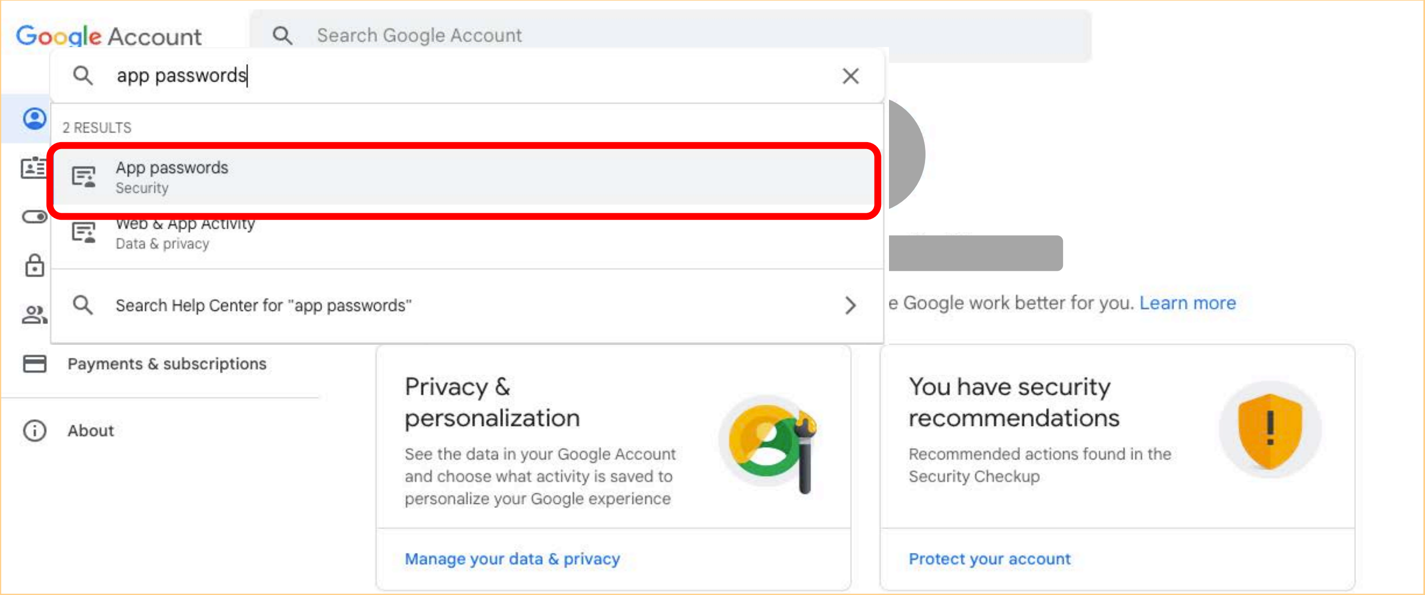
Below are the instructions on how to set it up.

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

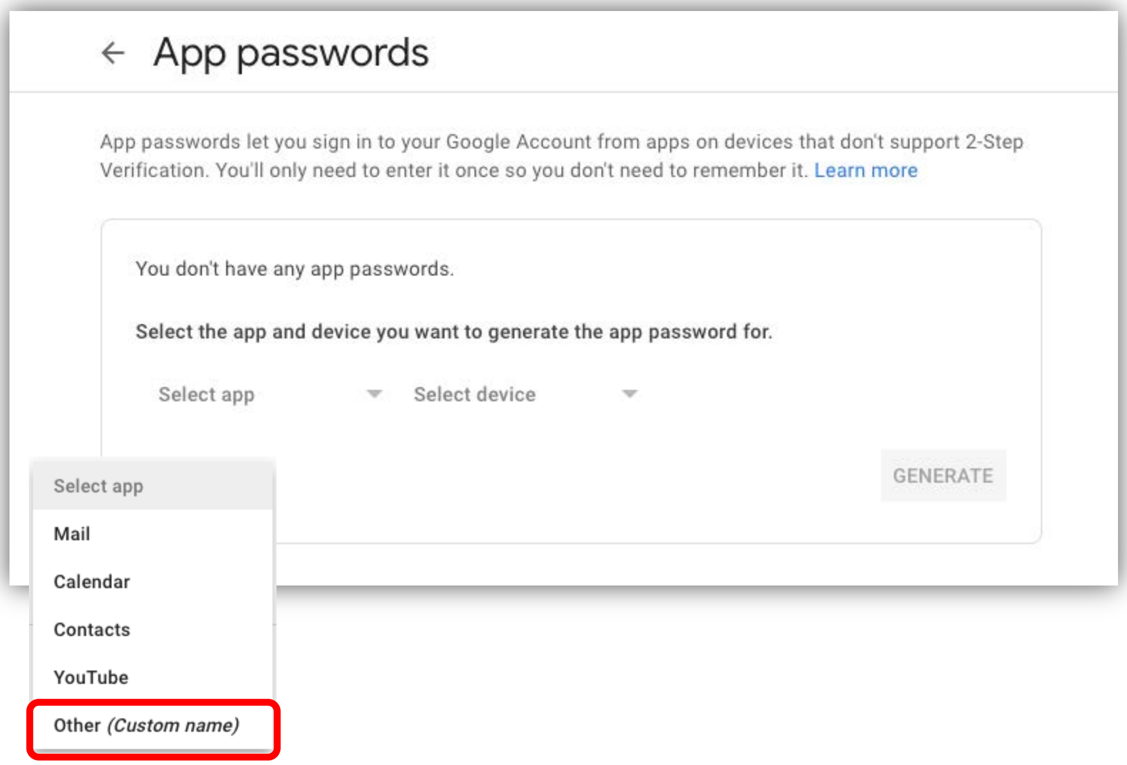


2. On the search bar type in **"App Passwords."**

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


Google Account
Search Google Account
app passwords
2 RESULTS
App passwords
Security
Web & App Activity
Data & privacy
Search Help Center for "app passwords"
Payments & subscriptions
About
e Google work better for you. Learn more
Privacy & personalization
See the data in your Google Account and choose what activity is saved to personalize your Google experience
Manage your data & privacy
You have security recommendations
Recommended actions found in the Security Checkup
Protect your account

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



App passwords

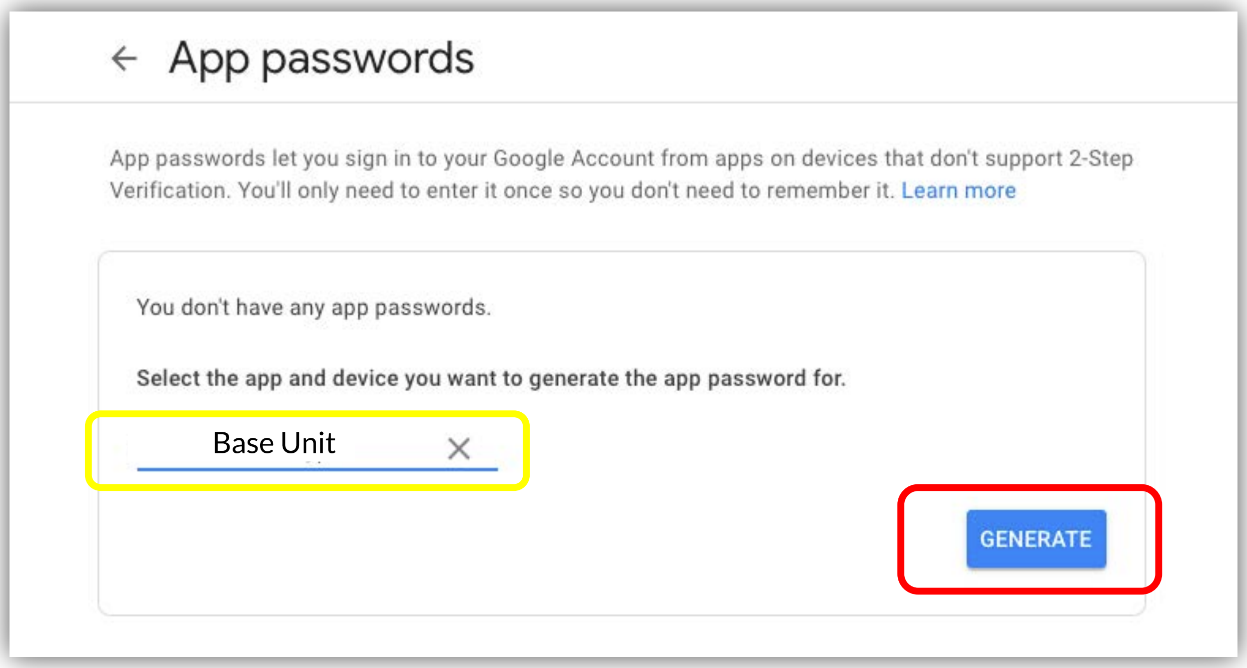
App passwords let you sign in to your Google Account from apps on devices that don't support 2-Step Verification. You'll only need to enter it once so you don't need to remember it. Learn more

You don't have any app passwords.

Select the app and device you want to generate the app password for.

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

App passwords let you sign in to your Google Account from apps on devices that don't support 2-Step Verification. You'll only need to enter it once so you don't need to remember it. Learn more

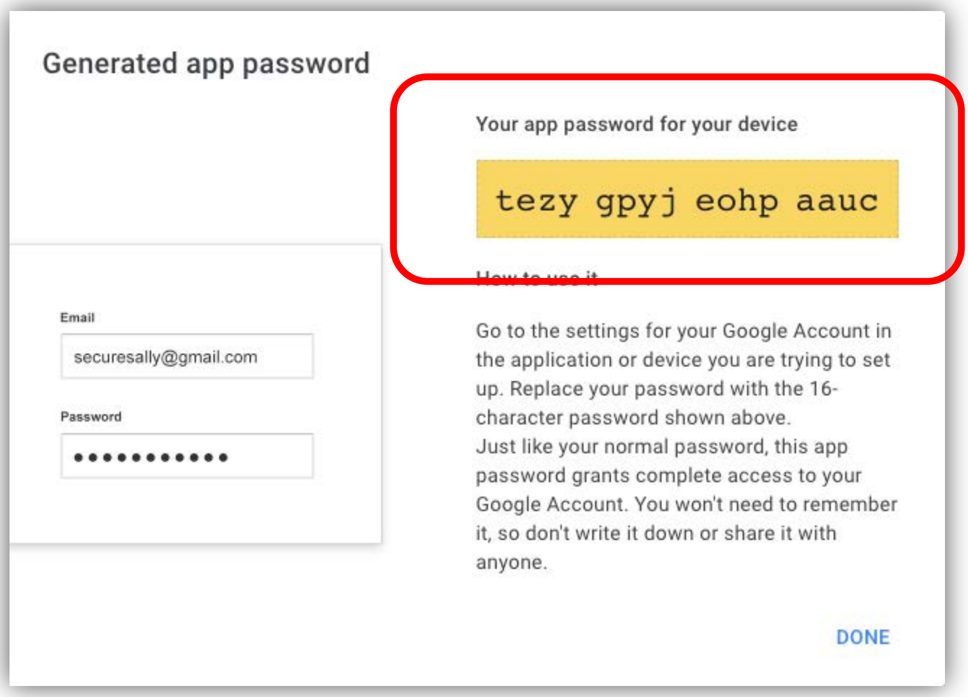
You don't have any app passwords.

Select the app and device you want to generate the app password for.

Base Unit

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

Email

securesally@gmail.com

Password

●●●●●●●●●●●●

Your app password for your device

tezy gpyj eohp aauc

How to use it

Go to the settings for your Google Account in the application or device you are trying to set 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: yourgmailname@gmail.com 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.

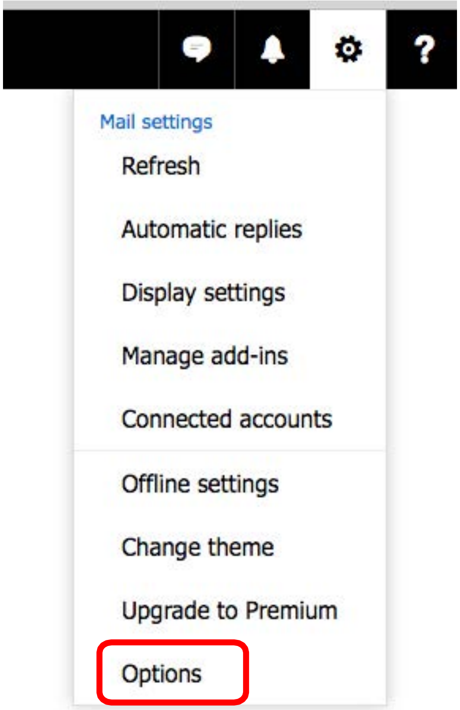
Note: Only version 5 Base Units are supported with Gmail's SSL ever since they offered RSA 2048-bit encryption.

3.2.2 Outlook mail as e-mail server (https://outlook.live.com)

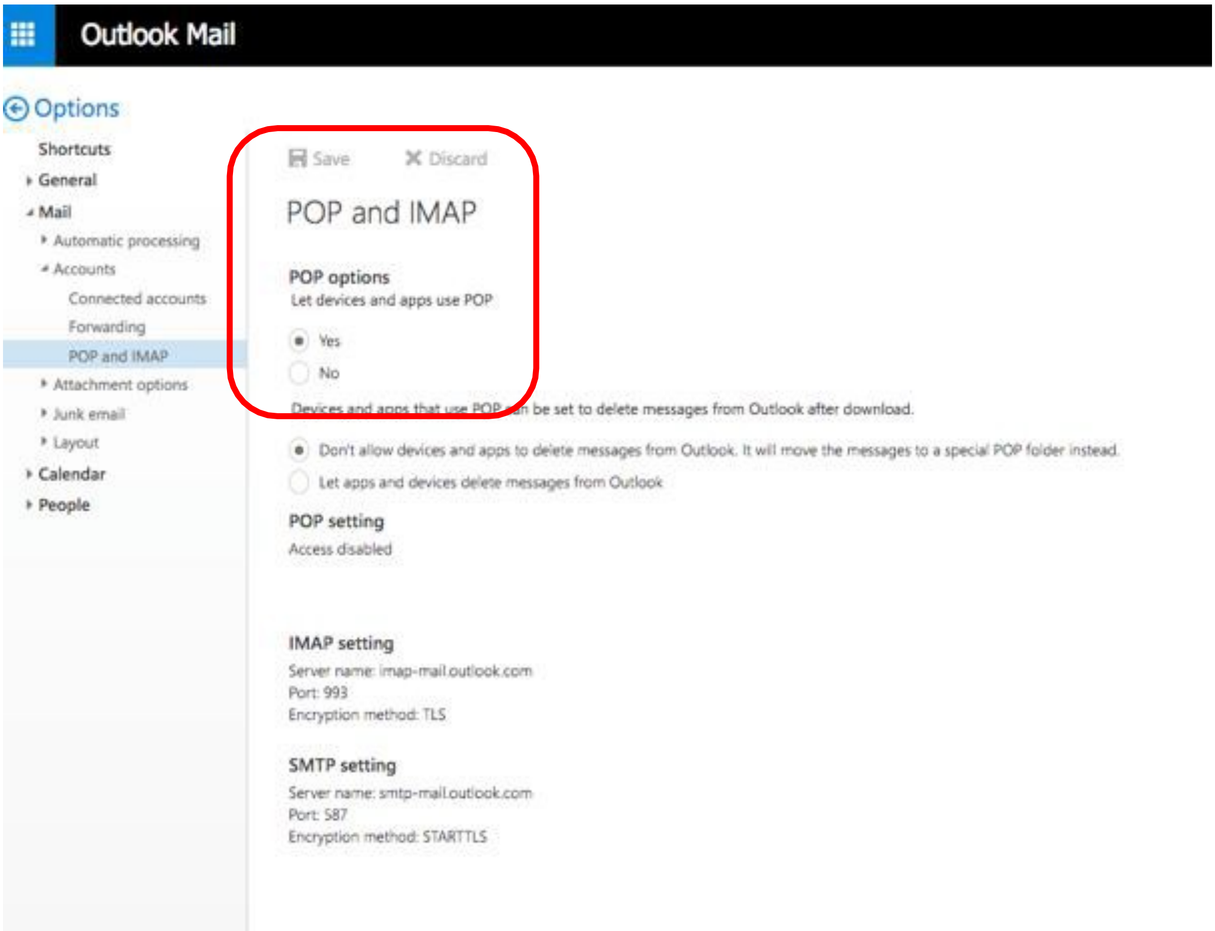
Outlook mail is another example of an SMTP server, which can be used on the gateway

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 Icon 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”



POP and IMAP

POP options
Let devices and apps use POP

● Yes
○ No

Devices and apps that use POP can be set to delete messages from Outlook after download.

● Don't allow devices and apps to delete messages from Outlook. It will move the messages to a special POP folder instead.
○ Let apps and devices delete messages from Outlook

POP setting
Access disabled

IMAP setting
Server name: imap-mail.outlook.com
Port: 993
Encryption method: TLS

SMTP setting
Server name: smtp-mail.outlook.com
Port: 587
Encryption method: STARTTLS

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.

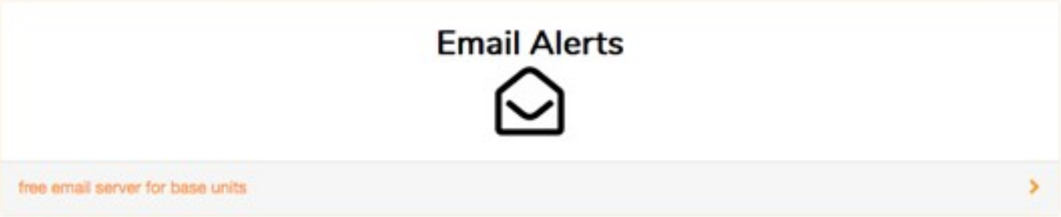
Note:
Check if your account allows User Consent to apps:

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.

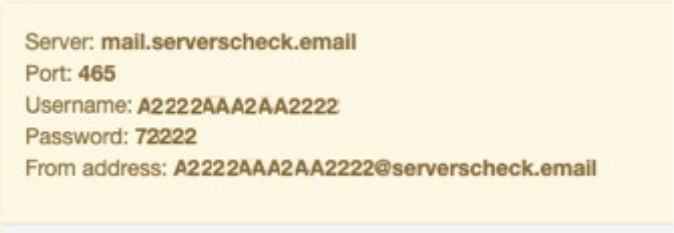
3.2.3 Using InfraSensing premium e-mail (https://my.InfraSensing.com)

**A premium Account is free to create and is required to enjoy the service **

1. Log in to your InfraSensing Premium account and click on Alerts and then **Email Alerts** or simply log in and go to this link https://my.infrasensing.com/email/



2. You should now see the configuration you have to copy in to your gateway's email settings to receive alerts using your accounts UID and PIN.

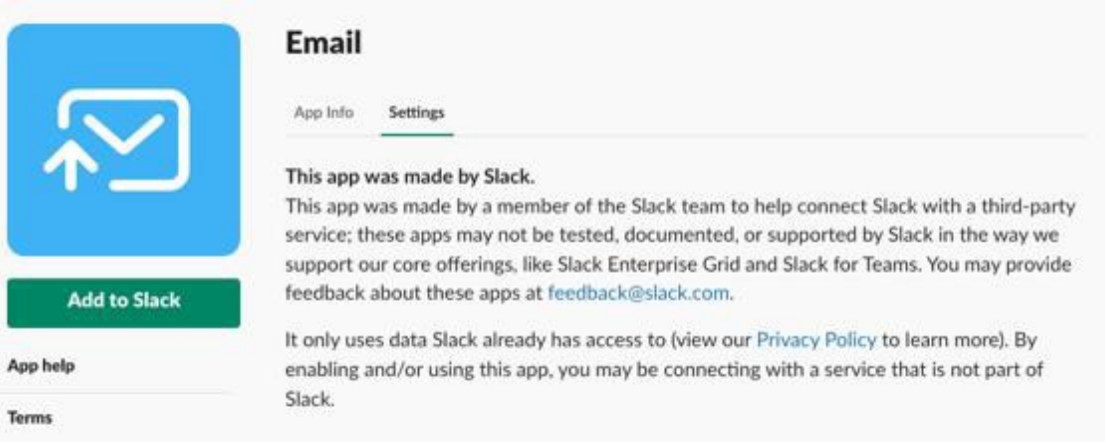


Server: **mail.serverscheck.email**
Port: **465**
Username: **A2222AAA2AA2222**
Password: **72222**
From address: **A2222AAA2AA2222@serverscheck.email**

Note: Make sure you copy all details and leave the box for SSL unchecked. The service is FREE on every premium account.

3.3 Slack channel integration via e-mail alerts

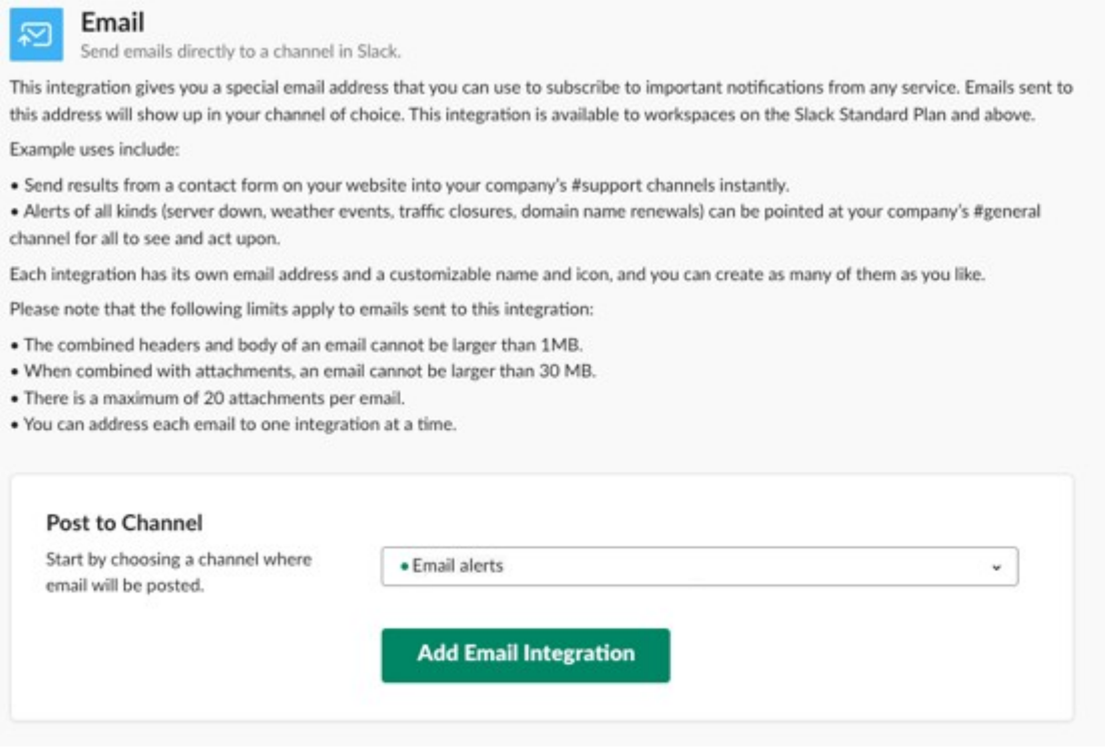
To receive alerts via slack we first need to have the email app integrated into our slack account



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 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 enabling and/or using this app, you may be connecting with a service that is not part of 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.

This integration gives you a special email address that you can use to subscribe to important notifications from any service. Emails sent to this address will show up in your channel of choice. This integration is available to workspaces on the Slack Standard Plan and above.

Example uses include:

- Send results from a contact form on your website into your company's #support channels instantly.
- Alerts of all kinds (server down, weather events, traffic closures, domain name renewals) can be pointed at your company's #general channel for all to see and act upon.

Each integration has its own email address and 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:

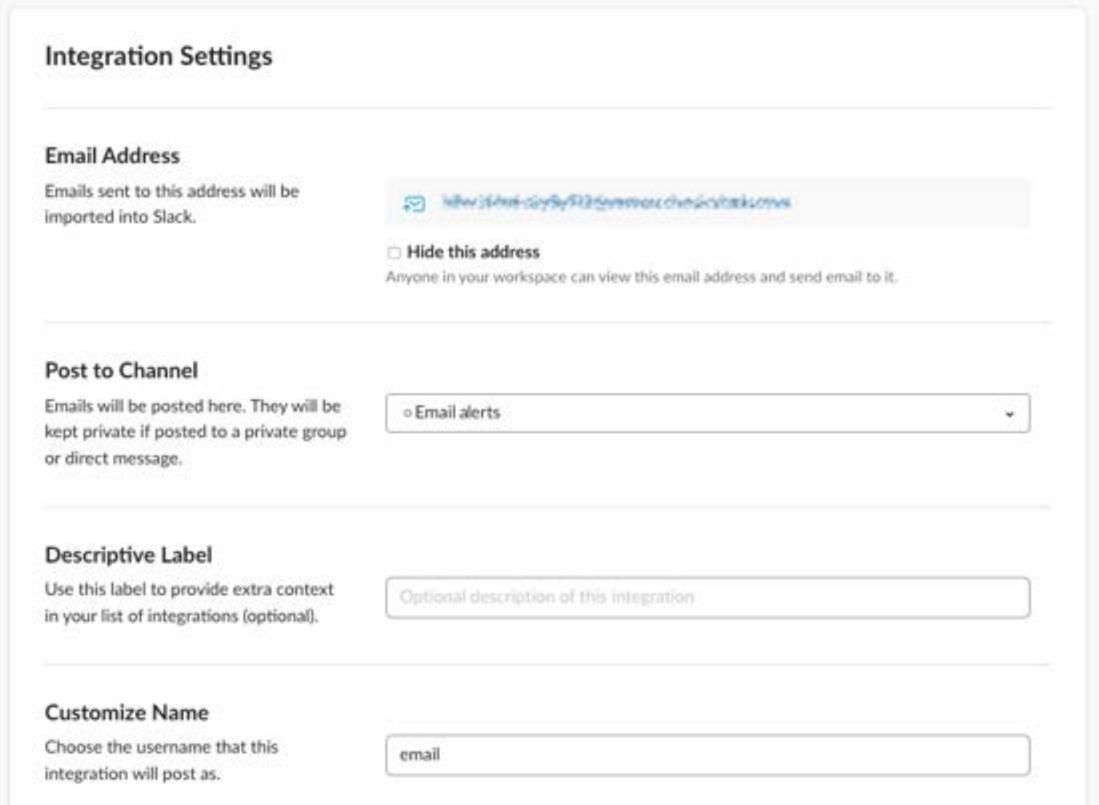
- The combined headers and body of an email cannot be larger than 1MB.
- When combined with attachments, an email cannot be larger than 30 MB.
- There is a maximum of 20 attachments per email.
- You can address each email to one integration at a time.

Post to Channel

Start by choosing a channel where email will be posted.

• Email alerts

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



Integration Settings

Email Address

Emails sent to this address will be imported into Slack.

[redacted]

□ 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.

○ Email alerts

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.**

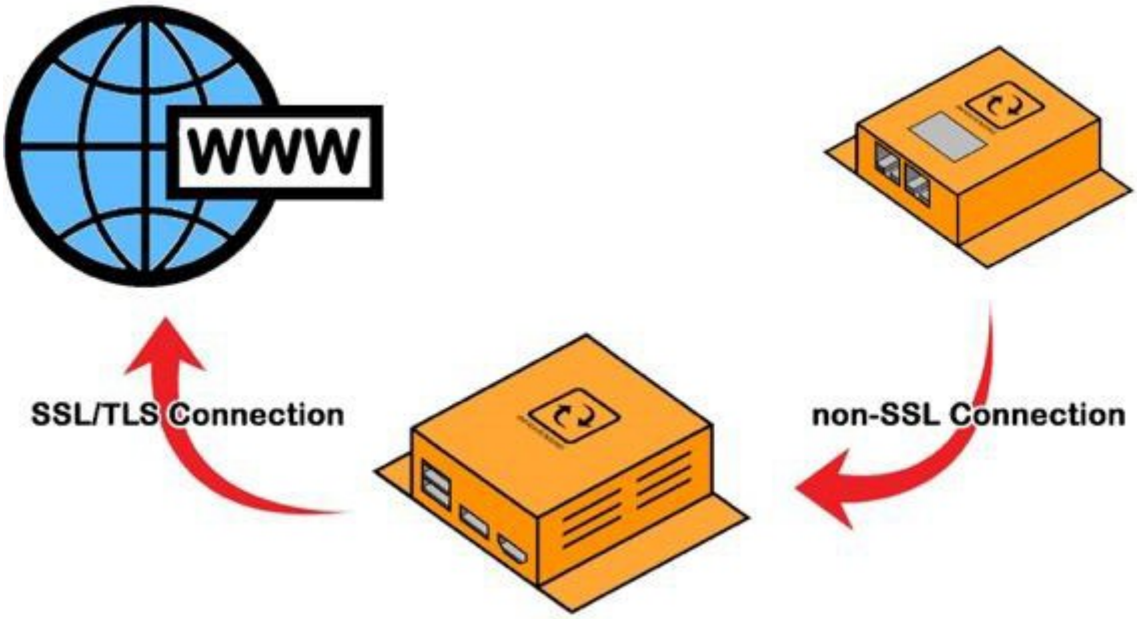
3.4 Tunneling an SSL connection

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.

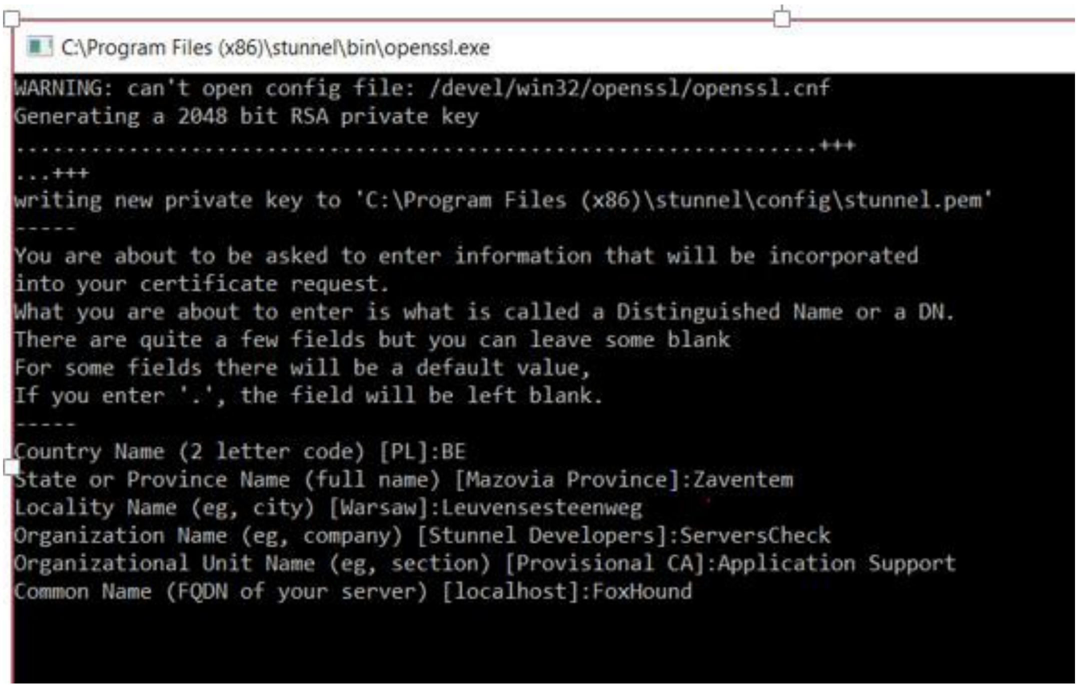
Network Diagram

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:

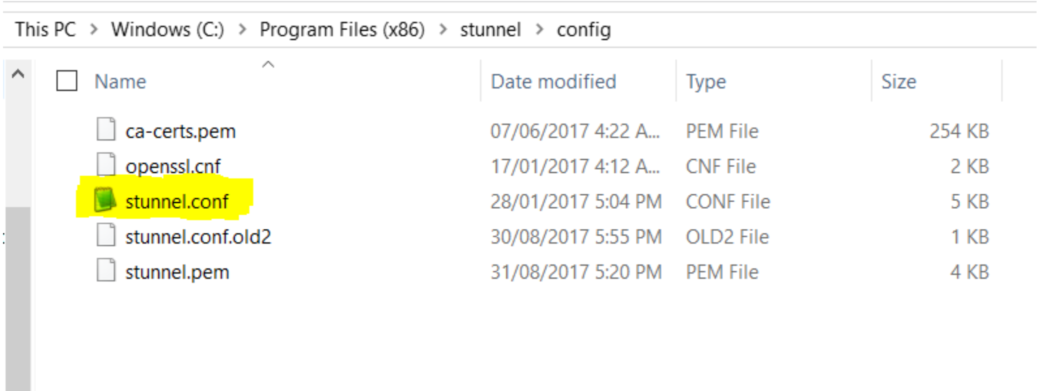
1. Download and Install the STunnel Software (can be downloaded from: http://www.stunnel.org/)
2. During the installation you will be prompt to input details, which will be needed to created certificates.



C:\Program Files (x86)\stunnel\bin\openssl.exe

```
WARNING: can't open config file: /devel/win32/openssl/openssl.cnf
Generating a 2048 bit RSA private key
...................................................................+++
...+++
writing new private key to 'C:\Program Files (x86)\stunnel\config\stunnel.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [PL]:BE
State or Province Name (full name) [Mazovia Province]:Zaventem
Locality Name (eg, city) [Warsaw]:Leuvensesteenweg
Organization Name (eg, company) [Stunnel Developers]:ServersCheck
Organizational Unit Name (eg, section) [Provisional CA]:Application Support
Common Name (FQDN of your server) [localhost]:FoxHound
```

3. Access the config folder as shown in the image below and open stunnel.conf using a text editor.
   Ex. Notepad, Notepad++



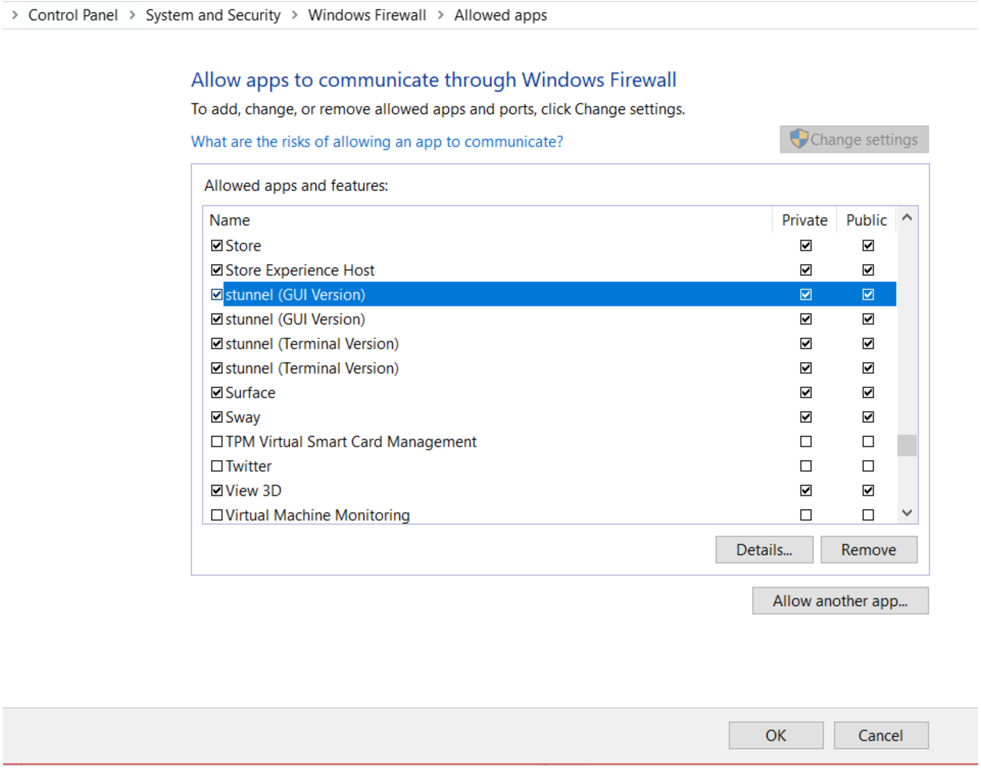
This PC > Windows (C:) > Program Files (x86) > stunnel > config

□ Name	Date modified	Type	Size
ca-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


› Control Panel › System and Security › Windows Firewall › Allowed apps
Change settings
Details...
Remove
Allow another app...
OK
Cancel

Allow apps to communicate through Windows Firewall

To add, change, or remove allowed apps and ports, click Change settings.

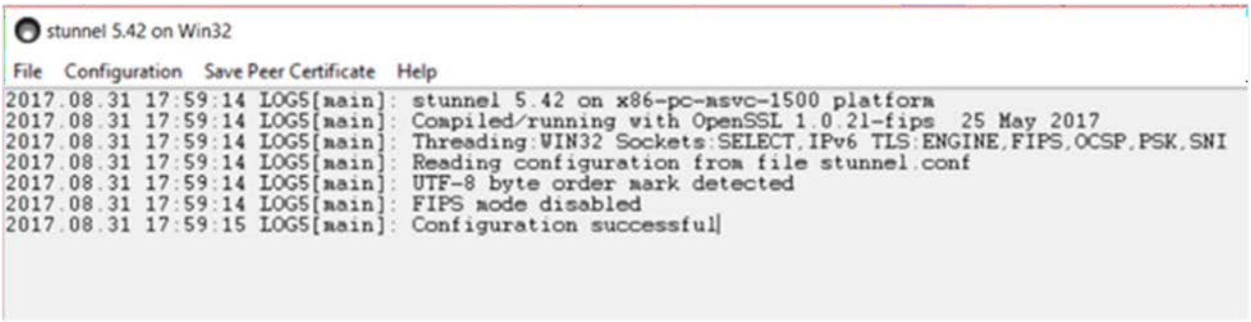
What are the risks of allowing an app to communicate?

Allowed apps and features:

Name	Private	Public
☑ Store	☑	☑
☑ Store Experience Host	☑	☑
☑ stunnel (GUI Version)	☑	☑
☑ stunnel (GUI Version)	☑	☑
☑ stunnel (Terminal Version)	☑	☑
☑ stunnel (Terminal Version)	☑	☑
☑ Surface	☑	☑
☑ Sway	☑	☑
☐ TPM Virtual Smart Card Management	☐	☐
☐ Twitter	☐	☐
☑ View 3D	☑	☑
☐ Virtual Machine Monitoring	☐	☐

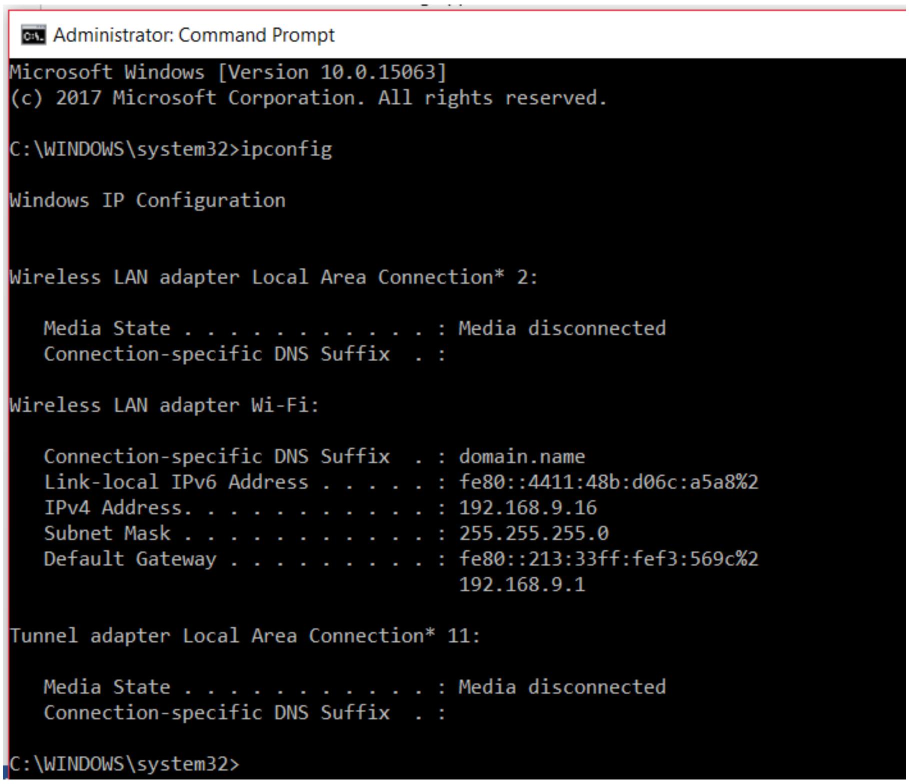
6. Click on the desktop icon of the STunnel. You can also see and choose options on the Icon created on the system tray.

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



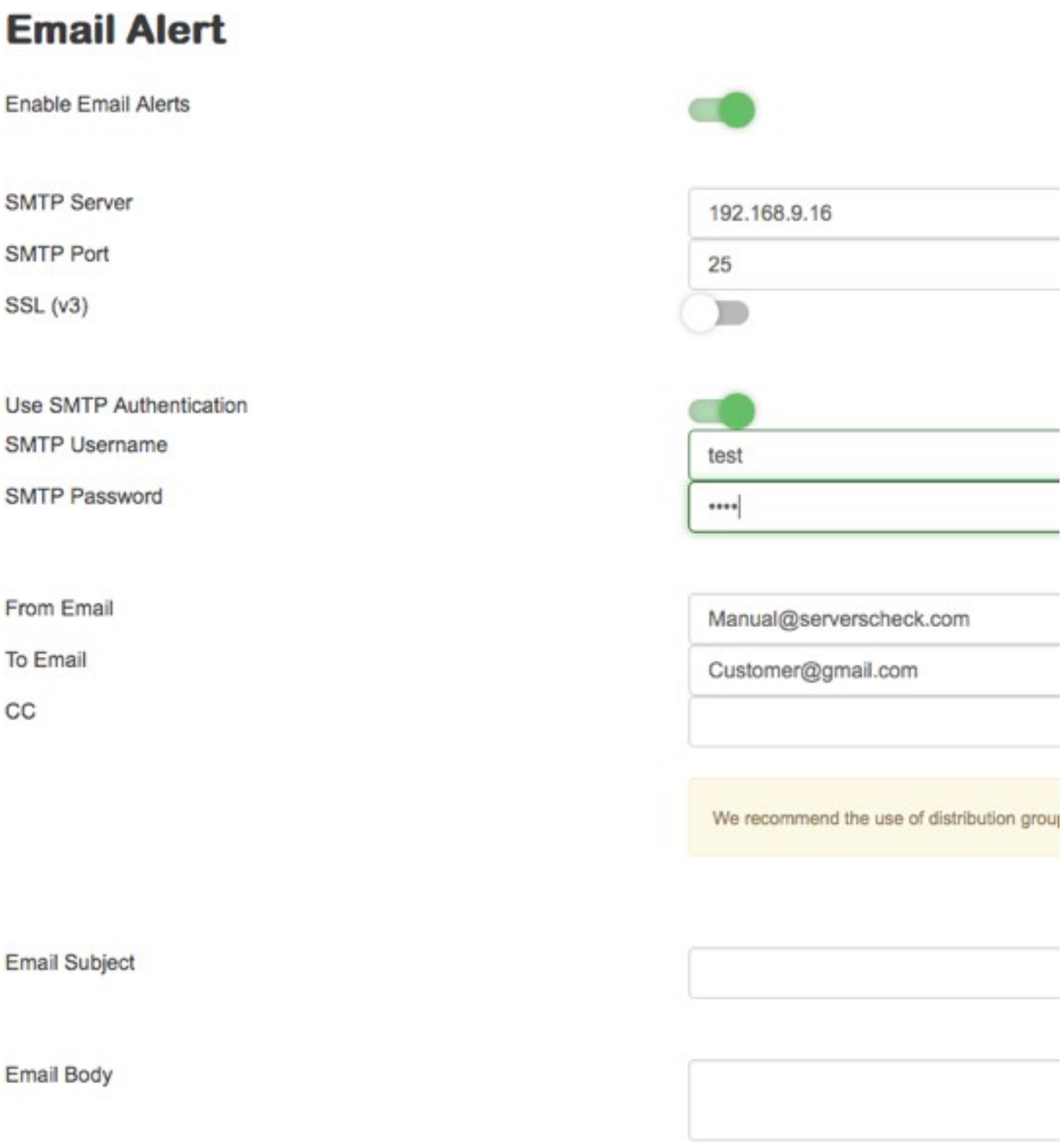
```
2017.08.31 17:59:14 LOG5[main]: stunnel 5.42 on x86-pc-msvc-1500 platform
2017.08.31 17:59:14 LOG5[main]: Compiled/running with OpenSSL 1.0.2l-fips  25 May 2017
2017.08.31 17:59:14 LOG5[main]: Threading:WIN32 Sockets:SELECT,IPv6 TLS:ENGINE,FIPS,OCSP,PSK,SNI
2017.08.31 17:59:14 LOG5[main]: Reading 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”)



```
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
CC	
	We recommend the use of distribution grou
Email Subject	
Email Body	

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

3.5 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).

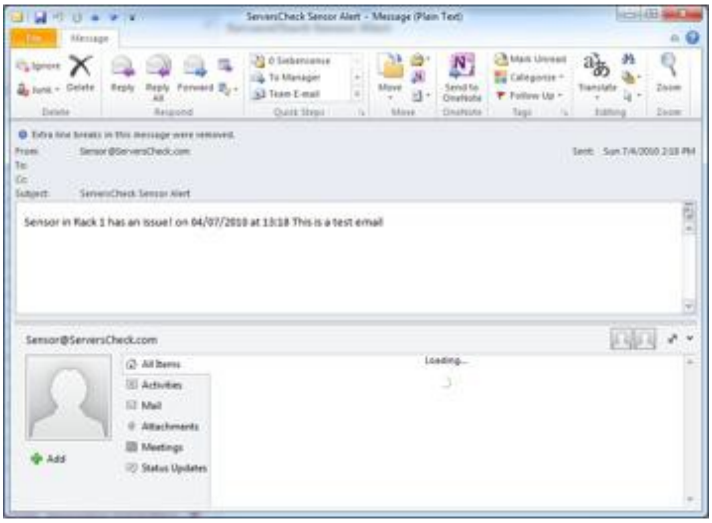
More information on http://www.authsmtp.com

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.



ServersCheck Sensor Alert - Message (Plain Text)

Extra line breaks in this message were removed.

From: Sensor@ServersCheck.com

Sent: Sun 7/4/2010 2:18 PM

To:

Cc:

Subject: ServersCheck Sensor Alert

Sensor in Rack 1 has an issue! on 04/07/2010 at 13:18 This is a test email

Sensor@ServersCheck.com

3.6 Beta TLS/STARTTLS firmware (Beta 8.x)

The Beta firmware allows user to send emails that require TLS/STARTTLS protocol. It also supports HTTPS and custom certificates. You can download the BETA firmware here

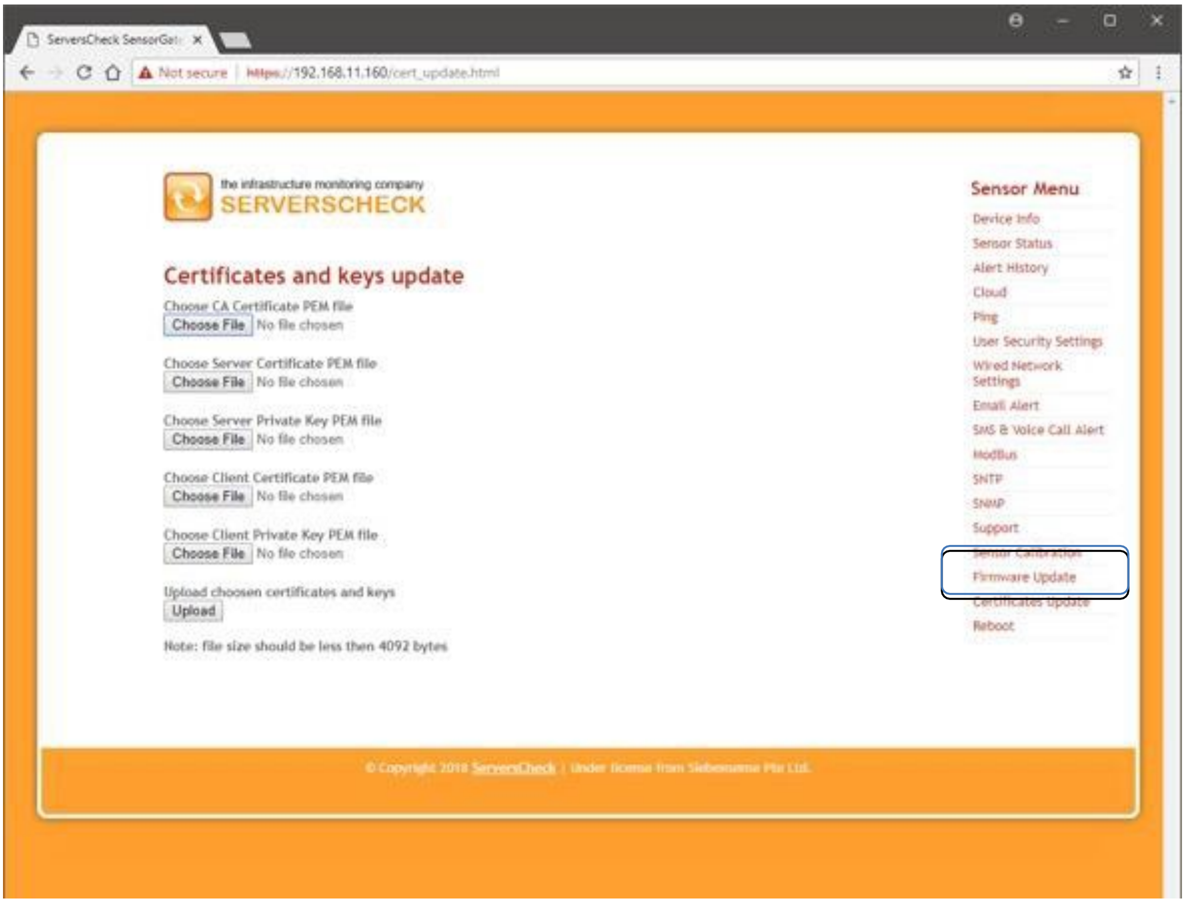
DOWNLOAD BETA FIRMWARE

3.7 HTTPS and custom certificates (BETA Firmware 8.x)

To access the gateway with the BETA firmware instead of http://192.x.x.x it is now by default in HTTPS https://192.x.x.x

It takes a couple of seconds more to load than the regular firmware due to the added security.

The image below shows the option where you upload your custom certificate.



https://192.168.11.160/cert_update.html

Certificates and keys update

Choose CA Certificate PEM file
Choose File No file chosen

Choose Server Certificate PEM file
Choose File No file chosen

Choose Server Private Key PEM file
Choose File No file chosen

Choose Client Certificate PEM file
Choose File No file chosen

Choose Client Private Key PEM file
Choose File No file chosen

Upload choosen certificates and keys
Upload

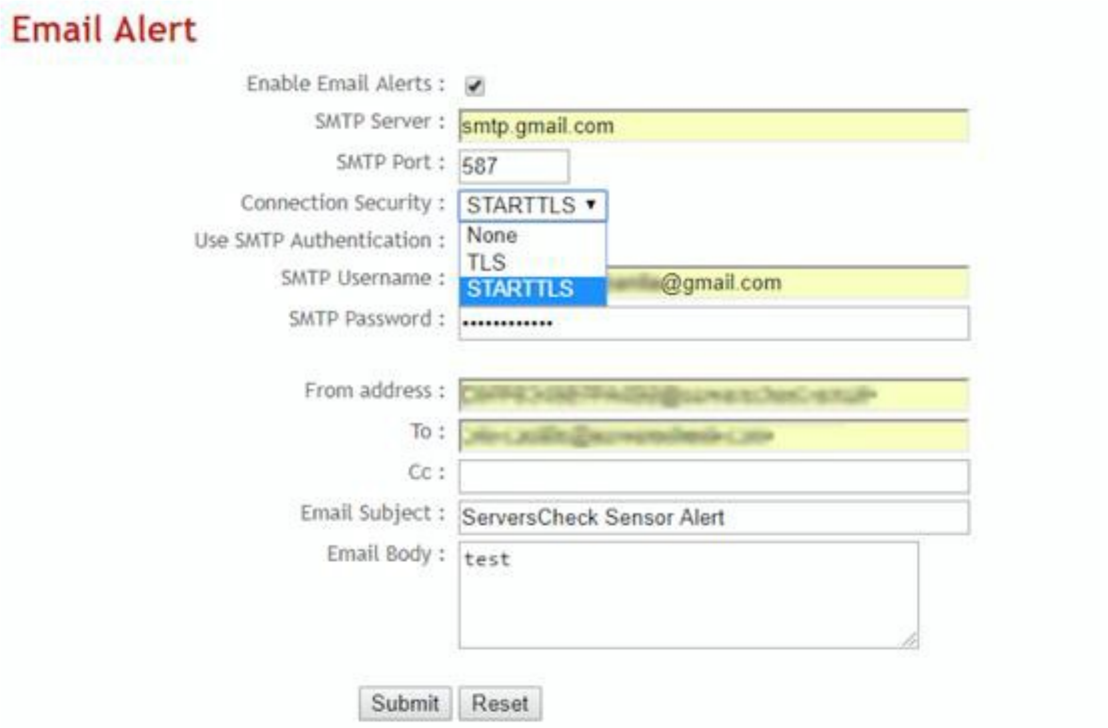
Note: file size should be less then 4092 bytes

© Copyright 2018 ServersCheck | Under license from Siebennama Pte Ltd.

3.8 TLS / STARTTLS support

The email option will look different than the regular email option we have on our official firmware.

A new interface where you can choose between TLS or STARTTLS has been implemented similar to the ADDON-LTE.



Email Alert

Enable Email Alerts : ☑
SMTP Server : smtp.gmail.com
SMTP Port : 587
Connection Security : STARTTLS ▾
Use SMTP Authentication :
SMTP Username : [redacted]@gmail.com
SMTP Password : ••••••••••••

From address : [redacted]
To : [redacted]
Cc :
Email Subject : ServersCheck Sensor Alert
Email Body : test

Configuration examples

GMAIL TLS

SMTP Server: smtp.gmail.com
SMTP port: 465
Connection Security: TLS
Username: “your email address” @gmail.com
Password: the password of your email

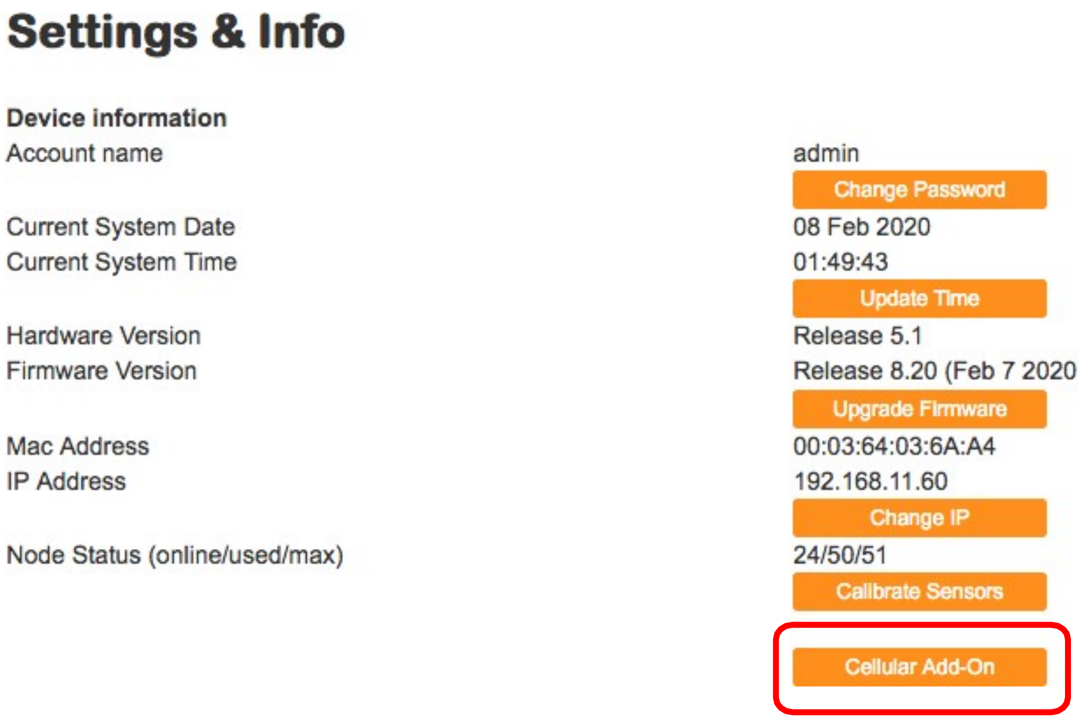
GMAIL STARTTLS

SMTP Server: smtp.gmail.com
SMTP port: 587
Connection Security: STARTTLS
Username: “your email address” @gmail.com
Password: the password of your email

Note: as the Firmware is still in BETA some SMTP servers might not work. The firmware was tested working on GMAIL, YAHOO and OUTLOOK. The firmware is also not compatible with Mac OS Sierra but can be accessed using Mac OS High Sierra

3.9 SMS alerting from Base Unit

3.9.1 SMS alerts via ADDON-LTE



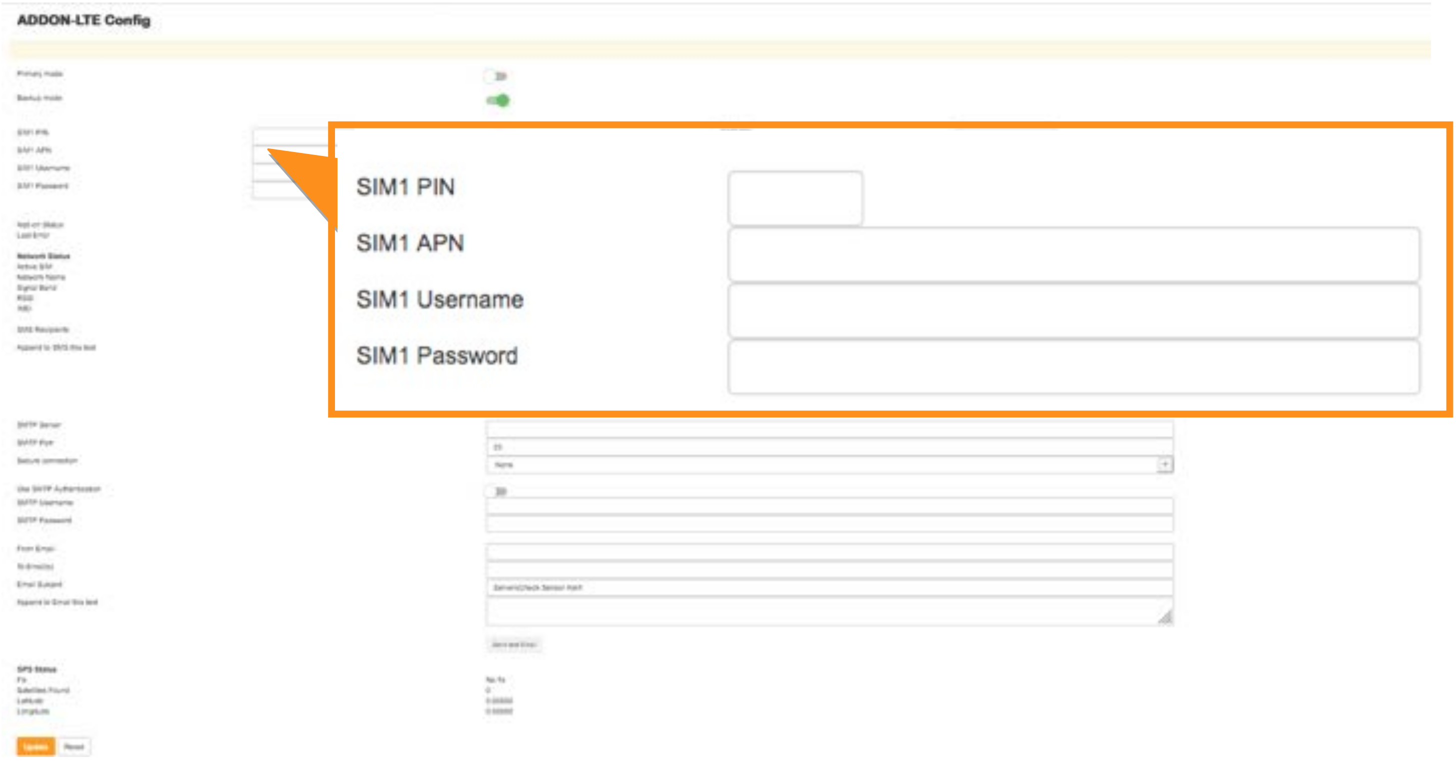
Settings & Info

Device information

Account name	admin Change Password
Current System Date	08 Feb 2020
Current System Time	01:49:43 Update Time
Hardware Version	Release 5.1
Firmware Version	Release 8.20 (Feb 7 2020) Upgrade Firmware
Mac Address	00:03:64:03:6A:A4
IP Address	192.168.11.60 Change IP
Node Status (online/used/max)	24/50/51 Calibrate Sensors
	Cellular Add-On

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

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



ADDON-LTE Config

Primary mode
Backup mode

SIM1 PIN
SIM1 APN
SIM1 Username
SIM1 Password

Add-on Status
Last Error

Network Status
Active SIM
Network Name
Signal Band
RSSI
IMEI

SMS Recipients
Append to SMS this text

SMTP Server
SMTP Port — 25
Secure connection — None

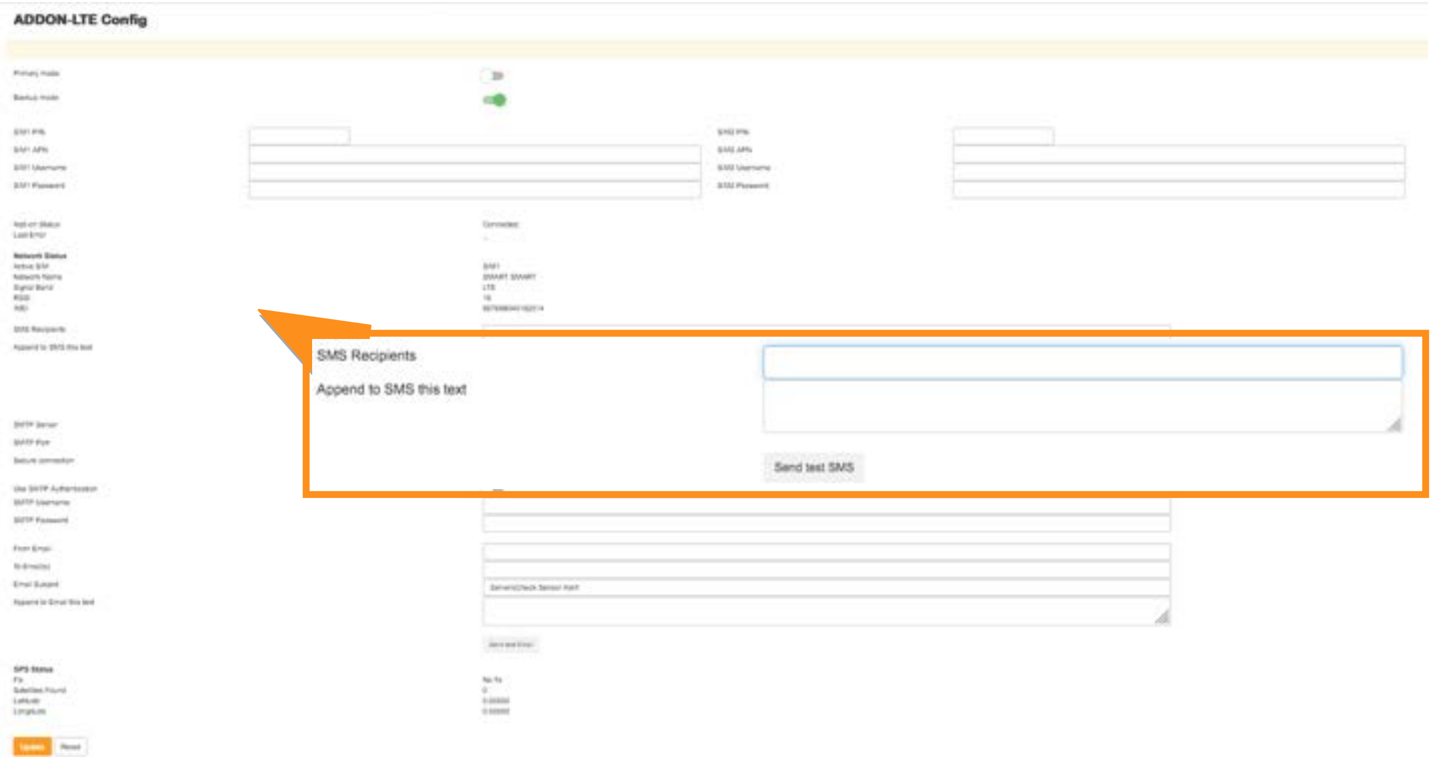
Use SMTP Authentication
SMTP Username
SMTP Password

From Email
To Email(s)
Email Subject
Append to Email this text

GPS Status
Fix — No fix
Satellites Found — 0
Latitude — 0.00000
Longitude — 0.00000

Update Reset

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

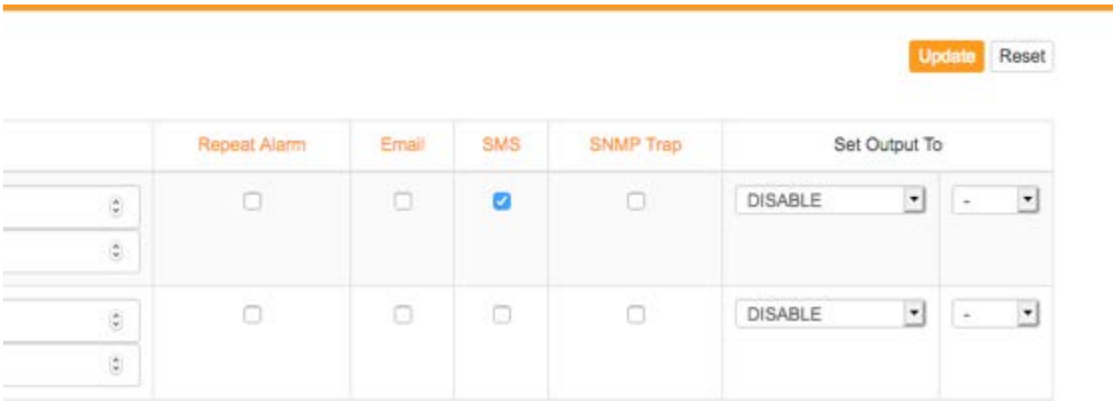


ADDON-LTE Config

SMS Recipients

Append to SMS this text

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



	Repeat Alarm	Email	SMS	SNMP Trap	Set Output To	
	☐	☐	☑	☐	DISABLE	-
	☐	☐	☐	☐	DISABLE	-

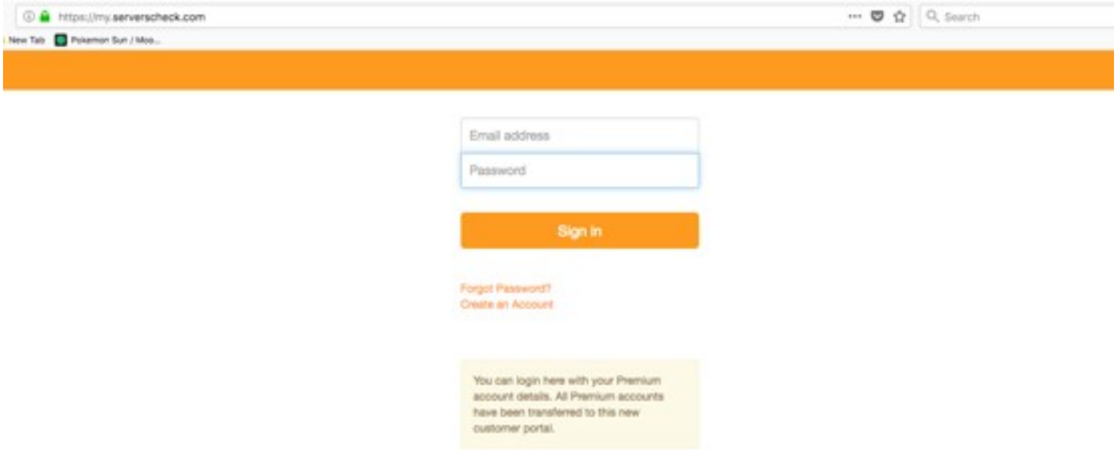
Make sure that the SMS checkbox is ticked to receive alerts via SMS for the sensors you are monitoring.

3.9.2 SMS alerts via my.infrasensing premium credits

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

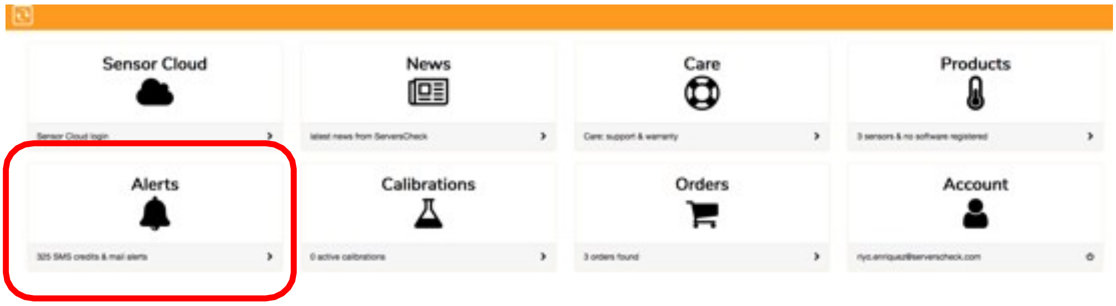
For SMS alerting, SMS messages are sent by InfraSensing's SMS Gateway. Base Units make a connection over TCP/IP with the SMS Gateway servers for delivering SMS messages.

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



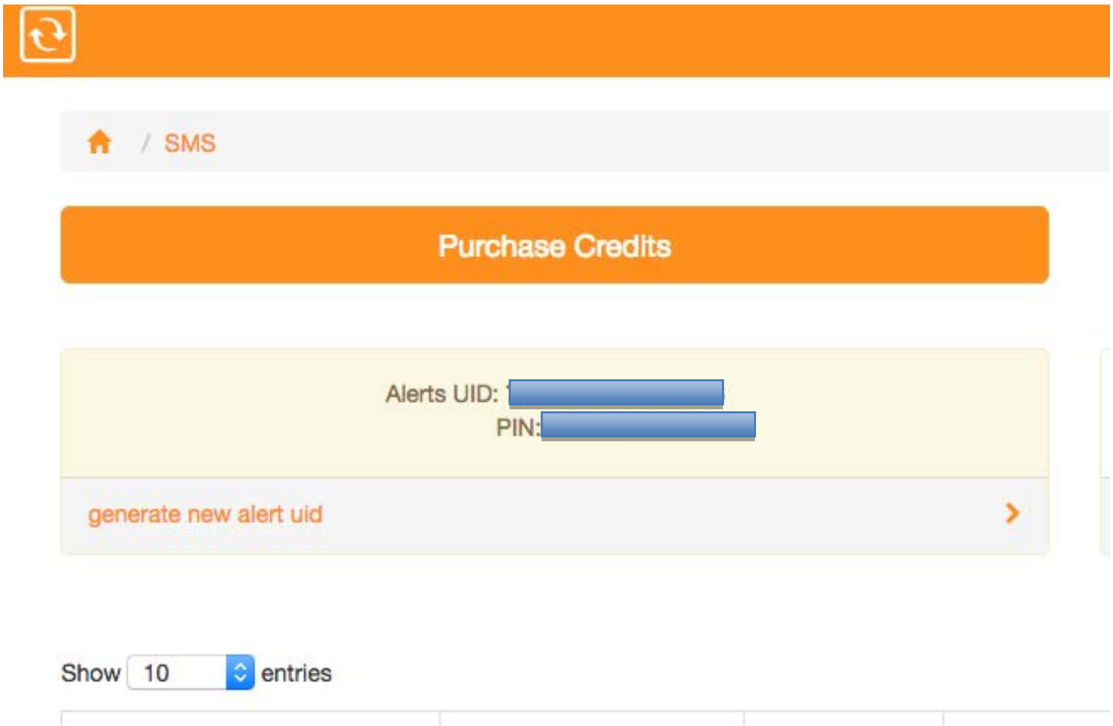
You can login here with your Premium account details. All Premium accounts have been transferred to this new customer portal.

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



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.

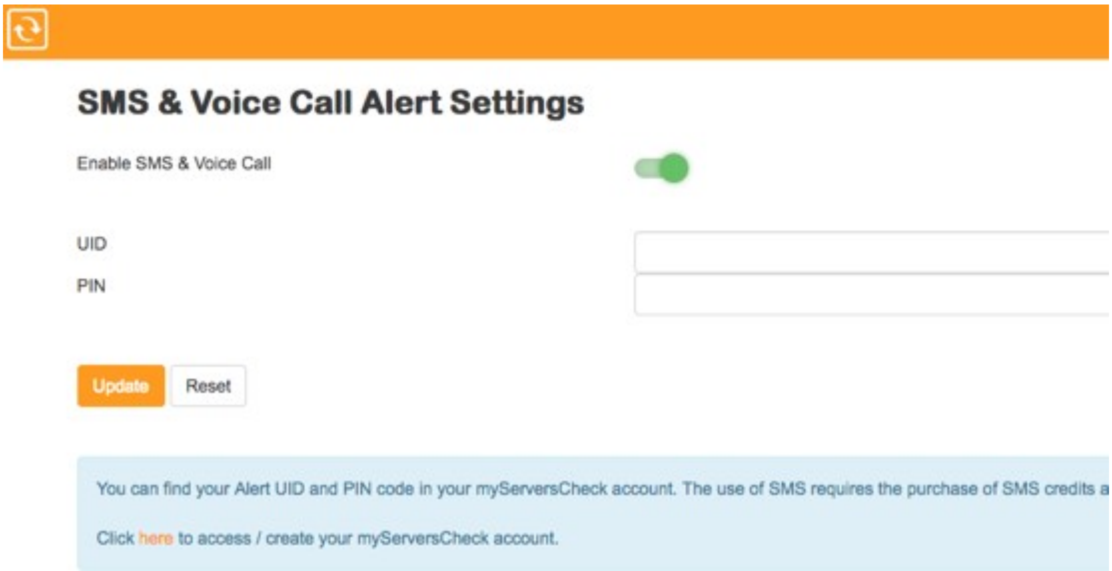


Alerts UID: [redacted]
PIN: [redacted]

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

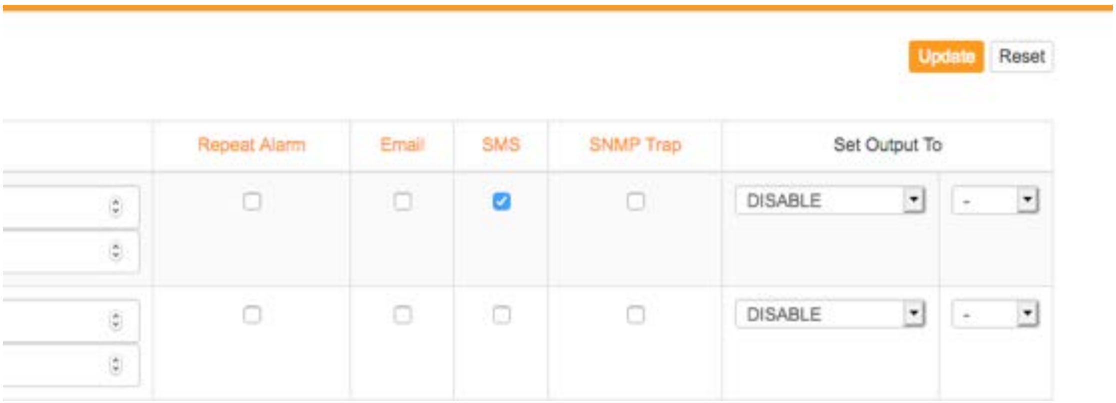

SMS & Voice Call Alert Settings

You can find your Alert UID and PIN code in your myServersCheck account. The use of SMS requires the purchase of SMS credits a

Click here to access / create your myServersCheck account.

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.



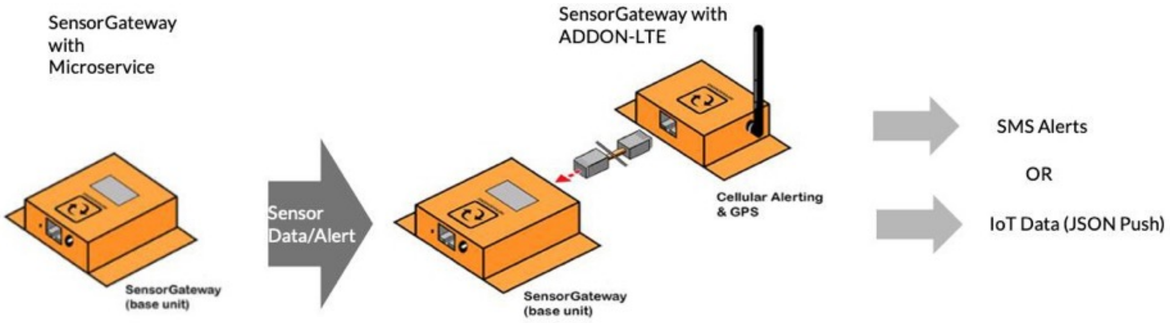
	Repeat Alarm	Email	SMS	SNMP Trap	Set Output To	
	□	□	☑	□	DISABLE	-
	□	□	□	□	DISABLE	-

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

3.9.3 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



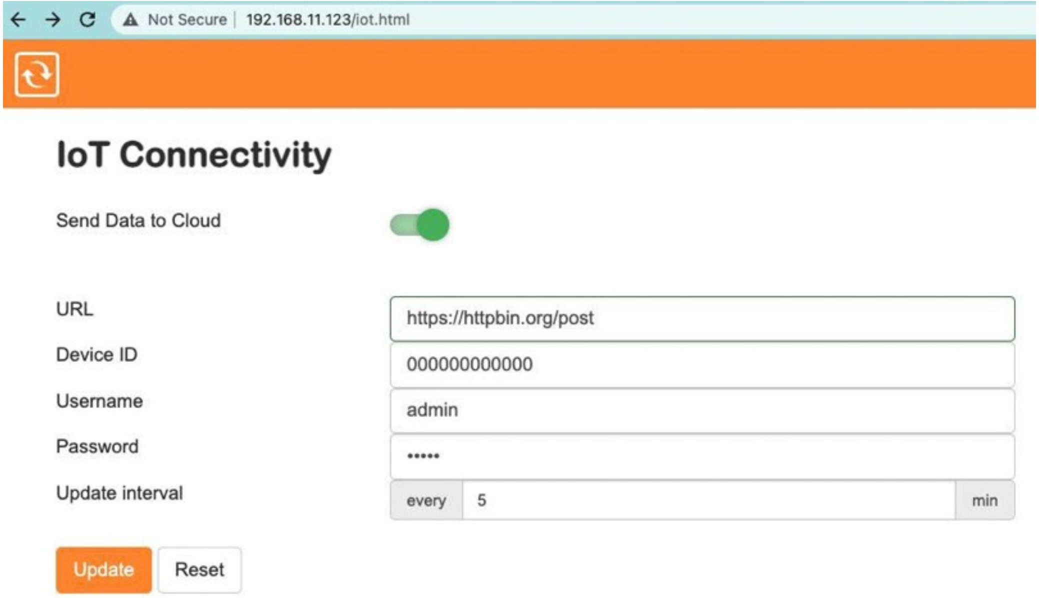
SensorGateway with Microservice
SensorGateway (base unit)
Sensor Data/Alert
SensorGateway with ADDON-LTE
Cellular Alerting & GPS
SensorGateway (base unit)
SMS Alerts
OR
IoT Data (JSON Push)

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:



Not Secure | 192.168.11.123/iot.html

IoT Connectivity

Send Data to Cloud

URL	https://httpbin.org/post
Device ID	000000000000
Username	admin
Password	•••••
Update interval	every 5 min

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

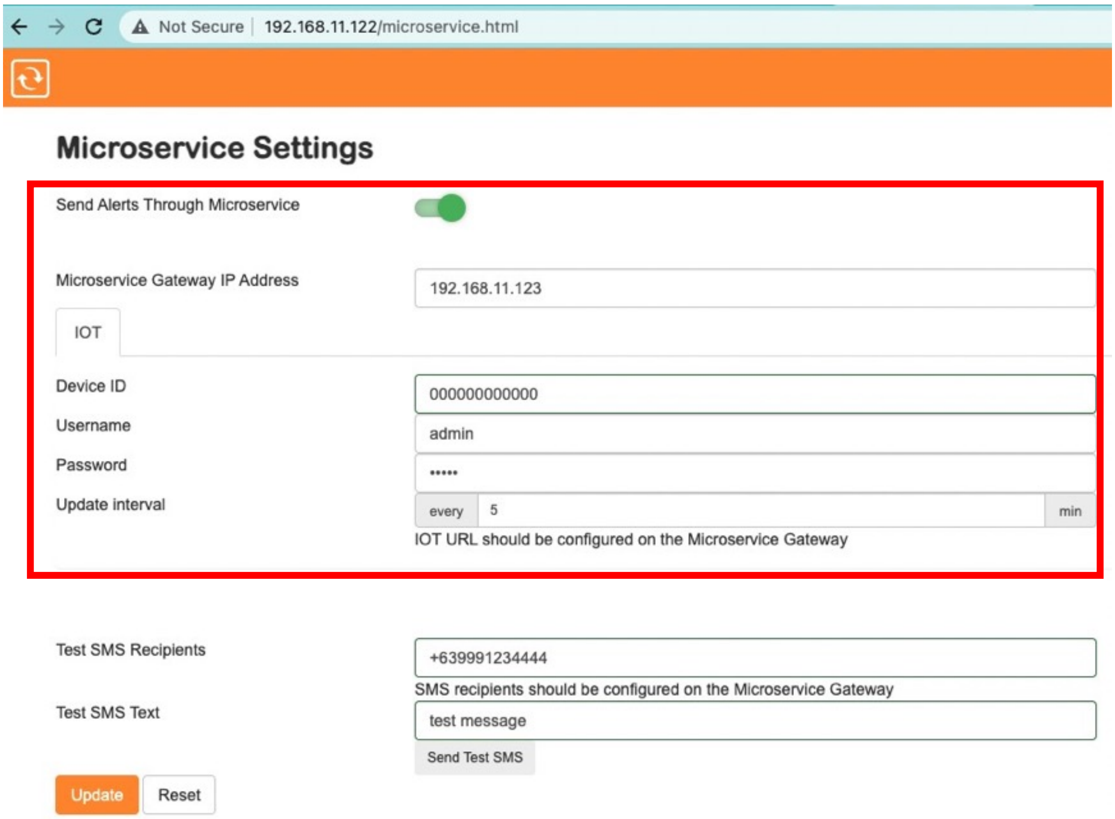
4. After the details are entered, click **Update**.

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 Settingsbutton 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: 000000000000

Username: admin

Password: •••••

Update interval: every 5 min

IOT URL should be configured on the Microservice Gateway

Test SMS Recipients: +639991234444

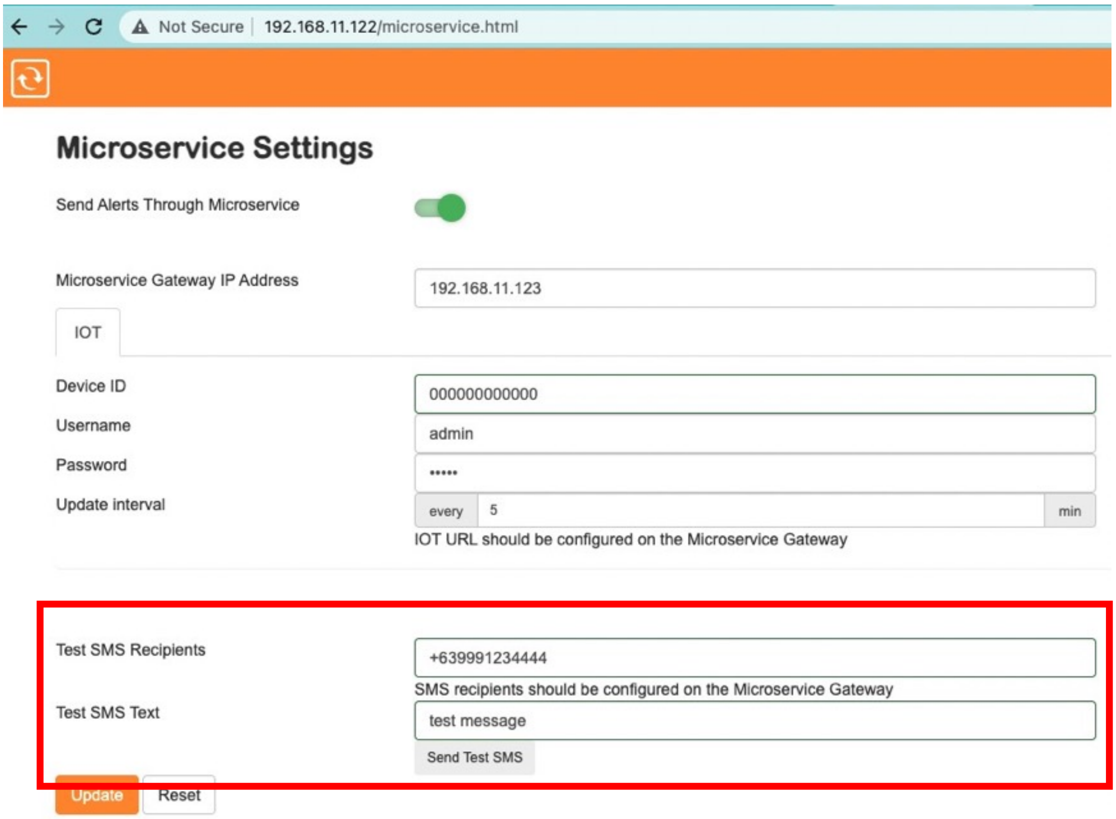
SMS recipients should be configured on the Microservice Gateway

Test SMS Text: test message

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**.

Sending Test SMS for Microservice



Not Secure | 192.168.11.122/microservice.html

Microservice Settings

Send Alerts Through Microservice: on

Microservice Gateway IP Address: 192.168.11.123

IOT

Device ID: 000000000000

Username: admin

Password: •••••

Update interval: every 5 min

IOT URL should be configured on the Microservice Gateway

Test SMS Recipients: +639991234444

SMS recipients should be configured on the Microservice Gateway

Test SMS Text: test message

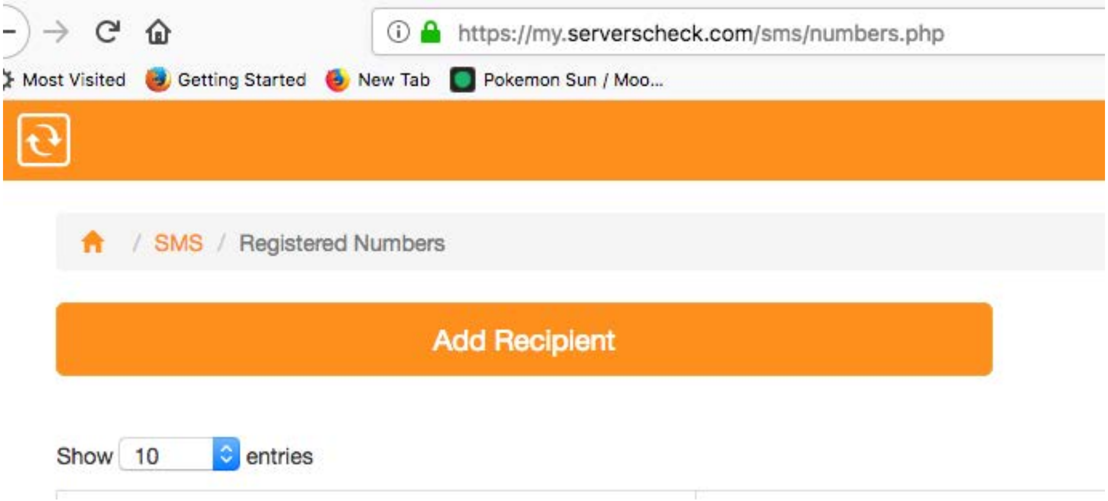
1. On the Microservice Settings, fill in the mobile numbers for the Test SMS Recipients.
2. Input the Test SMS Text that the recipients should receive.
3. Click **Send Text SMS**.

3.10 Voice call alerts

Aside from SMS messages, InfraSensing also offers voice calls as an alert by using text-to-speech 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.

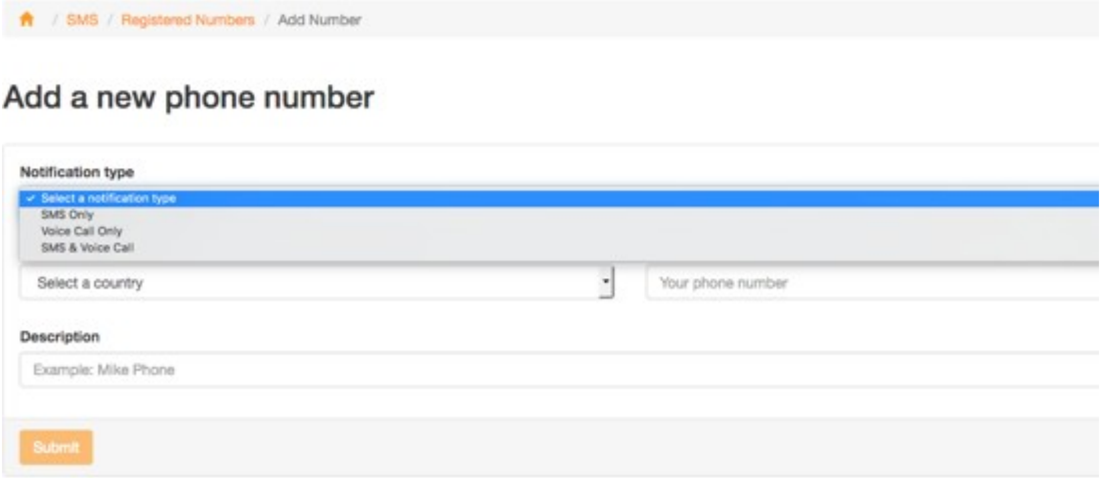


/ SMS / Registered Numbers

Add Recipient

Show 10 entries

Fill in the required fields



/ SMS / Registered Numbers / Add Number

Add a new phone number

Notification type

- ✓ Select a notification type
- SMS Only
- Voice Call Only
- SMS & Voice Call

Select a country

Your phone number

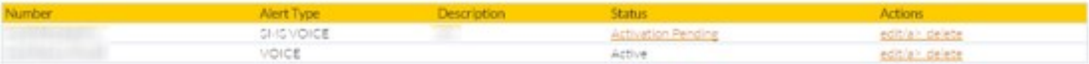
Description

Example: Mike Phone

Submit

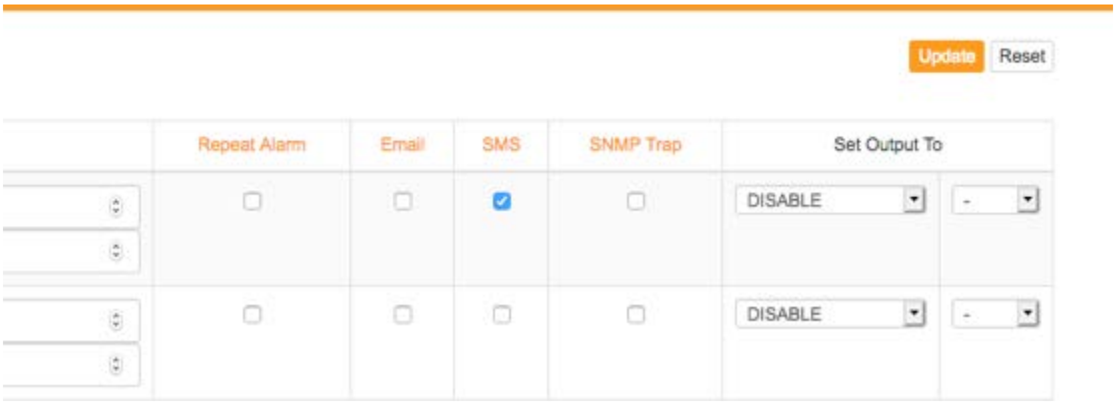
Then select “Voice” or “SMS and Voice”

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
[redacted]	SMS VOICE	[redacted]	Activation Pending	edit/a> delete
[redacted]	VOICE		Active	edit/a> 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.



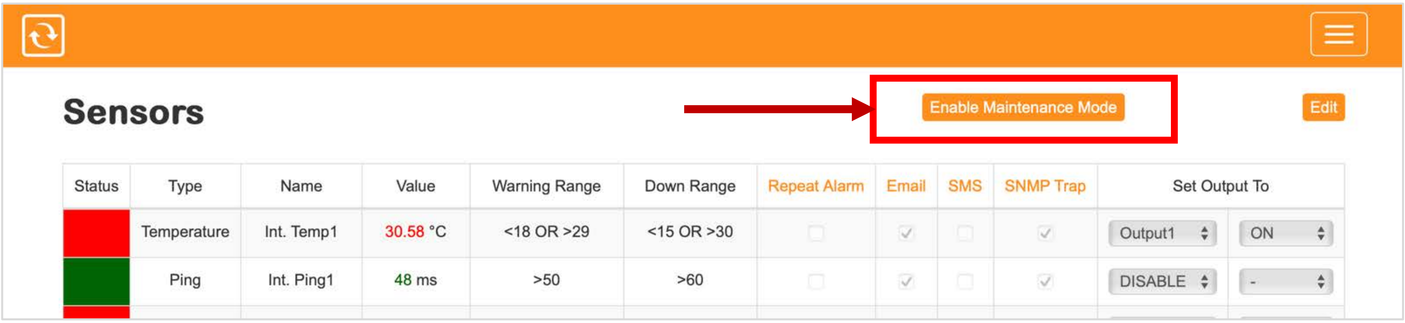
	Repeat Alarm	Email	SMS	SNMP Trap	Set Output To	
	□	□	☑	□	DISABLE	-
	□	□	□	□	DISABLE	-

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.

3.11 Maintenance Mode

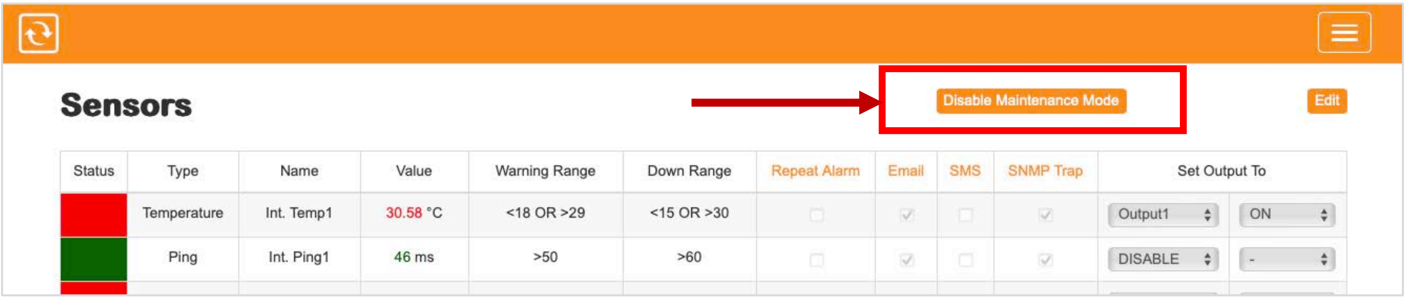
Maintenance Mode is one of the newest features that can be found in the latest firmware version 9.1.

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.



Status	Type	Name	Value	Warning Range	Down Range	Repeat Alarm	Email	SMS	SNMP Trap	Set Output To	
🟥	Temperature	Int. Temp1	30.58 °C	<18 OR >29	<15 OR >30	□	☑	□	☑	Output1	ON
🟩	Ping	Int. Ping1	48 ms	>50	>60	□	☑	□	☑	DISABLE	-

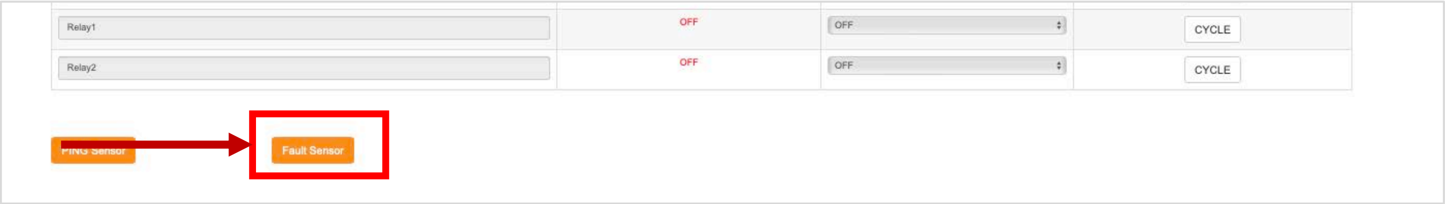
Once you click "Enable Maintenance Mode," it will change to "Disable Maintenance Mode." To deactivate it, simply click again.



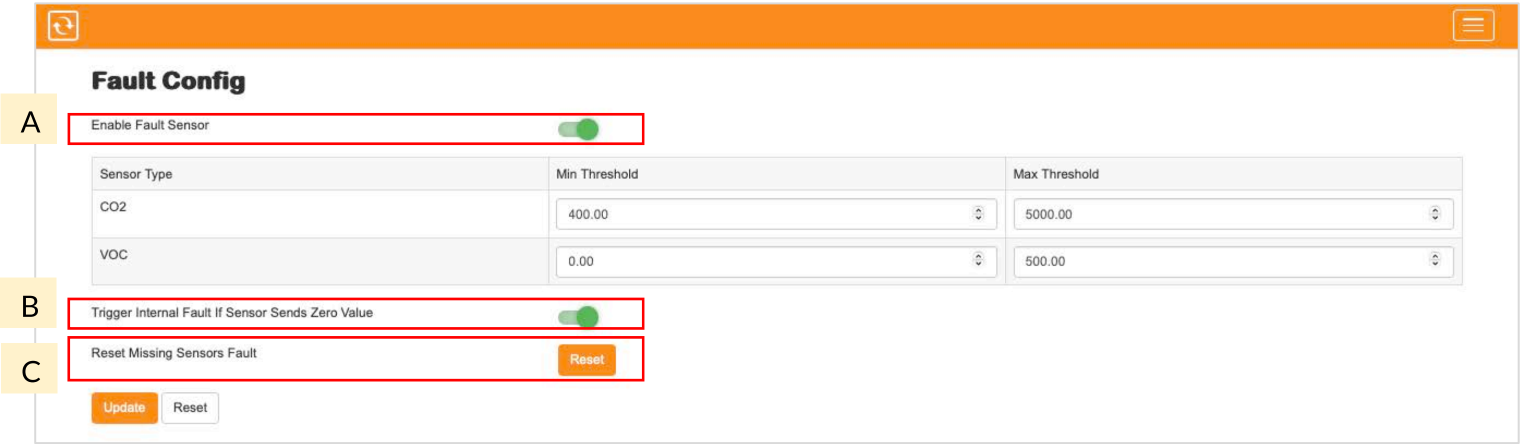
Status	Type	Name	Value	Warning Range	Down Range	Repeat Alarm	Email	SMS	SNMP Trap	Set Output To	
🟥	Temperature	Int. Temp1	30.58 °C	<18 OR >29	<15 OR >30	□	☑	□	☑	Output1	ON
🟩	Ping	Int. Ping1	46 ms	>50	>60	□	☑	□	☑	DISABLE	-

3.12 **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



Fault Config

Enable Fault Sensor ●

Sensor Type	Min Threshold	Max Threshold
CO2	400.00	5000.00
VOC	0.00	500.00

Trigger Internal Fault If Sensor Sends Zero Value ●

Reset Missing Sensors Fault

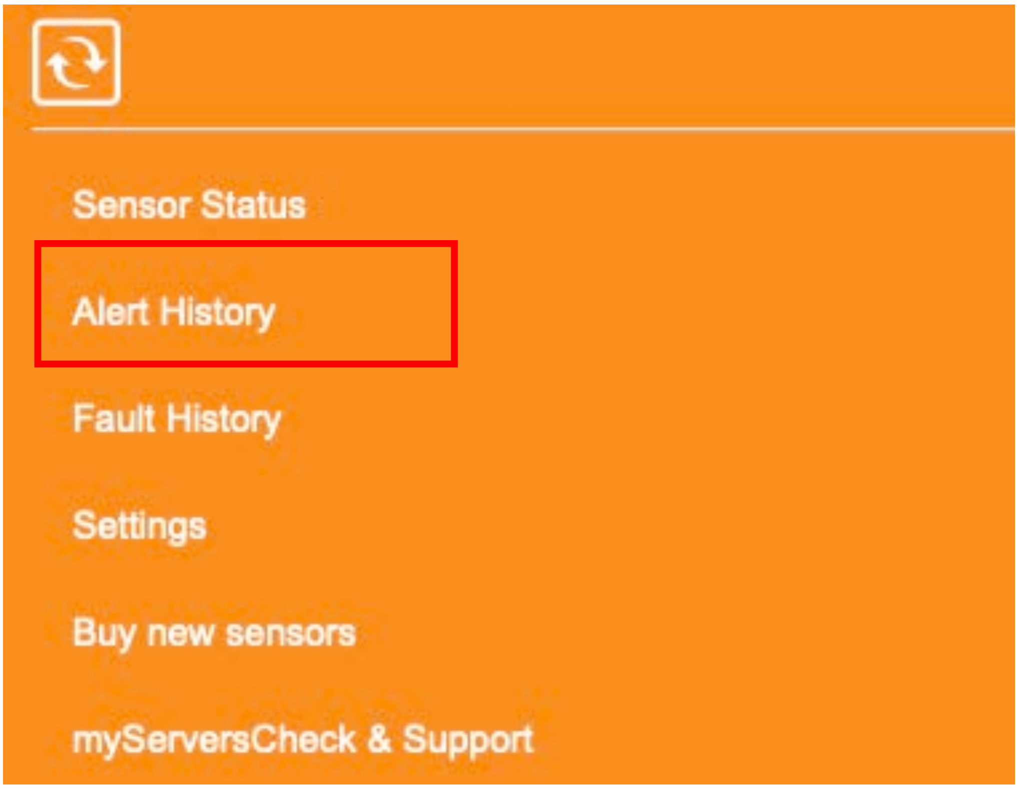
A. Enable Fault Sensor – When this feature is enabled, it will send out an alert whenever a sensor gets disconnected.

B. Trigger internal Fault if Sensor Sends Zero Value – Enabling this feature will generate an alert whenever a sensor transmit a zero value.

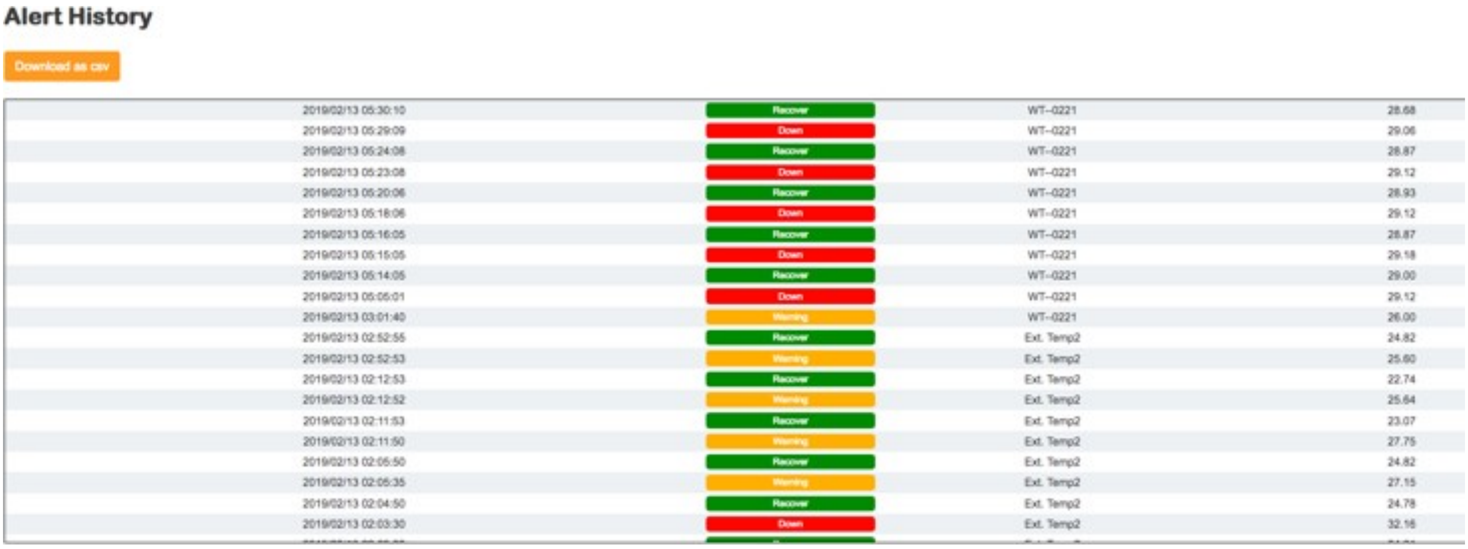
C. Reset Missing Sensors Fault – This option enables you to reset Fault alerts triggered by missing sensors.

4 History

4.1 Alert history



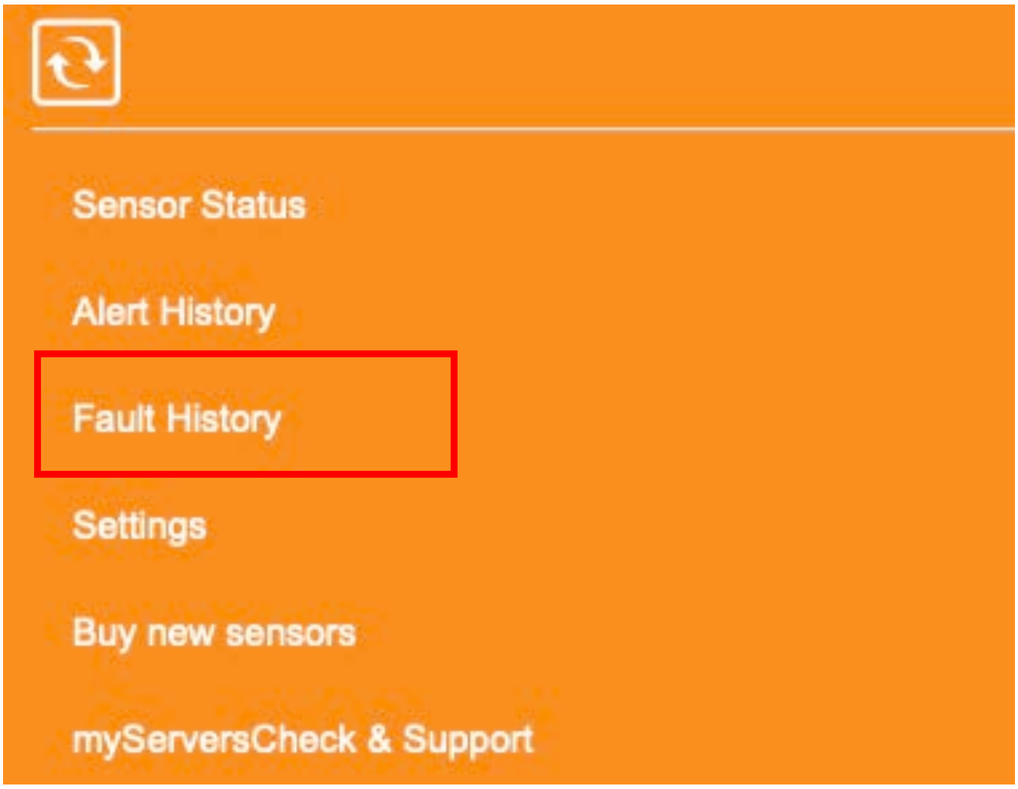
Each time a threshold is hit, an entry is automatically recorded on the log. And as seen on the screenshot, recovery alerts are also included. The Base Unit is able to store up to 2048 entries and are downloadable in CSV format. On column F of the CSV file, the following legend is used for the alerts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



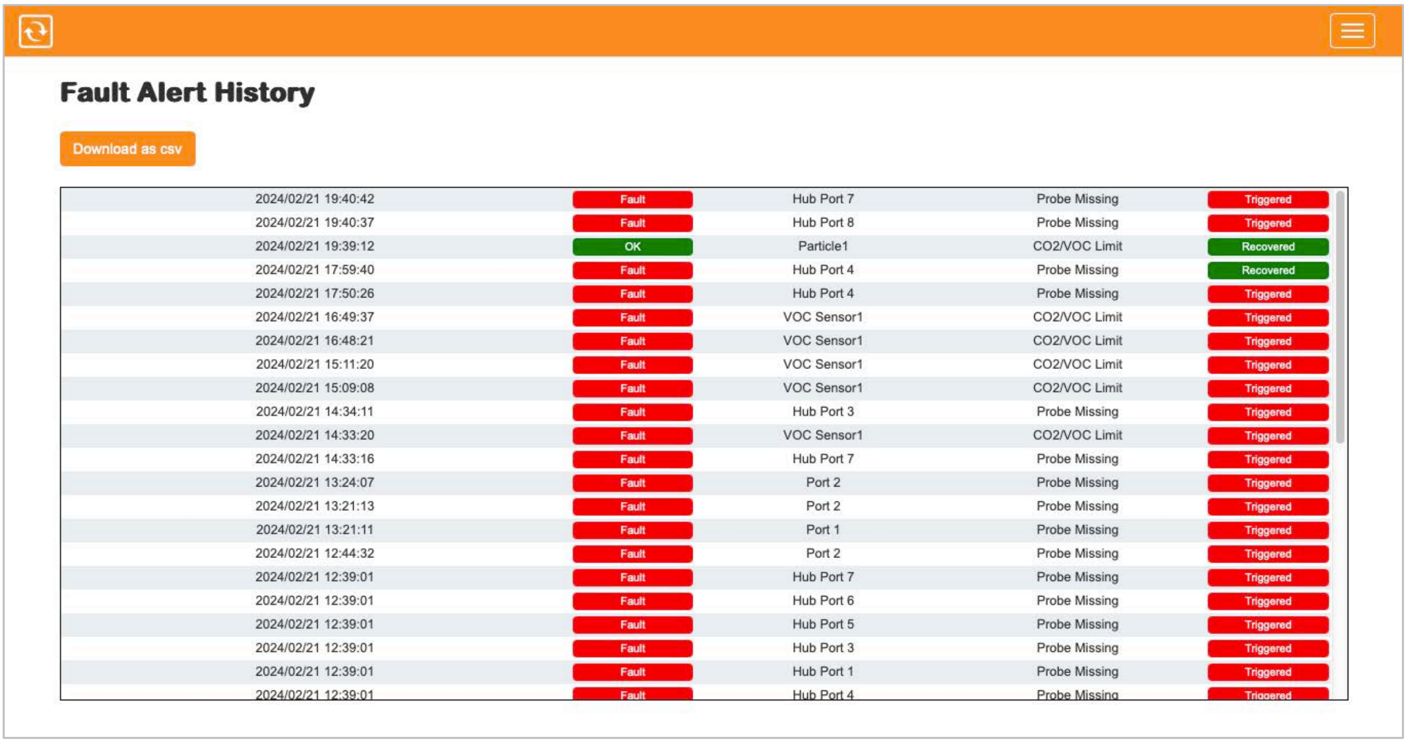
Alert History

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	Recover	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	Warning	WT--0221	26.00
2019/02/13 02:52:55	Recover	Ext. Temp2	24.82
2019/02/13 02:52:53	Warning	Ext. Temp2	25.60
2019/02/13 02:12:53	Recover	Ext. Temp2	22.74
2019/02/13 02:12:52	Warning	Ext. Temp2	25.64
2019/02/13 02:11:53	Recover	Ext. Temp2	23.07
2019/02/13 02:11:50	Warning	Ext. Temp2	27.75
2019/02/13 02:05:50	Recover	Ext. Temp2	24.82
2019/02/13 02:05:35	Warning	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

4.2 Fault history



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



Fault Alert History

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	OK	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

5 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

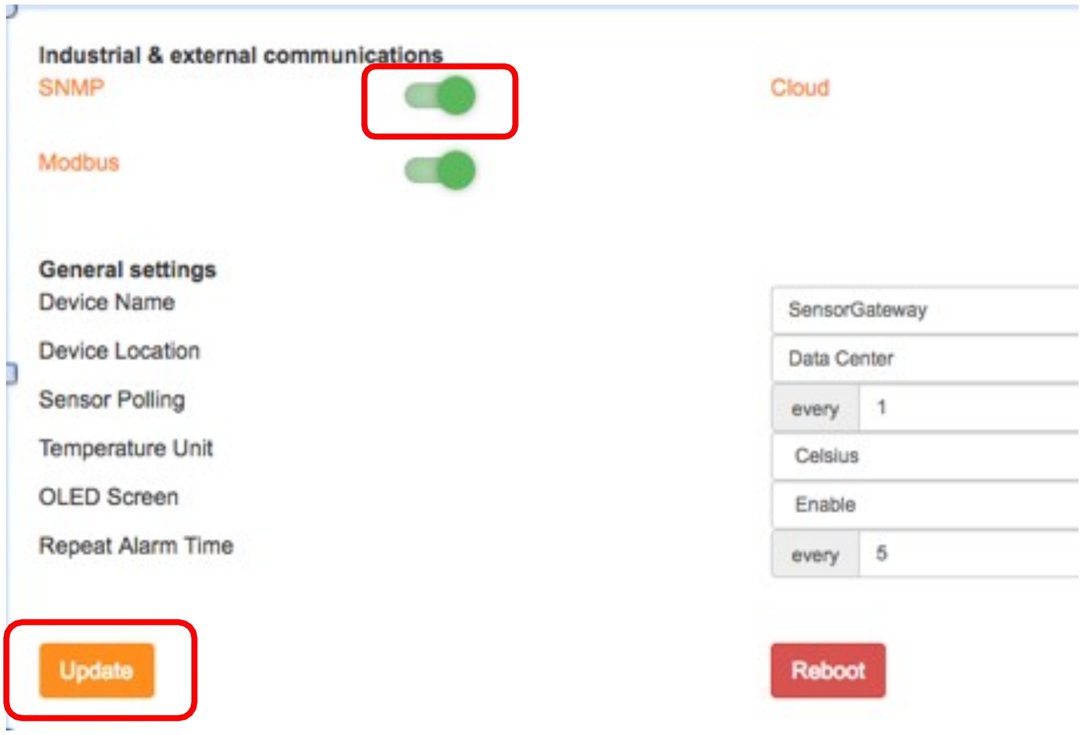
To illustrate SNMP, we will use the free (for personal use) SNMP Browser from iReasoning which is available from the following URL:
http://ireasoning.com/mibbrowser.shtml

5.1 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:
http://downloads.infrasensing.com/sensors/Base Unit.mib

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.*



Industrial & external communications

SNMP ●

Modbus ●

Cloud

General settings

Device Name: SensorGateway

Device Location: Data Center

Sensor Polling: every 1

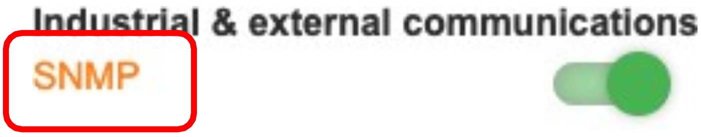
Temperature Unit: Celsius

OLED Screen: Enable

Repeat Alarm Time: every 5

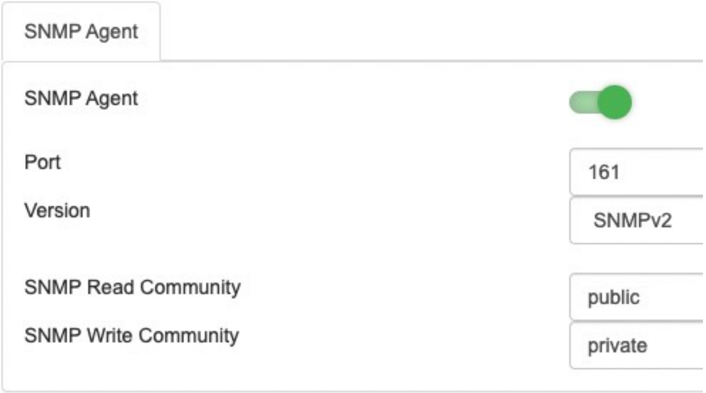
Community string is limited to 16 characters.

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

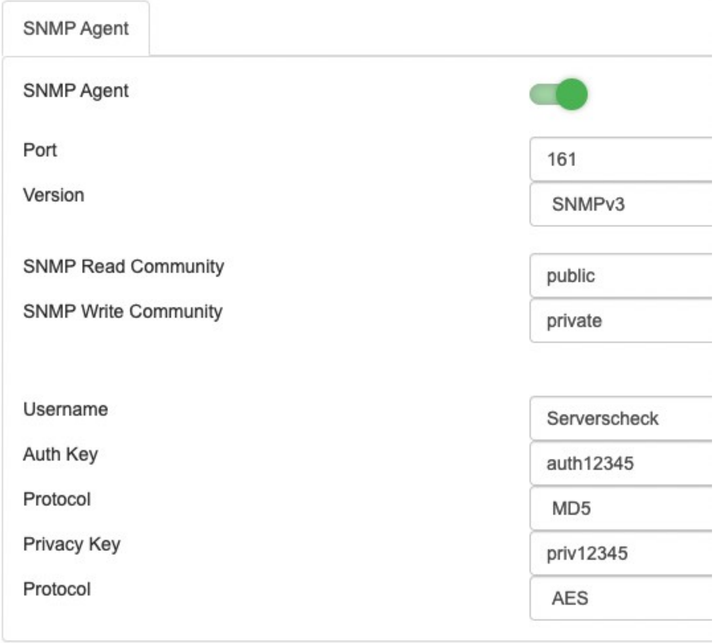
Port 161

Version SNMPv2

SNMP Read Community public

SNMP Write Community private

SNMP settings for v2



SNMP Agent

SNMP Agent

Port 161

Version SNMPv3

SNMP Read Community public

SNMP Write Community private

Username Serverscheck

Auth Key auth12345

Protocol MD5

Privacy Key priv12345

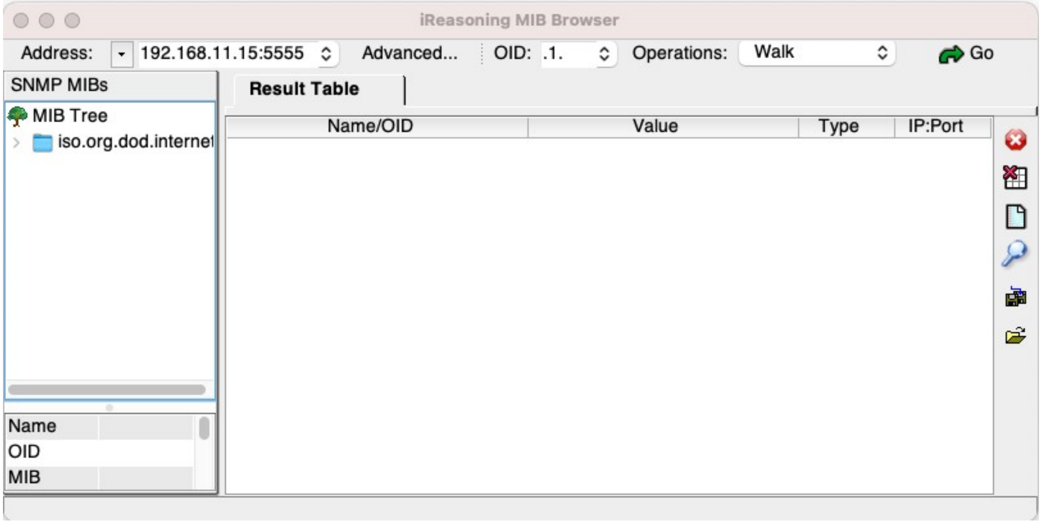
Protocol AES

SNMP settings for v3

Note. On v3, additional settings will appear. Select a username, then select *MD5* and *AES* for the 1st and 2nd Protocol respectively, and enter a 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.



iReasoning MIB Browser

Address: 192.168.11.15:5555 Advanced... OID: .1. Operations: Walk Go

SNMP MIBs

MIB Tree

iso.org.dod.internet

Result Table

Name/OID	Value	Type	IP:Port

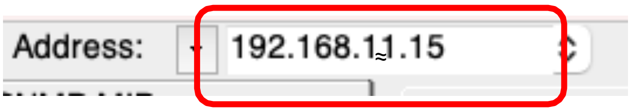
Name

OID

MIB

iReasoning MIB Browser main screen

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

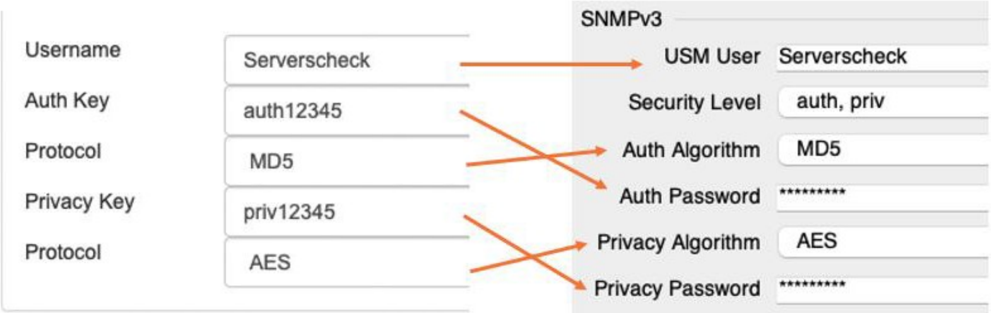


Address: 192.168.11.15

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.

SensorGateway iReasoning MIB Browser



Username: Serverscheck

Auth Key: auth12345

Protocol: MD5

Privacy Key: priv12345

Protocol: AES

SNMPv3

USM User: Serverscheck

Security Level: auth, priv

Auth Algorithm: MD5

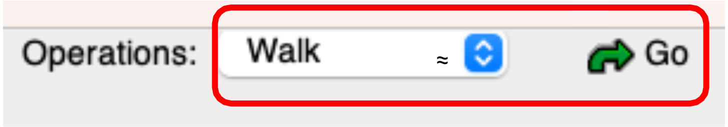
Auth Password: *********

Privacy Algorithm: AES

Privacy Password: *********

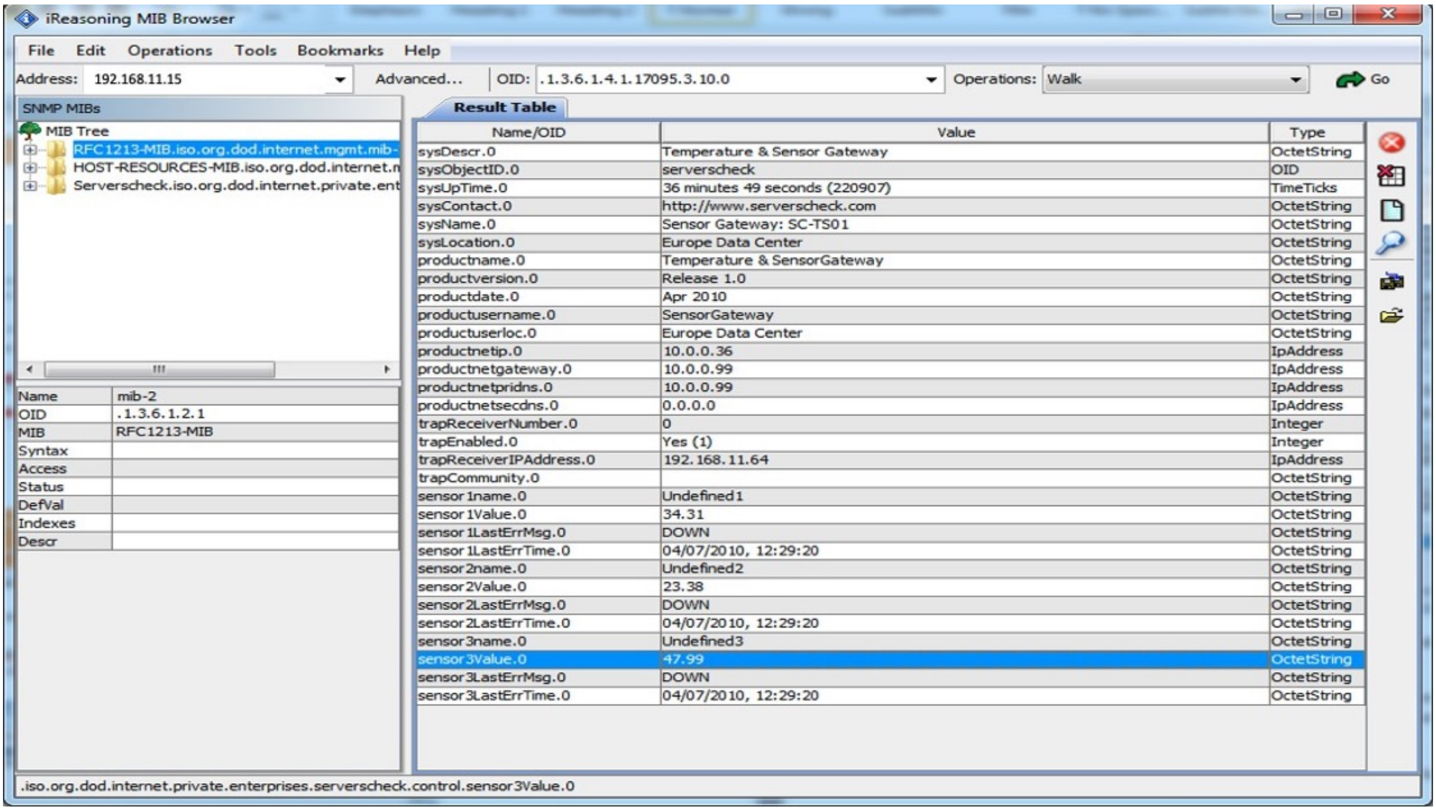
For the remaining settings of SNMPv3, leave it blank and it will later have values after it has undergone the SNMP Walk operation.

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

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



iReasoning MIB Browser
File
Edit
Operations
Tools
Bookmarks
Help
Advanced...
Go
SNMP MIBs
MIB Tree
RFC1213-MIB.iso.org.dod.internet.mgmt.mib-
HOST-RESOURCES-MIB.iso.org.dod.internet.n
Serverscheck.iso.org.dod.internet.private.ent
Result Table

Address: 192.168.11.15

OID: .1.3.6.1.4.1.17095.3.10.0

Operations: Walk

Name	mib-2
OID	.1.3.6.1.2.1
MIB	RFC1213-MIB
Syntax	
Access	
Status	
DefVal	
Indexes	
Descr	

Name/OID	Value	Type
sysDescr.0	Temperature & Sensor Gateway	OctetString
sysObjectID.0	serverscheck	OID
sysUpTime.0	36 minutes 49 seconds (220907)	TimeTicks
sysContact.0	http://www.serverscheck.com	OctetString
sysName.0	Sensor Gateway: SC-TS01	OctetString
sysLocation.0	Europe Data Center	OctetString
productname.0	Temperature & SensorGateway	OctetString
productversion.0	Release 1.0	OctetString
productdate.0	Apr 2010	OctetString
productusername.0	SensorGateway	OctetString
productuserloc.0	Europe Data Center	OctetString
productnetip.0	10.0.0.36	IpAddress
productnetgateway.0	10.0.0.99	IpAddress
productnetpridns.0	10.0.0.99	IpAddress
productnetsecdns.0	0.0.0.0	IpAddress
trapReceiverNumber.0	0	Integer
trapEnabled.0	Yes (1)	Integer
trapReceiverIPAddress.0	192.168.11.64	IpAddress
trapCommunity.0		OctetString
sensor1name.0	Undefined1	OctetString
sensor1Value.0	34.31	OctetString
sensor1LastErrMsg.0	DOWN	OctetString
sensor1LastErrTime.0	04/07/2010, 12:29:20	OctetString
sensor2name.0	Undefined2	OctetString
sensor2Value.0	23.38	OctetString
sensor2LastErrMsg.0	DOWN	OctetString
sensor2LastErrTime.0	04/07/2010, 12:29:20	OctetString
sensor3name.0	Undefined3	OctetString
sensor3Value.0	47.99	OctetString
sensor3LastErrMsg.0	DOWN	OctetString
sensor3LastErrTime.0	04/07/2010, 12:29:20	OctetString

.iso.org.dod.internet.private.enterprises.serverscheck.control.sensor3Value.0

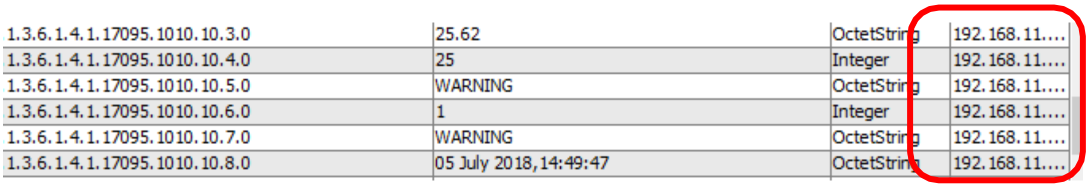
In the above screen copy you see all the SNMP parameters as made available by the InfraSensing Base Unit.

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**

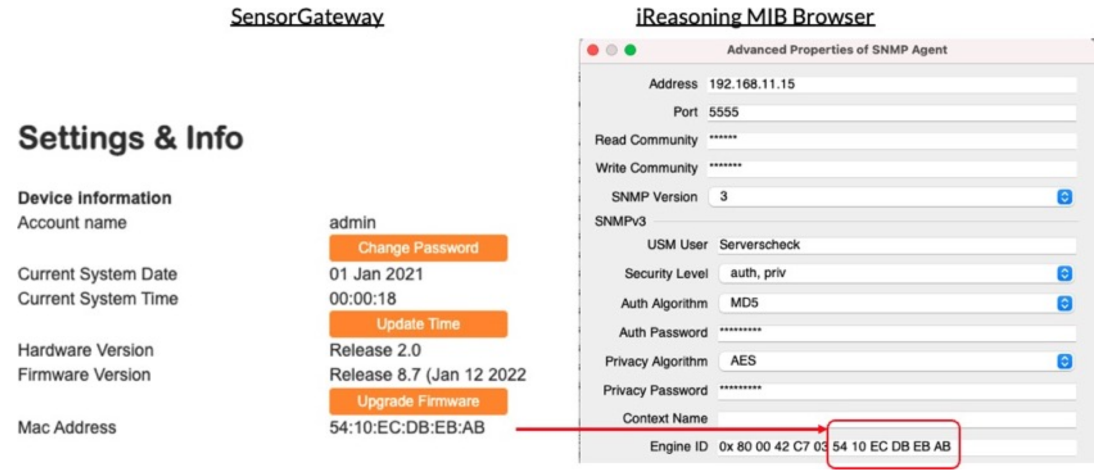
Note: for Firmware 7.5 and above a new OID structure is implemented which would have sensor values as String and Integer. The update will not affect the OLD OID structure and can still be used.

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.



SensorGateway

Settings & Info

Device information

Account name	admin
	Change Password
Current System Date	01 Jan 2021
Current System Time	00:00:18
	Update Time
Hardware Version	Release 2.0
Firmware Version	Release 8.7 (Jan 12 2022
	Upgrade Firmware
Mac Address	54:10:EC:DB:EB:AB

iReasoning MIB Browser

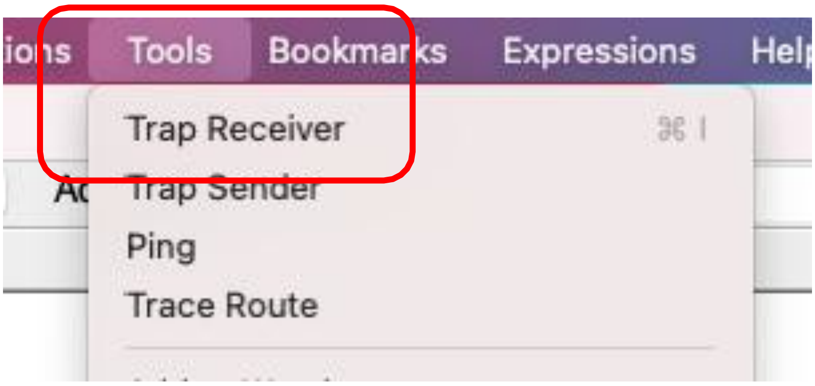
Advanced Properties of SNMP Agent

Address	192.168.11.15
Port	5555
Read Community	******
Write Community	*******
SNMP Version	3
SNMPv3	
USM User	Serverscheck
Security Level	auth, priv
Auth Algorithm	MD5
Auth Password	*********
Privacy Algorithm	AES
Privacy Password	*********
Context Name	
Engine ID	0x 80 00 42 C7 03 54 10 EC DB EB AB

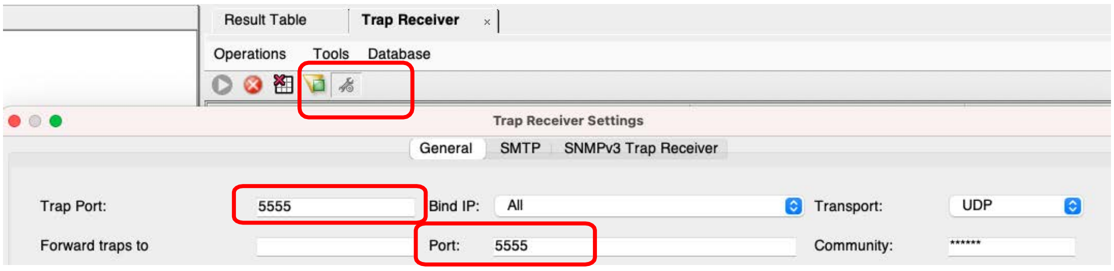
5.2 SNMP traps

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**

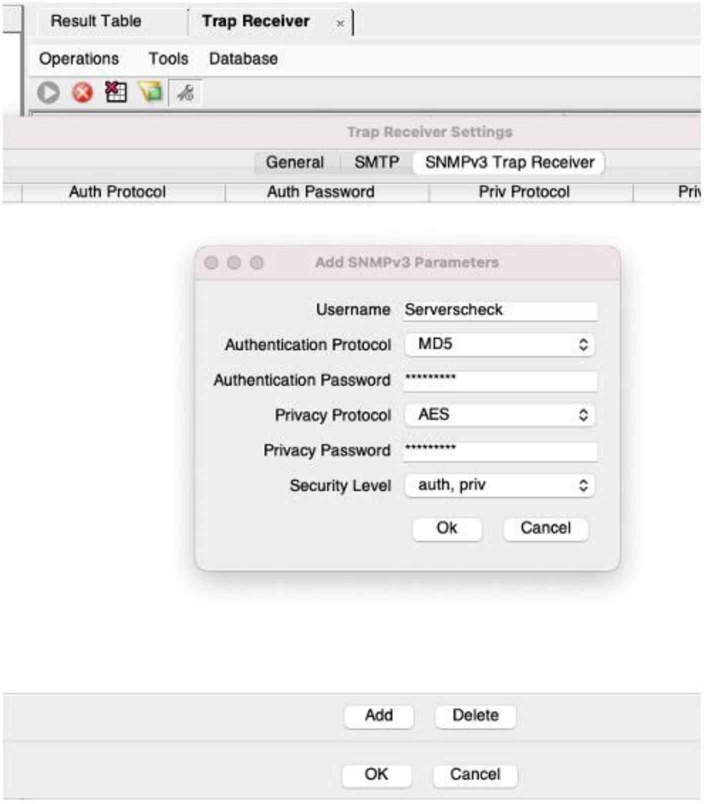


2. In the Trap Receiver, click on the Tools button for SNMP Trap settings.
   Set the Trap Receiver Port. This is the UDP port used by the SNMP Trap Receiver to receive incoming messages. In our example we set it to 5555.



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*.

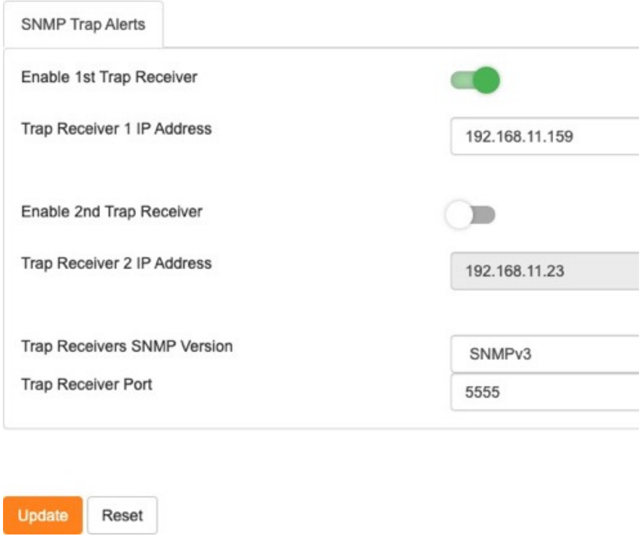


Username: Serverscheck
Authentication Protocol: MD5
Authentication Password: *********
Privacy Protocol: AES
Privacy Password: *********
Security Level: auth, priv

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

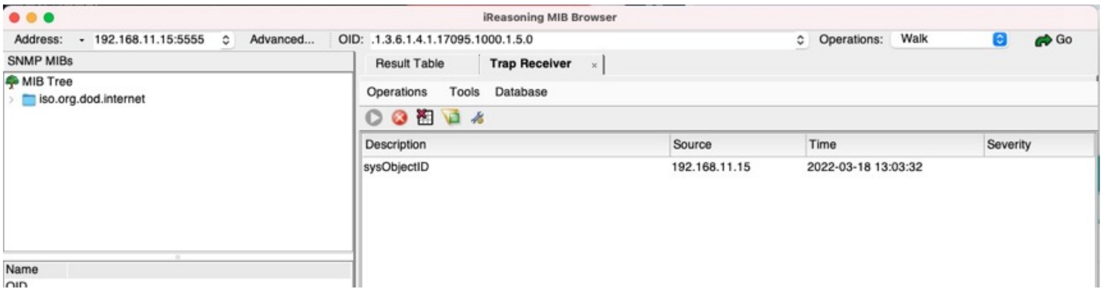
3. Go back to the Base Unit to set the SNMP Trap Alerts by:
   3.1. Click on the Enable 1st Trap Receiver
   Note: With the firmware version 7.40 and above you can have up to 2 trap receivers meaning you can install iReasoning or any trap receiver on any two computers and have the gateway send trap alerts 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: on
Trap Receiver 1 IP Address: 192.168.11.159
Enable 2nd Trap Receiver: off
Trap Receiver 2 IP Address: 192.168.11.23
Trap 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.



Address: 192.168.11.15:5555
OID: .1.3.6.1.4.1.17095.1000.1.5.0
Operations: Walk

Description	Source	Time	Severity
sysObjectID	192.168.11.15	2022-03-18 13:03:32	

Above shows the SNMP Trap as received by iReasoning MIB Browser

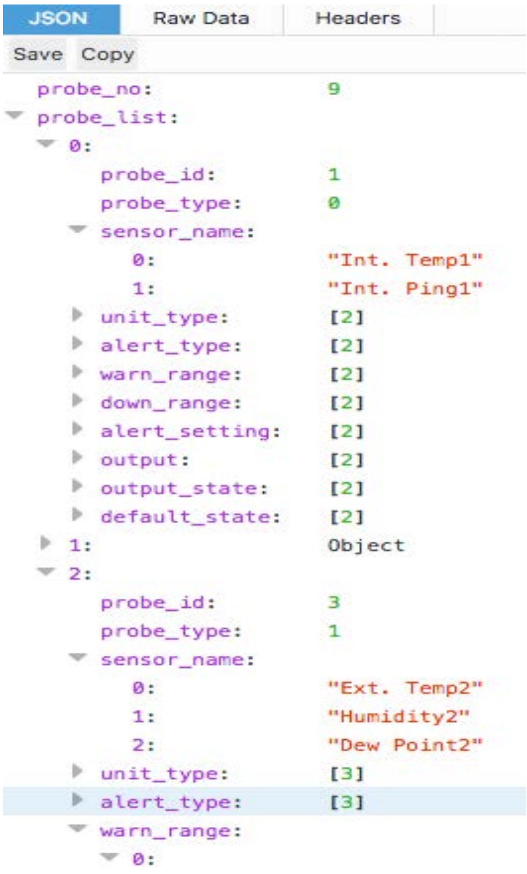
5.3 JSON (PULL)

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



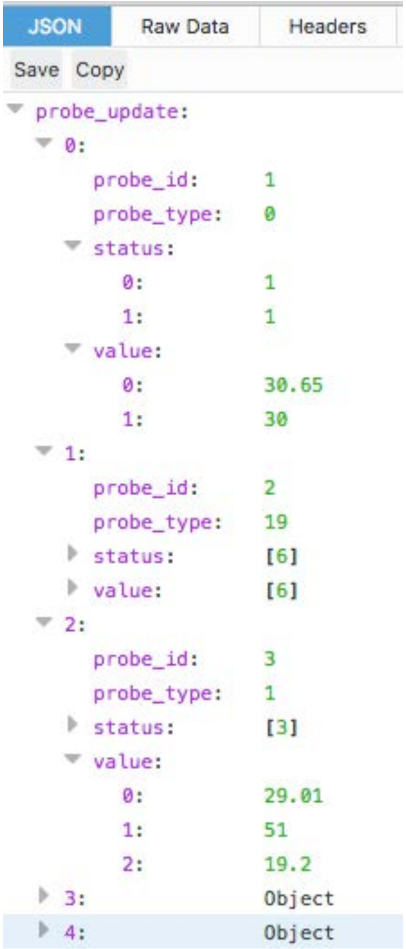
```
probe_no:              9
probe_list:
  0:
    probe_id:          1
    probe_type:        0
    sensor_name:
      0:               "Int. Temp1"
      1:               "Int. Ping1"
    unit_type:         [2]
    alert_type:        [2]
    warn_range:        [2]
    down_range:        [2]
    alert_setting:     [2]
    output:            [2]
    output_state:      [2]
    default_state:     [2]
  1:                   Object
  2:
    probe_id:          3
    probe_type:        1
    sensor_name:
      0:               "Ext. Temp2"
      1:               "Humidity2"
      2:               "Dew Point2"
    unit_type:         [3]
    alert_type:        [3]
    warn_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

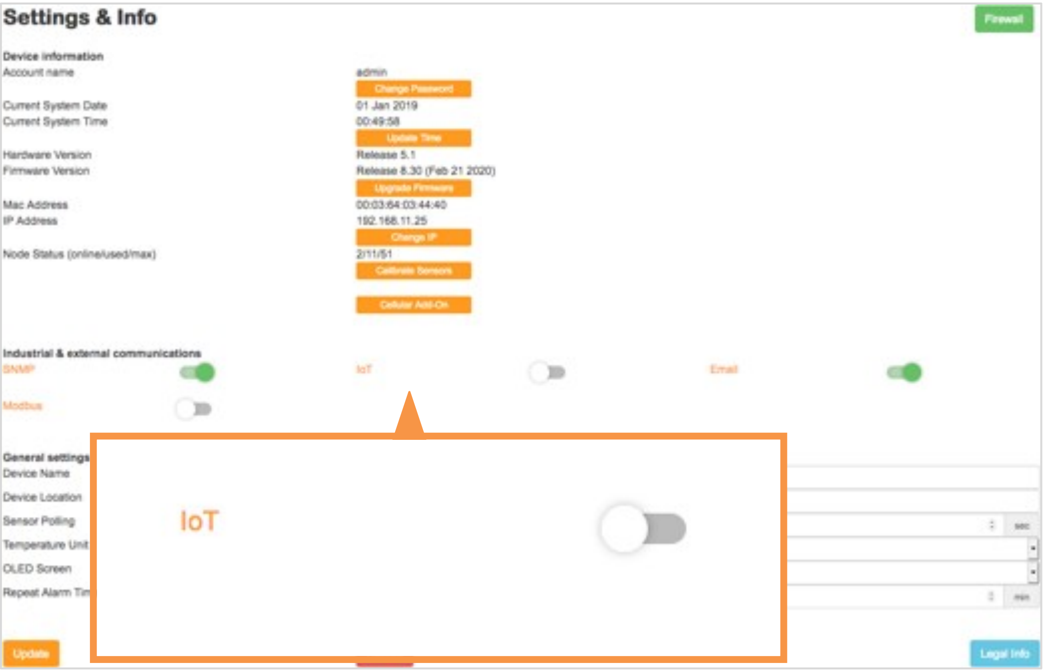


```
▼ probe_update:
  ▼ 0:
      probe_id:     1
      probe_type:   0
    ▼ status:
        0:          1
        1:          1
    ▼ value:
        0:          30.65
        1:          30
  ▼ 1:
      probe_id:     2
      probe_type:   19
    ▶ status:       [6]
    ▶ value:        [6]
  ▼ 2:
      probe_id:     3
      probe_type:   1
    ▶ status:       [3]
    ▼ value:
        0:          29.01
        1:          51
        2:          19.2
  ▶ 3:              Object
  ▶ 4:              Object
```

5.4 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 ourbase unit, we will have a new option for IoT under the settings menu.



Settings & Info

Device information

Account name	admin
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)
Mac Address	00:03:64:03:44:40
IP Address	192.168.11.25
Node Status (online/used/max)	2/11/51

Industrial & external communications

SNMP	● on	IoT	○ off	Email	● on
Modbus	○ off				

General settings

Device Name

Device Location

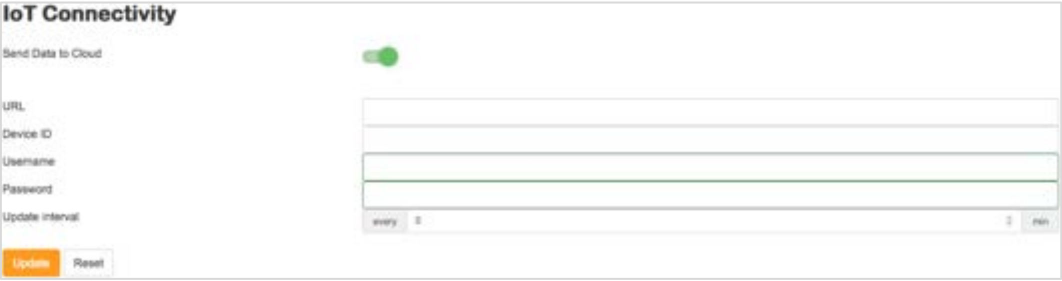
Sensor Polling

Temperature Unit

OLED Screen

Repeat Alarm Tim

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	● on
URL	
Device ID	
Username	
Password	
Update interval	every 5 min

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":"2020-02-21T05:20:33Z","d":"000364037961","u":"user","p":"pass","lo":"27.674","la":"53.874","nsg":"14","nty":"3G","nsi":"sim1"}
{"t":"2020-02-21T05:20:33Z","d":"000364037961","u":"user","p":"pass","sensors":[{"si":"1","sn":"Int. Temp1","st":"Int. Temp","sv":"24.40"}]}
{"t":"2020-02-21T05:20:33Z","d":"000364037961","u":"user","p":"pass","sensors":[{"si":"2","sn":"Int. Ping1","st":"Int. Ping","sv":"1.00"}]}
...
{"t":"2020-02-21T05:21:36Z","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

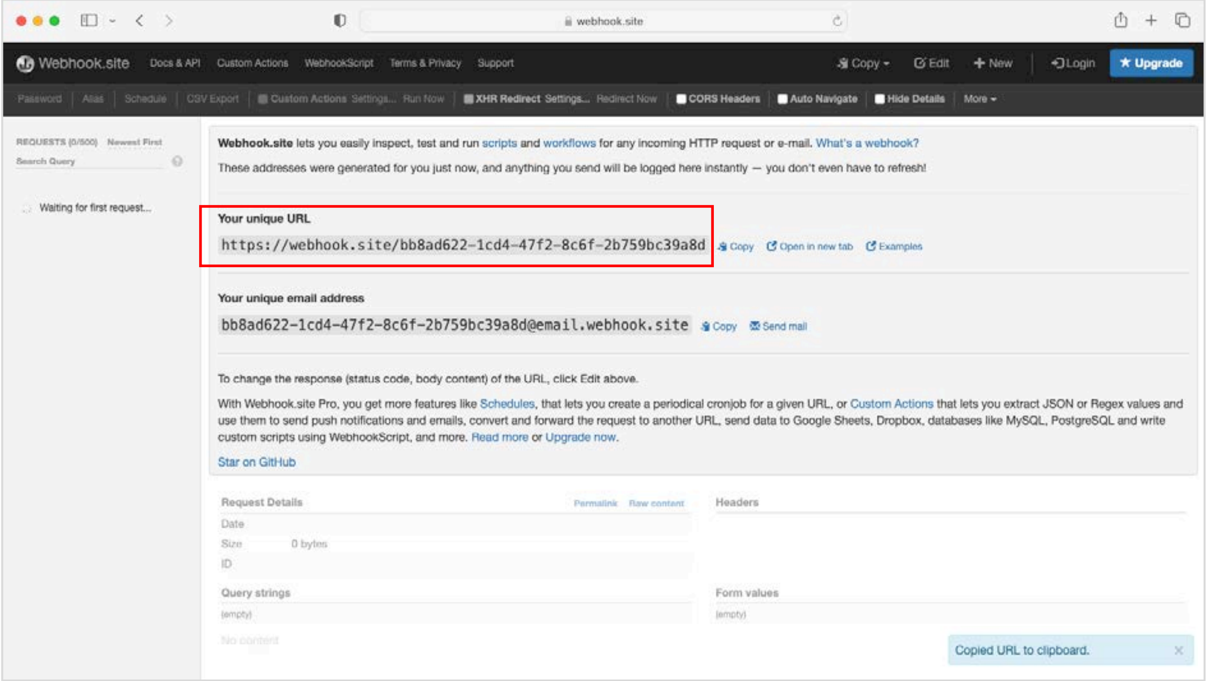
The first call is the connectivity details:
lo: longitude from GPS
la: latitude from GPS
nsg: network signal strength
nty: network type 4G/3G/2G
nsi: sim used

```
"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

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

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



Waiting for first request...

Webhook.site lets you easily inspect, test and run scripts and workflows for any incoming HTTP request or e-mail. What's a webhook?

These addresses were generated for you just now, and anything you send will be logged here instantly — you don't even have to refresh!

Your unique URL

`https://webhook.site/bb8ad622-1cd4-47f2-8c6f-2b759bc39a8d`

Your unique email address

`bb8ad622-1cd4-47f2-8c6f-2b759bc39a8d@email.webhook.site`

To change the response (status code, body content) of the URL, click Edit above.

With Webhook.site Pro, you get more features like Schedules, that lets you create a periodical cronjob for a given URL, or Custom Actions that lets you extract JSON or Regex values and use them to send push notifications and emails, convert and forward the request to another URL, send data to Google Sheets, Dropbox, databases like MySQL, PostgreSQL and write custom scripts using WebhookScript, and more. Read more or Upgrade now.

Star on GitHub

Request Details
Date
Size 0 bytes
ID

Headers

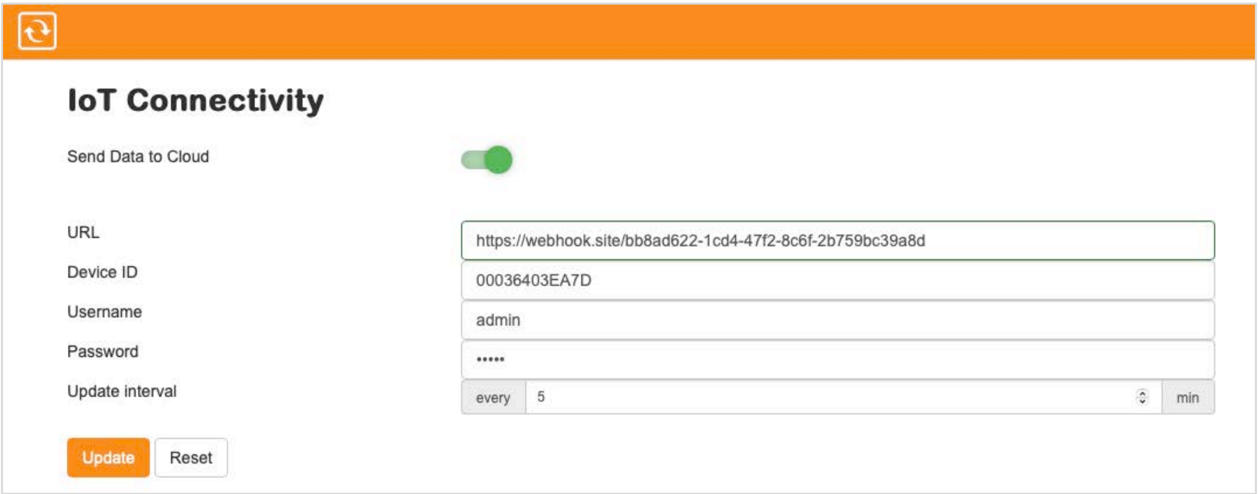
Query strings
(empty)

Form values
(empty)

No content

Copied URL to clipboard. ×

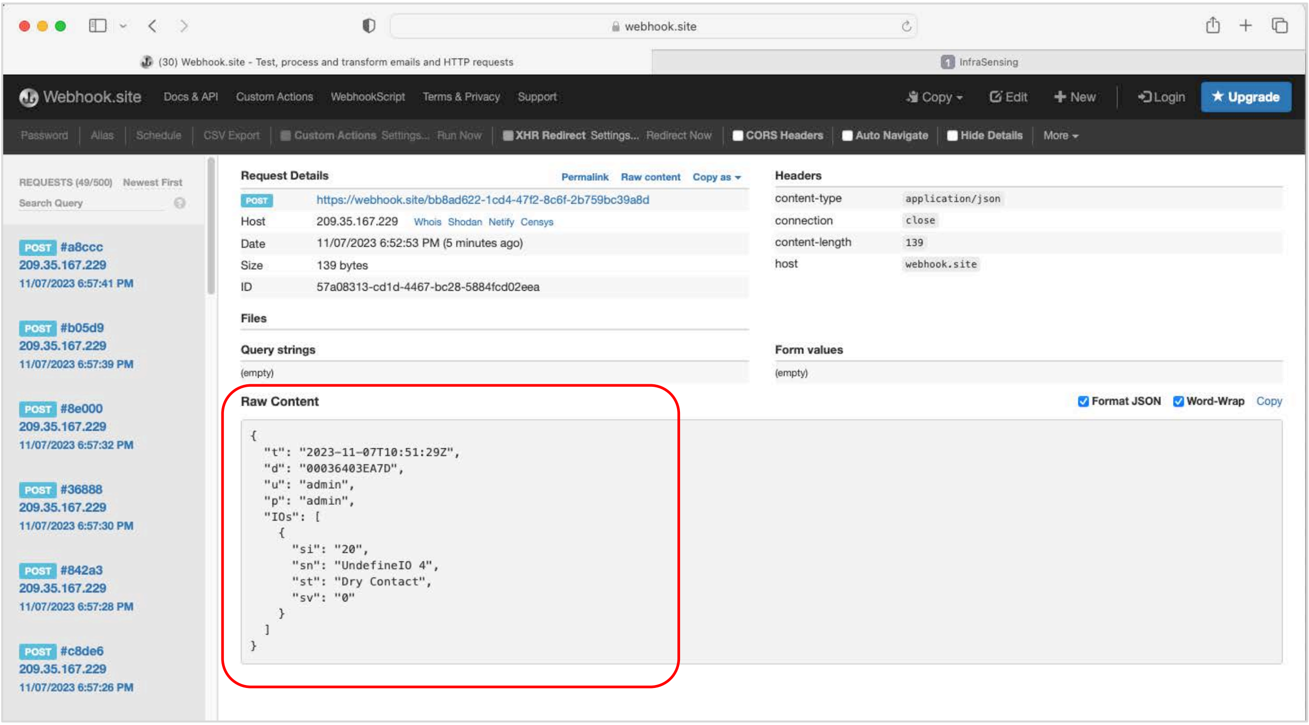
After copying the URL, let's return to our IoT settings to input the credentials.



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

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



POST #a8ccc	209.35.167.229	11/07/2023 6:57:41 PM
POST #b05d9	209.35.167.229	11/07/2023 6:57:39 PM
POST #8e000	209.35.167.229	11/07/2023 6:57:32 PM
POST #36888	209.35.167.229	11/07/2023 6:57:30 PM
POST #842a3	209.35.167.229	11/07/2023 6:57:28 PM
POST #c8de6	209.35.167.229	11/07/2023 6:57:26 PM

Request Details

POST	https://webhook.site/bb8ad622-1cd4-47f2-8c6f-2b759bc39a8d
Host	209.35.167.229 Whois Shodan Netify Censys
Date	11/07/2023 6:52:53 PM (5 minutes ago)
Size	139 bytes
ID	57a08313-cd1d-4467-bc28-5884fcd02eea

Headers

content-type	application/json
connection	close
content-length	139
host	webhook.site

Files

Query strings

(empty)

Form values

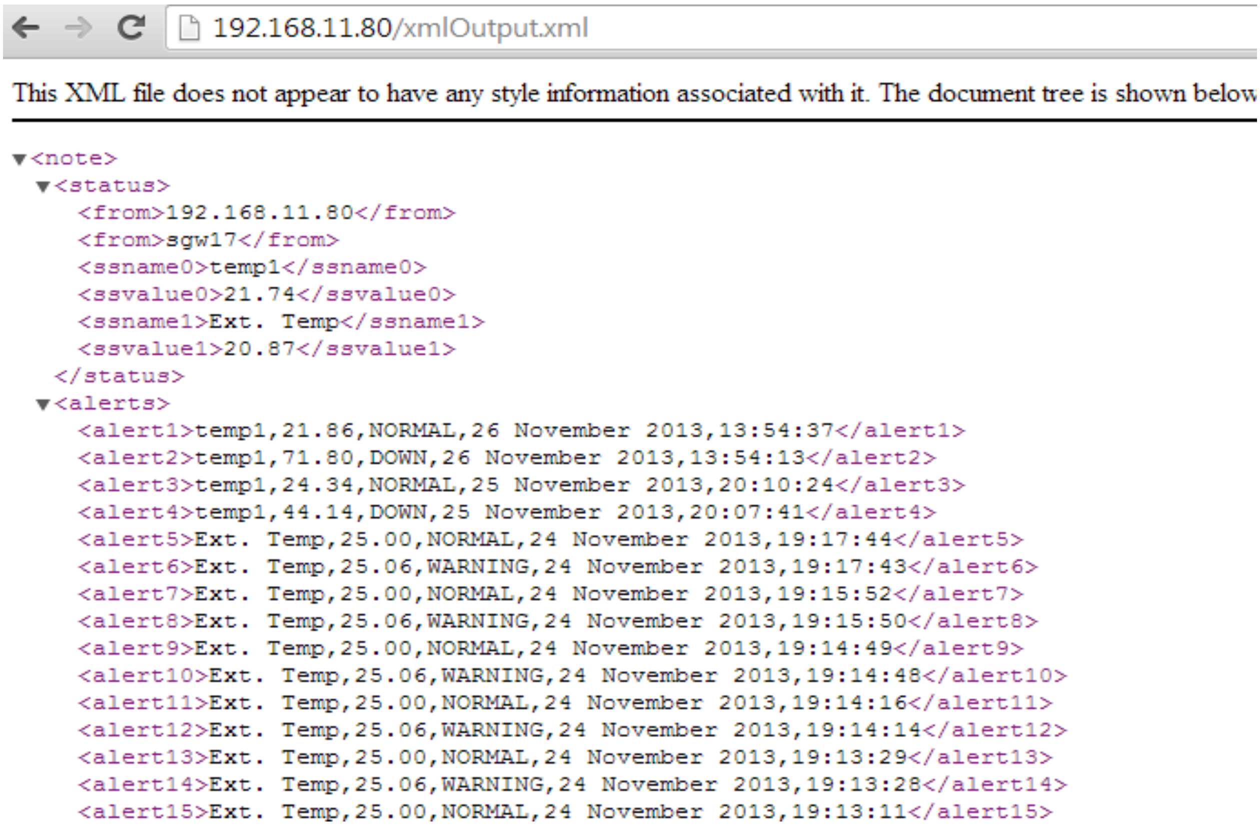
(empty)

Raw Content ☑ Format JSON ☑ Word-Wrap Copy

```
{
  "t": "2023-11-07T10:51:29Z",
  "d": "00036403EA7D",
  "u": "admin",
  "p": "admin",
  "IOs": [
    {
      "si": "20",
      "sn": "UndefineIO 4",
      "st": "Dry Contact",
      "sv": "0"
    }
  ]
}
```

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

5.6 XML output



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

```
▼<note>
  ▼<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>
  ▼<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.

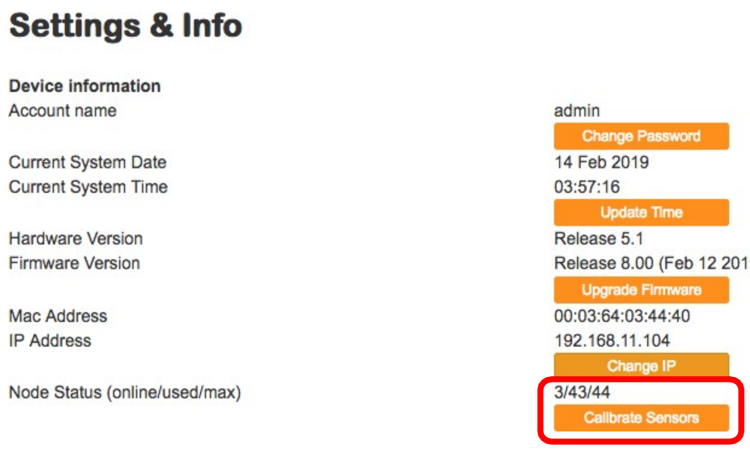
5.7 ModBus TCP / RTU

We have a separate manual for ModBus just click on this linkLINK TO MODBUS, then click on ModBus Manual.

6 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.



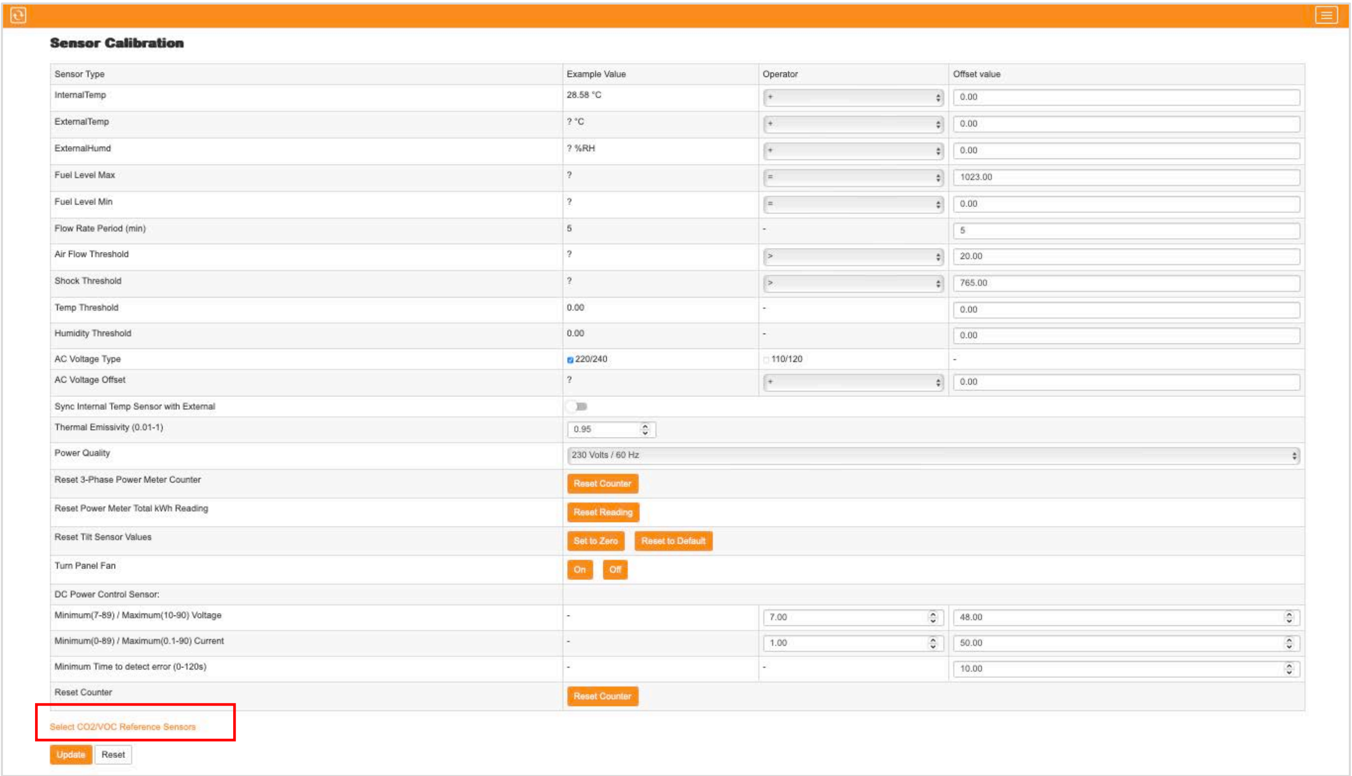
Settings & Info

Device information

Account name	admin 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

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 Calibration

Sensor Type	Example Value	Operator	Offset value
InternalTemp	28.58 °C	+	0.00
ExternalTemp	? °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 Default		
Turn Panel Fan	On Off		
DC Power Control Sensor:			
Minimum(7-89) / Maximum(10-90) Voltage	-	7.00	48.00
Minimum(0-89) / Maximum(0.1-90) Current	-	1.00	50.00
Minimum Time to detect error (0-120s)	-	-	10.00
Reset Counter	Reset Counter		

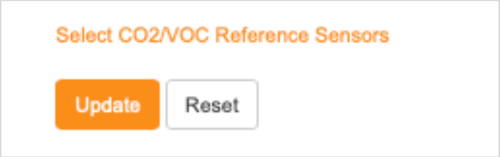
Select CO2/VOC Reference Sensors

Update Reset

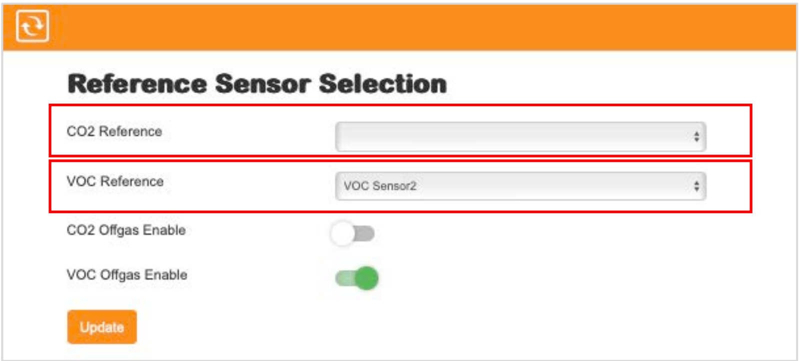
With the introduction of firmware version 9.1, a new feature has been incorporated, allowing users to designate CO2/VOC sensors as reference points. For more information, refer to section 6.1.

6.1 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.



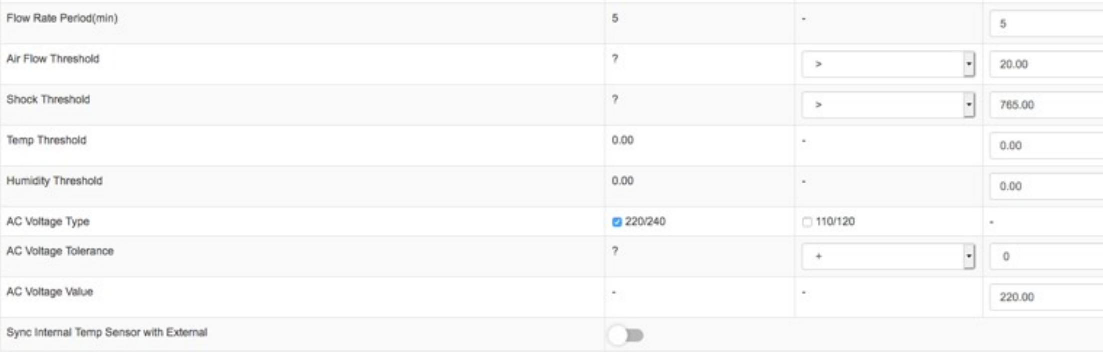
Select CO2/VOC Reference Sensors



Reference Sensor Selection

CO2 Reference	
VOC Reference	VOC Sensor2
CO2 Offgas Enable	
VOC Offgas Enable	

6.2 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	?	+	0
AC Voltage Value	-	-	220.00
Sync Internal Temp Sensor with External			

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.

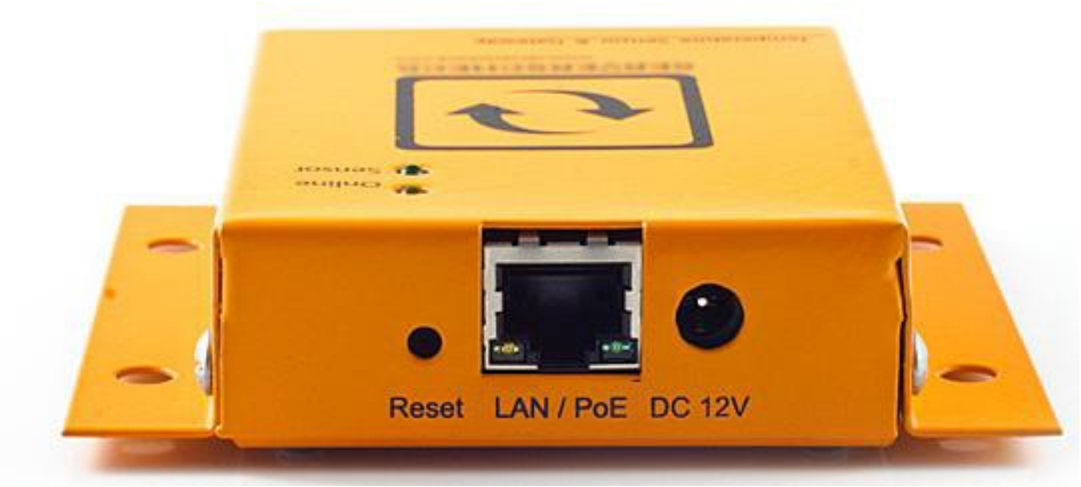
Warning. For Thermal Emissivity calibration, it is recommended to be set to 0.95 or depending on the surface to be scanned with ENV-THIMG.Failure to calibrate may give off incorrect values for the ENV-THIMG sensor.

7 Factory resetting of Base Unit

7.1 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**

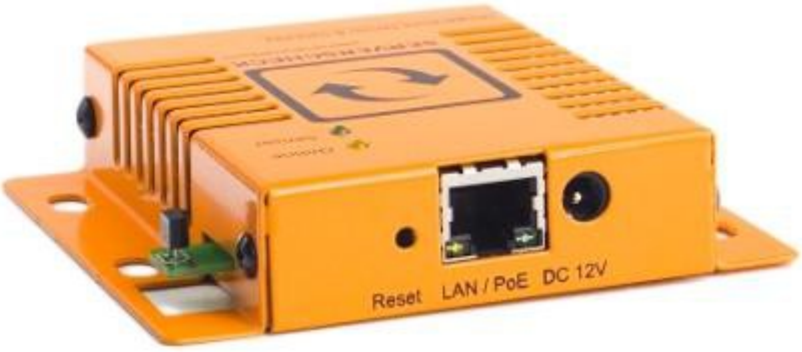
7.2 Base Unit v3 and v4

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

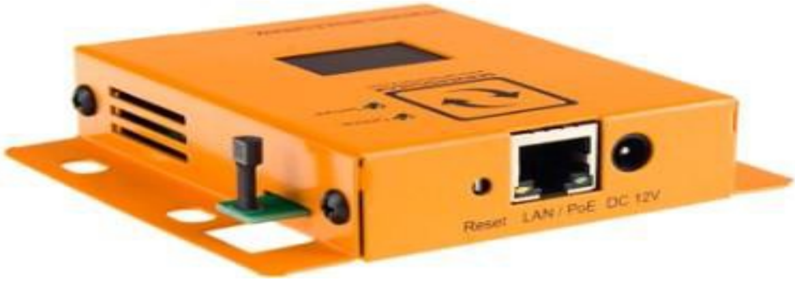


Remove the external sensor probe
Remove the power adapter or PoE cable
Push the **Reset** button
While the **Reset** button is pushed, plug in the power adapter or PoE Cable
After 10 seconds the Green & Yellow LED’s will be on steady (not blinking)
Remove power adapter or PoE cable
Wait 3 seconds
Plug 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 **http://192.168.11.160**

7.3 Base Unit v5

Following only applies to Base Units v5

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

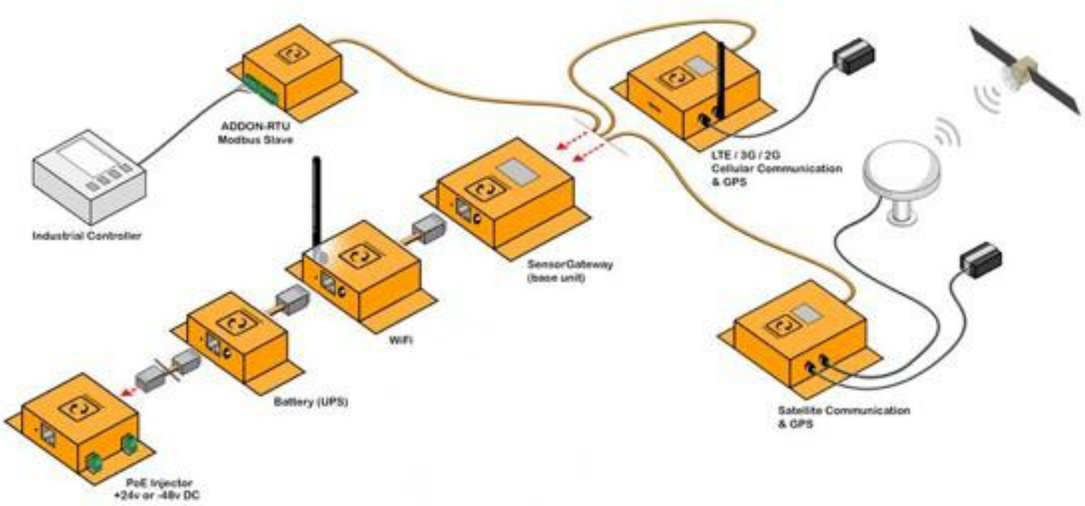


1. Remove the external sensor probe.
2. Remove the power adapter or PoE powered network cable.
3. Push the **Reset** button.
4. While the **Reset** button is pushed, plug in the power adapter or PoE powered network cable .
5. Hold it for 15 seconds before releasing it. The yellow LED should be blinking 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 by loading to the firmware 3.2; it might not have an OLED display active
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 - https://infrasensing.com/support/downloads.asp

(Refer to section 2.8)

8 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.



8.1 Wifi Add-On

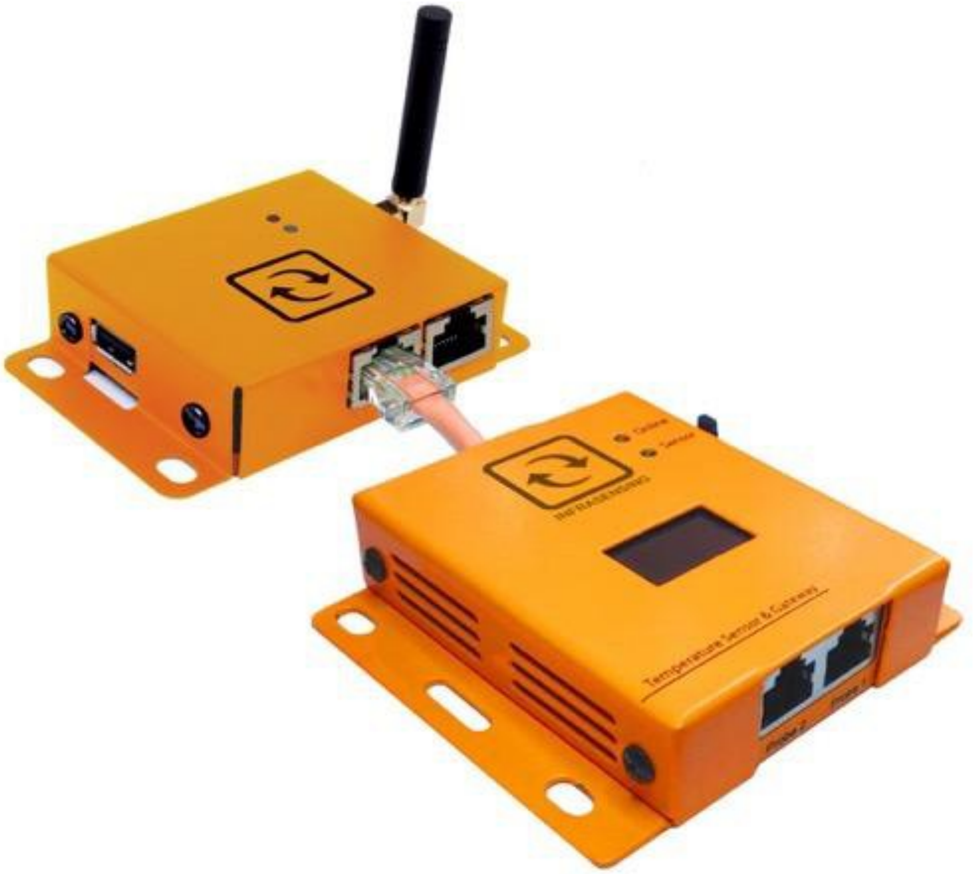
The InfraSensing Add on Wifi module is an expansion unit to the Base Unit which enables wired and wireless networking application. The Add on Wifi module supports 802.11n standards, and provides backward compatibility with older 802.11b/g standards as well. The up-to-150Mbps wireless speed makes it ideal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

8.1.1 Features

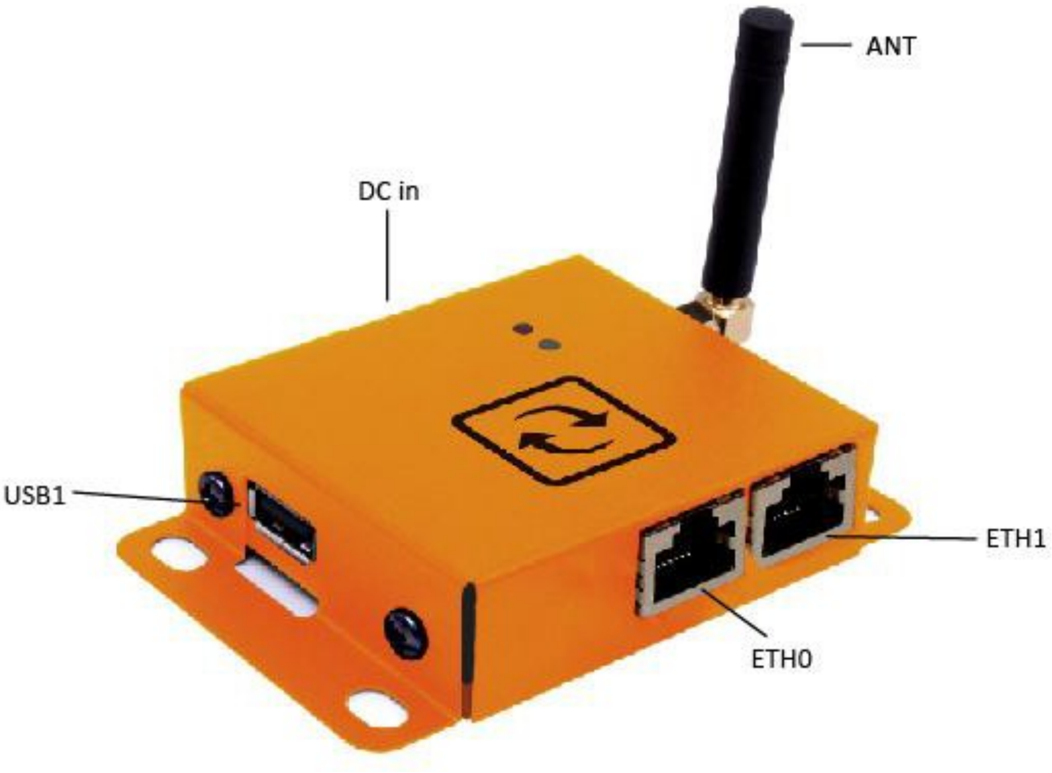
Portable design
Connects directly to the Base Unit
Directly powers the Base Unit via the 12v DC adapter output GUI
accessible using any browser
USB support for 3G and LTE dongles
Pre-encryption that prevents unauthorized access from users outside of the network

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

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



8.1.3 Hardware interface

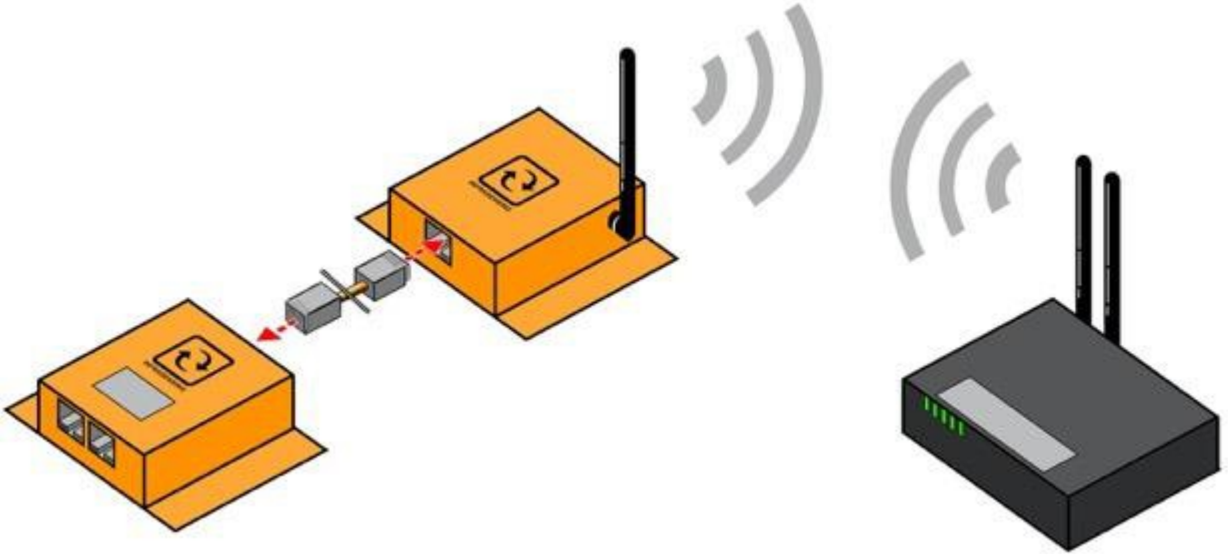


Interface	Description
ANT	Wireless antenna
ETH1	WAN/LAN port
ETH0	LAN port to Base Unit
DC IN	12-volt DC adapter socket
USB1	USB for 3G and LTE dongle

8.1.4 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 ETH0

8.1.5 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

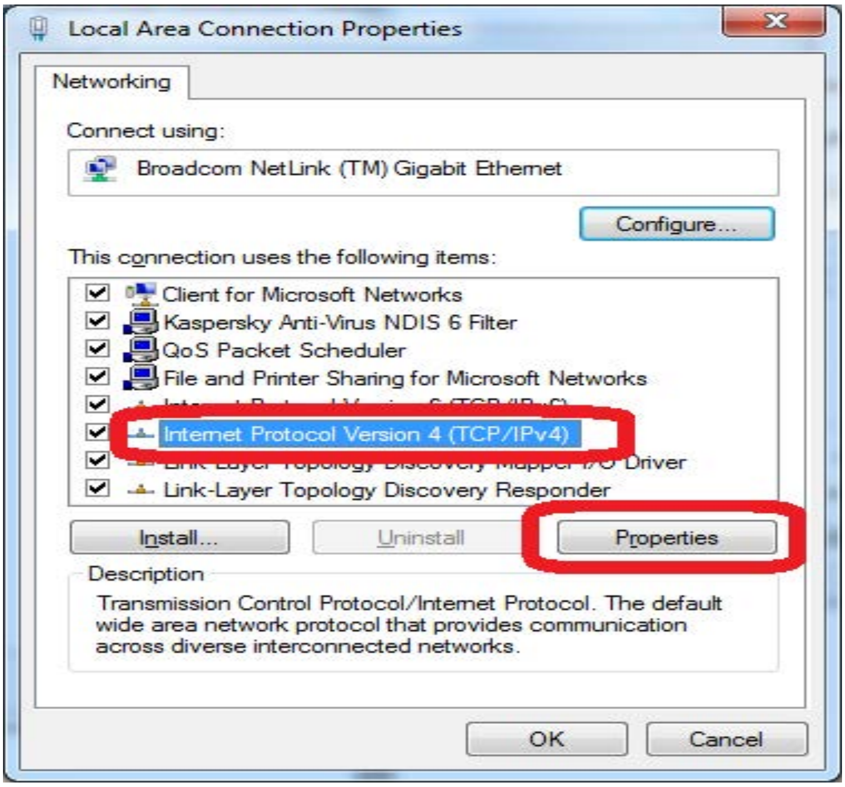
As an access point (WLAN)

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

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 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Install... | Uninstall | Properties

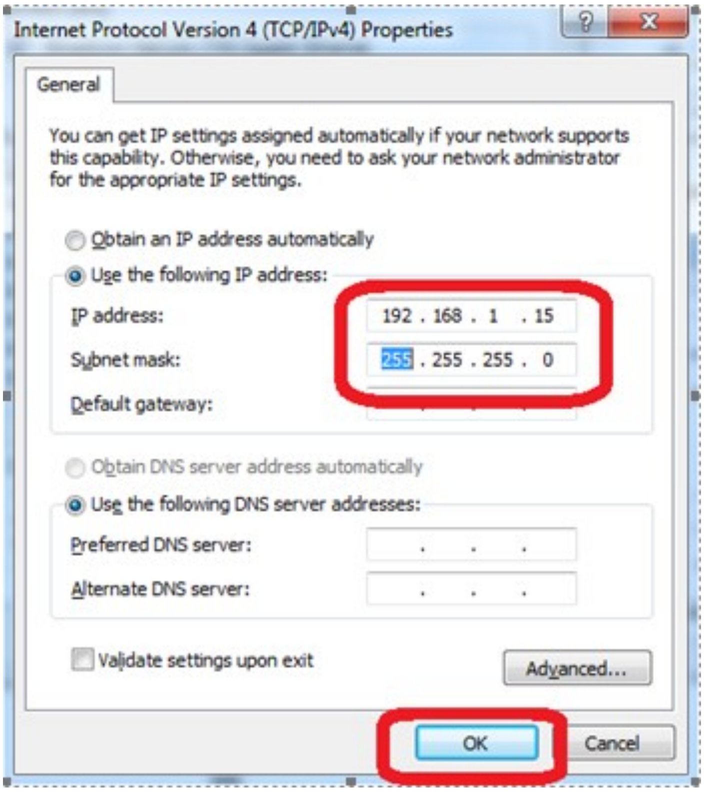
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK | Cancel

Set the corressponding IP ranges

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 1 . 15
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	

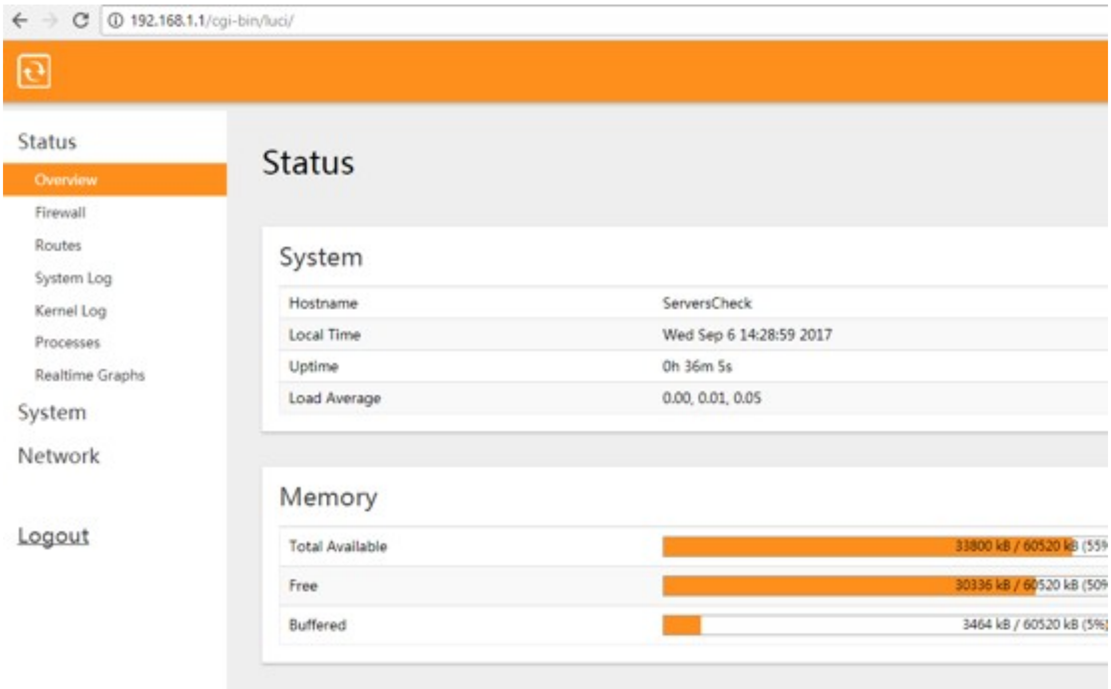
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	. . .
Alternate DNS server:	. . .

□ Validate settings upon exit

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.



192.168.1.1/cgi-bin/luci/

Status

System

Hostname	ServersCheck
Local Time	Wed Sep 6 14:28:59 2017
Uptime	0h 36m 5s
Load Average	0.00, 0.01, 0.05

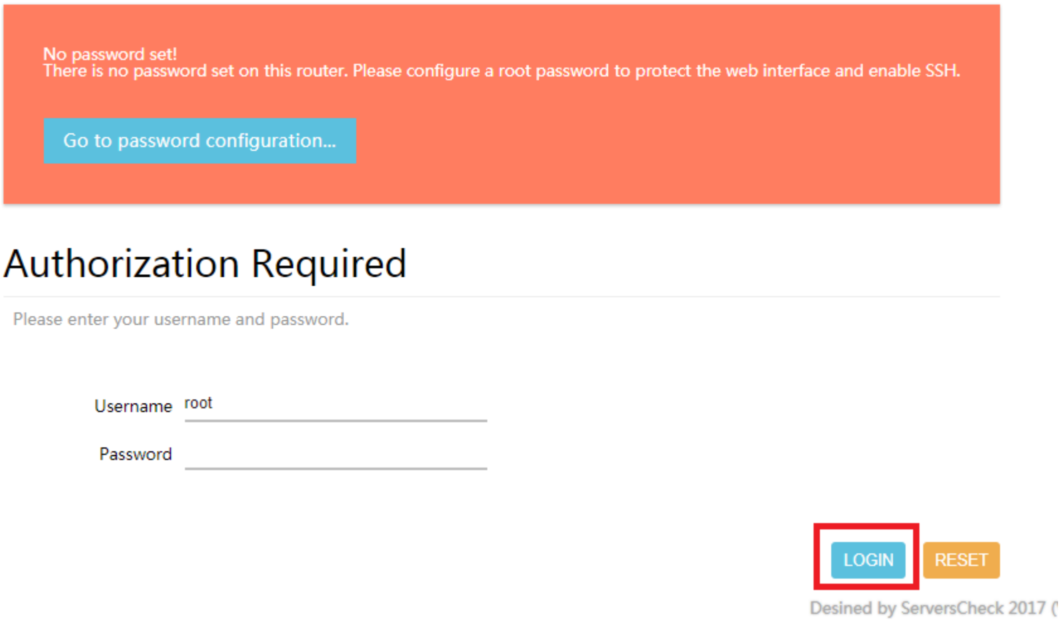
Memory

Total Available	33800 kB / 60520 kB (55
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

8.1.6 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. Please configure a root password to protect the web interface and enable SSH.

Authorization Required

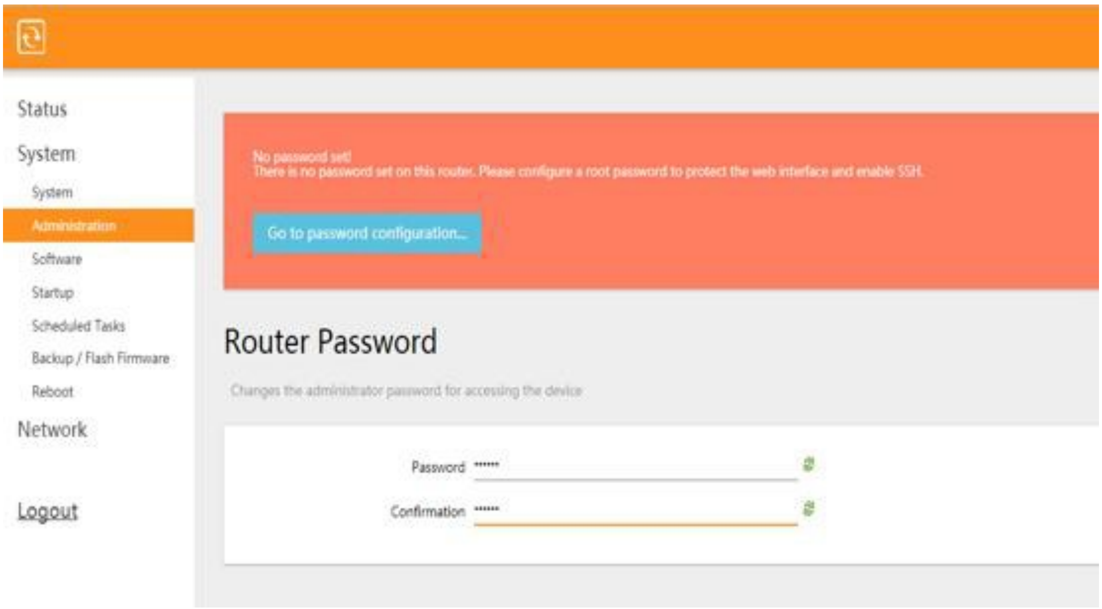
Please enter your username and password.

Username root

Password

Go to password configuration...
LOGIN
RESET
Desined by ServersCheck 2017 (

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



No password set!
There is no password set on this router. Please configure a root password to protect the web interface and enable SSH.

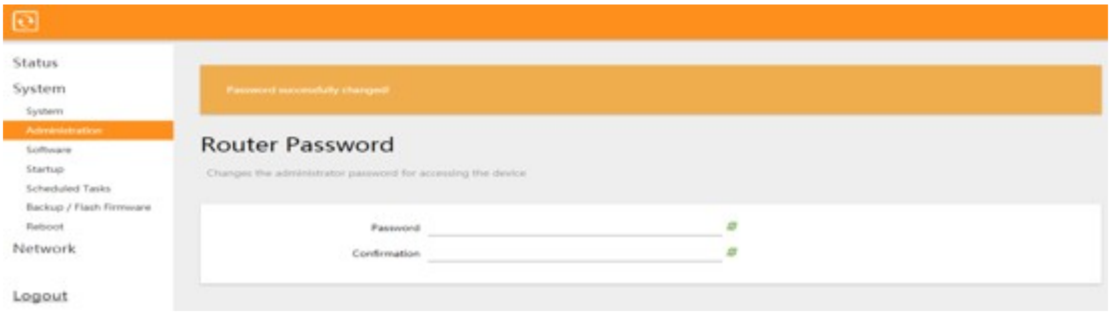
Router Password

Changes the administrator password for accessing the device

Password ******

Confirmation ******

There will be a notification that the password was successfully set



Password successfully changed!

Router Password

Changes the administrator password for accessing the device

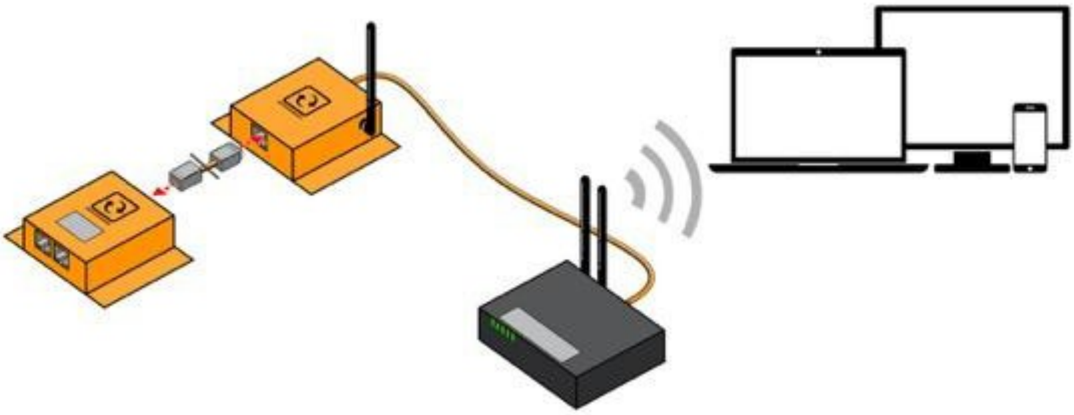
Password

Confirmation

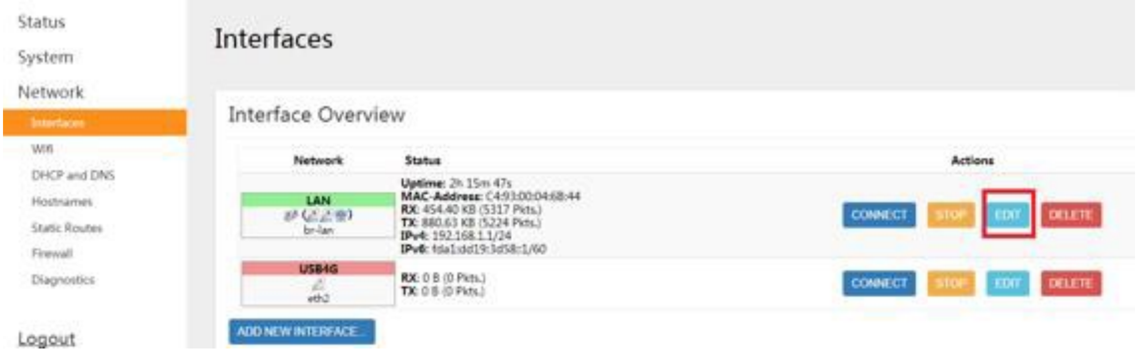
8.1.7 Configuration modes

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

As wireless router



Access the GUI using WLAN
Go to Network > Interfaces
Edit LAN network

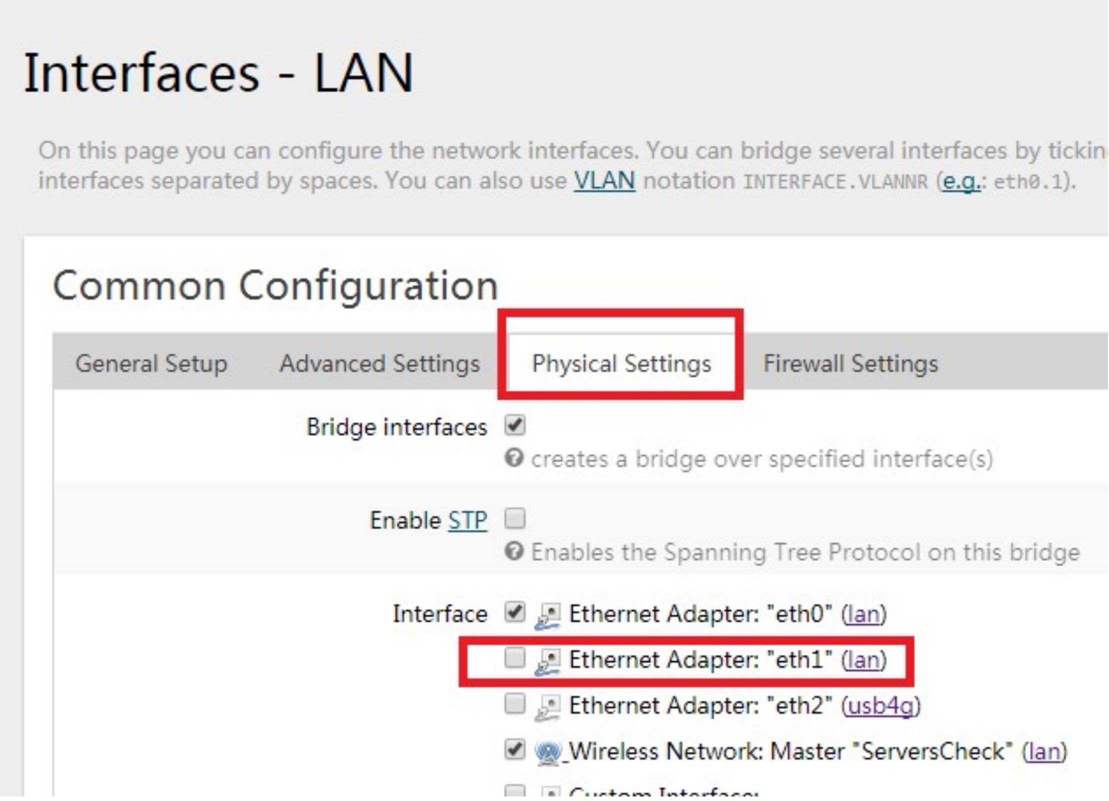


Interfaces

Interface Overview

Network	Status	Actions
LAN br-lan	**Uptime:** 2h 15m 47s **MAC-Address:** C4:93:00:04:68:44 **RX:** 454.40 KB (5317 Pkts.) **TX:** 880.63 KB (5224 Pkts.) **IPv4:** 192.168.1.1/24 **IPv6:** fda1:dd19:3d58::1/60	CONNECT STOP EDIT DELETE
USB4G eth2	**RX:** 0 B (0 Pkts.) **TX:** 0 B (0 Pkts.)	CONNECT STOP EDIT DELETE

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 VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

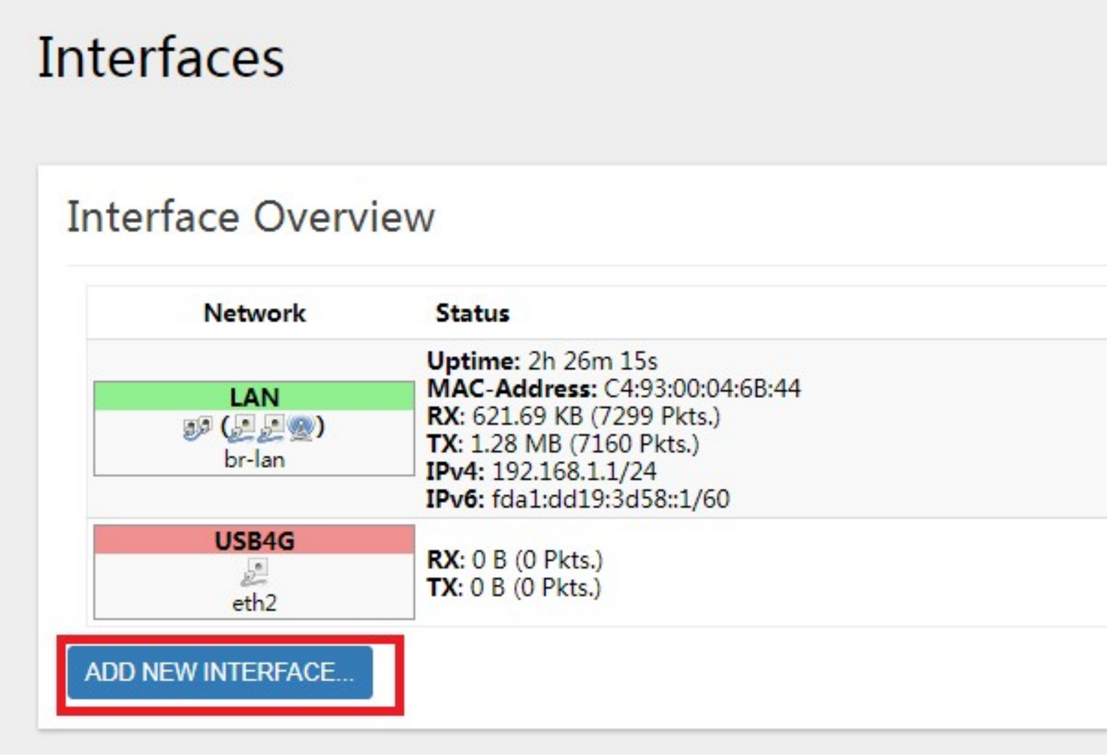
Common Configuration

Bridge interfaces ☑
creates a bridge over specified interface(s)

Enable STP □
Enables the Spanning Tree Protocol on this bridge

Interface
☑ Ethernet Adapter: "eth0" (lan)
□ Ethernet Adapter: "eth1" (lan)
□ Ethernet Adapter: "eth2" (usb4g)
☑ Wireless Network: Master "ServersCheck" (lan)
□ Custom Interface:

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

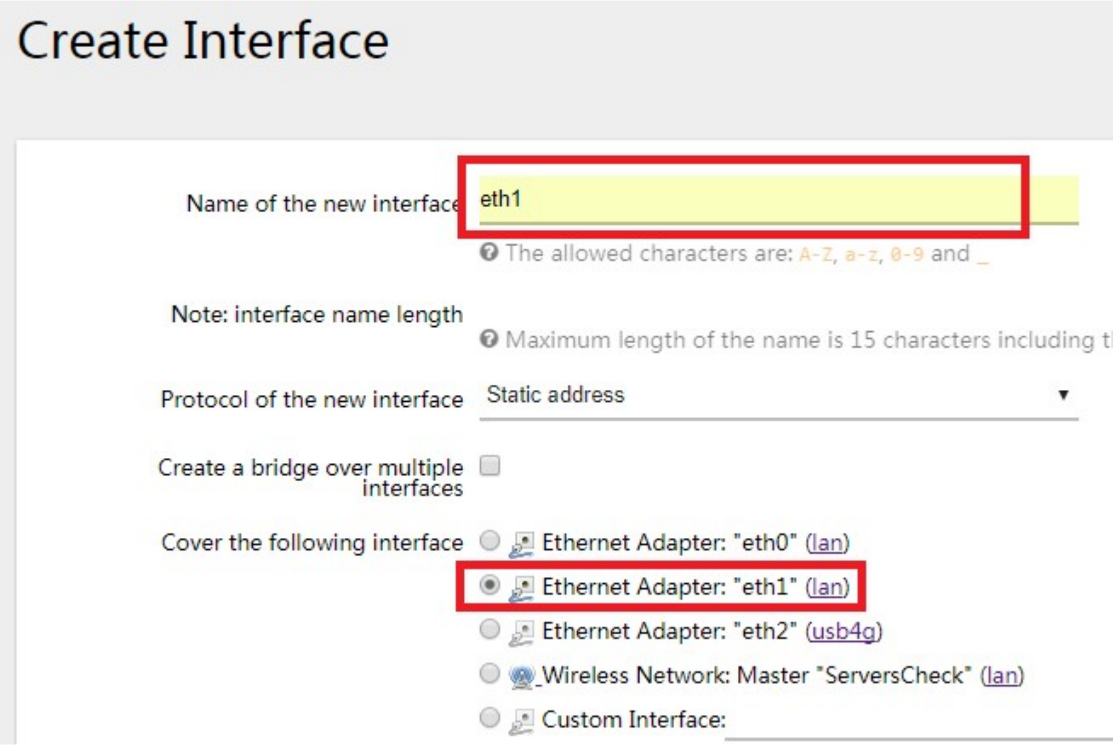


Interfaces

Interface Overview

Network	Status
LAN br-lan	**Uptime:** 2h 26m 15s **MAC-Address:** C4:93:00:04:6B:44 **RX:** 621.69 KB (7299 Pkts.) **TX:** 1.28 MB (7160 Pkts.) **IPv4:** 192.168.1.1/24 **IPv6:** fda1:dd19:3d58::1/60
USB4G eth2	**RX:** 0 B (0 Pkts.) **TX:** 0 B (0 Pkts.)

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



Create Interface

Name of the new interface: eth1

The allowed characters are: A-Z, a-z, 0-9 and _

Note: interface name length

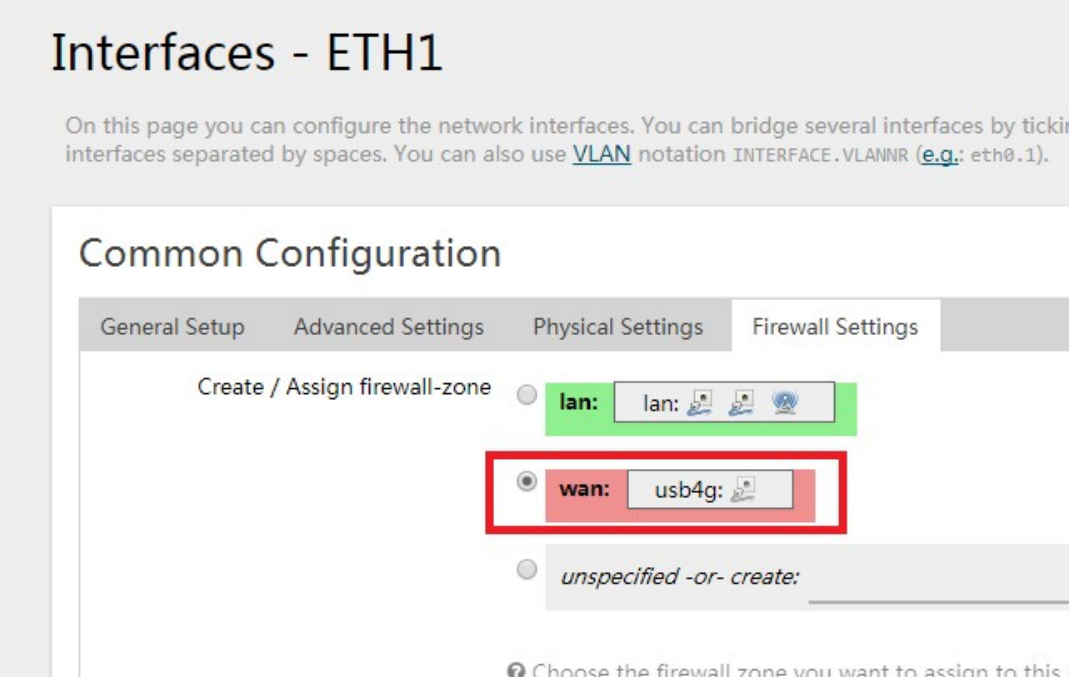
Maximum length of the name is 15 characters including t

Protocol of the new interface: Static address

Create a bridge over multiple interfaces: □

Cover the following interface:
- ○ Ethernet Adapter: "eth0" (lan)
- ● Ethernet Adapter: "eth1" (lan)
- ○ Ethernet Adapter: "eth2" (usb4g)
- ○ Wireless Network: Master "ServersCheck" (lan)
- ○ Custom Interface:

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



Interfaces - ETH1

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

Common Configuration

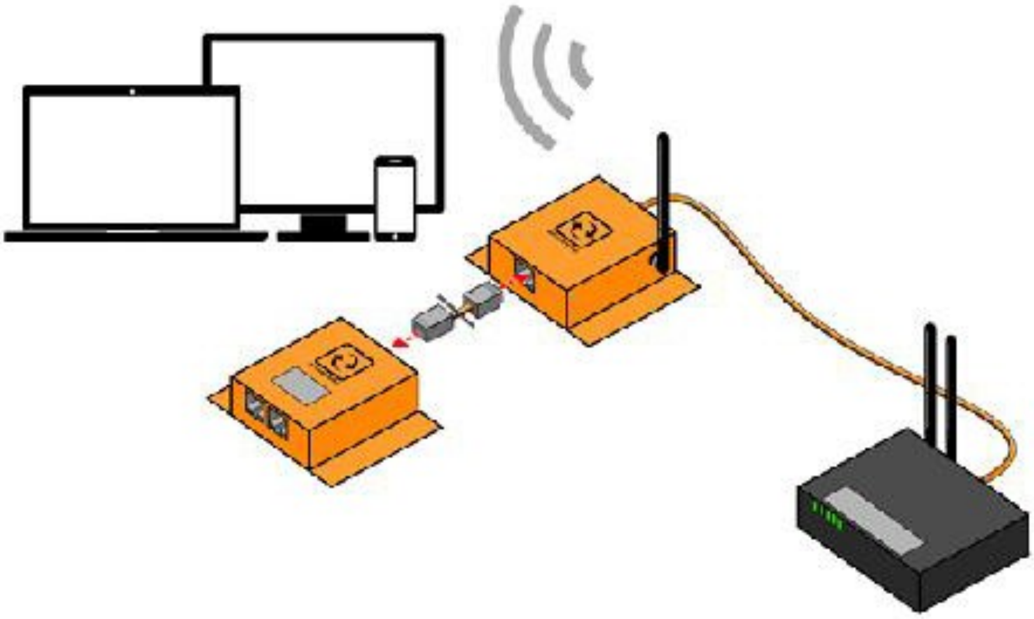
Create / Assign firewall-zone:
- ○ lan: lan:
- ● wan: usb4g:
- ○ *unspecified -or- create:*

Choose the firewall zone you want to assign to this

Click SAVE and APPLY
Connect ETH1 to WAN port

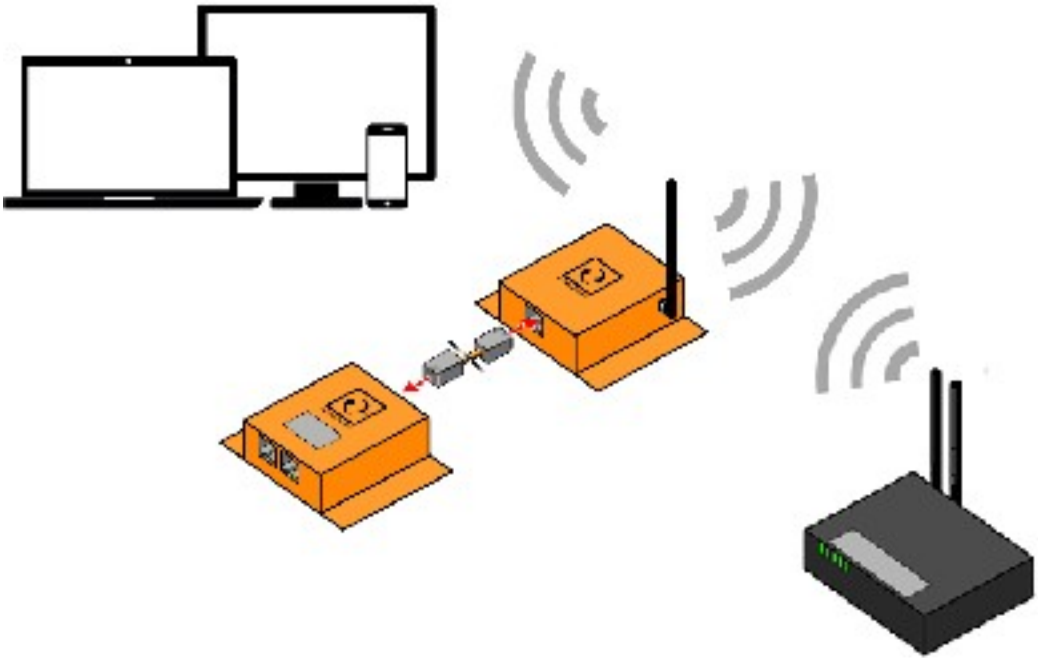
Internet connection will be available on ETH0

As an access point

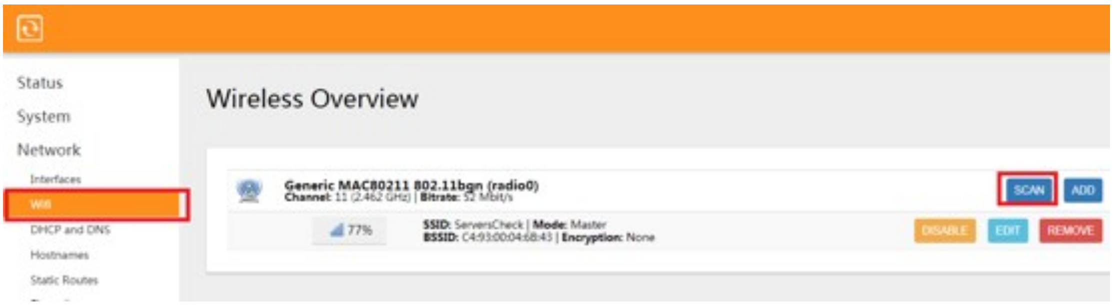


Do steps 1 to 12 from Wireless Router configuration (section 9.1.7)
Connect ETH1 to any of the LAN port of the Router
Internet connection will be available on ETH0

As a Wifi client



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

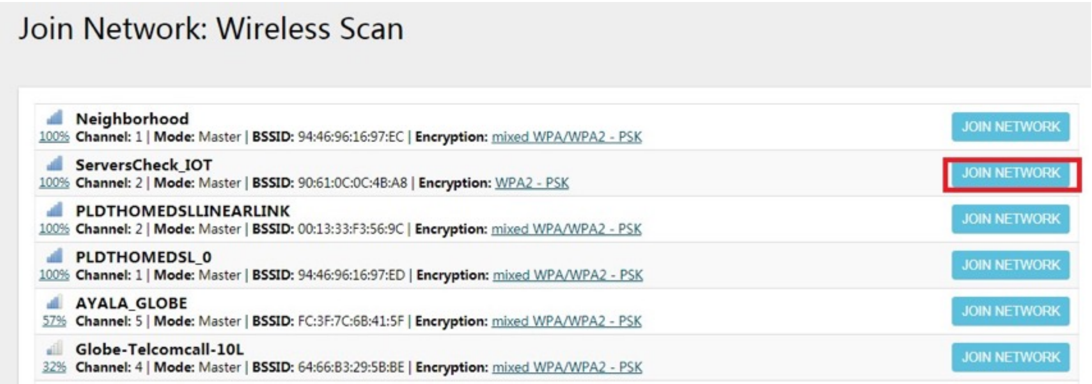


Wireless Overview

Generic MAC80211 802.11bgn (radio0)
Channel: 11 (2.462 GHz) | **Bitrate:** 52 Mbit/s

77% **SSID:** ServersCheck | **Mode:** Master
BSSID: C4:93:00:04:68:43 | **Encryption:** None

Join the desired Wifi network



Join Network: Wireless Scan

Neighborhood
100% **Channel:** 1 | **Mode:** Master | **BSSID:** 94:46:96:16:97:EC | **Encryption:** mixed WPA/WPA2 - PSK

ServersCheck_IOT
100% **Channel:** 2 | **Mode:** Master | **BSSID:** 90:61:0C:0C:4B:A8 | **Encryption:** WPA2 - PSK

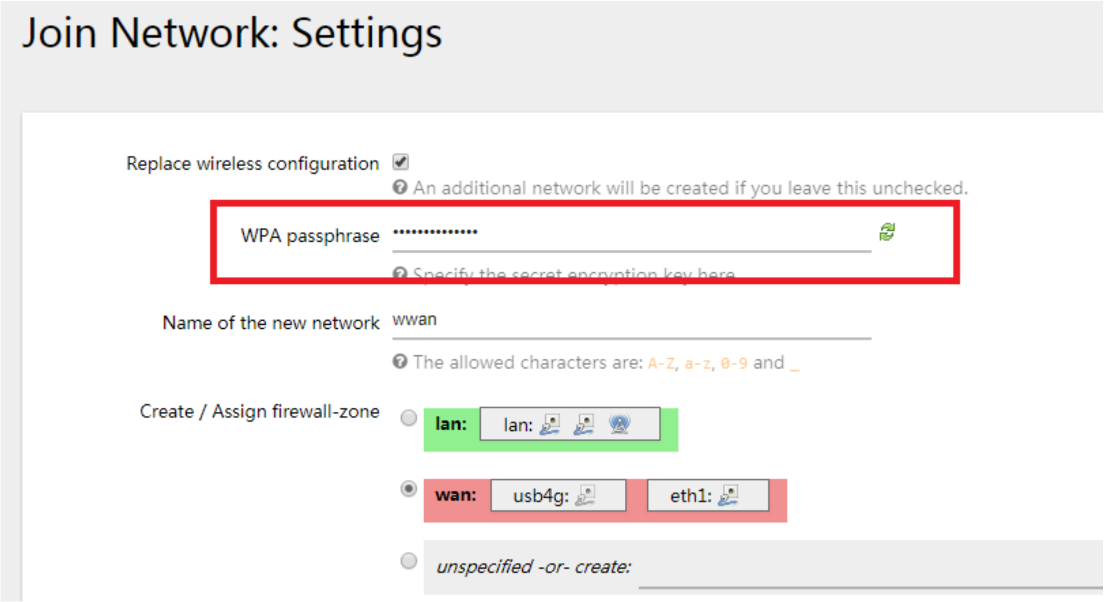
PLDTHOMEDSLLINEARLINK
100% **Channel:** 2 | **Mode:** Master | **BSSID:** 00:13:33:F3:56:9C | **Encryption:** mixed WPA/WPA2 - PSK

PLDTHOMEDSL_0
100% **Channel:** 1 | **Mode:** Master | **BSSID:** 94:46:96:16:97:ED | **Encryption:** mixed WPA/WPA2 - PSK

AYALA_GLOBE
57% **Channel:** 5 | **Mode:** Master | **BSSID:** FC:3F:7C:6B:41:5F | **Encryption:** mixed WPA/WPA2 - PSK

Globe-Telcomcall-10L
32% **Channel:** 4 | **Mode:** Master | **BSSID:** 64:66:B3:29:5B:BE | **Encryption:** mixed WPA/WPA2 - PSK

Type the password for the Wifi network and uncheck the “replace wireless configuration”



Join Network: Settings

Replace wireless configuration ☑

An additional network will be created if you leave this unchecked.

WPA passphrase ••••••••••••••

Specify the secret encryption key here

Name of the new network wwan

The allowed characters are: A-Z, a-z, 0-9 and _

Create / Assign firewall-zone

○ lan: lan:

● wan: usb4g: eth1:

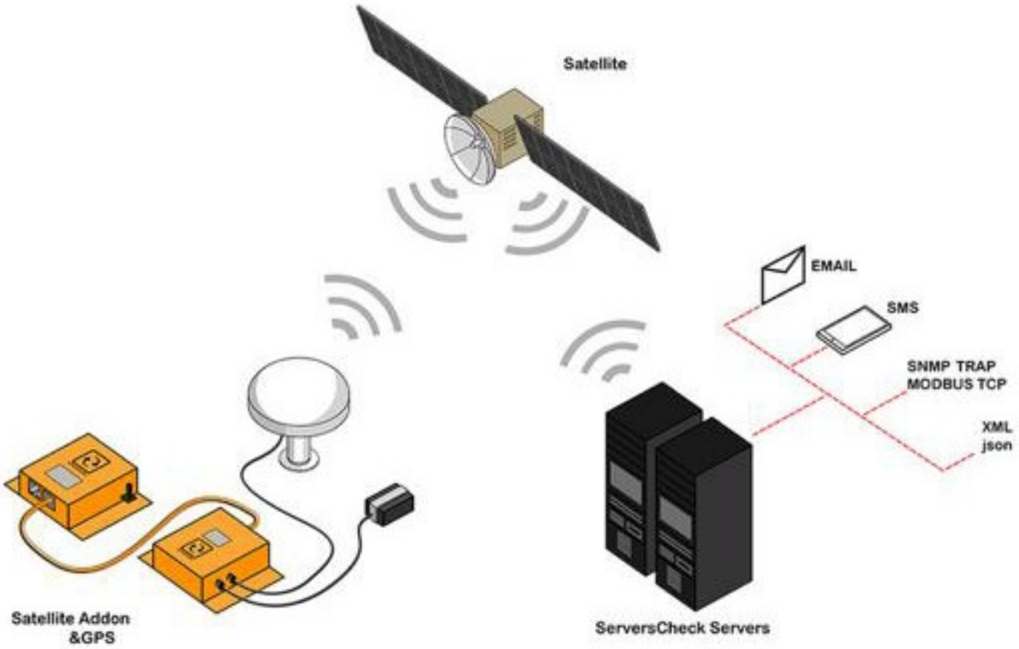
○ unspecified -or- create:

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.

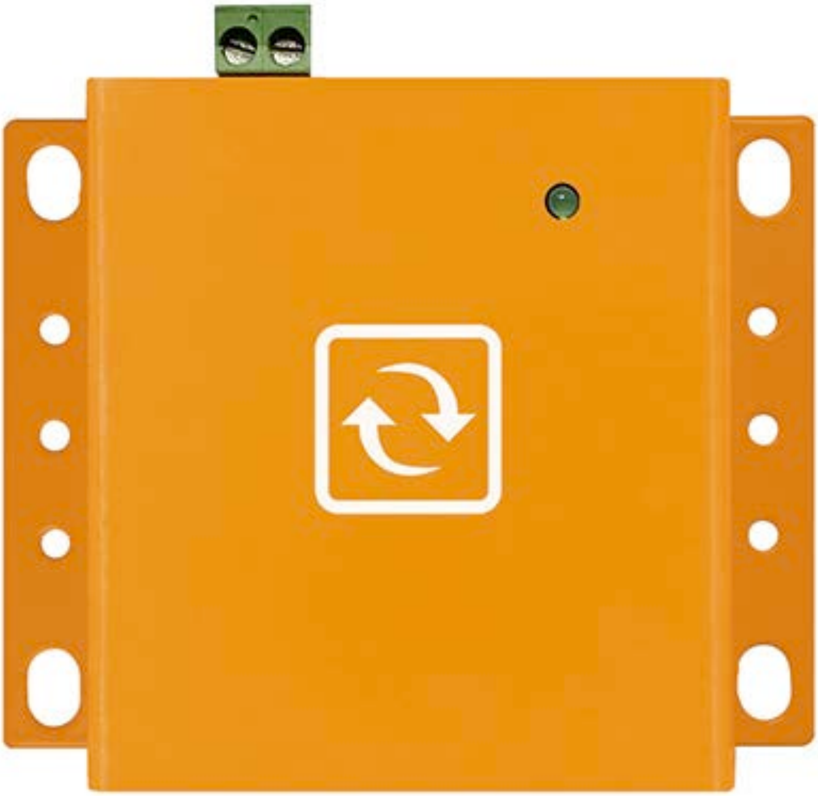
8.2 Satellite Communication Add-On (ADDON-SATELLITE)

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.

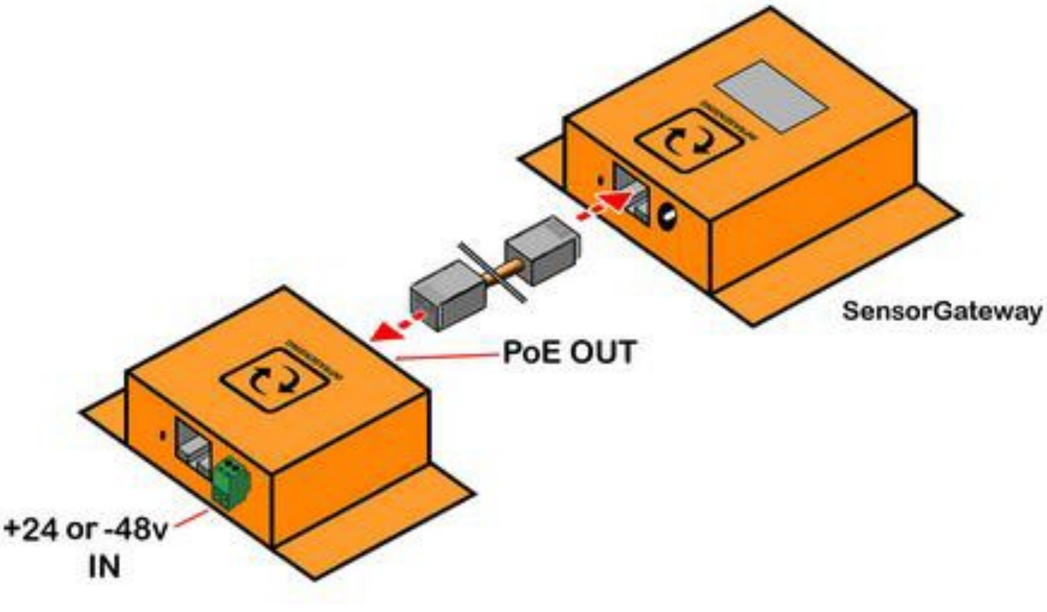


In order to use the add-on a monthly subscription through InfraSensing is required to connect the device onto the satellite network. Credits are required per message sent or received by the Base Unit

8.3 Industrial PoE+ Injectors +24 or -48v (ADDON-POE-24 / ADDON-POE-48)



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.



8.4 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:

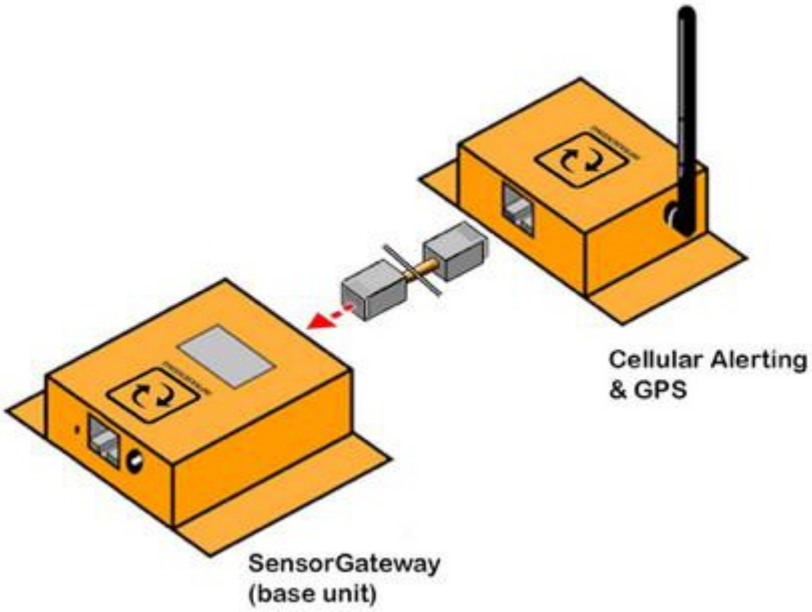
Carrier approvals: Deutsche Telekom(Europe), AT&T/Sprint/U.S. Cellular (North America), Telus (Canada)

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:

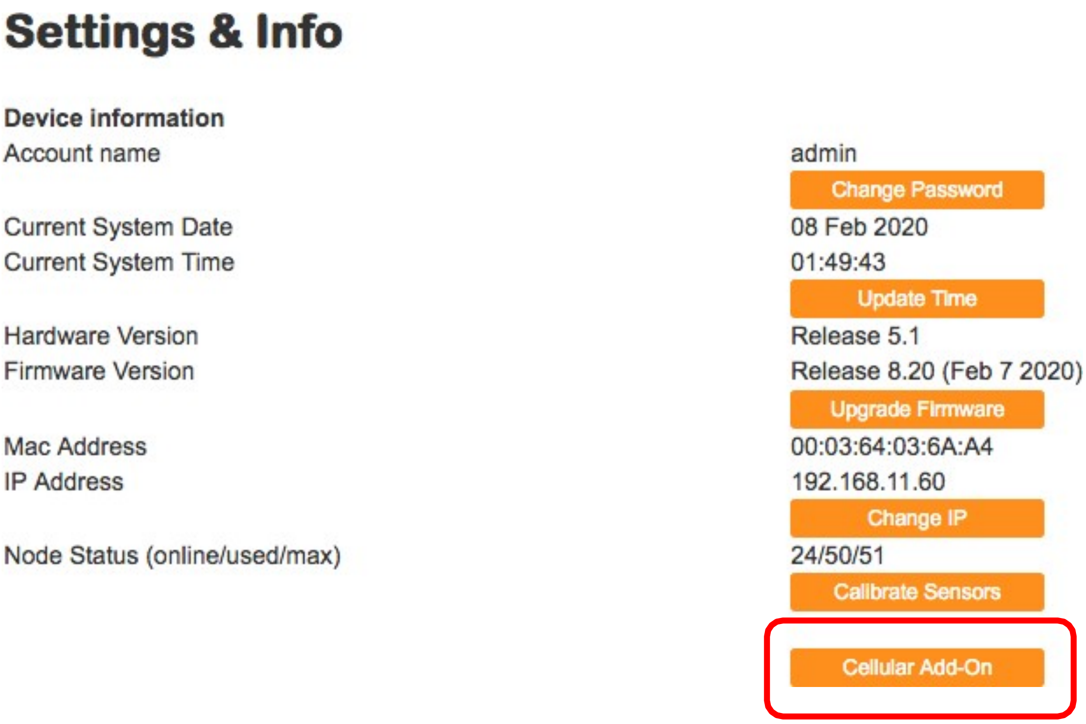
The LTE add-on currently does not support cloud data upload and will automatically disable the cloud option when connected.

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.



8.4.1 GUI of the ADDON-LTE

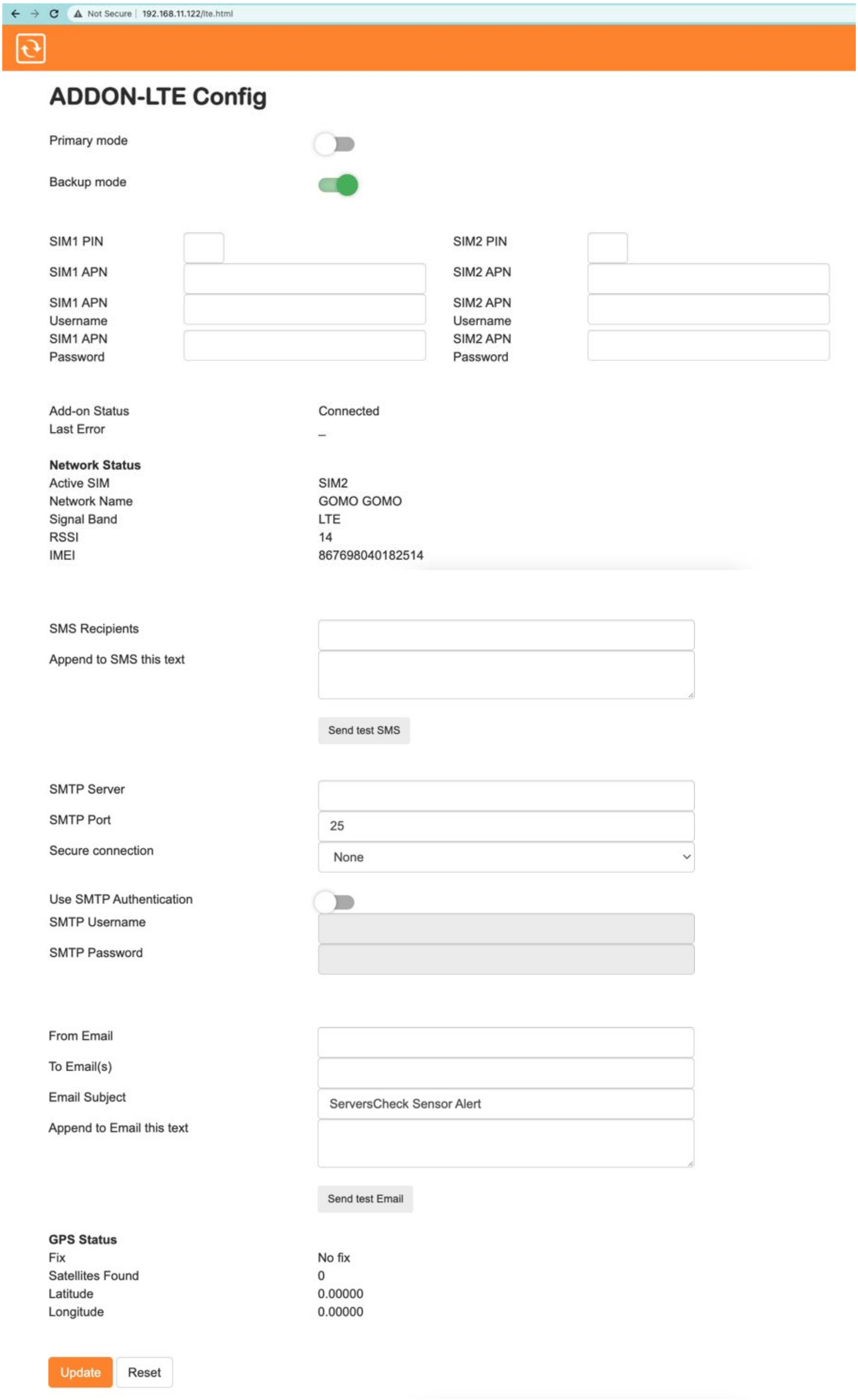
To access the ADDON set up, login to your base unit and go to settings, under settings click Cellular Add-On



Settings & Info

Device information

Account name	admin
	Change Password
Current System Date	08 Feb 2020
Current System Time	01:49:43
	Update Time
Hardware Version	Release 5.1
Firmware Version	Release 8.20 (Feb 7 2020)
	Upgrade Firmware
Mac Address	00:03:64:03:6A:A4
IP Address	192.168.11.60
	Change IP
Node Status (online/used/max)	24/50/51
	Calibrate Sensors
	Cellular Add-On



ADDON-LTE Config

Primary mode ○

Backup mode ●

SIM1 PIN		SIM2 PIN	
SIM1 APN		SIM2 APN	
SIM1 APN Username		SIM2 APN Username	
SIM1 APN Password		SIM2 APN Password	

Add-on Status	Connected
Last Error	–

Network Status

Active SIM	SIM2
Network Name	GOMO GOMO
Signal Band	LTE
RSSI	14
IMEI	867698040182514

SMS Recipients

Append to SMS this text

SMTP Server	
SMTP Port	25
Secure connection	None

Use SMTP Authentication ○

SMTP Username

SMTP Password

From Email	
To Email(s)	
Email Subject	ServersCheck Sensor Alert
Append to Email this text	

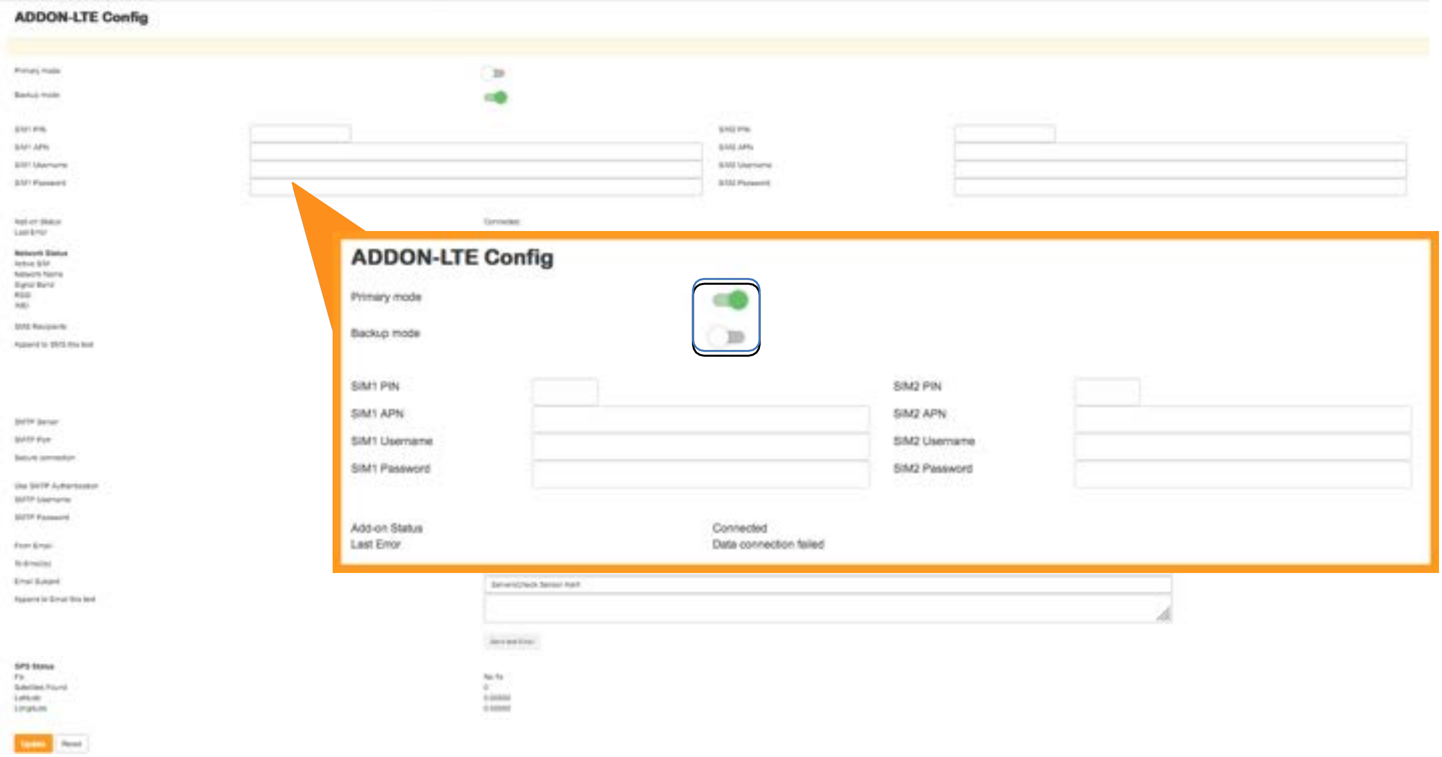
GPS Status

Fix	No fix
Satellites Found	0
Latitude	0.00000
Longitude	0.00000

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

8.4.2 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 ●

Backup mode ○

SIM1 PIN

SIM1 APN

SIM1 Username

SIM1 Password

SIM2 PIN

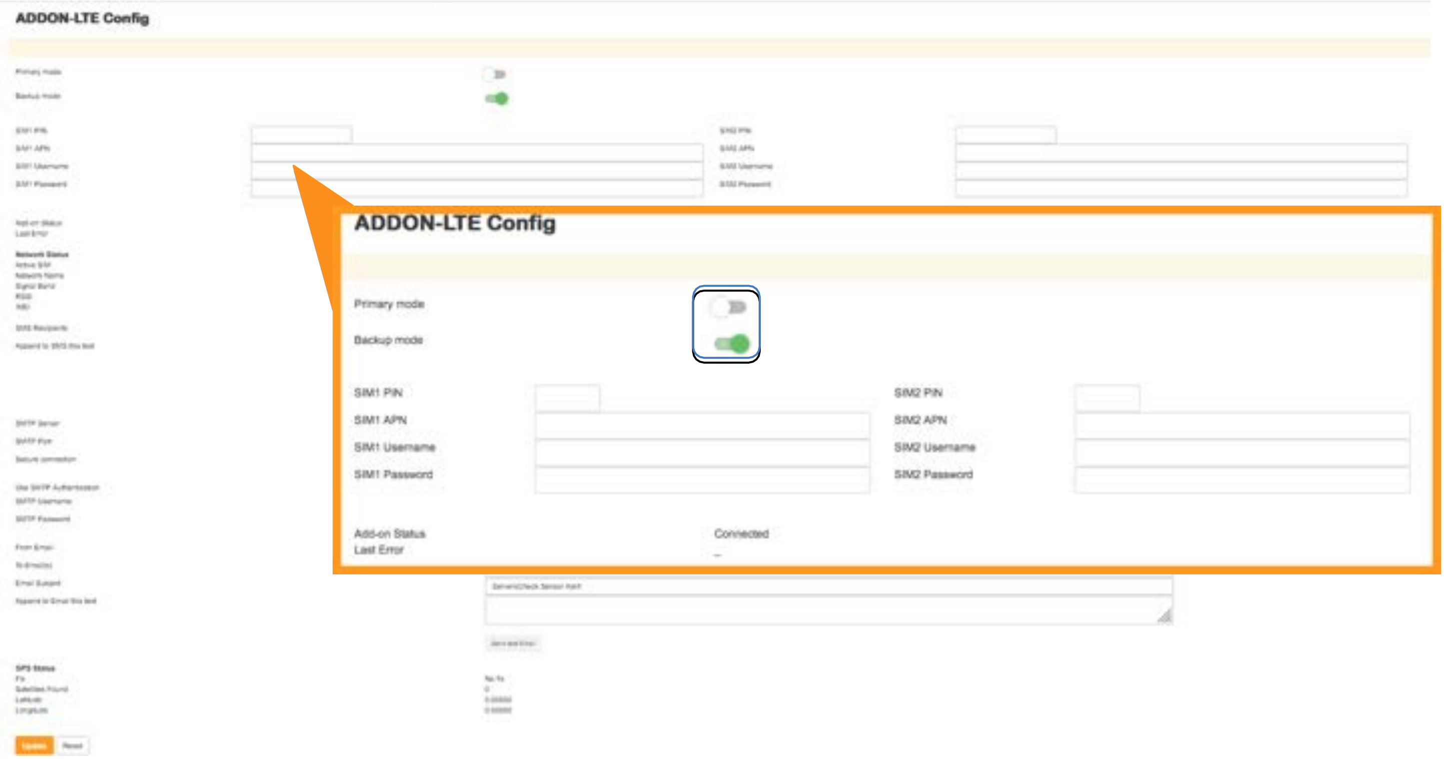
SIM2 APN

SIM2 Username

SIM2 Password

Add-on Status Connected
Last Error Data connection failed

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

Backup mode

SIM1 PIN

SIM1 APN

SIM1 Username

SIM1 Password

SIM2 PIN

SIM2 APN

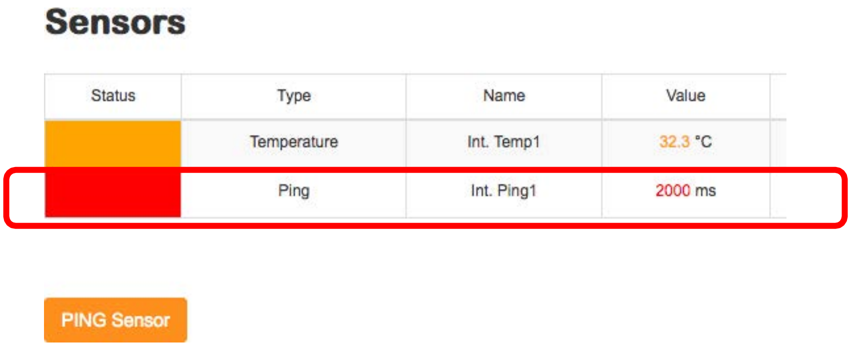
SIM2 Username

SIM2 Password

Add-on Status Connected

Last Error –

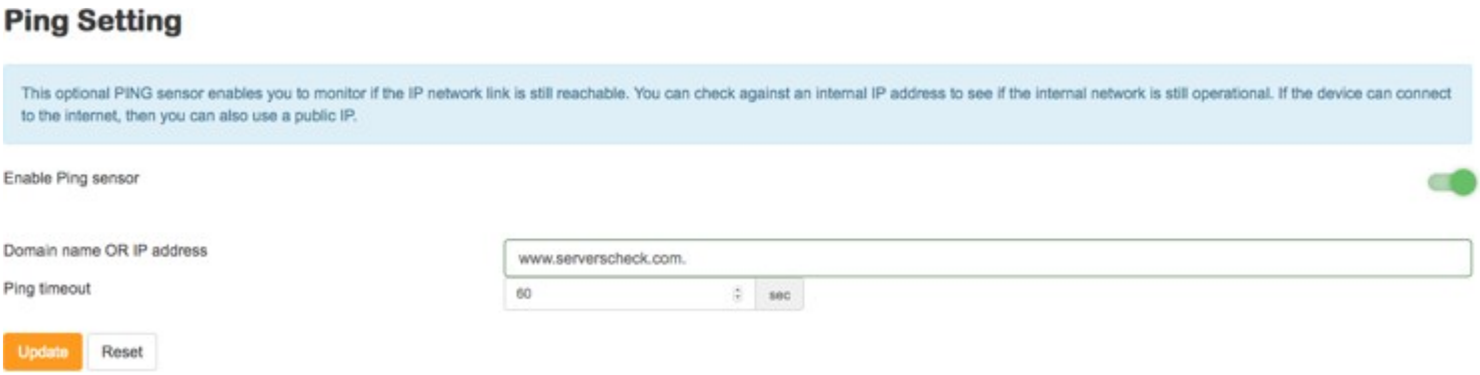
As shown on the image below the Internal ping is down, this will then signal the LTE add-on that the local network is down and will now use the SIM’s data connection to send alerts.



Sensors

Status	Type	Name	Value
🟧	Temperature	Int. Temp1	32.3 °C
🟥	Ping	Int. Ping1	2000 ms

In Backup mode, the internal Ping is required to be enabled (Ping set-up is under **Section 3.2**) 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

This optional PING sensor enables you to monitor if the IP network link is still reachable. You can check against an internal IP address to see if the internal network is still operational. If the device can connect to the internet, then you can also use a public IP.

Enable Ping sensor

Domain name OR IP address: www.serverscheck.com.

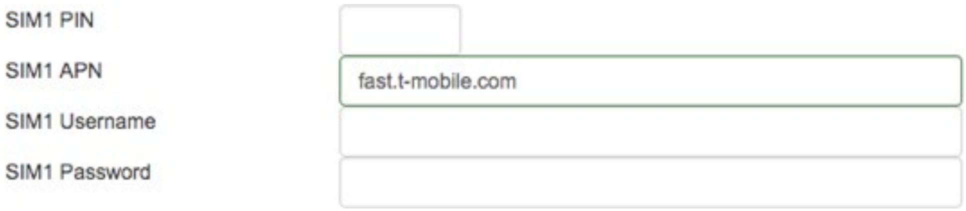
Ping timeout: 60 sec

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.

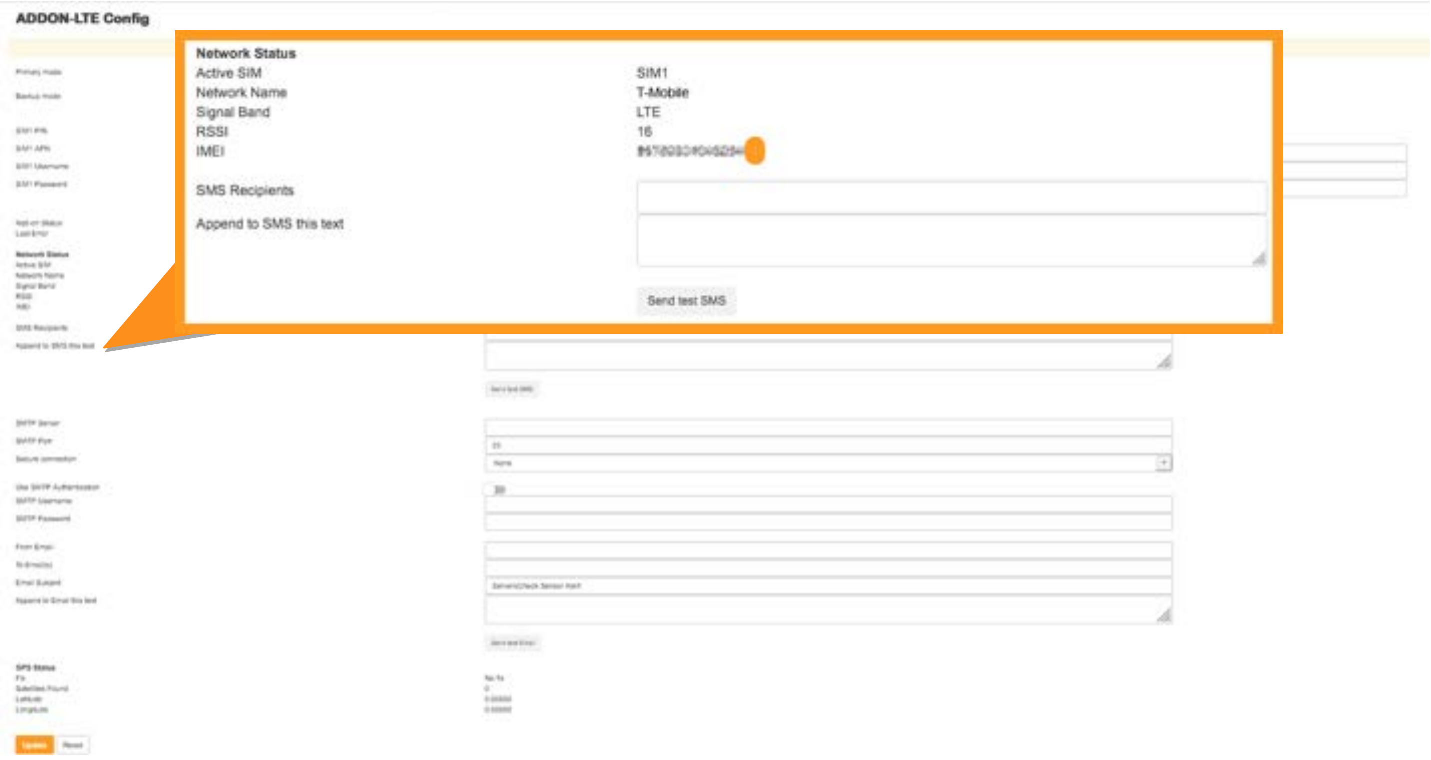
8.4.3 Setting up data connection

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.

Here is an example from T-mobile using the APN: fast.t-mobile.com (all other fields are blank since we only need the APN for T-mobile)



SIM1 PIN	
SIM1 APN	fast.t-mobile.com
SIM1 Username	
SIM1 Password	



ADDON-LTE Config

Network Status	
Active SIM	SIM1
Network Name	T-Mobile
Signal Band	LTE
RSSI	16
IMEI	[redacted]
SMS Recipients	
Append to SMS this text	

Primary mode	
Backup mode	
SIM1 PIN	
SIM1 APN	
SIM1 Username	
SIM1 Password	
Add-on Status	
Last Error	
SMTP Server	
SMTP Port	25
Secure connection	None
Use SMTP Authentication	
SMTP Username	
SMTP Password	
From Email	
To Email(s)	
Email Subject	
Append to Email this text	
GPS Status	
Fix	No fix
Satellites Found	0
Latitude	0.00000
Longitude	0.00000

We suggest performing a test mail to make sure you have data connection and that your APN is correct (see section 4.1 for test mail)

here are other known APN's (subject to change depending on provider)

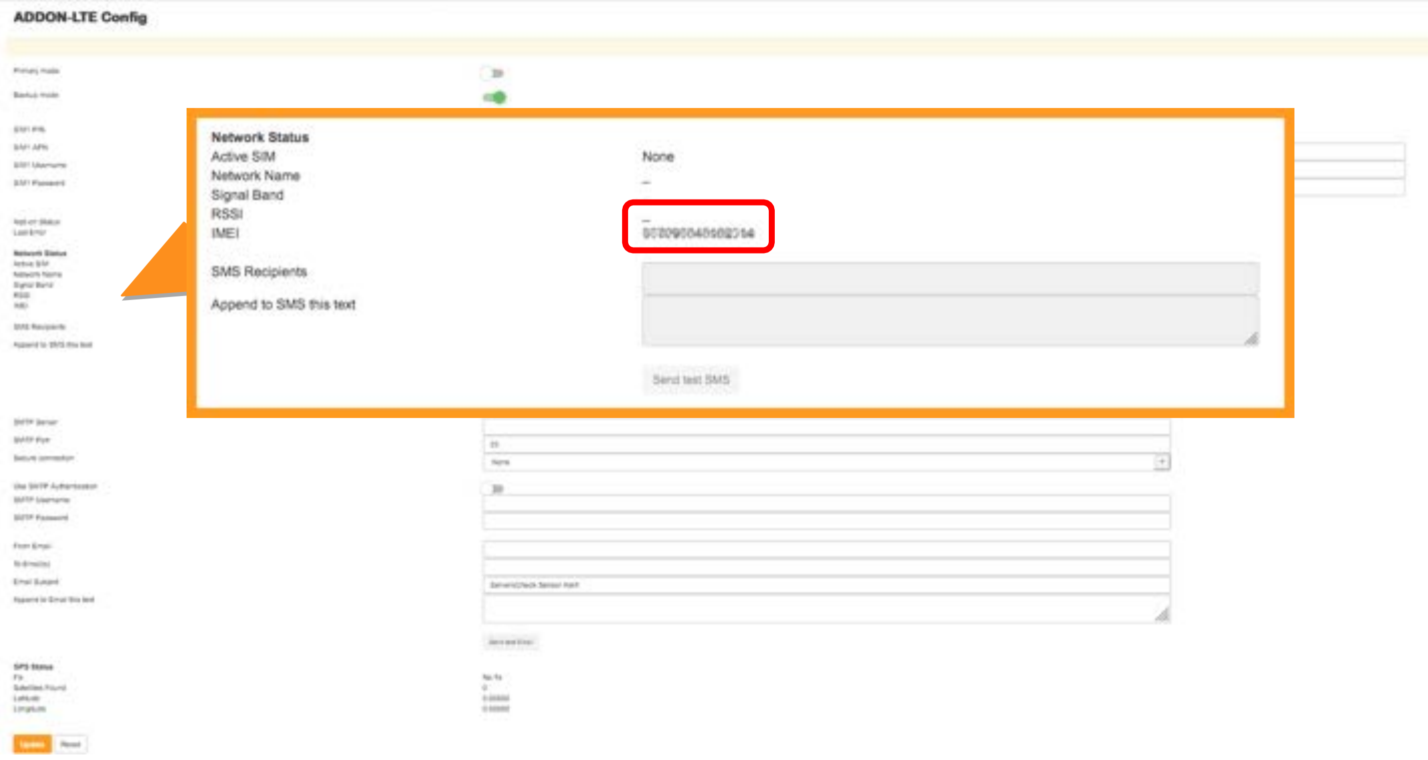
T-mobile - fast.t-mobile.com
AT&T for IoT devices - m2m.com.attz

The device has been tested to work with AT&T's network.

if you don't see your provider from the above please contact them for your APN settings

Setting up the Cellular Add-On device with AT&T

Prior to setting up, you will need a Prepaid or Postpaid ATT SIM card and the IMEI number of the device (this can be found in the lte.html page of the Base Unit, base unit).



ADDON-LTE Config

Network Status

Active SIM None

Network Name –

Signal Band

RSSI –

IMEI [illegible]

SMS Recipients

Append to SMS this text

IMEI number shown on the illustration above.

To setup the device:

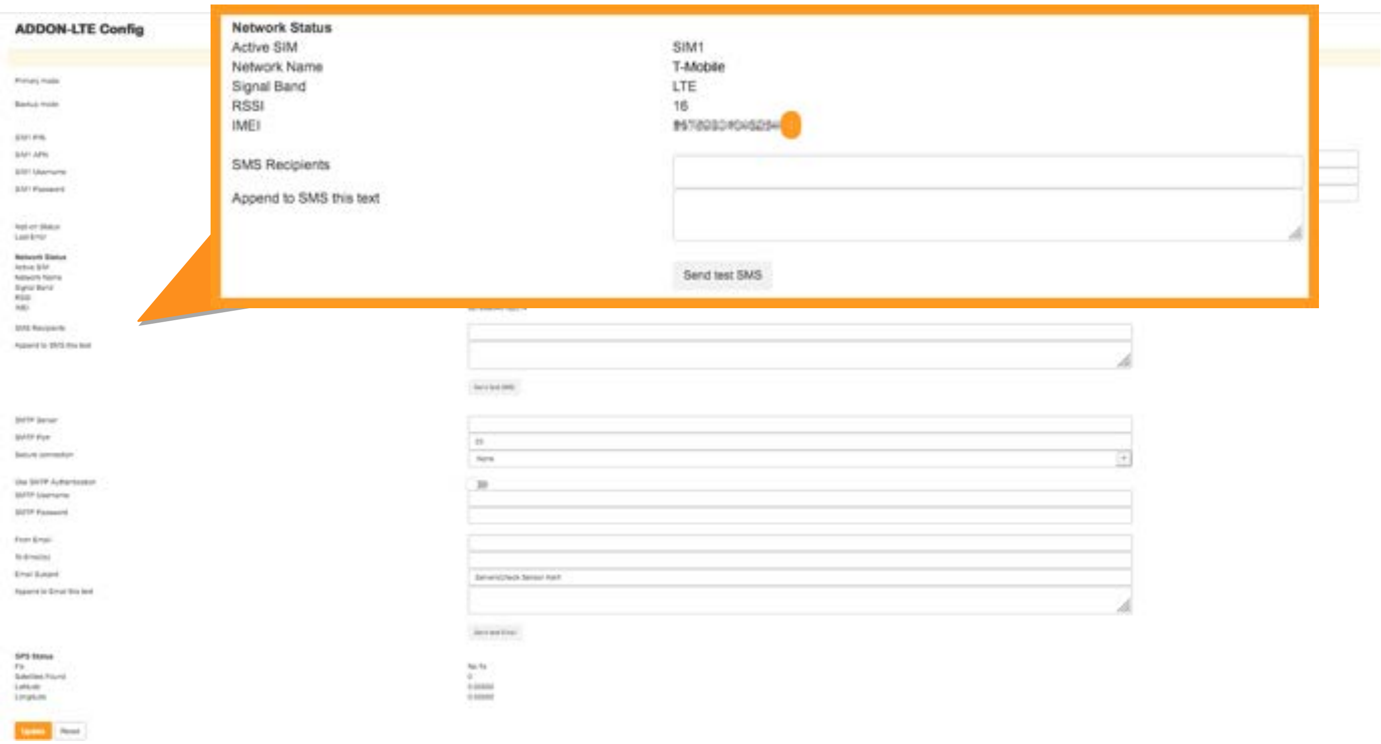
- Call AT&T to add the IMEI number to the SIM card. Any plan will work; you will not need a voice plan.
- For alerting you only need data (for email) and SMS can be purchased as an add-on.
- The IMEI number will need to be provided for the device to register on the network. You will need to tell AT&T that this is an “other” device and not a phone or modem
- Once the plan and IMEI number is associated with the SIM, ensure that the antenna is attached and to the GSM port on the addon
- Once powered up, the initial registration on the network will take longer than the subsequent power on times
- The initial startup will take between 3-5 minutes and is normal
- Once the device is registered, the OLED screen on the addon will have AT&T on the top line
- If the device does not register, power off the device, wait 60 seconds and reseat the SIM card and repeat the procedure, the registration can take up to three attempts depending on the availability of bandwidth on the network
- After registration, the subsequent power on instances will take between 45-60 seconds

Troubleshooting steps

- Ensure that the IMEI number is associated with SIM card for the plan to sync to the device
- A voice plan is not needed, it will simply need texting and data only. However, a voice plan associated will not cause any problems
- A prepaid SIM works as well as a postpaid SIM; the plan will not affect the ability for the device to work

8.4.4 SIM section

Following the data settings is the SIM information and SMS settings



ADDON-LTE Config

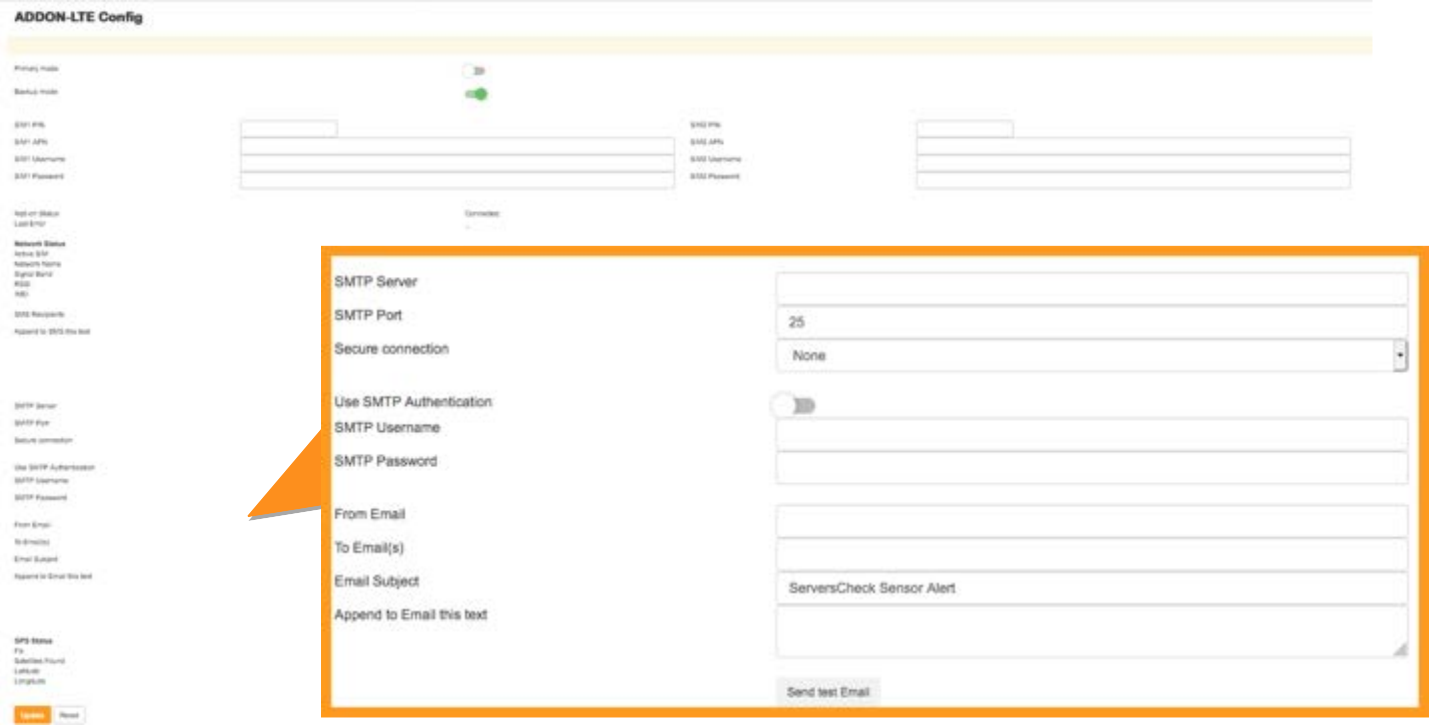
Network Status

Active SIM	SIM1
Network Name	T-Mobile
Signal Band	LTE
RSSI	16
IMEI	[redacted]
SMS Recipients	
Append to SMS this text	

See section 8.4.7 on how to insert a SIM card and foralerting, see section 3.9

8.4.5 Email section

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



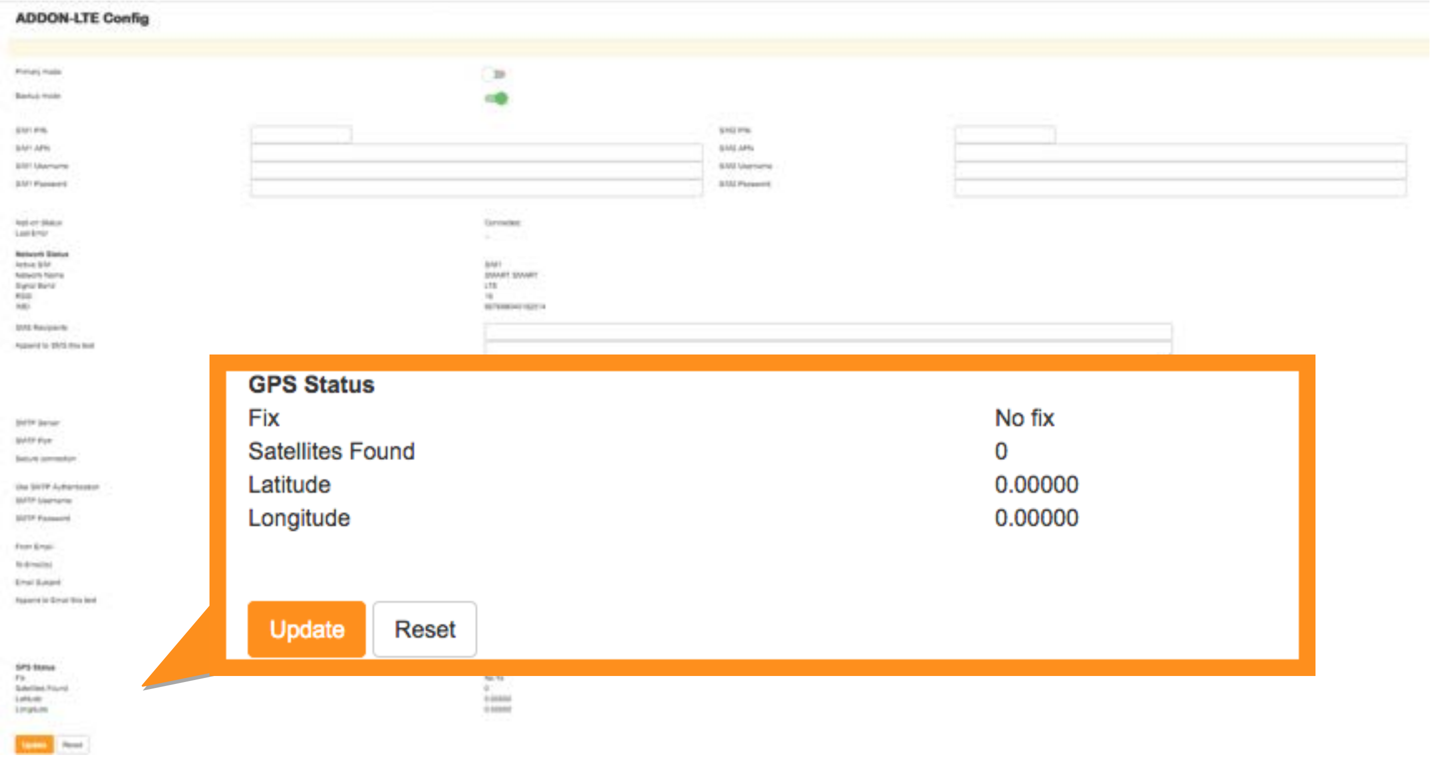
ADDON-LTE Config

SMTP Server	
SMTP Port	25
Secure connection	None
Use SMTP Authentication	
SMTP Username	
SMTP Password	
From Email	
To Email(s)	
Email Subject	ServersCheck Sensor Alert
Append to Email this text	

8.4.6 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

SIM1 PIN
SIM1 APN
SIM1 Username
SIM1 Password

SIM2 PIN
SIM2 APN
SIM2 Username
SIM2 Password

Add-on Status	Connected
Last Error	-
Network Status	
Active SIM	SIM1
Network Name	SMART SMART
Signal Band	LTE
RSSI	16
IMEI	[illegible]

SMS Recipients
Append to SMS this text

SMTP Server
SMTP Port
Secure connection

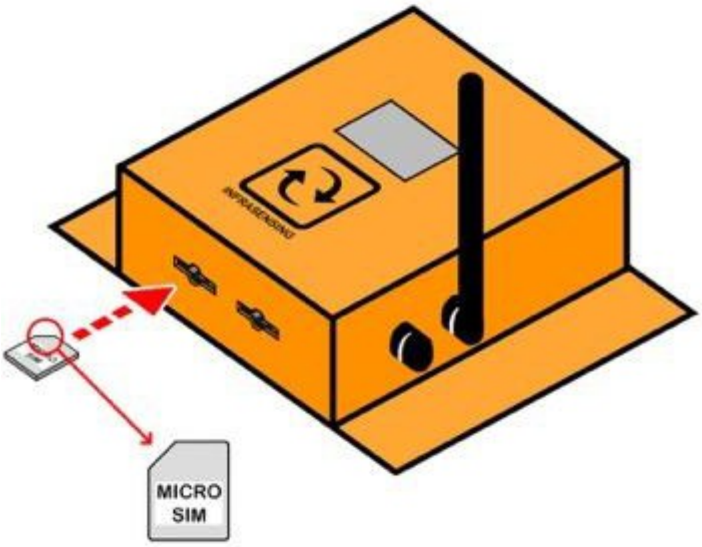
Use SMTP Authentication
SMTP Username
SMTP Password

From Email
To Email(s)
Email Subject
Append to Email this text

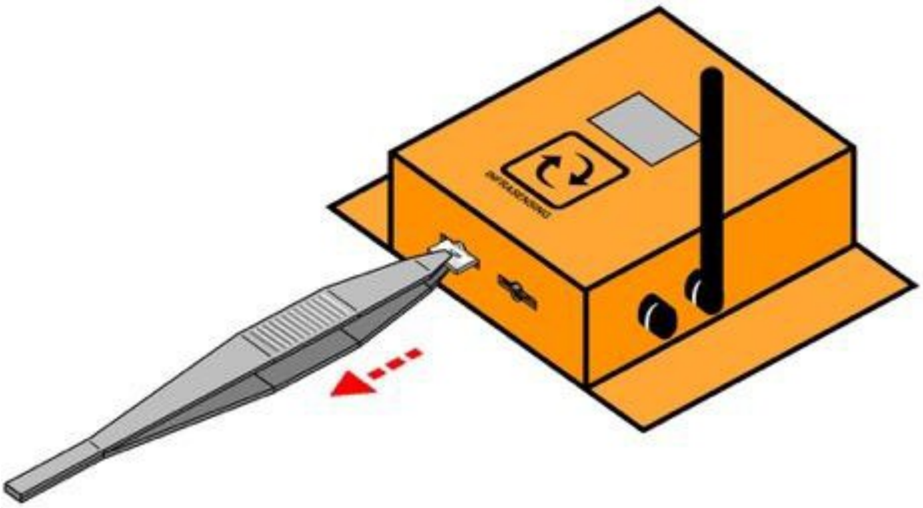
GPS Status	
Fix	No fix
Satellites Found	0
Latitude	0.00000
Longitude	0.00000

8.4.7 Inserting the SIM card into the LTE Add-On

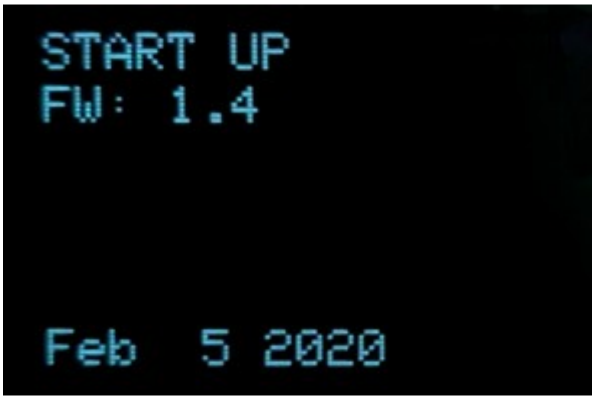
1. Insert the SIM card(s) as shown in the image below(SIM card should be inserted all the way to the back).



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

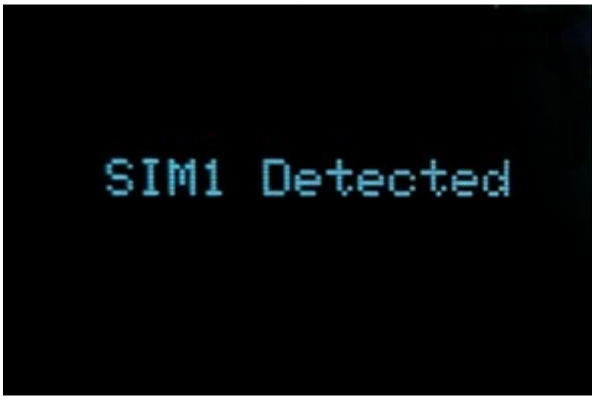


2. Connect your ADDON-LTE into your base unit, initialization will start.



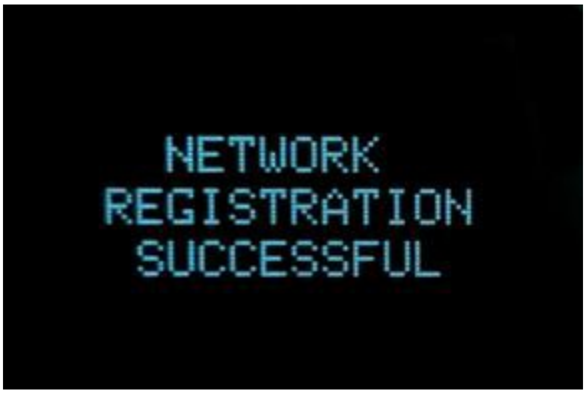
```
START UP
FW: 1.4



Feb  5 2020
```

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



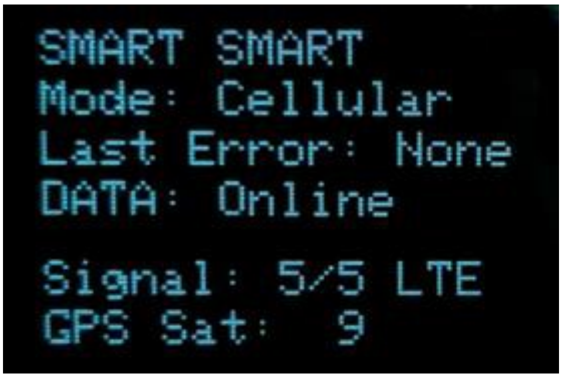
```
SIM1 Detected
```

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.



NETWORK
REGISTRATION
SUCCESSFUL

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



```
SMART SMART
Mode: Cellular
Last Error: None
DATA: Online

Signal: 5/5 LTE
GPS Sat:  9
```

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.

9 InfraSensing sensor probes

9.1 External sensor probes

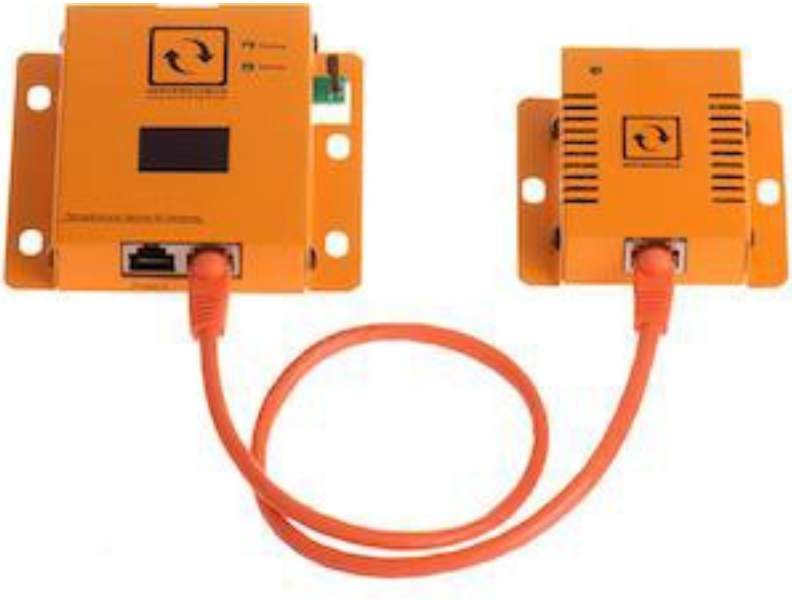
InfraSensing uses external sensor probes for its environmental monitoring solution.

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.

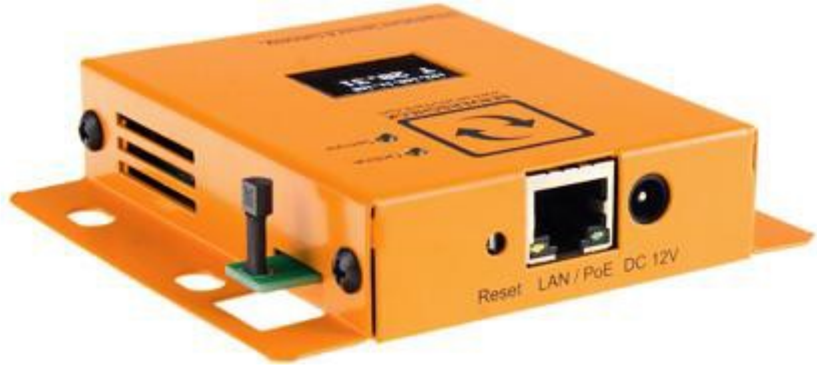
You can replace the shipped RJ45 cable with a custom standard RJ45 for a length of up to 10 meters or 33 ft between the Base Unit and an external probe. And can go longer with the use of CAT6/ CAT7 cables for up to 100m or 330 ft.

9.2 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.

10 THERMAL IMAGING SENSORS

10.1 Thermal Imaging Sensor (THIMG-XX)

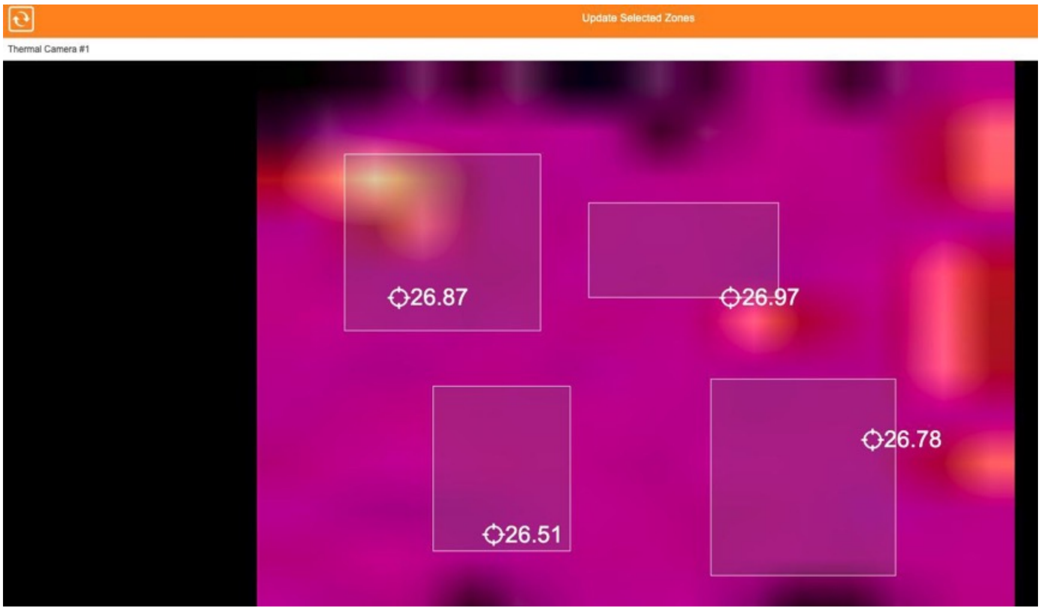
The world's first SNMP & Modbus temperature monitoring sensor that tells you what it actually sees. 192(XS), 768(S), 4800(M), or 19200(L) temperature measurement points in one image, analyzed every 2 seconds.

THIMG-(XS/S)

THIMG-(M/L)

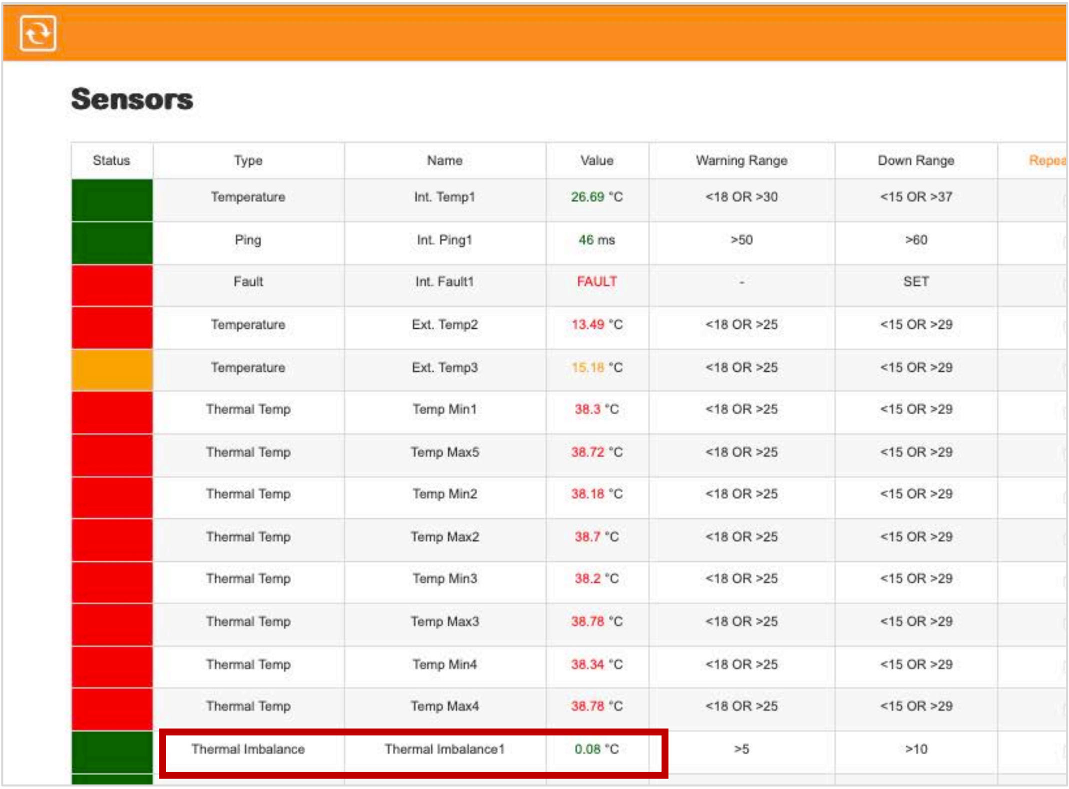
10.1.1 Installation of Thermal Image

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.



Sensors

Status	Type	Name	Value	Warning Range	Down Range	Repea
🟩	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 : https://infrasensing.com/sensors/sensor-thermal-image-temperature.asp

10.1.2 Adding Zones to the Thermal Imaging 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"

10.1.3 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"

10.2 Industrial Infrared Spot Sensor (THIMG-STD-IRSPOT)

Daisy Chain Option

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

11 Gas Sensors

11.1 Ammonia (NH3) Gas Sensor (GAS-NH3)

Measures Ammonia in the air between 0-100 ppm (parts per million).

11.2 Carbon Dioxide (CO2-NDIR) Gas Sensor (GAS-CO2-NDIR)

Measures carbon dioxide in the air between 0-5000 ppm (parts per million).

11.3 Carbon Monoxide (CO) Gas Sensor (GAS-CO)

Measures Carbon Monoxide (CO) in the air between 0 to 1000 ppm (parts per million).

11.4 Chlorine (CL2) Gas Sensor (GAS-CL2)

Measures Chlorine in the air between 0-10 ppm (parts per million).

11.5 **Ethylene (C2H4) Gas Sensor (GAS-C2H4)**

Measures Ethylene in the air between 0-100 ppm (parts per million).

11.6 **Formaldehyde (CH2O) Gas Sensor (GAS-CH2O)**

Measures Formaldehyde in the air between 0-10 ppm (parts per million).

11.7 Hydrogen (H2) Gas Sensor (GAS-H2)

Measures Hydrogen in the air between 0 to 100% LEL (lower explosive limit).

After powering the sensor through your Base Unit, the H2 sensor needs 10 minutes to warm up.

Green – _less than 10% LEL
Orange – _10-50%
Red – _50% - 100%
Magenta – _Greater than 100%

11.8 Hydrogen Chloride (HCL) Gas Sensor (GAS-HCL)

Measures Hydrogen Chloride in the air between 0-20ppm (parts per million).

11.9 **Hydrogen Fluoride (HF) Gas Sensor (GAS-HF)**

Measures Hydrogen Fluoride in the air between 0 to 10 ppm (parts per million).

11.10 **Hydrogen Sulfide (H2S) Gas Sensor (GAS-H2S)**

Measures Hydrogen Sulfide in the air between 0-100 ppm (parts per million).

11.11 **Methane (CH4) Gas Sensor (GAS-CH4)**

Measures Methane in the air between 0-100% LEL (lower explosive limit).

11.12 **Methyl Mercaptan (CH3SH) Gas Sensor (GAS-CH3SH)**

Measures Methyl Mercaptan in the air between 0-10 ppm (parts per million).

11.13 **Nitric Oxide (NO) Gas Sensor (GAS-NO)**

Measures Nitric Oxide in the air between 0-250ppm (parts per million).

11.14 **Nitrogen Dioxide (NO2) Gas Sensor (GAS-NO2)**

Measures Nitrogen Dioxide in the air between 0-20ppm (parts per million).

11.15 **Oxygen (O2) Gas Sensor (GAS-O2)**

Measures Oxygen in the air between 0-30% Vol

11.16 **Ozone (O3) Gas Sensor (GAS-O3)**

Measures Ozone in the air between 0-5 ppm (parts per million).

11.17 Phospine (PH3) Gas Sensor (GAS-PH3)

Measures Phospine in the air between 0-2000ppm (parts per million).

11.18 Sulfur Dioxide (SO2) Gas Sensor (GAS-SO2)

Measures Sulfur Dioxide in the air between 0-20ppm (parts per million).

11.19 **Sulfur Hexafluoride (SF6) Gas Sensor (GAS-SF6)**

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

11.20 **Refrigerant A1 (R-404A, R-22, and R-410A) Gas Sensor (GAS-A1)**

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

11.21 Refrigerant A2L (R-32, R-1234YF, R-1234ZE and R-454B) Gas Sensor (GAS-A2L)

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

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

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

11.23 **Refrigerant (R-134a) Gas Sensor (GAS-R134a)**

Measures Refrigerant (R-134a) in the air between 0-2000ppm (parts per million).

11.24 **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)
2. Gas sensor
3. 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.

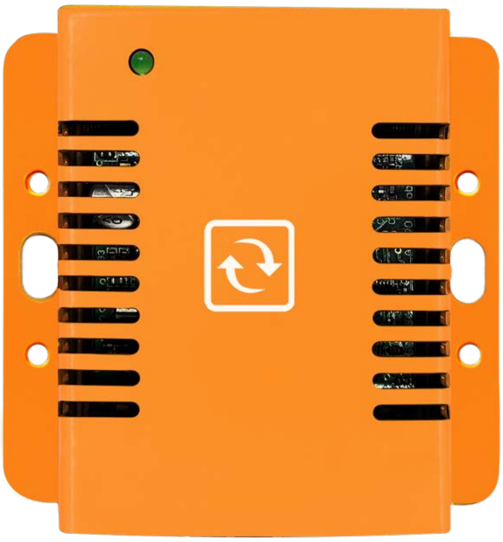
Procedure:

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.

12 Environmental Sensors

12.1 Temperature Sensor (ENV-TEMP)

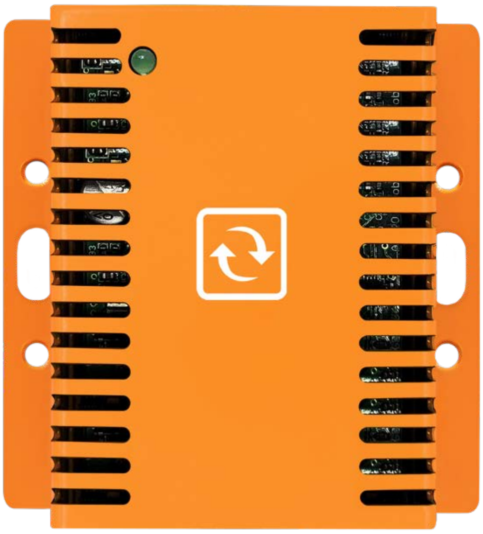
Daisy Chain Option



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

12.2 Temperature & Humidity Sensor (ENV-THUM)

Daisy Chain Option



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

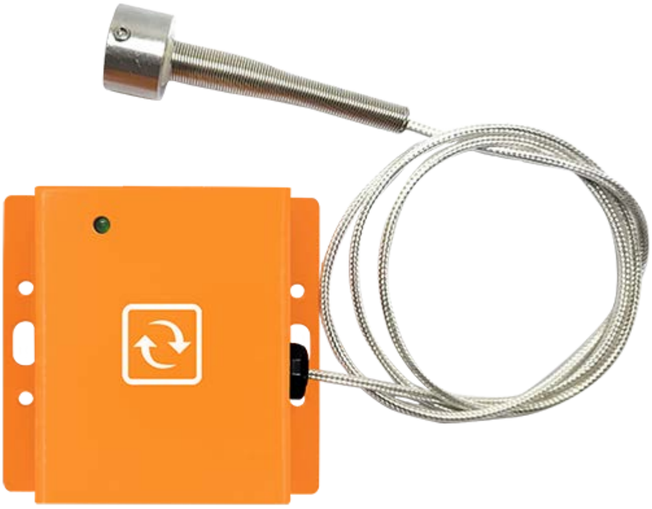
Considerations for humidity sensor:

- 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

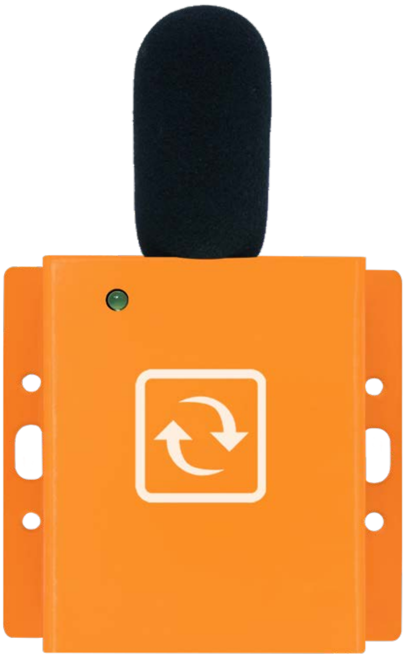
12.3 Magnetic Surface Temperature Sensor (ENV-TEMP-MAGNETIC)

Daisy Chain Option

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

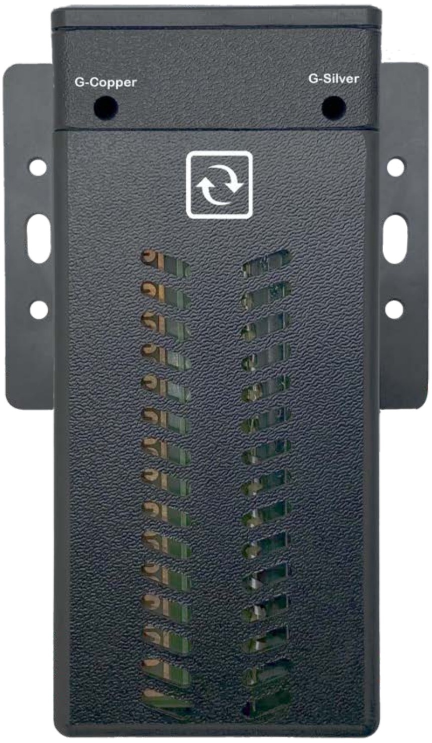


12.4 Digital Sound and Noise level Sensor(dbA) (ENV-NOISE)

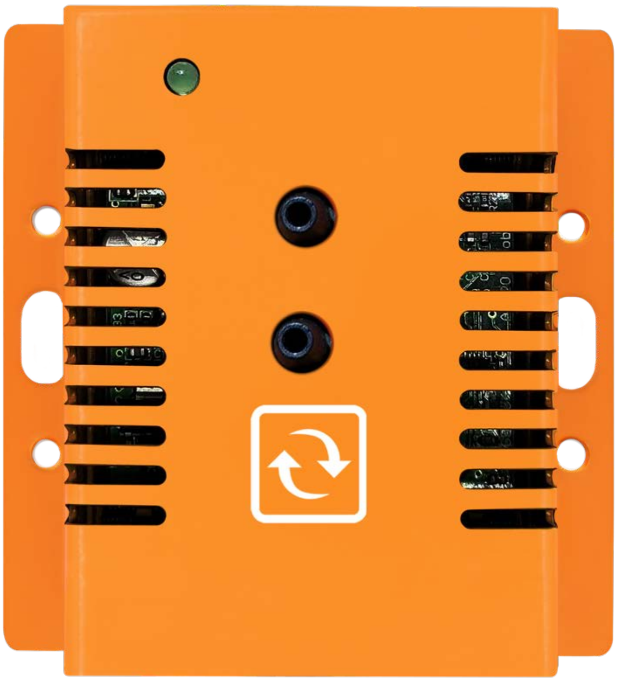


Note: Detection for ENV-NOISE Takes up to 30 seconds before appearing on your interface.

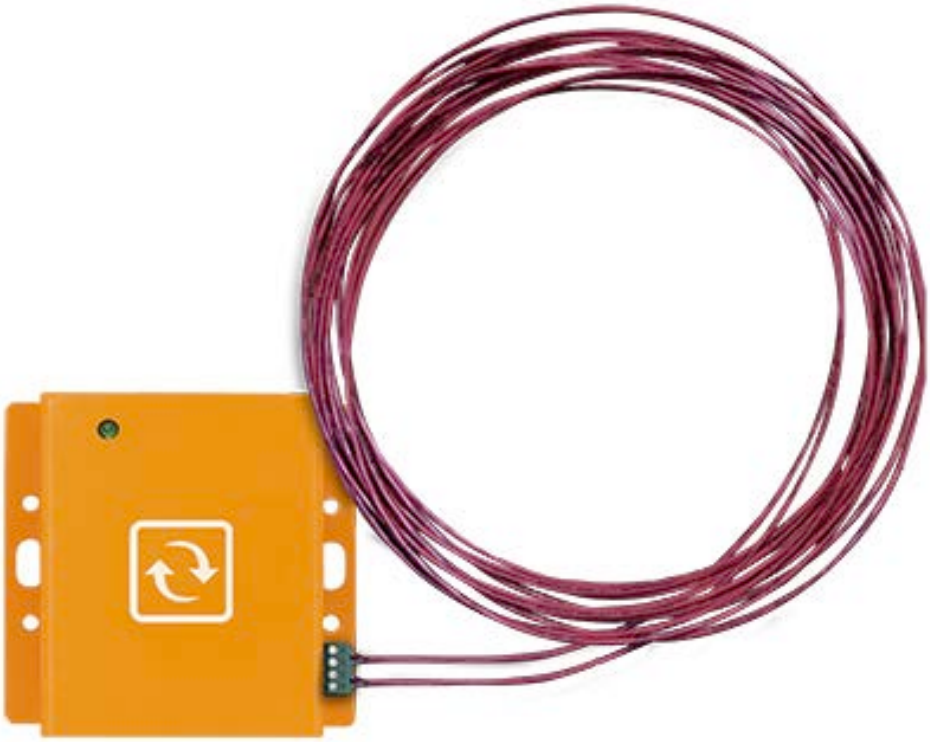
12.5 Atmospheric Corrosion Sensor (ENV-CORROSION)



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



12.7 Linear Heat Detection Sensor (ENV-LHD)



12.8 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.

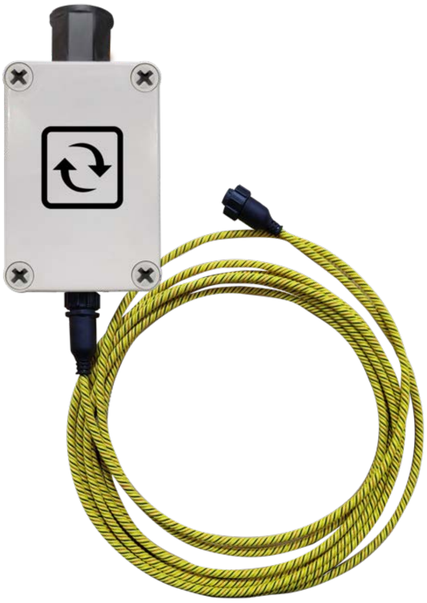
Our sensor is designed to monitor dust particles in data centers, server rooms & cabinets.

12.9 Particle Sensor (ENV-PARTICLE)

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

12.10 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)

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

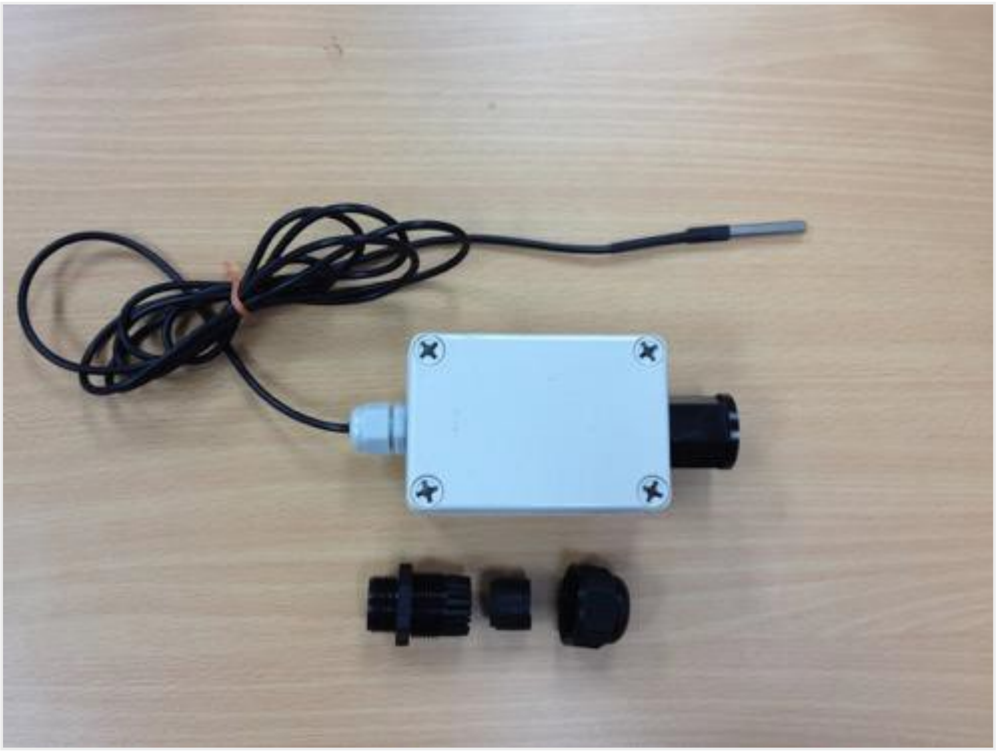
12.12 **Stainless Steel Temperature Probe (ENV-TSTAIN)**

12.13 **Extreme Low Temperature Sensor (ENV-TULTRA)**

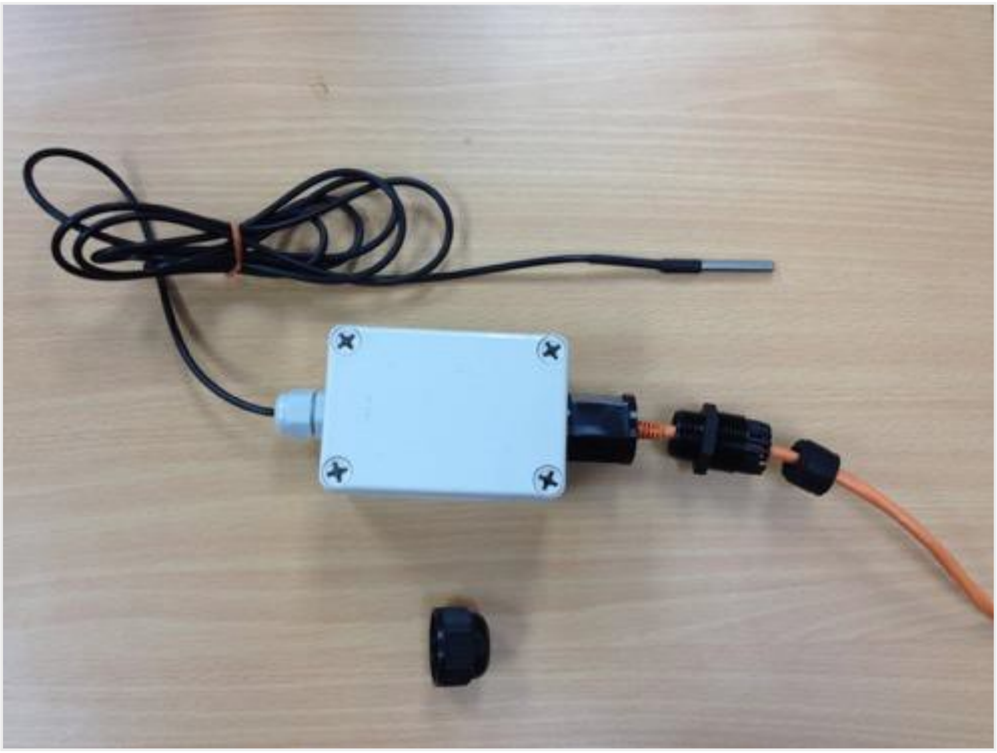
12.14 **Industrial Surface Temperature Sensor (ENV-TSURFACE)**

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

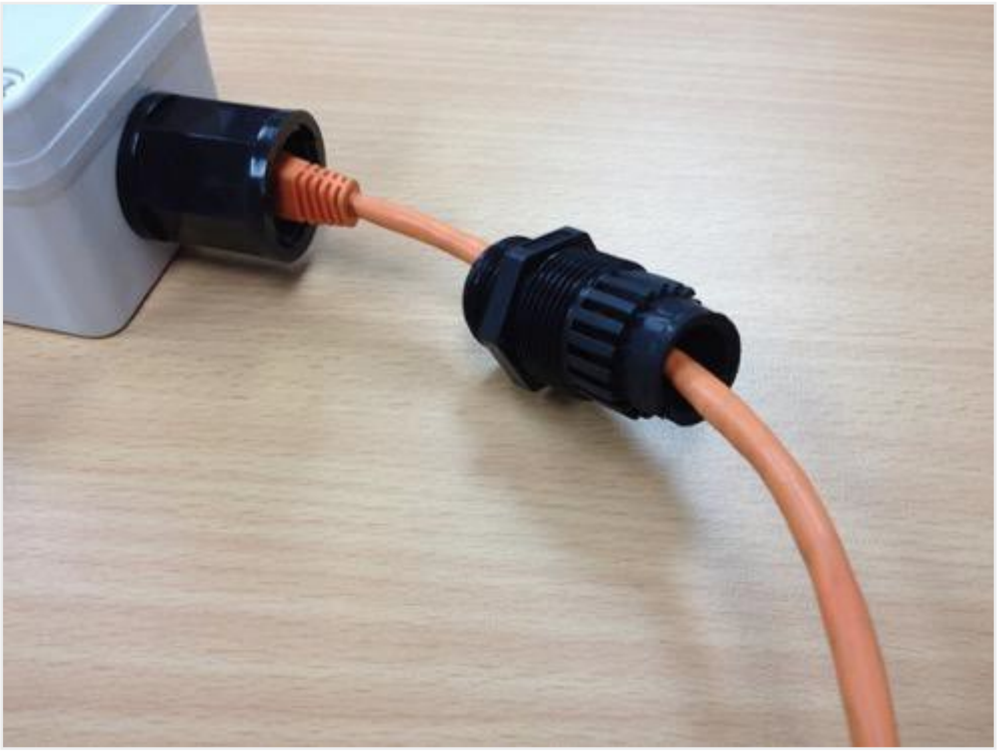
Out from the box, for the Ethernet connector, you should have the 3 parts that are yet to be assembled: the over-nut, rubber gasket, and contracting gland (from left to right).



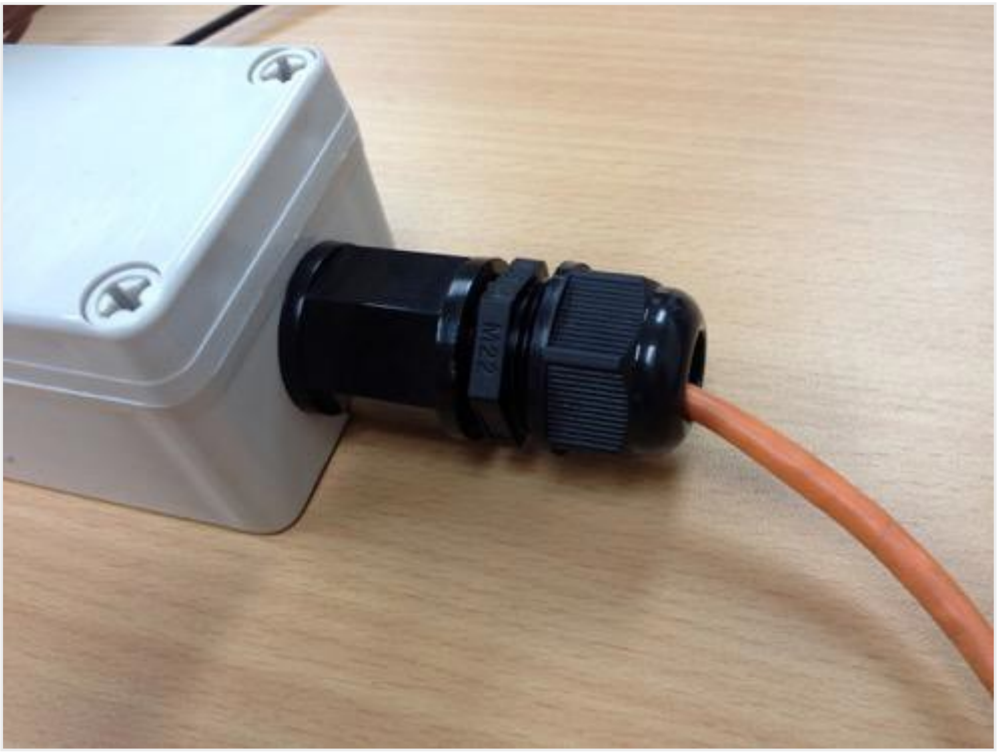
To get started, insert the over-nut and rubber gasket in your LAN cable then plug it in on the protruding RJ 45 connector from the sensor probe.



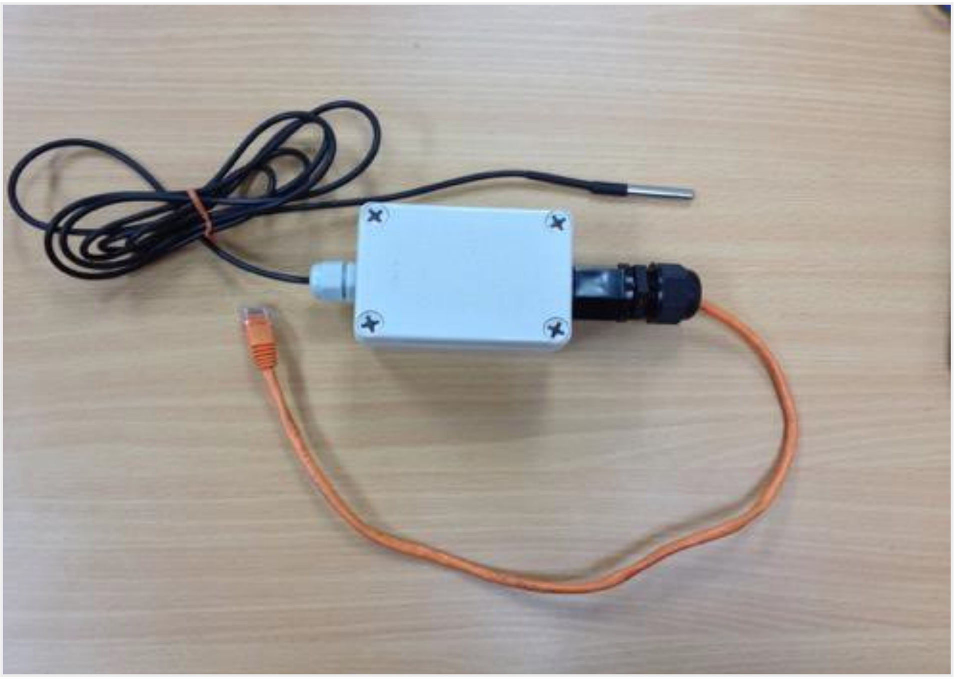
Once that's done, insert the rubber gasket all the way inside the over-nut.



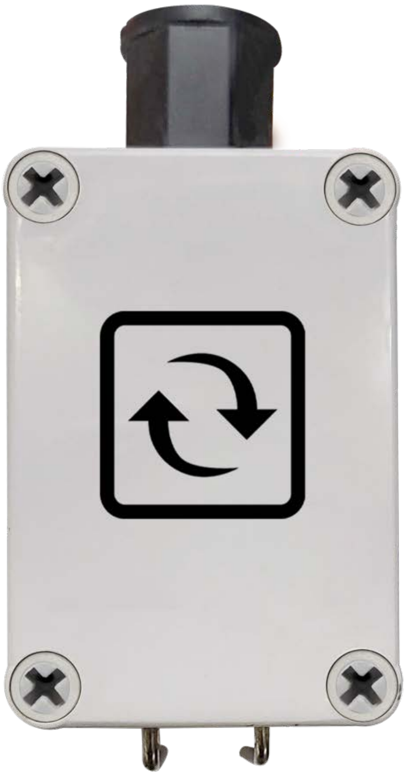
After that, connect them both on the RJ 45 connector of the sensor.



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.

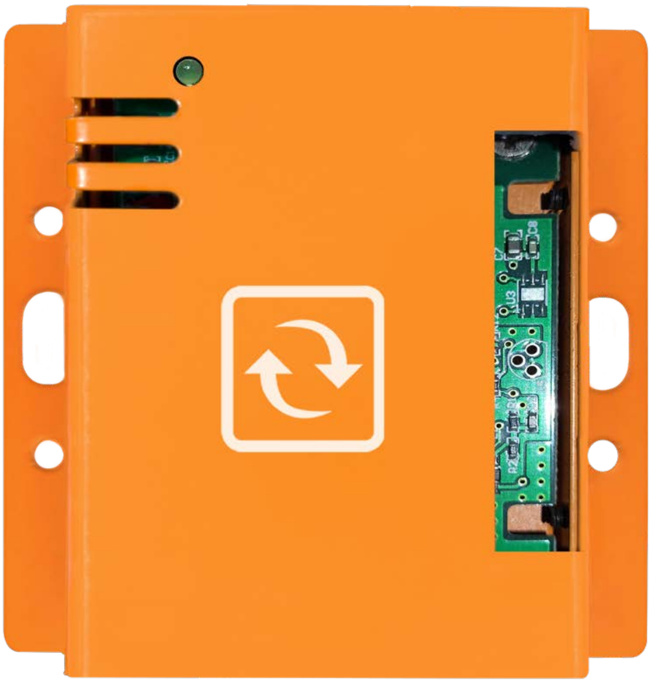


12.16 **Water Spot Detection Sensor (monitors a specific spot) (ENV-WSPOT)**

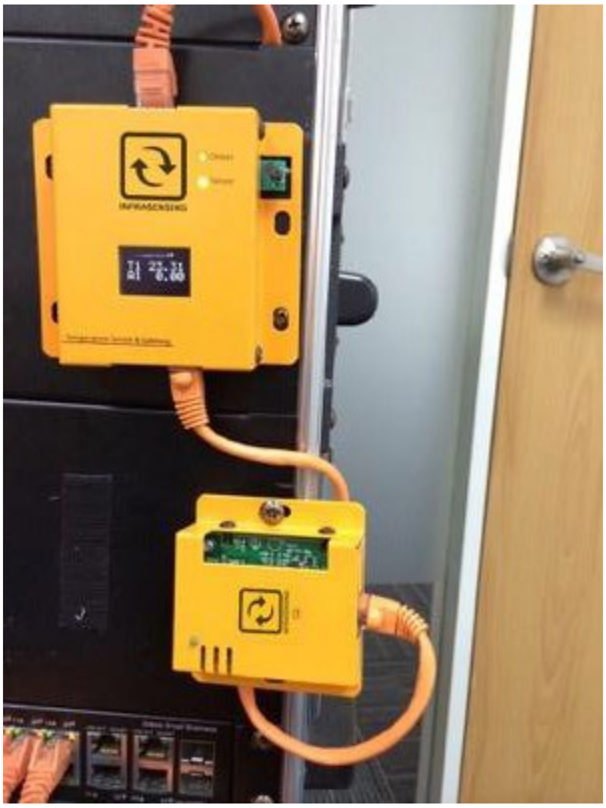


Note: Once an alert is triggered using our water spot detection sensor, make sure the metal prongs are dried before reusing.

12.17 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.

13 Daisy Chain

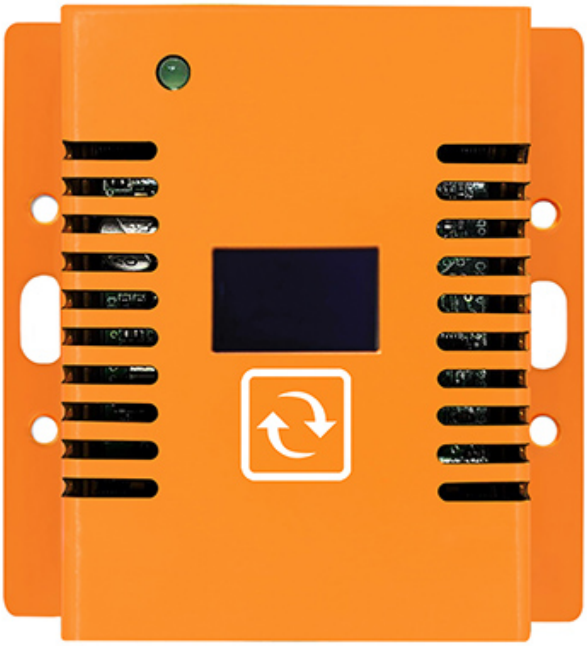
Daisy Chain Option

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 Daisy Chain Firmware

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

13.1 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:

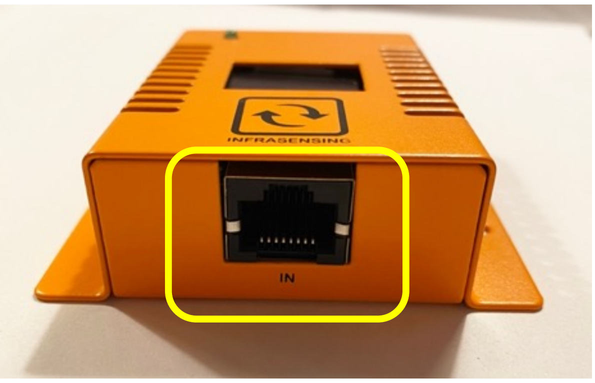
The DAISY-STARTER cannot be connected to Sensorhub (EXP-8HUB) and Multi-Sensor & Hub (EXP-4HUB)

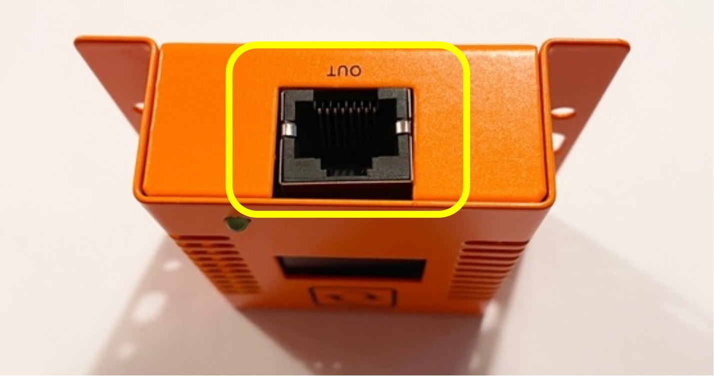
Only one DAISY-STARTER can be connected to one Base Unit (BASE-XX).

13.1.1 Connecting Daisy Chain Sensor

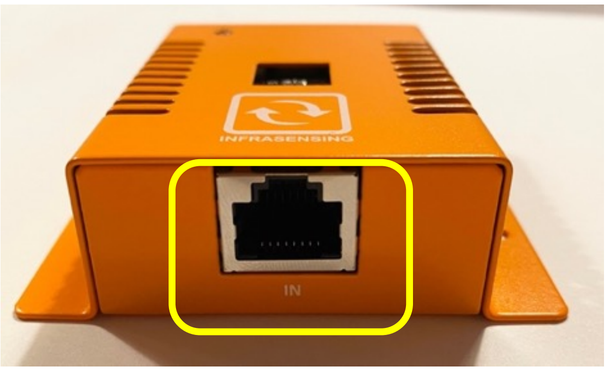
The ports on DAISY-STARTER and DAISY SENSORS are labeled **"IN"** and **"OUT"**. This is to ensure that you are connecting each device accordingly. See images below for reference.

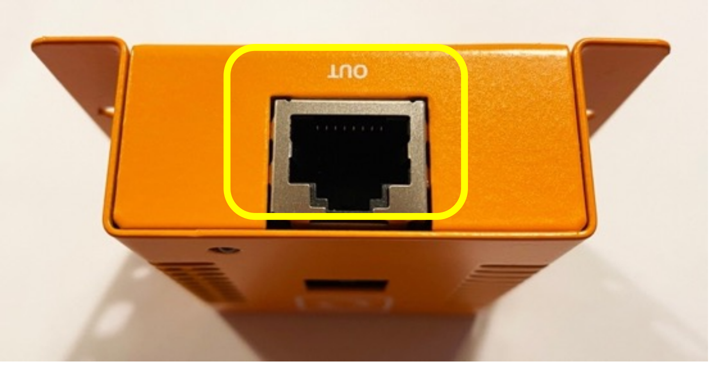
DAISY-STARTER





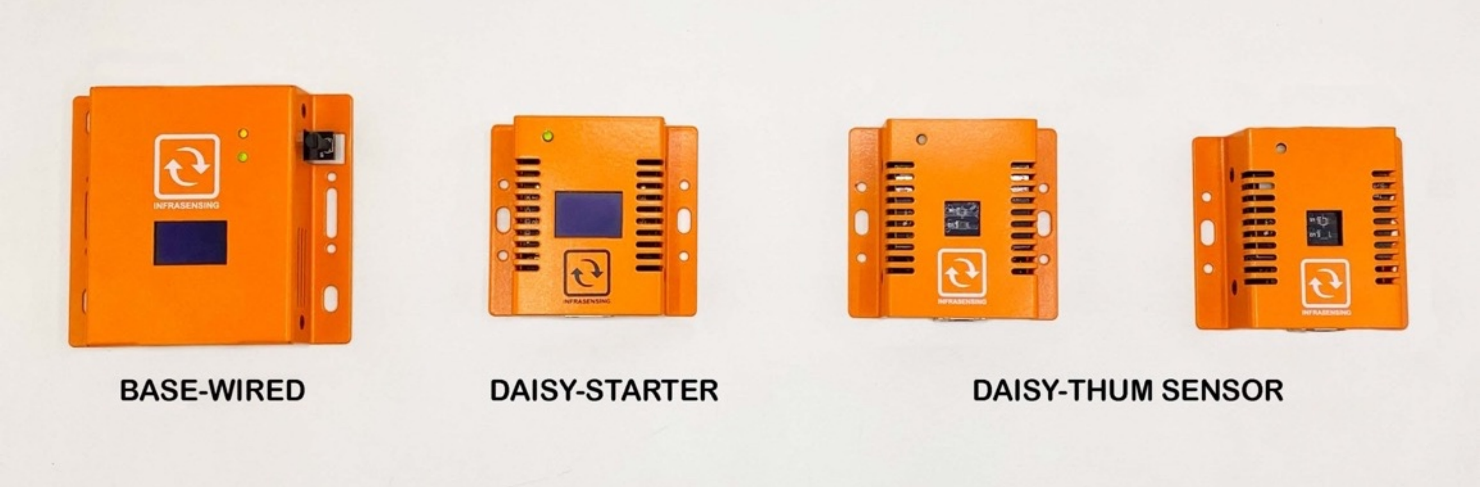
DAISY-THUM



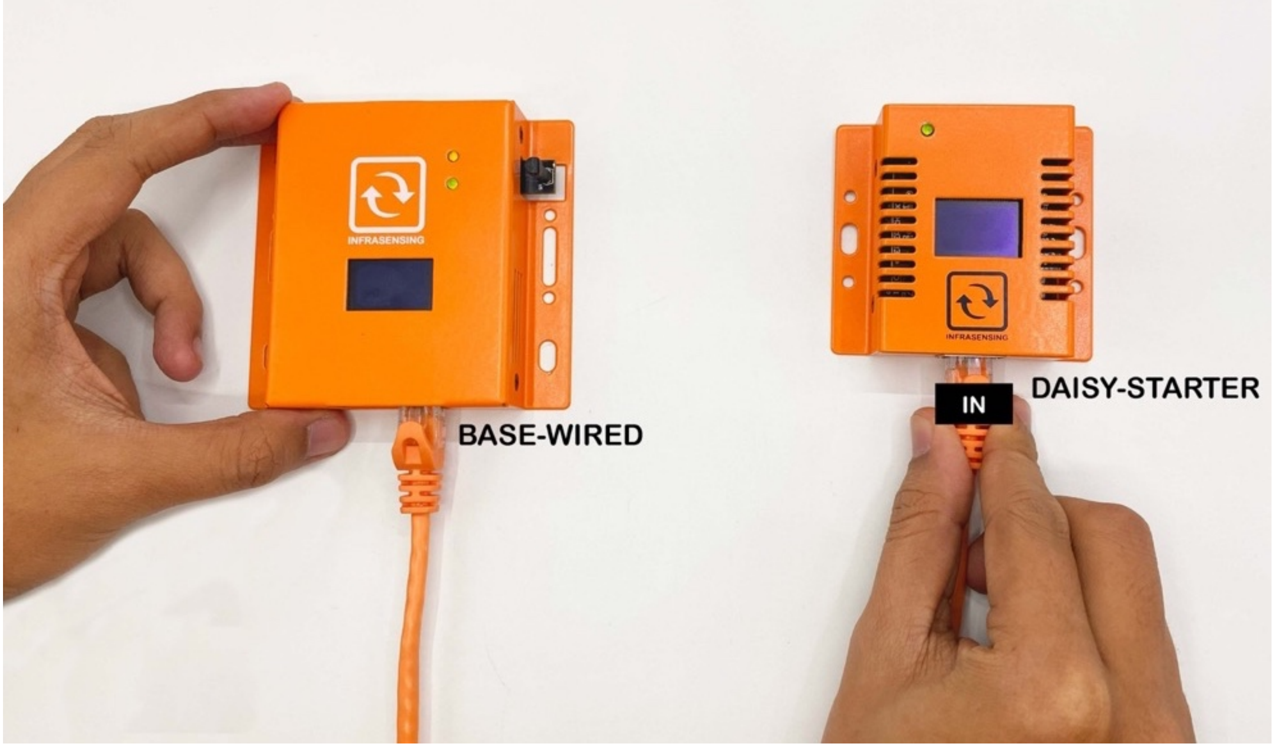


Images above shows the IN and OUT ports labeled on your sensors.

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 :

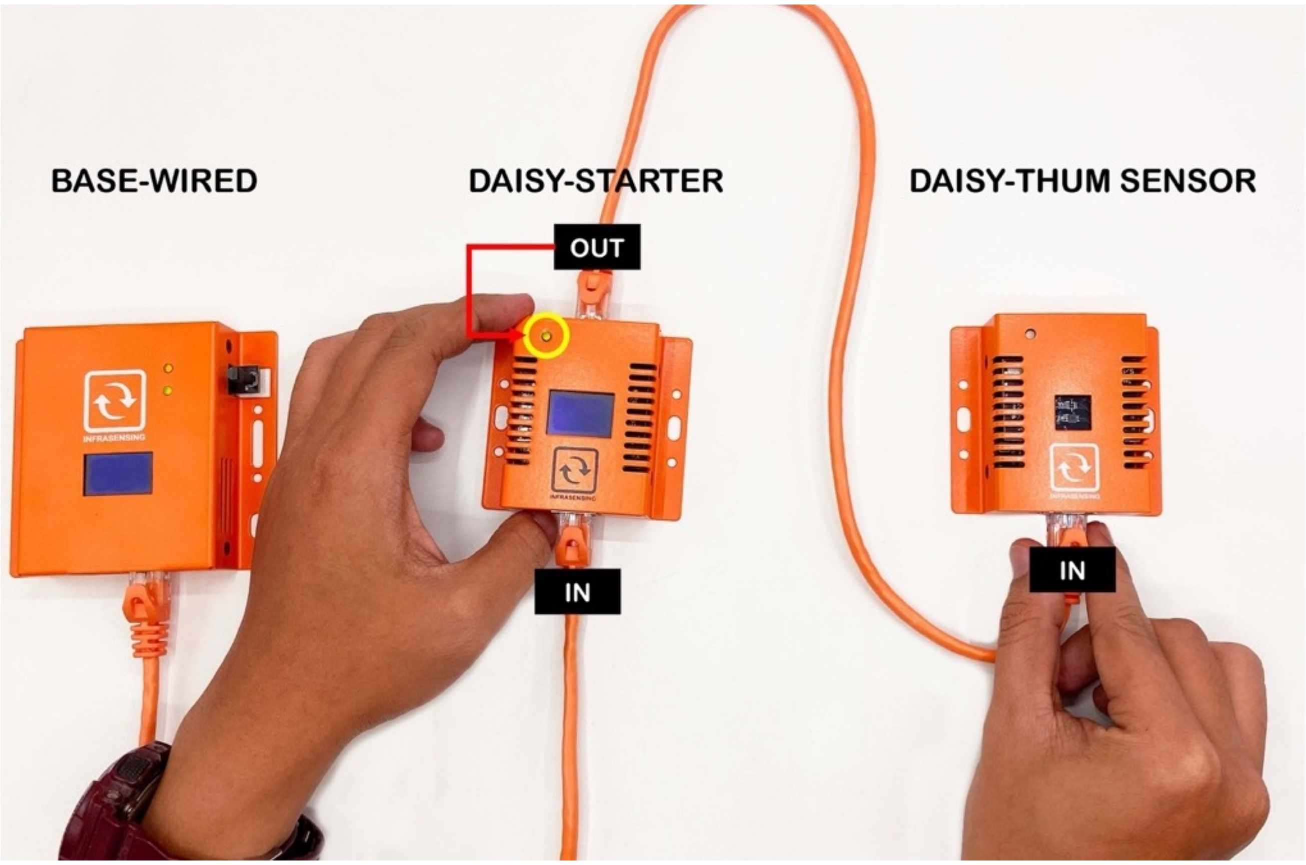


Once you have connected the BASE-XX and DAISY-STARTER, it's time to connect the DAISY-THUM sensor. Begin by locating the OUT port on the DAISY-STARTER and the IN port on the DAISY-THUM sensor. These ports are typically labeled for easy identification.

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.

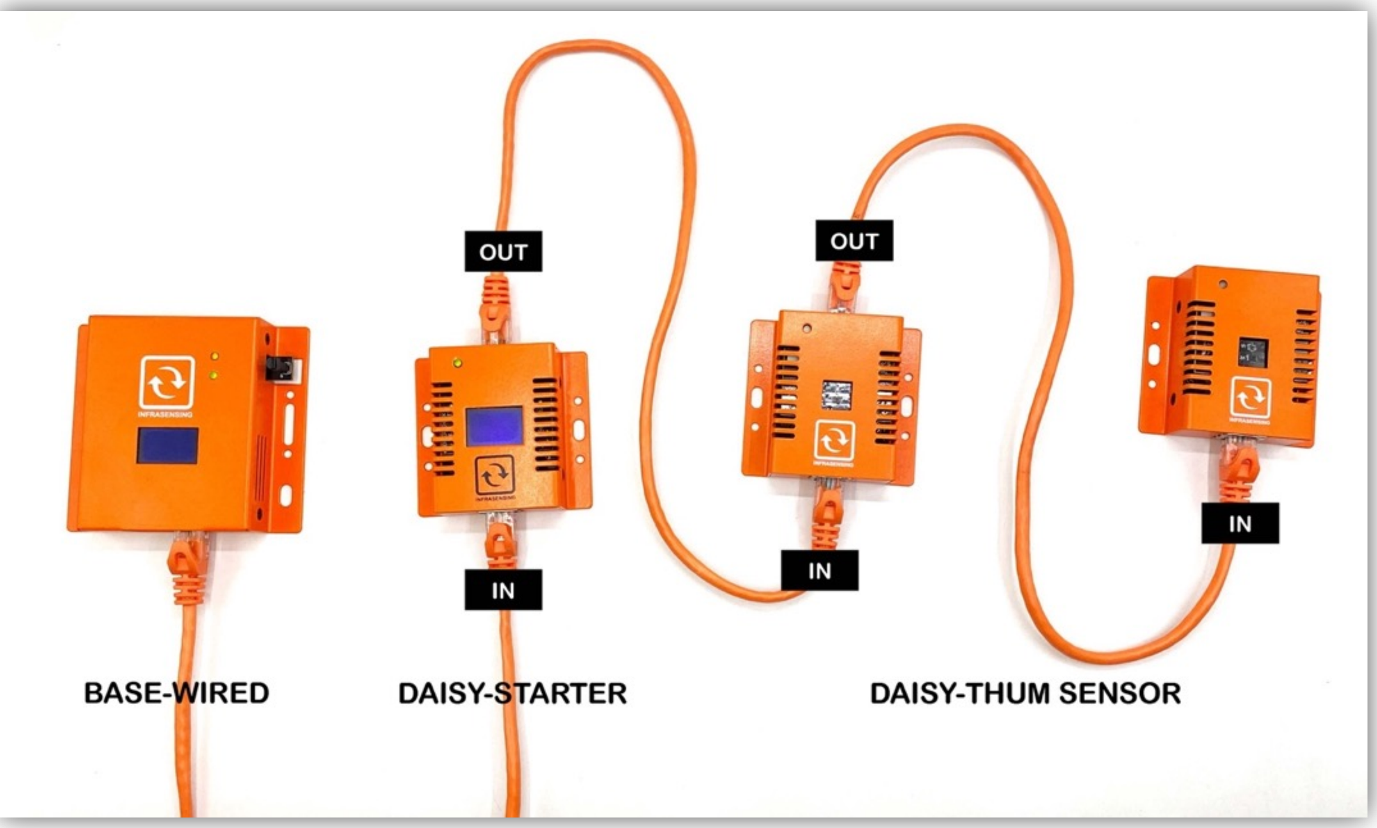


Now that you've successfully connected the first DAISY-THUM sensor, you can repeat the same process for any additional sensors you have. Remember to locate the OUT and IN ports labeled on each sensor.

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.

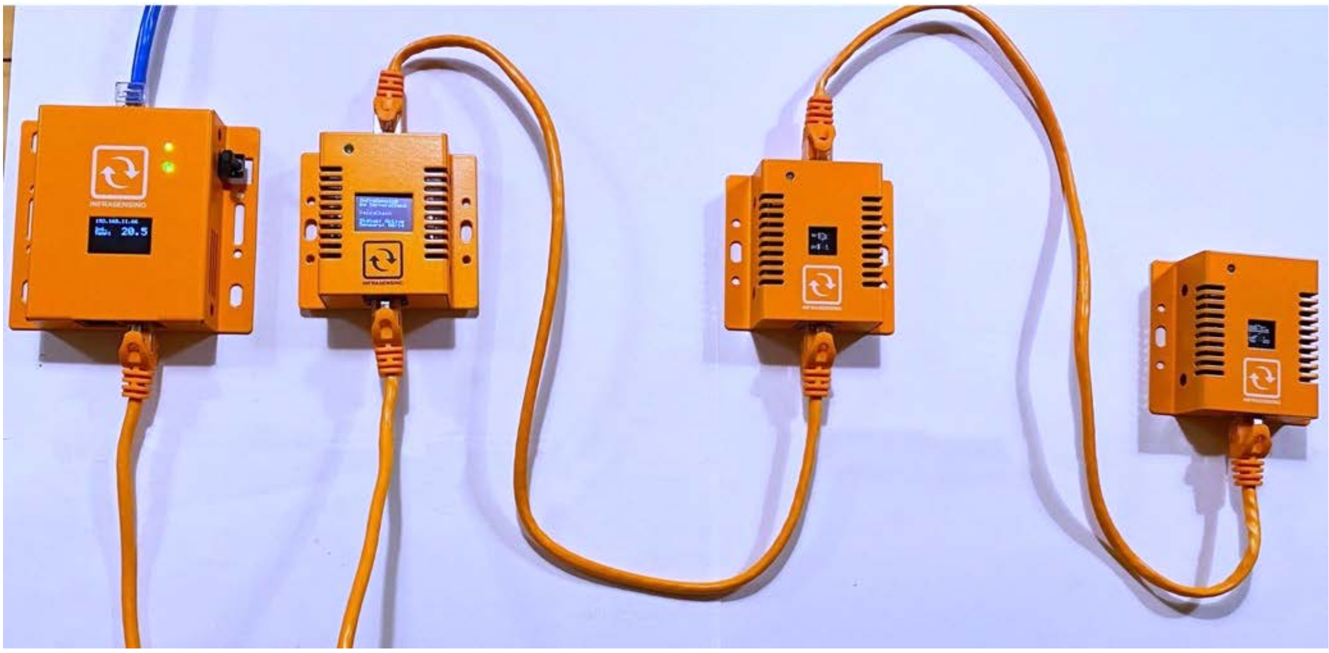
Make sure to refer to the diagram below for guidance. It's important to ensure that all sensors are securely connected and that the cables are not tangled or stretched too far.

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.

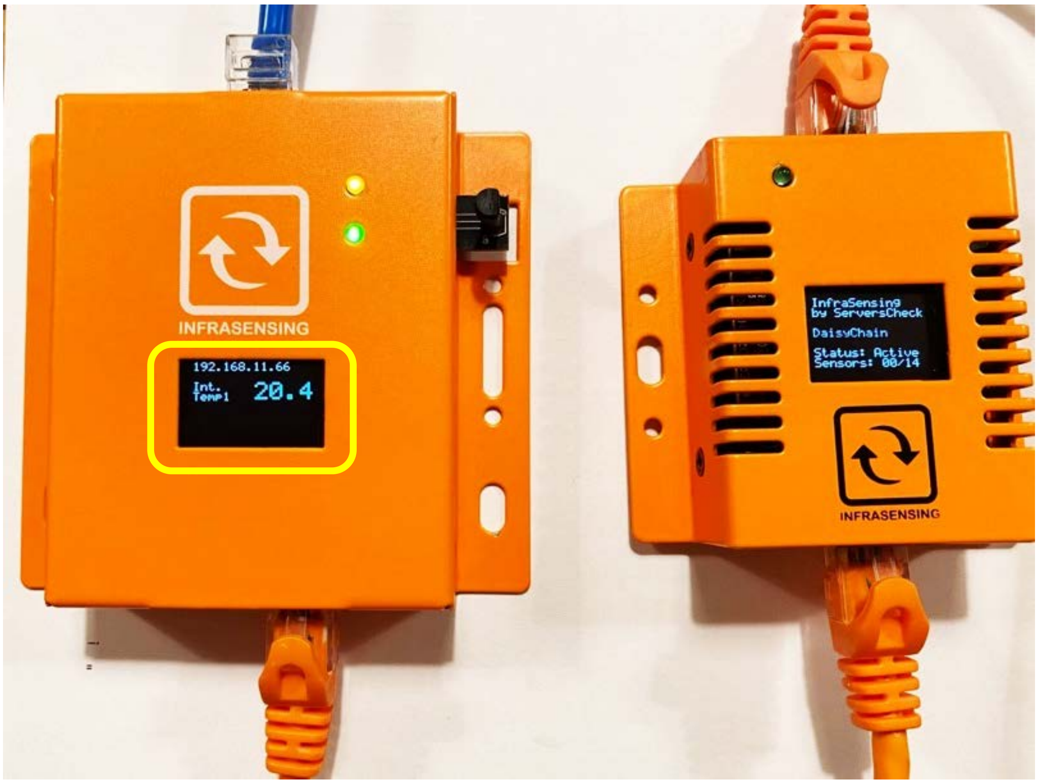


Note:

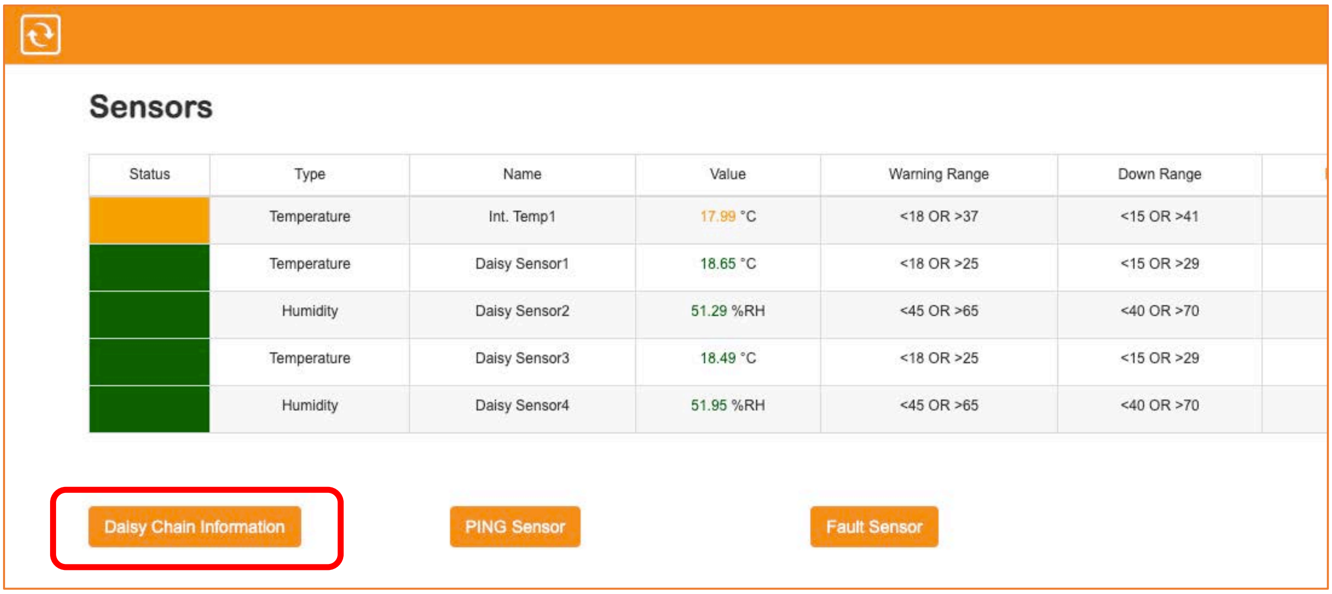
The Base Unit and Daisy Chain Start connecting cable should not be more than 2 meters (6.6 ft.) in length. Additionally, the total length of the daisy chain, including the Daisy Start and Gateway, should not exceed 100 meters. However, if you require a longer distance, you may extend the daisy chain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

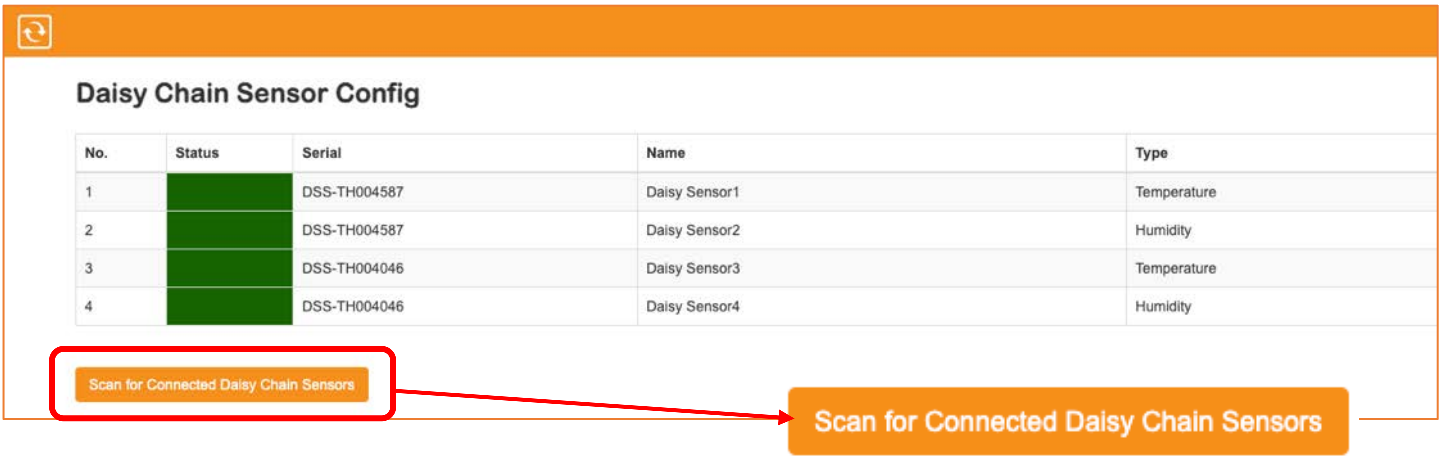


Sensors

Status	Type	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.



Daisy Chain Sensor Config

No.	Status	Serial	Name	Type
1	🟩	DSS-TH004587	Daisy Sensor1	Temperature
2	🟩	DSS-TH004587	Daisy Sensor2	Humidity
3	🟩	DSS-TH004046	Daisy Sensor3	Temperature
4	🟩	DSS-TH004046	Daisy Sensor4	Humidity

Scan for Connected Daisy Chain Sensors
Scan for Connected Daisy Chain Sensors

13.2 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.

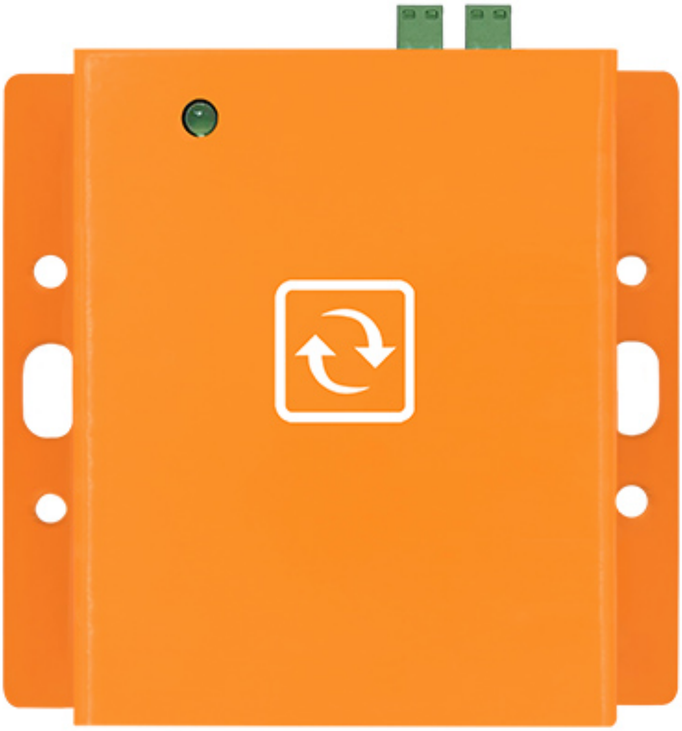
Color Indicator :

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

14 Power Sensors

14.1 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..

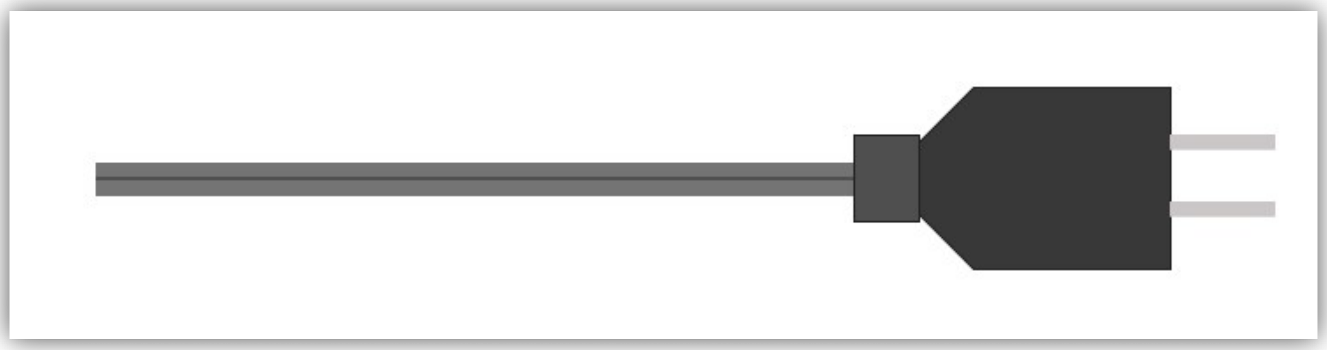


14.2 View of Current Sensor (PWR-AC-CUR)

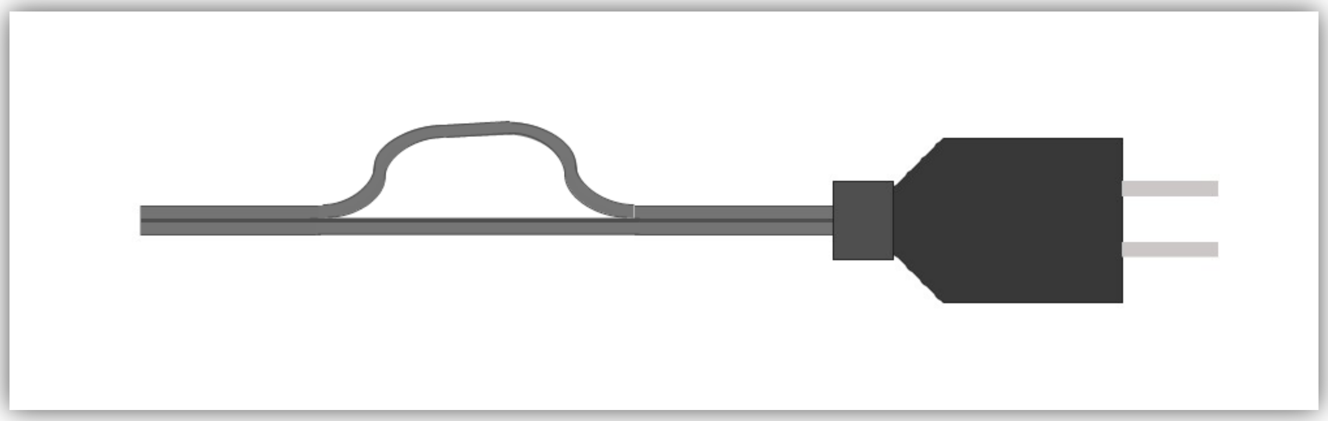
Connecting the Current Sensor

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

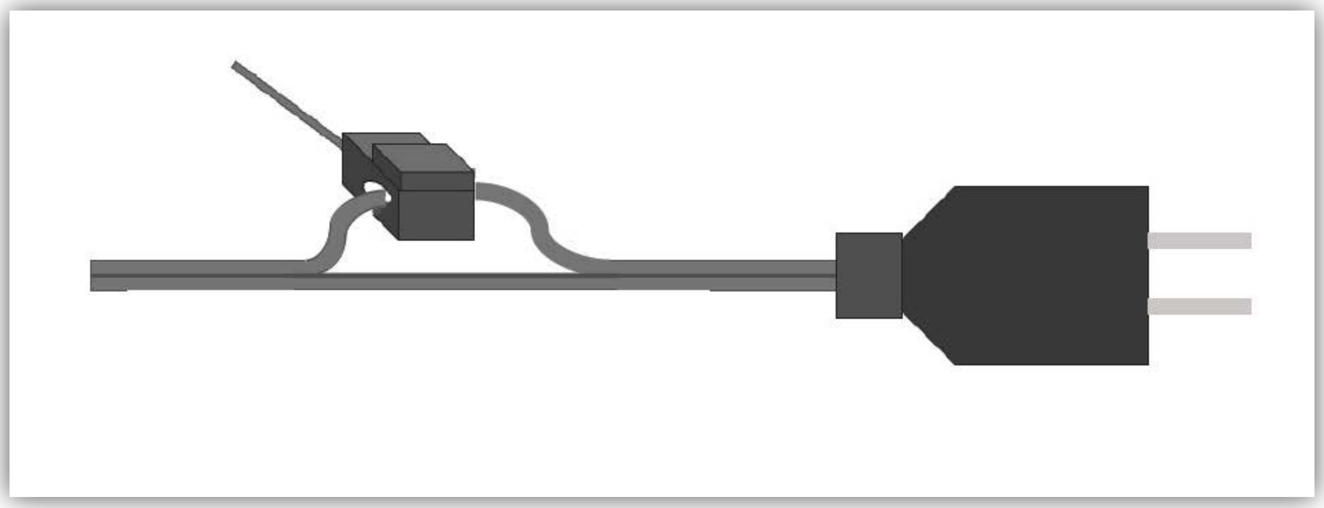
Example Plug going to the wall outlet



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.



14.3 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.

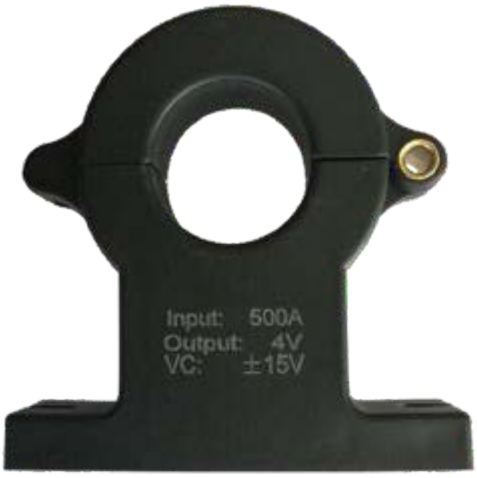
The power failure sensors from enable you to get alerts when the main power goes out as well as measure the actual voltage.

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

14.3.1 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.

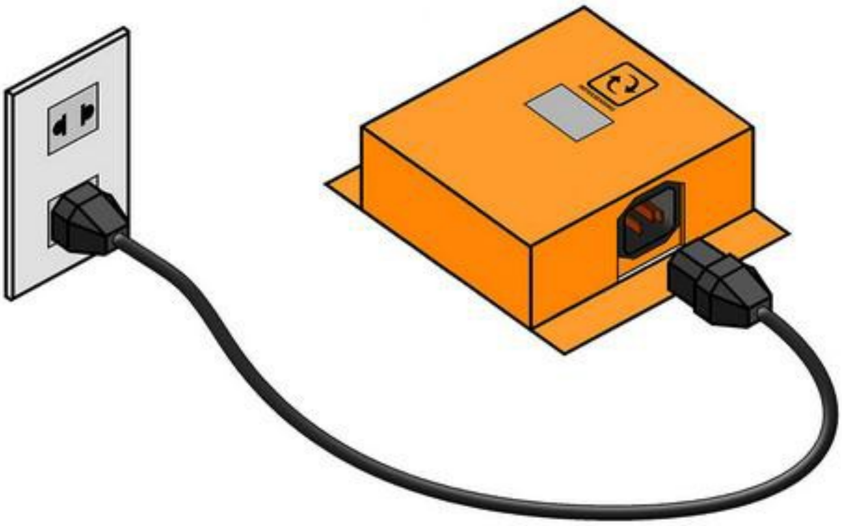
You can chain connect up to 15 PWR-BAT-CELL for every PWR-BAT-STRING.

14.4 Power Quality Sensor (PWR-AC-QUAL)

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

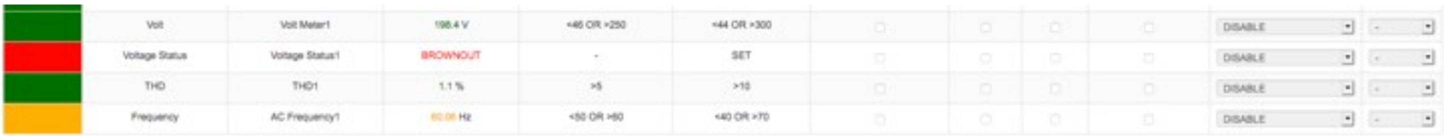
Plug and play. Simply connect an IEC C13-C14 cable to the unit and into the power wall outlet you want to monitor. As soon as it is powered, it starts monitoring. It is that simple.

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



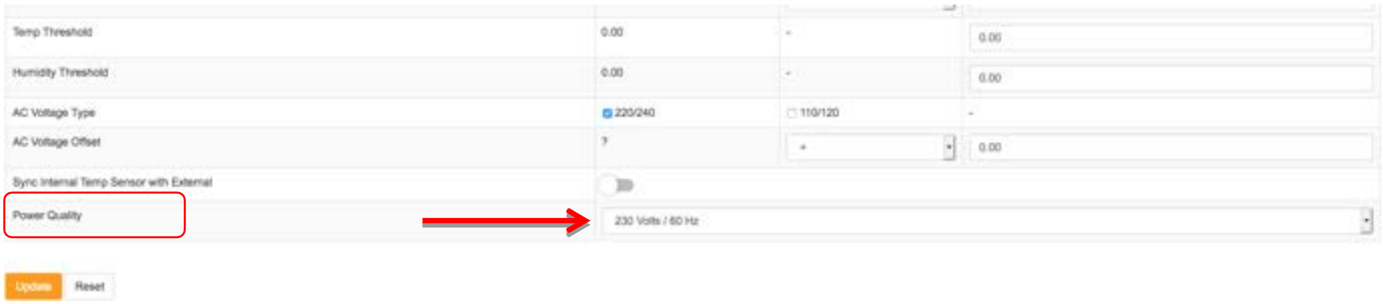
14.4.1 Initial set up for the power quality sensor using BASE-XX

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.



🟩	Volt	Volt Meter1	198.4 V	<46 OR >250	<44 OR >300	□	□	□	□	DISABLE	-
🟥	Voltage Status	Voltage Status1	BROWNOUT	-	SET	□	□	□	□	DISABLE	-
🟩	THD	THD1	1.1 %	>5	>10	□	□	□	□	DISABLE	-
🟨	Frequency	AC Frequency1	60.06 Hz	<50 OR >60	<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 Voltage Type	☑ 220/240	□ 110/120	-
AC Voltage Offset	?	+	0.00
Sync Internal Temp Sensor with External			
Power Quality	230 Volts / 60 Hz		

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.)

14.4.2 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

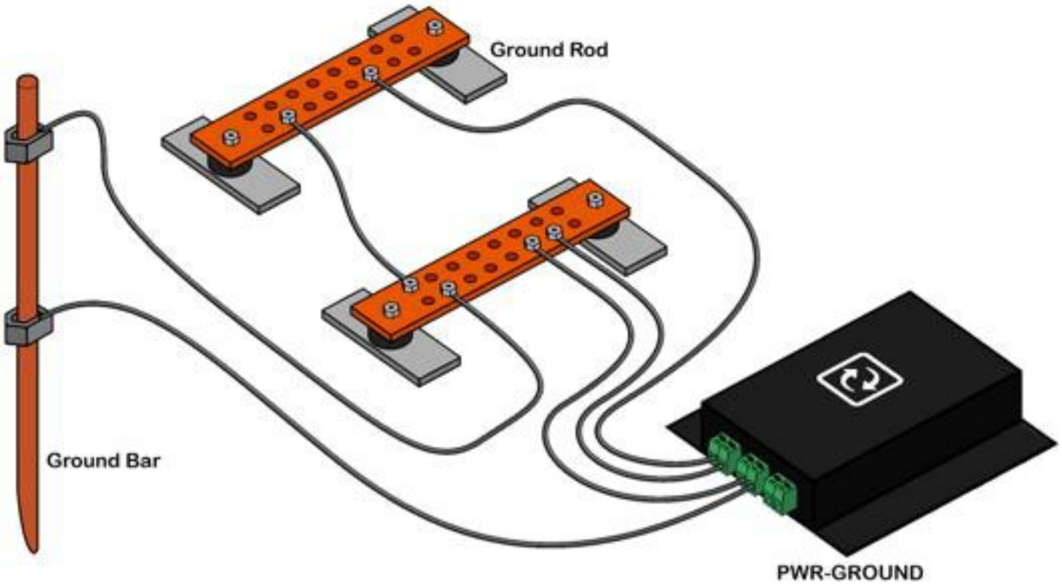
Sample file:

```
"RELEASE"            3.00
"DATE"               Sep_25_2019
"VOLT_DEFAULT"              230
"F_DEFAULT"          60
"CALIBRATED"         YES
"VOLT_OFFSET"               1
"VOLT_CODE100"              455300
"VOLT_CODE200"              912400
"SET_TIME"           YES
"YEAR"        2022
"MONTH"       02
"DAY"         03
"HOUR"        17
"MIN"         24
"SEC"         00
}
```

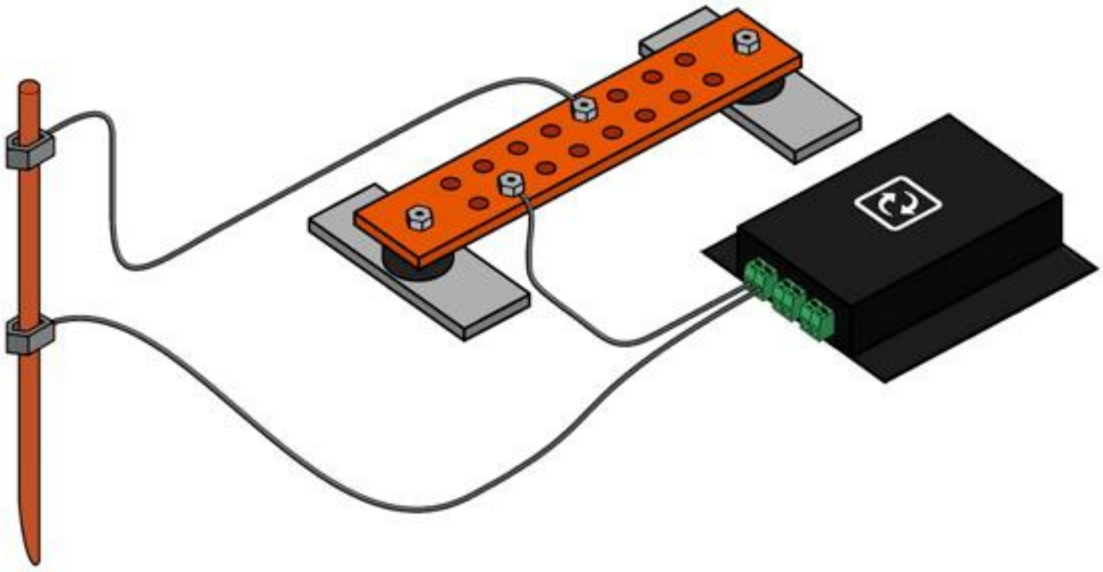
4. After the parameters are changed, save the file.

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

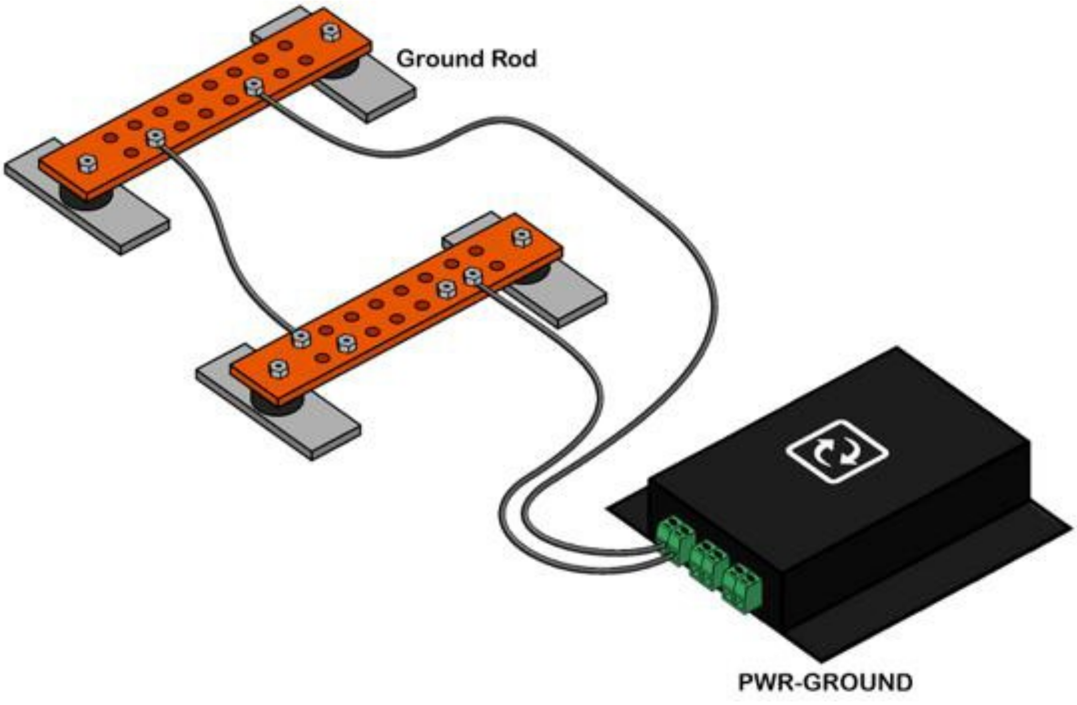
The InfraSensing Grounding Monitoring system connects to your facilities or sites electrical ground system. It checks non-stop the grounding's resistance. This allows you to get early warning on your grounding system.



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.

14.5 **IP68 Ultrasonic Fuel Level Sensor (PWR-FUEL)**

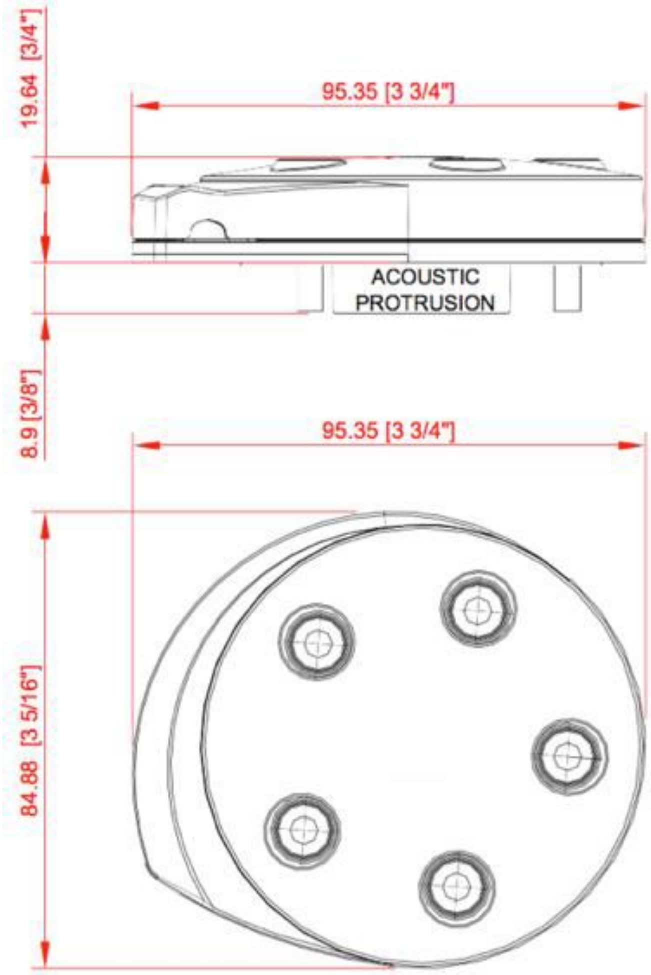
14.5.1 Features

- 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

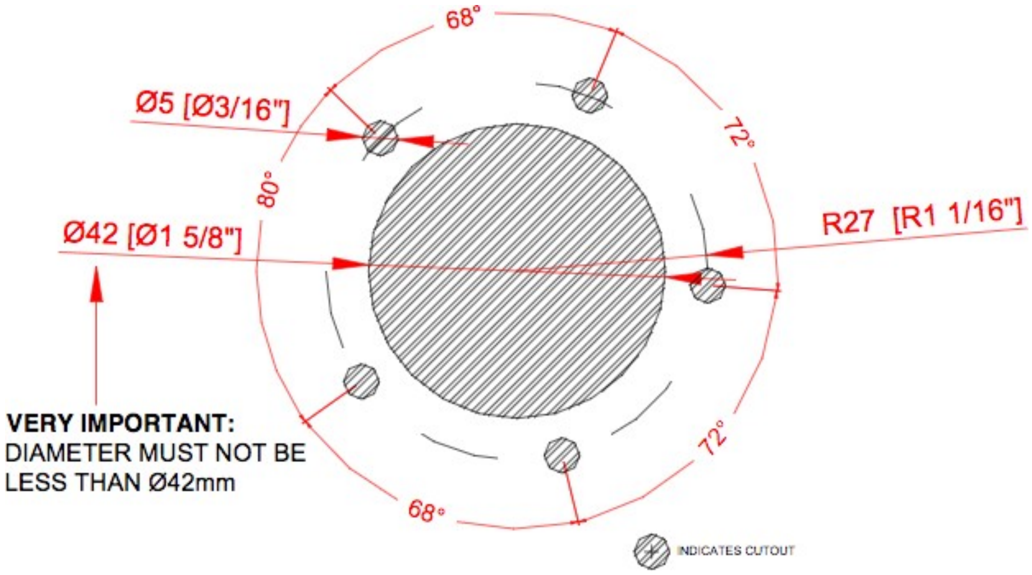
14.5.2 Maximum Tank Depths

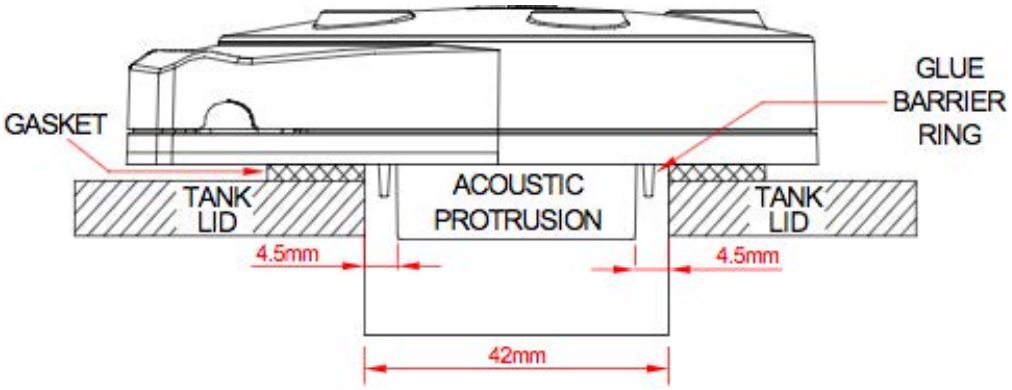
- Operating distance of 0mm to 1100mm for Petrol tanks
- Operating distance of 0mm to 2000mm for Diesel tanks
- Operating distance of 0mm to 1500mm at 55°c

14.5.3 Dimensions



14.5.4 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.

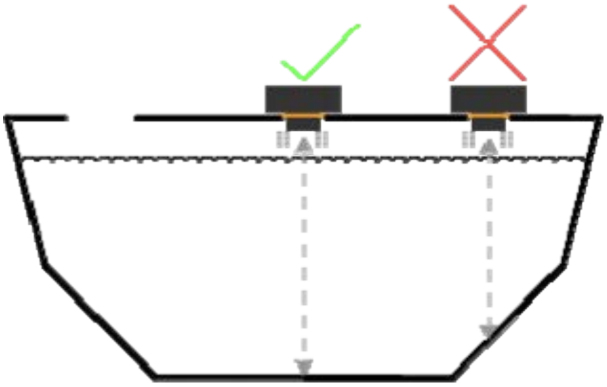
Note: Drawing is not to scale. Please use the tank gasket as a template and make sure the tank hole is 42mm.

14.5.5 Tips and example installations

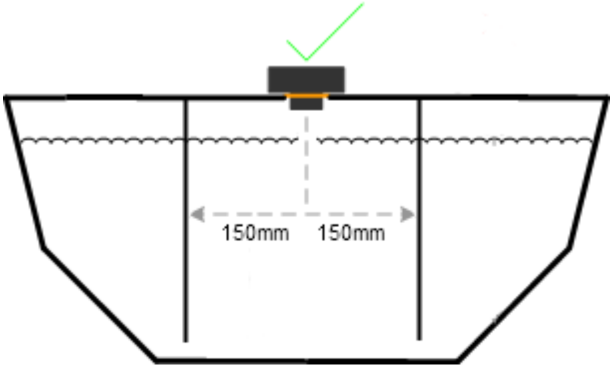
- The sensor must not be mounted closer than 150mm from the center to the sides of the tank, baffles or other intrusions.
- Only use on tanks greater than 200mm in depth.
- Sensor must be mounted parallel to the surface of the liquid.
- Make sure that sensor protrusion is NOT in contact with any object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

Case 1
The sensor must be mounted at the deepest tank point!

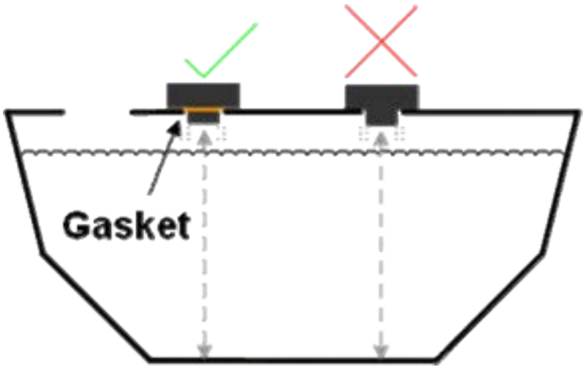
It is recommended the sensor is mounted in the middle of the tank, this is particularly important on low or no baffled tanks that are mounted in moving vehicles or vessels. This allows the sensor to average waves of fuel to the correct level when the depth is varying due to wave slop.



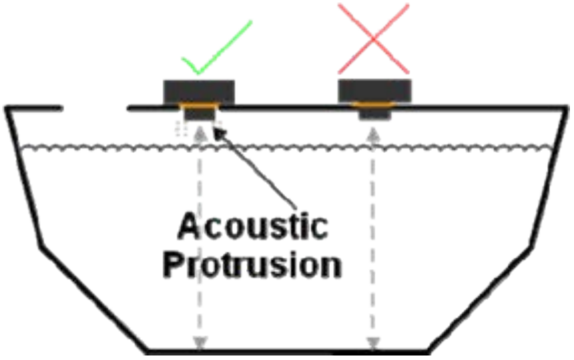
Case 2
The sensor must be mounted at least 150mm from a vertical tank baffle, tank walls and piping.



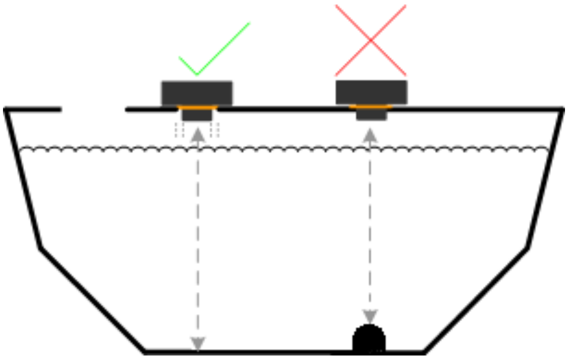
Case 3
Use 5 washers provided, washers must be placed under screw heads to prevent rubber lid damage.



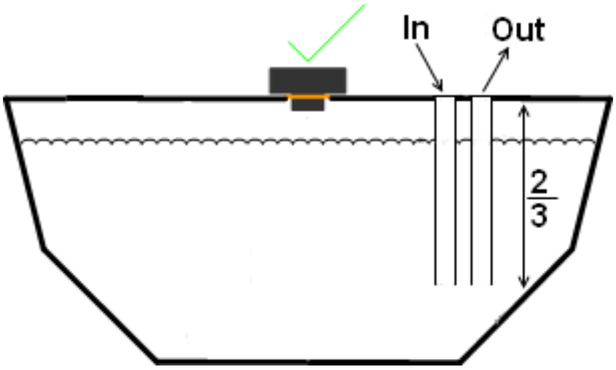
Case 4
Acoustic protrusion must not touch the tank frame.



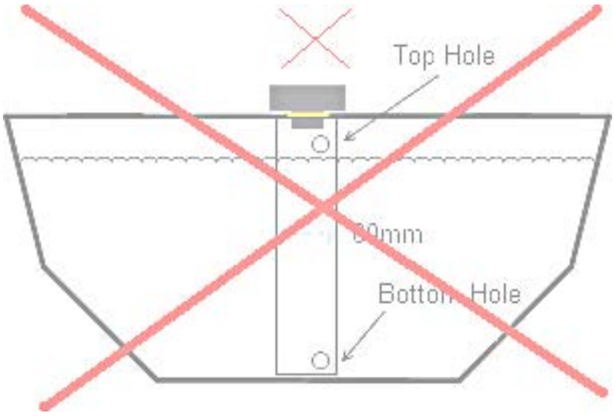
Case 5
The sensor must be mounted so it can see the bottom of the tank if the fuel is to be measured to the bottom.



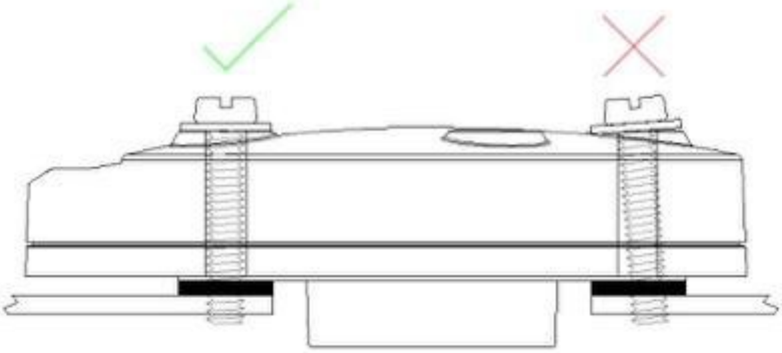
Case 6
Inlet and Outlet piping must go in at least 2⁄3rds of the way in to the tank to stop turbulence when filling.



Case 7
Do not fit the sensor with a tube.



Case 8
Ensure bolts and mounting holes are aligned properly to keep plastic body isolated acoustically from tank.
Do not over tighten the screws.



15 Industrial sensor

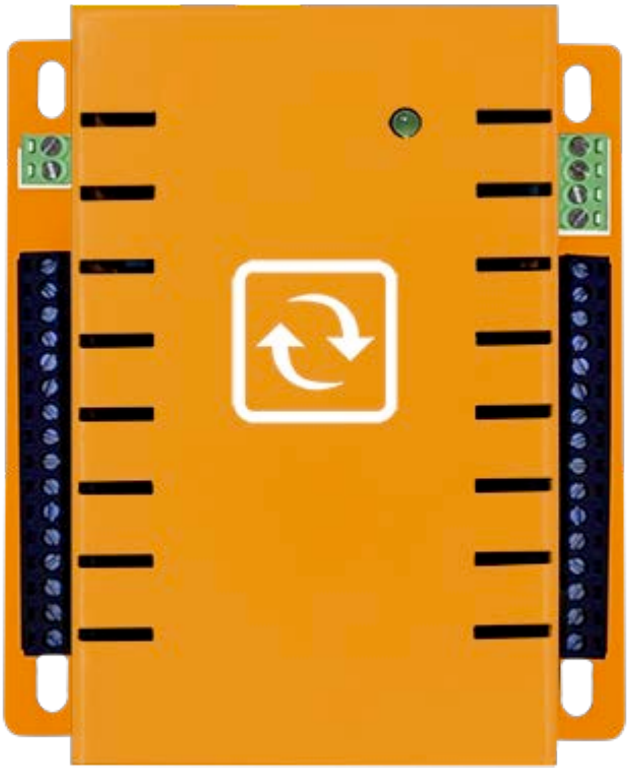
15.1 **Industrial 0-10V (IND-0-10V)**

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

15.2 **Industrial 4-20mA (IND-4-20mA)**

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

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



15.4 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)

15.5 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

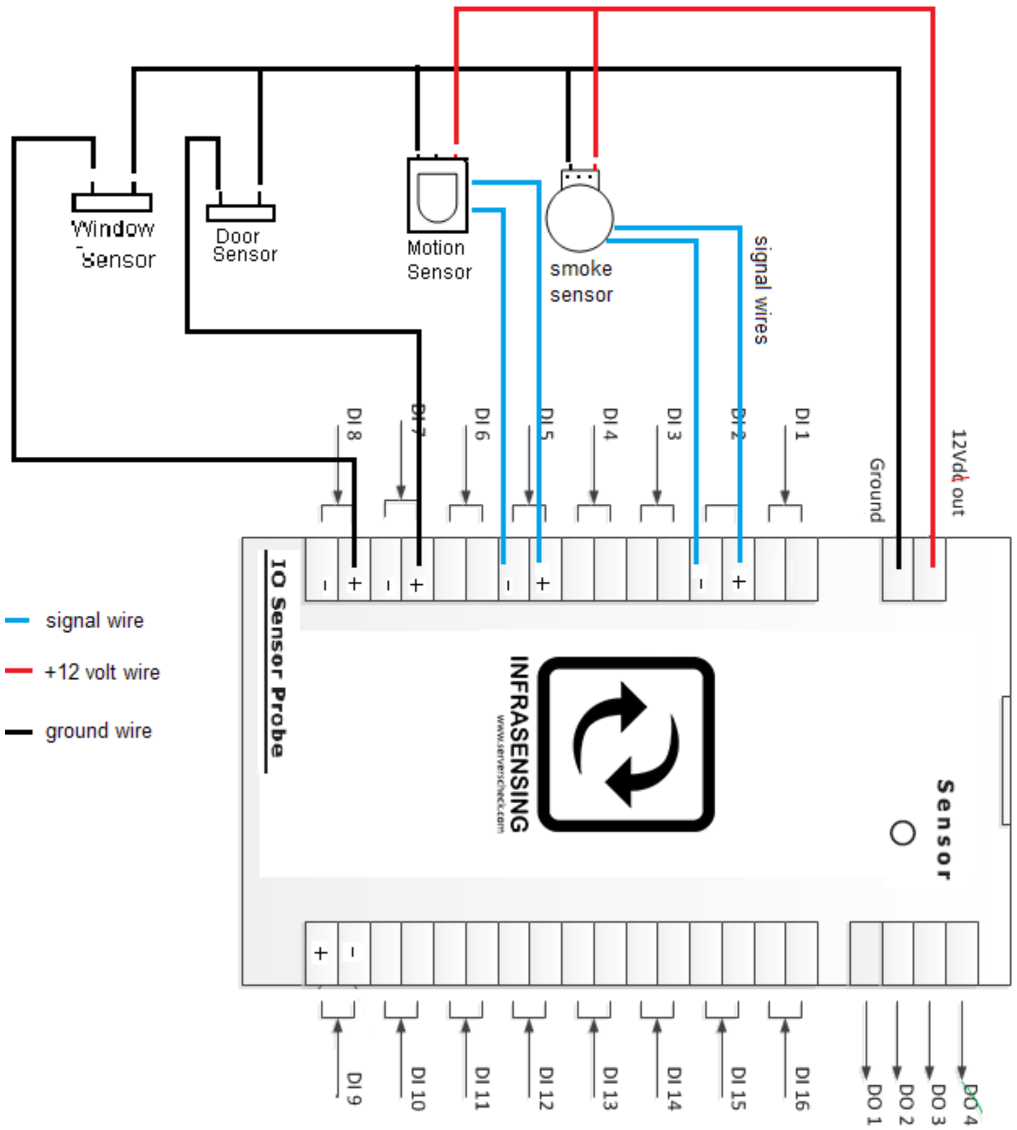
15.6 Terminal description

TERMINAL BLOCKS

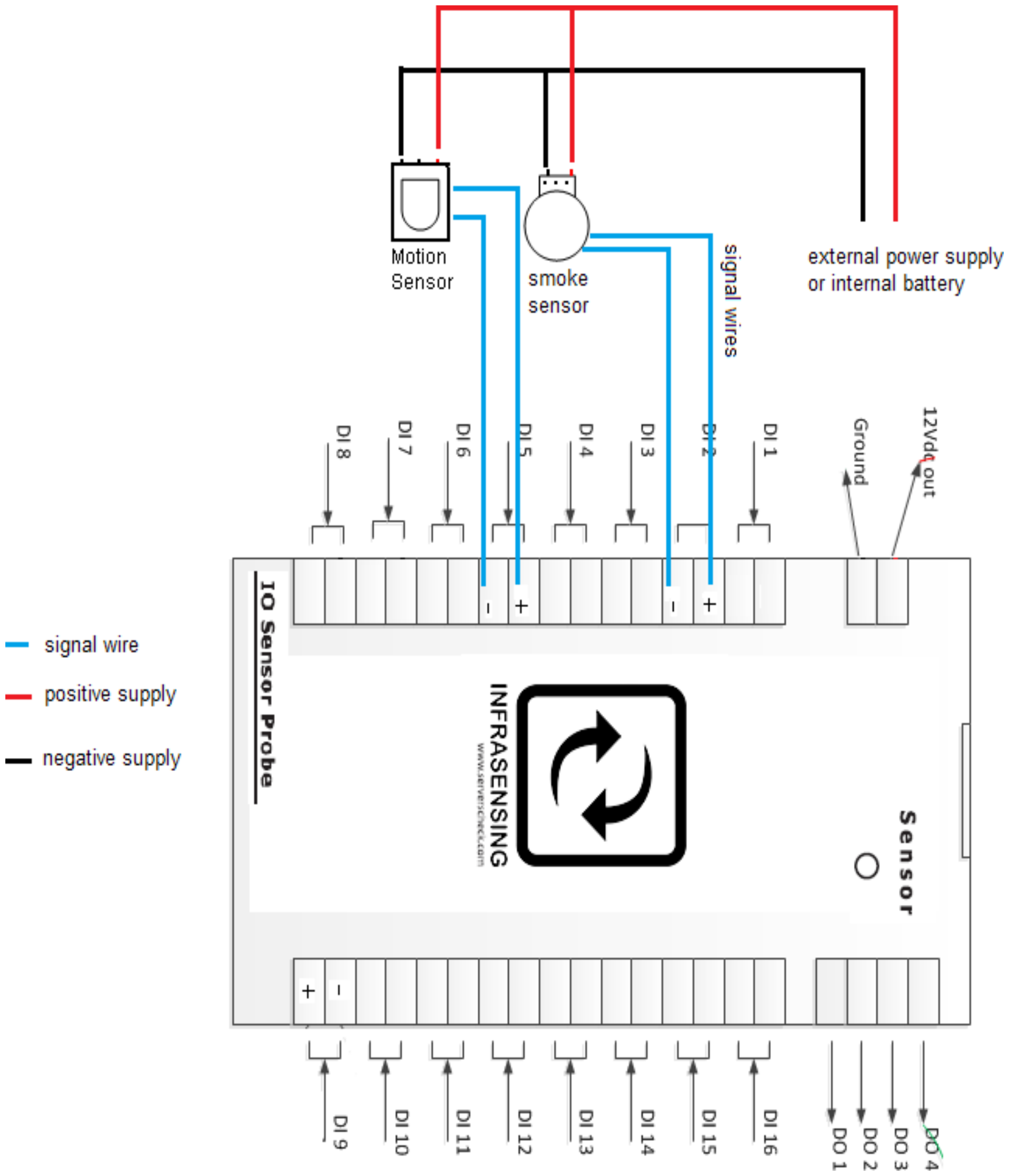
DI1 to DI16	: 16 digital inputs
DO1 to DO4	: 4 digital outputs
+12V	: 12 VDC supply
GND	: supply ground

15.7 Basic wiring diagram

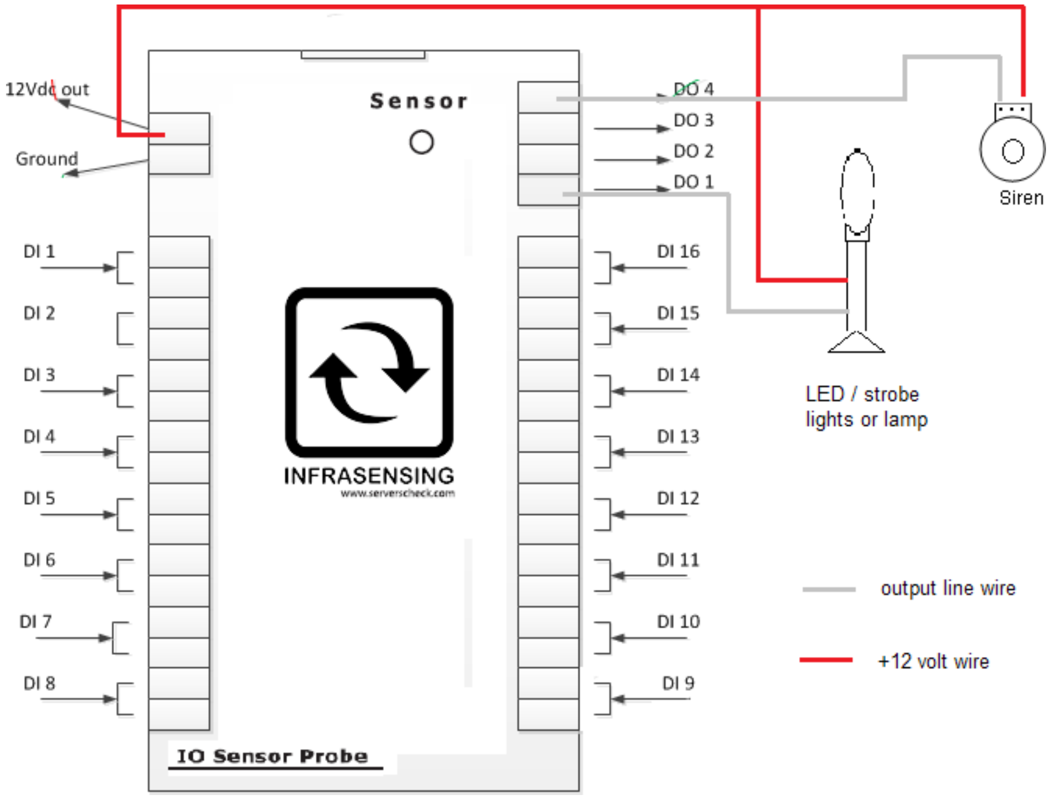
Inputs: if sensors are getting their power supply from the IO sensor probe



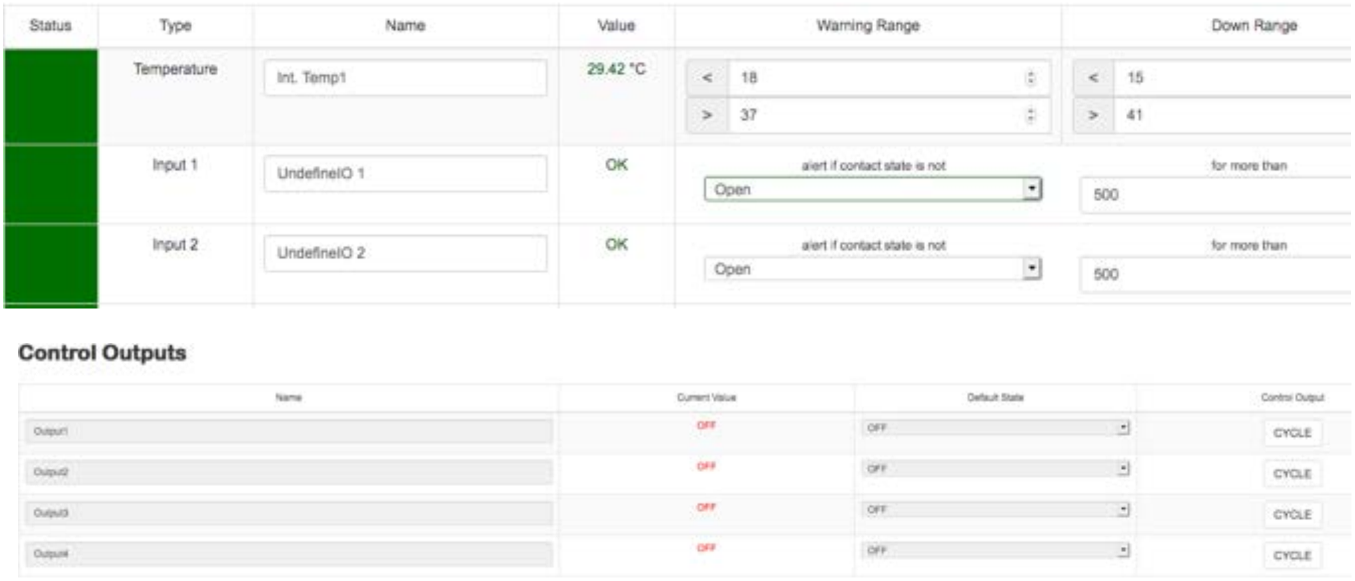
Inputs: if sensors are getting their power supply from an external source or internal battery



Outputs: to drive a siren, lamp/strobe or any output device



15.8 Base Unit IO sensor probe interface



Status	Type	Name	Value	Warning Range	Down Range
🟩	Temperature	Int. Temp1	29.42 °C	< 18 > 37	< 15 > 41
🟩	Input 1	UndefinelO 1	OK	alert if contact state is not Open	for more than 500
🟩	Input 2	UndefinelO 2	OK	alert if contact state is not Open	for more than 500

Control Outputs

Name	Current Value	Default State	Control Output
Output1	OFF	OFF	CYCLE
Output2	OFF	OFF	CYCLE
Output3	OFF	OFF	CYCLE
Output4	OFF	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

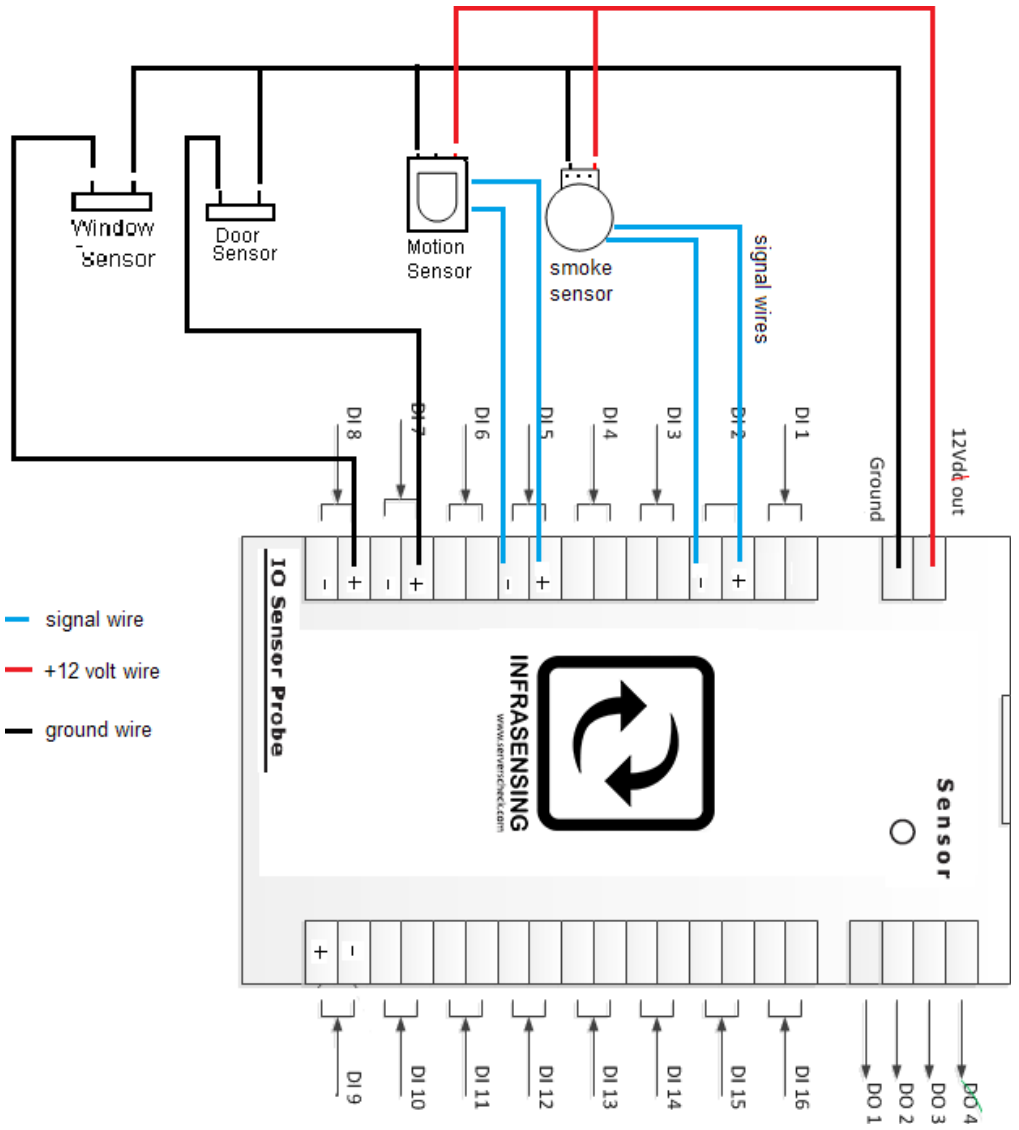
- The default state can be set to either ON or OFF and is used in conjunction with triggers (ex. siren or strobe /lamp)
- CYCLE button is used to switch the button on and then off or vice versa depending on the default state.

15.9 Wiring configuration and settings (anti tampering)

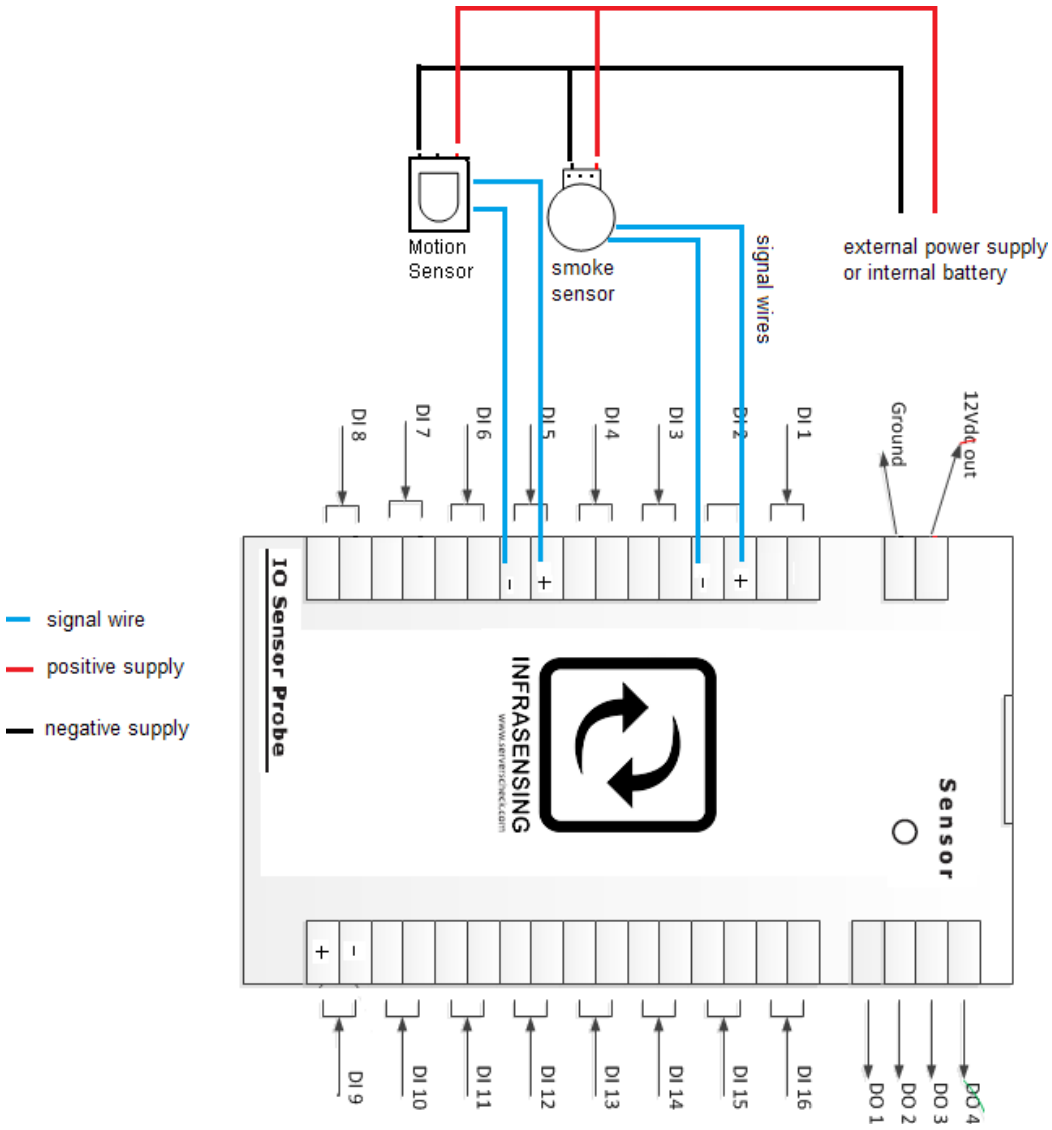
The IO sensor probe does not have the ability to give out specifically a “tamper” alert. But it can be wired and set to give out a “normal” alert.
If ever a power supply wire or a signal wire was cut off in which case the monitoring team must still attend to.

Basic wiring diagram for Inputs still applies

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

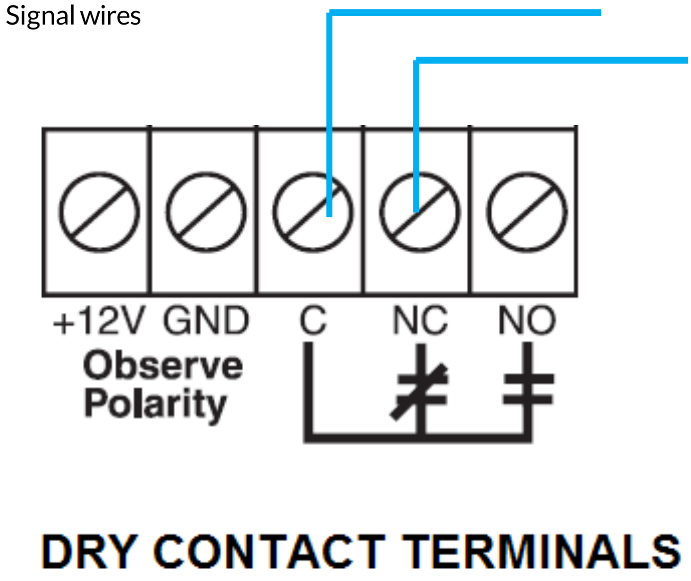


Inputs: if sensors are getting their power supply from an external source or internal battery



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



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)

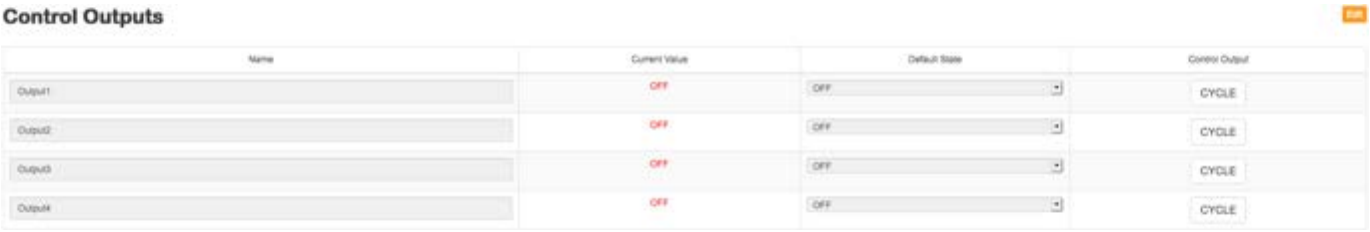
Set the all Normal State to **“Closed”** (setting the trigger logic to normally closed)

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

15.10 **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.

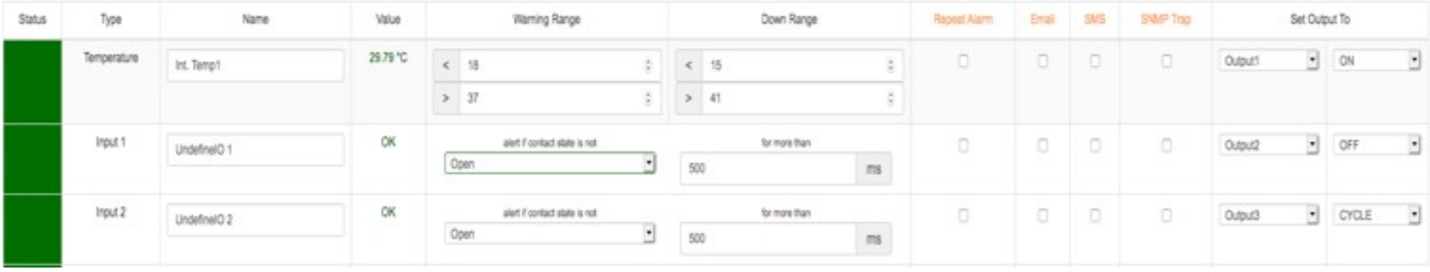


Control Outputs

Name	Current Value	Default State	Control Output
Output1	OFF	OFF	CYCLE
Output2	OFF	OFF	CYCLE
Output3	OFF	OFF	CYCLE
Output4	OFF	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	Email	SMS	SNMP Trap	Set Output To	
🟩	Temperature	Int. Temp1	29.79 °C	< 18 > 37	< 15 > 41	□	□	□	□	Output1	ON
🟩	Input 1	UndefinedIO 1	OK	alert if contact state is not Open	for more than 500 ms	□	□	□	□	Output2	OFF
🟩	Input 2	UndefinedIO 2	OK	alert if contact state is not Open	for more than 500 ms	□	□	□	□	Output3	CYCLE

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

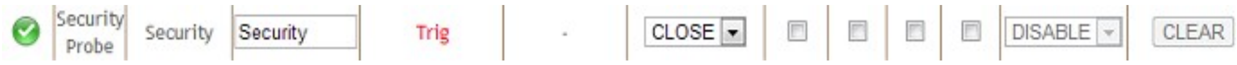
16 Security Sensors

16.1 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.

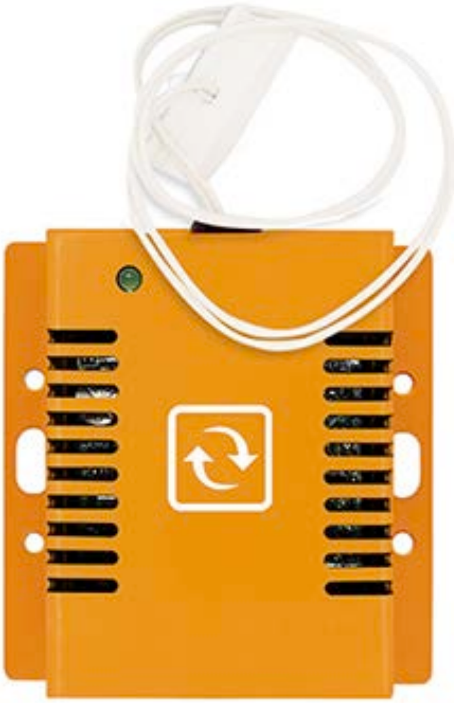
It is important to note that all security probes have the same web interface so it is advisable to attach one at a time and immediately rename it according to your naming conventions.



✓	Security Probe	Security	Security	Trig	-	CLOSE ▾	□	□	□	□	DISABLE ▾	CLEAR

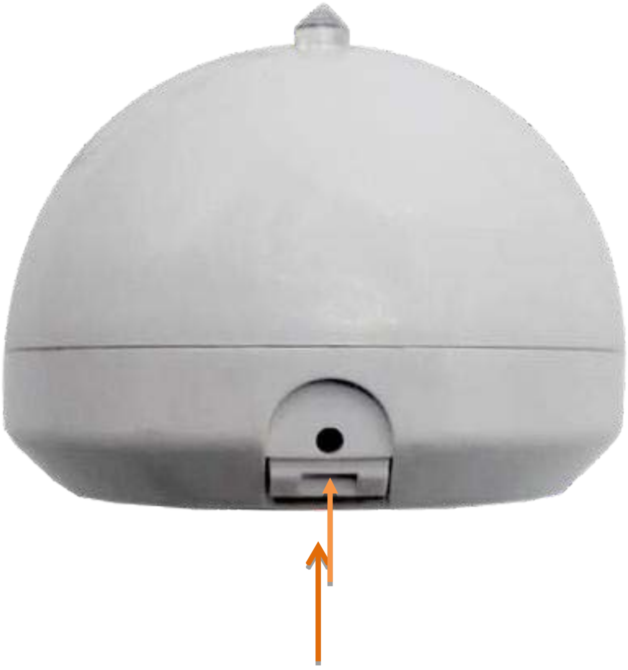
16.2 Door Sensor (SEC-DOOR)

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



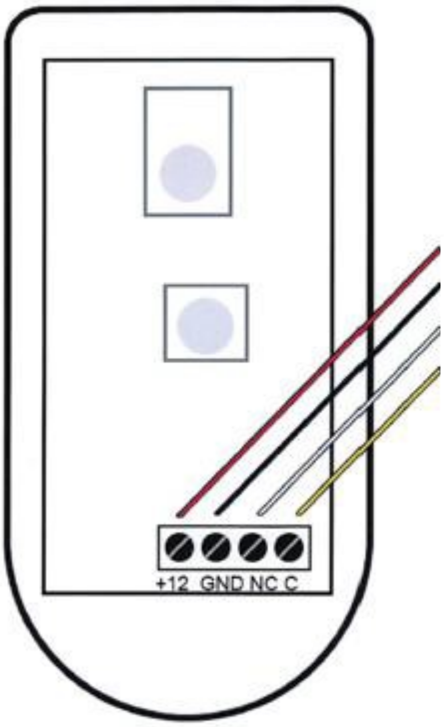
16.3 Motion Sensor (SEC-MOTION)

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
Black
White/Brown
Yellow/Orange

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.

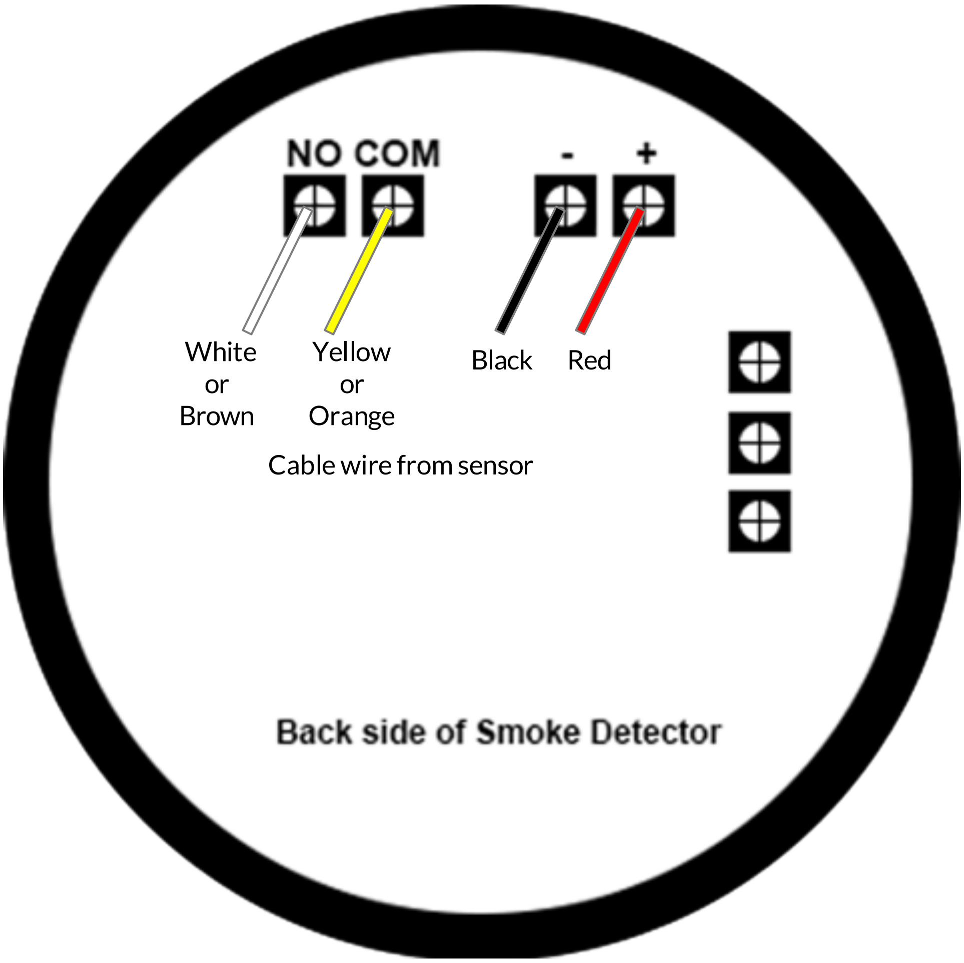
Yellow or Orange Wire: Connect to the Common terminal (C) of the Motion Sensor.

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

16.4 Smoke Sensor (SEC-SMOKE)

16.4.1 Installation guide for Security Smoke Sensor

Wiring



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

16.5 Sound Sensor (SEC-SOUND)

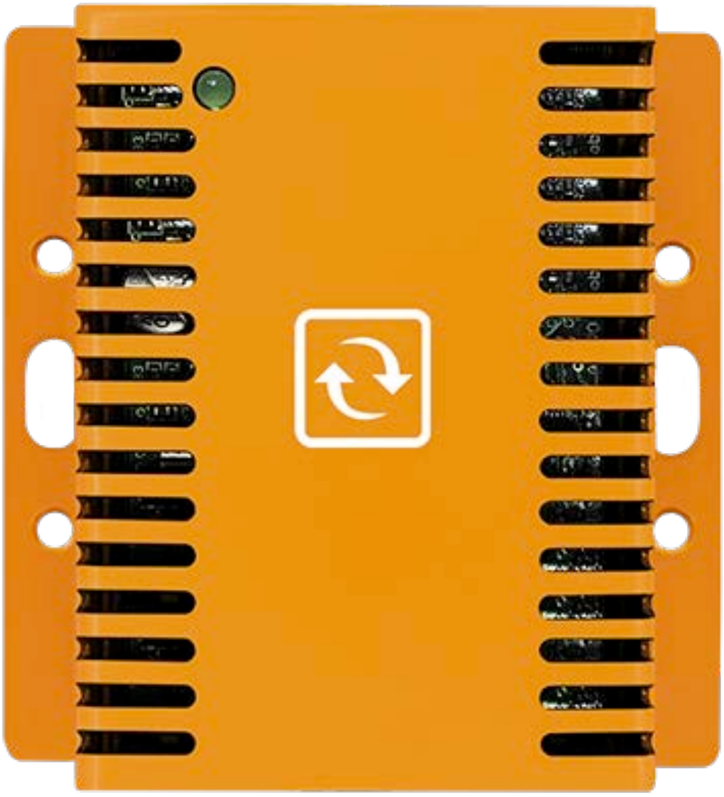
With the data center demanding a very conducive environment for the services it provides, we know that the people making all those possible needs to be safeguarded as well from any anomaly-producing situations.

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.

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

16.7 Shock / Vibration Sensor (SEC-SHOCK)

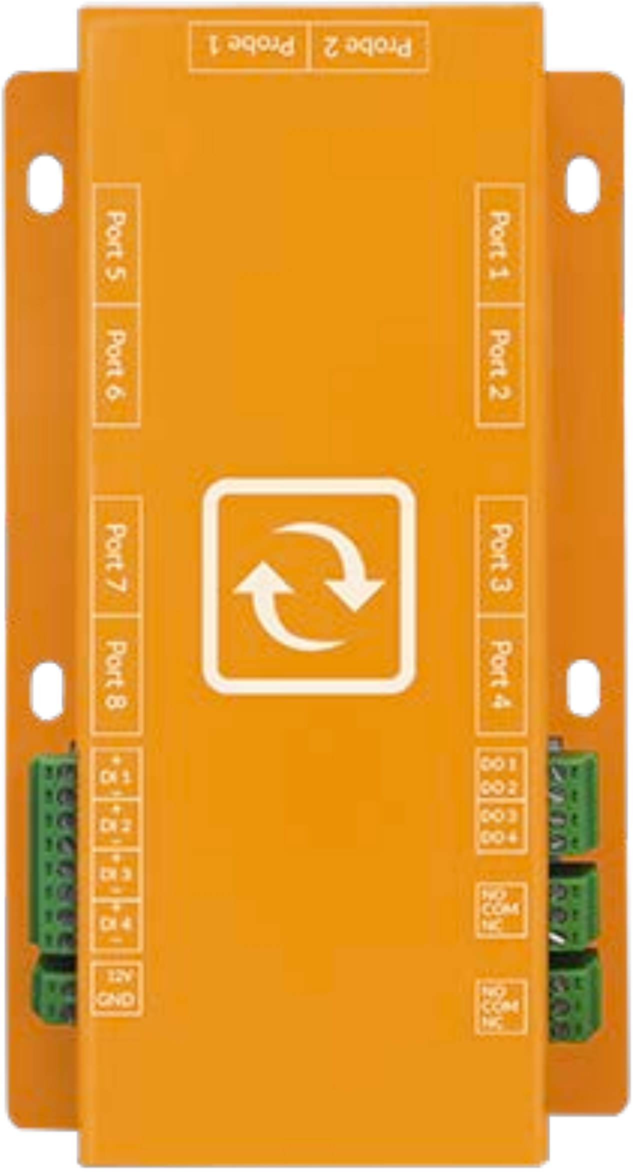
16.8 Tilt Sensor (SEC-TILT)



17 The Sensor Hub (EXP-8HUB)

17.1 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.

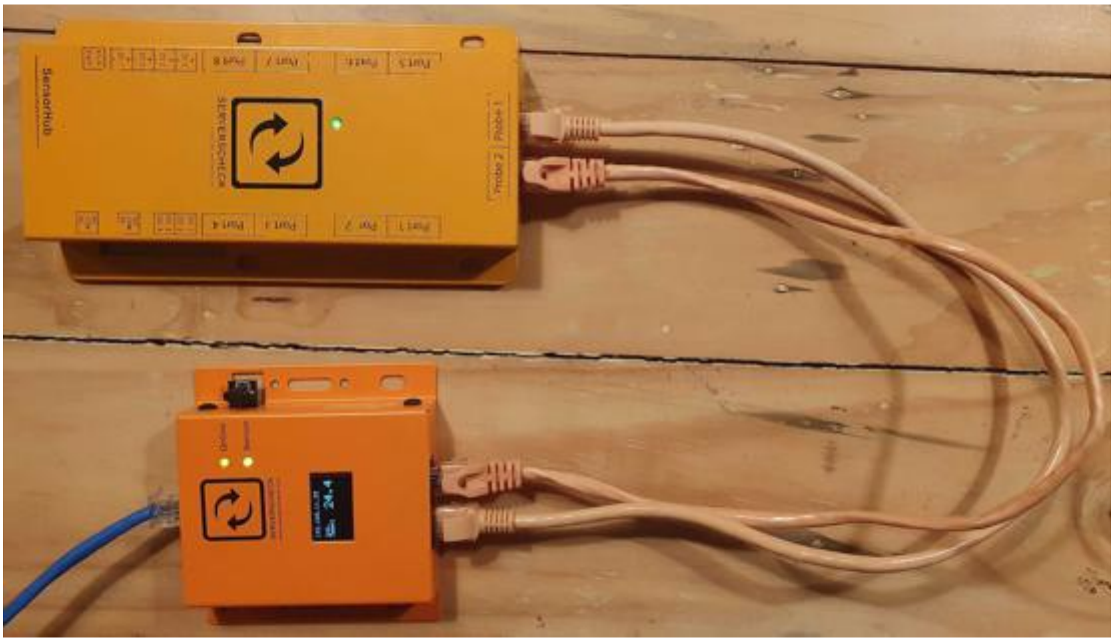


17.2 Probe restrictions

- 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

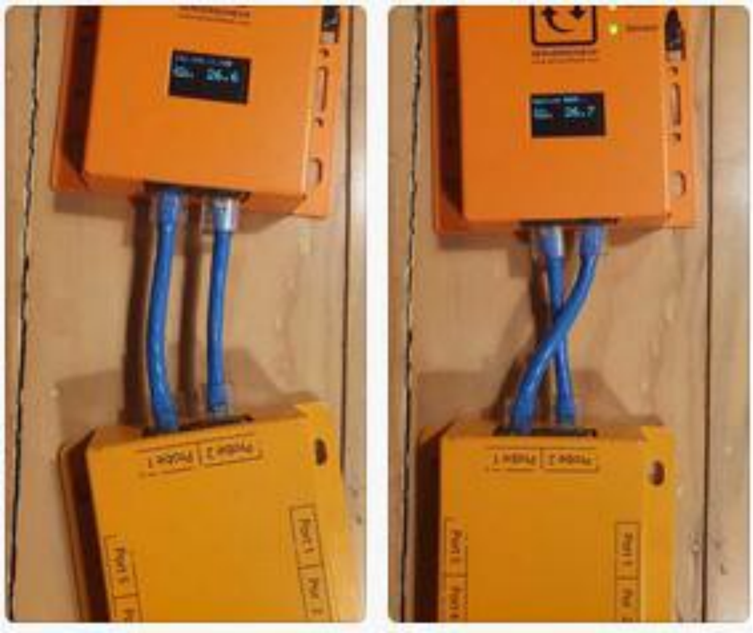
17.3 Connecting the SensorHub to the Base Unit



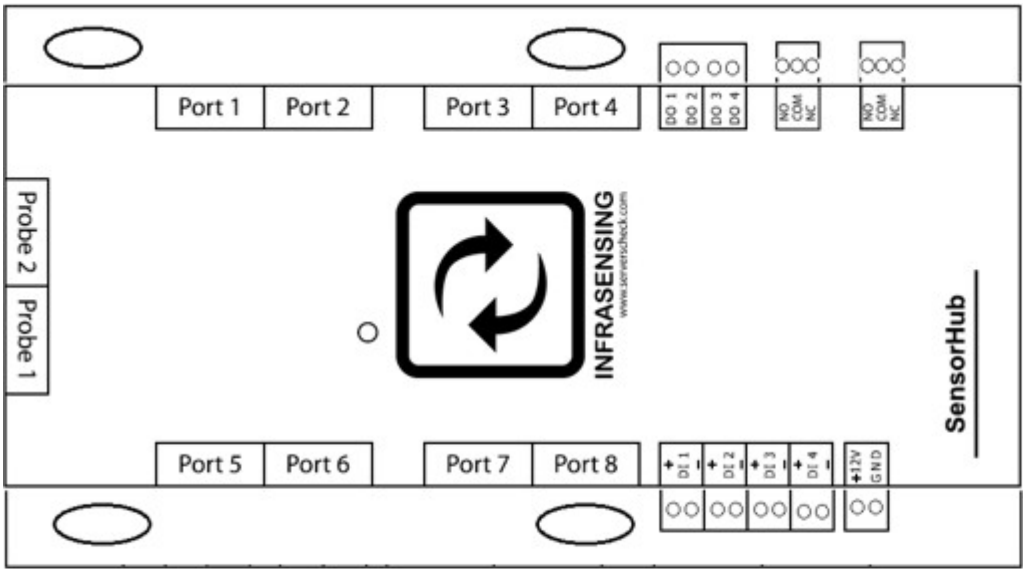
The sensor hub connects through regular RJ45 cables to the Base Unit. The connection from the base unit going to the SensorHub should not exceed 1 meter / 3.3 ft.

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.



17.4 **Terminal connections**

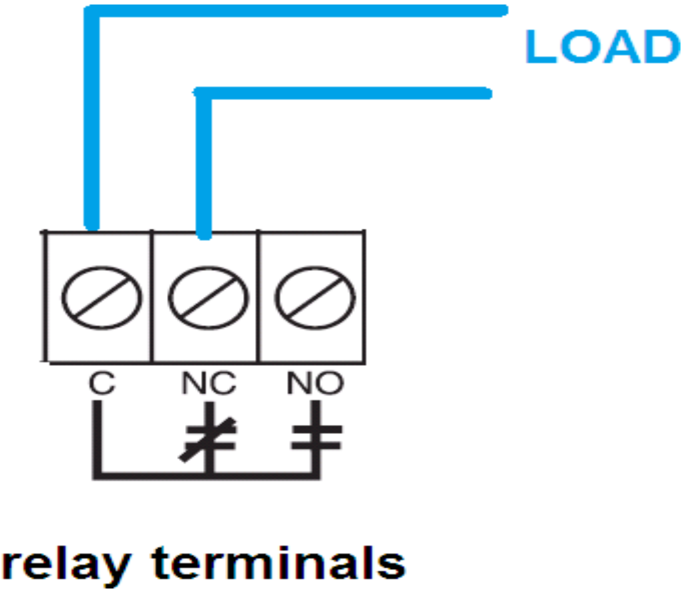


PROBE 1 AND PROBE 2:connect to Base Unit using two RJ 45 cables
PORT 1 TO PORT 8 : connect sensor probes

DI 1 to DI 4	:connect to 4 dry contact inputs
DO 1 to DO4	:connect to 4 digital outputs
NO, COM and NC	:relay outputs

17.5 Basic wiring

INPUTS (dry contact)	: same wiring diagram as the IO sensor probe for inputs
OUTPUTS (digital)	: same wiring diagram as the IO sensor probe for outputs
OUTPUTS (relay)	: connection to a load will depend on the wiring convention



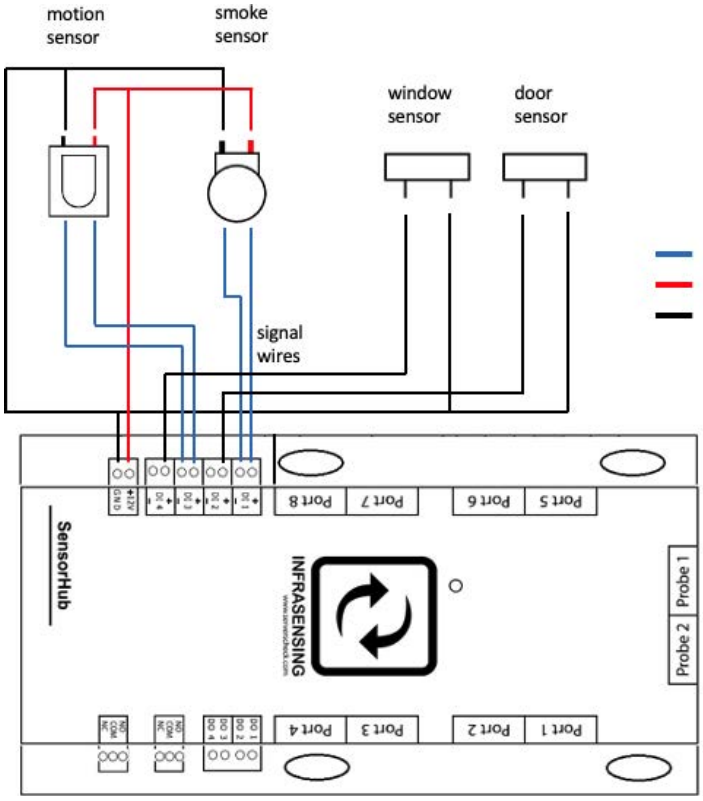
NO : normally open(always open contact/not connected)

NC : normally closed(always shorted contact/connected)

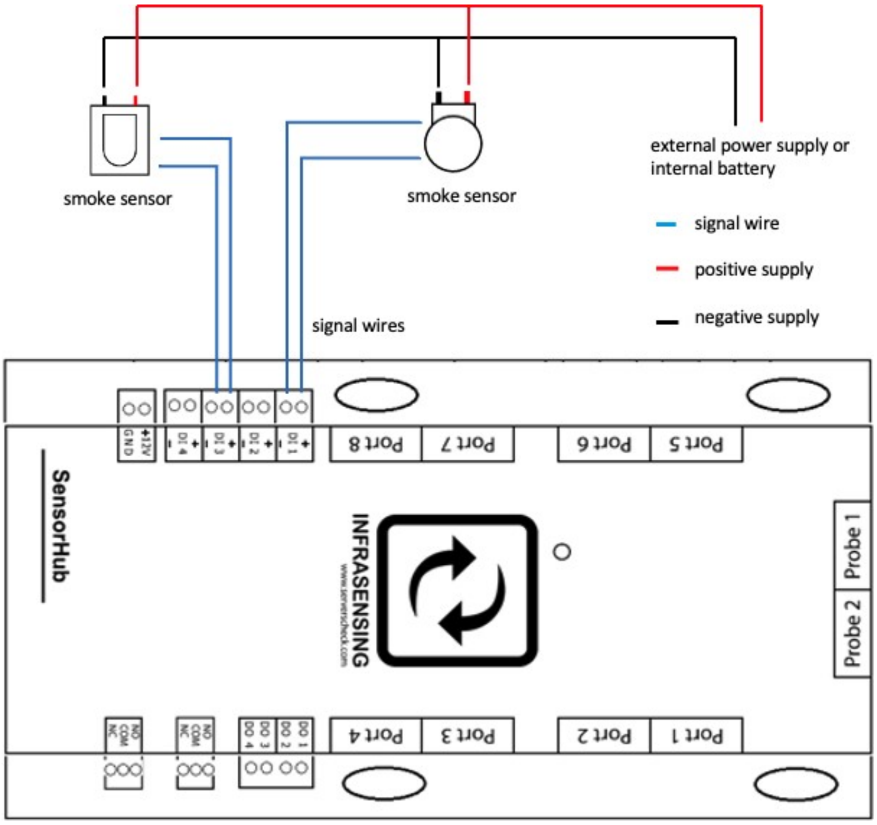
C : common(common terminal)

17.6 Basic wiring diagram

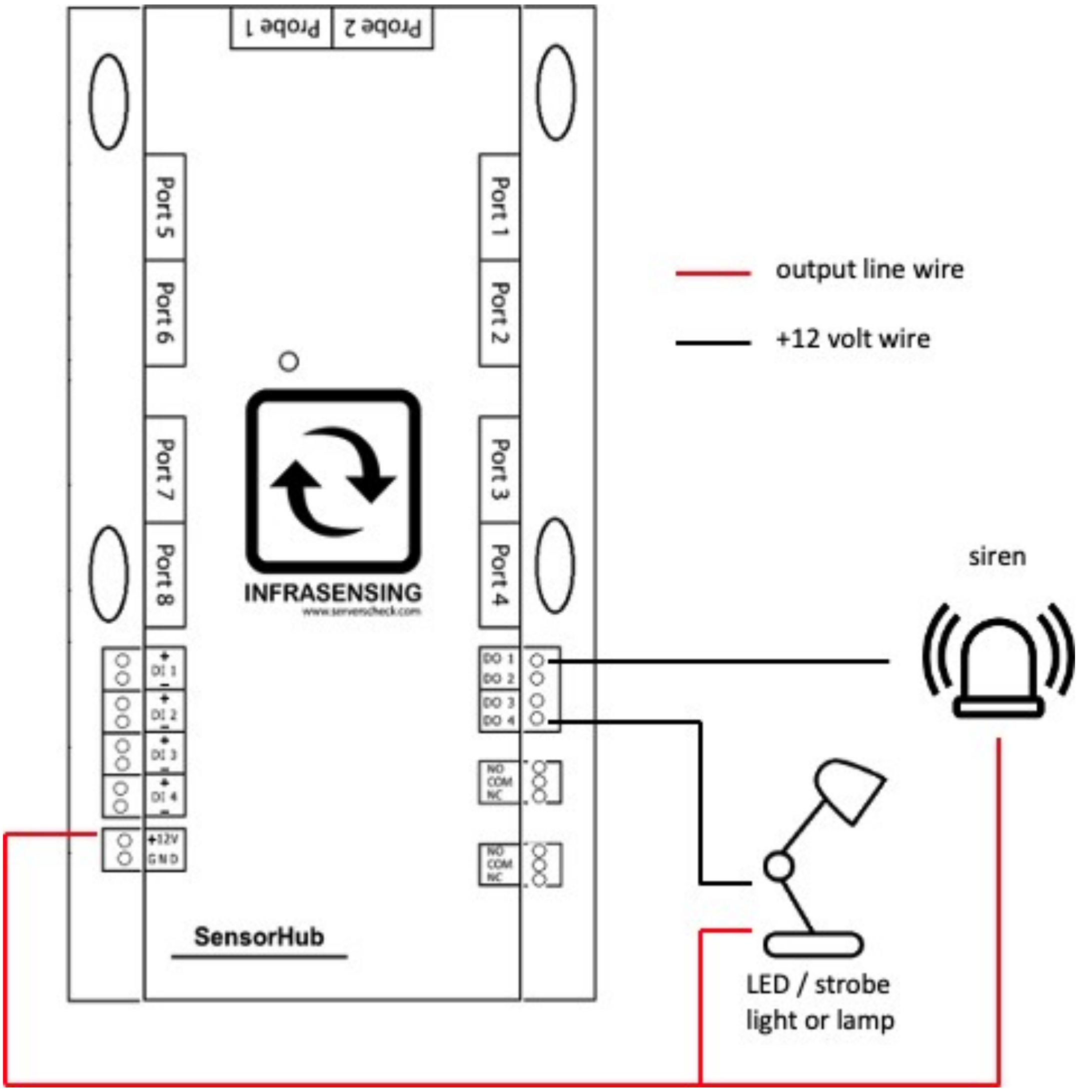
INPUTS: If sensors are getting their supply from the EXP-8HUB



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



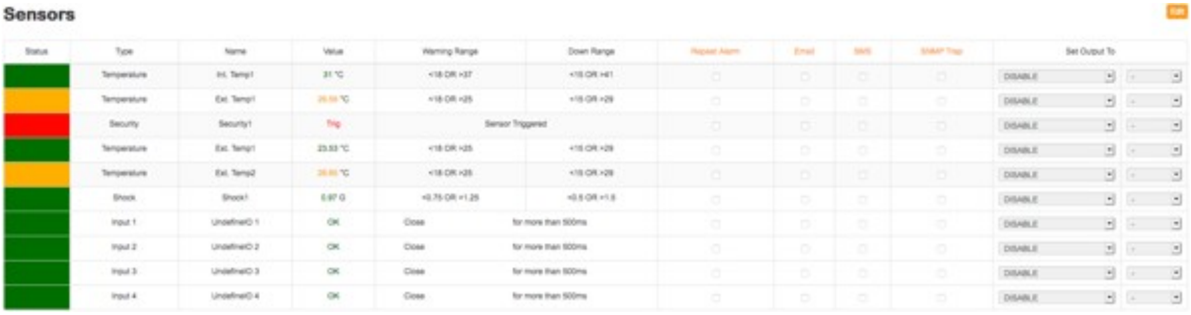
OUTPUTS: To drive a siren, lamp/strobe or any output device



17.7 SensorHub web interface

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

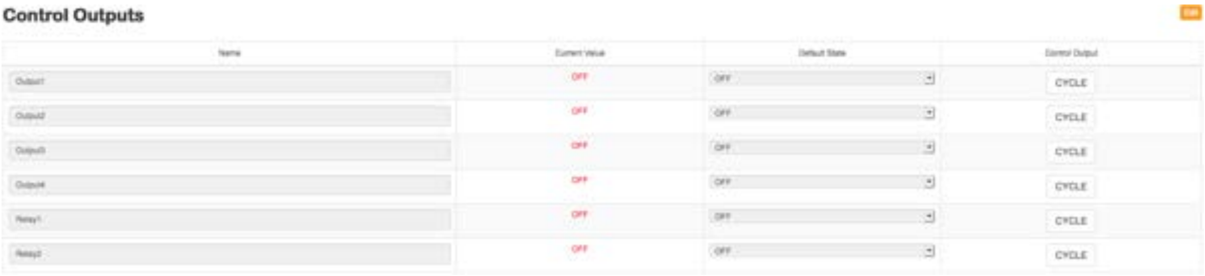
Expansion of probes along with Inputs along with a new option for outputs.



Sensors

Status	Type	Name	Value	Warning Range	Down Range	Repeat Alarm	Email	SMS	SNMP Trap	Set Output To	
🟩	Temperature	Int. Temp1	31 °C	<18 OR >37	<15 OR >41	□	□	□	□	DISABLE	-
🟧	Temperature	Ext. Temp1	[illegible] °C	<18 OR >25	<15 OR >29	□	□	□	□	DISABLE	-
🟥	Security	Security1	Trig	Sensor Triggered		□	□	□	□	DISABLE	-
🟩	Temperature	Ext. Temp1	23.53 °C	<18 OR >25	<15 OR >29	□	□	□	□	DISABLE	-
🟧	Temperature	Ext. Temp2	[illegible] °C	<18 OR >25	<15 OR >29	□	□	□	□	DISABLE	-
🟩	Shock	Shock1	0.97 G	<0.75 OR >1.25	<0.5 OR >1.5	□	□	□	□	DISABLE	-
🟩	Input 1	UndefinedIO 1	OK	Close	for more than 500ms	□	□	□	□	DISABLE	-
🟩	Input 2	UndefinedIO 2	OK	Close	for more than 500ms	□	□	□	□	DISABLE	-
🟩	Input 3	UndefinedIO 3	OK	Close	for more than 500ms	□	□	□	□	DISABLE	-
🟩	Input 4	UndefinedIO 4	OK	Close	for more than 500ms	□	□	□	□	DISABLE	-

Outputs



Control Outputs

Name	Current Value	Default State	Control Output
Output1	OFF	OFF	CYCLE
Output2	OFF	OFF	CYCLE
Output3	OFF	OFF	CYCLE
Output4	OFF	OFF	CYCLE
Relay1	OFF	OFF	CYCLE
Relay2	OFF	OFF	CYCLE

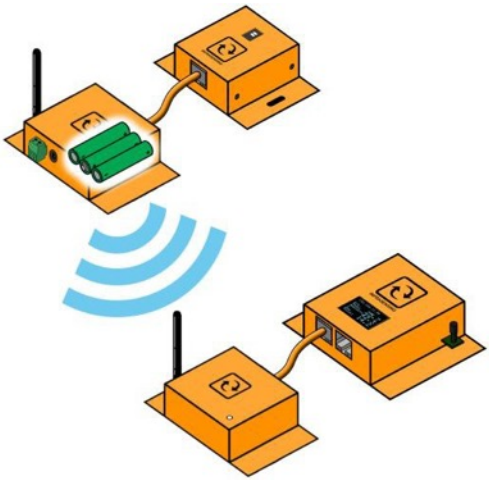
We will discuss triggering outputs in the in section 16.1.

18 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

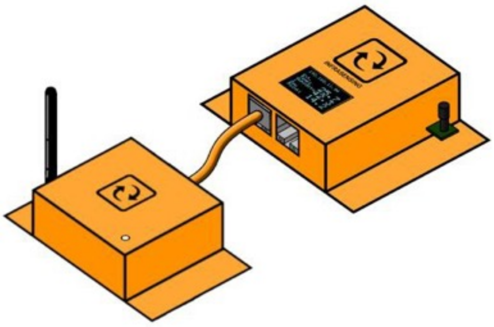
Ethernet Cable

Sensors

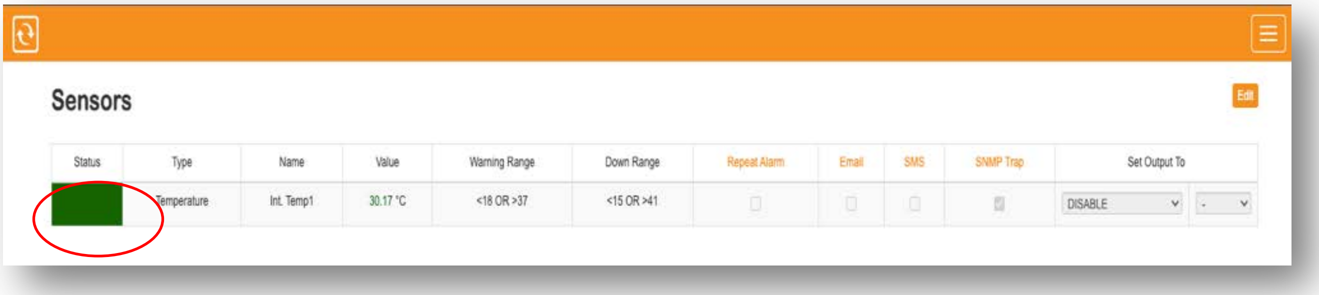
18.1 Connecting and Pairing

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

The Base Unit should be running firmware version 8.9.



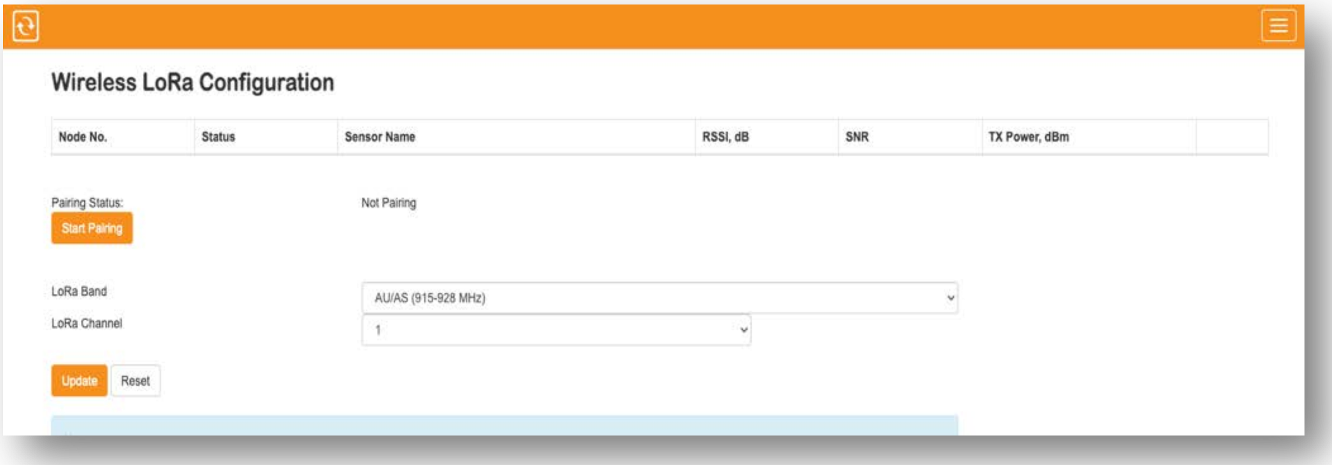
Wireless LoRa should appear in the Base Unit GUI.



Sensors

Status	Type	Name	Value	Warning Range	Down Range	Repeat Alarm	Email	SMS	SNMP Trap	Set Output To	
🟩	Temperature	Int. Temp1	30.17 °C	<18 OR >37	<15 OR >41	□	□	□	☑	DISABLE	-

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



Wireless LoRa Configuration

Node No.	Status	Sensor Name	RSSI, dB	SNR	TX Power, dBm

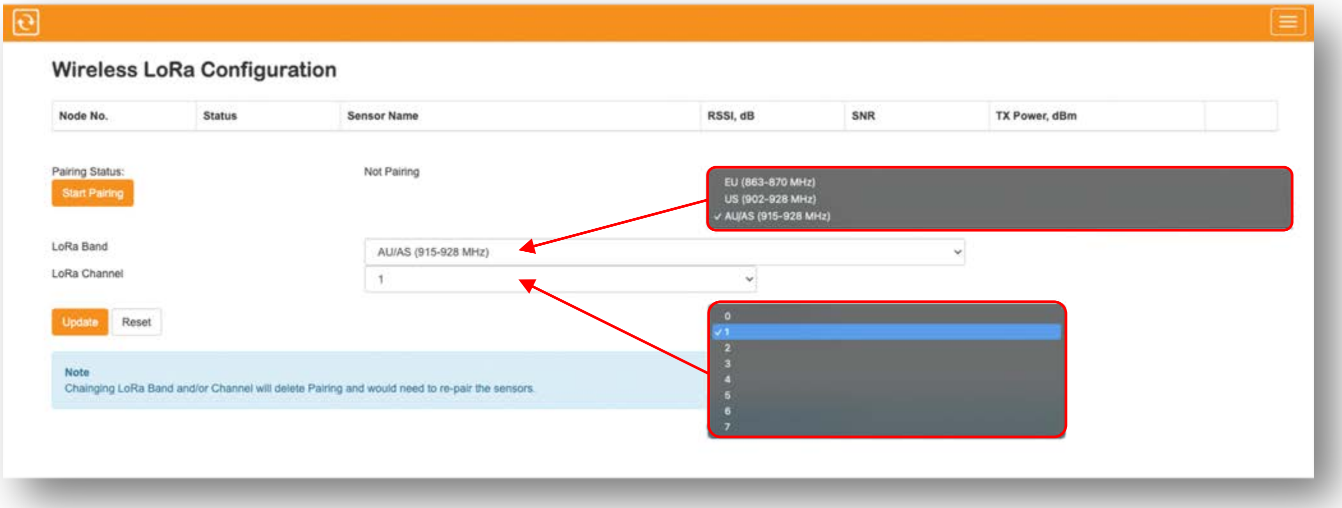
Pairing Status: Not Pairing

LoRa Band: AU/AS (915-928 MHz)

LoRa Channel: 1

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.



Wireless LoRa Configuration

Node No.	Status	Sensor Name	RSSI, dB	SNR	TX Power, dBm

Pairing Status: Not Pairing

LoRa Band: AU/AS (915-928 MHz)

LoRa Channel: 1

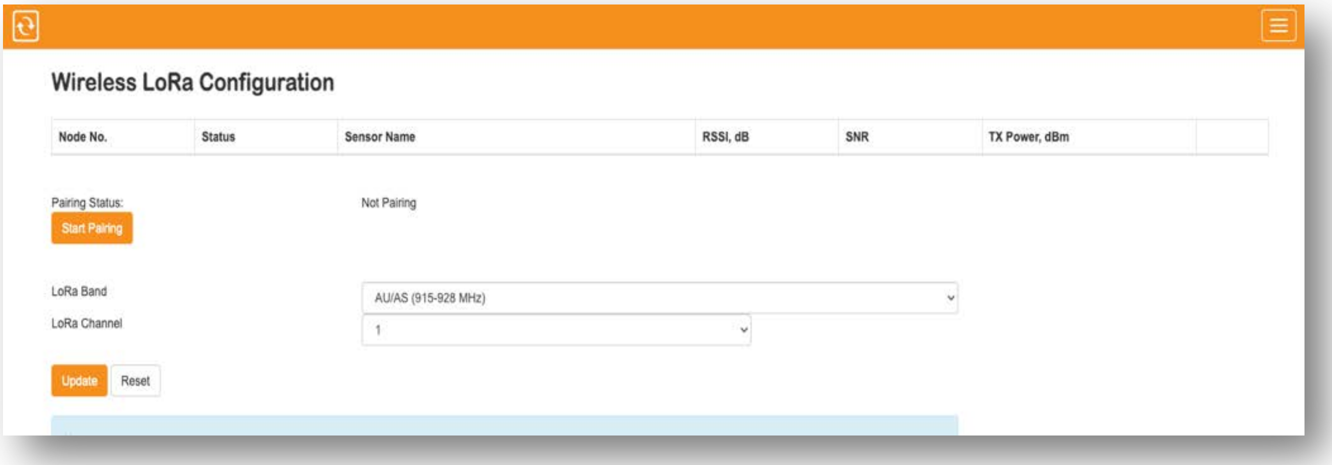
Note
Chainging LoRa Band and/or Channel will delete Pairing and would need to re-pair the sensors.

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.



Wireless LoRa Configuration

Node No.	Status	Sensor Name	RSSI, dB	SNR	TX Power, dBm

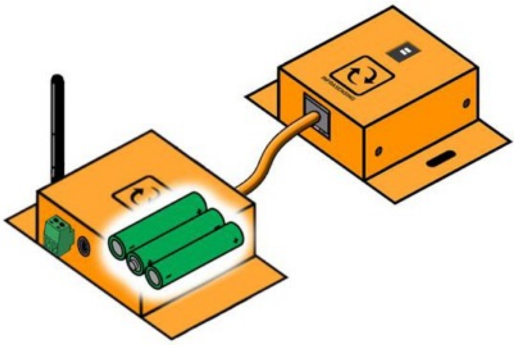
Pairing Status: Not Pairing

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.

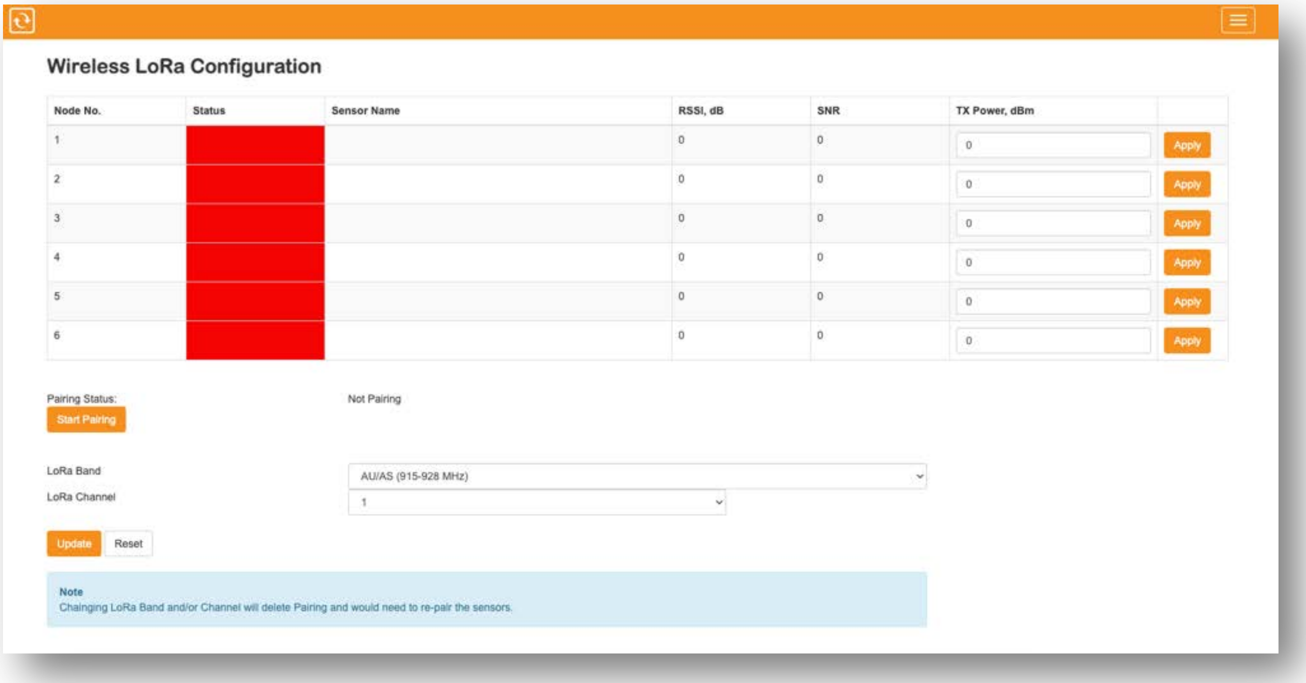


NOTE:

-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.



Wireless LoRa Configuration

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: Not Pairing

Start Pairing

LoRa Band: AU/AS (915-928 MHz)

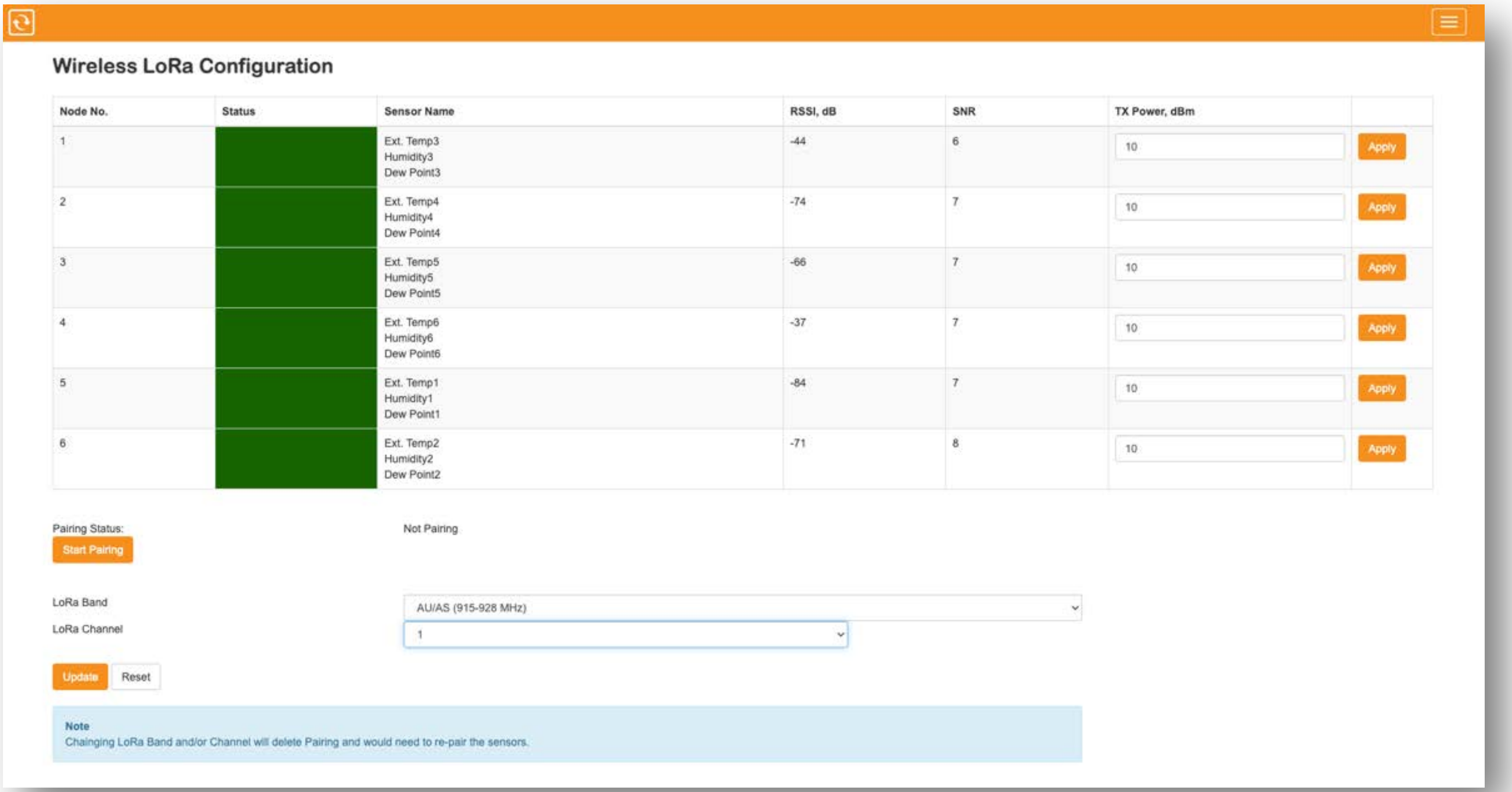
LoRa Channel: 1

Update Reset

Note
Chainging LoRa Band and/or Channel will delete Pairing and would need to re-pair the sensors.

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.



Wireless LoRa Configuration

Node No.	Status	Sensor Name	RSSI, dB	SNR	TX Power, dBm	
1	🟩	Ext. Temp3 Humidity3 Dew Point3	-44	6	10	Apply
2	🟩	Ext. Temp4 Humidity4 Dew Point4	-74	7	10	Apply
3	🟩	Ext. Temp5 Humidity5 Dew Point5	-66	7	10	Apply
4	🟩	Ext. Temp6 Humidity6 Dew Point6	-37	7	10	Apply
5	🟩	Ext. Temp1 Humidity1 Dew Point1	-84	7	10	Apply
6	🟩	Ext. Temp2 Humidity2 Dew Point2	-71	8	10	Apply

Pairing Status: Not Pairing

LoRa Band: AU/AS (915-928 MHz)

LoRa Channel: 1

Note
Chainging LoRa Band and/or Channel will delete Pairing and would need to re-pair the sensors.

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 (16.1.3)” of this document.

19 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.

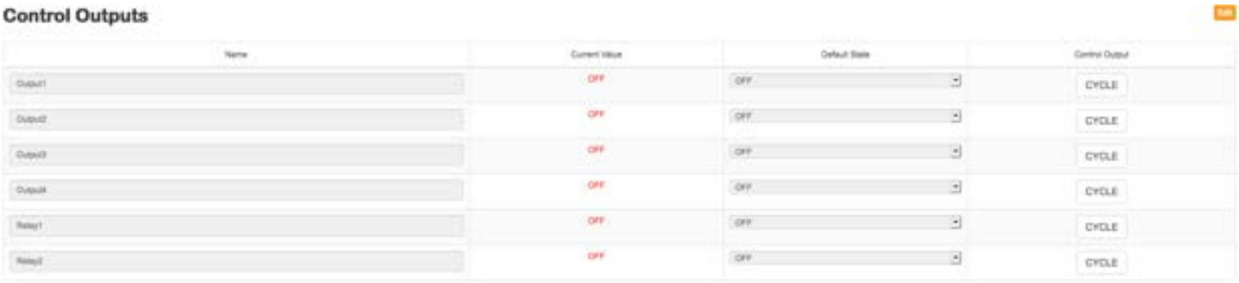
Requirement:
To use the control features you need a Base Unit with firmware 6 or higher and with an IO sensor or a SensorHub.

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.

19.1 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.

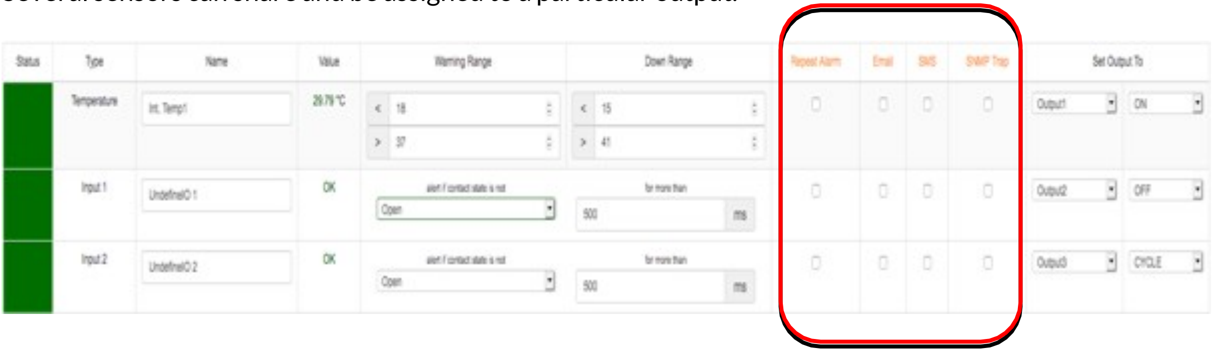


Control Outputs

Name	Current Value	Default State	Control Output
Output1	OFF	OFF	CYCLE
Output2	OFF	OFF	CYCLE
Output3	OFF	OFF	CYCLE
Output4	OFF	OFF	CYCLE
Relay1	OFF	OFF	CYCLE
Relay2	OFF	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.

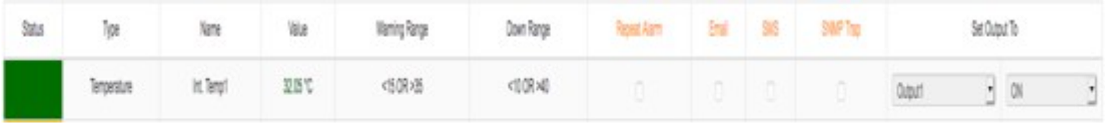


Status	Type	Name	Value	Warning Range	Down Range	Repeat Alarm	Email	SMS	SNMP Trap	Set Output To	
🟩	Temperature	Int. Temp1	29.79 °C	< 18 > 37	< 15 > 41	☐	☐	☐	☐	Output1	ON
🟩	Input 1	UndefinedIO 1	OK	alert if contact state is not Open	for more than 500 ms	☐	☐	☐	☐	Output2	OFF
🟩	Input 2	UndefinedIO 2	OK	alert if contact state is not Open	for more than 500 ms	☐	☐	☐	☐	Output3	CYCLE

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

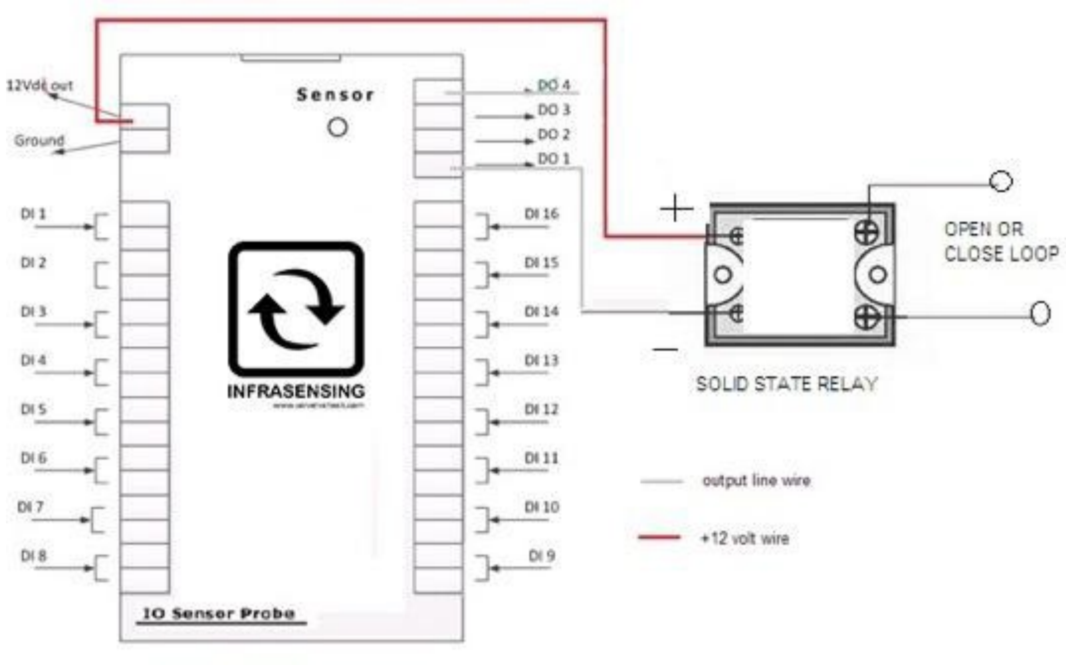


Status	Type	Name	Value	Warning Range	Down Range	Repeat Alarm	Email	SMS	SNMP Trap	Set Output To	
🟩	Temperature	Int. Temp1	32.05 °C	<15 OR >35	<10 OR >40	☐	☐	☐	☐	Output1	ON

- 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

19.2 Wiring for a control output

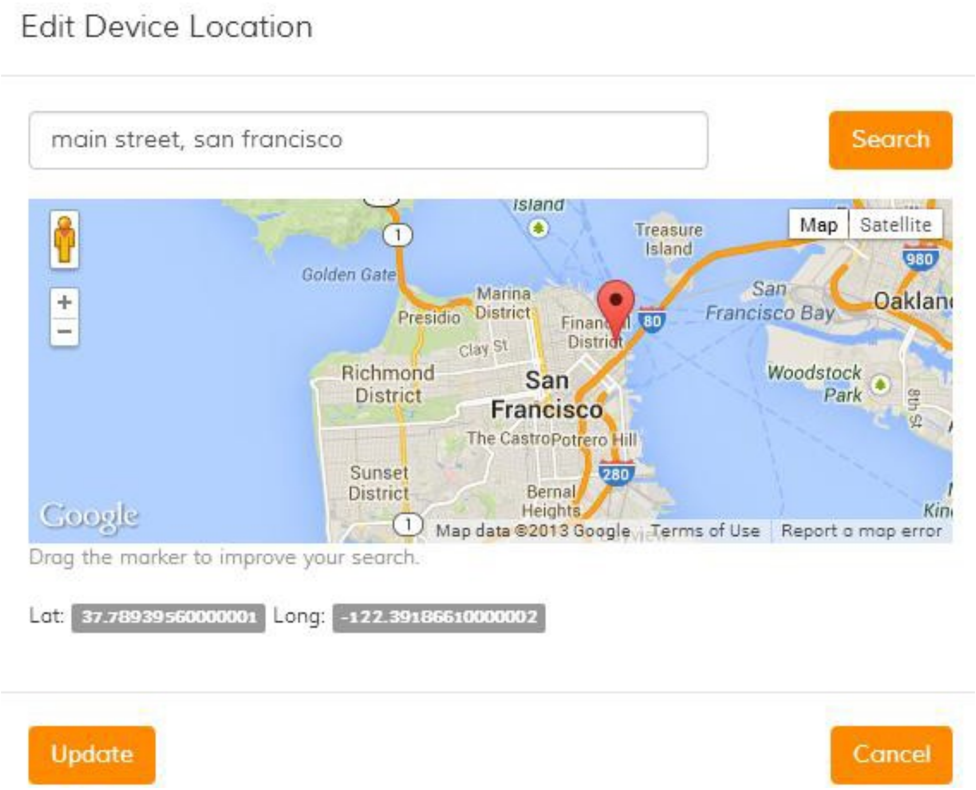
Now that we have those configured, for the output wiring, kindly refer to**section13.6**. If an external relay will be used, refer to the following diagram:



19.3 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.



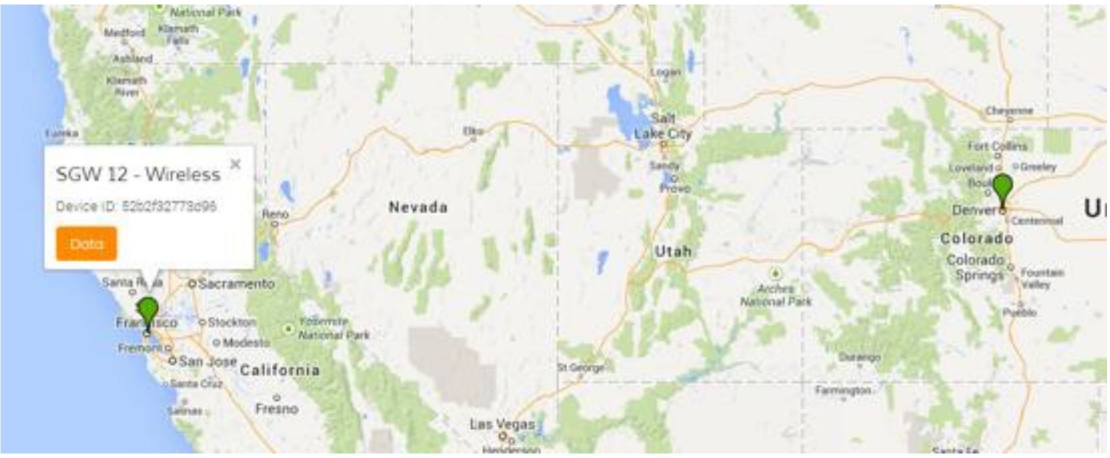
Edit Device Location

main street, san francisco

Drag the marker to improve your search.

Lat: 37.78939560000001 Long: -122.39186610000002

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



SGW 12 - Wireless

Device ID: 52b2f32778d96

20 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-XX Base Unit	540 mW
EXP-8HUB SensorHub	588 mW
EXP-WHUB-ZB Wireless Hub	180 mW
EXP-4HUB MultiSensor & Hub	650 mW
ENV-TEMP Temperature Sensor Probe	60 mW
ENV-THUM Temperature/Humidity Sensor Probe	60 mW
ENV-TSURFACE Surface Temperature Sensor Probe	60 mW
ENV-TSTAIN Stainless Steel Temperature Sensor Probe	60 mW
ENV-DUST Optical Dust Particle Sensor Probe	156 mW
ENV-AIRFLW Airflow Sensor Probe	84 mW
ENV-WLEAK-COMBO5M Water Leak Sensor Probe	264 mW
ENV-WSPOT Water Spot Sensor Probe	288 mW
ENV-FLEAK-COMBO Fuel Leak Sensor Probe	264 mW
ENV-THIMG-M Thermal Imaging Sensor	492mW
ENV-NOISE Sound and Noise Level Sensor	360 mW
ENV-TVOC Air Quality Sensor	180 mW
ENV-AIRPRESSURE Differential Air Pressure Sensor	240 mW
DAISY -STARTER Daisy Chain Controller	252 mW
DAISY-IRSPOT Daisy Chain IR Sensor	204 mW
ENV-WLEAK-LOC-COMBO5 Water Leak Location Sensor Probe	1200 mW
SEC-LUX Light Sensor lux	60 mW
SEC-SOUND Sound Pressure Sensor Probe	312 mW
SEC-SMOKE Smoke Sensor Probe	204 mW
SEC-DOOR Door Security Probe	204 mW
SEC-SHOCK Shock Sensor Probe	72 mW
SEC-MOTION Motion Sensor	456 mW
PWR-AC-QUAL Power Quality Sensor	2040 mW
PWR-AC-VOLT AC Voltage Sensor	276mW
AC-Volt with voltage transducer	864 mW
PWR-AC-CUR AC Current Sensor	384 mW
PWR-AC-FAIL AC Power Failure Sensor	216 mW
PWR-FUEL Fuel Sensor Probe	1008 mW
PWR-DC-VOLT DC Meter Probe	276 mW
DC Probe with Current Transducer	660 mW
PWR-GROUND Grounding Sensor	36 mW
IND-IO IO Probe	371 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).

21 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 order page or from your my.infrasensing.com account.

If purchased from a reseller, add your products to your my.infrasensing.com account.

Customers with an InfraSensing+ agreement enjoy express warranty service for their warranty covered defects.

Warranty covered repairs:

All InfraSensing products are covered by a limited 1 year world-wide warranty as detailed here.
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.