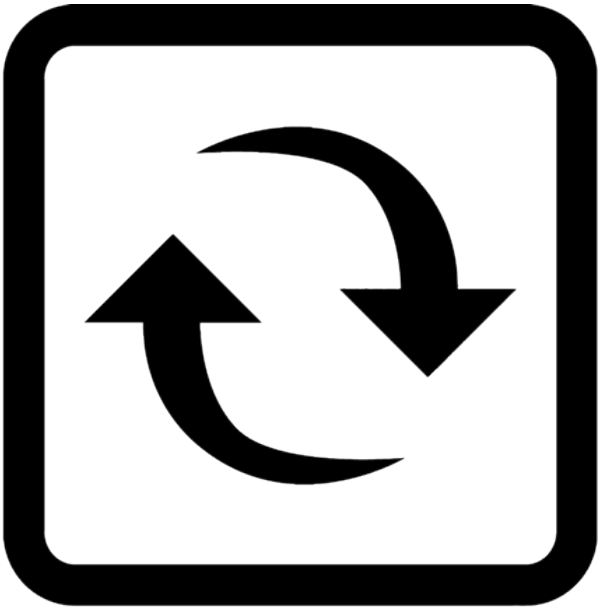
NGP
New Generation Platform
User Manual



INFRASENSING

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

Trademarks:
InfraSensing is a licensed trademark by InfraSensing Distribution BV. All other trademarks or registered marks in this manual belong to their respective manufacturers.

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

Table of Contents

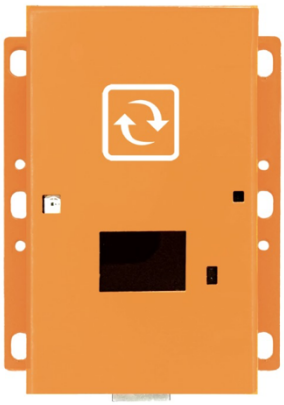
1 Base Unit Quick Overview

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. Below are the Base Units that are compatible with Firmware version 10:

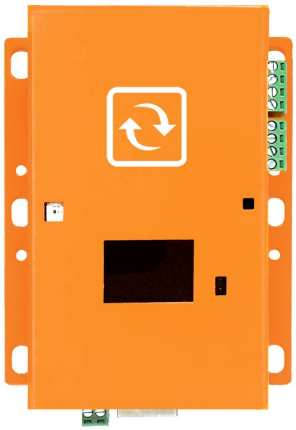
BASE-5

BASE-SM-5-24V

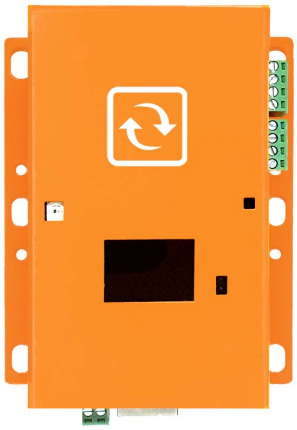
BASE-PI-5-24V



BASE-6



BASE-SM-6



BASE-PI-6

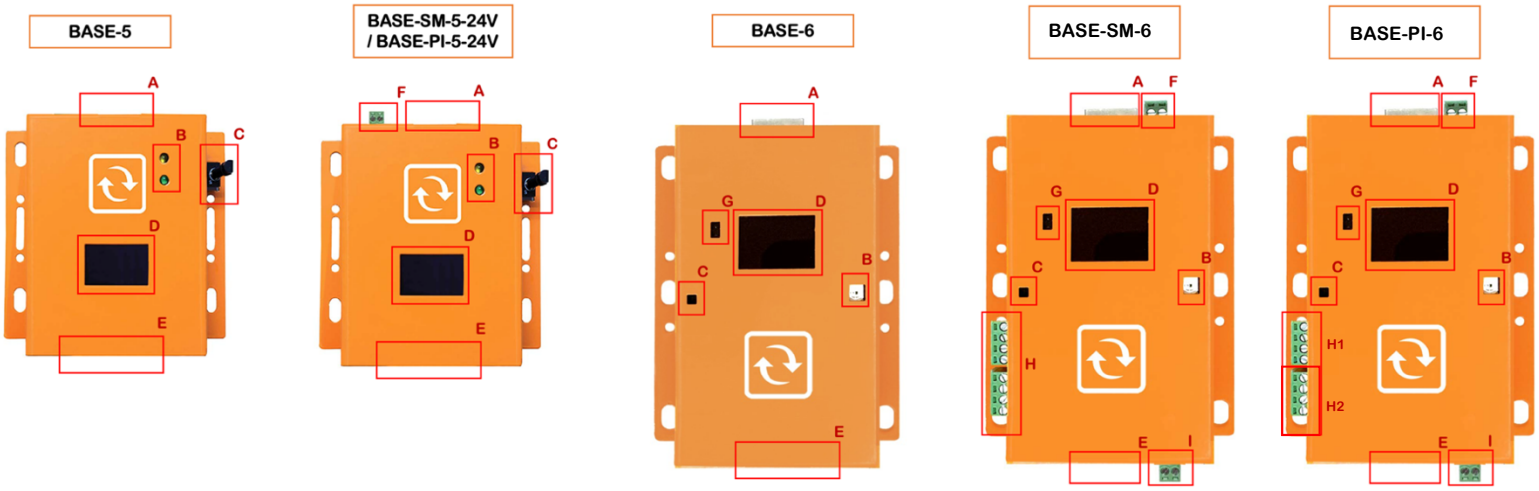
The Base Unit is connected to the network via a standard network cable over a 10/100Mbps network. It supports PoE too. This allows for powering the sensors without having to rely on external power adapters. If you don't have a PoE network then a power adapter is optionally available. Each Base unit is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

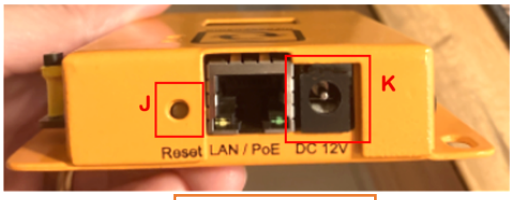
Note : If a power adapter (BASE-PWR) and PoE is plugged into the Base Unit to supply power at the same time the Base Unit will automatically switch to the power adapter and use the PoE as backup. Also the Base Unit will not shutdown or restart if either one is unplugged.

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

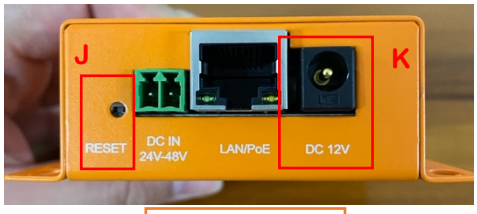
The maximum tested length between a PoE switch and the Base Unit is 330ft or 100meters (using Cat6 shielded cables). Actual results may vary depending on cable quality, switch and environmental factors.

1.1 Base Unit Hardware Overview





BASE-5



BASE-6

A. Ethernet/PoE Port – for network and PoE connection via RJ45
B. Status LED
    a. Yellow (Network) – Stable = Network established, No Light = No Network
    b. Green (Sensor) – Stable =External Probe detected, No Light = No External Probe
    c. In v6 the LED status is turns orange and red as an indicator
C. Int. Temp. – Base Unit's built in Temperature Sensor
D. OLED Screen
    a. OLED displays a rolling banner that has the following information:
        - Base Unit IP Address
        - Date
        - Time
        - Internal Temperature of Base Unit
E. Sensor Probe Ports – where sensor probes connect via RJ45
F. Power supply input – another option to power up the base unit with 12v DC to 24v DC input via the terminal block
G. Proximity sensor – this feature activates when motion is detected or when you hover your hand above it, causing the OLED display to light up, this can also be disabled.
H. RS485 output Slave (BASE-SM6)
H1. Relay output (BASE-PI-6)
H2. RS485 output Slave (BASE-PI-6)
I. Relay output
J. Reset Button - Pressing the Reset button will present you with three options: '**Start Webserver**', '**Reboot**', and '**Load Defaults**'. To perform any of the options, hold the reset button until the desired option appears on the OLED display. Once the desired option is displayed, release the reset button.

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

1.2 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 LEDs 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 ale to sync with NTP (time) server

Reboot, New Firmware Uploaded

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

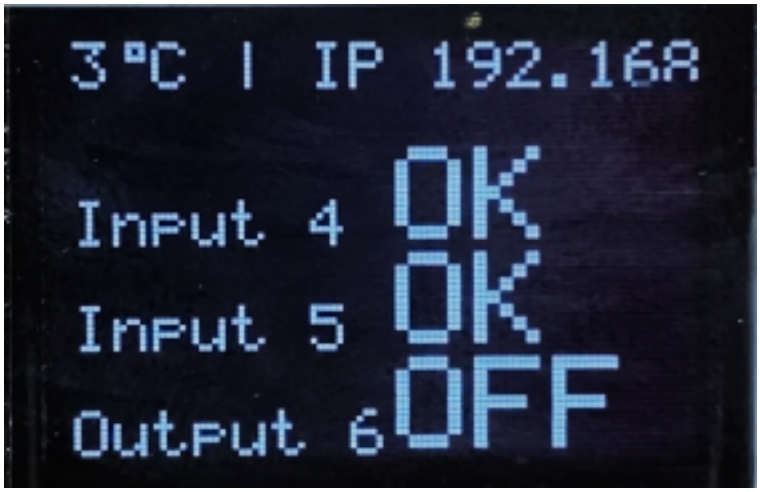
Updating firmware state: takes around 20 seconds
Green LED stays ON
Yellow LED will flash very fast (about 1/10 seconds)

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

Note :

Various options will appear including Start, Webserver, Reboot, and Load Default, depending on how long the reset button is pressed.

1.3 OLED Display Subscripts



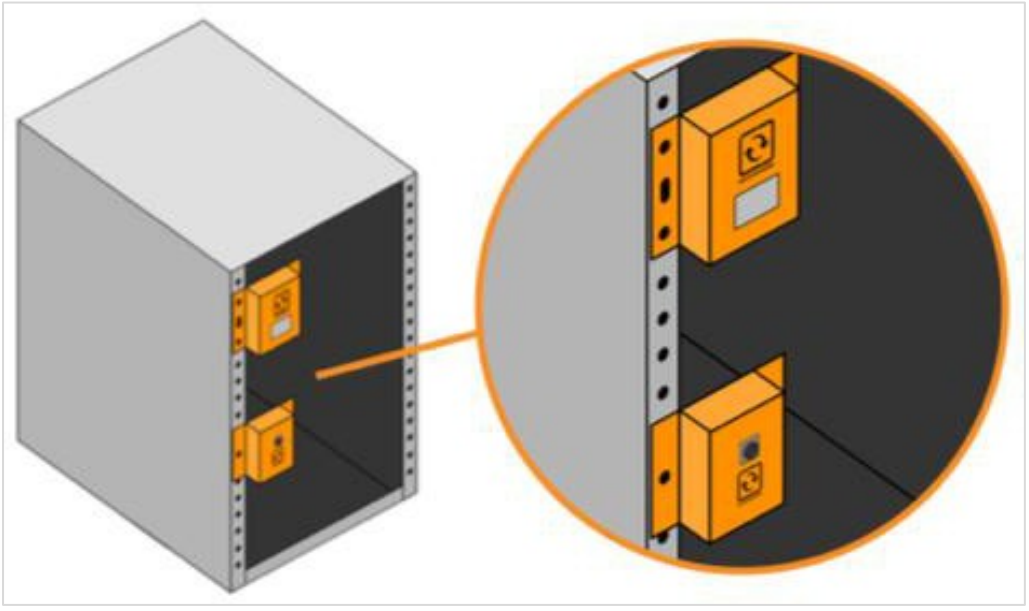
The OLED displays a rolling banner of the values the Base Unit is reading. The reference for the order of the subscript numbering is completely dependent on how the web page is showing it.

1.4 Mounting Options

1.4.1 0U Rack Mounting

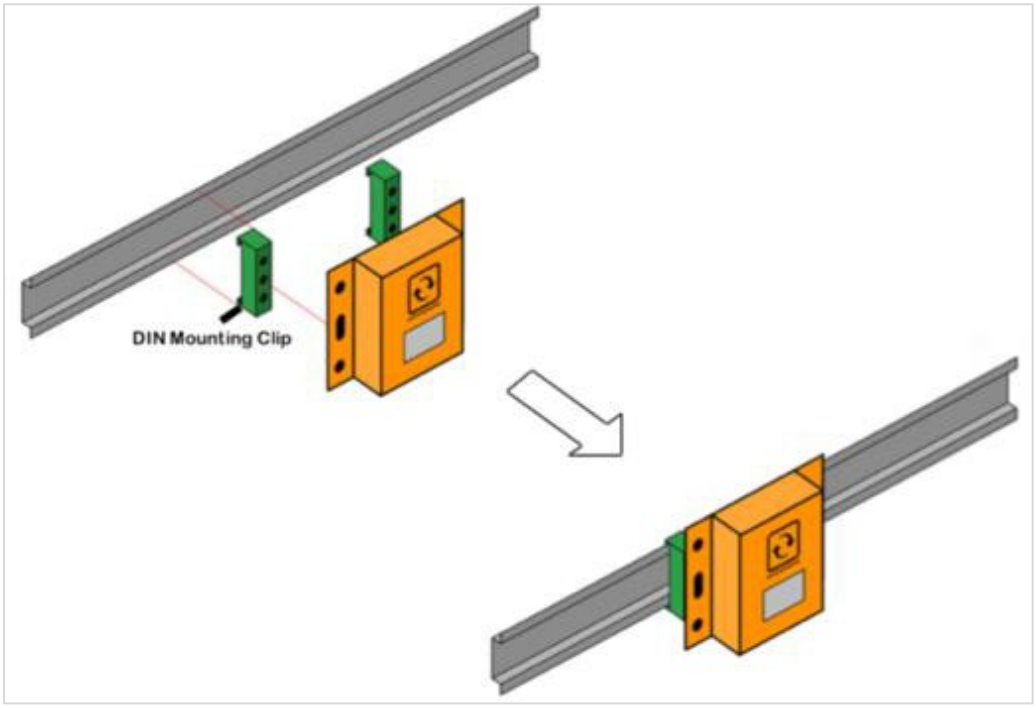
The Base Unit and most of our sensors are 0U devices that can be easily and securely mounted in a rack using standard rack mount screws with a head of at least 0.65cm / 0.26inch. Although one screw is sufficient to hold the whole equipment in place, a second one improves stability.

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.



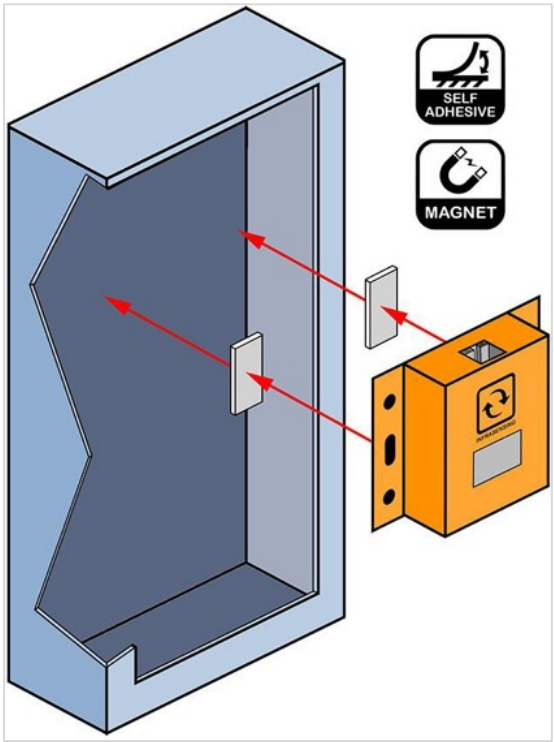
1.4.2 DIN Rail Mounting

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



1.4.3 Magnetic Mounting

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



2 Accessing the Base Unit

1. Ensure that the Base Unit is powered up (via PoE or Power Adapter) and connected to the network.

2. Connect the sensor to the Base Unit port using an RJ45 LAN cable. Please note that the THIMG sensor is not currently supported by this firmware. Please see section 13 for further details about limitation

3. By default, the Base Unit is set to obtain an IP automatically (DHCP), the acquired IP will be displayed on the OLED screen in a rolling banner style.

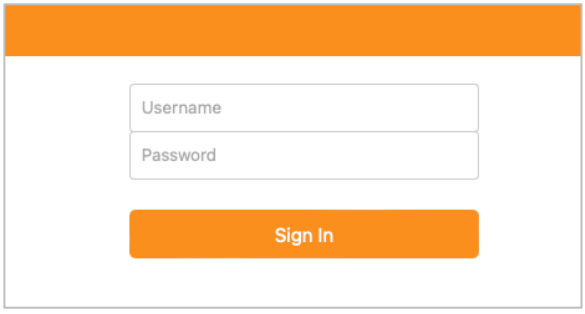
4. On the OLED display, if the IP displays 'Link down' it means no IP address is acquired.

5. Aside from the information on the Banner, the OLED will display readings coming from the connected sensors.

6. In order to access your web UI, type the IP address showing on the OLED on any of your browser. A connection will be made to the web server on board of the Base Unit and you will be prompted for a username & password.

    - The default admin credentials are: **admin / 1234**
    - If you are logging in as a viewer, the default viewer credentials are: **viewer / viewer**

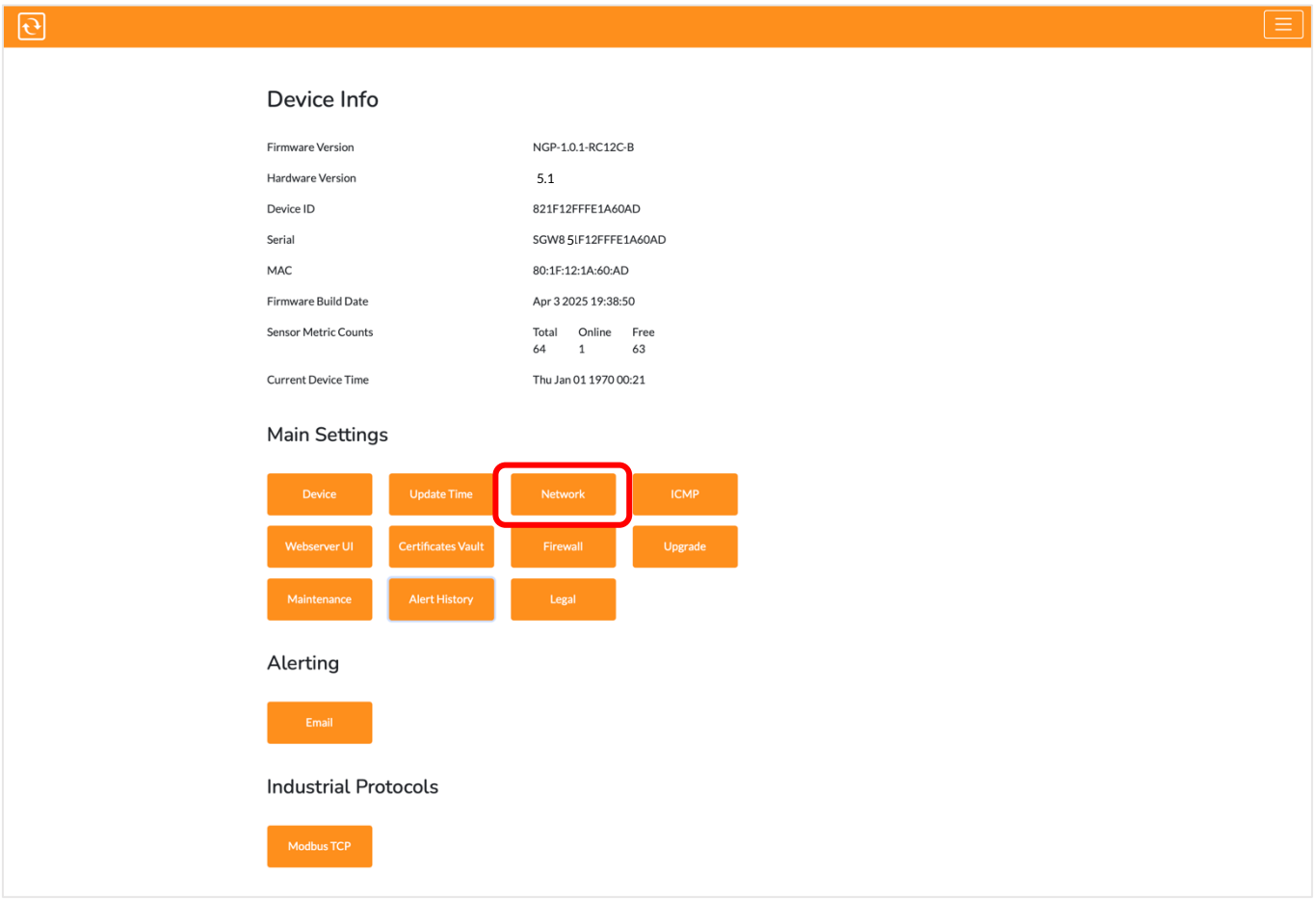
    Note: The device needs to be in the same network as the base unit.



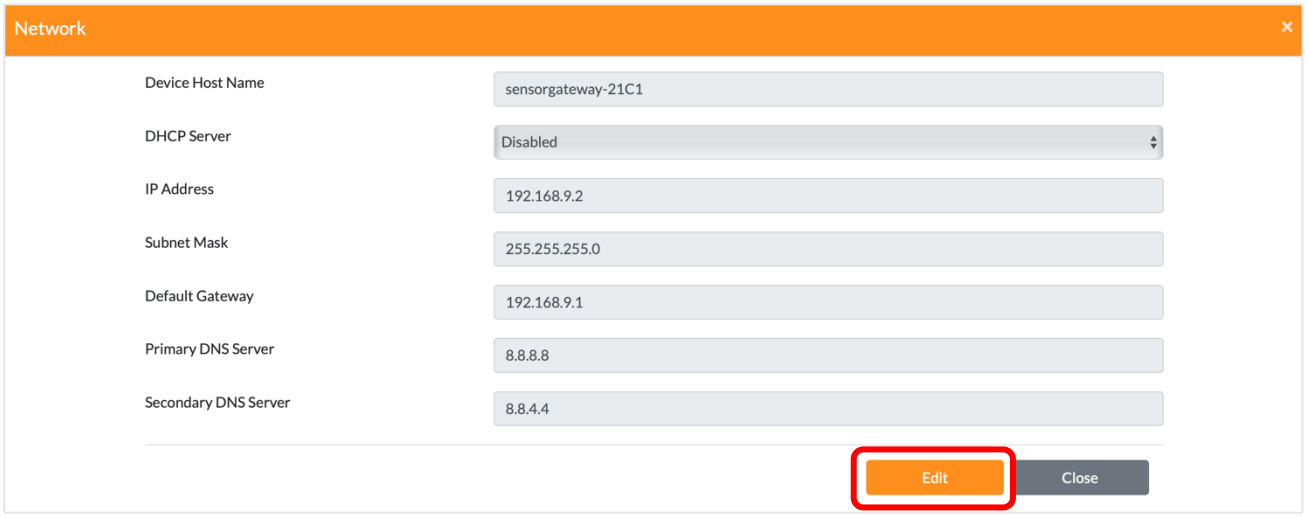
3 Network Configuration

3.1 Hardware version 5

The network configuration for hardware version 5 only supports IPv4. In the main window, click on the Menu Button located on the upper right corner of the page. Then click on settings and look for Main Settings

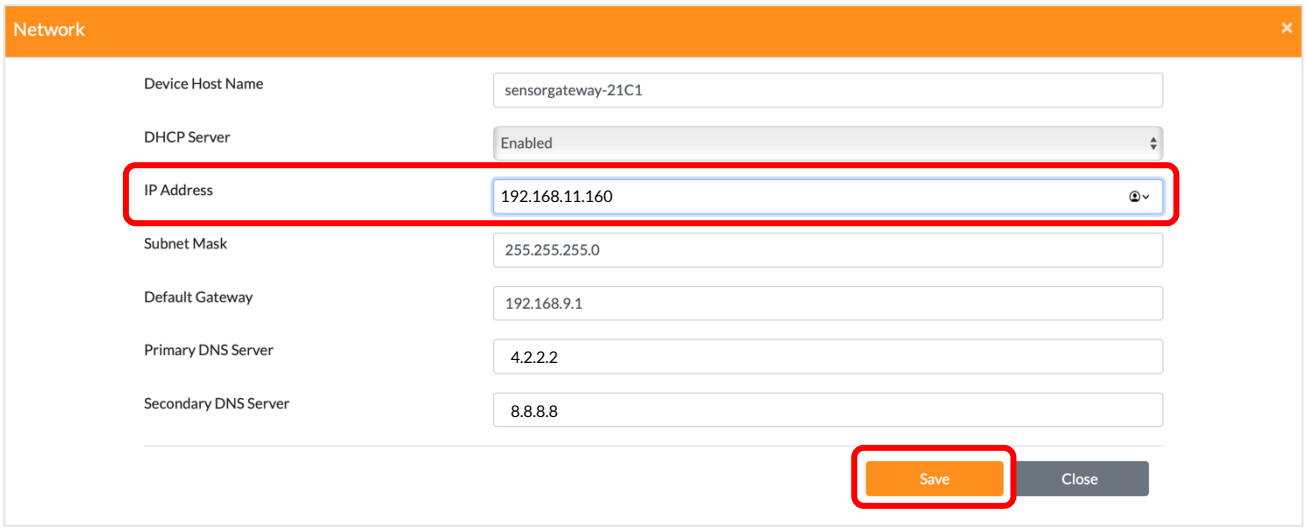


Within Main Settings, click on Network and then select Edit. Here, you can edit or change the IP Address. Once you've made the necessary changes, click the Save button to apply them.



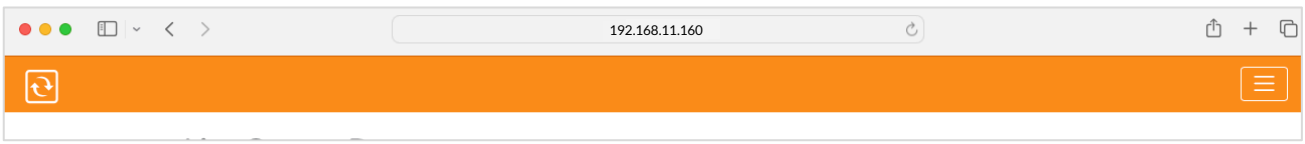
You can now change the Base Unit's IP address to any value you like: either to DHCP or to a fixed IP that would fit your local network. We will now set it to 172.168.0.2 with its default gateway to 192.168.11.160 respectively. As for the DNS server feel free to use any, in this set up, we will use 4.2.2.2 and 8.8.8.8. You can also see the MAC address of the gateway and set the Device Host Name

Note: If you want to make a device accessible via bios name please make sure that the 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 you have updated the IP address to 192.168.11.160, simply hit the **SAVE** button to apply the changes. A notification will appear at the top saying "**Reboot to Apply**". To finalize the changes, click **Reboot to Apply**, which will restart the base unit and apply the updated settings.

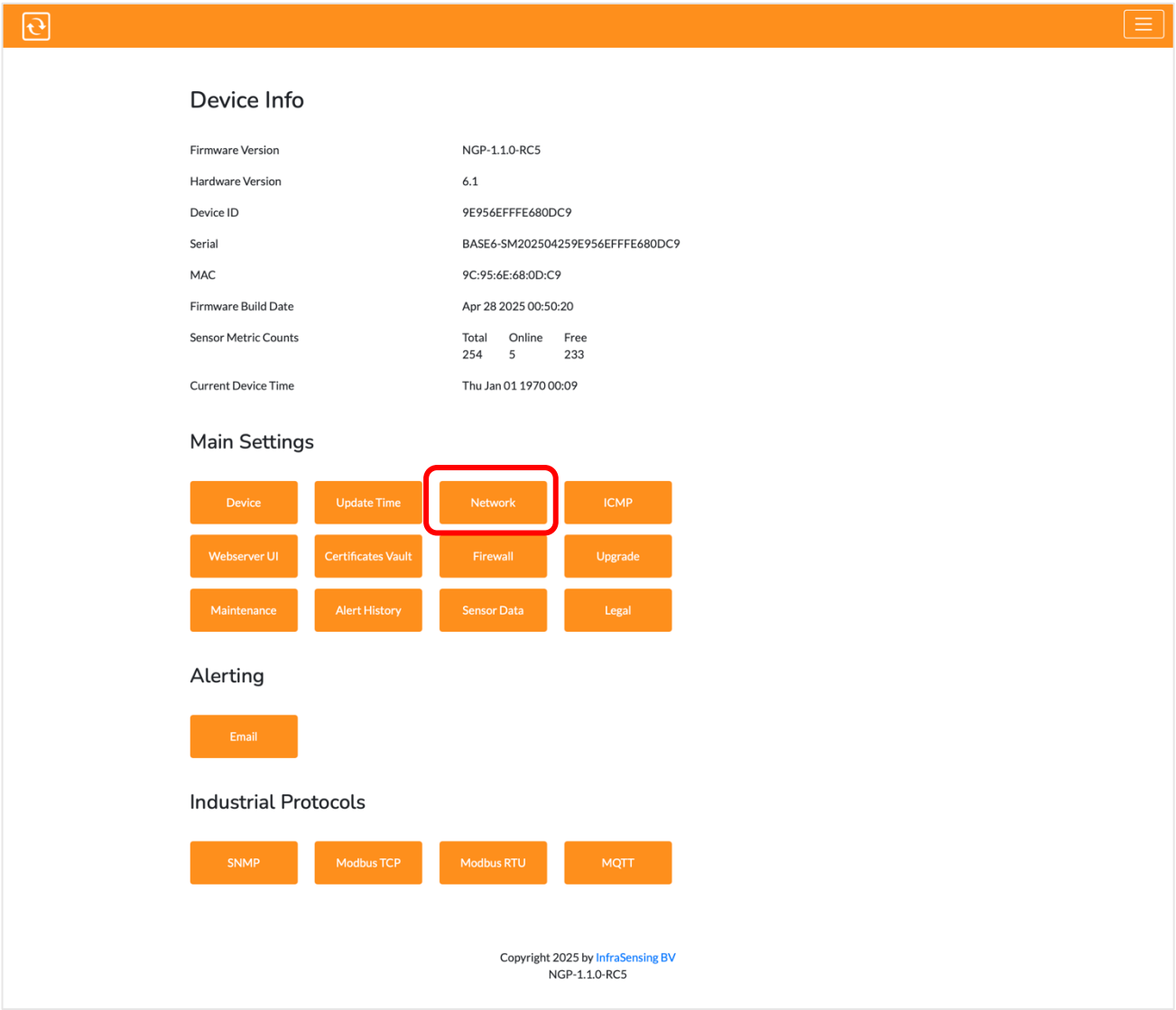
Please note that : if the DHCP Server is set to Disabled it means that it is FIXED.



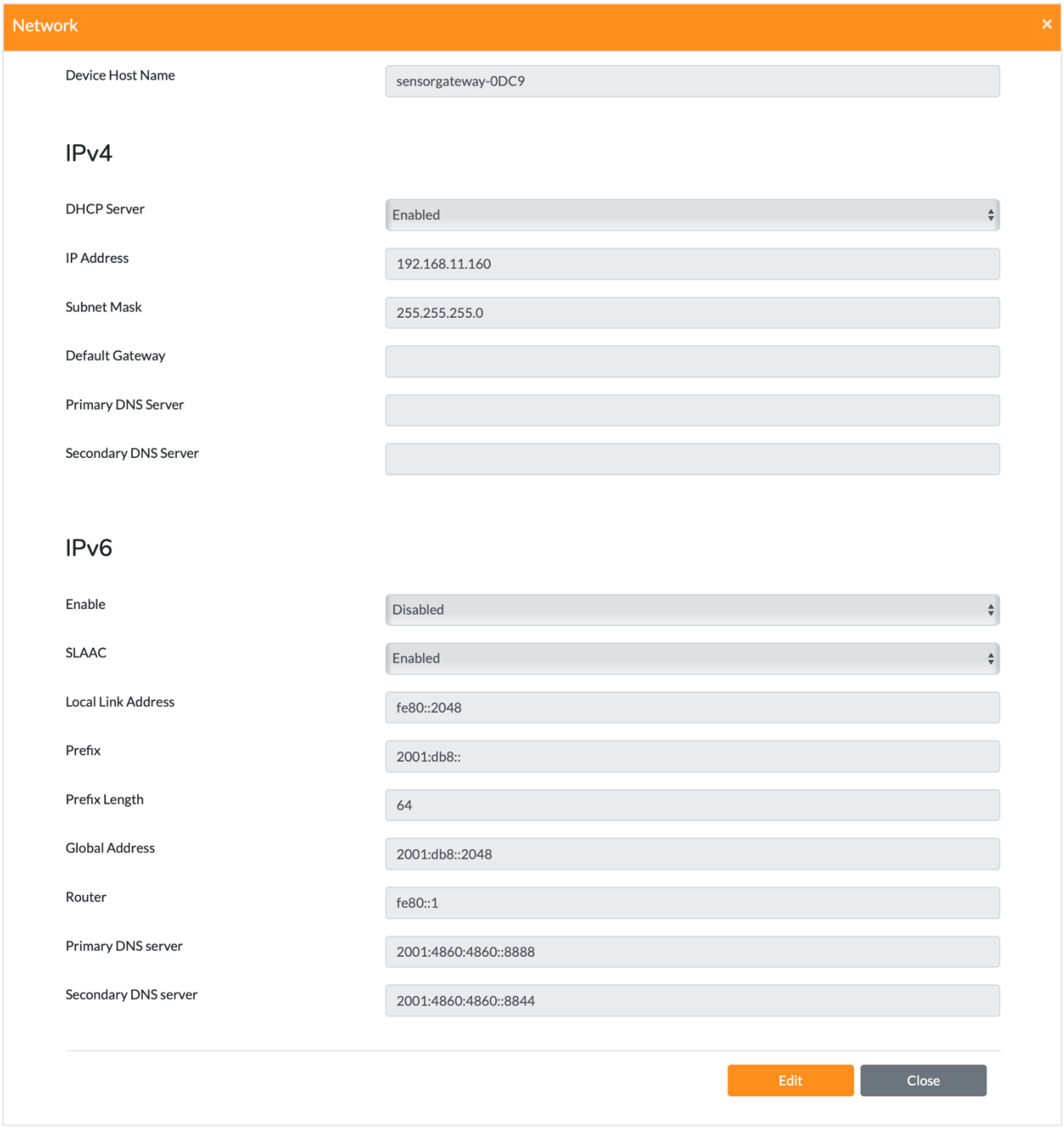
As seen on the image above, We were able to access the gateway via its new IP address since our network segment is set at 192.168.11.160 and we set our computer back to DHCP the gateway is now connected and can be accessed through our network.

3.2 Hardware version 6

In the main window, click on the Menu Button located on the upper right corner of the page. Then click on settings and look for Main Setting



Within Main Settings, click on Network and then select Edit. Here, you can edit or change the IP Address. Once you've made the necessary changes, click the Save button to apply them.



- **Device Host Name** – This is the name of the device on the network. It's like giving your device a nickname to identify it.
- **IPv4** Section – These settings are used for most networks today. Here's what the fields mean:
    - **DHCP Server**
        - If **Enabled,** the device automatically gets its IP address, subnet mask, and other settings from the network's DHCP server.
        - If **Disabled**, you need to manually enter these settings. Disabling the DHCP server means you need to manually assign the device a specific (fixed) IP address.
    - **IP Address**
        - This is the unique address of the device on the network using IPv4.

- **Subnet Mask**
  - Defines which part of the IP address refers to the network and which parts refers to device.

- **Default Gateway**
  - The IP address of the router, acting as the "doorway" to other networks, including the internet.

- **Primary and Secondary DNS Servers**
  - These servers translate domain names (like google.com) into IP addresses. If left blank, the device may default to DNS servers provided by the network.

- **IPv6** Section – This settings are used for newer networks with advanced capabilities.

  - **DHCP Server**
    - If **Enabled,** the device automatically gets its IP address, subnet mask, and other settings from the network's DHCP server.
    - If **Disabled**, you need to manually enter these settings. Disabling the DHCP server means you need to manually assign the device a specific (fixed) IP address.

  - **SLAAC**
    - SLAAC stands for "Stateless Address Auto-Configuration."
    - If this is **Enabled,** the device automatically configures its IPv6 address without needing a DHCP server.

  - **Local-Link Address**
    - This is an IPv6 address that works only within the local network (like a private IPv4 address)

  - **Prefix**
    - This specifies the network part of the IPv6 address. It's like a subnet mask for IPv6.

  - **Prefix Length**
    - This defines how much of the IPv6 address is for the network. A length of 64 is standard for most networks.

  - **Global Address**
    - This is the device's public IPv6 address, used to connect to the internet.

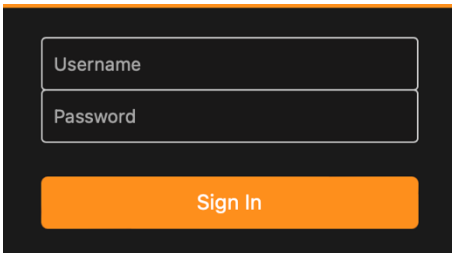
  - **Router**
    - This is the IPv6 address of the router.

  - **Primary and Secondary DNS Servers**
    - These translate website names to IP addresses using IPv6. The primary server is 2001:4860:4860:8888, and the secondary is 2001:4860:4860:8844

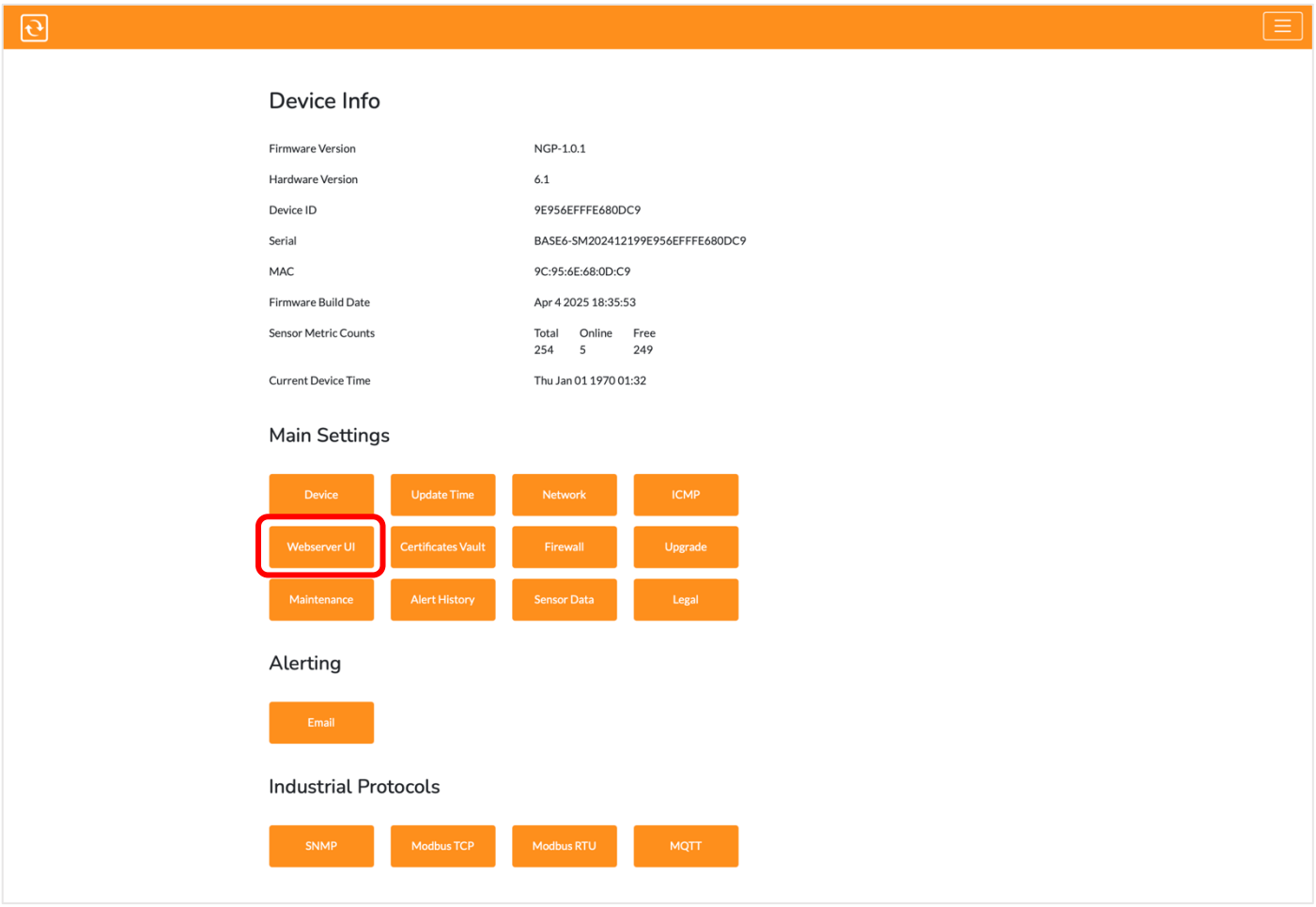
4 Base Unit Security Feature

4.1 Username and Password configuration

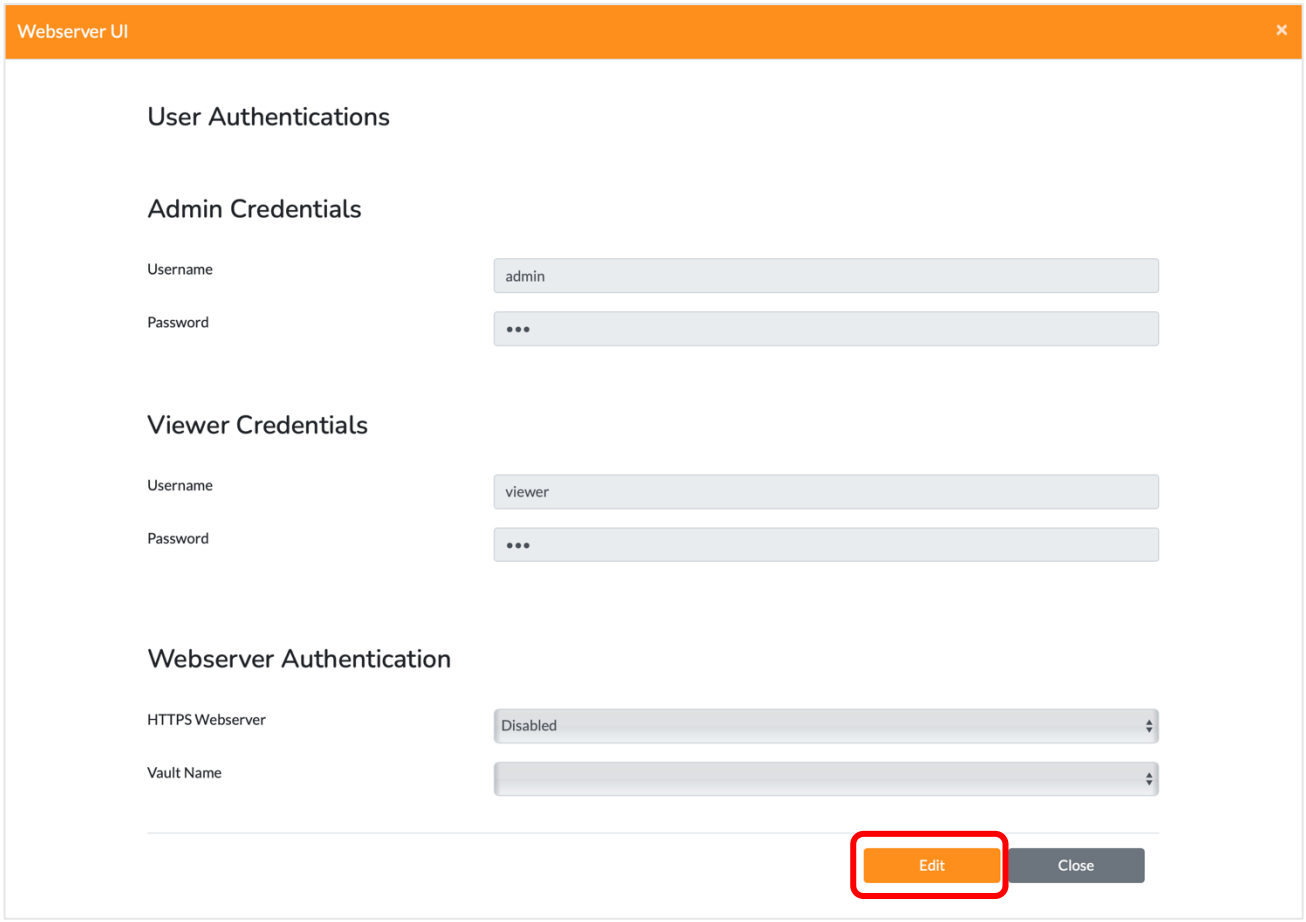
Every time you access your Base Unit, a pop-up message will appear prompting you to enter your username and password.



In the main window, click on the Menu Button located on the upper right corner of the page. Then click on settings and look for Webserver UI under Main Settings.



Within this dedicated section, users have the capability to fine-tune the configuration of **ADMIN** and **VIEWER** credentials. This enables users to establish secure and personalized access levels, granting administrative and viewing privileges as needed for efficient and customized control over the webserver user interface.



Note: The screen is currently in read-only mode, this is to prevent any accidental changes, editing can be initiated by clicking the 'Edit' button. When you click 'Edit' and choose to close without saving by clicking the close button, a warning window will be displayed, asking 'Are you sure you want to close the modal without saving?'

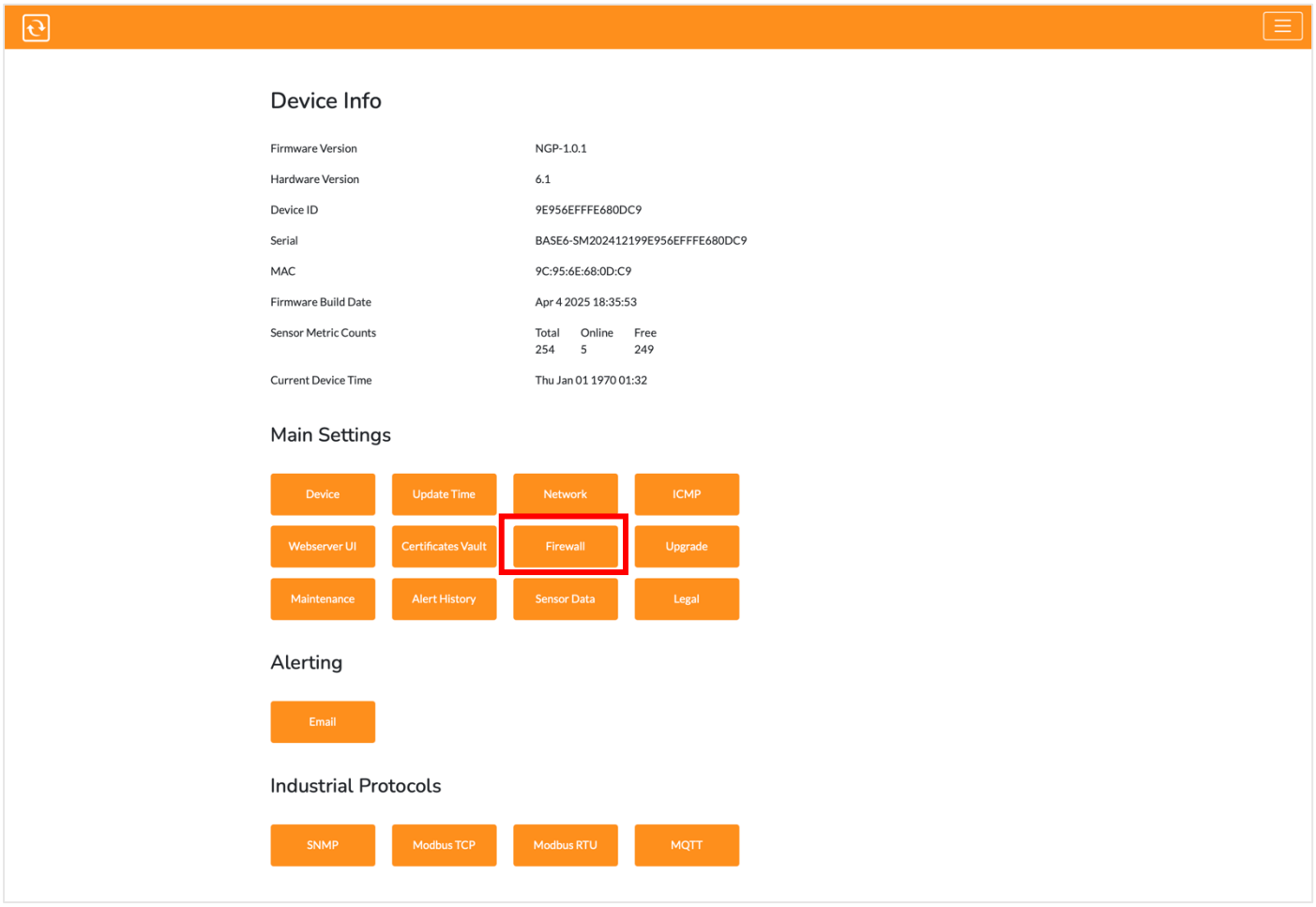
However, after you click the 'Edit' button and proceed to save changes by clicking the save button, a green banner will appear, indicating 'Successfully Saved.'

- **Admin Credentials**
  This set of login credentials grants users the ability to edit information stored within the BASE-WIRED, providing comprehensive control over configuration settings and data management.
  Note: The maximum length for both the username and password in the admin credentials 20 characters.

- **Viewer Credentials**
  Designed for viewers, this set of login credentials ensures access to information on the BASE-WIRED without permitting any editing capabilities. It offers a secure and restricted viewing mode, ideal for those who require information access without the ability to make changes
  Note: The maximum length for both the username and password in the viewer credentials 20 characters.

4.2 Firewall Settings

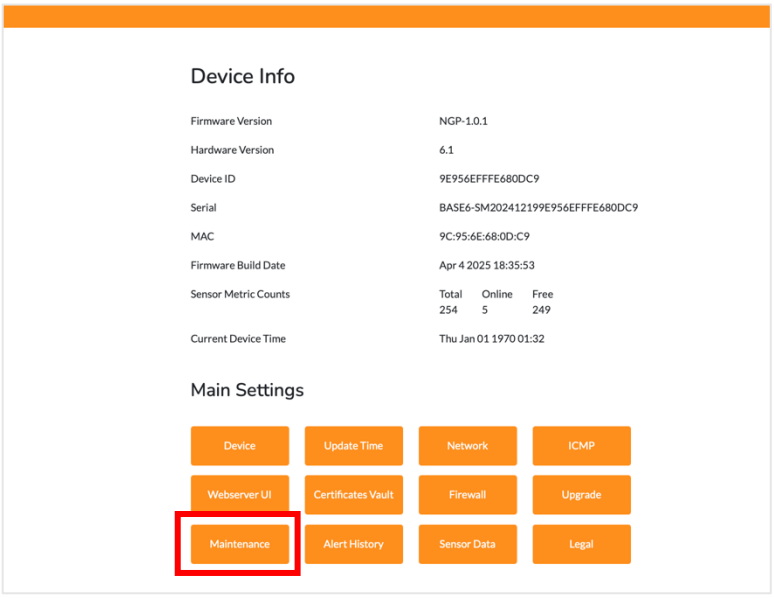
Firewall can be accessed through the Base Unit's settings by clicking on the button on the upper right, and under Main Settings you can find the 'Firewall' option.

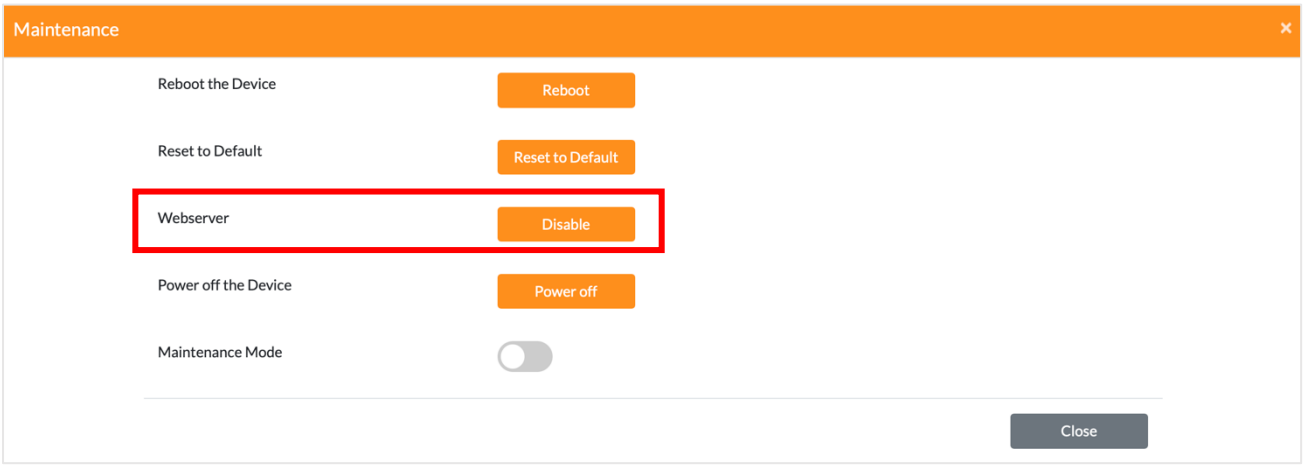


With this feature you may configure it for enhanced security, the firewall is designed to proactively block any unauthorized access attempts to the Base Unit.

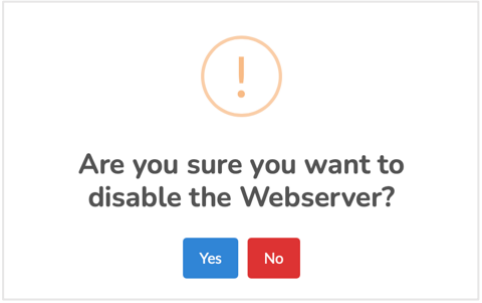
4.3 Enabling and Disabling Web Server

Disabling the web server option restricts the ability to send commands or configure settings. The Webserver option can be accessed through the Base Unit's settings by clicking on the button on the upper right, and under the Main setting click on 'Maintenance' option. To disable it, simply select "Webserver Disable".

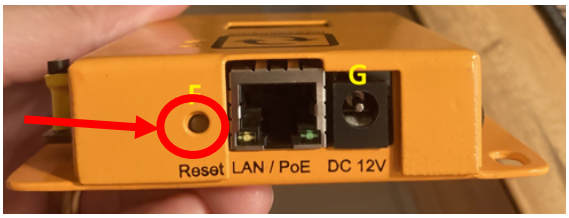




Once you click on "Disable", a pop-up message will appear asking if you want to disable the web server. After you click "Ok" and then "Update", the web server is disabled. You will not be able to load the web server, send commands or configure it.



To re-enable the device, you need to be physically near it. Press and hold the reset button until 'Start Webserver' appears on the OLED display.

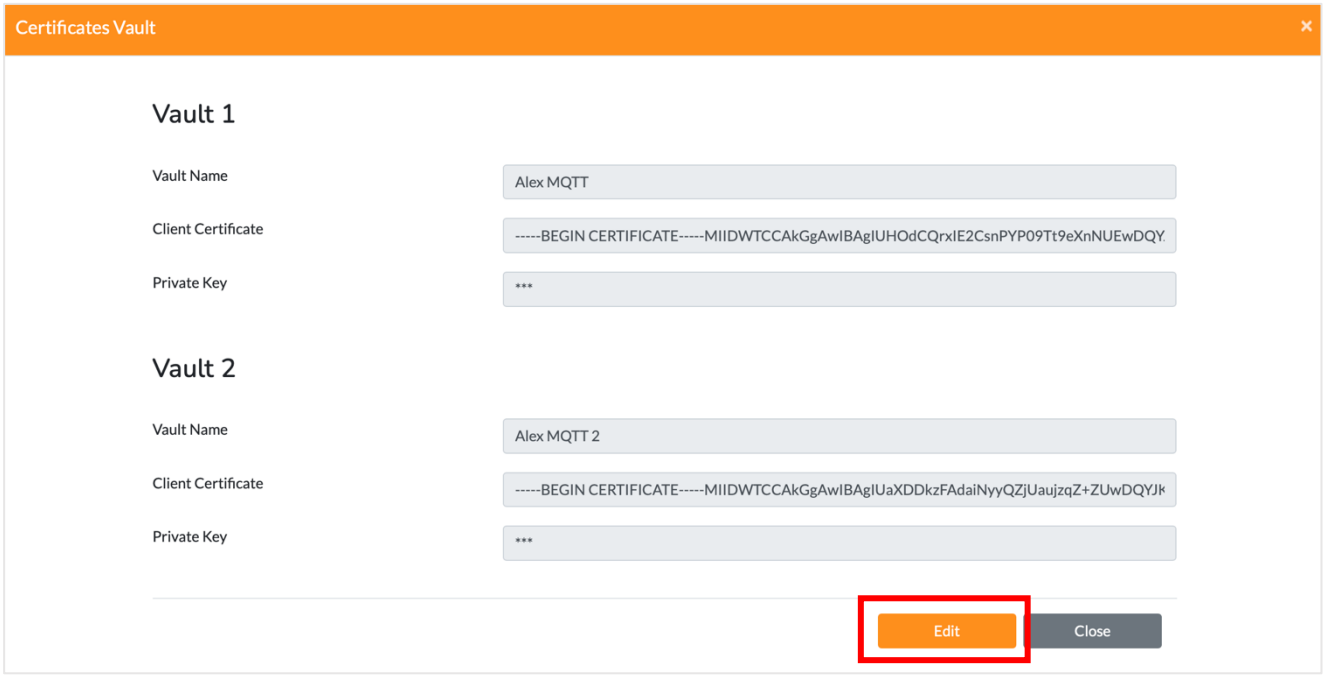


Release the button once you see this message, and the device will be re-enabled. This additional security measure ensures that you must be physically present to manually re-enable the Web Server feature.

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

4.4 Certificates Vault

This feature provides a secure storage space for managing and safeguarding cryptographic keys and certificates.



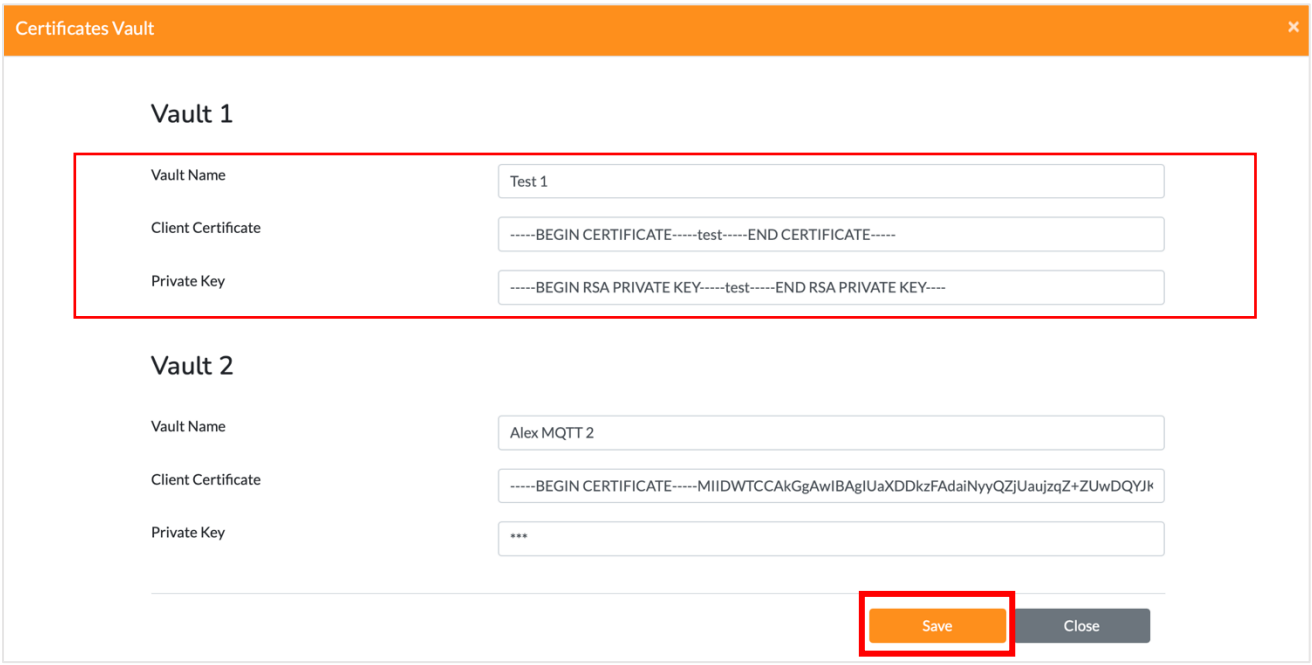
- **Vault Name**
  – Set a custom name based on user preferences.

- **Client Certificate**
  – Input the required certificates. Please note that when copying the client certificate make sure that there are no spaces except for the 'Begin Certificate' and 'End Certificate' parameters.

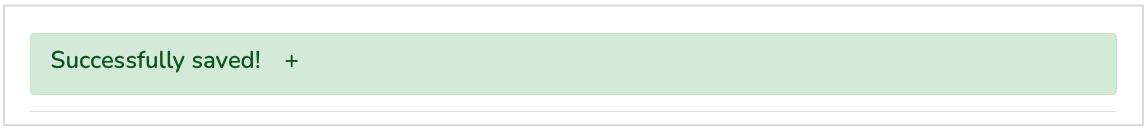
- **Private Key**
  – This is where you can input the string of characters used as a form of authentication or what we called Community String. Please note that when copying the private key make sure that there are no spaces.

In our example below, we will update our Client Certificate and Private key using the following values and publish it to the Base Unit.

Vault Name: Test 1
Client Certificate: -----BEGIN CERTIFICATE-----test-----END CERTIFICATE-----
Private Key: -----BEGIN RSA PRIVATE KEY-----test-----END RSA PRIVATE KEY----



After entering the Client Certificate and Private Key, do not forget to click the 'Save' button. Upon clicking 'Save,' a green banner will appear at the bottom of the pop-up, indicating that the changes have been successfully saved.

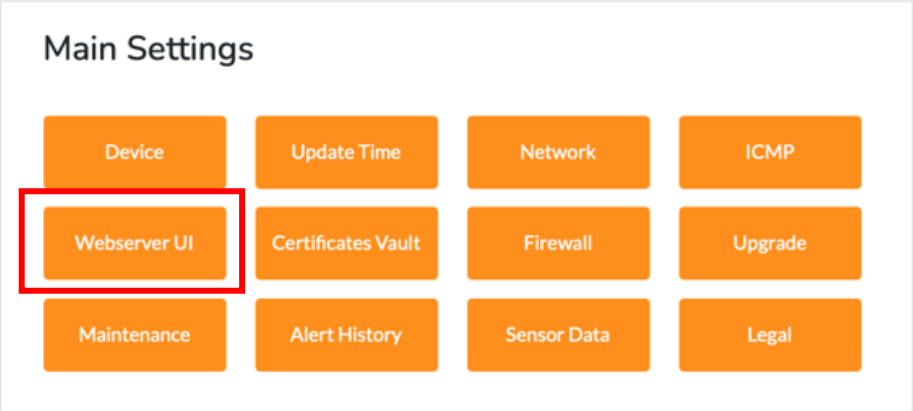


After saving, a button at the top of the page will appear, prompting you to reboot to apply the changes. To implement the modifications, it's essential to reboot the base unit.

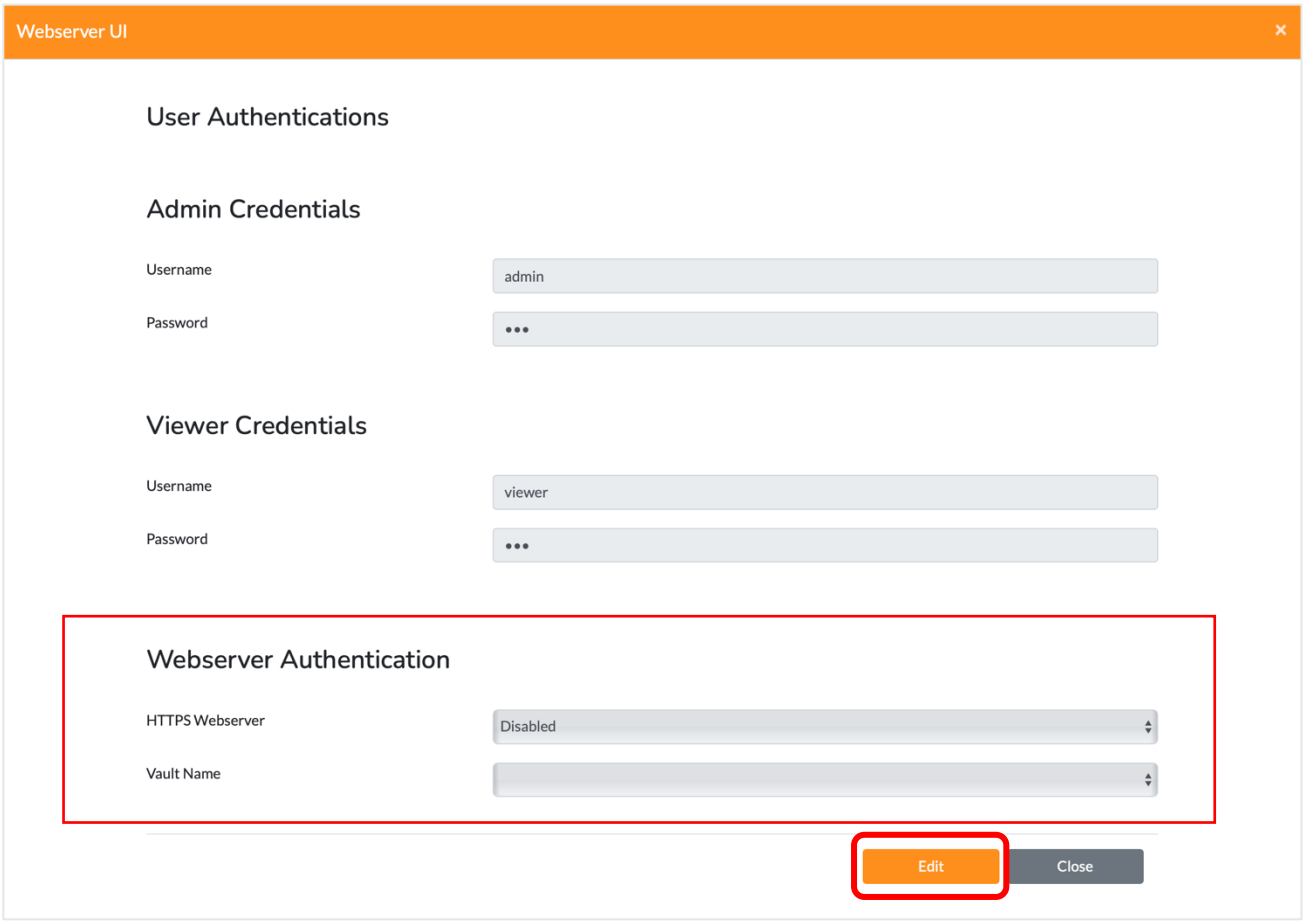
4.5 HTTPS

HTTPS ensures the data exchanged between your browser and the website is encrypted and secure. It protects the integrity and confidentiality of data. In order to enable the HTTPS, access the base unit settings, and under Main Settings, look for the Certificate Vaults.

Note: The HTTPS option is only applicable for hardware version 6.



After updating the Certificates Vault, you may enable the HTTPS webserver and choose your desired certificate from the vault name dropdown. Once you enable the HTTPS webserver and select the vault name from the dropdown, click the Save button to apply the changes.

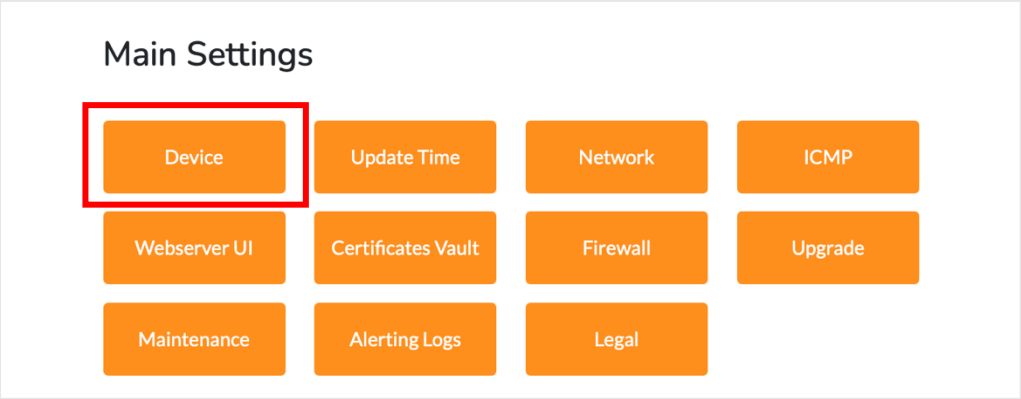


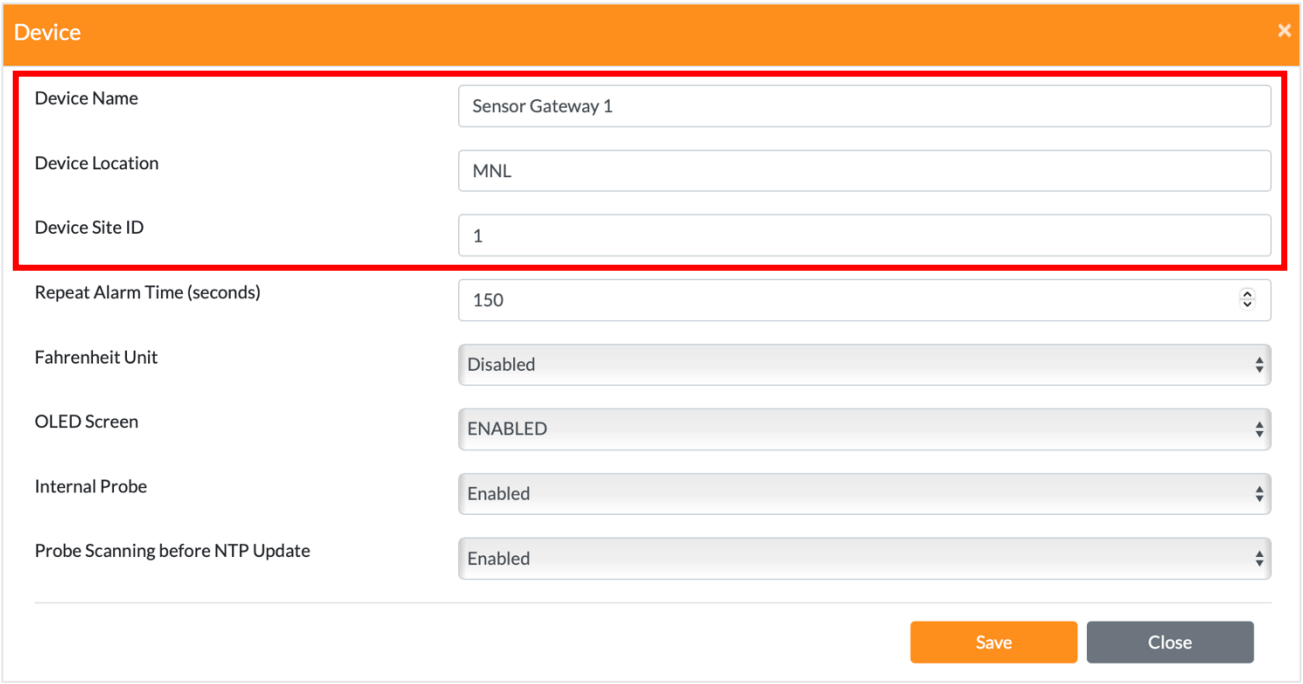
To finalize these changes, click the 'Reboot to Apply' button at the top of the page. This will apply the modifications to the Certificate Vaults and Webserver UI.

5 Base Unit Features

5.1 About Device

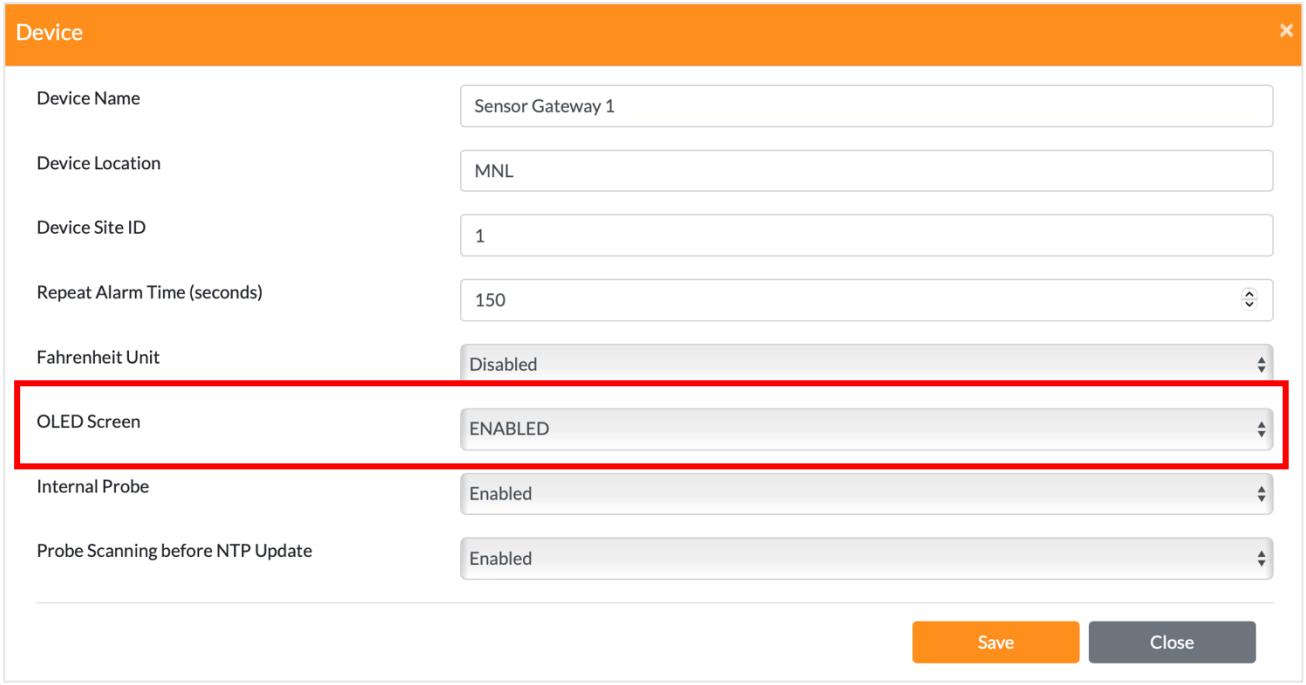
You can customize your device by modifying its **Device Name, Device Location** and **Site ID** to better fit your set up. To access these settings, connect to the base unit, open the menu, and navigate to **Settings.** Under **Main Settings,** select **Device,** where you can easily update these details.





5.2 OLED Screen

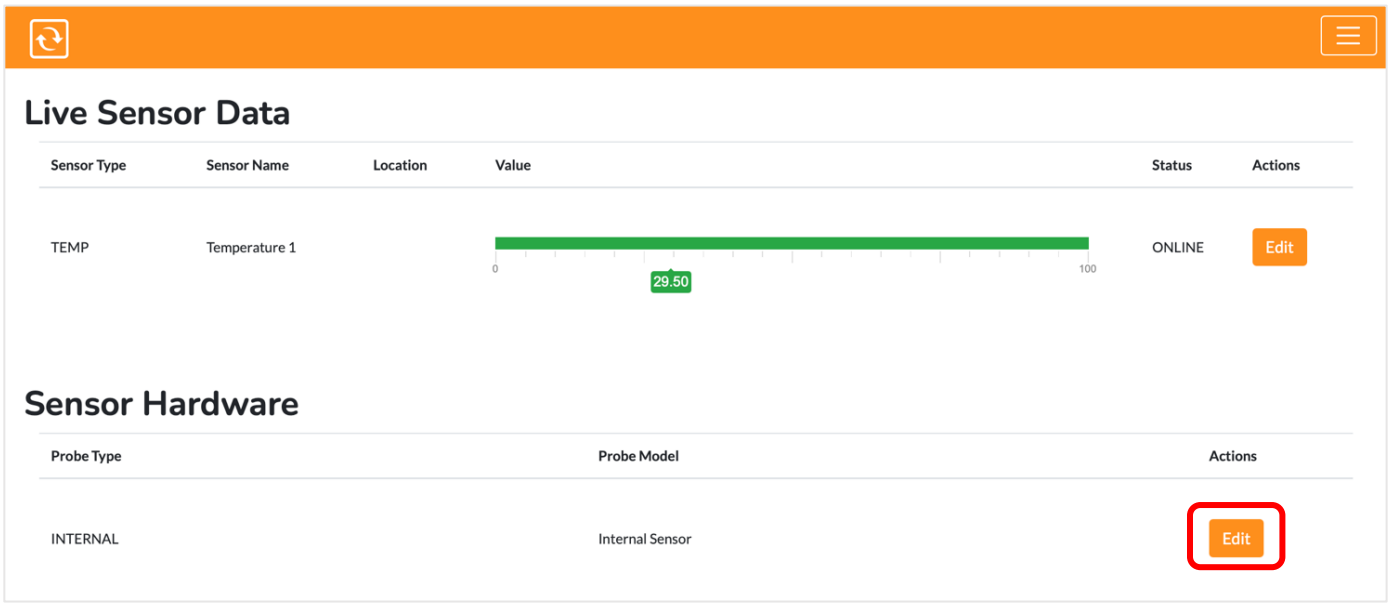
By default, the OLED screen is **enabled,** but you have the flexibility to turn it on and off as needed. To adjust this setting, access your device's **Settings,** open the **Menu,** and navigate to **Device.** There, you'll find the **OLED screen** option, which you can toggle between "Enabled" and "Disabled".

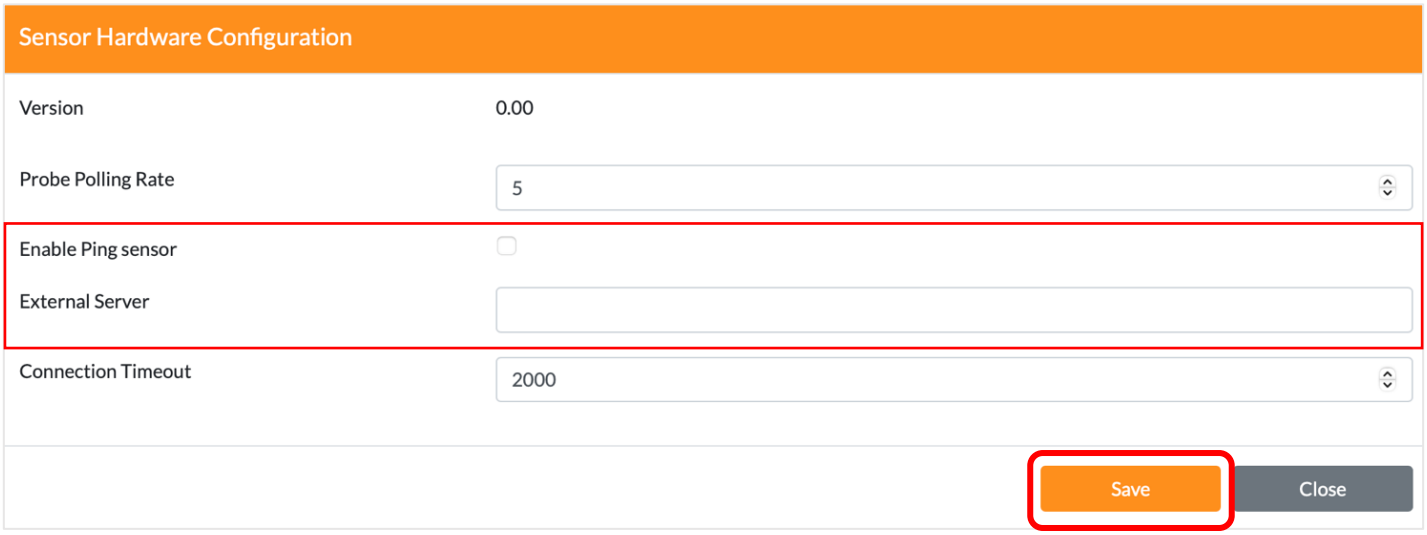


5.3 Internal Ping

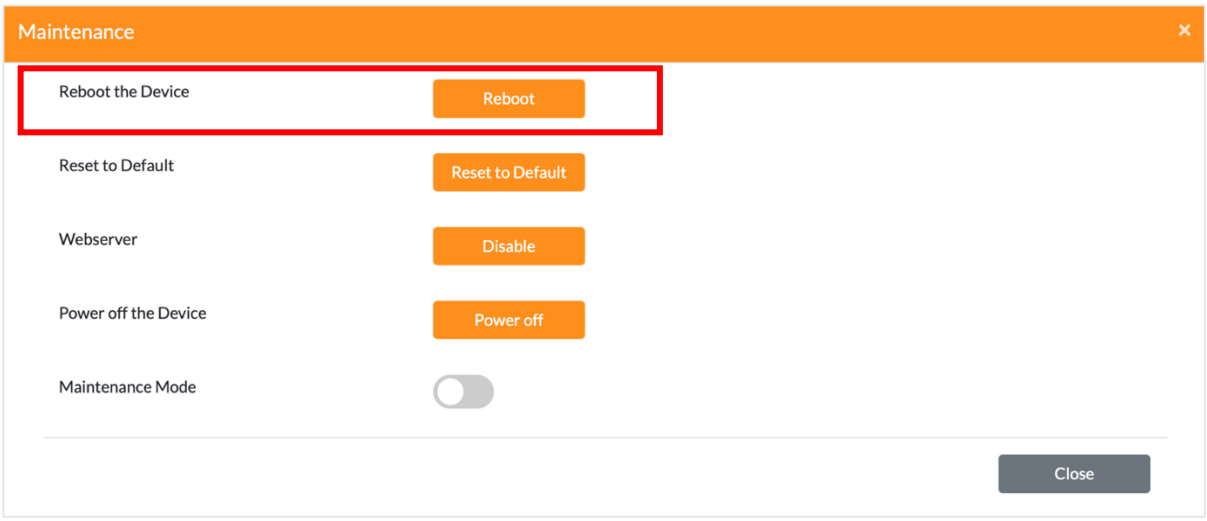
Internal ping check is where you can check the status of your connection to a specific URL or IP address in which a great example is trying to ping another Base Unit

To access the "PING" option, navigate to the home page, under 'Sensor Hardware' tab, click on the Edit button located next to the sensor where you wish to apply this option under Live Sensor Data and a pop window will appear wherein you can configure.

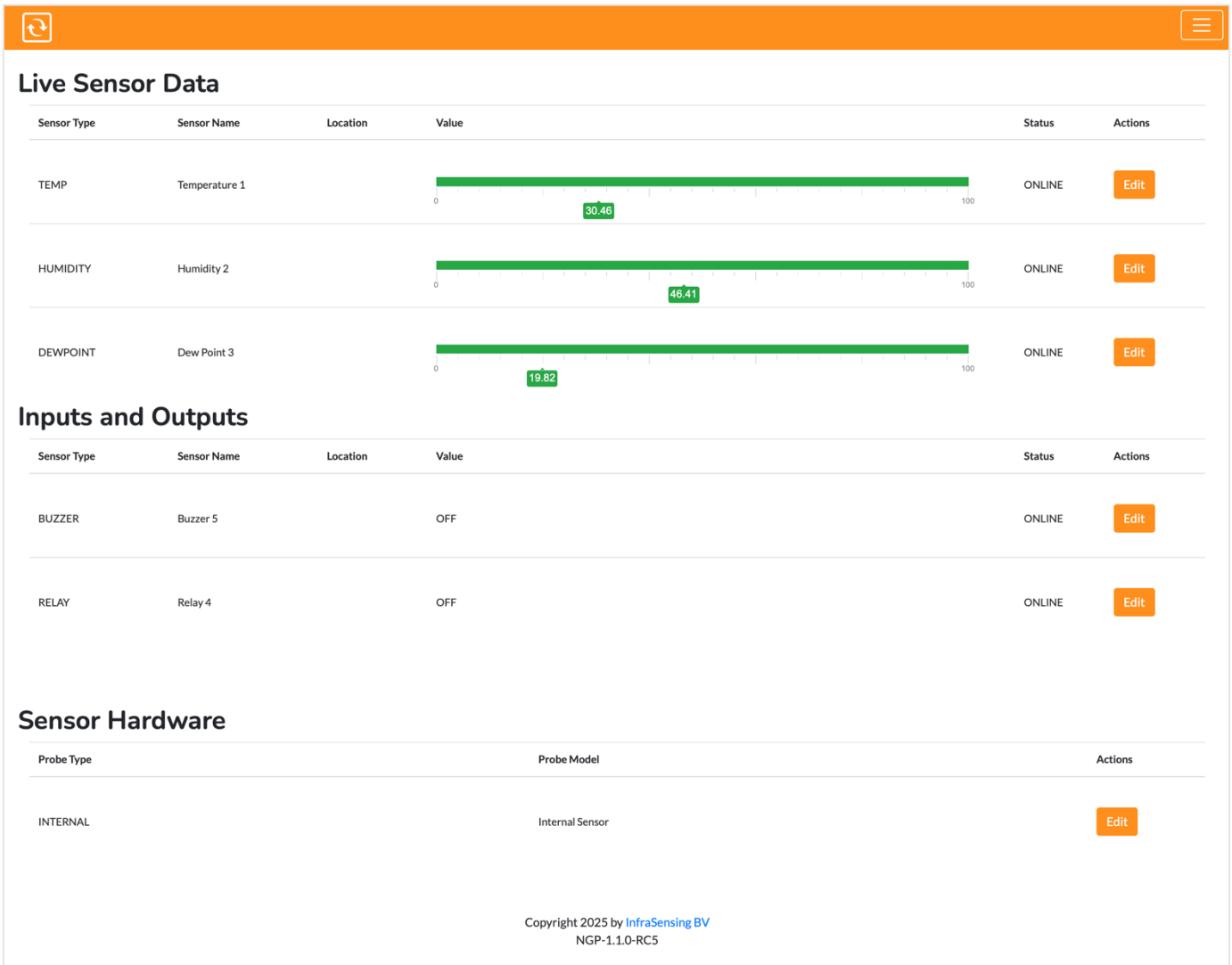




Once you hit 'Save', manually reboot your Base Unit by accessing the reboot option through the Base Unit's main settings. Click on the button in the upper right corner, then select 'Maintenance' under the 'Main Settings'. To reboot, simply click the 'Reboot' button. The changes will then take effect.

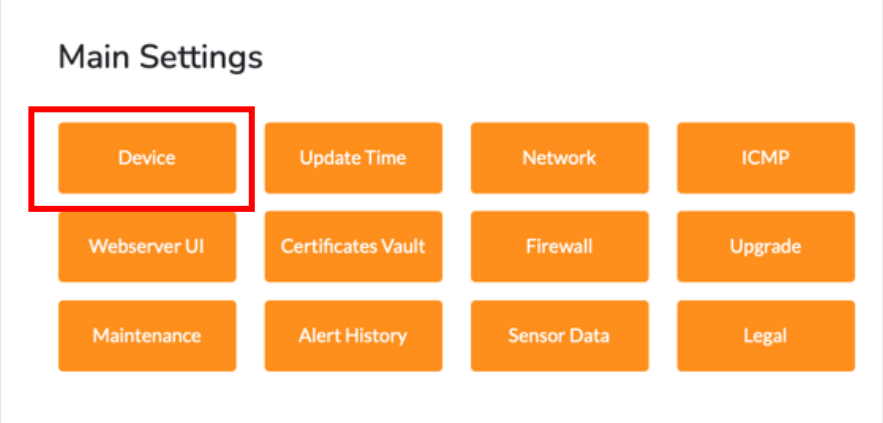


Once the Base Unit has reloaded, you will be able to see the URL/IP address you pinged under Live Sensor Data.

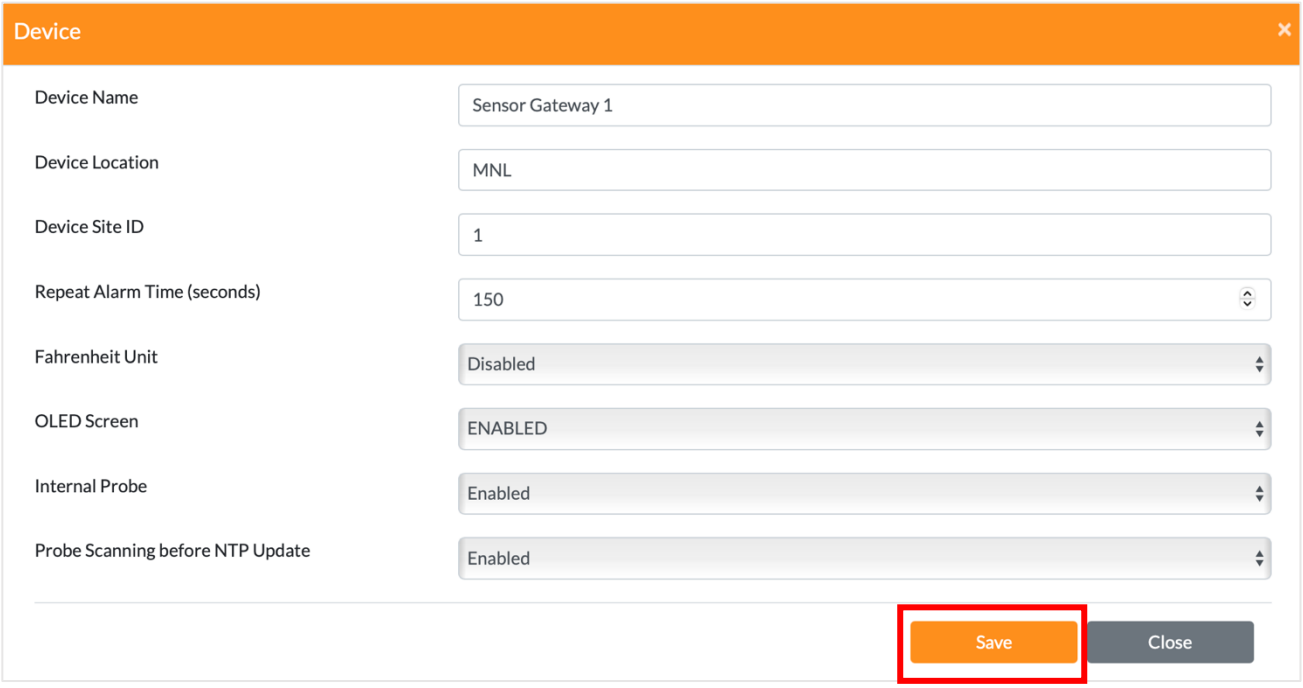


5.4 Switching between Fahrenheit or Celsius

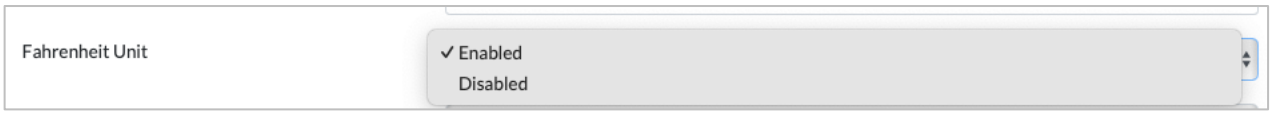
The default setup displays readings in Celsius. However, you can easily switch the sensor readings to Fahrenheit. Simply connect to the Base Unit, navigate to the menu, and click on settings. Under Main Settings, select Device to make the change.



This mode is read-only by default. To make changes, click on the 'Edit' button. Under the Fahrenheit Unit section, you will find a dropdown menu where you can select either "Disabled" or "Enabled".



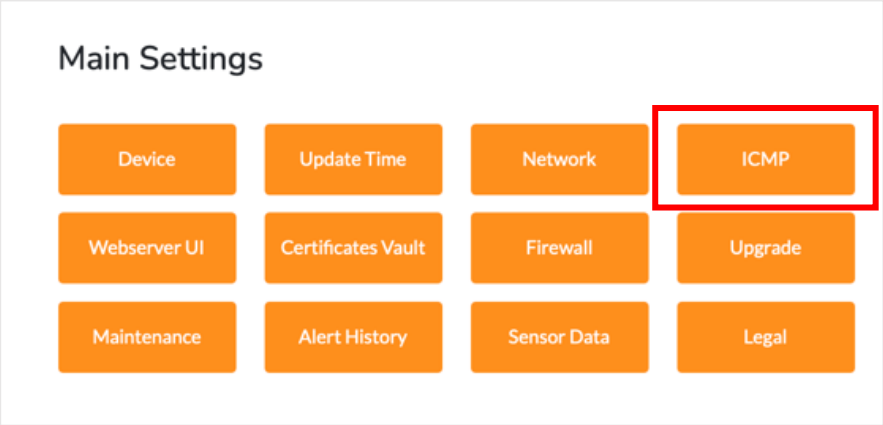
- **Enabled** : Temperature will be set to Fahrenheit
- **Disabled** : Temperature will be set to Celsius



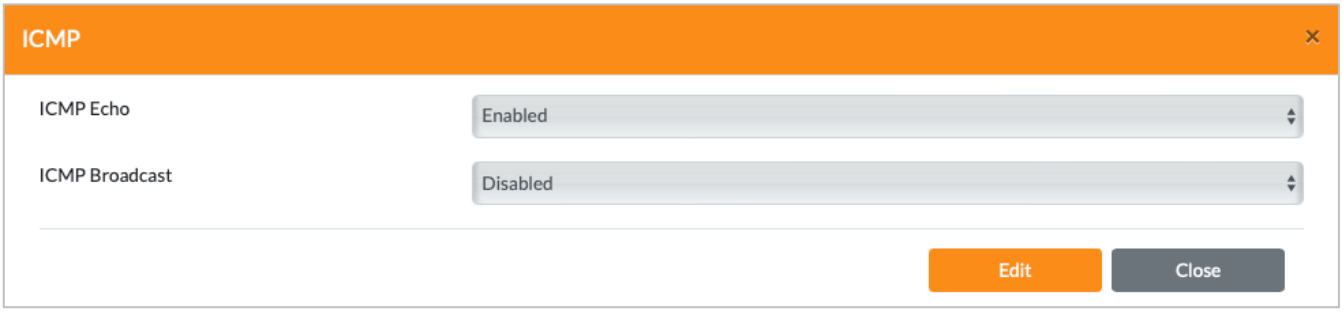
Once you have made the changes, click on 'Save'. A green banner will appear confirming that the settings have been 'Successfully Saved'. Simply reload the page for the changes to take effect.

5.5 ICMP Server

This feature provides the ability to manage incoming ping requests, allowing users to either permit or block such requests. ICMP (Internet Control Message Protocol) configurations empower users to tailor the responsiveness of the BASE-UNIT to incoming ping signals, optimizing network control and security based on the specific preference. In order to access the ICMP just simply go to Settings and under Main Settings you will be able to see ICMP.



The screen is currently in read-only mode, this is to prevent any accidental changes, editing can be initiated by clicking the 'Edit' button.



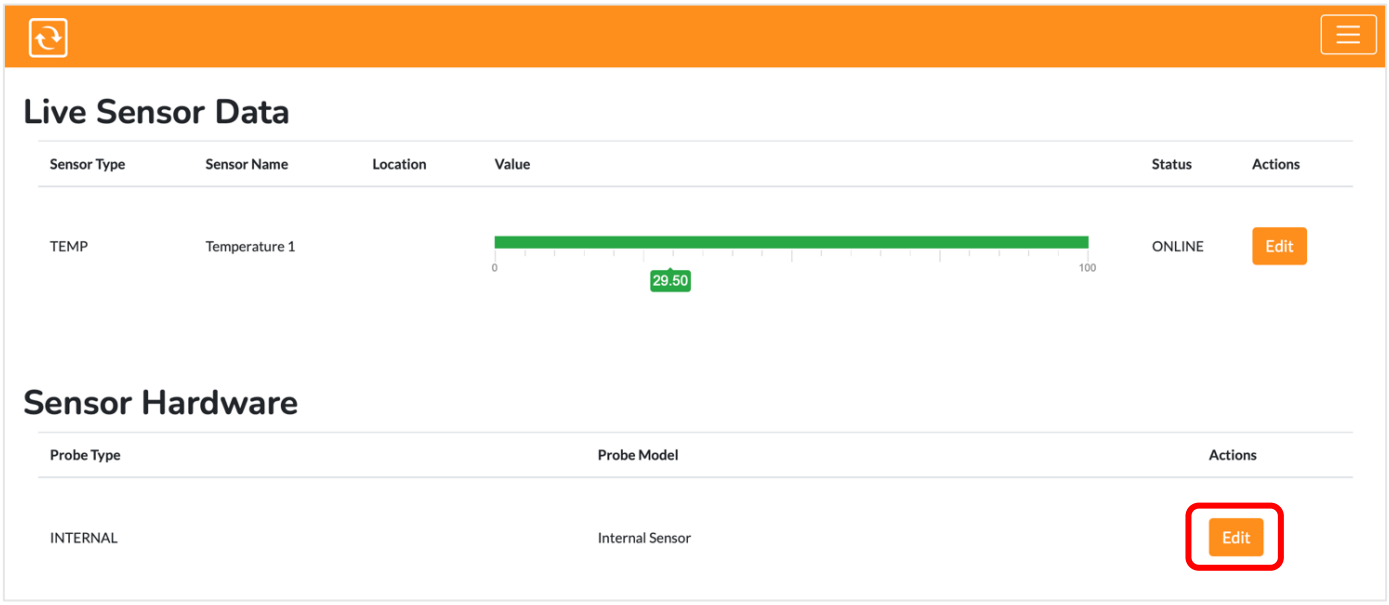
- **ICMP Echo**
  - **Enabled** : Allows PING to the BASE-UNIT.
  - **Disabled** : Blocks PING to the BASE-UNIT.
- **ICMP Broadcast**
  - **Enabled** : Allows PING to the BASE-UNIT.
  - **Disabled** : Blocks PING to the BASE-UNIT.

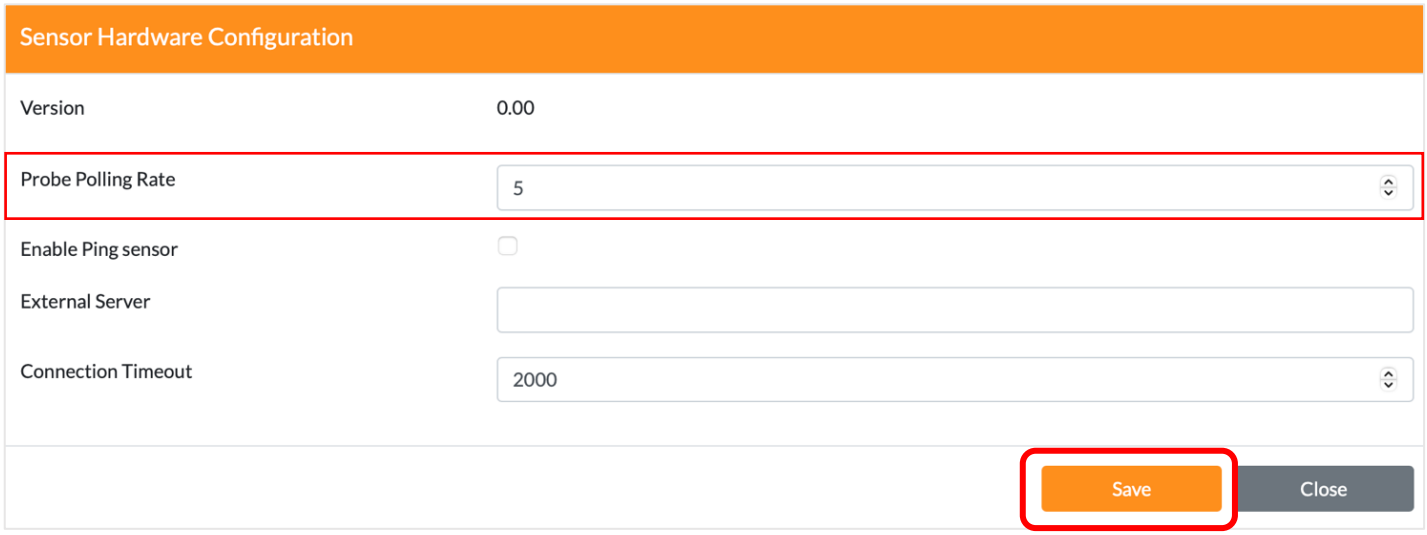
After you click the 'Edit' button and proceed to save changes by clicking the save button, a green banner will appear, indicating 'Successfully Saved.'.

Please Note:
If you see a notification at the top left of the page that says **"Reboot to Apply",** it means a reboot is required for the changes you've made to take effect. Be sure to restart the system to ensure all updates are properly applied.

5.6 Sensor Polling / Refresh Time

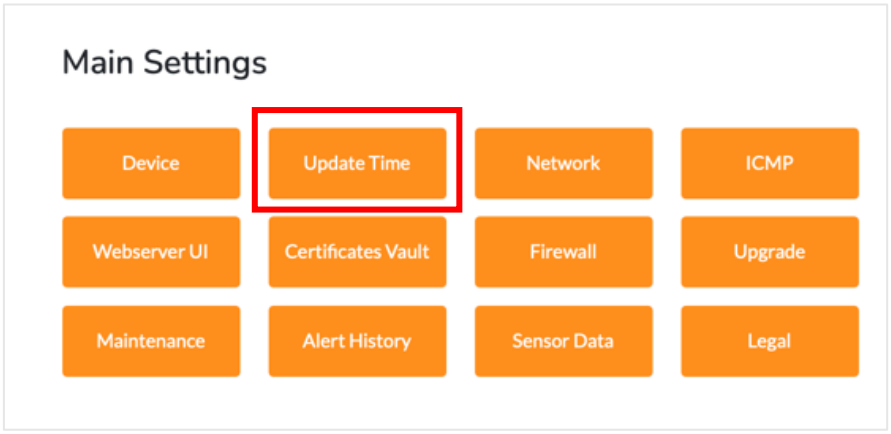
The Polling Rate, located under Sensor Hardware Configuration, determines the interval at which the base unit retrieves data from the specified sensors. It is recommended to set this interval between 1 to 5 seconds for optimal performance.

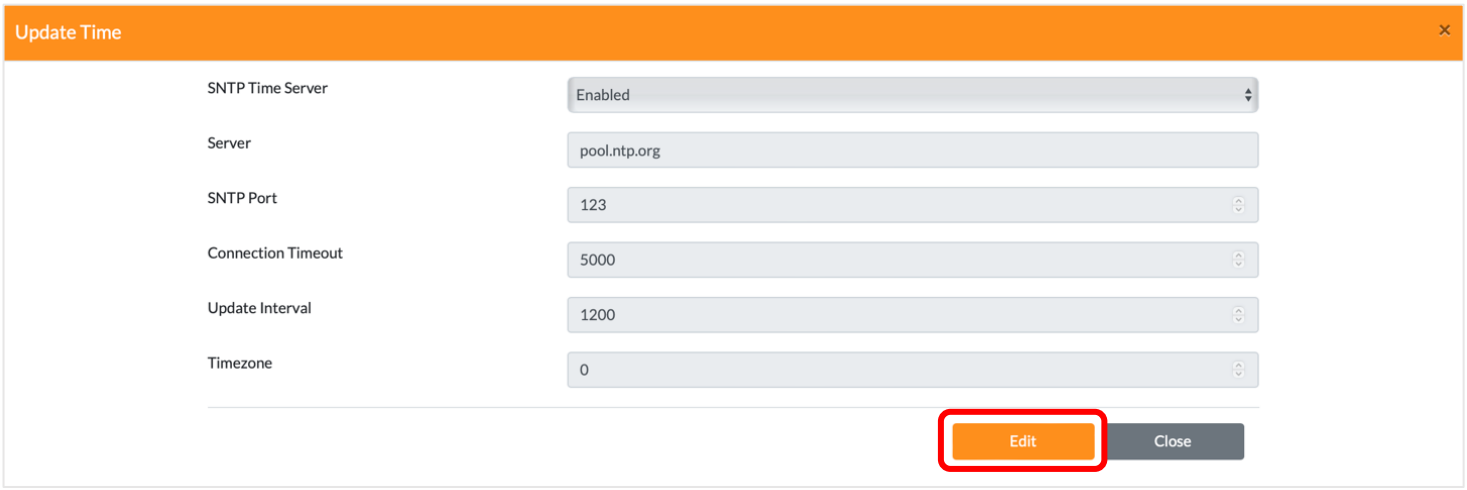




5.7 Configuring internal clock of the Base Unit

To modify the internal clock, navigate to Settings, then go to Main Settings and find "Update Time." In order to adjust the time, click on Edit and you can set the time manually or synchronize it with a time server. Once you have made your adjustments, click on "Save" to save the changes.



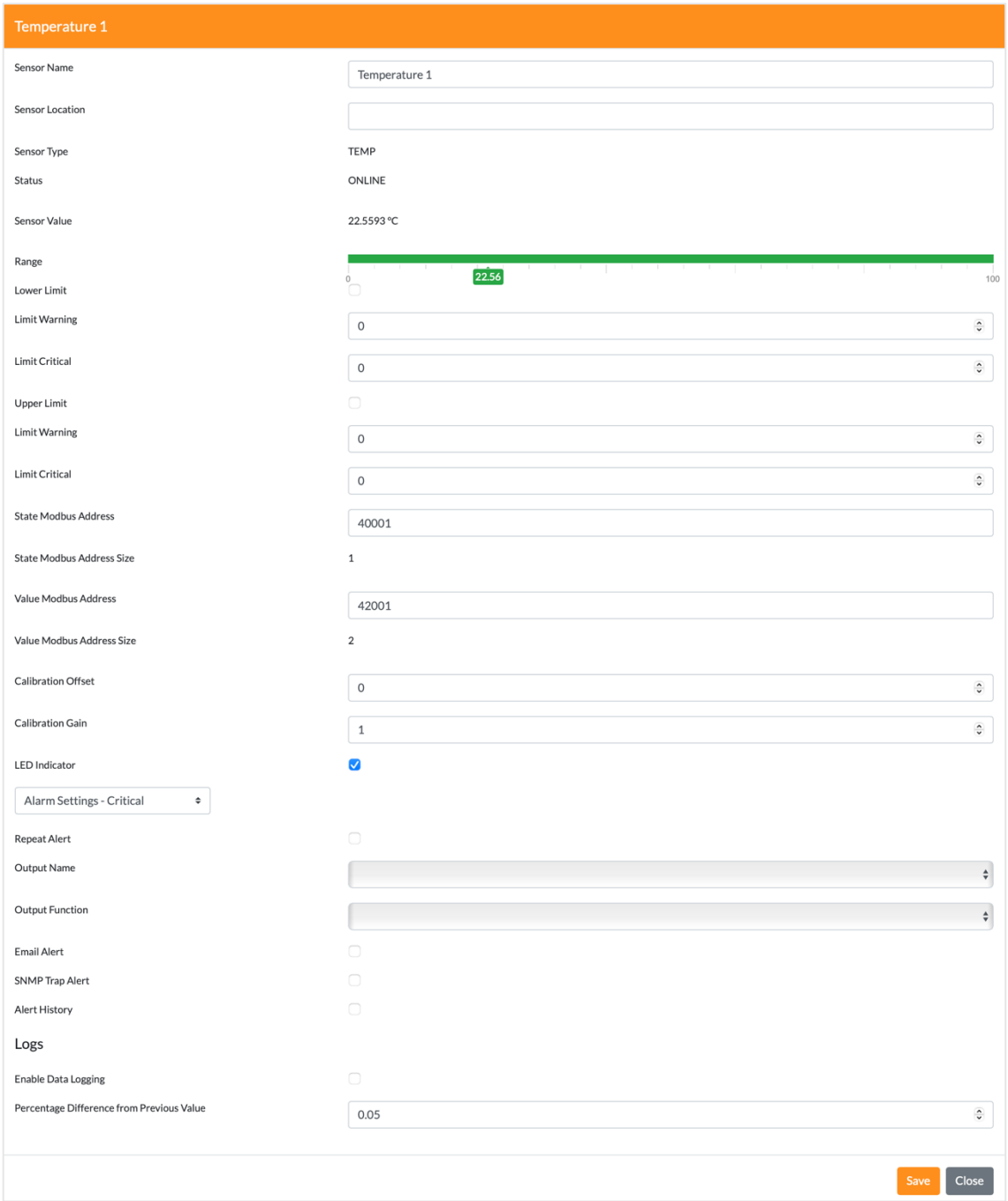


6 Setting threshold values and alert configuration

6.1 Setting Threshold

To set the threshold values in the base unit for alerting, connect to the Base Unit and navigate to the home page. Click on the Edit button located next to the sensor where you wish to apply this option under Live Sensor Data.

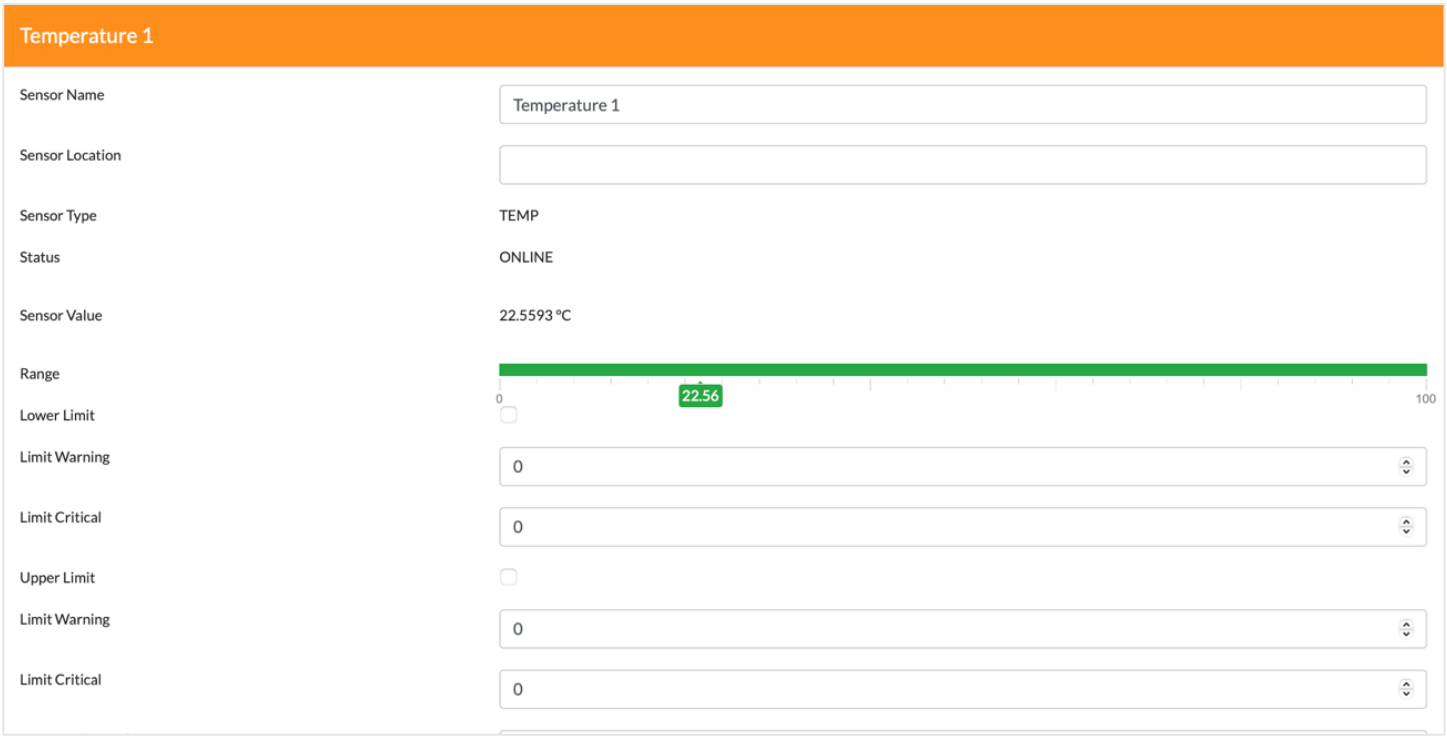
These are the options that you will see for each device once you click the 'Edit' button.



- **Sensor Name, Sensor Location**
  – This is where you can customize the details of your sensor.

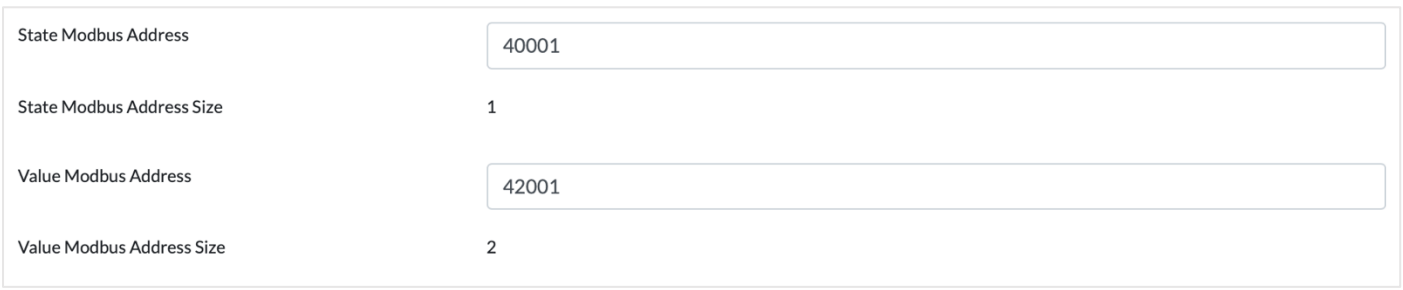
- **Sensor Type, Status, Sensor Value, and Range**
  – These details are automatically detected based on the connected sensor.

- **Lower Limit, Limit Warning, Limit Critical, Upper Limit, Limit Warning and Limit Critical**
  – These are the options that you can enable or disabled and also configure depending on your requirements.



- **Modbus Addresses**
  – You can see the registers to be used for the State address and Value address. Please see image below for reference.
  – When external sensors are connected, each one is automatically assigned a Modbus address. These assigned addresses can be viewed directly within the sensor settings interface, allowing users to easily identify and reference each sensor's Modbus address for integration. Users also have option to customize the Modbus addresses according to their preferences.
  –When checking the Modbus table, you may encounter the following status codes. These indicate the current state of each sensor:

    - 0 – Offline: The sensor is not responding or is disconnected
    - 2 – Online: The sensor is connected and functioning
    - 3 – Safe: The sensor is operating normally within expected parameters
    - 4 – Warning: The sensor has detected a value outside of the safe range
    - 5 – Down: The sensor has encountered a critical error or failure.

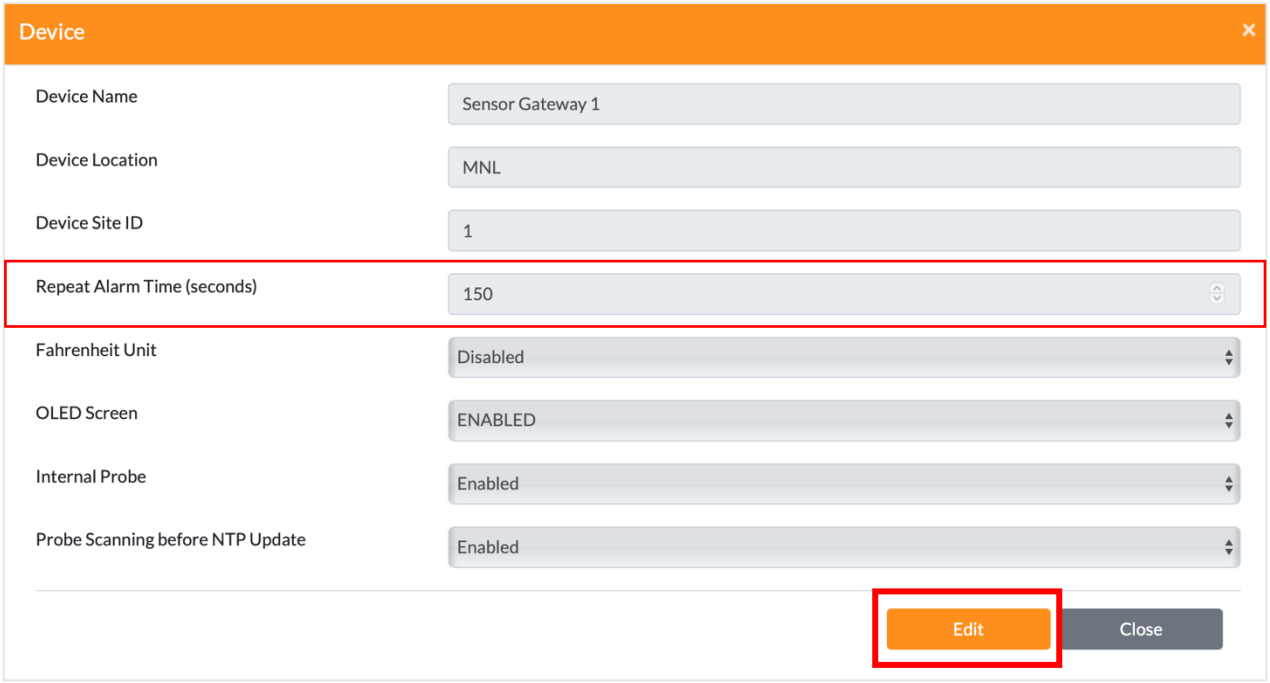


6.2 Alarm Settings

6.2.1 Repeat Alarm Time (seconds)

If this option is enabled, it will repeat the alert messages at the interval of the time you set.

To access this option, navigate to the Base Unit settings and under Main settings, click on Device. Here, you can find the option for Repeat Alarm Time.



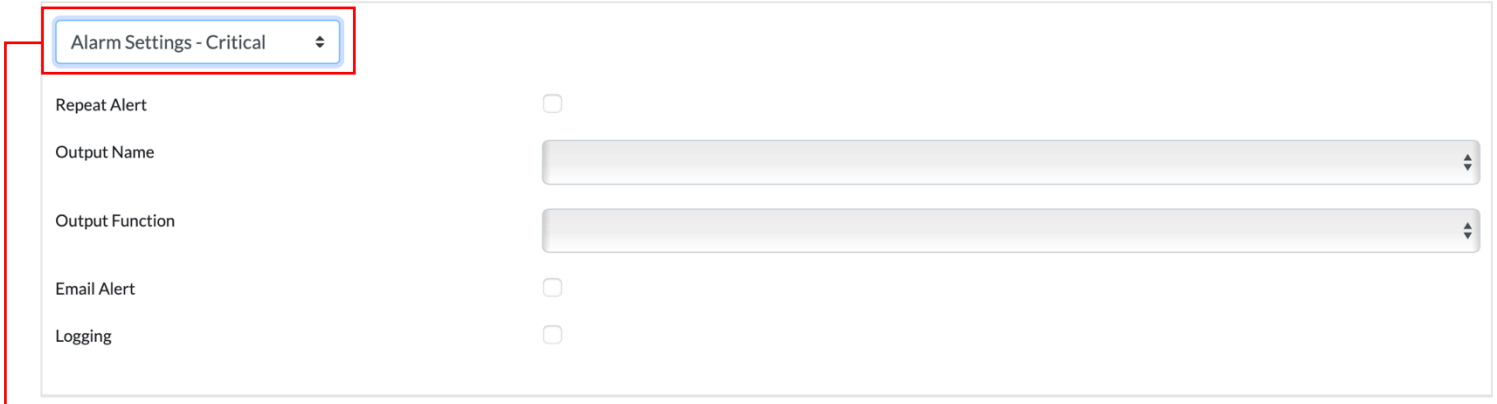
Please note that it is initially a read-only window, and to adjust it, you need to click on the 'Edit' button. Once the changes have been made, click on Save, and a green banner will appear, indicating that the changes have been successfully saved.

6.2.2 Comprehensive Alarm Setting Categories

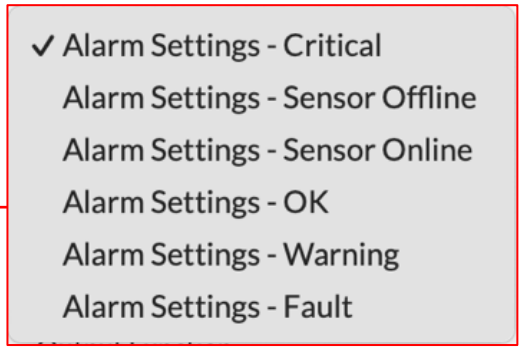
To access the various types of Alarm Settings, navigate to the Home Page and click the **Edit** button located next to the sensor under **Live Sensor Data**, where you want to apply the desired option. Upon clicking **Edit**, a pop-up window will appear displaying several configuration options. Scroll to the bottom of this page, to locate the **Alarm Settings** dropdown. From this dropdown, you can select the appropriate settings to apply based on your requirements:

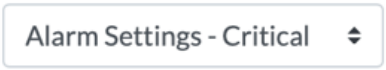
- Critical
- Sensor Offline
- Sensor Online
- OK
- Warning
- Fault

Each setting will be explained in detail on the next page.

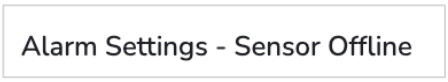


- **Repeat Alert**
  - A checkbox option to enable or disable repeated alerts for this settings
- **Output Name**
  - Allows you to define or assign an output node for specific trigger
- **Output Function**
  - Provides options for the output behavior when triggered, such as **ON, OFF,** or **TOGGLE Cycle**
- **Email Alert**
  - A checkbox option to activate or deactivate email notifications for the alarm
- **Logging**
  - Enables you to save the sensor status logs.

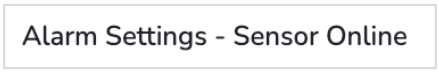




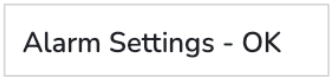
Alarm Setting - Critical is a feature that allows you to enable alarms for a specific sensor. When enabled, an alarm will trigger if the sensor goes down. To access this setting, click on the "Edit" button next to the desired sensor under Live Sensor Data or in the home page. A pop-up window will appear, allowing you to configure this option.



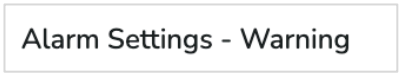
Alarm Setting - Offline is a feature that is when enabled, an alarm will be sent if the sensor goes offline. To access this setting, click on the "Edit" button next to the desired sensor under Live Sensor Data. A pop-up window will appear, allowing you to configure this option.



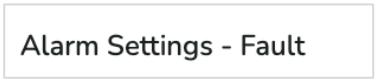
Alarm Setting - Online is a feature that is when enabled, an alarm will be sent if the desired sensor is working normally or if it goes online. To access this setting, click on the "Edit" button next to the desired sensor under Live Sensor Data. A pop-up window will appear, allowing you to configure this option.



Alarm Setting - OK is a feature that is when enabled, an alarm will be sent if the threshold is OK which doesn't meet the critical or warning threshold. To access this setting, click on the "Edit" button next to the desired sensor under Live Sensor Data. A pop-up window will appear, allowing you to configure this option.



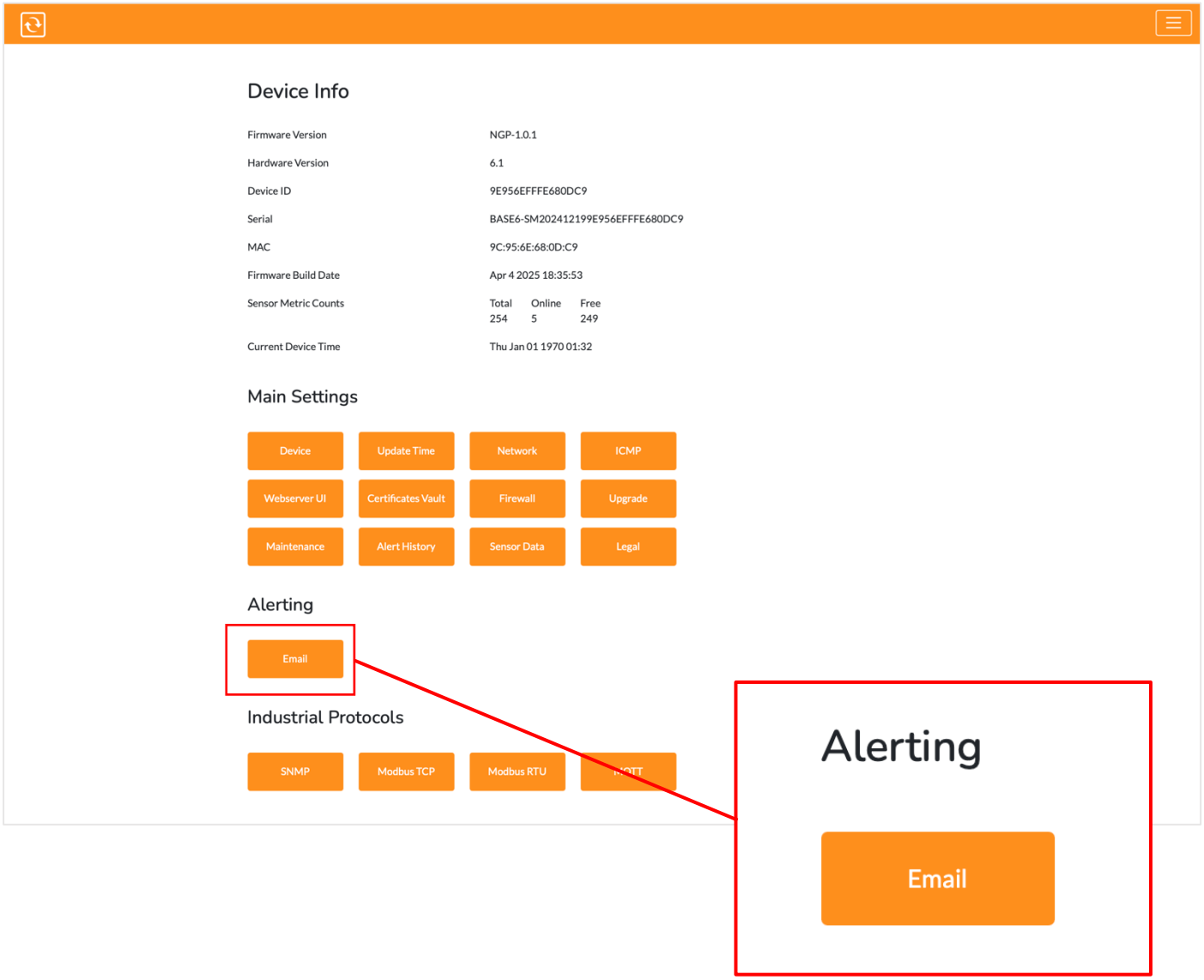
Alarm Setting - Warning is a feature that is when enabled, an alarm will be sent if the sensor reaches the warning threshold. To access this setting, click on the "Edit" button next to the desired sensor under Live Sensor Data. A pop-up window will appear, allowing you to configure this option.



Alarm Setting - Fault is a feature that triggers an alarm when the sensor value falls outside the normal range. To access this setting, click on the "Edit" button next to the desired sensor under Live Sensor Data. A pop-up window will appear, allowing you to configure this option.

6.3 Base Unit Alerting Feature

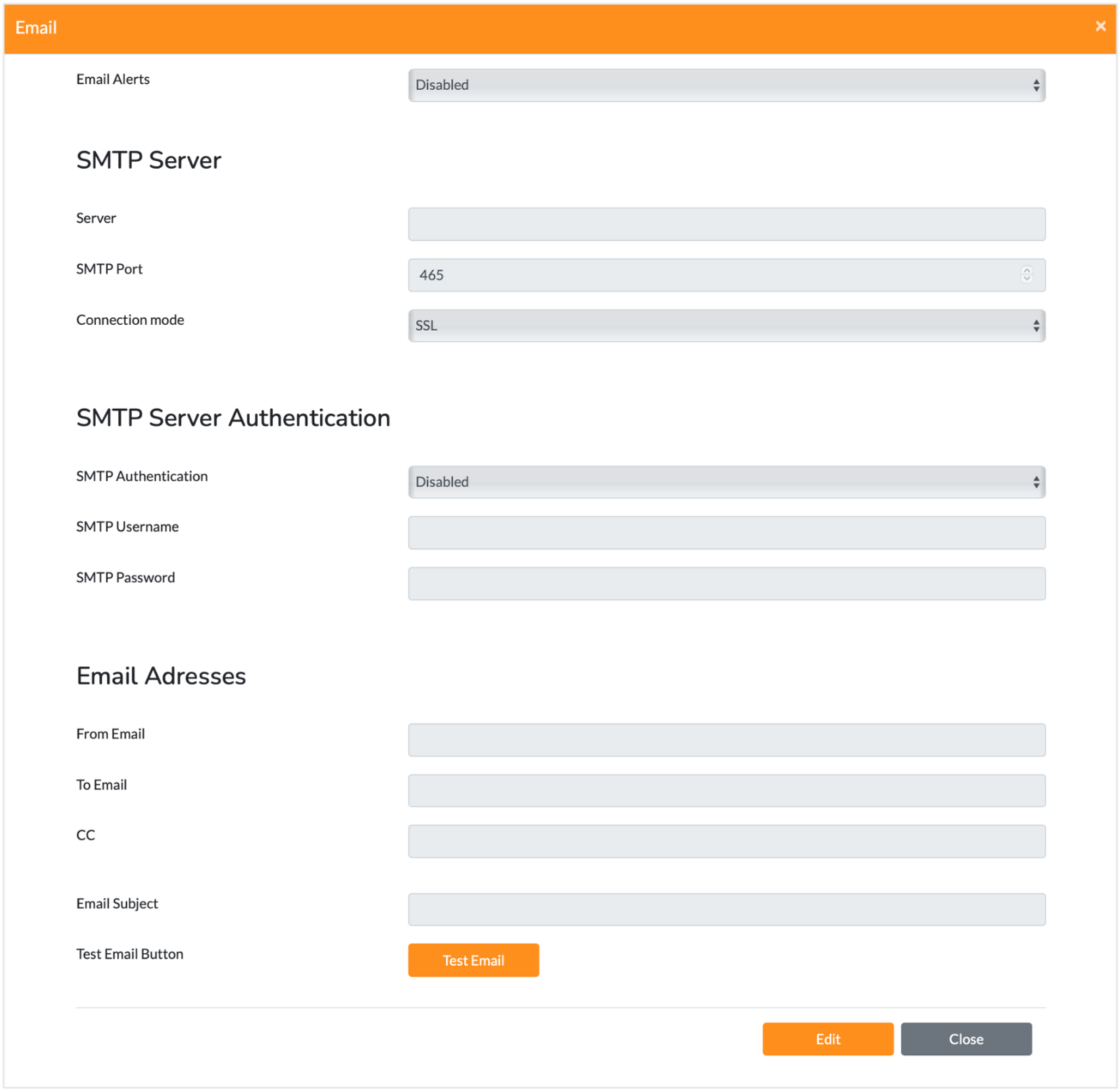
To access alerting options, navigate to the base unit settings. Directly below the Main settings option, you'll find Alerting option.



6.3.1 Email Configuration for Alerts

This option is enabling the Base Unit to send Email Alerts. Enter the SMTP Server Authentication details. Once you have entered the required information, hit **Save**. After saving, close the pop-up window and a **Reboot to Apply** button will appear. Click the button to ensure the changes are implemented.

Once the reboot is complete, you may test the setup by clicking the **Test Email** button.



There are various ways to send emails using different server options, such as free mail, Gmail, Outlook, and more. You can also utilize your own mail server.

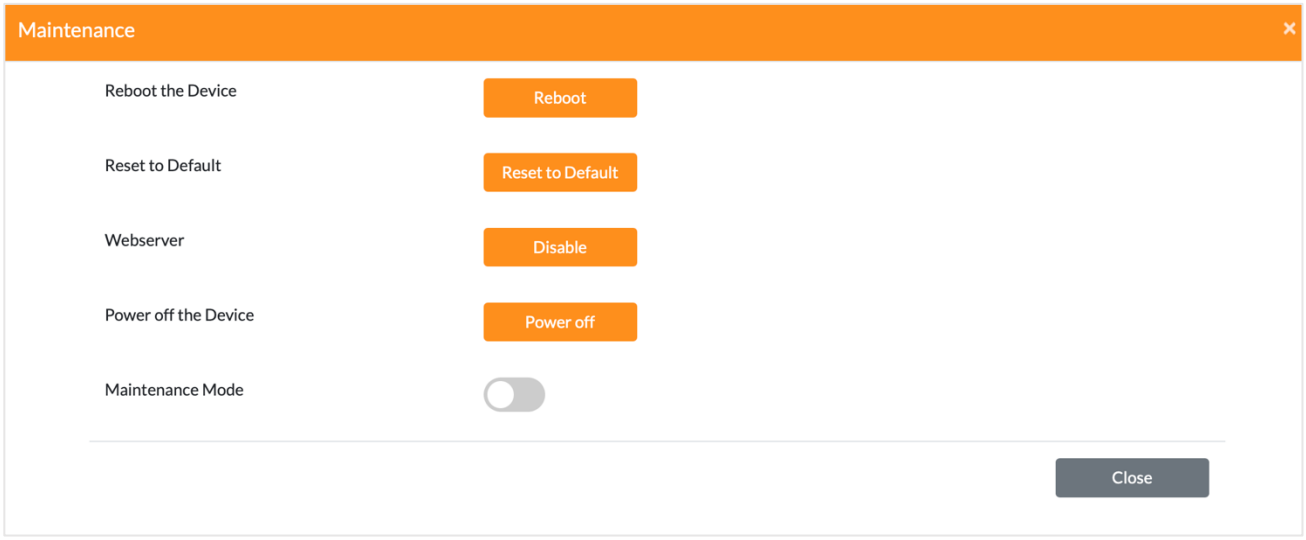
Please note that the settings will depend on the configuration of the mail server you are using.

Disclaimer:

Configuration may still vary depending on the mail server you are using.

6.4 Maintenance Options

This section provides the functionality to perform various actions such as manual device reboot, resetting to default, disabling the web server, or entering Maintenance mode, offering users a comprehensive suite of options for system upkeep and management.



6.4.1 Reboot

Rebooting the device restarts its operating system and hardware without changing any of the current settings or configurations. This is typically used to refresh the system, apply new settings, or troubleshoot minor issues.

6.4.2 Reset to Default

The "Reset to Default" option restores the device's configuration to its default settings when enabled. This process erases all custom configurations, user data, and preferences, returning the device to its default state.

6.4.3 Webserver

Disabling the web server option restricts the ability to send commands or configure settings. The Webserver option can be accessed through the Base Unit's settings by clicking on the button on the upper right, and under the Main setting click on 'Maintenance' option. To disable it, simply select "Webserver Disable". (please refer to section 4.3)

6.4.4 Power Off

Powering off the device completely shuts it down, turning off all hardware and software components. This is useful when the device needs to be physically reset, when performing maintenance, or when it will not be in use for an extended period. Note that powering off the device will stop all active processes, so it should only be done when necessary.

6.4.5 Maintenance Mode

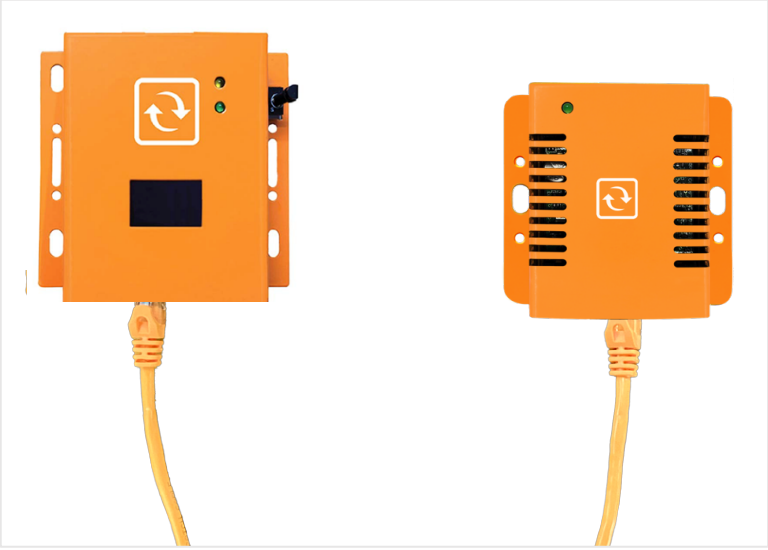
Enabling the Maintenance Mode allows you to configure the sensors without triggering any alerts, even when the alerting is enabled. In order to enable this feature, just click on the button "Enable Maintenance mode".

7 InfraSensing Sensor Probes

7.1 Sensor Connection Guide

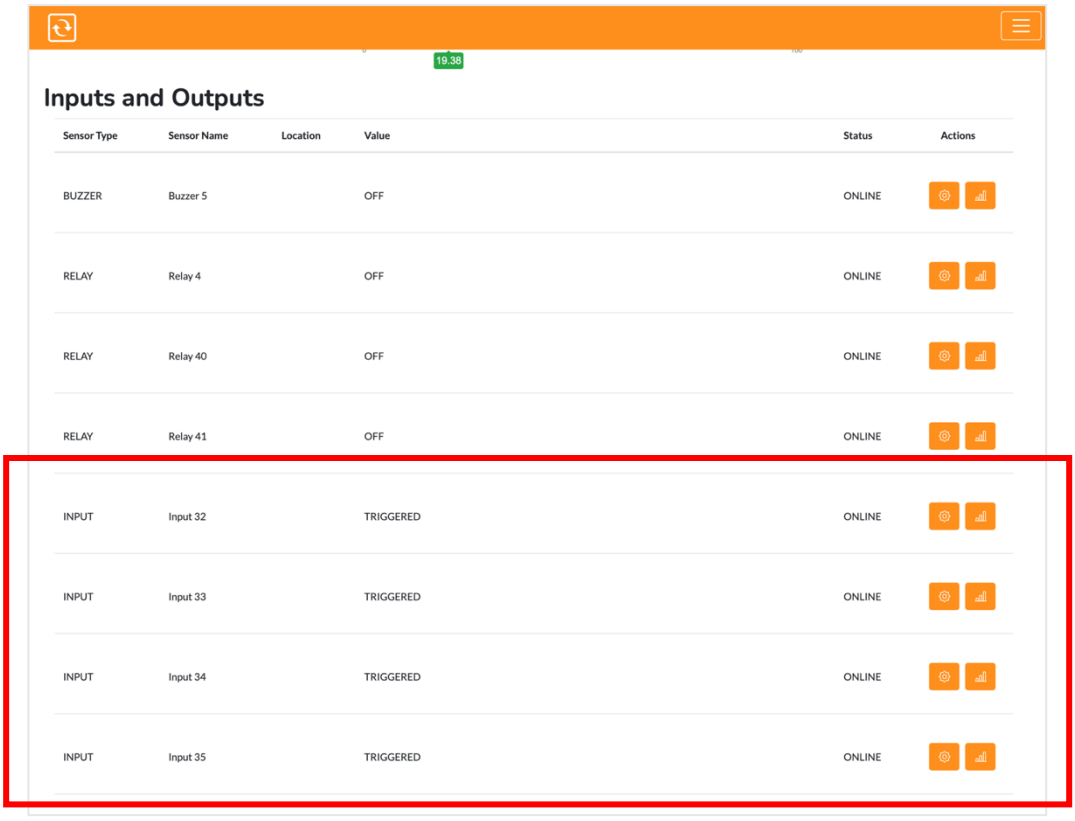
The sensor should be connected as shown in the image below. Use the RJ45-to-RJ45 cable to connect the external sensor probe to the RJ45 port at the bottom of the Base Unit.

The base unit has two RJ45 connectors at the bottom for the external probes, labeled **Sensor1** and **Sensor2.**

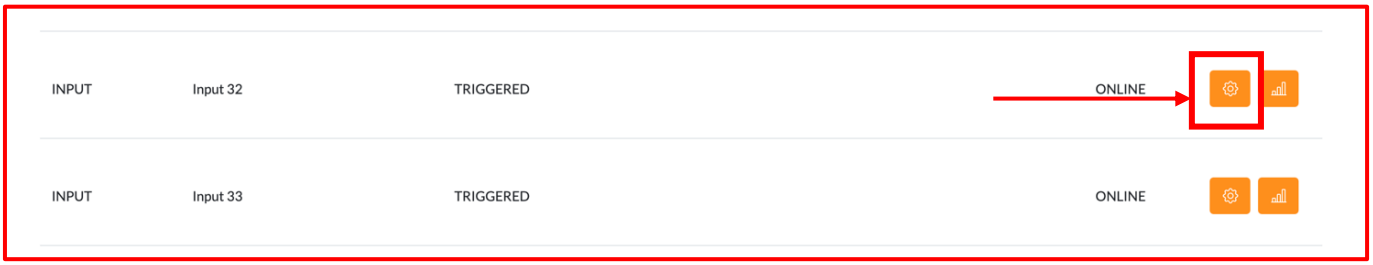


7.2 Adding EXP-8HUB

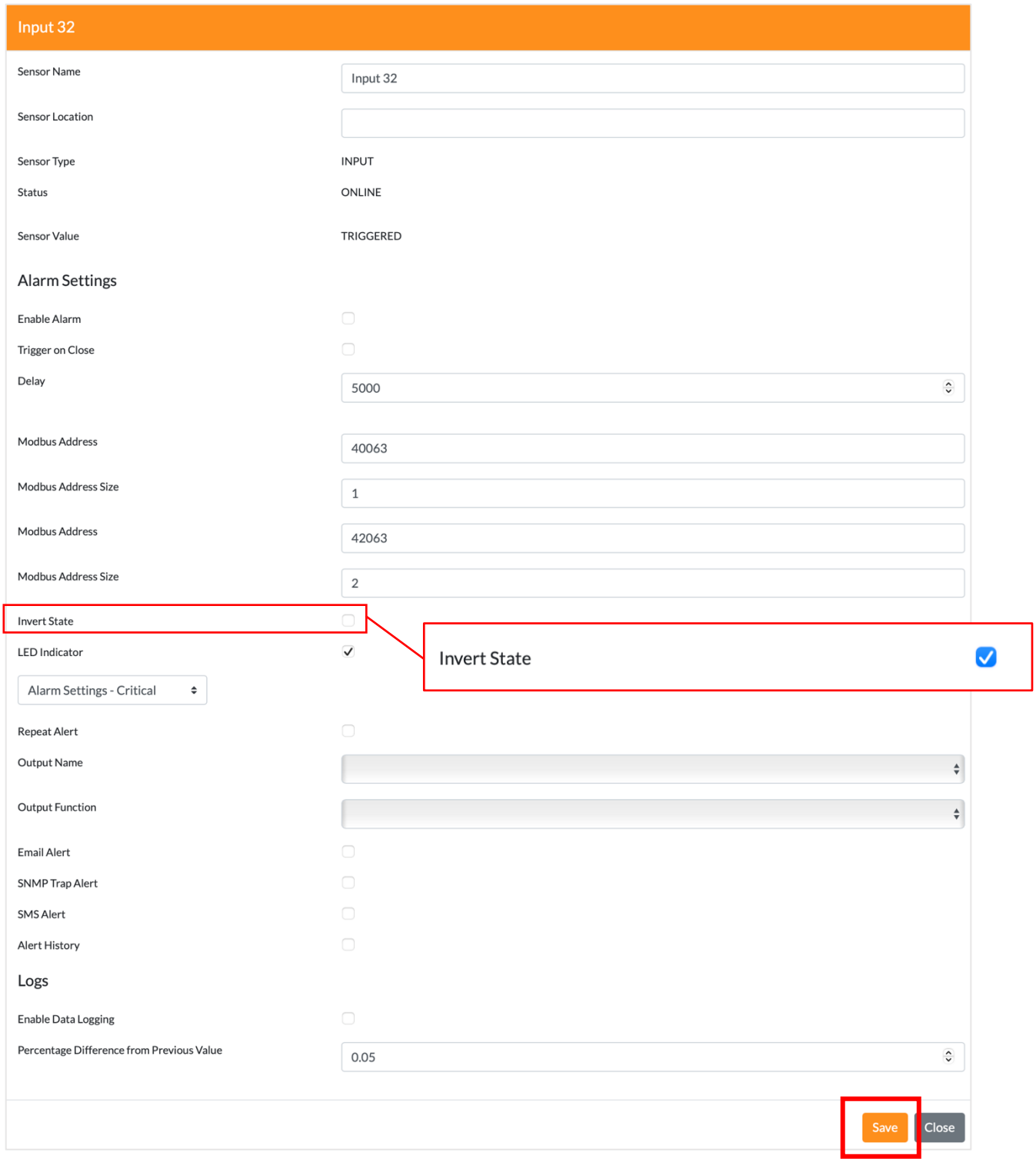
The EXP-8HUB is designed to trigger immediately upon connection due to security reasons. However, in order for it to use, the user must enable the 'Invert State' setting. The same settings applies when using IND-IO.



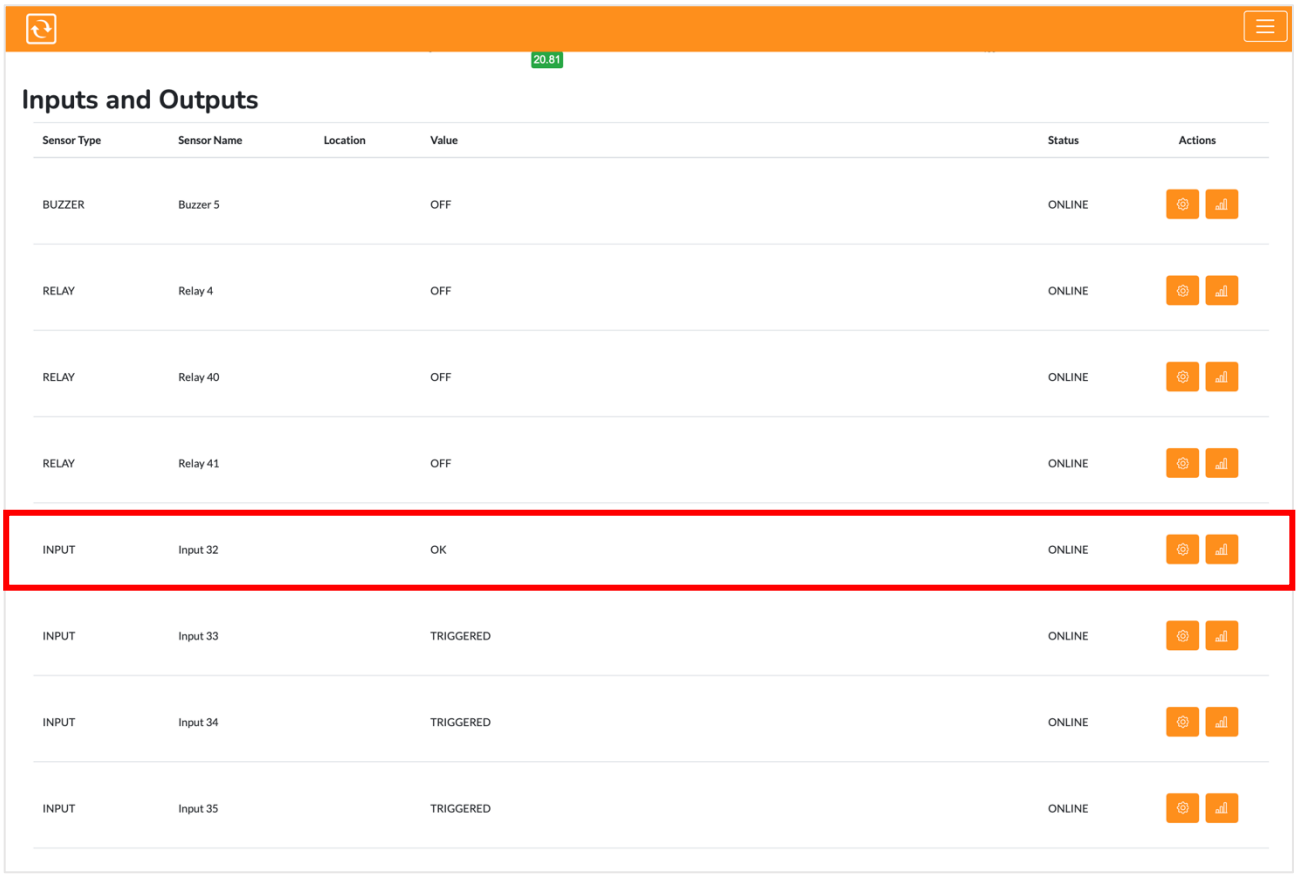
To enable Invert State, click on the gear icon located on the right-hand side to access the settings.



Under the Alarm Settings, there's an option for 'Invert State' and in order to enable it, just tick the box and hit on Save and reload the page and the changes will applied.



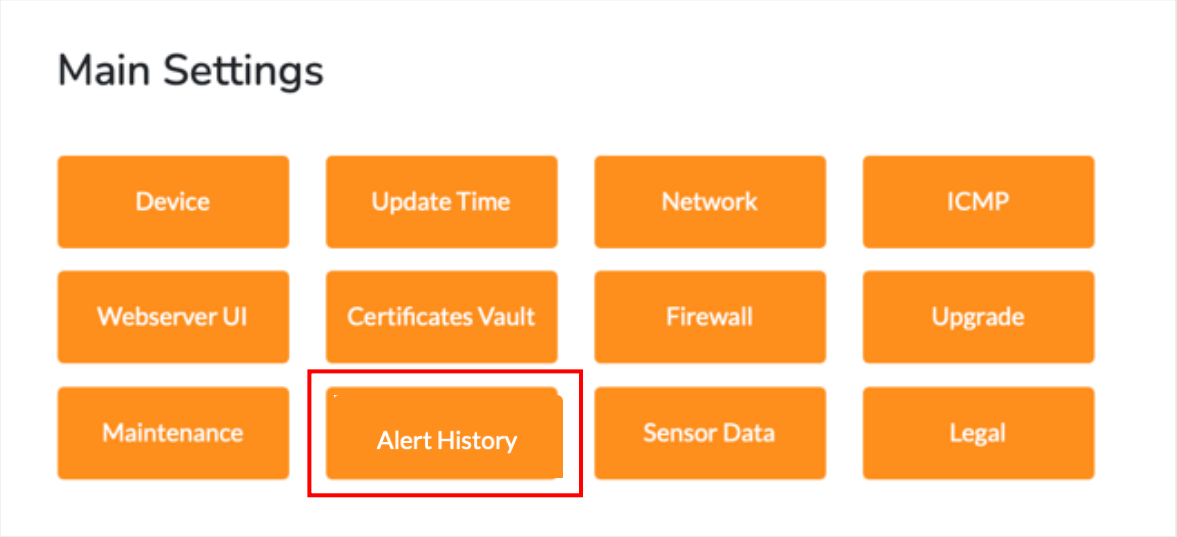
After saving and reloading the page, the value will update from ‘TRIGGERED’ to ‘OK’.

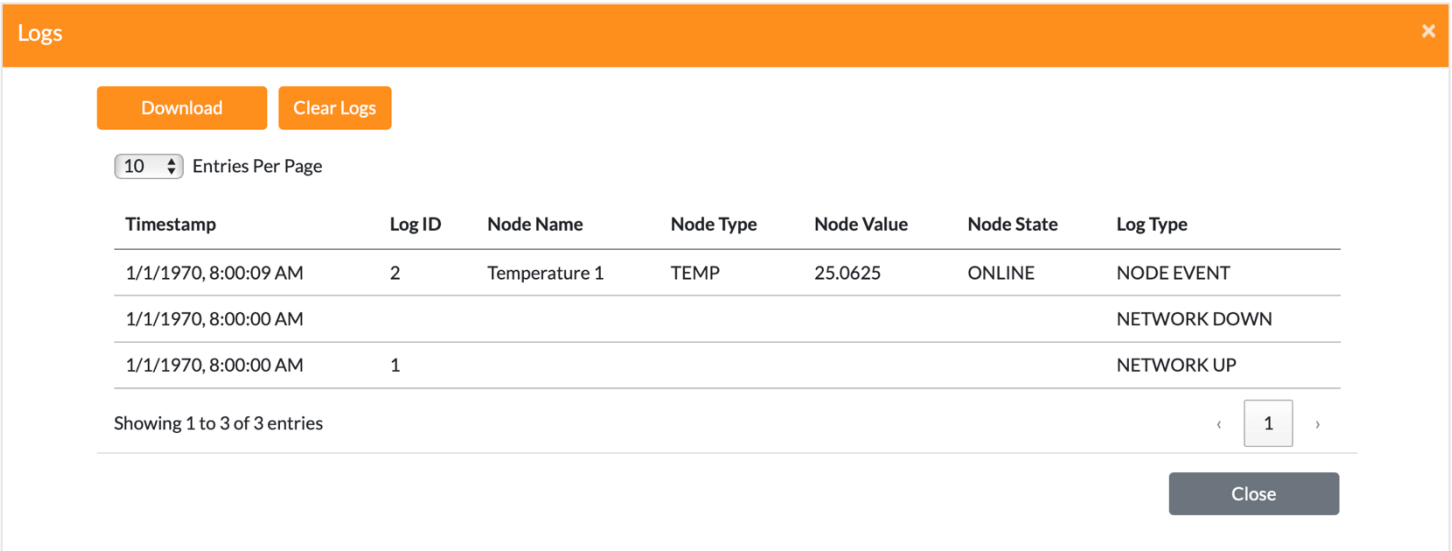


8 History

8.1 Alerting History

Each time a threshold is reached, an entry is automatically logged, and these entries can be downloaded in CSV format. Alerting Logs can be access in the Main settings.

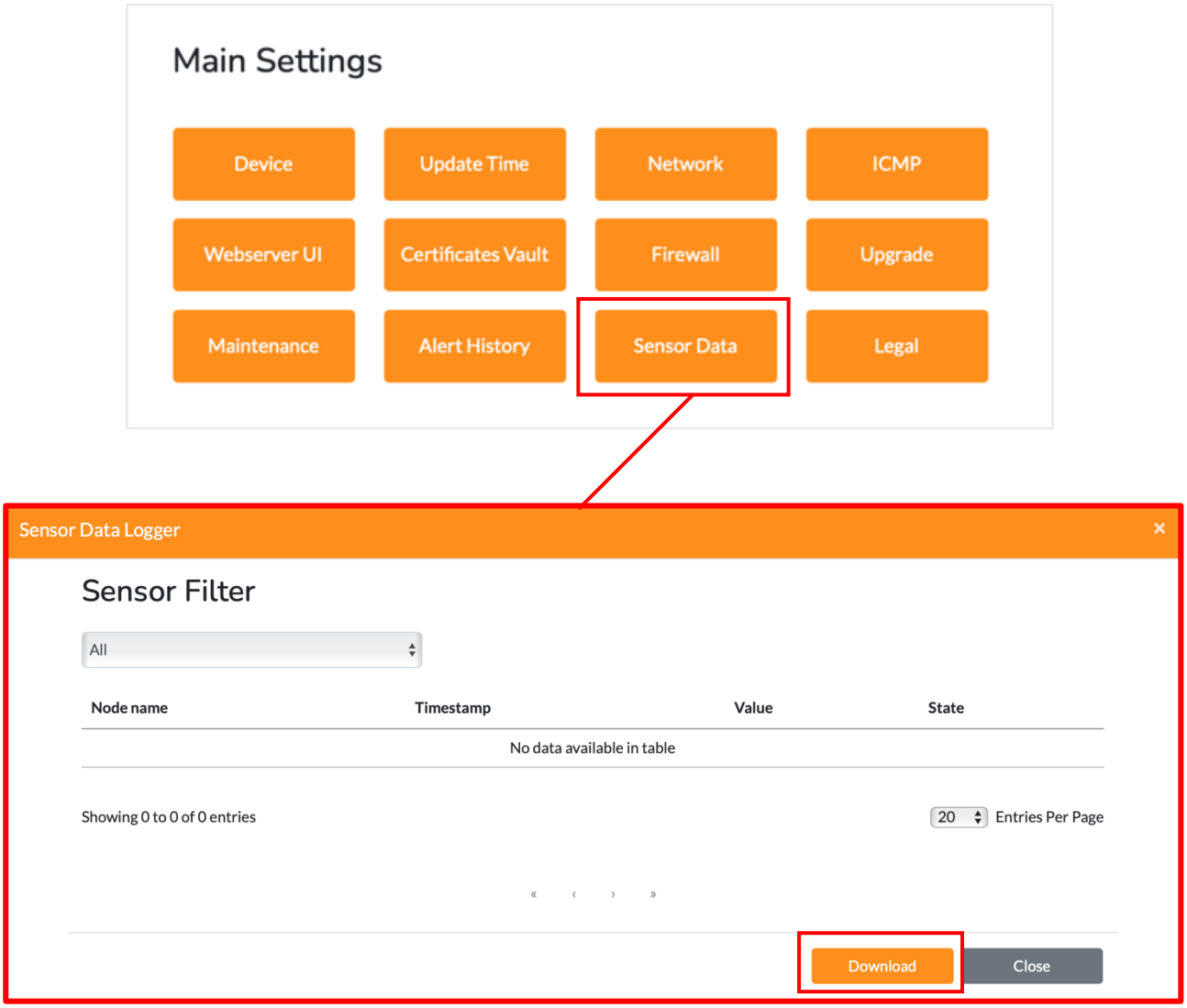




8.2 Data Logger

The **Data Logger** is a setting available exclusively on **Hardware Version 6**, allowing users to view recorded sensor data. It provides key information, including the **node name, timestamp (date and time), sensor value,** and **sensor state,** offering a detailed log of system activity for monitoring and analysis.

This feature is accessible through the **Main Settings.** Clicking on **Data Logger** opens a pop-up window displaying all recorded data logs. The system supports up to **2 GB of storage,** ensuring extensive historical tracking. Additionally, the data logs can be **downloaded** for further review, backup, or external analysis.



9 Integrating using Open Protocols

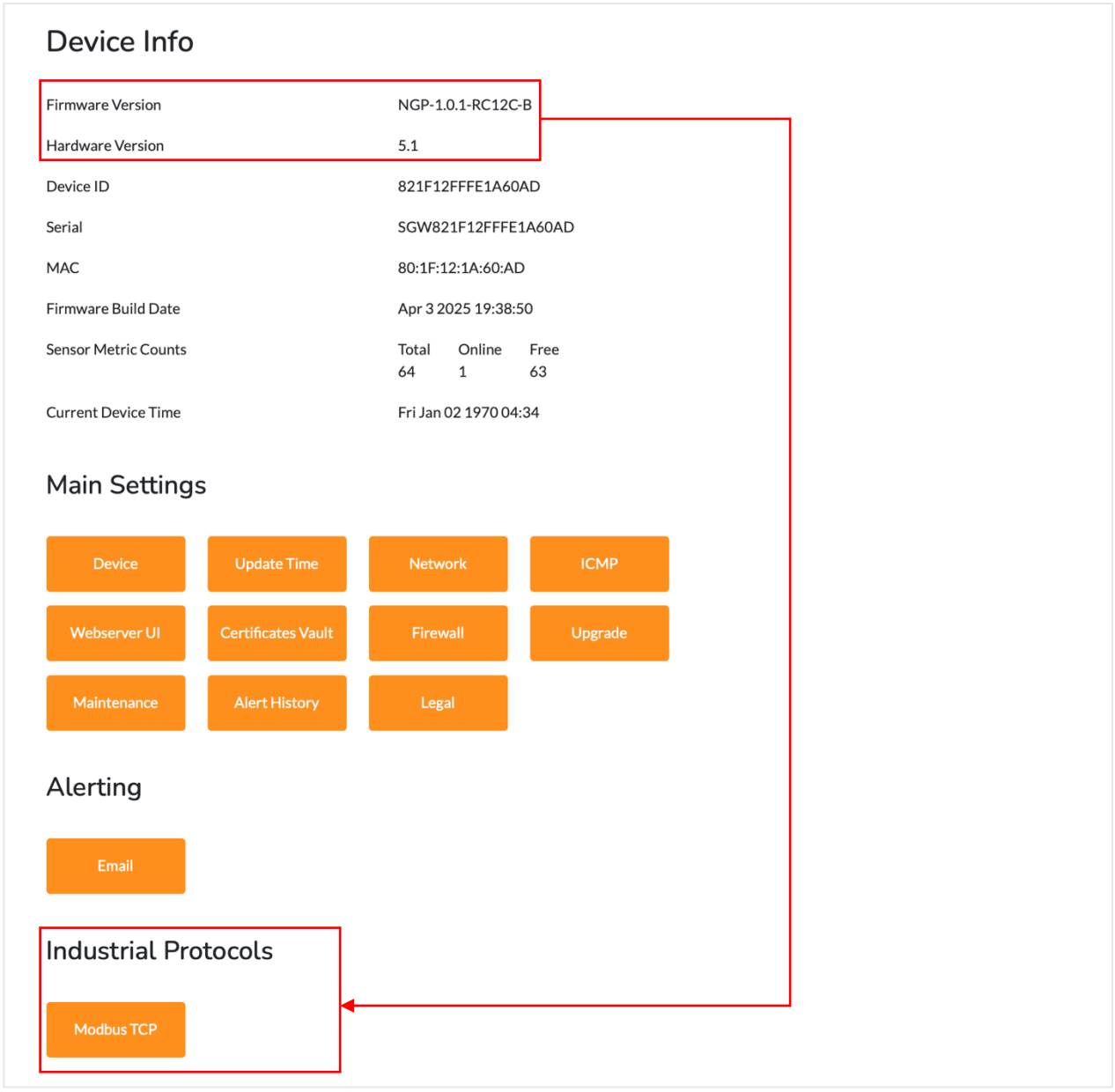
This section allows you to configure the Base Unit for industrial Protocols. To access it, simply navigate to the Base Unit Settings, and under the Alerting option, you'll find 'Industrial Protocol'. Please note that the option for integration using an open protocol may vary depending on the hardware version in use and the specific firmware version you select or require.

9.1 Hardware Version 5

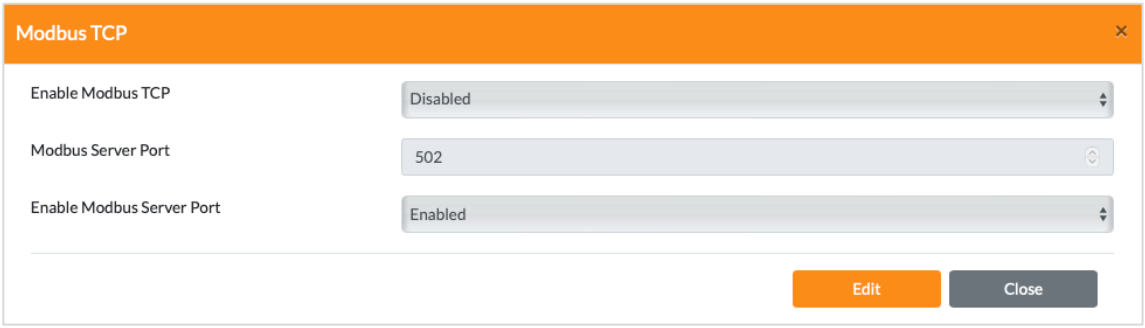
For Hardware Version 5, we offer three firmware versions, each tailored to a specific industrial protocol to suit your needs:

9.1.1 Firmware Version B | Modbus TCP

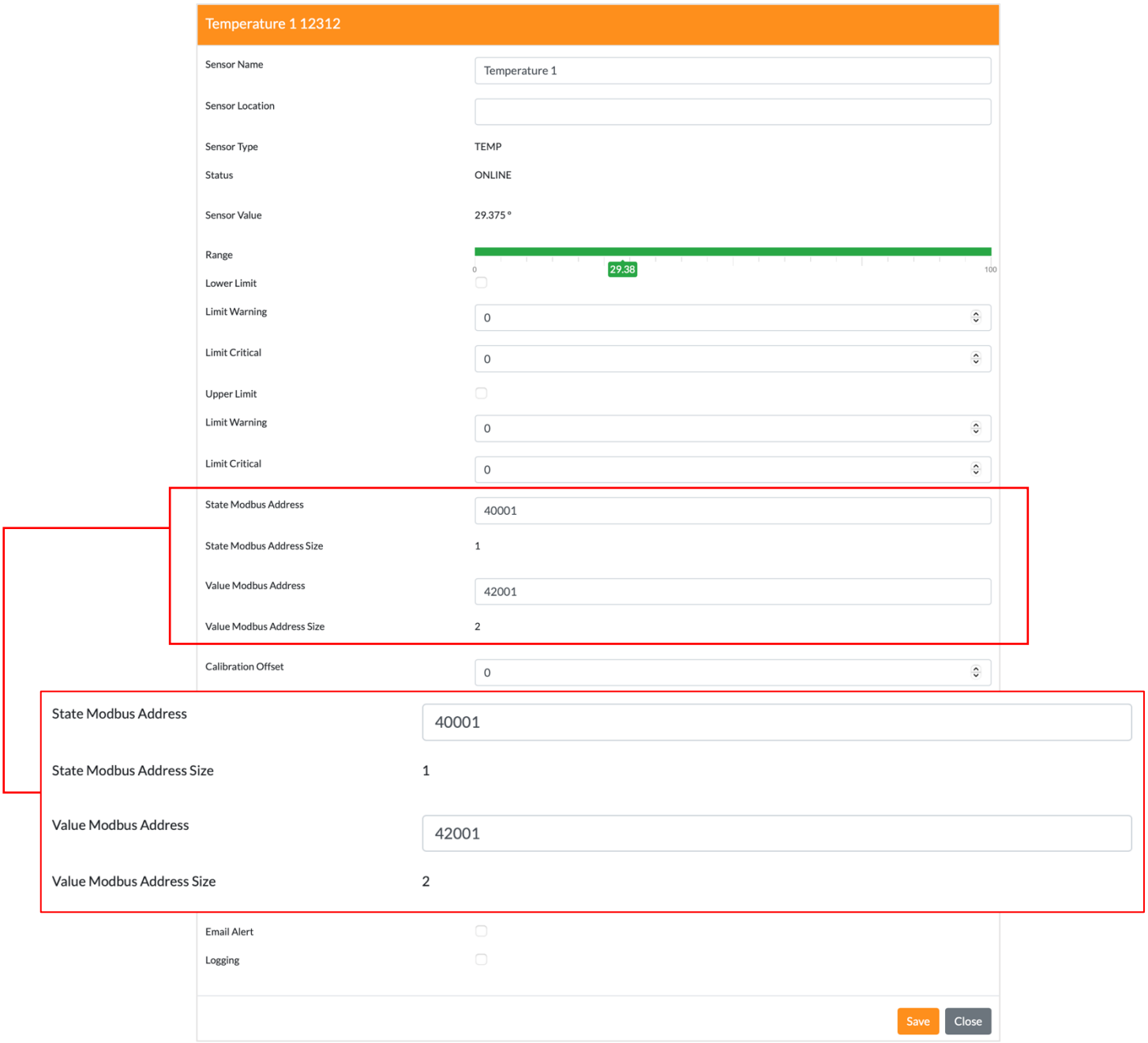
This firmware version supports the **Modbus TCP** industrial protocol, commonly used for communication between industrial devices and control systems, ensuring reliable and standardized data exchange.



This option allows the users to enable or disable Modbus functionality.



You can check the State Modbus Address, State Modbus Address Size, Value Modbus Address, and Value Modbus Address Size for each sensor on the Home Page. Simply click the Edit button on the right side of the sensor, and a pop-up window will appear. In the latter part of this window, you will find the Modbus address details.

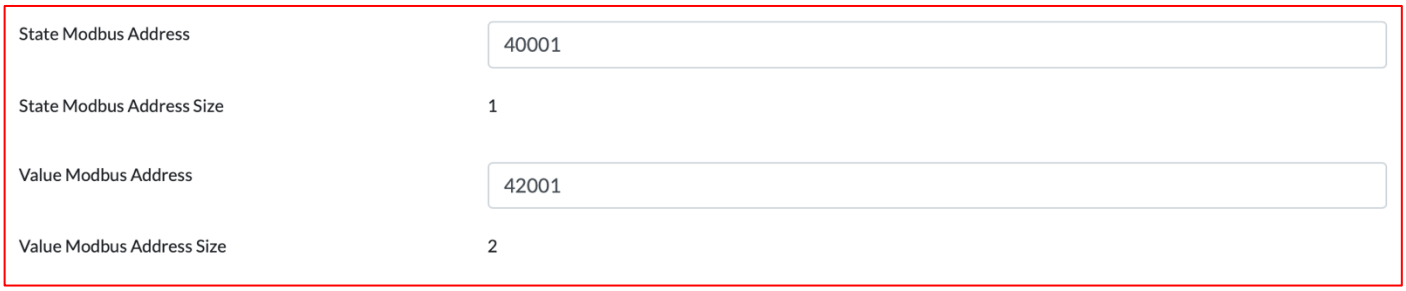


Modbus Addresses

- You can see the registers to be used for the State address and Value address. Please see image below for reference.
- When external sensors are connected, each one is automatically assigned a Modbus address. These assigned addresses can be viewed directly within the sensor settings interface, allowing users to easily identify and reference each sensor's Modbus address for integration. Users also have option to customize the Modbus addresses according to their preferences.

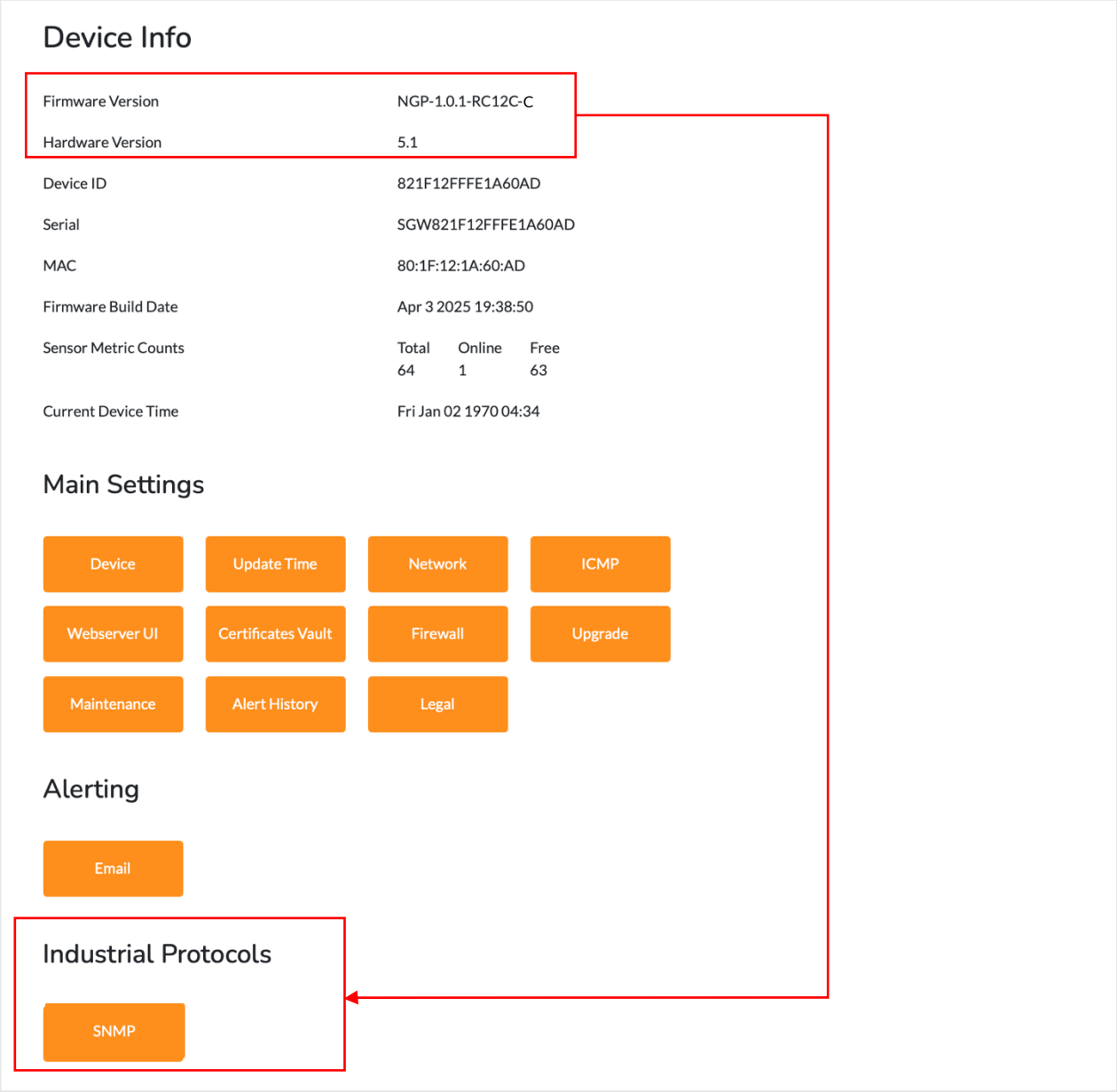
- When checking the Modbus table, you may encounter the following status codes. These indicate the current state of each sensor:

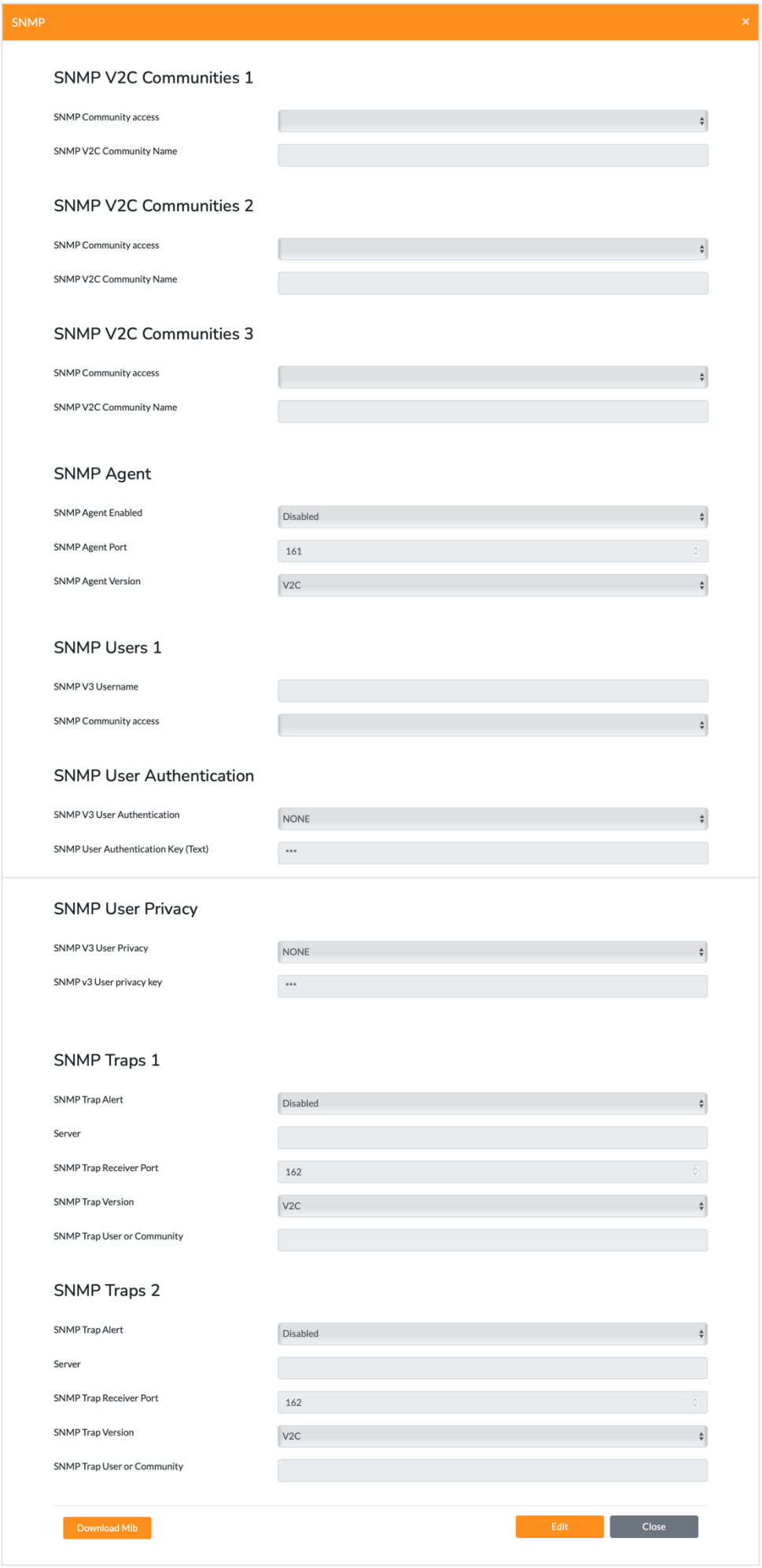
    - 0 – Offline: The sensor is not responding or is disconnected
    - 2 – Online: The sensor is connected and functioning
    - 3 – Safe: The sensor is operating normally within expected parameters
    - 4 – Warning: The sensor has detected a value outside of the safe range
    - 5 – Down: The sensor has encountered a critical error or failure.



9.1.2 Firmware Version C | SNMP

This firmware version supports SNMP industrial protocol, ideal for network management and monitoring, enabling efficient control of devices within IT and industrial networks.



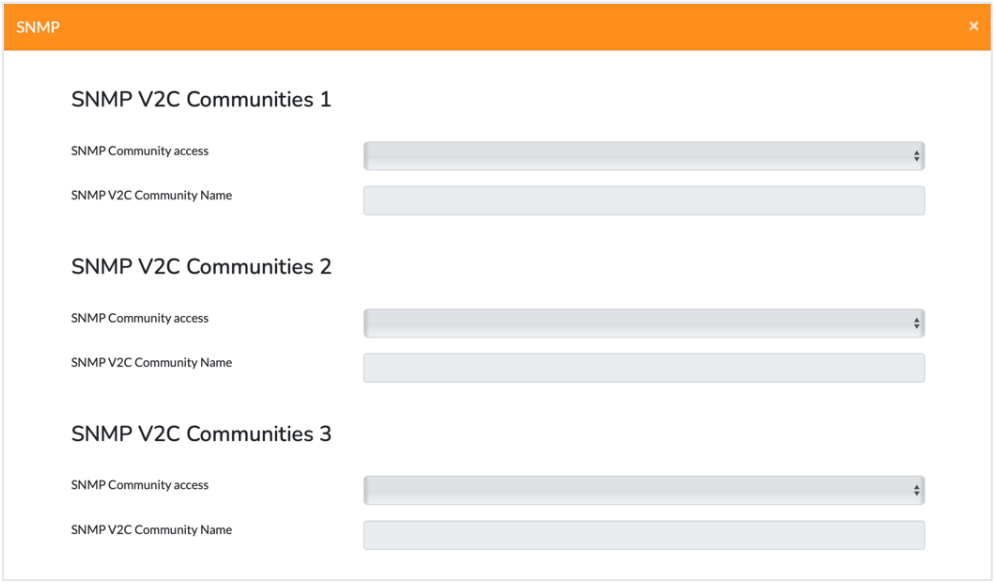

SNMP
SNMP V2C Communities 1
SNMP Community access
SNMP V2C Community Name
SNMP V2C Communities 2
SNMP Community access
SNMP V2C Community Name
SNMP V2C Communities 3
SNMP Community access
SNMP V2C Community Name
SNMP Agent
SNMP Agent Enabled
Disabled
SNMP Agent Port
161
SNMP Agent Version
V2C
SNMP Users 1
SNMP V3 Username
SNMP Community access
SNMP User Authentication
SNMP V3 User Authentication
NONE
SNMP User Authentication Key (Text)
SNMP User Privacy
SNMP V3 User Privacy
NONE
SNMP v3 User privacy key
SNMP Traps 1
SNMP Trap Alert
Disabled
Server
SNMP Trap Receiver Port
162
SNMP Trap Version
V2C
SNMP Trap User or Community
SNMP Traps 2
SNMP Trap Alert
Disabled
Server
SNMP Trap Receiver Port
162
SNMP Trap Version
V2C
SNMP Trap User or Community
Download Mib
Edit
Close

- **SNMP V2C**

  SNMP V2C can be configured with community strings, typically set as "**public**" or "**private**". Each SNMP Community access can be assigned a specific access level:

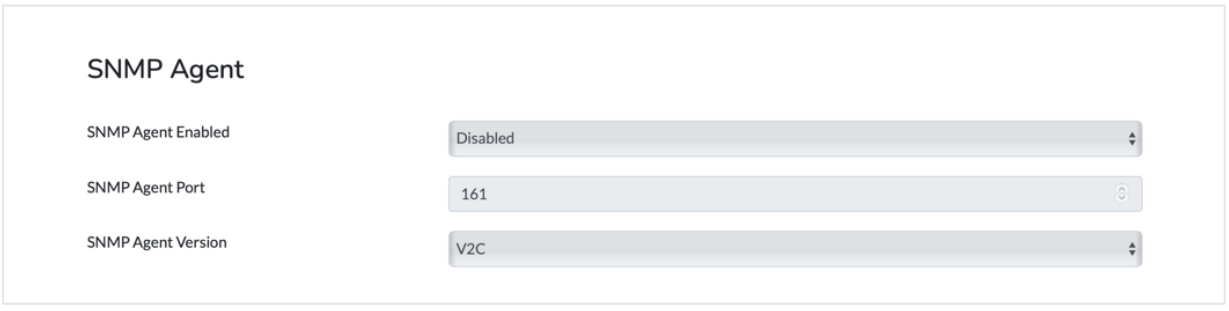
  - **RO (Read Only):** View data only
  - **WO (Write Only):** Send commands without reading data
  - **RW (Read and Write):** Full access to both view and modify data

  The SNMP community name and access level should be set according to the user's monitoring and control requirements.



- **SNMP Agent**

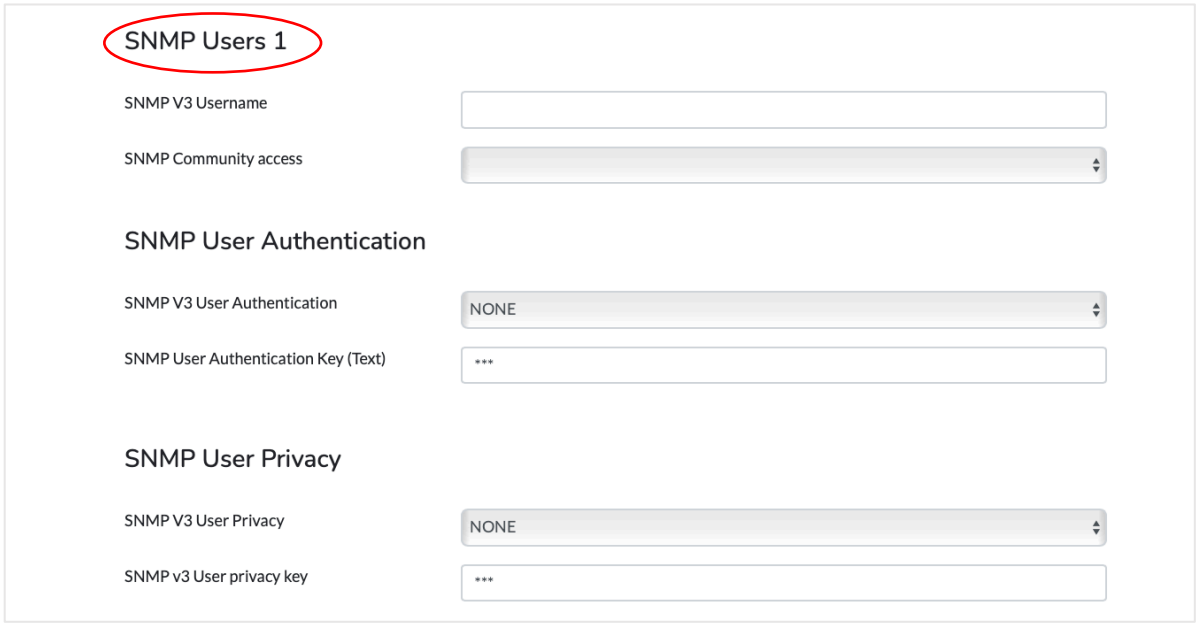
  This is where you can enable the SNMP integration, set the port and choose which SNMP version you want to use.

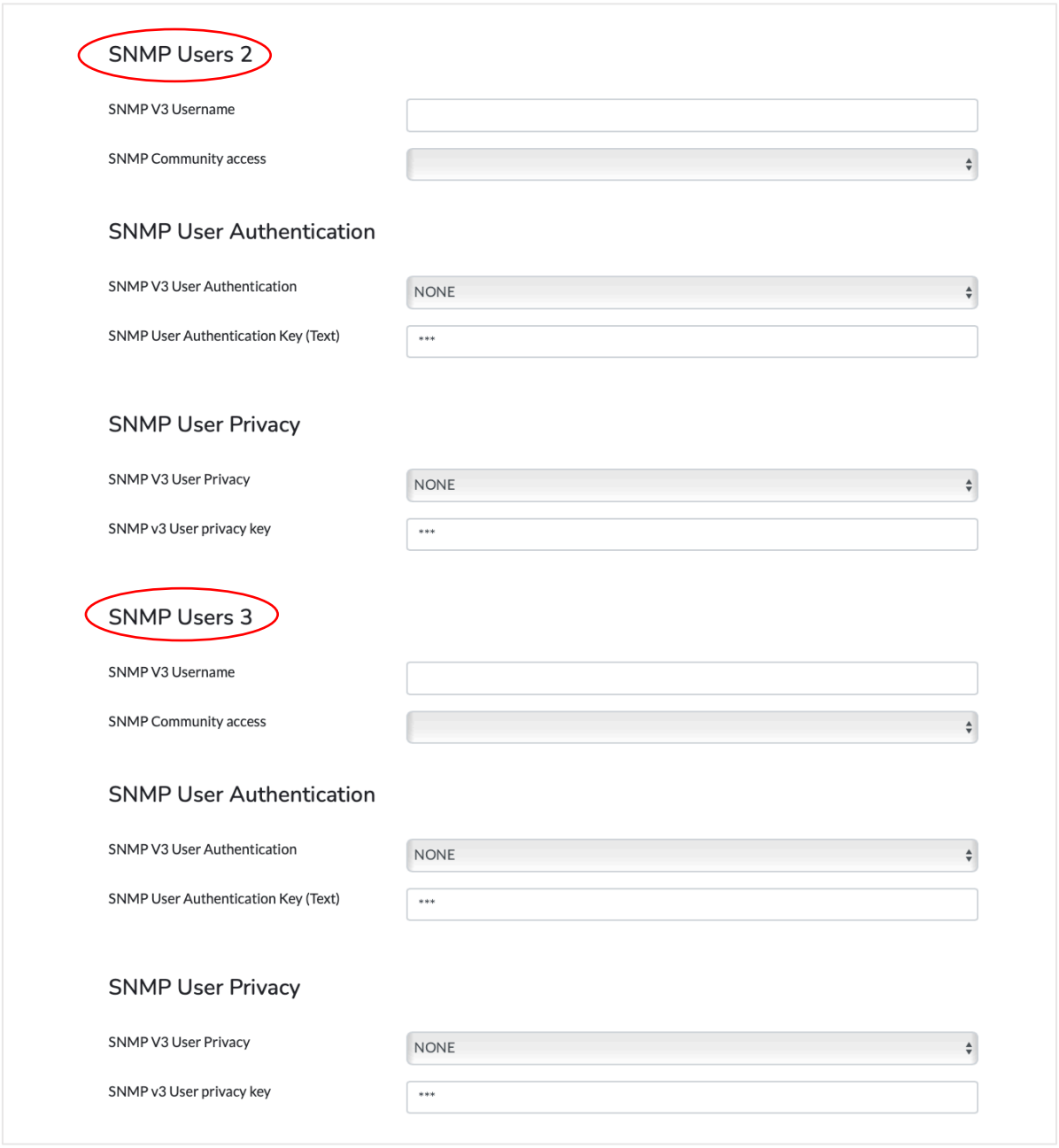


- **SNMP Users 1 / 2 / 3**

  This is settings for SNMP V3, you may configure up to 3 separate SNMP V3 credentials. You can configure up to **three separate SNMPv3 user profiles,** each with its own credentials and access permissions.

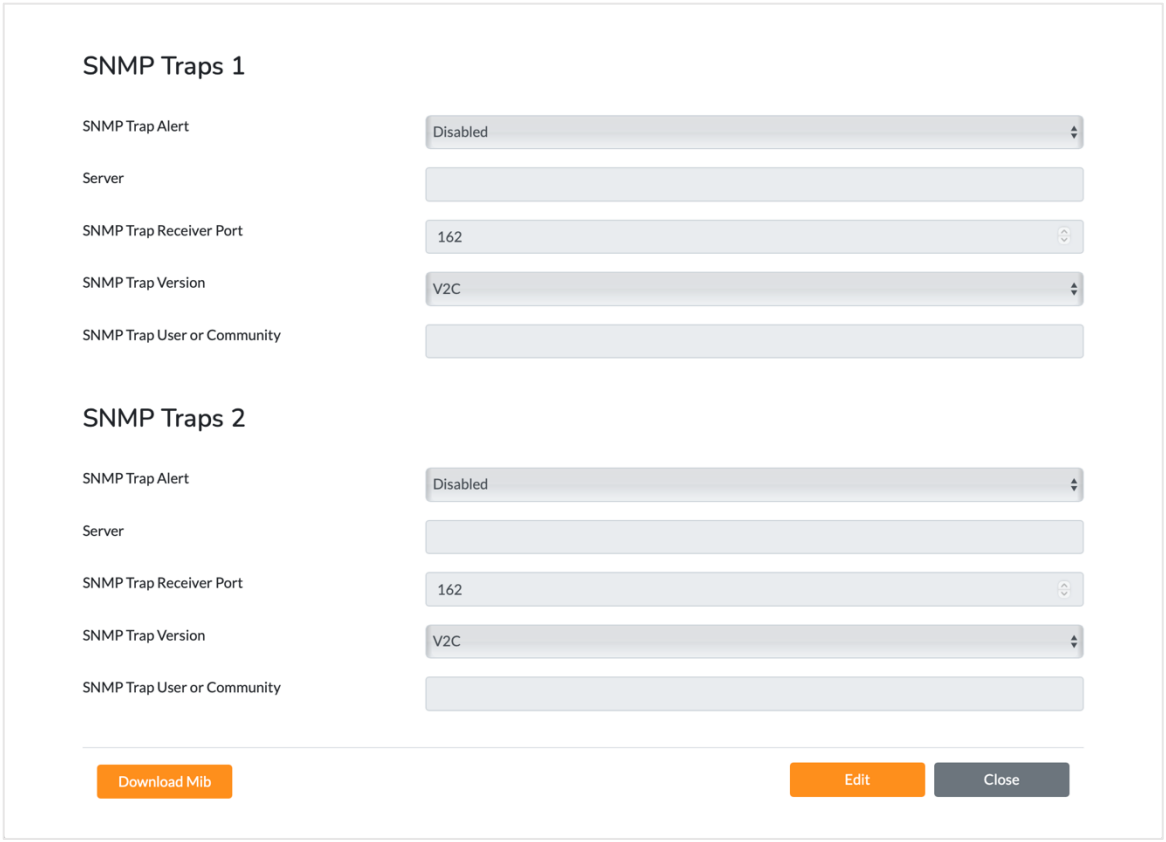
  - SNMP Users
    - SNMPv3 Username
    - SNMP Community Access: Define the access level (e.g.; read-only or read/write) for this user
  - SNMP User Authentication
    - SNMPv3 User Authentication: Choose the authentication method. This ensures that only authorized users can access SNMP data.
    - SNMP User Authentication Key (text): Enter the password used for authentication.
  - SNMP User Privacy
    - SNMPv3 User Privacy: Select the encryption method to protect SNMP data during transmission.
    - SNMPv3 User Privacy Key: Enter the password used for encrypting SNMP messages.




SNMP Users 2
SNMP V3 Username
SNMP Community access
SNMP User Authentication
SNMP V3 User Authentication
NONE
SNMP User Authentication Key (Text)
***
SNMP User Privacy
SNMP V3 User Privacy
NONE
SNMP v3 User privacy key
***
SNMP Users 3
SNMP V3 Username
SNMP Community access
SNMP User Authentication
SNMP V3 User Authentication
NONE
SNMP User Authentication Key (Text)
***
SNMP User Privacy
SNMP V3 User Privacy
NONE
SNMP v3 User privacy key
***

- **SNMP Trap**

  This is where you can enable the SNMP Trap alert, set the SNMP Trap receiver port and choose which SNMP Trap version you want to use by clicking the dropdown.



Important Note:

This section is critical, as the users must enter their preferred community user name that they want since they have 3 options that they can use. **Failure to set this will prevent their traps from working.**

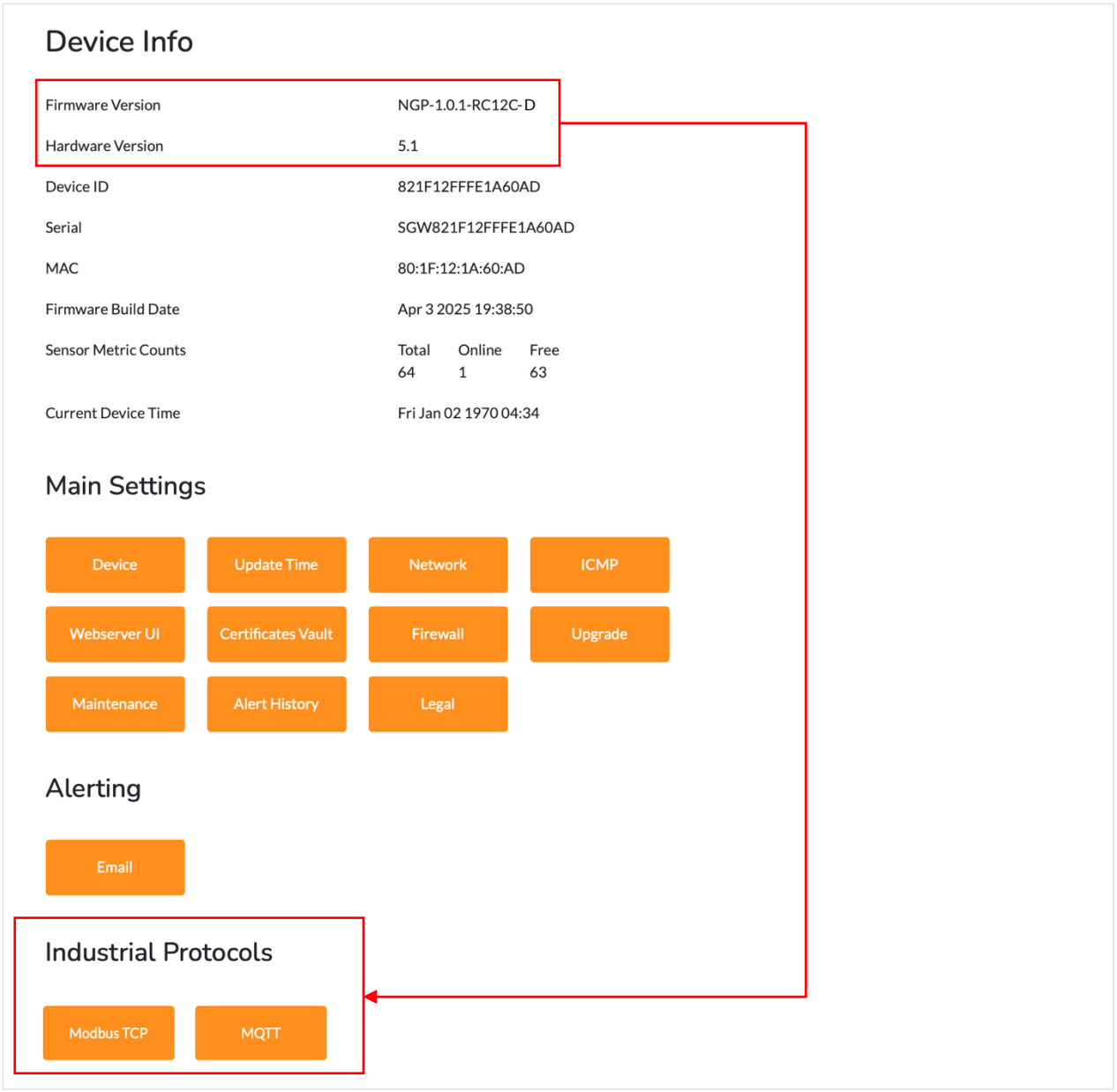
- **Download MIB**

  The 'Download MIB' option allows user to obtain the MIB file for their device and downloading the MIB is require to see the sensors value.

  Please note that an MIB file is required for your SNMP software to access and display the sensor readings.

9.1.3 Firmware Version D | Modbus TCP & MQTT

This Firmware Version D offers two options: **Modbus TCP** and **MQTT** industrial protocols. This version is designed for flexibility, supporting reliable communication for industrial systems (Modbus TCP) and lightweight, efficient messaging for IoT and remote monitoring applications (MQTT).

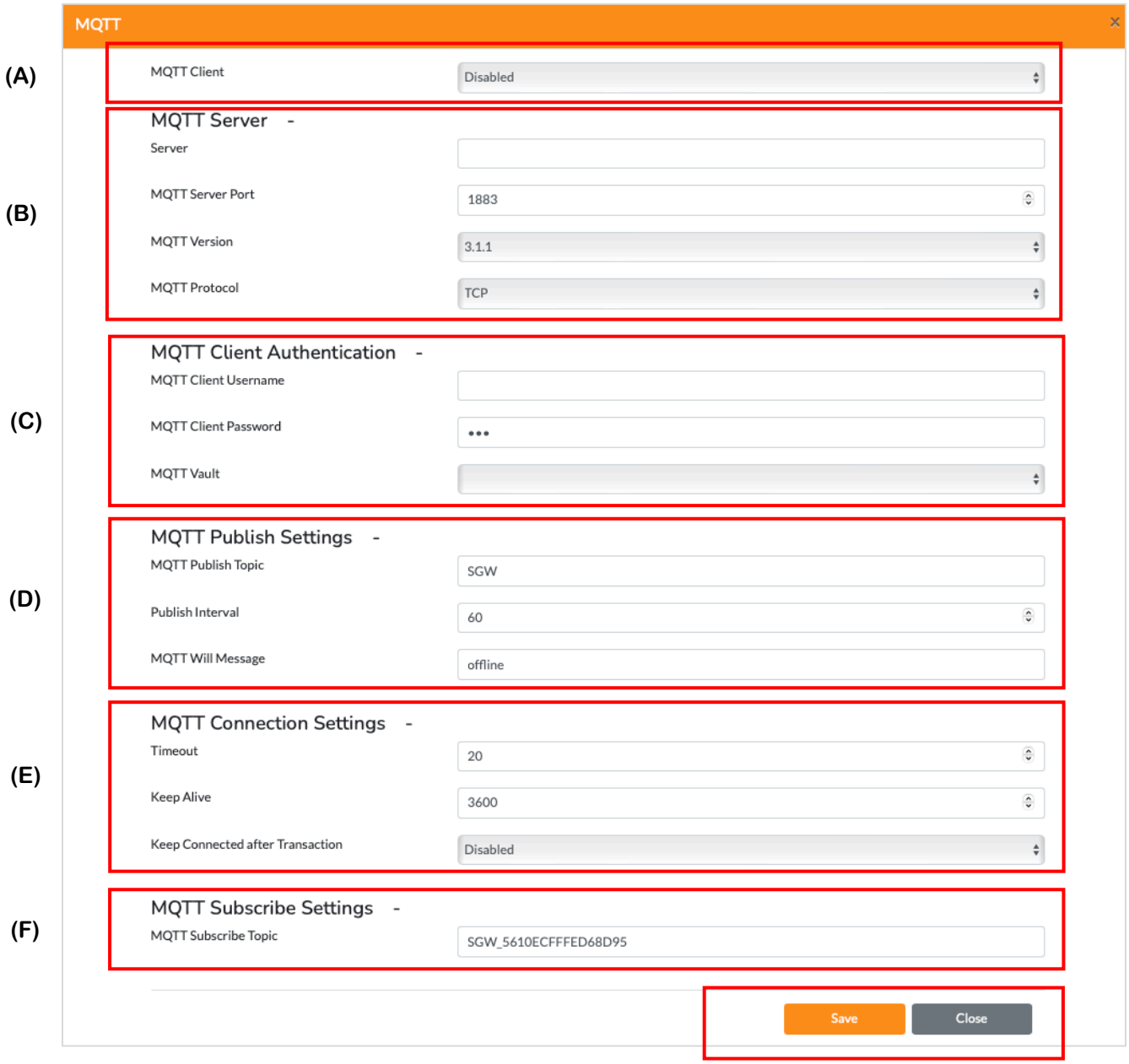


9.1.3.1 Modbus TCP

This option allows the users to enable or disable Modbus functionality. For more detailed on **Modbus TCP**, please refer to **Section 9.1.1.**

9.1.3.2 MQTT

This section is where you can navigate and configure the MQTT, click on the 'Edit' button to enable the configuration fields.



1. **MQTT Client**
   This is where you can toggle your MQTT Client settings between 'Disabled' and 'Enabled'.

2. **MQTT Server**
   This section is where you can enter your Server, edit your MQTT Server Port, choose your MQTT version, and the MQTT Protocol (TCP, TLS, TLS_CERT).

   Note: When selecting "TLS CERT", users must first upload a certificate to the Certificates Vault . The TLS CERT selection will be pulled from the Certificates Vault – failure to upload a certificate beforehand will result in no available options.

3. **MQTT Client Authentication**
   This is the section where you can set your Username, password, and the MQTT Vault. Please note that these options are greyed out and can only be edited if the MQTT protocol is set to TCP.

4. **MQTT Publish Settings**
   This is where you can enter or input your MQTT Publish Topic, which refers to the specific channel or location to which a message is sent (published) by an MQTT client.
   Publish Interval is a configurable parameter and depends on the specific requirements of the application. MQTT will message is a feature that allows a client to specify a message that will be sent by the broker if the client unexpectedly disconnects.

5. **MQTT Connection Settings**
   Configure up to two receivers for SNMP traps. When setting up traps, ensure careful consideration of the receiver ports, and verify that the time on BASE-UNITs is synchronized

6. **MQTT Subscribe Settings**
   Configure up to two receivers for SNMP traps. When setting up traps, ensure careful consideration of the receiver ports, and verify that the time on BASE-UNIT is synchronized

Once you have input the necessary details for each configuration, simply click on 'Save' and a banner will show 'Successfully Saved!' at the bottom part of the screen . Reboot the Base Unit via the maintenance page or reset button to apply all the changes.

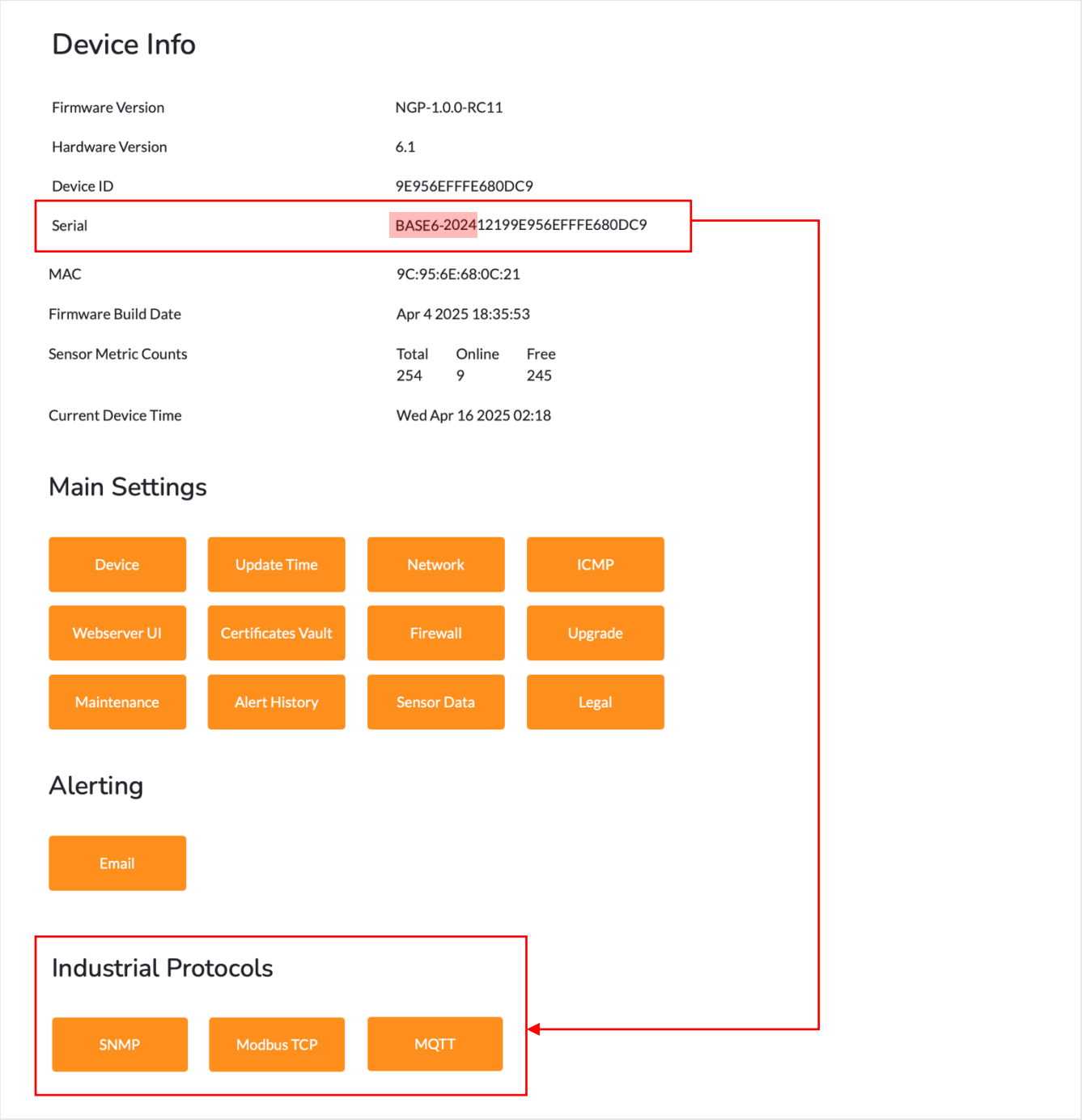
When the settings and certificates applies. We can also verify it with the MQTT broker. The image below shows a sample payload.

9.2 Hardware Version 6

For Hardware Version 6, we provide a variety of industrial protocols tailored to the specific base Unit you are using or require.

9.2.1 BASE-6 | SNMP, Modbus TCP, and MQTT

BASE-6 supports SNMP, Modbus TCP and MQTT, offering robust and efficient communication options for various industrial and IT environments.



9.2.1.1 SNMP

Ideal for network management, allowing seamless monitoring and control of devices. For more detailed information about **SNMP** please refer to **Section 9.1.2.**

9.2.1.2 Modbus TCP

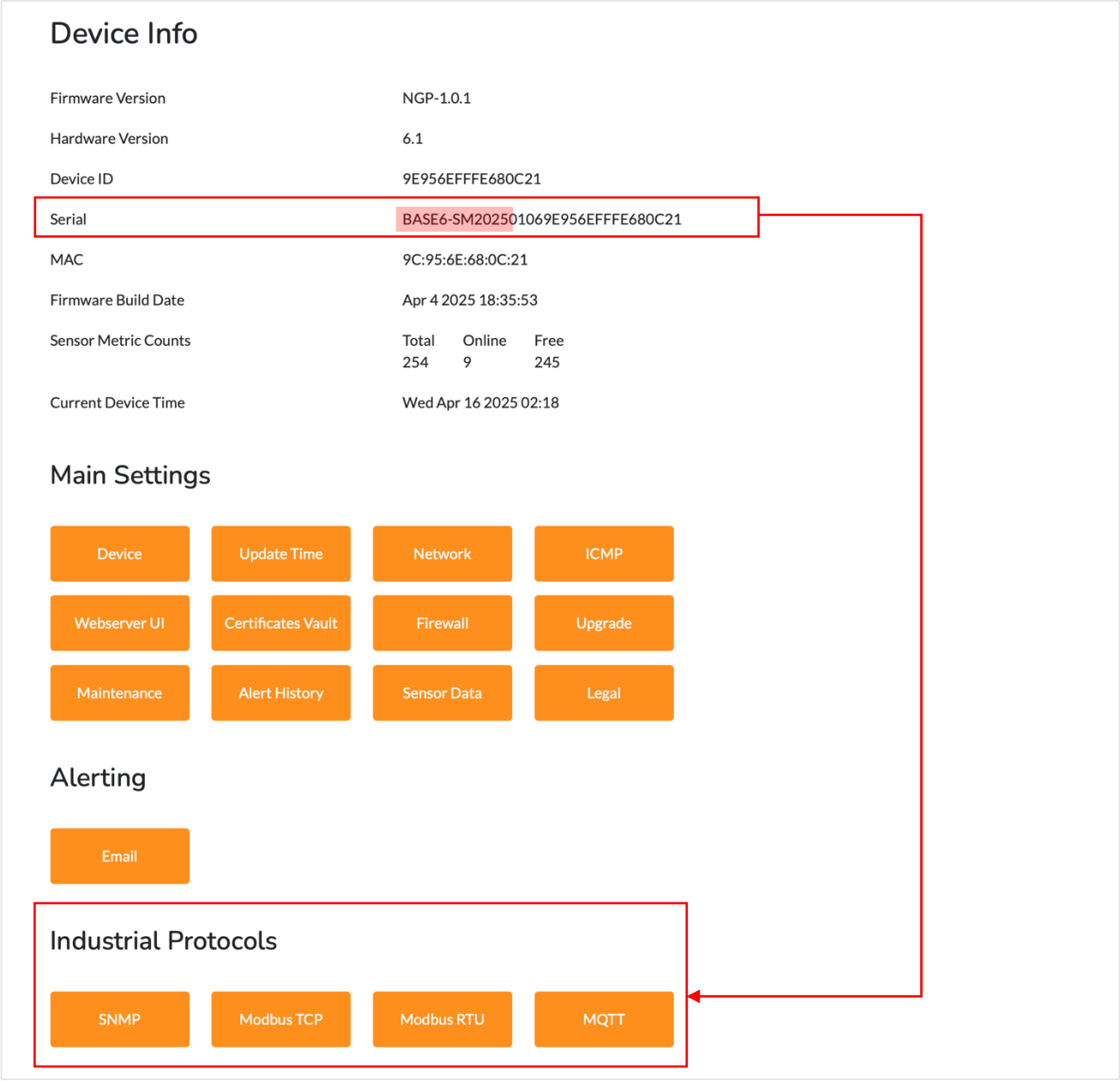
This option allows the users to enable or disable Modbus functionality. For more detailed on **Modbus TCP,** please refer to **Section 9.1.1.**

9.2.1.3 MQTT

For comprehensive guide on **Modbus TCP**, please refer to Sect**ion 9.1.3.2.**

9.2.2 BASE-SM-6 | SNMP, Modbus TCP, MQTT and Modbus RTU

BASE-SM-6 includes support for SNMP, Modbus TCP, MQTT and Modbus RTU, providing flexibility and compatibility for a wide range of applications, from traditional industrial setups to advanced IoT integrations. The BASE-SM-6 is serving as the foundational unit for our entire SwitchMon sensor solution lineup and is equipped with 1 relay offering basic control functionality.



9.2.2.1 SNMP

Ideal for network management, allowing seamless monitoring and control of devices. For more detailed information about **SNMP** please refer to **Section 9.1.2.**

9.2.2.2 Modbus TCP

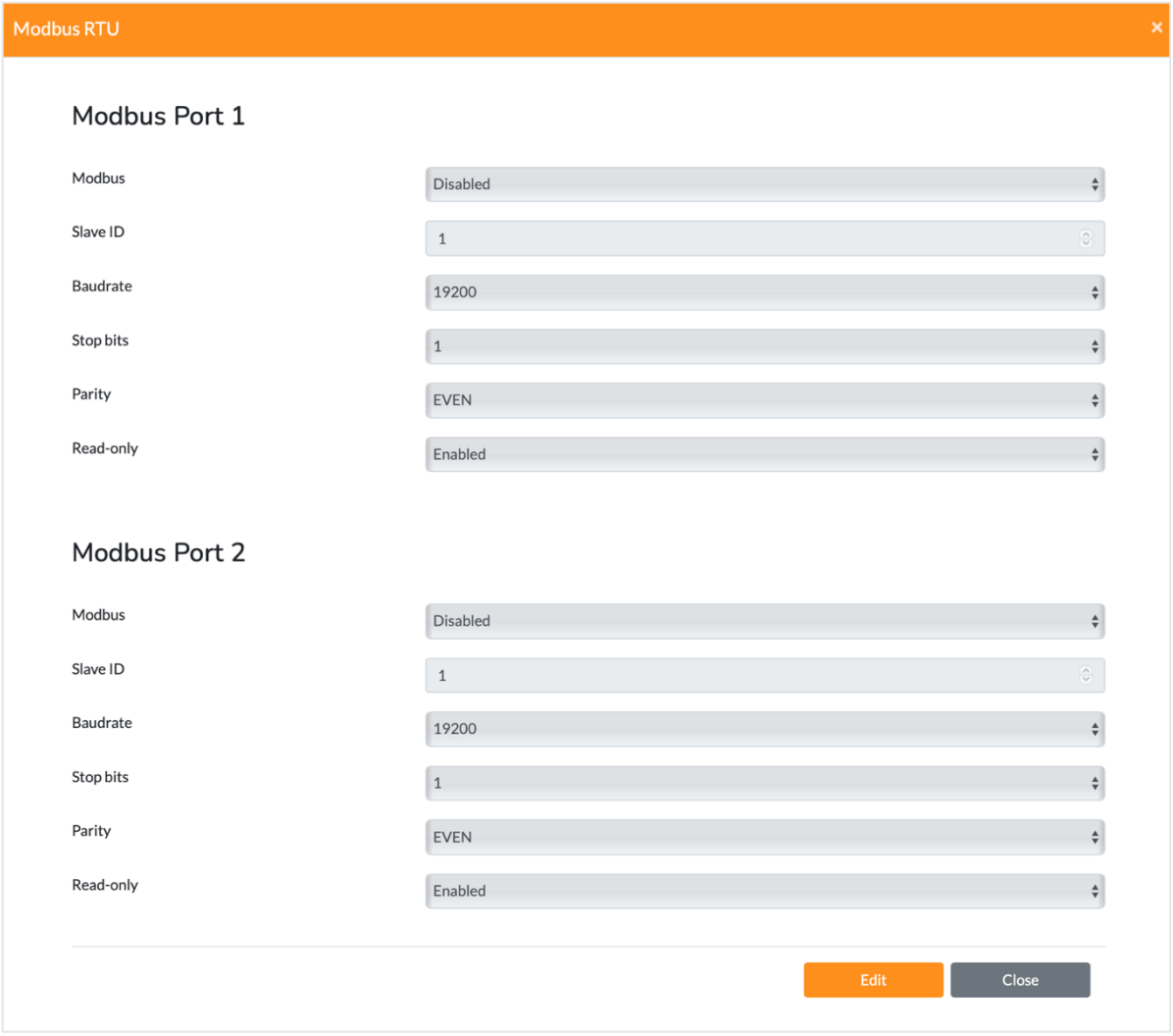
This option allows the users to enable or disable Modbus functionality. For more detailed on **Modbus TCP,** please refer to **Section 9.1.1.**

9.2.2.3 MQTT

For comprehensive guide on **Modbus TCP**, please refer to Sectio**n 9.1.3.2.**

9.2.2.4 Modbus RTU

Supports legacy serial communications, widely used in traditional industrial systems.



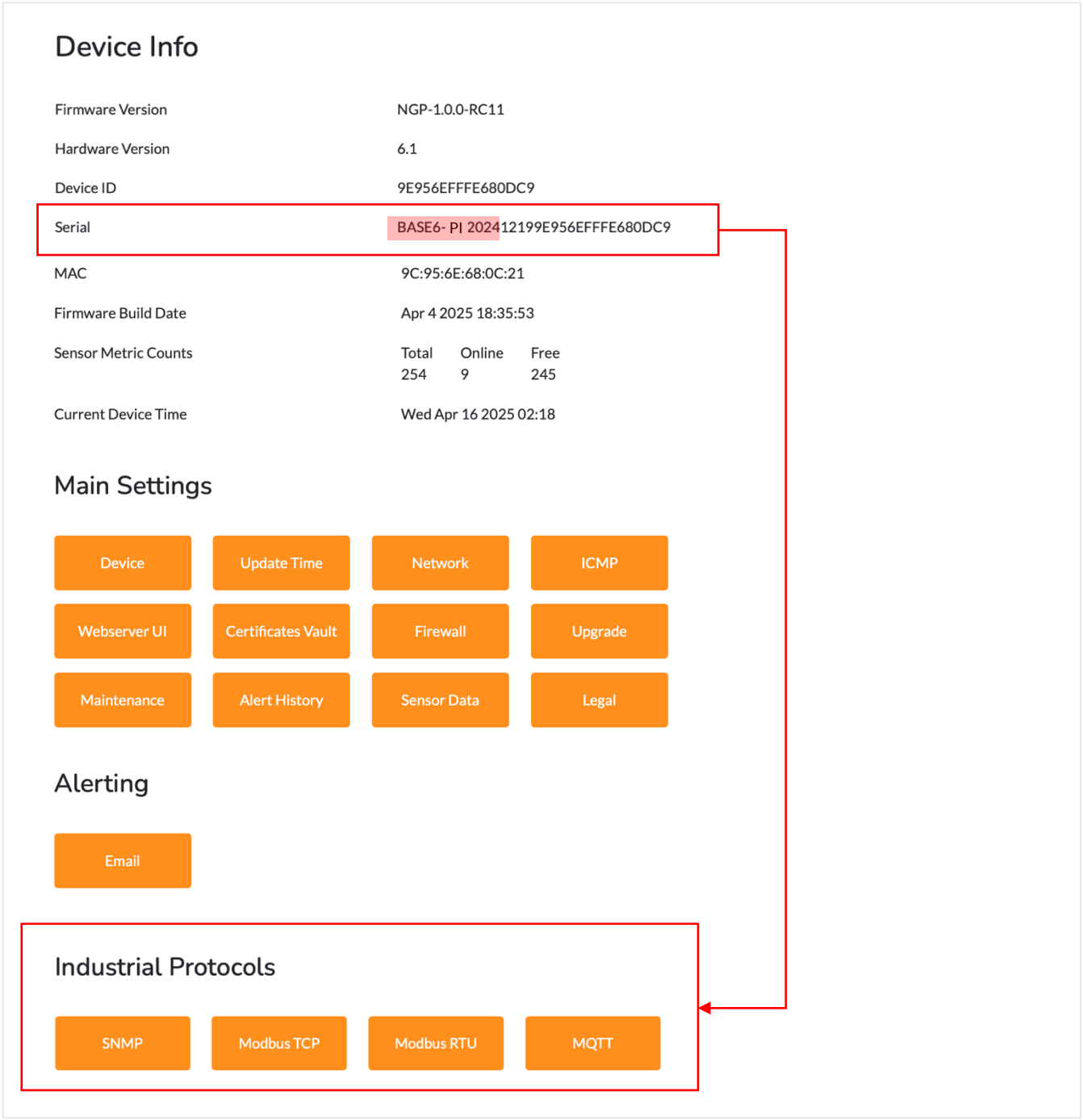
To enable the Modbus and configure the settings, begin by clicking the **Modbus** dropdown menu to activate or enable the functionality. Please note that this window is in read-only mode, so you must click the **Edit** button to modify any settings.

Once in edit mode, configure the following based on your parameters. **Slave ID** which is the unique identification number of your device for communication with the master; **Baud Rate**, with multiple options by default setting it is set to 19200, but you can configure it based on your requirement; **Stop Bits,** where you can select either 1 or 2 based on your systems requirements; and **Parity**, choosing between Odd or Even to match the master device's configuration.

After making the necessary adjustments, ensure you save the settings to enable communication with the master device.

9.2.3 BASE-PI-6 | SNMP, Modbus TCP, MQTT and Modbus RTU

BASE-PI-6 extends support to SNMP, Modbus TCP, MQTT and Modbus RTU, making it versatile for both modern networked systems and legacy serial communications. The BASE-PI-6 is an updated version of the Base Unit that includes new built-in features, such as RS485 on a terminal block with 3 relay output.



9.2.3.1 SNMP

Ideal for network management, allowing seamless monitoring and control of devices. For more detailed information about **SNMP** please refer to **Section 9.1.2.**

9.2.3.2 Modbus TCP

This option allows the users to enable or disable Modbus functionality. For more detailed on **Modbus TCP,** please refer to **Section 9.1.1.**

9.2.3.3 MQTT

For comprehensive guide on **Modbus TCP**, please refer to **Section 9.1.3.2.**

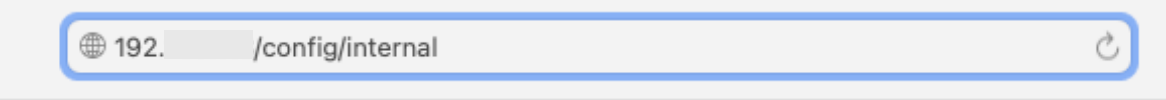
9.2.3.4 Modbus RTU

Supports legacy serial communications, widely use in traditional industrial systems. For more details about **Modbus RTU** please refer to **section 9.2.2.4**

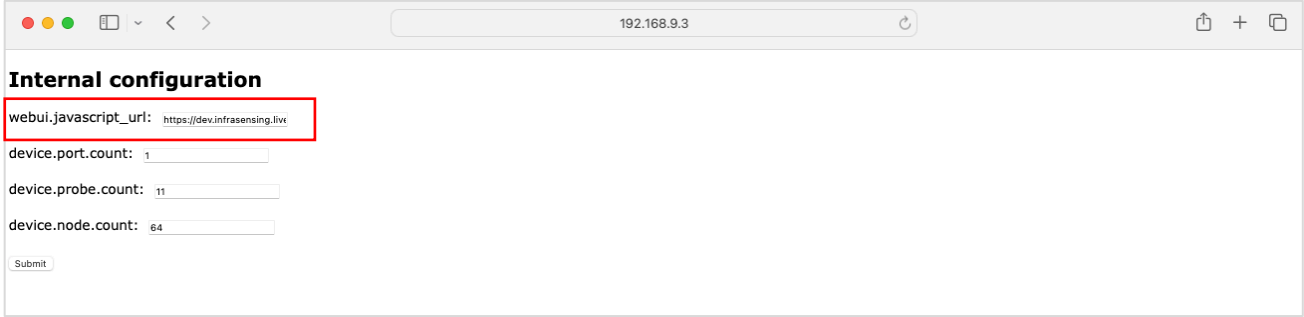
10 UI Files

By default, the web GUI is hosted by InfraSensing. However, customers have the option to host the user interface (UI) files using their own server.

To accomplish this, you need to access this: IP address of your base unit/config/internal



And you will be routed to this page, wherein you can modify the web.javascript_url using your own server. Please see image below for reference:



Disclaimer

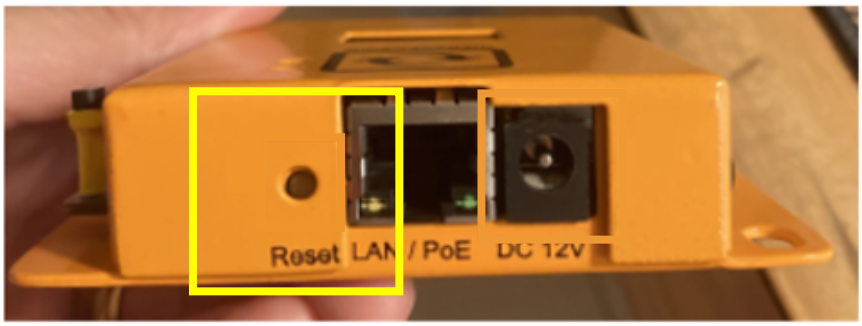
If the UI doesn't load, simply refresh the page. This might occur because the UI files are stored on an external server, and there could be a potential network issue affecting the connection.

When accessing the web UI internet is required as it fetches resources online. However the base unit itself doesn't required internet connection to work. Meaning if you already integrated or perform any integration, it will work normally.

11 Factory Reset

A factory reset is typically performed when the firmware fails to load or function properly. This process restores the device to its original factory firmware.

11.1 Version 5



How to Perform a Factory Reset

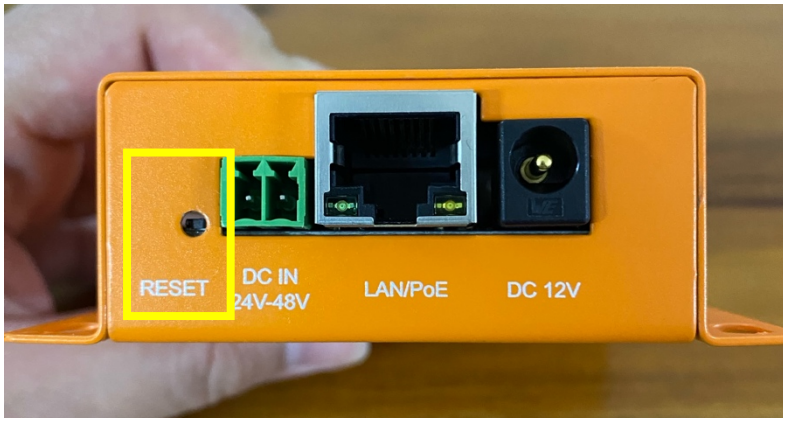
1. Remove the external sensor probe.
2. Remove the power adapter or PoE powered network cable.
3. Push the Reset button.
4. While the Reset button is pushed, plug in the power adapter or PoE powered network cable .
5. Hold it for 15 seconds before releasing it. The yellow LED should be blinking fast.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

11.2 Version 6

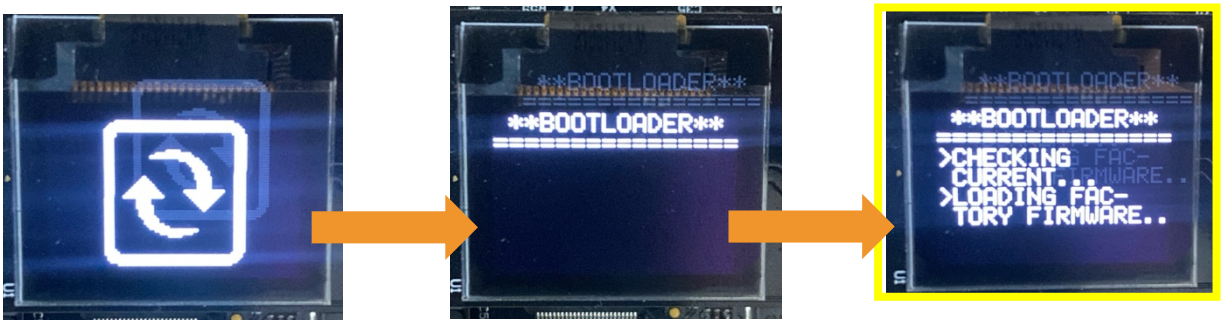
How to Perform a Factory Reset

1. Power off the Base Unit – Ensure that the base unit is unplugged or turned off before proceeding.

2. Initiate the Reset Process – Press and hold the reset button on the base unit. While holding the reset button, power on the device. Note: Ensure to press and hold the reset button until the message **"Loading Factory Firmware"** appears on the OLED display.



3. Wait for the Firmware Restoration – The display will show "BOOTLOADER", followed by "CHECKING CURRENT", "LOADING FACTORY FIRMWARE". Once the third image below appears, you can safely release the reset button.



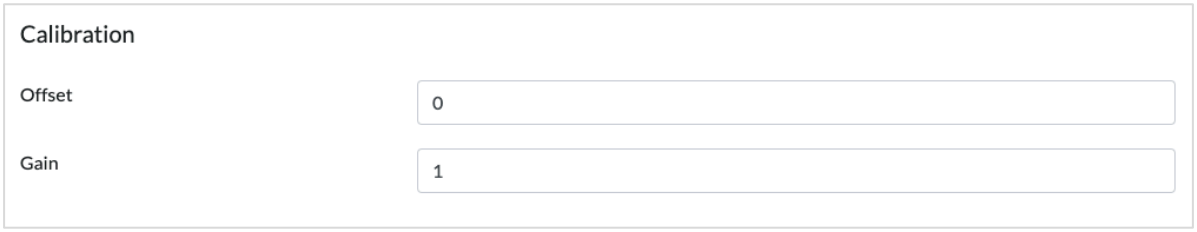
4. Completion – Once "LOADING FACTORY FIRMWARE" appears on the OLED display, the factory reset is complete.

The base unit is now successfully restored to its original factory firmware.

12 Sensor Calibration

With FW10, you can now directly calibrate specific sensors with ease. Unlike older versions where calibration required multiple steps, FW10 allows you to simply adjust the Offset and Gain settings for each sensor.

In order to access this settings, simply click on the Edit button located next to the sensor where you wish to apply this option under Live Sensor Data and a pop window will appear wherein you can see all the threshold and settings that you can configure, at the very bottom of the pop up window you can find the Calibration settings.



Once you have completed all the desired adjustments, click the 'Save' button to apply the changes. A green banner will appear, confirming with the message 'Successfully Saved'.

13 Limitations

With the firmware 10, please note that certain sensors are not yet supported:

- ADDON-LTE
- ENV-CORROSION
- ENV-LHD
- ENV-LEAK-OPTICAL
- ENV-WLEAK-LOC
- IND-0TO10
- IND-4TO20
- R-EGD-PANEL
- R-GAS-FLAMMABLE
- SEC-TILT
- THIMG-XXX
- DAISY-STARTER

Additionally, ensure that only .FULL firmware files are used for upgrades for v6 and .BIN for v5.

14 Legal

The Legal Notices section provides important legal information related to the firmware, including intellectual property rights, licensing terms, disclaimers, and usage limitations. It outlines the legal framework under which the firmware is distributed and used, protecting both the developer/manufacturer and the end user.