GR-7600/V2

Wireless Emergency Lighting System Guide

The present document compiles a complete documentation of the GR-7600/V2 software's User Interface (UI) and user manual. It is to be used as the user's main point of reference for installing, initializing, launching, configuring, and using the software's features. Furthermore, it is designed to help the user understand some of the product's technical aspects and as such, basic technical knowledge is recommended. This manual is structured hierarchically using static screenshots of each element that is of interest.

Table of Contents

1. Introduction

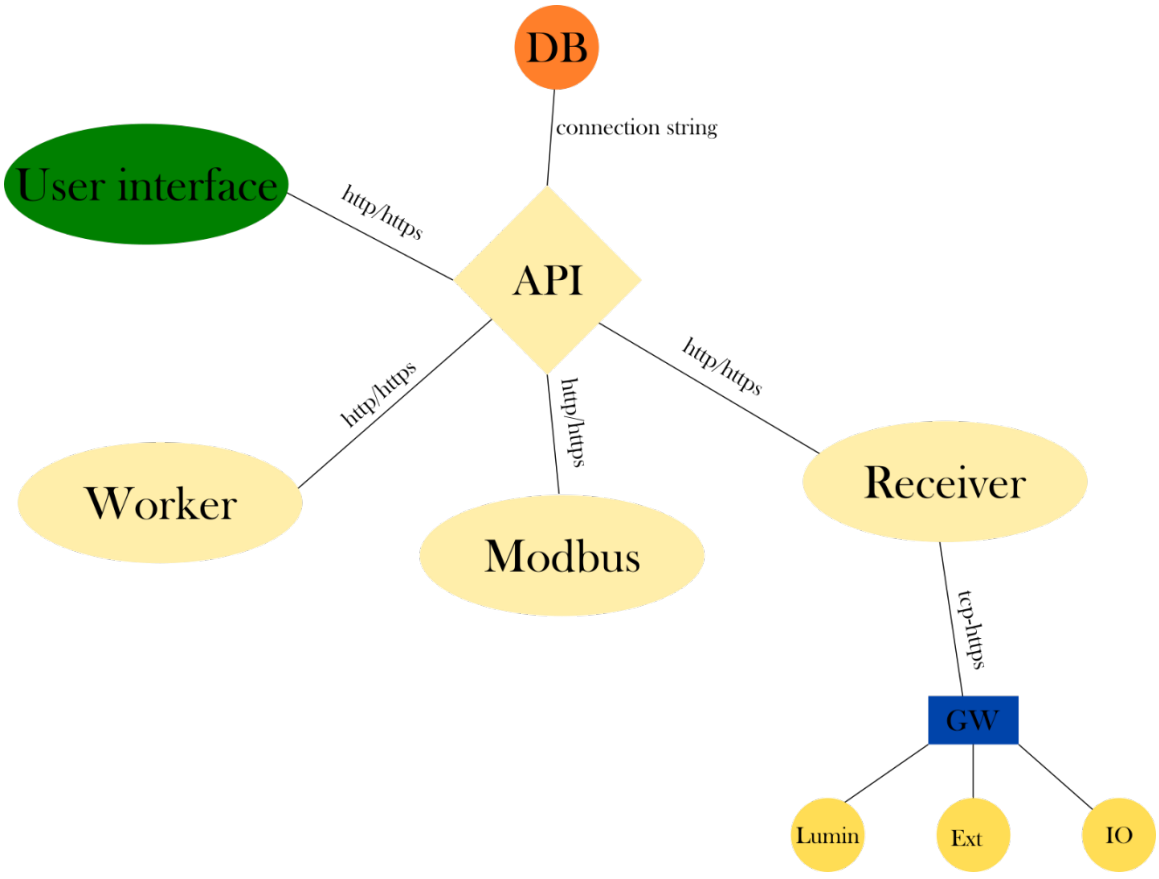
This guide is designed to provide documentation for users and technical staff who will install, configure, maintain, and set the software up on desktop and tablet computers, and use it daily, covering the functionality of every available element and feature, most basic needs and answering most questions that would assist them in solving issues and difficulties.

Note: For a clearer understanding of this user manual, it is recommended that chapter 1.3.1., containing a list of useful keywords and terms that are being repeatedly used throughout the document, be advised.

1.1. Specifications & Features

The product's architecture can be broken down to the following elements, or specifications: the *database*, *API*, *worker*, *data receiver*, *Modbus*, and *User Interface* that essentially is the primary element the present manual describes.

The following image provides a simple overview of the system's architecture.



(i) **Database** – The database is installed along with the main software application. The engine powering the database is the Microsoft SQL Server 2019 software. The database serves as the main storage location for several procedures, the devices' status and information, and floor plan files among others.

- The database has a limit of 10GB of storage, depending on Microsoft's specifications.

- Only one database is required for the entire network of wireless devices, and it can be installed on a single computer.

(ii) **API** – The API is built using the .NET 6 technology. It communicates with the database using a connection string, which is a string that specifies information about a data source and the means of connecting to it. All queries placed to the database are carried out through the Entity framework, using ORM. It serves as the bridge for the communication of each separate element with one another.

- It can be installed anywhere on the network and is installed as an always-on service in the background.

- All calls placed to the API use the HTTPS protocol utilizing a self-signed certificate.

(iii) **Worker** – It is a Windows service built with the .NET 6 technology. Its purpose is to receive specific information from the tables of the database and record and store it in another table that will facilitate the UI and serve as a summary.

- It checks for any scheduled tasks or procedures that are selected by the user to ensure their successful execution.

- It utilizes the SMTP protocol and other e-mail services to distribute general reports and notification messages to the software's users.

(iv) **Data receiver** – It is a Windows service built with the .NET 6 technology. The data receiver is installed on the main computer and is responsible for all communication between the installed gateways and the wireless points – luminaires and I/O units – for the transmission of the various commands the user may send. It records and stores the status of those devices in the database.

- It is installed as an always-on service in the background.

- All requests are being monitored in real time.

- The tasks assigned to devices through user commands may be programmed or ad hoc created.

- Multiple data receivers can be installed – one receiver per installed panel – on multiple computers within the same network, while enabling their communication with the same database through the API.

(v) **Modbus** – It is a Windows service using the .NET 6 technology, responsible for the Modbus protocol implementation in the software. More information can be found in chapter 3.1.7.5.

(vi) **User Interface** – The UI is a Windows Forms application built with the .NET 6 technology and comprises the graphical environment for the system's functionality, monitoring and maintenance. It can be installed on every computer that can be connected to the same network as the wireless devices and each software installation can be linked to a single panel to expedite the monitoring of larger installation sites.

- The UI has multiple-user capabilities.

- It facilitates the user's interaction with all of the devices within the network.

- It utilizes multiple selection criteria for filtering the search results of all connected devices.

- It enables the user to export any available screen as an HTML format file for future viewing and print any screen's contents.

- The floor plan files can be exported as various image formats.

- The software is translated into seven (7) different languages.

1.2. System Requirements

The minimum system requirements are:

- Windows 10/11 x64

- 8GB RAM, or more

- 10GB of free storage, or more

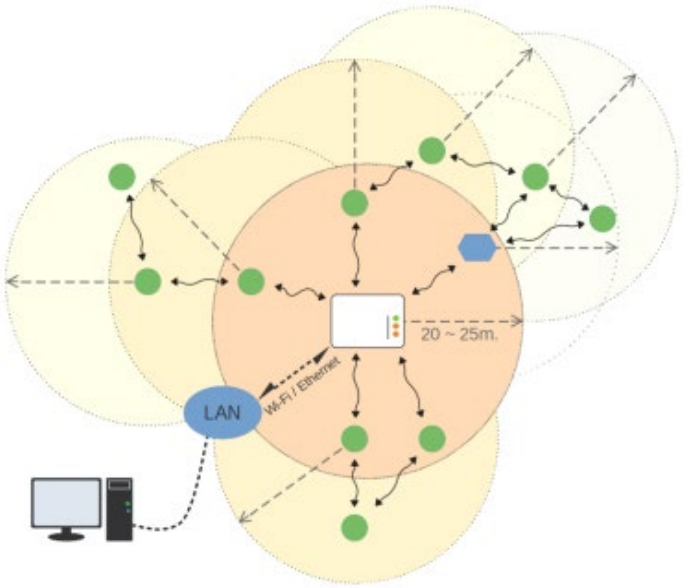
- .NET Framework 4.8

- Internet connection

1.3. Topology

The wireless connection among the devices is established through a fast, mesh-type network, at 868 MHz. A wireless network consists of a wireless network master – gateway – and a group of wireless devices – luminaires, network extenders and wireless input/output units – connected to the gateway, the master device of the network.

Each wireless device can be connected directly to the gateway or use other wireless devices that essentially serve as repeaters to reach the gateway, as per the mesh-type network.



Gateway

Wireless emergency luminaires

Wireless network extender

The previous image serves as a network formation example, of a mesh-type network. The wireless range in a building's interior is approximately 20 to 25 meters from device to device, when the in-between physical obstacles are typical brick walls and wooden or synthetic furniture.

Multiple wireless networks can co-exist in an installation simultaneously and be monitored through a single control panel. Each system can support up to 16 gateways and up to 200 wireless devices per gateway.

1.4. Wireless Network Specifications & Terms

(i) **Wireless network master** – The gateway is the master device of a wireless network. A gateway's role is to collect wireless data from the wireless emergency lighting installation and transfer this data to the master control panel. Available models include models with Ethernet/Wi-Fi, and USB connectivity.

(ii) **Wireless device** – Such a device may be any type of wireless device, i.e., emergency luminaires, network extenders and input/output units, that connect to a wireless network.

(iii) **UID (Unique ID)** – UID is the unique address of each wireless device. It is used by the central system to distinguish each wireless device from another. It comes in 8-digit hexadecimal values.

(iv) **SID (System ID)** – SID represents the wireless network's name. All wireless devices within a wireless network must share the same SID to form a connection. The default SID value is 00000001, in its 8-digit hexadecimal form.

(v) **NKey (Network Key)** – NKey is a key used to encrypt all transmitted communications, providing a high security level, and preventing attacks on the wireless network(s). The default NKey is set to 00000000, in its 8-digit hexadecimal form.

(vi) **RF Channel** – This is the operating frequency of the wireless network. There are four (4) available channels – numbered as 2, 3, 4 and 5 – within the 868.150 MHz – 868.450 MHz frequency range, to be used for the network(s), which can be changed through the Installation menu of the software. When there are other wireless networks operating nearby, a different RF channel should be used for each network to avoid data traffic. The default channel is 2.

(vii) **Hop level** – The hopping functionality constitutes the primary feature of a mesh-type network. Through this feature the wireless devices do not require to be directly connected to a gateway, as data can be re-transmitted by any wireless device located between the gateway and the target device, provided that every in-between device is within the same network and in range. Thus, each device in-between is also a repeater. The Hop level value indicates the number of times the data hopped from one nearby device to another till it reached the gateway. Typically, a wireless network is able to sustain up to 16 hops.

(viii) **Network level** – It is identical to the Hop level and indicates the number of devices serving as repeaters between the gateway and a wireless device.

(ix) **Self-healing** – If a wireless device, e.g., a luminaire, which connects to a gateway through hopping, loses its connection with its link, it will automatically search for a new available route, if there is one, and reconnect. This function does not require human interaction.

(x) **Listen-before-talk** – Prior to transmitting any data, a wireless device checks the communication channel for occupancy in order to avoid any collisions and data loss.

Note: In order for a gateway and a group of wireless devices to form a network and connect to one another, they must share the same SID, Nkey and RF Channel values.

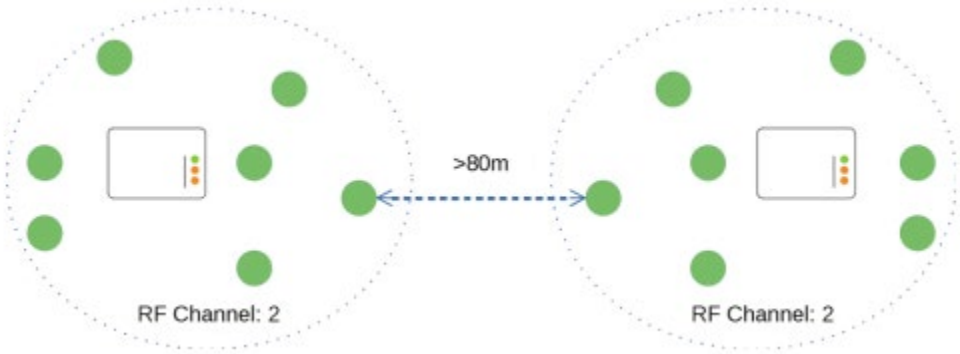
When the SID and RF channel between two devices match, but the NKey values do not, there will be a wireless connection where the transmitted data will not be able to be decrypted, and thus no valid data will be received. When the SID or the RF channel value between two devices differs, there will be no connection between those two devices, as they will belong to different networks.

1.5. Wireless Network Installation & Restrictions

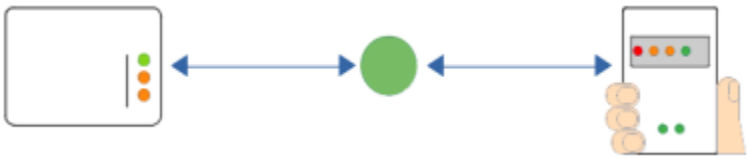
(i) If another wireless system operating at 868 MHz is present in the area, prior to installation, the external **Wireless Installation Tool** application needs to be used along with a GR-7605/V2 or GR-7607/V2 device to check the frequency spectrum, through the same application, on channels 2, 3, 4 and 5. During installation free channels are preferred over occupied RF channels, in order to avoid collisions and data loss.

(ii) It is recommended to use a different RF channel for neighboring wireless networks. An RF channel can be reused by two separate networks when their closest devices are at least 80 meters away. When the distances between two networks are shorter, a different RF channel should be used.

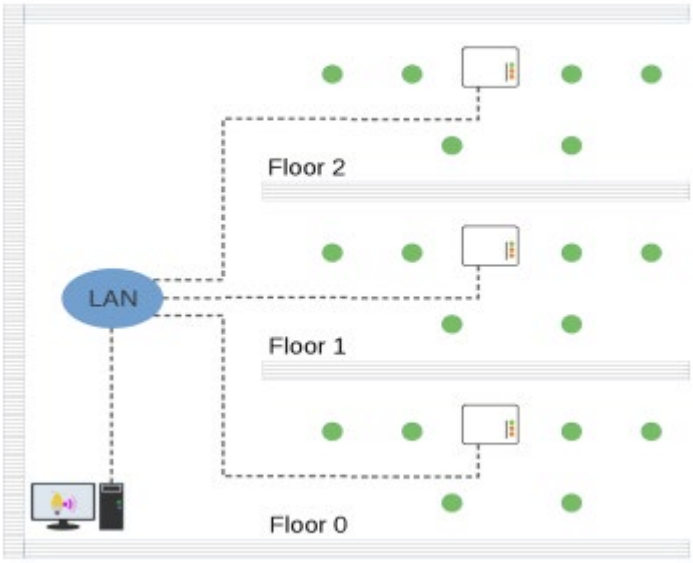
The distance can vary depending on the structure of the building.



(iii) During the installation of a wireless network, it is recommended that the GR-7605/V2 Wireless Signal Strength Tester – RSSI – be used to check the signal reception levels before installing and activating a wireless device, such as a luminaire, at that position. The installation area that is closest to the gateway should be measured first, persisting for at least 1 minute for better measurement results. The observation of level indications of 3 and above is recommended. The same should be repeated for each of the next installation areas. It should be noted that each signal reading originates from any active and re-transmitting wireless device. In cases where the signal is lower than level 3 and another emergency luminaire cannot be installed in-between, the installation of a wireless network extender should be considered.

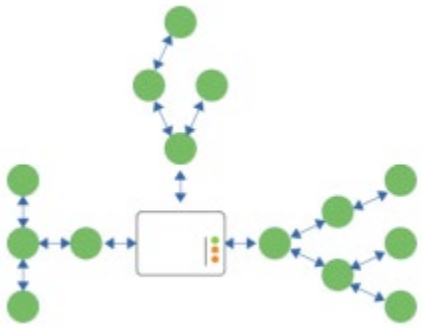


(iv) The wireless signal is capable of traveling through the interior brick walls and conventional furniture – wooden or synthetic – covering distances of 20 to 25 meters within the building's interior. Building floors are usually made of reinforced concrete with steel/iron bars that can interfere with the passing of the signal. Therefore, when the installation area requires the coverage of multiple floors, it is recommended that an independent wireless network be used for every floor. All gateways can be connected to a local network and monitored from a single control panel.



(v) The same wireless network to cover multiple buildings should be avoided, even when the number of wireless devices has not reached the gateway's limit of 200 devices. Attempting to cover multiple buildings with a single network may lead to connection instability, due to weather conditions or outside obstacles. Thus, an independent network should be created for every building, which can be controlled via the same control panel, provided that there is a single local area network that can be shared among the buildings.

(vi) Gateways are recommended to be installed at central points, where there is at least 1 wireless device, such as a luminaire, within range and that is directly connected to a gateway for every 15 wireless devices. For example, for a network of one hundred and 120 wireless devices in total, at least 8 of them should be directly connected to the gateway, within a 25-meter radius, in every direction. Thus, a formation closely resembles the star formation is achieved and the overall data load is split more efficiently.



(vii) The gateway's device limit of 200 should not be exceeded. For maximum capacity to be achieved, the previous rule must apply. Therefore, the gateway should be installed at a position where at least 12 or 13 wireless devices are in range to be directly connected to the gateway, spreading towards each direction.

(viii) During the technical study and prior to the installation, it is recommended that alternative routes for most of the wireless devices be predicted and created, to ensure proper communication, even in the event of a wireless link of a device with the other devices breaking. In-line connections should be avoided whenever possible because they do not provide alternative routes for the signal to pass through when a link is broken.

1.6. Wireless Devices & Peripherals

116-GR-7610/V2 PC Wireless

The PC Wireless is a standalone control panel for wireless emergency lighting. It is equipped with a 7" color touch screen and a backup battery of 1h duration. Runs the Standard version of the Autronica GR-7600/V2 software application – the currently described software, pre-installed. Works with the 116-GR-7607/V2 or 116-GR-

7605/V2 USB gateway and with 116-GR-7603/V2 gateway.
Max connected devices: 400
Max connected gateways:10
Max connected devices per gateway:200

116-GR-7620/V2 PC Wireless Rugged

The PC Wireless is a standalone control panel for wireless emergency lighting suitable for industrial usage. It is equipped with a 10” color touch screen and a backup battery of 4h duration. Runs the Standard version of the Autronica GR-7600/V2 software application – the currently described software, pre-installed. Works with the 116-GR-7607/V2 or 116-GR-7605/V2 gateway and with 116-GR-7603/V2 Wireless Network Master Eth/WiFi.
Max connected devices:1000
Max connected gateways:10
Max connected devices per gateway:200

116-GR-7630/V2 PC Wireless Tabletop

The PC Wireless is a standalone control panel for wireless emergency lighting suitable for reception etc. It is equipped with a 10” color touch screen and a backup battery of 4h duration. Runs the Standard version of the Autronica GR-7600/V2 software application – the currently described software, pre-installed. Works with the 116-GR-7607/V2 or 116-GR-7605/V2 gateway and with 116-GR-7603/V2 Wireless Network Master Eth/WiFi.
Max connected devices: 1000
Max connected gateways:10
Max connected devices per gateway:200

116-GR-7603/V2 Wireless Network Master Port/Wifi

The Wireless Network Master Port/Wifi T2 is a gateway device for the wireless emergency lighting that provides flexible connectivity options. It provides Wi-Fi (WPA/PSK or WPS) and Ethernet connection options, with dynamic – DCHP – or static IPv4 addressing, for local network connection and communication with the master PC – Autronica GR-7600/V2. The configurations are applied through a simple webpage – connect via its mini Access Point. Capable of controlling up to 200 wireless devices. It is supplied via the mains power – 220-240V / 50-60Hz – line without a self-contained backup operation. For uninterruptible operation a UPS power line must be used.

116-GR-7607/V2 Wireless Network Master USB

The Wireless Network Master USB T2 is a USB gateway for the wireless emergency lighting. It is connected via a USB port to the master PC – running Autronica GR-

7600/V2 – and is capable of controlling up to 200 wireless devices. It is power supplied via USB.

116-GR-7604/V2 Wireless Network Extender

The Wireless Network Extender is a signal range extension device, or signal repeater. It re-transmits received messages, similarly to wireless emergency luminaires – within a 20~25-meter range. It is supplied via the mains power – 220-240V / 50-60Hz – without a self-contained backup operation. For uninterruptible operation a UPS power line must be used.

116-GR-7605/V2 Wireless Signal Strength Tester RSSI

The Wireless Signal Strength Tester RSSI main functionality is to be used as a hand-held signal level measuring device during the installation of the wireless emergency lighting and to check signal coverage in an area, before installing a device. It can alternatively be used as a USB gateway, a spectrum analyzer or a manual installation tool – along with the 'Wireless Installation Tool' software application.

116-GR-7606 Wireless I/O Unit

The Wireless I/O unit is a device that can be used to bridge another system – safety or monitoring system – with the wireless emergency lighting. It implements 2 relay outputs – dry-contact – that are programmable and can be armed in case of emergency, fault, test, or other function. The 2 inputs are also programmable and can be used to run a test procedure – lamp or battery – or force an emergency operation.

116-GR-6600/V2 Plug-in module Wireless

The Plug-in module Wireless is the wireless adapter that can be installed in a compatible self-contained emergency luminaire, in order to provide wireless connectivity. It is supplied directly from the emergency luminaire internal power supply. It also works as a signal repeater – mesh-type / hop – and, thus, extends the signal range of a wireless network.

1.7. Wireless Devices Installation

Each wireless device comes with the factory default values for the SID, Nkey and RF channel of **00000001**, **00000000**, **2**, respectively. In order for a device to join a wireless network, the SID, Nkey and RF channel values must match those of the network.

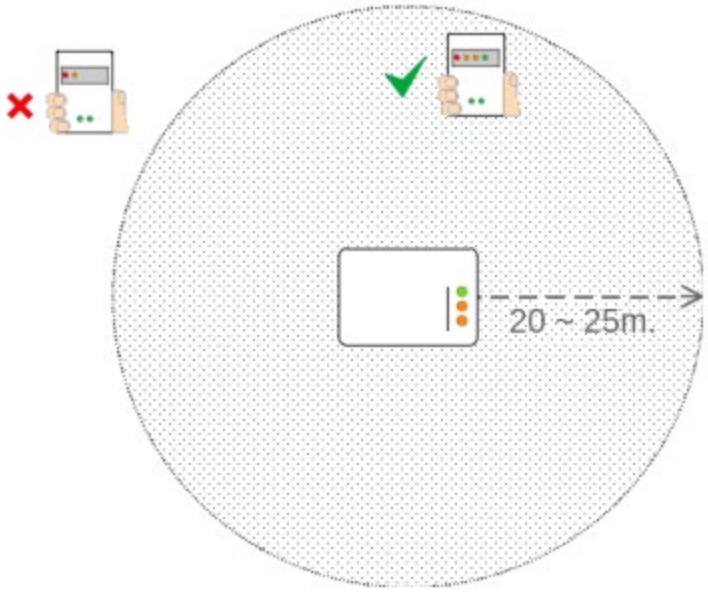
Before starting the installation process, it is recommended that at least 1 GR-7605/V2 Wireless Signal Strength Tester RSSI T2 be available with a fully charged battery. While it is plugged into a USB port for charging, the orange LED – **CHA** will remain lit as long as it is still in charging mode. When the battery is full, this LED will be turned off.

The step-by-step guide that follows is optional, but also the safest way to ensure that the quality of the connection among the wireless devices is adequate and stable.

(i) The gateway must be installed at its given location and activated. Chapter 3.1.6.1. should be referred to for further instructions on the installation or addition of a gateway device to the system.

(ii) Once the gateway is active, it will start transmitting. The transmitted signal is picked up by other wireless devices in order to detect and join a wireless network. It can also be tracked by the Wireless Signal Strength Tester RSSI T2 that can read and display the received signal level – Received Signal Strength Indication – with LED levels ranging from 1 through 5.

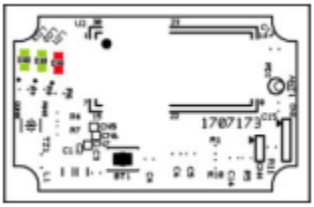
(iii) Once close to a position within 25 meters of the gateway, the Wireless Signal Strength Tester RSSI T2 should be used to measure the signal. First, it should be activated by pressing the main button for 3 seconds and then pushing it again to change to the RSSI Tester indication mode. The red LED on the left will immediately turn on. Within a few seconds, mode LEDs will be and remain turned on so long as there is signal present at that position. After at least a full minute passes, for better measurement results, the strength of the signal should have been stabilized. If the indication level contains 3 or more turned on LEDs, then the position is optimal for installing a wireless device and the quality of the connection will be within the acceptable levels. Afterwards, the wireless device, such as the luminaire, can be installed and activated. When the signal is weaker, the addition of another wireless device in-between, such as a network extender or another luminaire, should be considered to enhance the signal reception.



(iv) When installing a wireless device, it is advised that notes be taken regarding the device's location and UID address. The package-included extra UID stickers can be used towards this end. This action will assist a potential graphical installation plan later on.

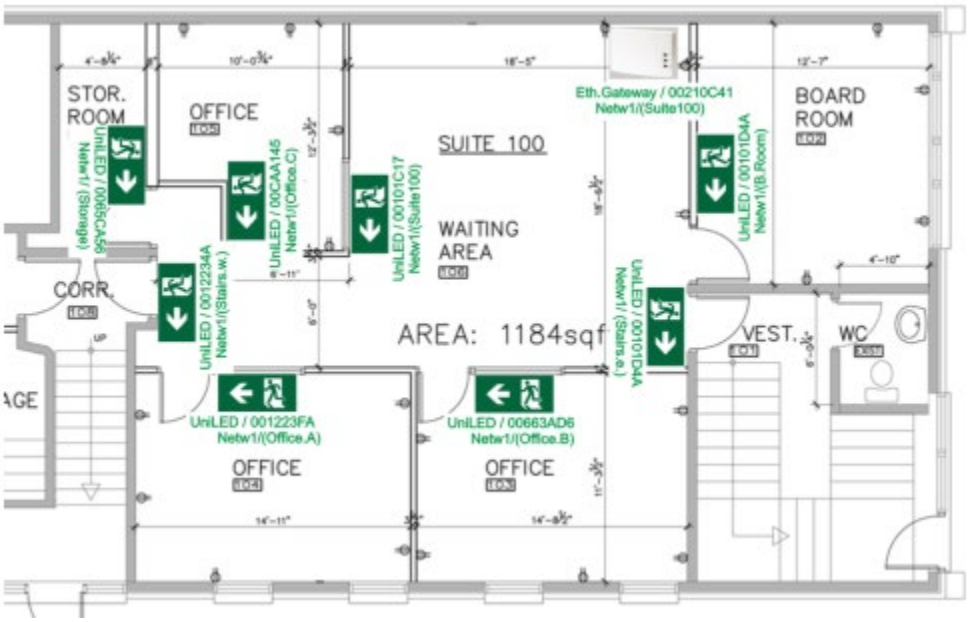
(v) After installing and activating the first wireless devices, the same method can be used to measure the signal's strength at the following closest installation position, and so on. It should be noted that every time a new device is activated, the signal-level reading indicates the signal level that is received from the gateway or any of the already installed wireless devices that operate as repeaters. Similarly, the process may continue until the installation is completed.

(vi) By observing the LED indicators on the wireless adapters inside a luminaire, it can be confirmed whether the device has joined the wireless network or not. The blinking of both the **LD2** and **LD3** green LEDs indicates the successful connection, while the blinking frequency indicates the connection's quality. When the **LD3** LED is turned off, there is no connection. The corresponding manual regarding the wireless adapter's indication should be referred to.



(vii) When the installation of the wireless devices has been completed, a graphical installation plan of the entire installation should be created, on paper or

via digital means. This step is important for any future installations, maintenance, and troubleshooting. A sample image of a floor plan is displayed below.



The above image is only an example. A graphical floor plan may be created to meet the needs of the installation.

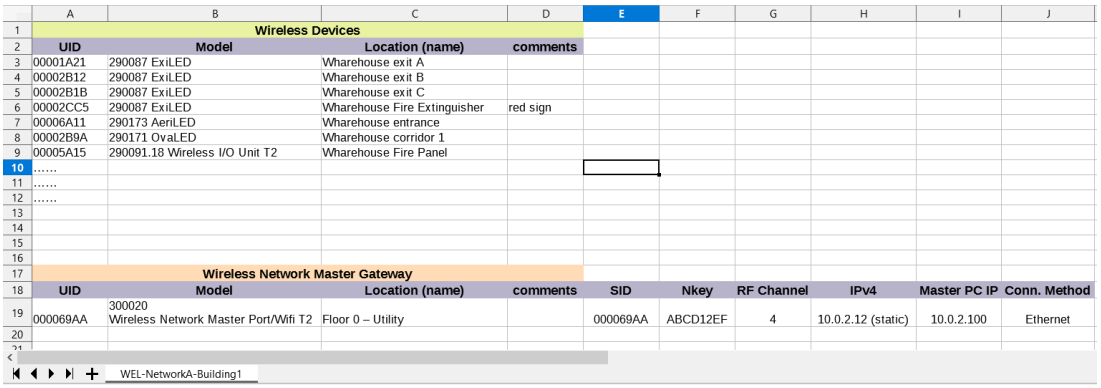
(viii) When the installation is completed, along with a detailed graphical installation plan, the networking of the wireless devices can commence, as described in chapter 3.1.6.4.

This document's layout contains chapters and sub-chapters that provide a detailed account of the software's installation and launch processes, a step-by-step course through the home page's functions and controls, and a detailed treatment of each of the menu items and their respective sub-items, in the above order.

Before starting

A very crucial step of the commissioning is to create proper documentation which describes every aspect of the wireless emergency lighting installation, in such a way that provides helpful information for later maintenance, replacements and troubleshooting in general.

For each individual wireless network; write network parameters (SID / NKEY / RF Channel), device location and models with matching UIDs, IP addresses for Gateways and Master PC, etc. An example is depicted below:



	A	B	C	D	E	F	G	H	I	J
1	**Wireless Devices**									
2	**UID**	**Model**	**Location (name)**	**comments**						
3	00001A21	290087 ExiLED	Wharehouse exit A							
4	00002B12	290087 ExiLED	Wharehouse exit B							
5	00002B1B	290087 ExiLED	Wharehouse exit C							
6	00002CC5	290087 ExiLED	Wharehouse Fire Extinguisher	red sign						
7	00006A11	290173 AeriLED	Wharehouse entrance							
8	00002B9A	290171 OvaLED	Wharehouse corridor 1							
9	00005A15	290091.18 Wireless I/O Unit T2	Wharehouse Fire Panel							
10	.....									
11	.....									
12	.....									
13										
14										
15										
16										
17	**Wireless Network Master Gateway**									
18	**UID**	**Model**	**Location (name)**	**comments**	**SID**	**Nkey**	**RF Channel**	**IPv4**	**Master PC IP**	**Conn. Method**
19	000069AA	300020 Wireless Network Master Port/Wifi T2	Floor 0 – Utility		000069AA	ABCD12EF	4	10.0.2.12 (static)	10.0.2.100	Ethernet
20										

WEL-NetworkA-Building1

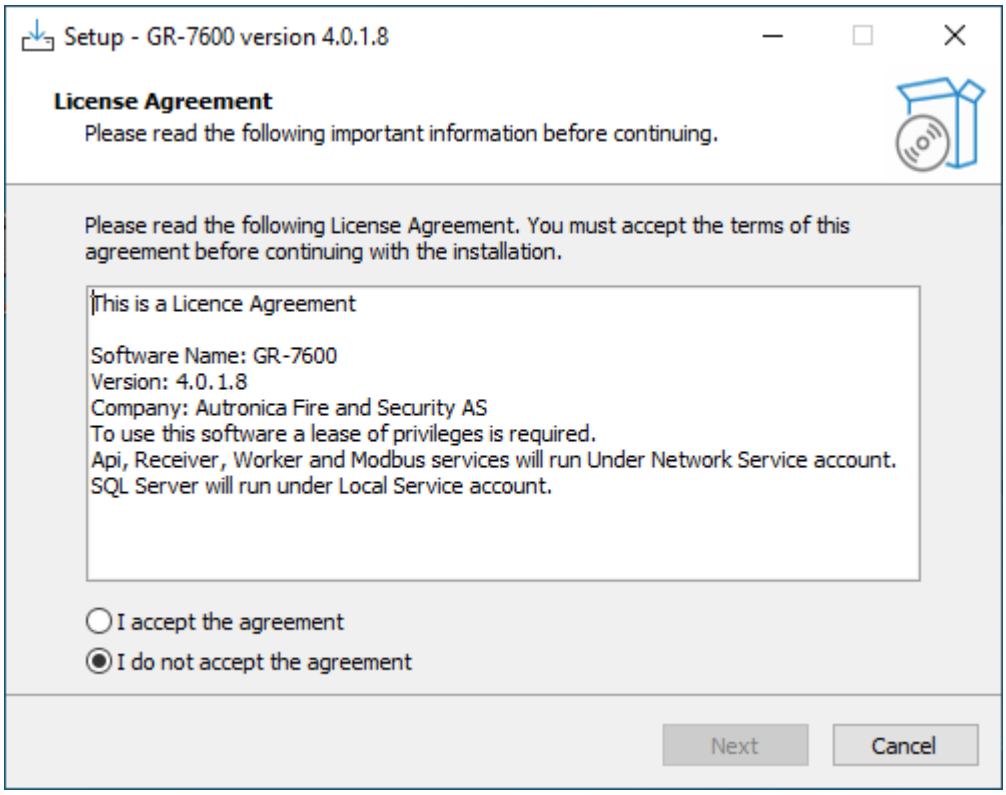
There is not any specific form for this spreadsheet document. You may write additional information or use a different formation, as long as the data are sufficient for later maintenance, inspection, or modifications.

For the IPv4 network parameters it is recommended to use the same subnet for Gateways and master PC. Consult an IT technician if needed. For the Gateway, the IPv4 can be set as static or DHCP. For the master PC that runs the “Autronica GR-7600/V2” application, the IPv4 always has to be static.

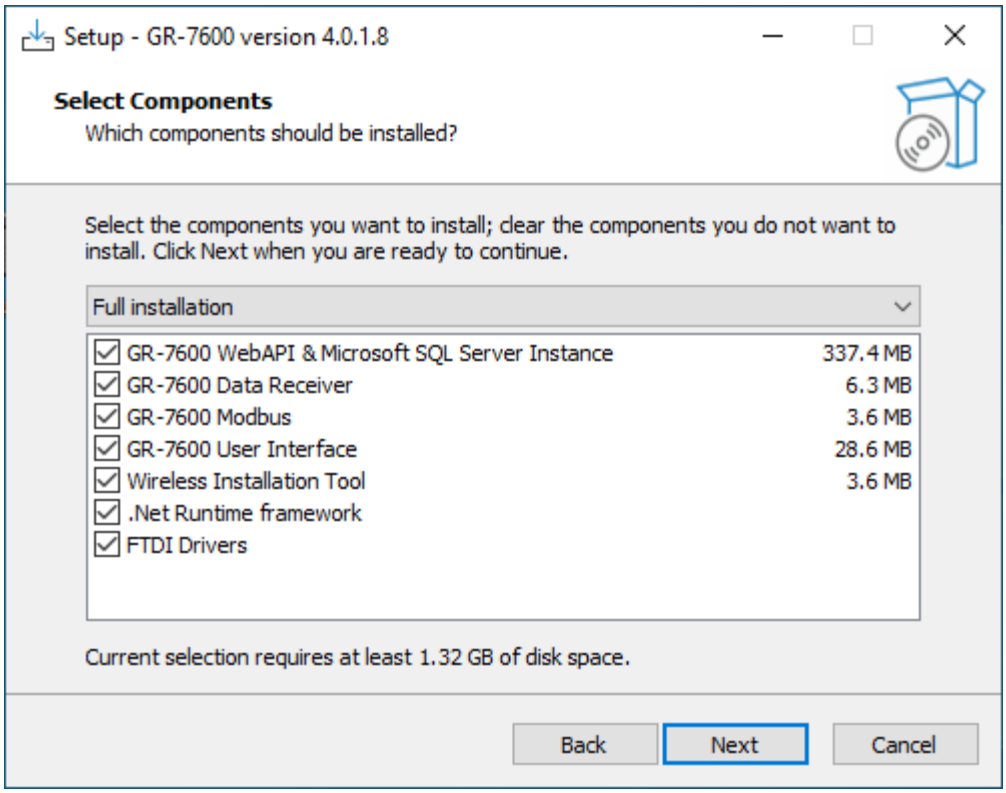
2. Software Installation

The installation process begins with the opening of the executable setup file.

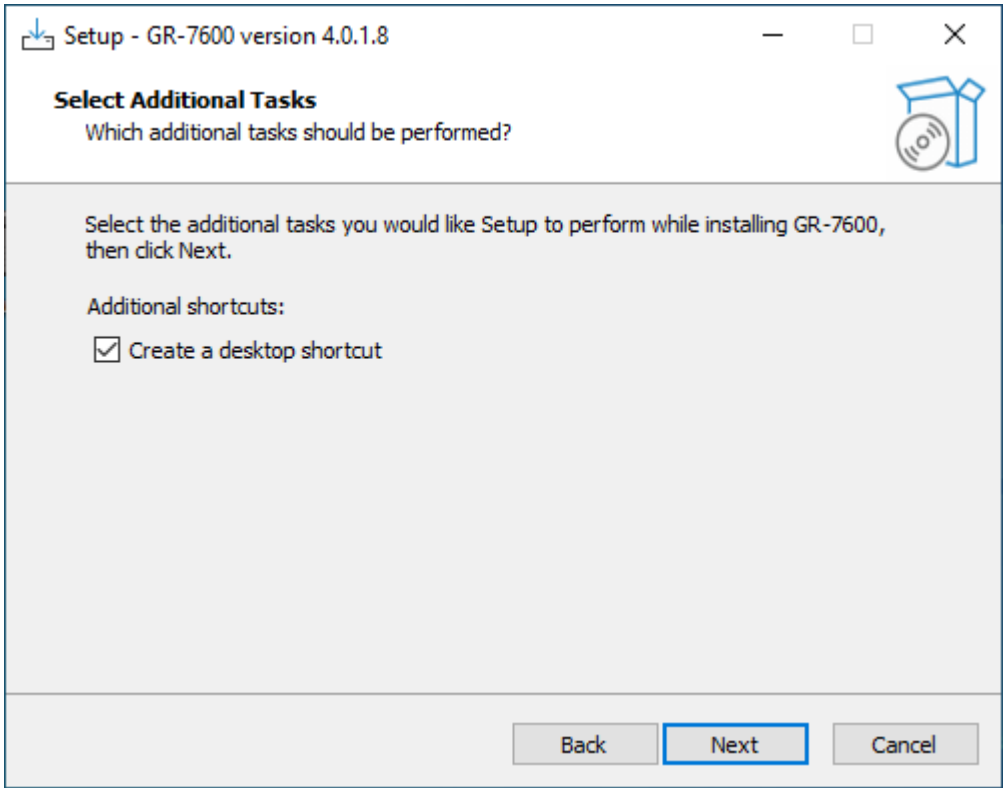
When the file runs, it initializes a common setup wizard that guides the user through the process.



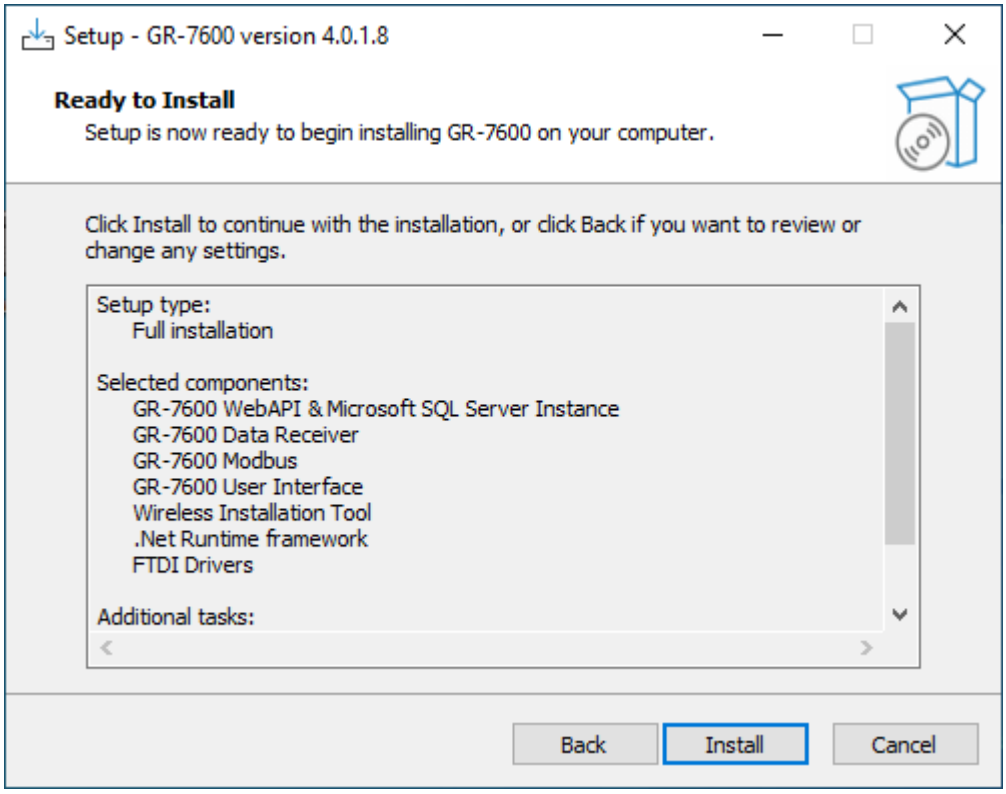
By clicking **Next**, the user will be prompted to select the components they wish to install. The default recommended option is the **Full installation**. All components are necessary for the software's complete functionality and first use. This package includes the SQL server for which the user will be required to create an account, all services that are needed to run the application, and the framework on which all components will operate.



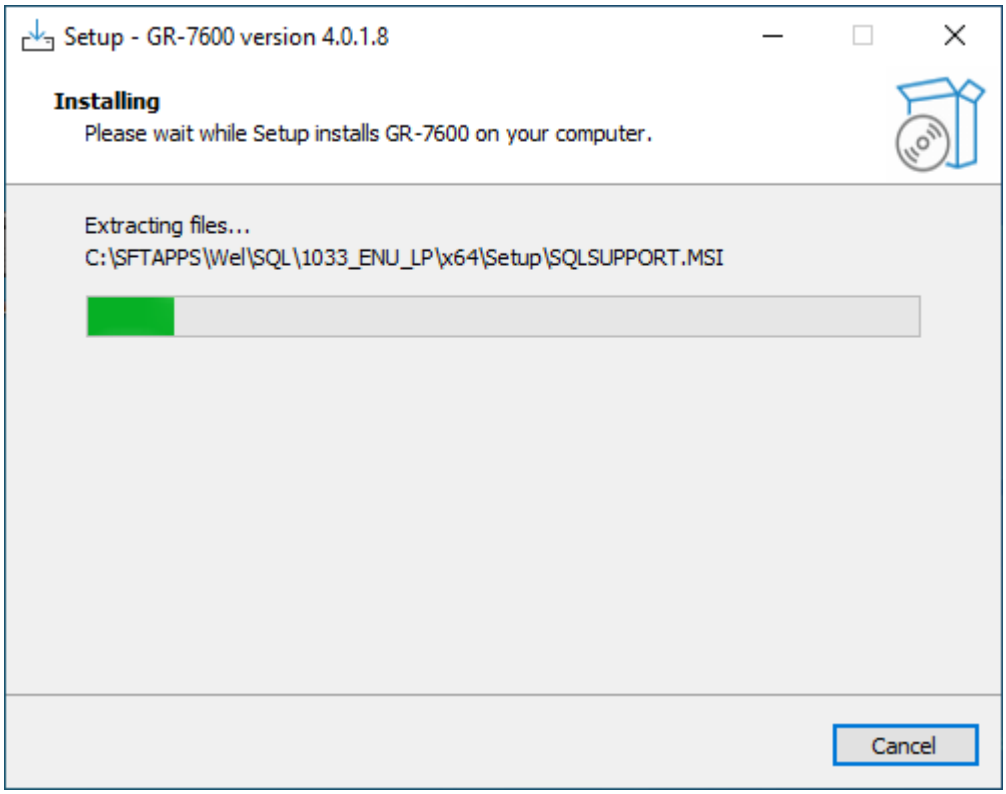
By clicking **Next**, the user will be given the option to create a desktop shortcut for the application.



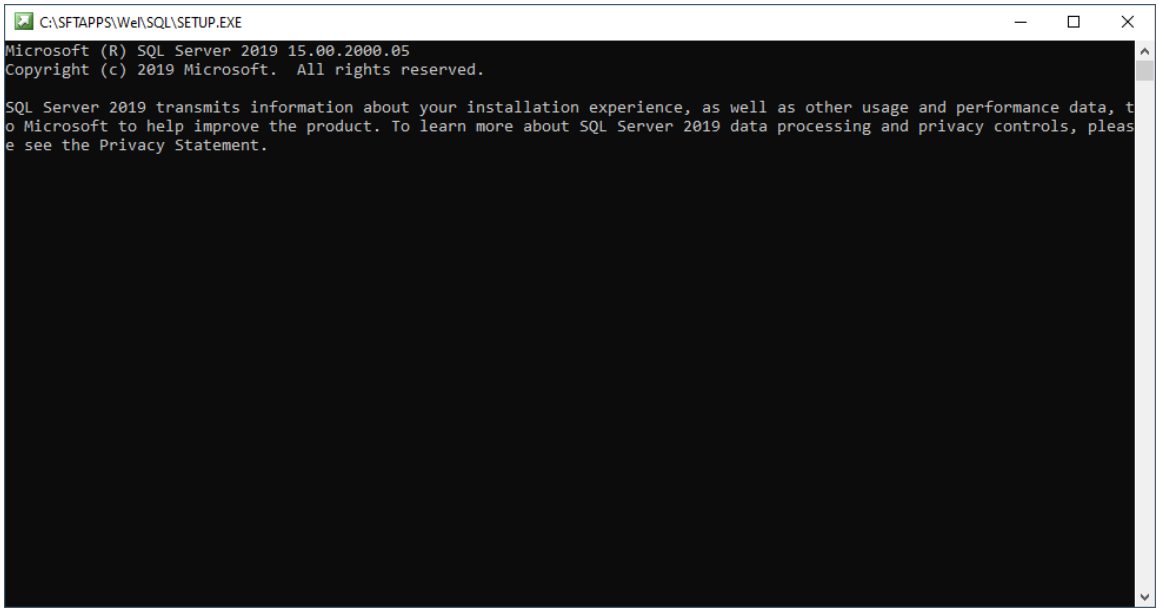
Next, the user can review their selections and begin the installation.

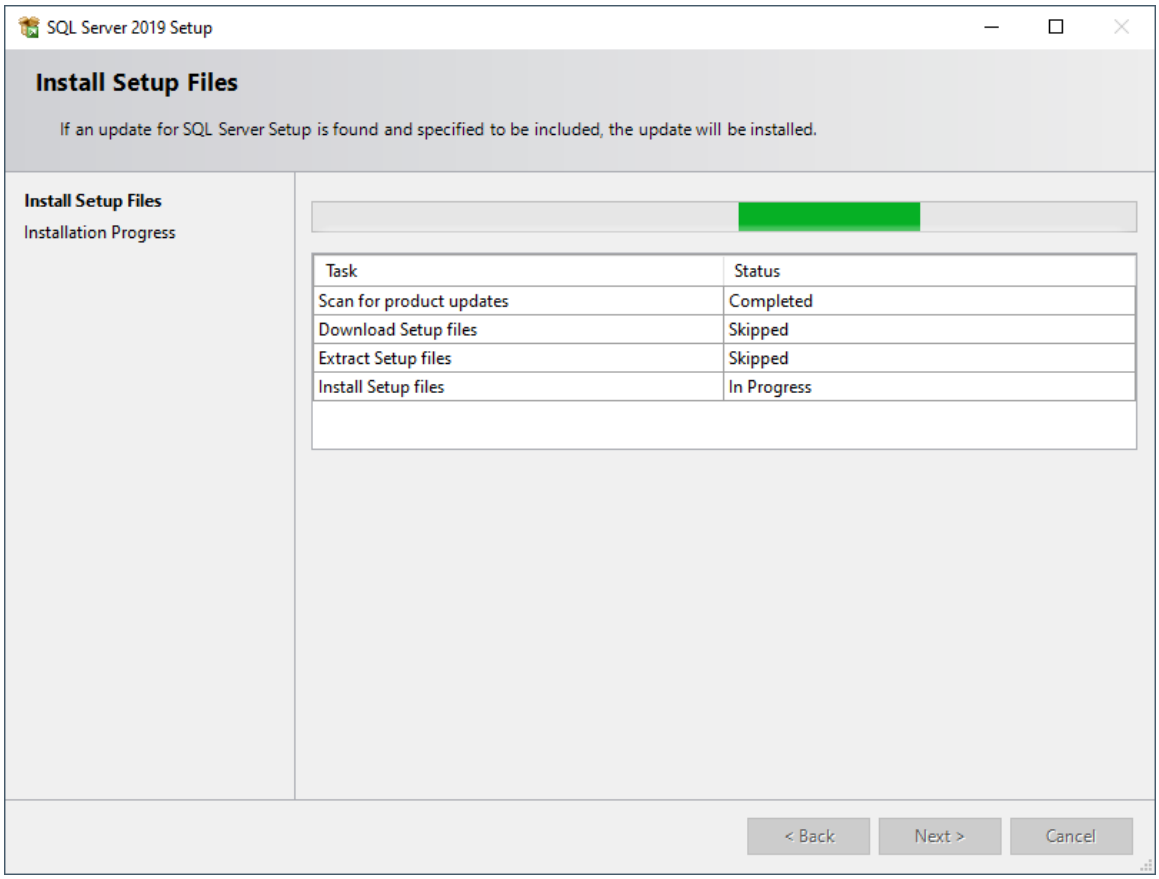


It should be noted that the process may last several minutes.

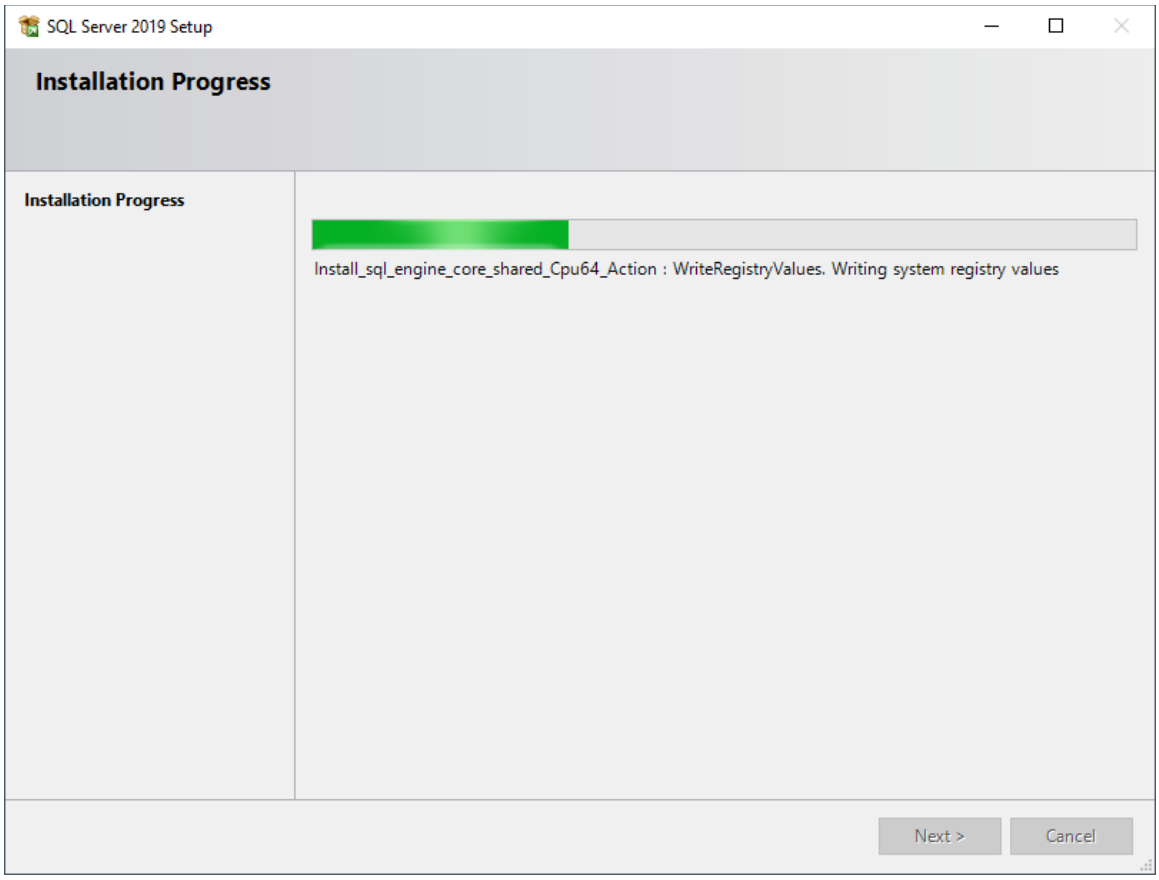


Before the process is completed, the following windows will open, preparing the computer for the SQL Server installation.

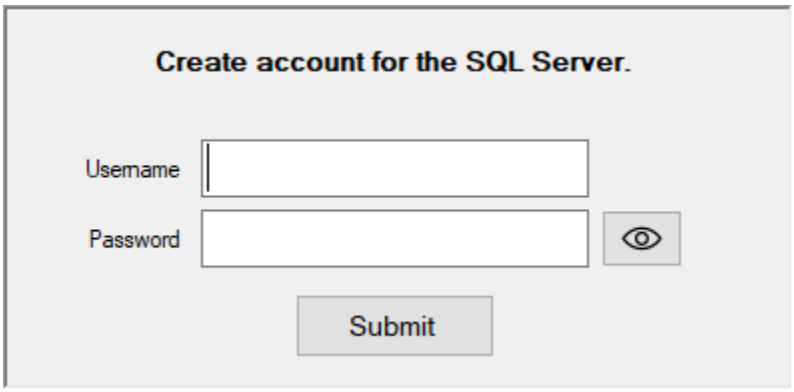




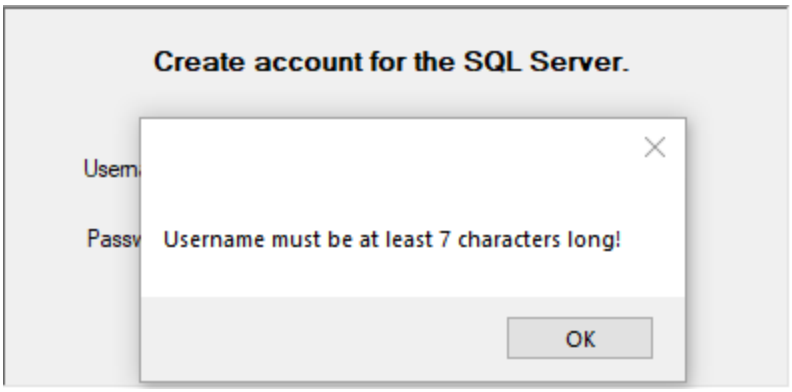
This procedure may last several minutes as well, depending on the specifications of the computer on which the software is being installed.

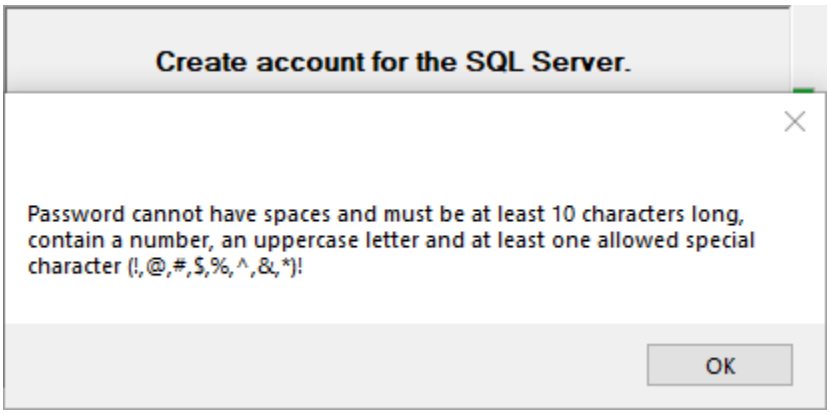


Once the SQL Server has finished its installation, the user will be prompted to create an account for the Server, registering their credentials. To this end, the following, validated form will appear.

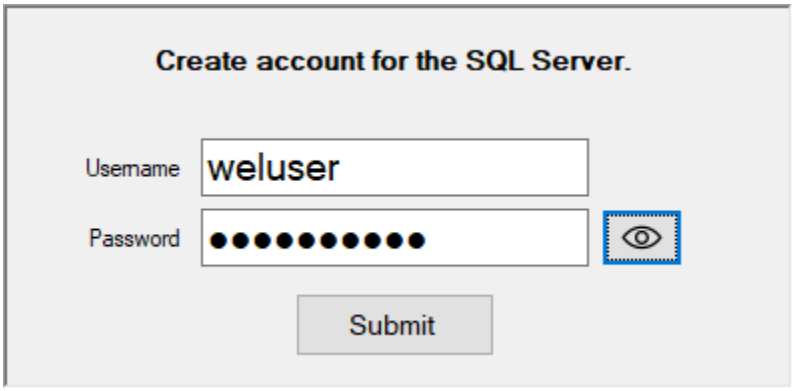


The validation includes a rule for the username, which is required to be at least 7 characters long and should not include any combination of the words ***admin*** and ***sa***. It also includes a rule for the password, which is required to be at least 10 characters long and should contain at least one number, one uppercase letter and one special character.

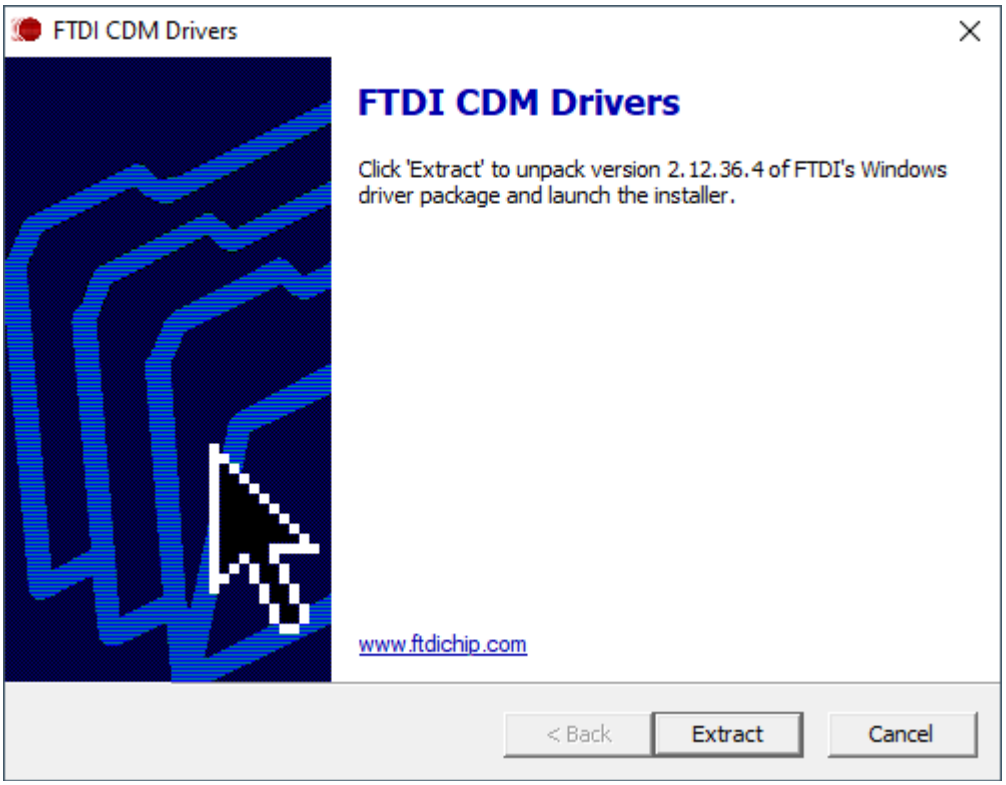


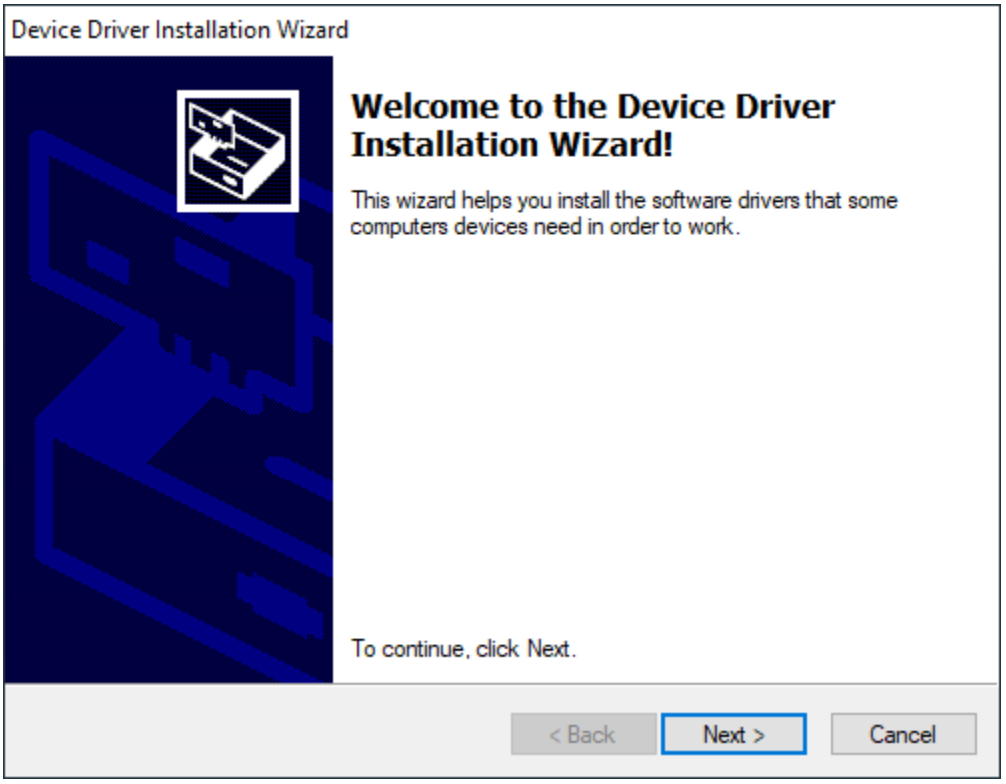


These rules prevent the user from registering a username that can in any way be confused with the *admin* user.

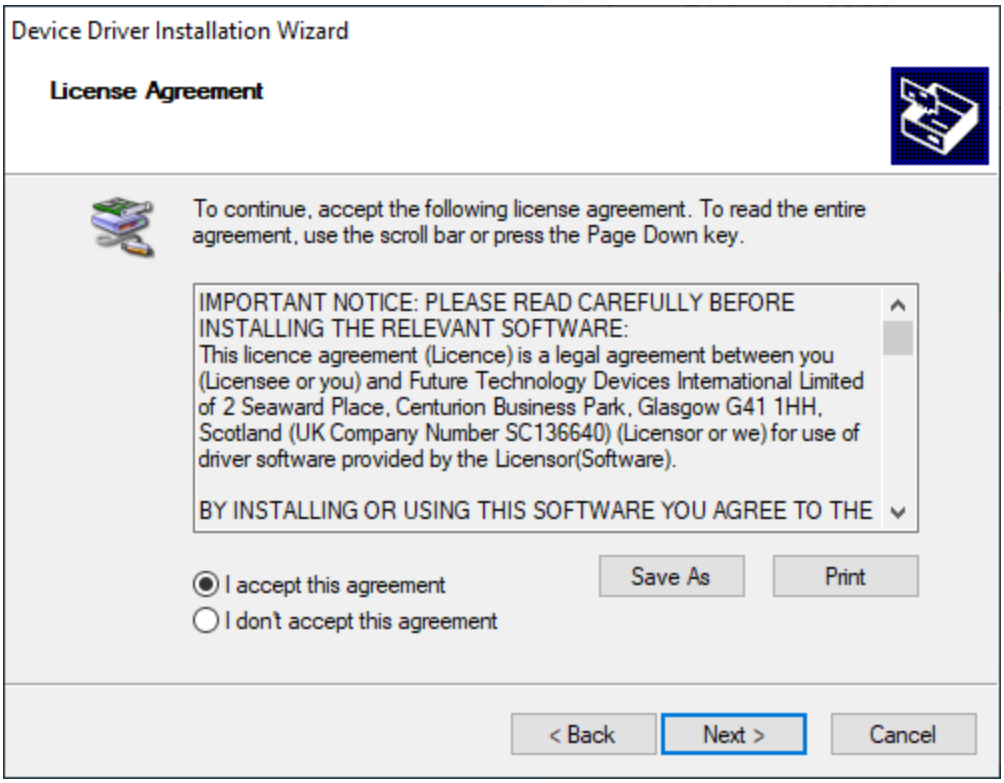


By submitting the process commences towards its last step, the extraction and installation of package of FTDI CDM drivers, generally responsible for USB communications. A new window will appear, prompting the user to extract the package and launch the drivers' installer.

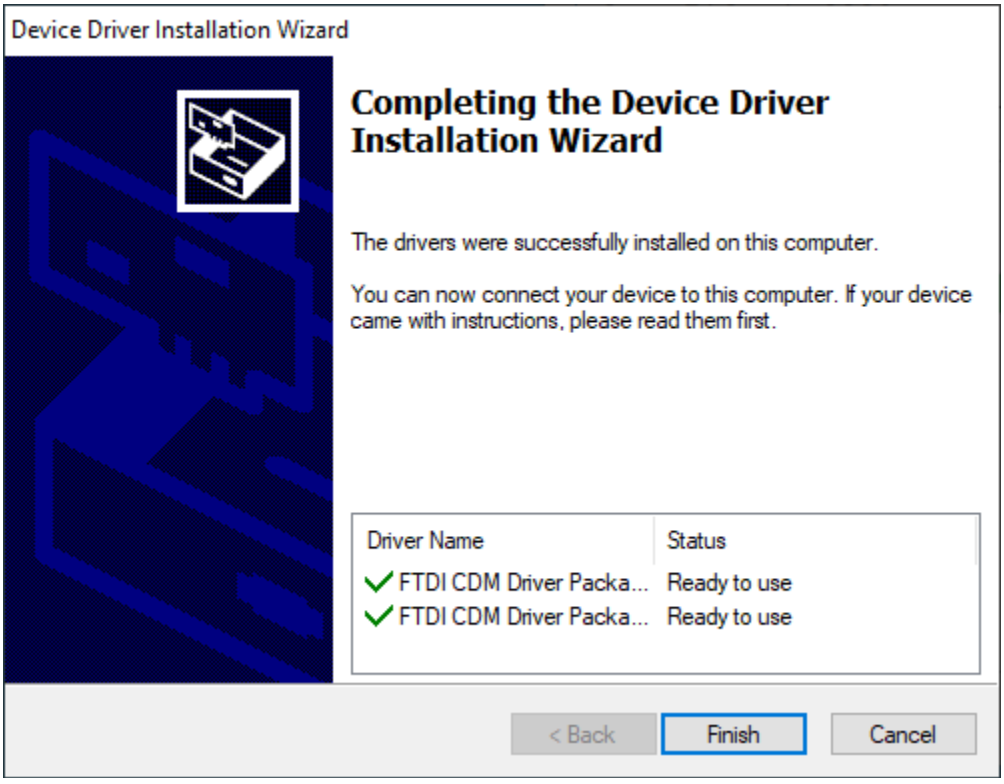




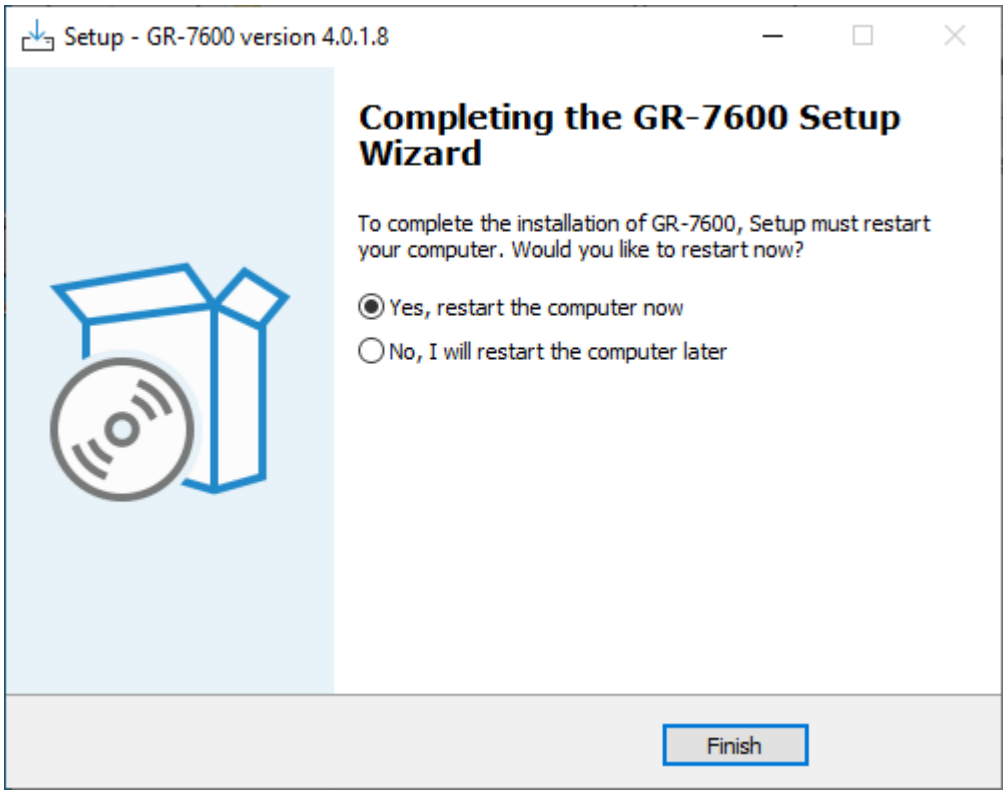
The user should select **Next** to continue and begin the installation.



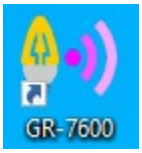
By accepting the terms of use, the package's drivers will finish their installation process.



By clicking on **Finish**, the initial wizard's window will appear informing the user that they successfully completed the software's setup process and is prompted to restart their computer. Restarting is the recommended option.

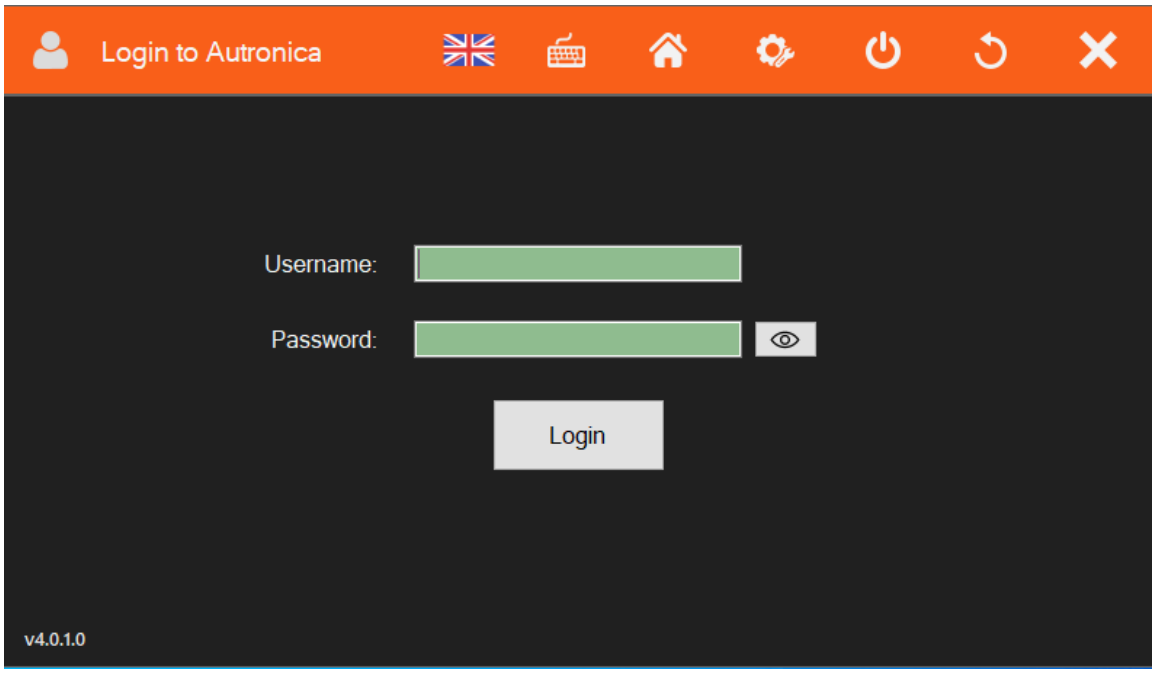


When the computer has been restarted, the following icon will have been created in the user's desktop, if they selected the creation of a shortcut earlier in the installation process.

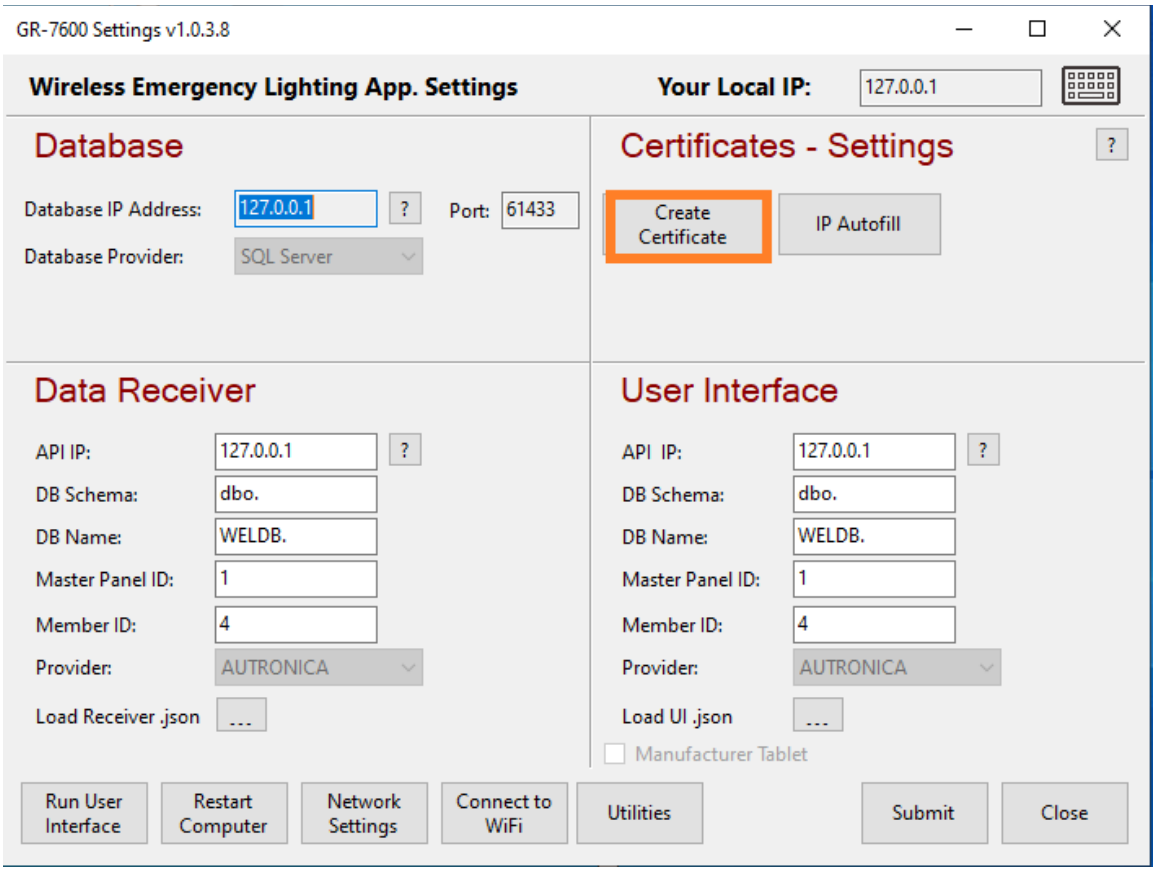


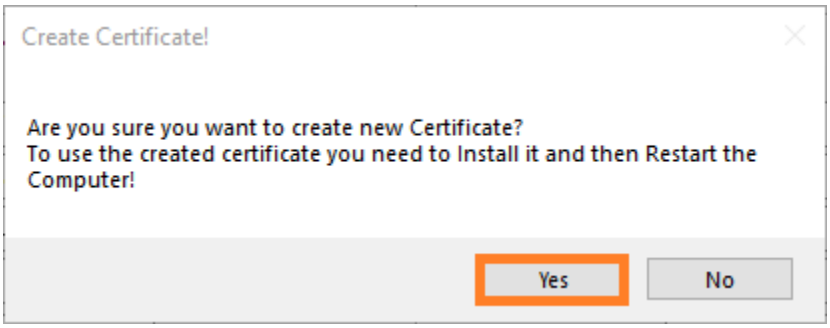
2.1. Launch

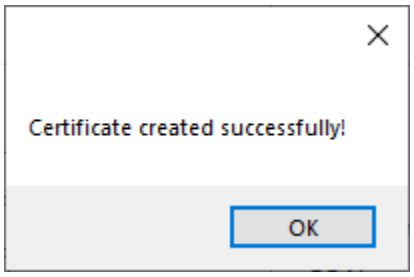
After selecting to run the application through the icon displayed above, the user will be presented with the following login form. Before the user is allowed to use the application and its functionality, a first-time procedure needs to be followed.



The user must proceed to the **Application Settings** option in the navigation bar at the top of the window to create α new certificate. In the settings window **Create Certificate** must be selected to proceed. The Local IP address must be the same as the API IP address, if it is not, click on IP Autofill and then Create Certificate.

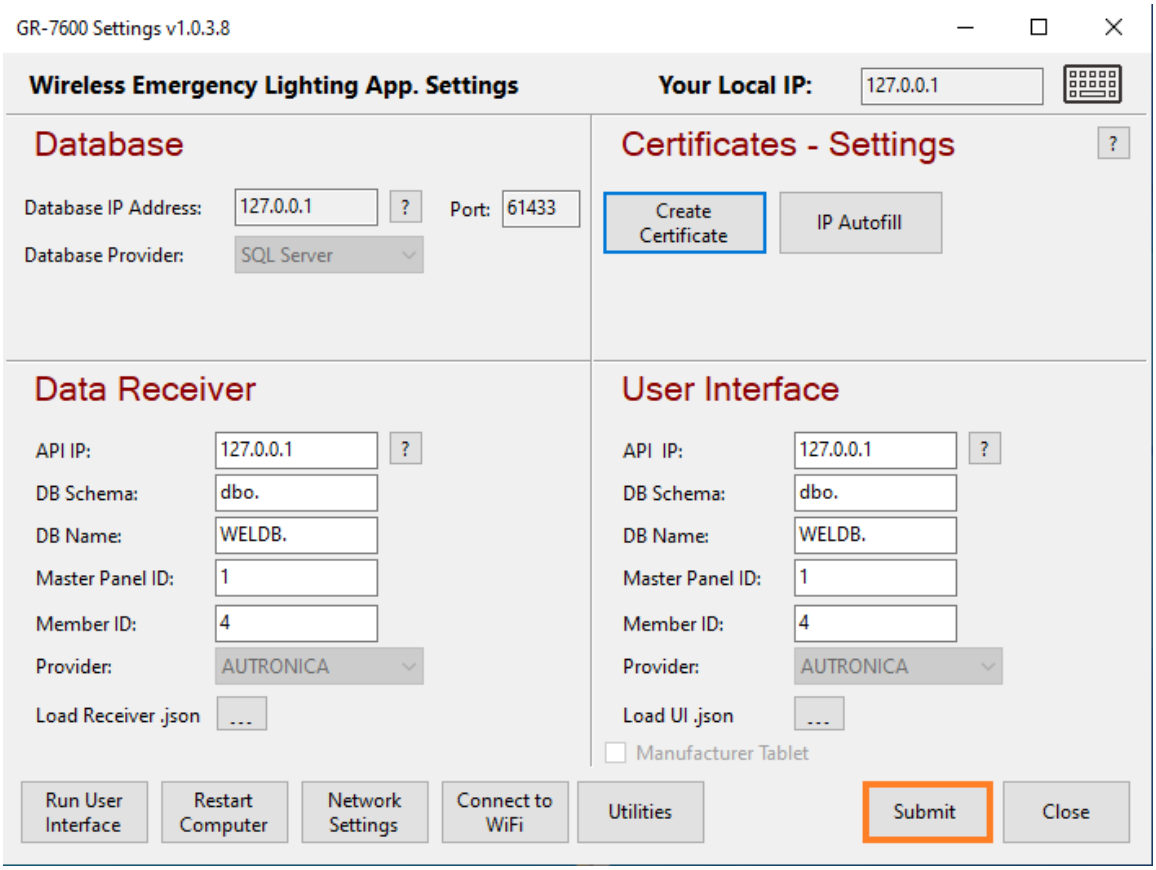


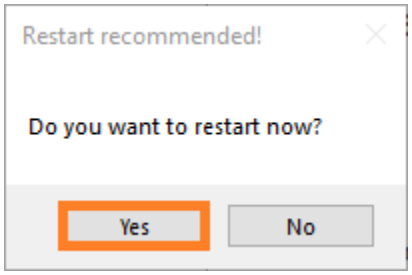




The user will then be directed to the application's settings window whereby clicking on **Submit** will complete the certificate process and also prompt them to

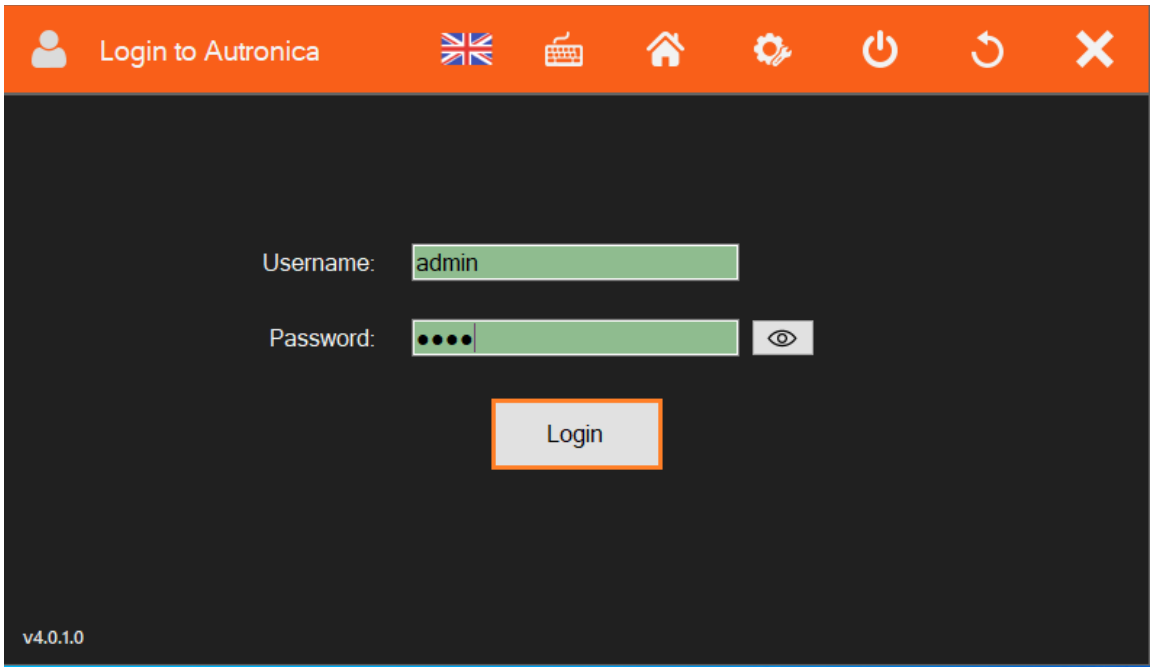
restart their system. A system restart is recommended in order for the certificate installation to successfully conclude.



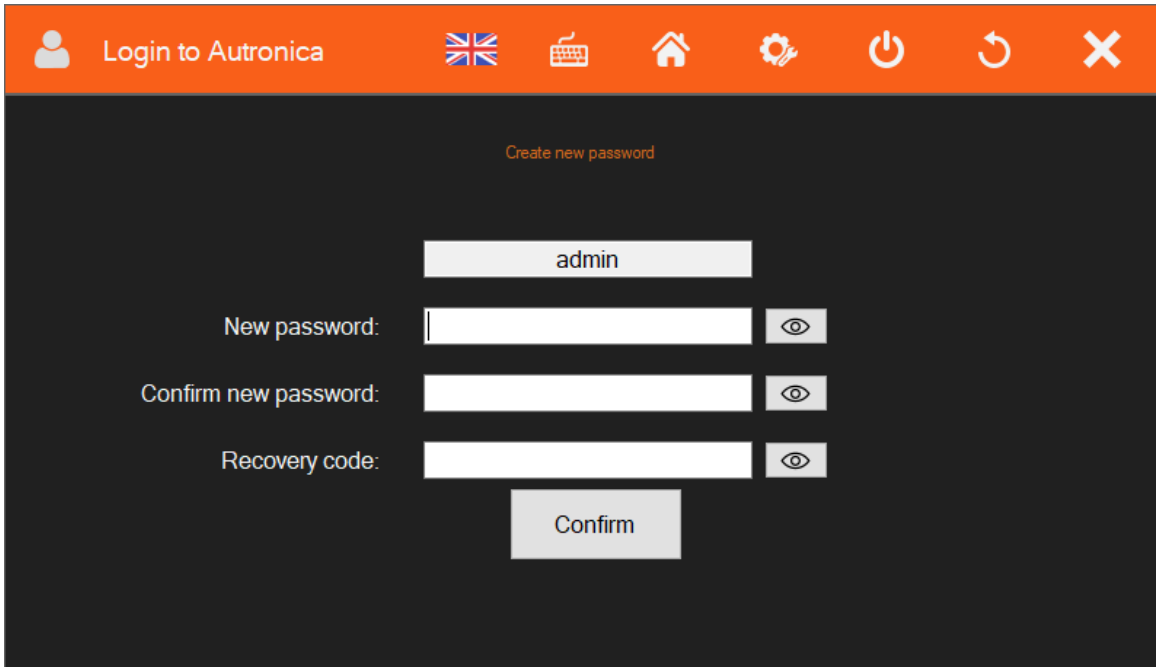


When the system is running again, the app can be run, similarly as before, by clicking on the following icon.

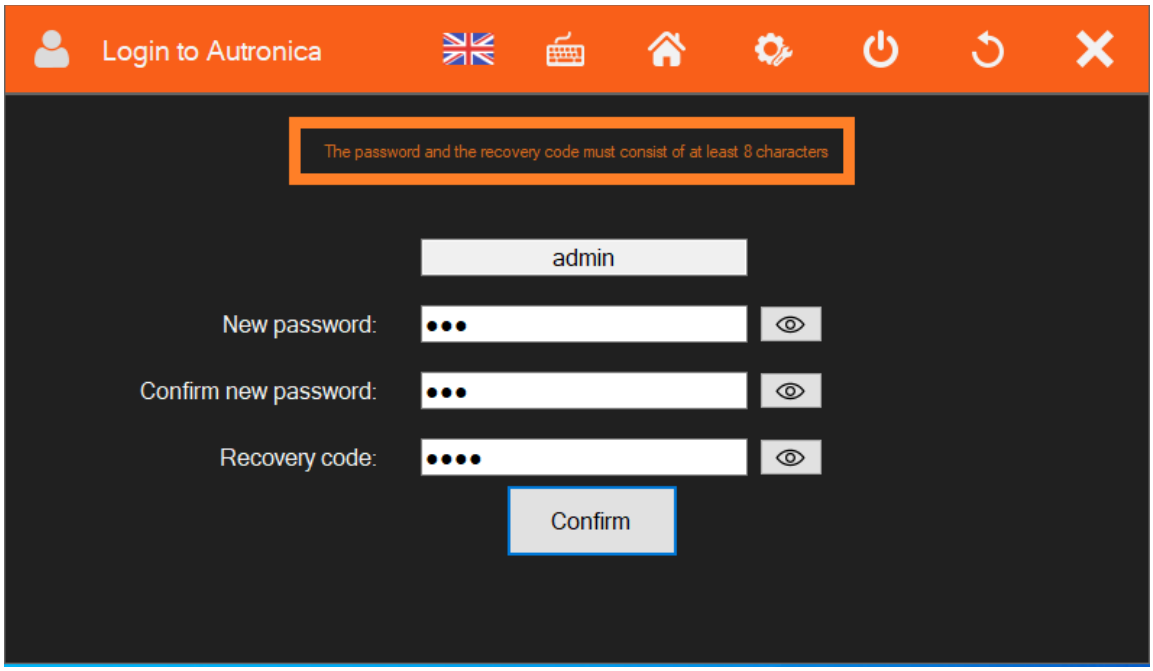
The sign in form will open a new within which the user may enter the following credentials to enable their first-time login; *username:* ***admin***, and *password:* ***1000***.

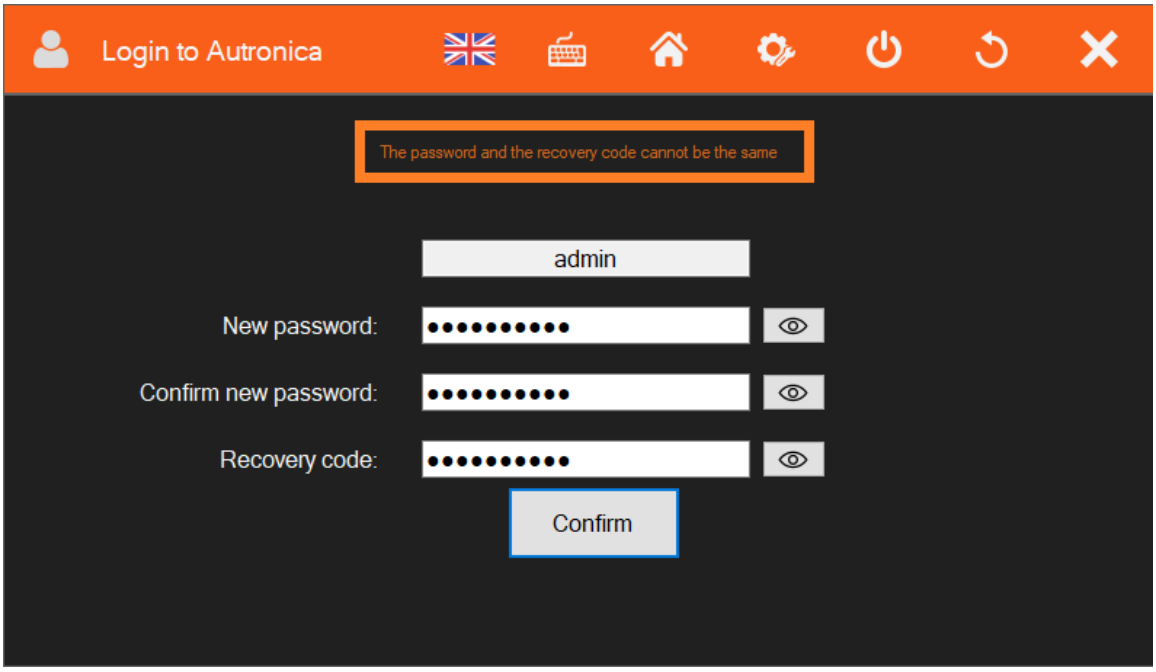


In the following screen the user is being asked to set up a new password and recovery code.

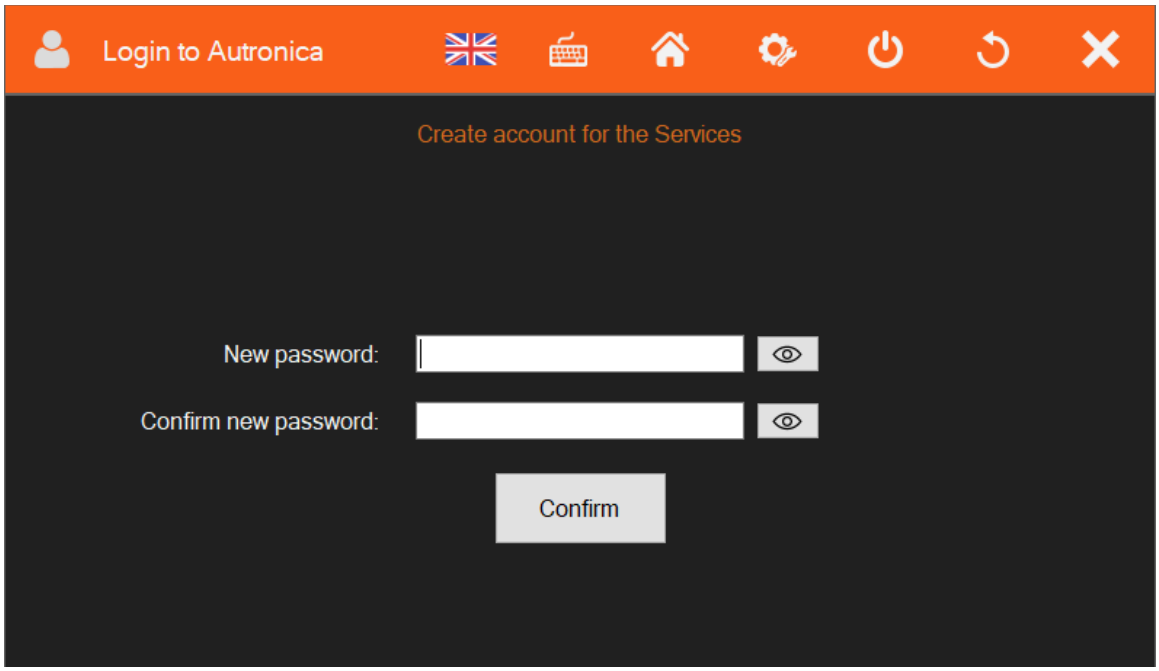


The preceding form is validated for correct input restricted by field related rules, which consist of the following: the password and recovery codes must be at least 8 characters long and they cannot share the same value.



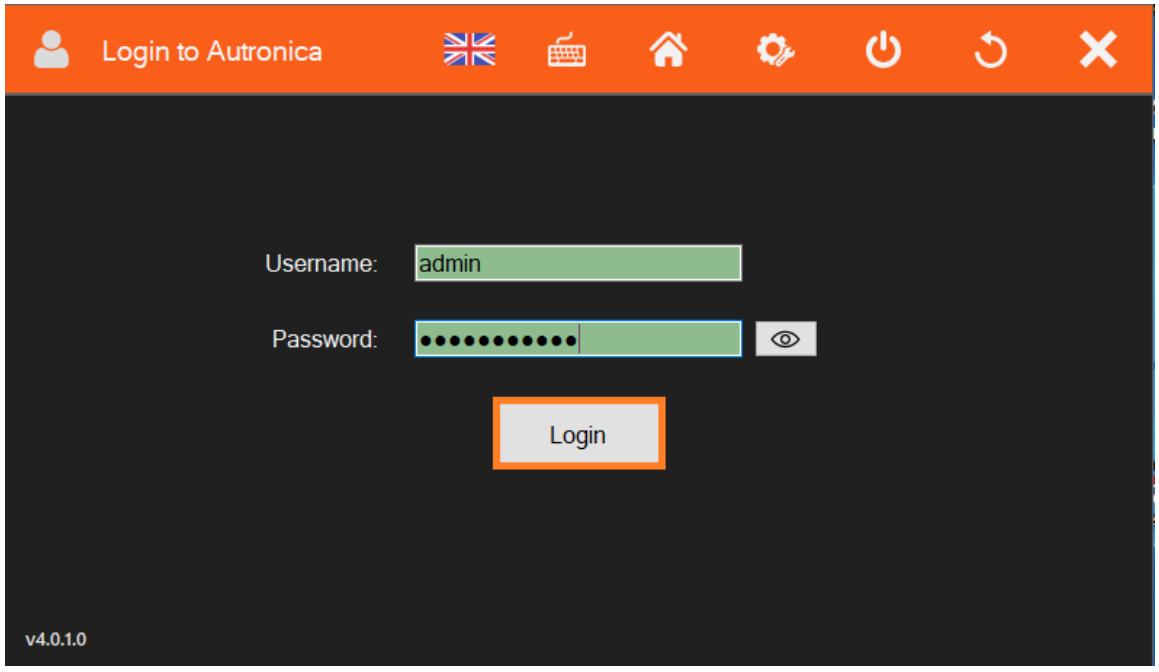


After successfully setting a new password and recovery code, the user will be asked to create an account for the software's services.



After a confirmation message, the user may finally sign into the application and start browsing and using its features.

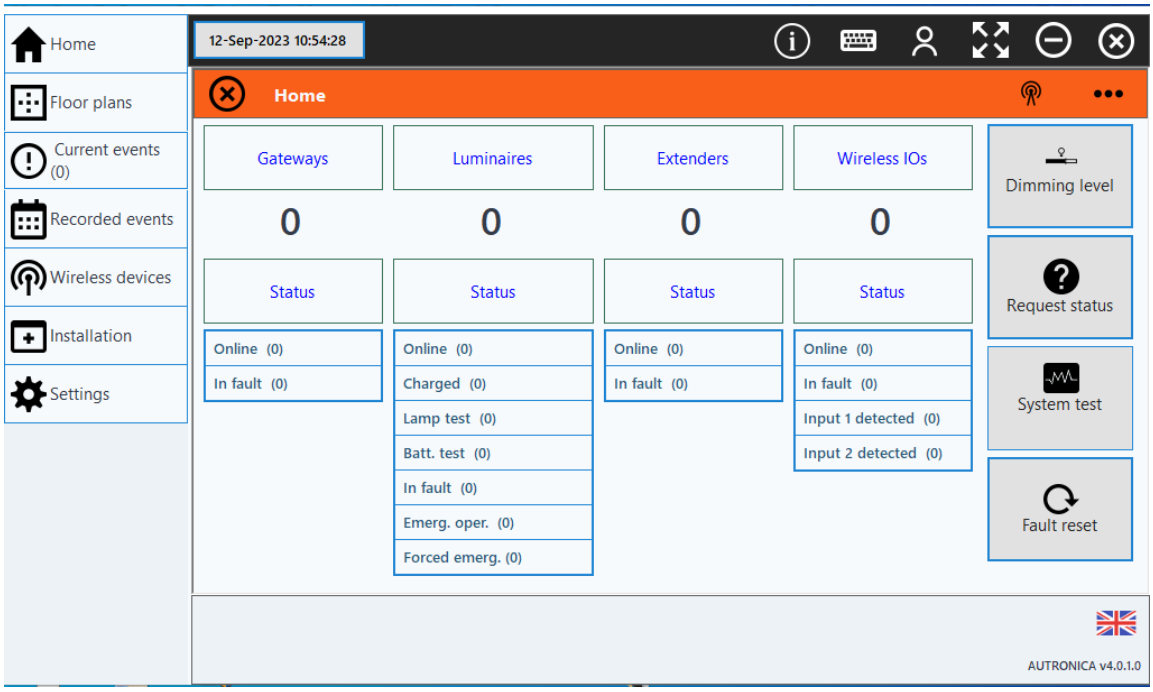
Notice!! Before completing all required actions the user is advised to safely store their credentials, locally.



A new interface that contains the **Emergency lighting system** application and a few controls will be shown. The following image highlights the basic elements that can be found within the new screen.

Within the navigation bar, two controls can be found. One that opens a window with additional information and another that enables the user to switch among several available languages.

Within the main window, there are a date and time, a display of the services for which the user created an account and their status. The main app is accessible through the button on the left (Emergency lighting system).

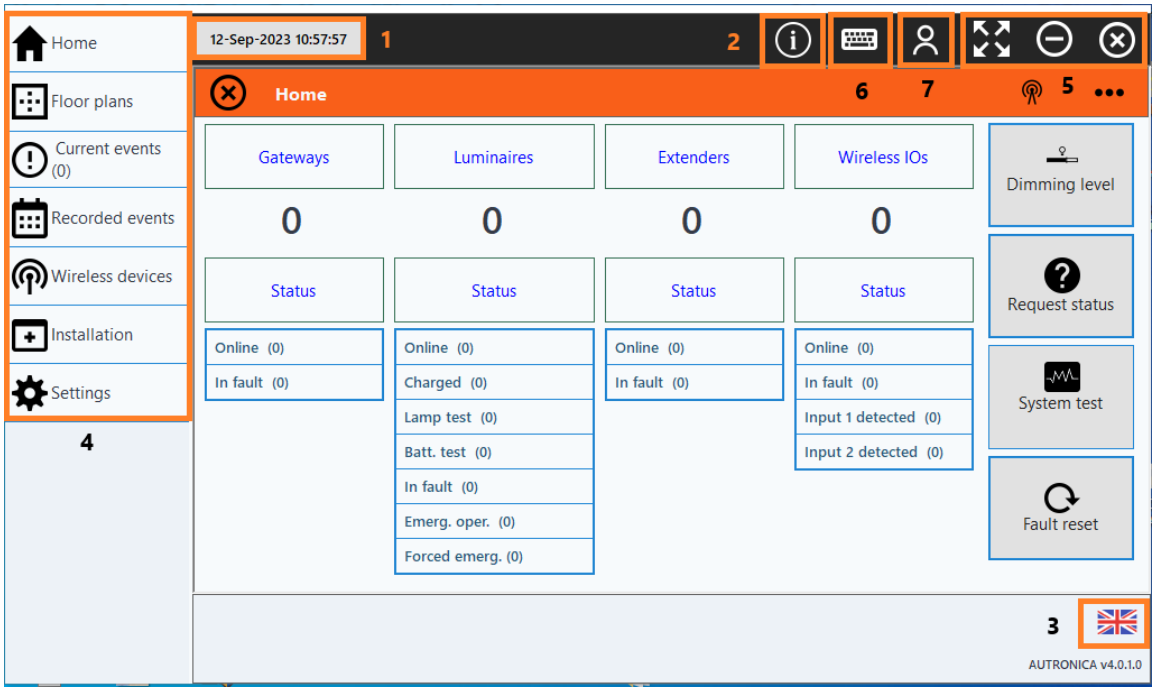


The above image shows the home screen the user initially sees, after successfully launching and signing into the app, and serves as the main fallback point for all available features.

This concludes the initial launch process. The following chapters will include details and instructions surrounding every element within the User Interface of the software, structured in the same order the menu items on the left appear, containing all necessary references to different parts of this manual as well.

3. Application

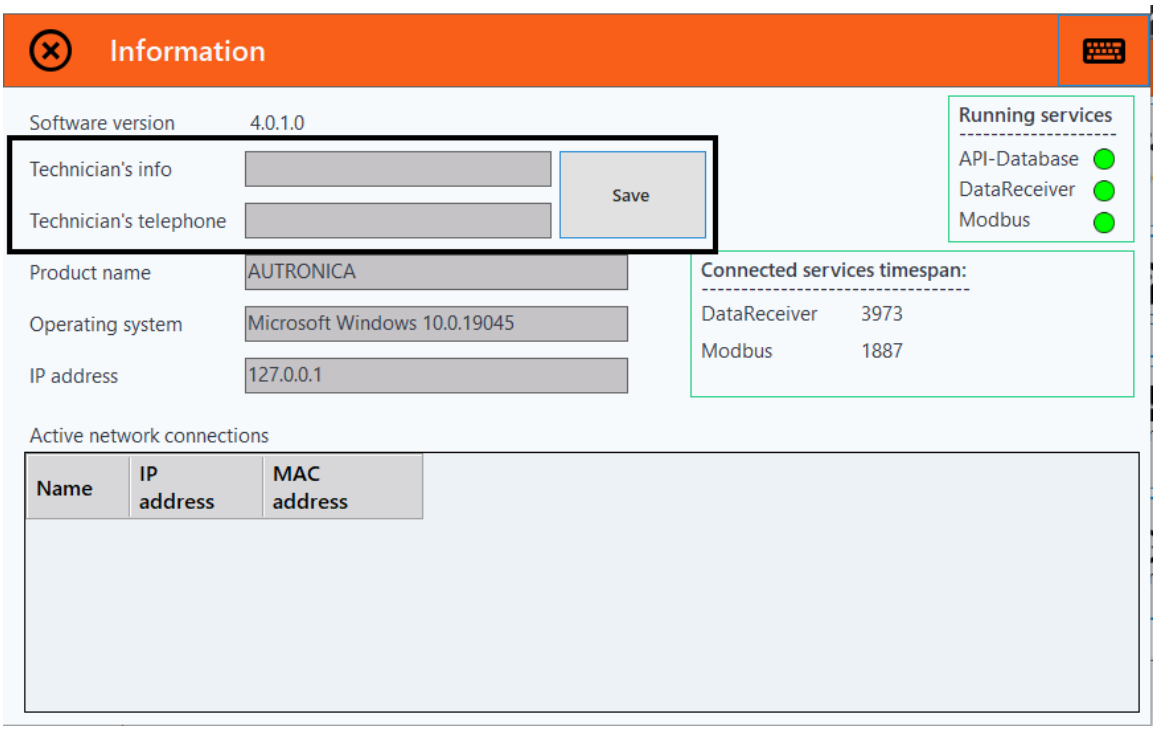
The chapter begins with a brief overview of all the elements within the app's main window. The main window is responsible for displaying all different screens that appear from the user's interaction with the interface. All major screens that in turn contain interactive elements of their own are displayed in the stead of where the Home screen appears in the following image.



There are 7 basic element the user can interact with. As shown in the above numbering: a date-time control, an additional information button, a control for language switching, a menu, a section with common window actions, a virtual keyboard, and a user drop-down menu.

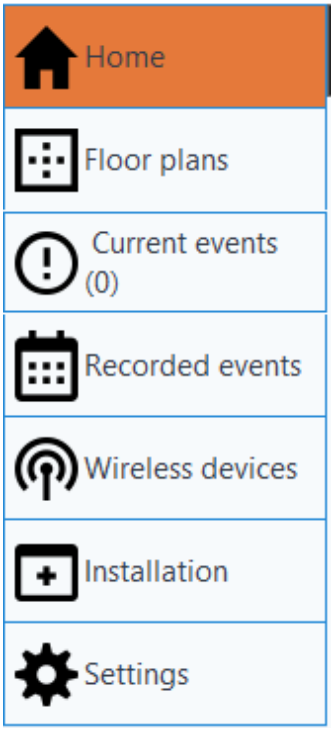
The date and time control **(1)** displays the date and the time of the system. To change the date and time go to Application settings>Utilities>Time settings or to your computer Settings.

The additional information button **(2)** displays certain software related information, while enabling the user to edit some of window's fields.



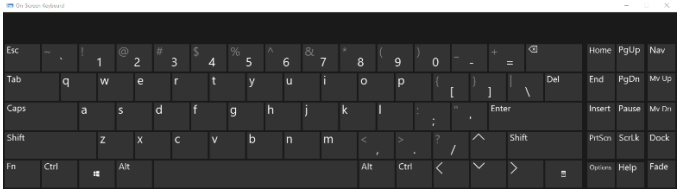
The language selection control **(3)** enables the user the change the language of the application to one of the available options.

The menu **(4)** allows the user to navigate all the different, available screens with their individual elements and sub-menus.

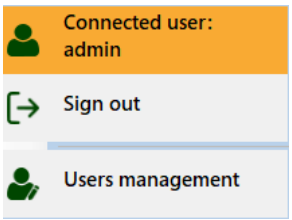


The window actions section **(5)** regards the three common options the user can encounter when handling a desktop window.

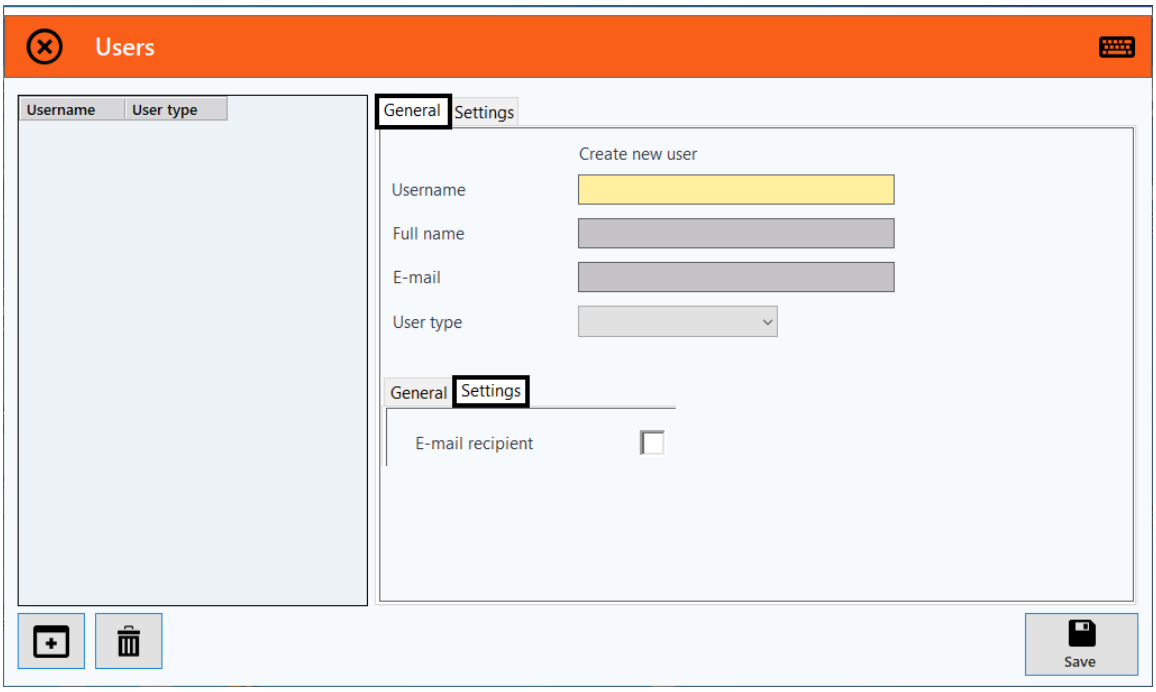
The virtual keyboard **(6)** opens a window that contains a virtual keyboard, in the case when there is no physical keyboard available.



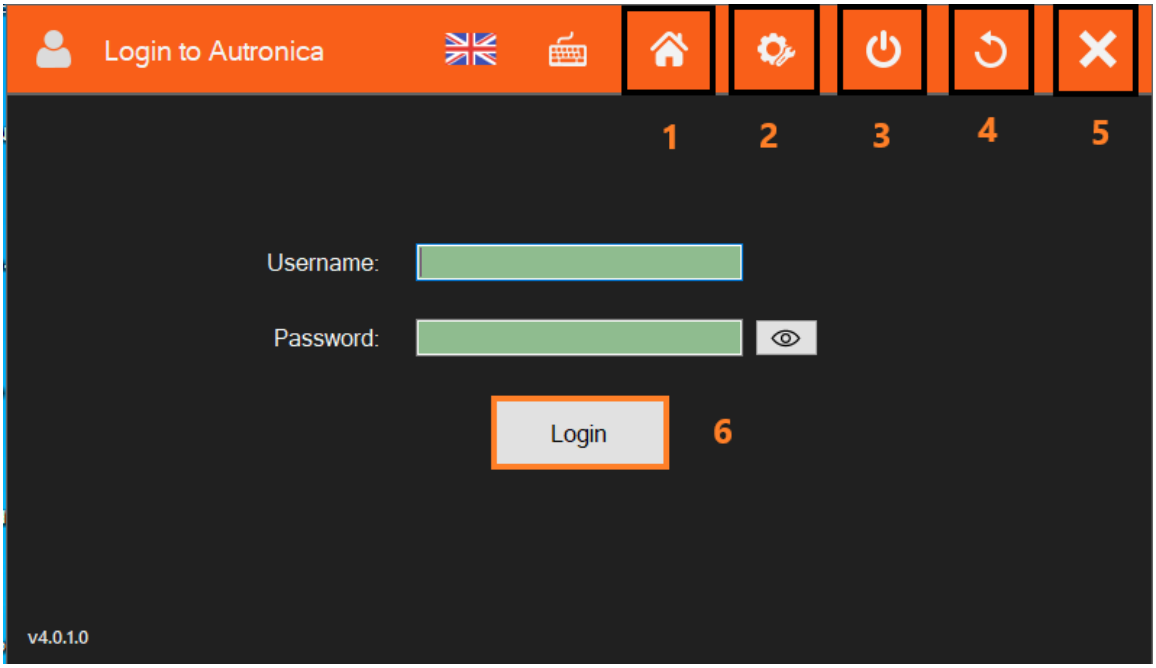
The user drop-down menu **(7)** includes the connected user's username, a sign-out option, and a user management control.



The user management option opens a new window that enables the administrator to add a new user, edit the information of existing users, or delete them. It should be noted that there are settings to edit in two different tabs.



After signing out, the user is redirected to the login form which contains the following basic elements: a home, a setting, a shutdown, a restart, a close and a login button. The user uses as username the name created for him by the administrator and for **first login password the 1000.**

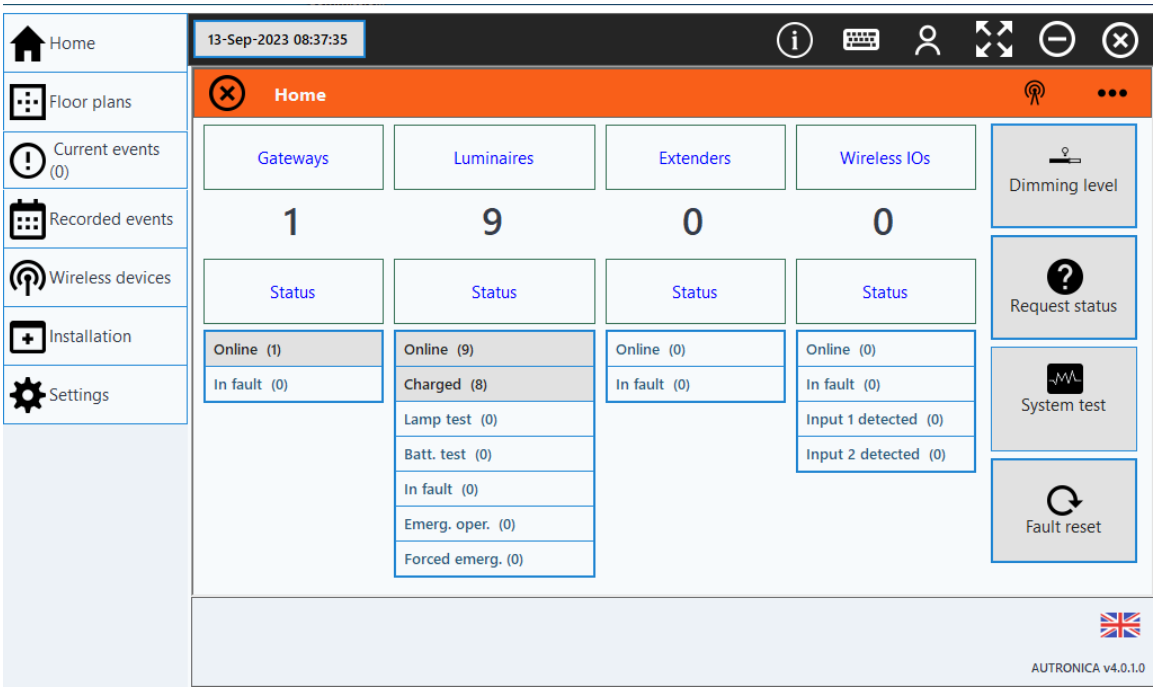


3.1. Menu

3.1.1. Home

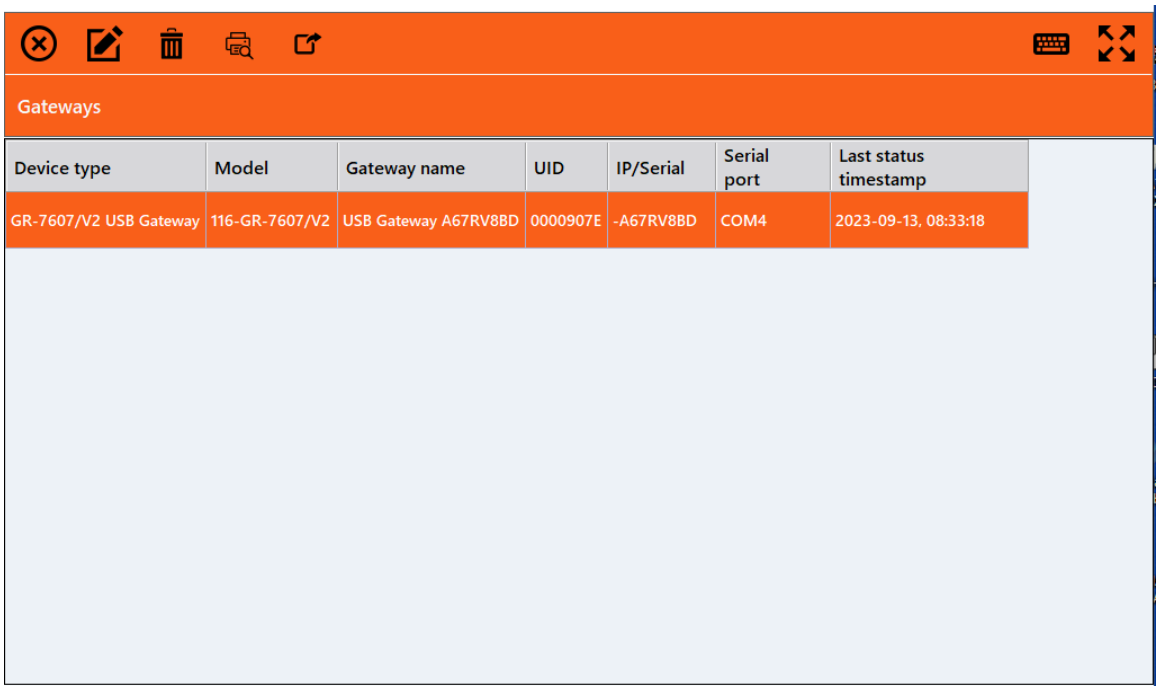
3.1.1.1. Gateways

The following image provides an overview of all elements of interest to the user. The screen is organized into two major sections; one displaying all of the connected devices, their quantity and various status attributes, and another displaying a short list of broadcast commands accompanied by a relevant button directly above and one button containing other, irrelevant options.



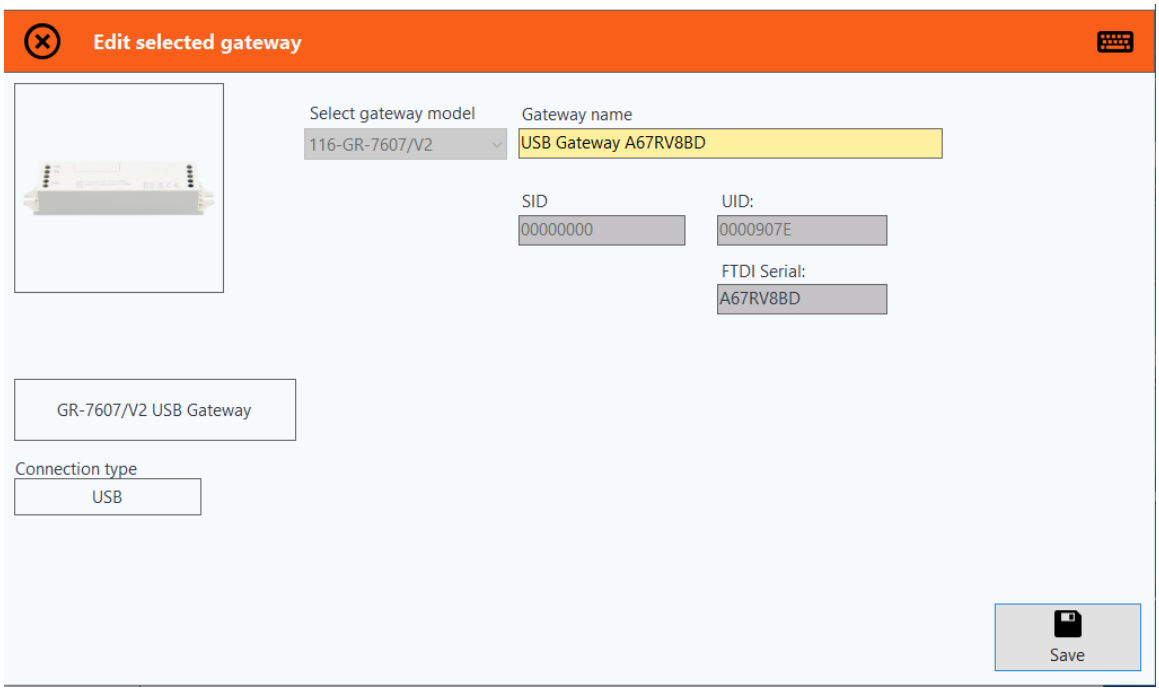
Further dissecting this screen, it can be organized into one column per different device. Starting from left to right, there are gateways, luminaires, extenders, and wireless IO devices.

Clicking on the Gateways field produces the following image.

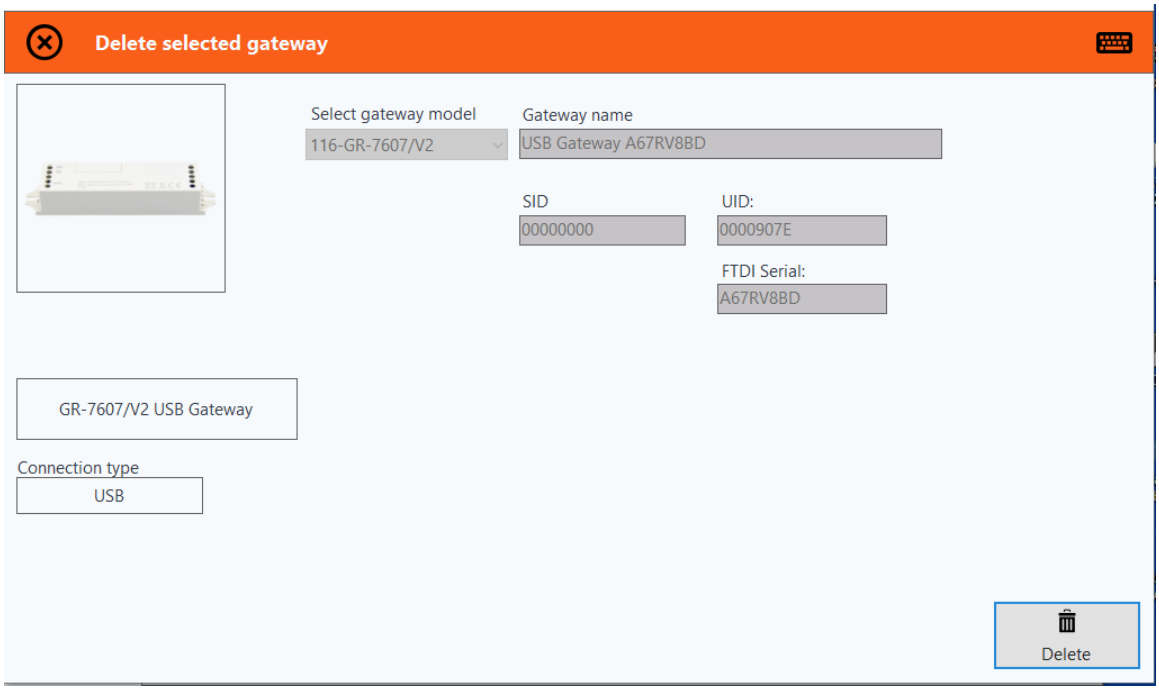


This screen includes the options to edit or delete a device, print the table, or export its contents locally to a file. It is notable that each similar screen includes options for printing and exporting. Furthermore, all descriptions of such screens will be given starting with the leftmost option.

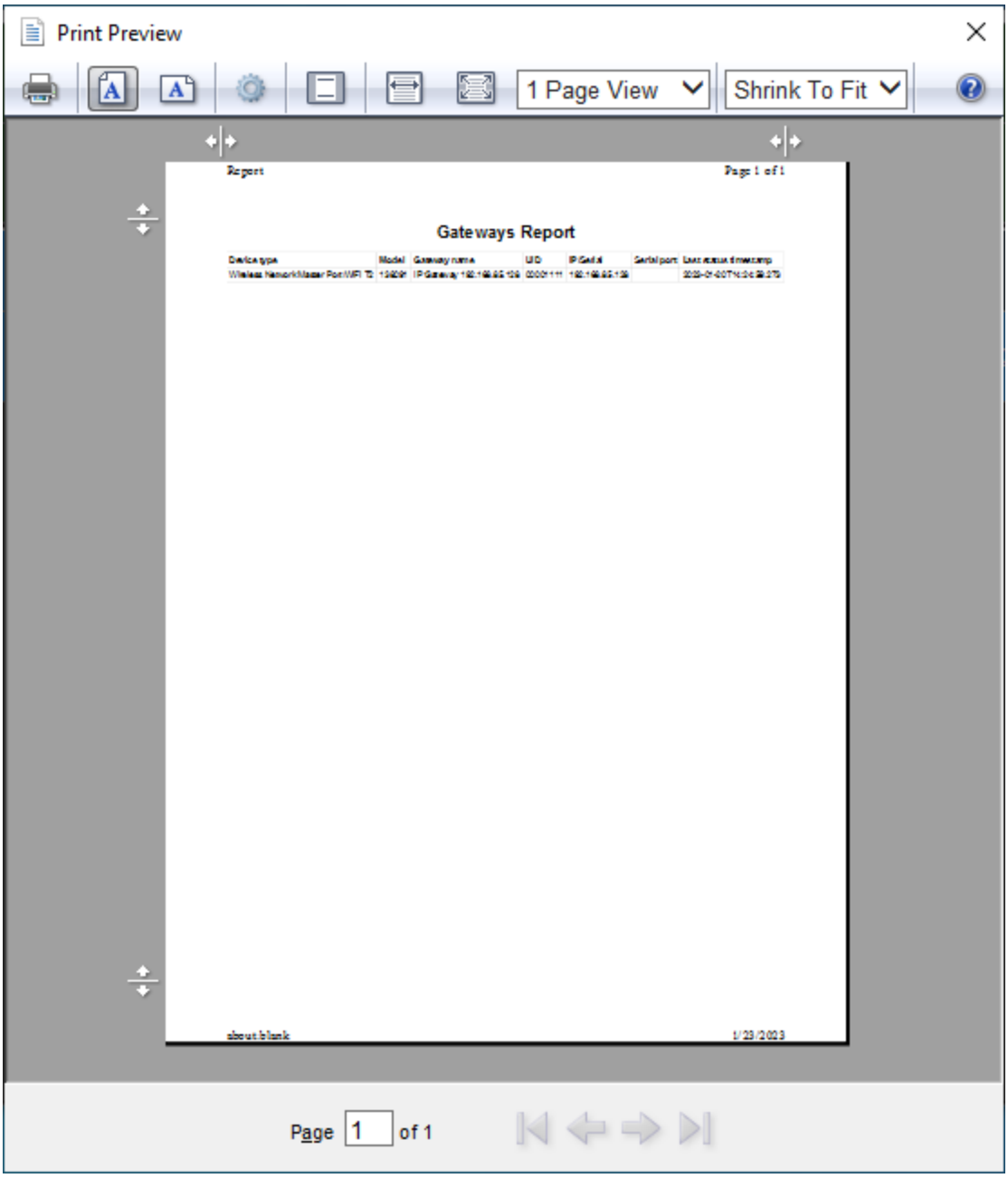
The following screen enables the user to edit the selected gateway.



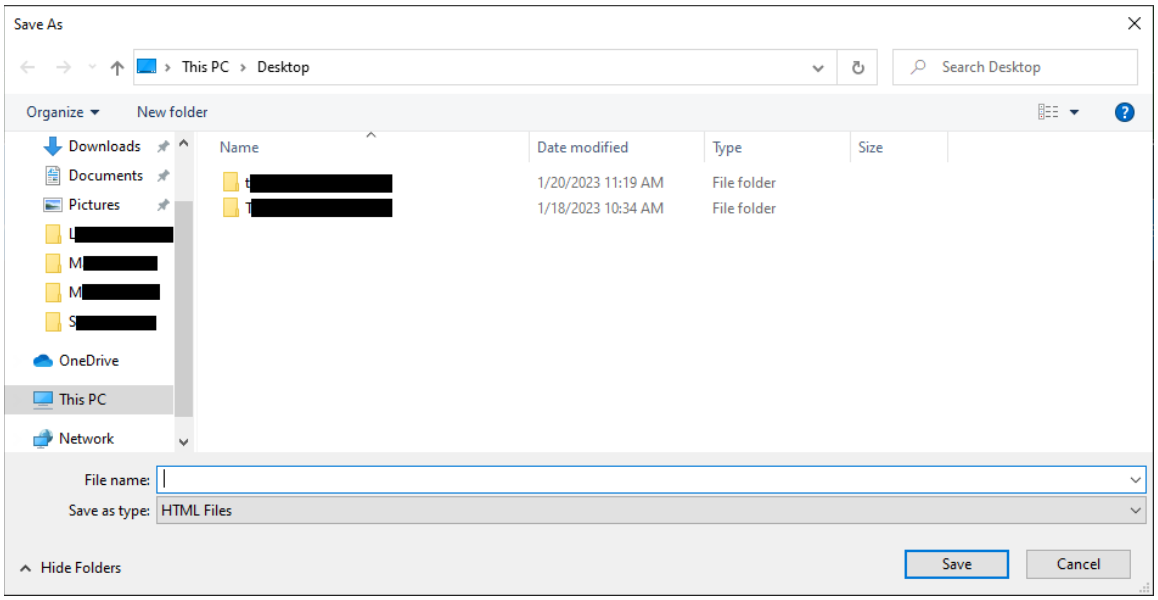
The following screen enables the user to delete the selected gateway.



The print preview option provides the user with an overview of the printable report.

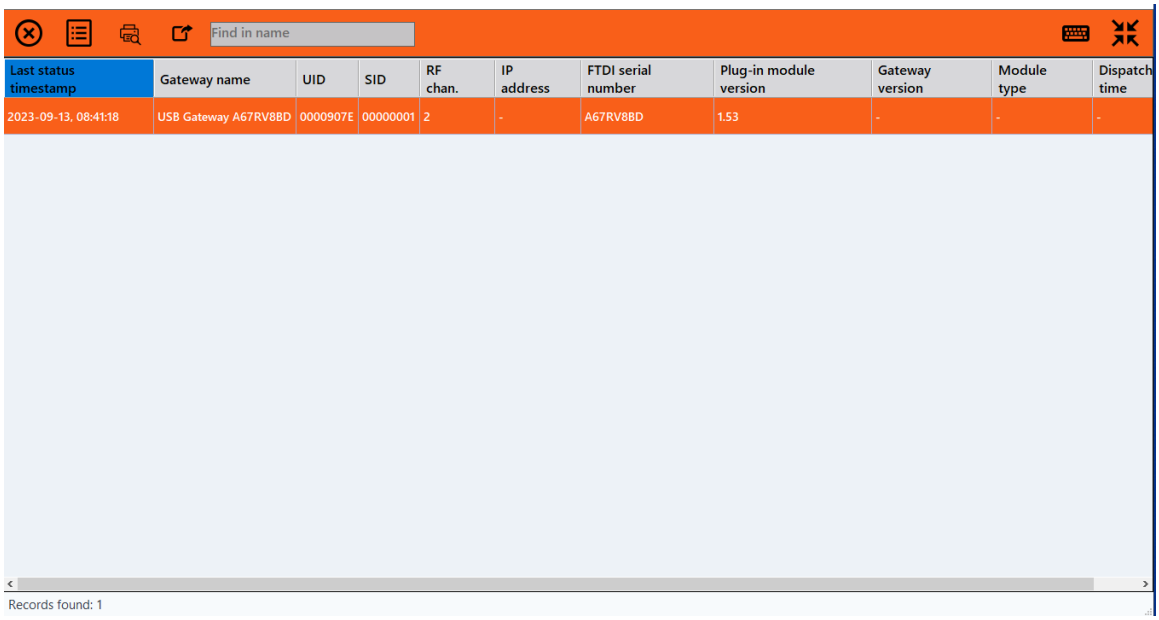

Print Preview
1 Page View
Shrink To Fit
Report
Page 1 of 1
Gateways Report
about:blank
1/23/2023
Page 1 of 1

The event export option enables the user to export the contents of the table to a file.

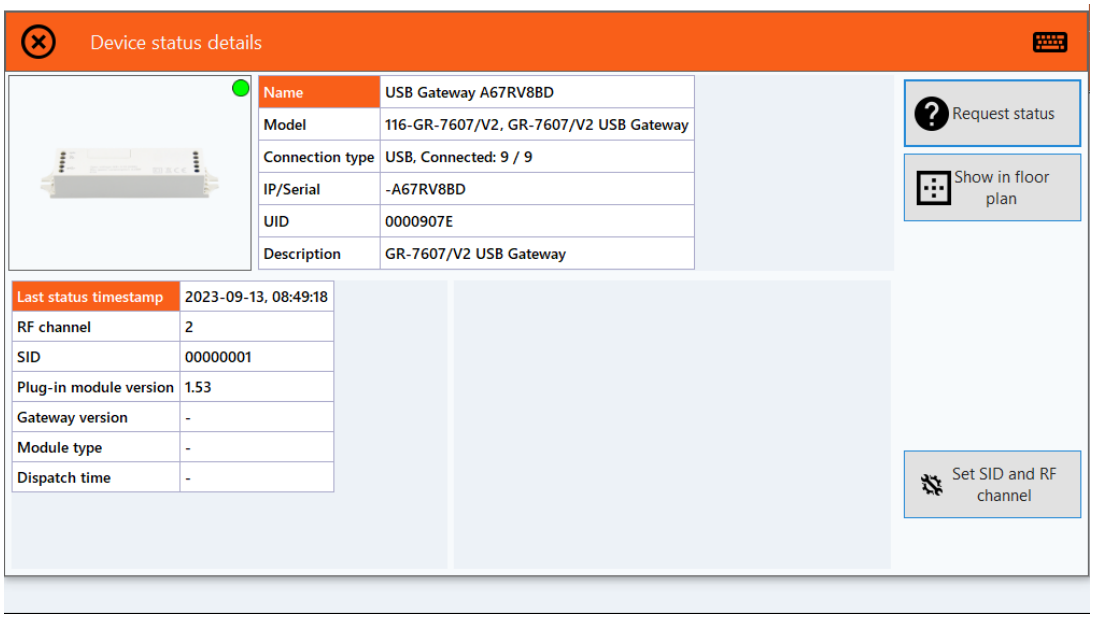


Double-clicking on a device will redirect the user to a window with details about the status of the device, which is a screen that is accessible in more than one way and will be described shortly.

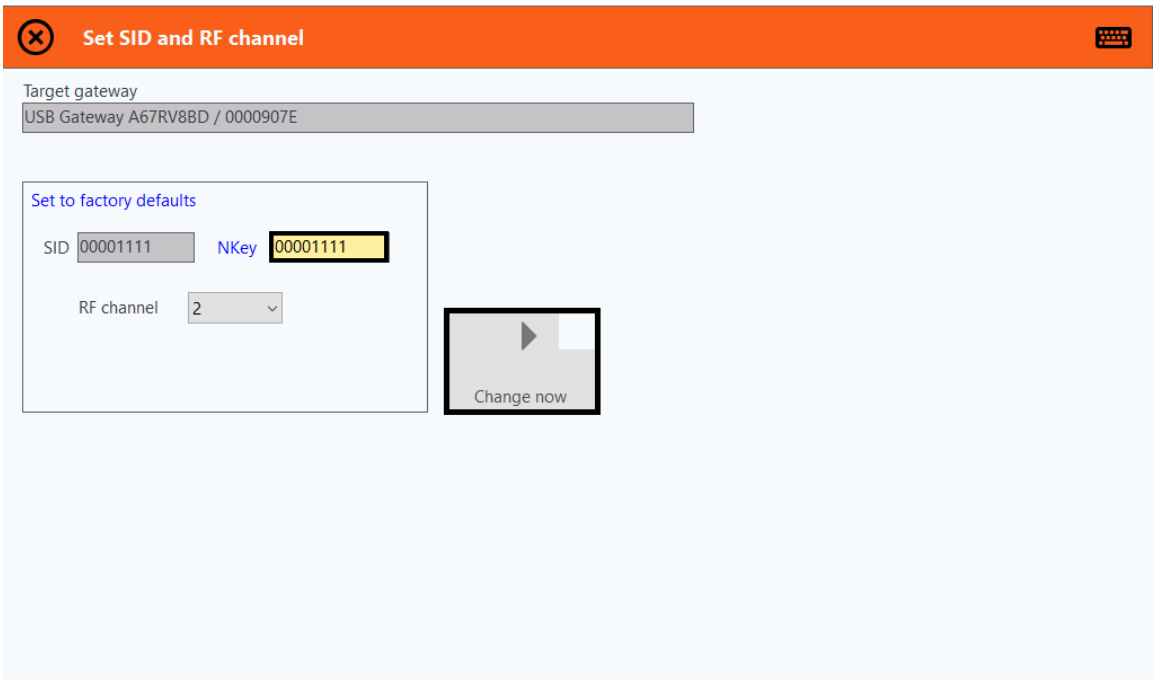
Clicking on the Gateways Status field produces the following image.



This screen contains more information about the status of the devices and the option to view a detailed form for a selected device in the table.



This screen compiles a detailed view of the status and the various measurements of the selected device, as well as a short list of additional options. As shown, these include a button to update the status of the device (Request status), the option to show the device on an uploaded floor plan and the option to configure the channel on which the device operates.



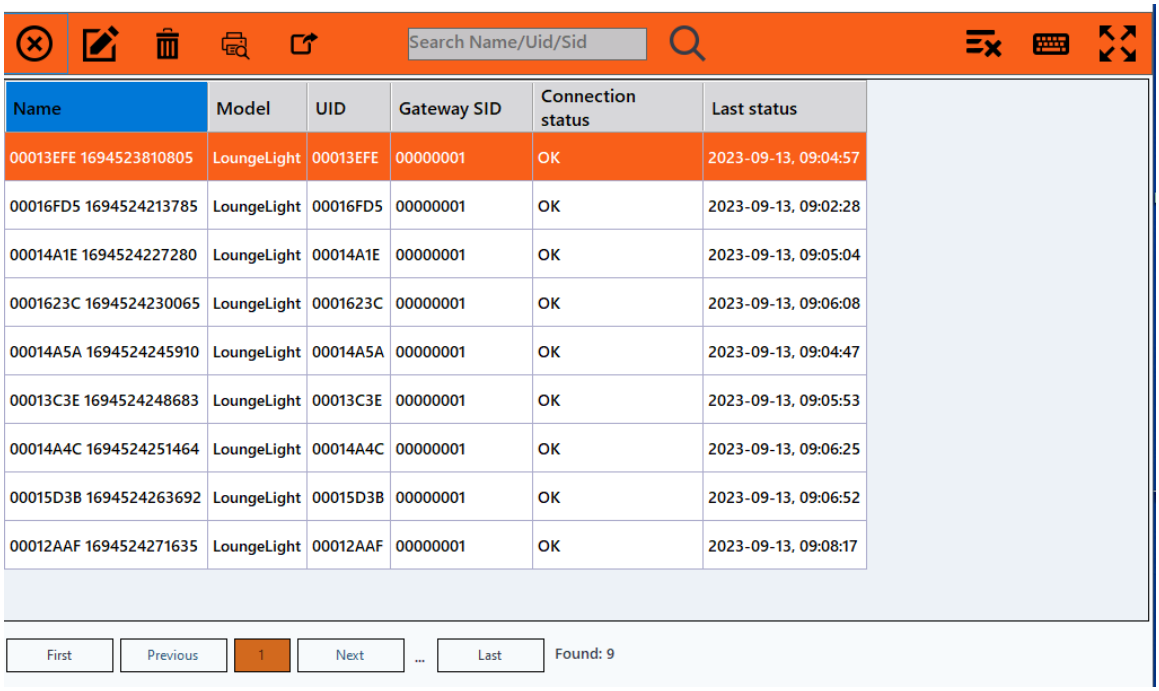
The last option does not include a value for the NKey field by default. The user will have to edit the field of which the recommended value is the same as the

SID. The option to change and save the configuration becomes available once the user leaves the focus of the NKey field.

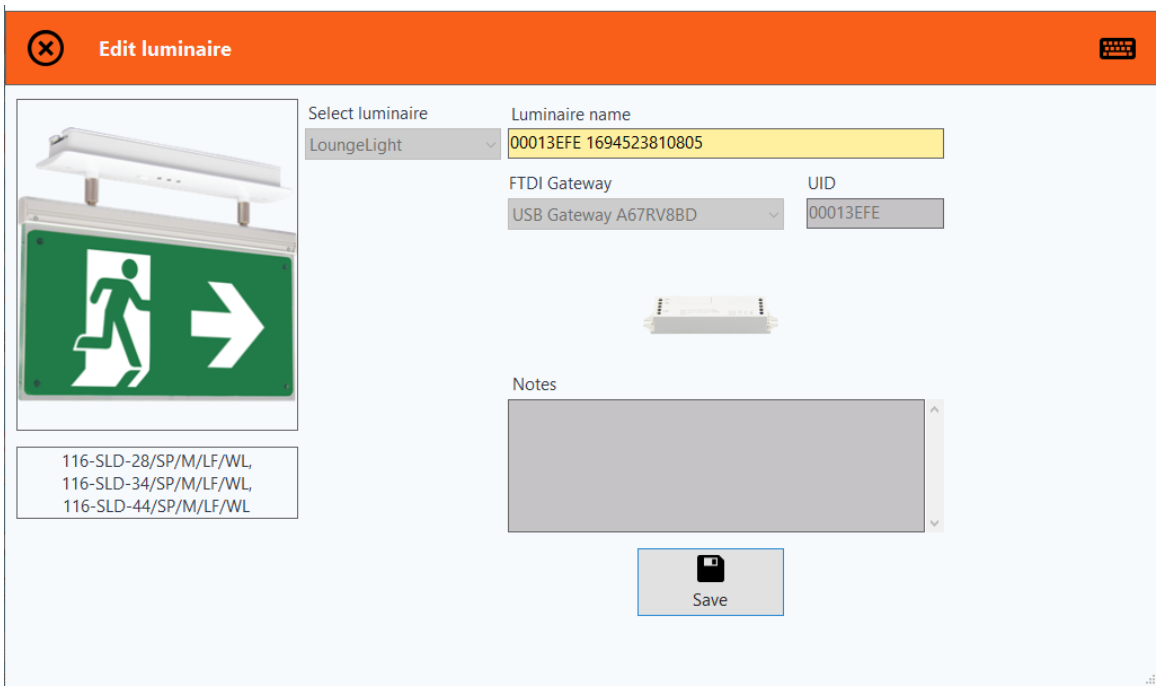
3.1.1.2. Luminaires

By clicking on the **Luminaires** field, a new window will open, displaying a table list of all the connected luminaires, their name, model, UID, Gateway SID, connection status and last status. The list presents 10 devices per page. With the search feature you are able to search in the whole list not only to the 10 presented devices.

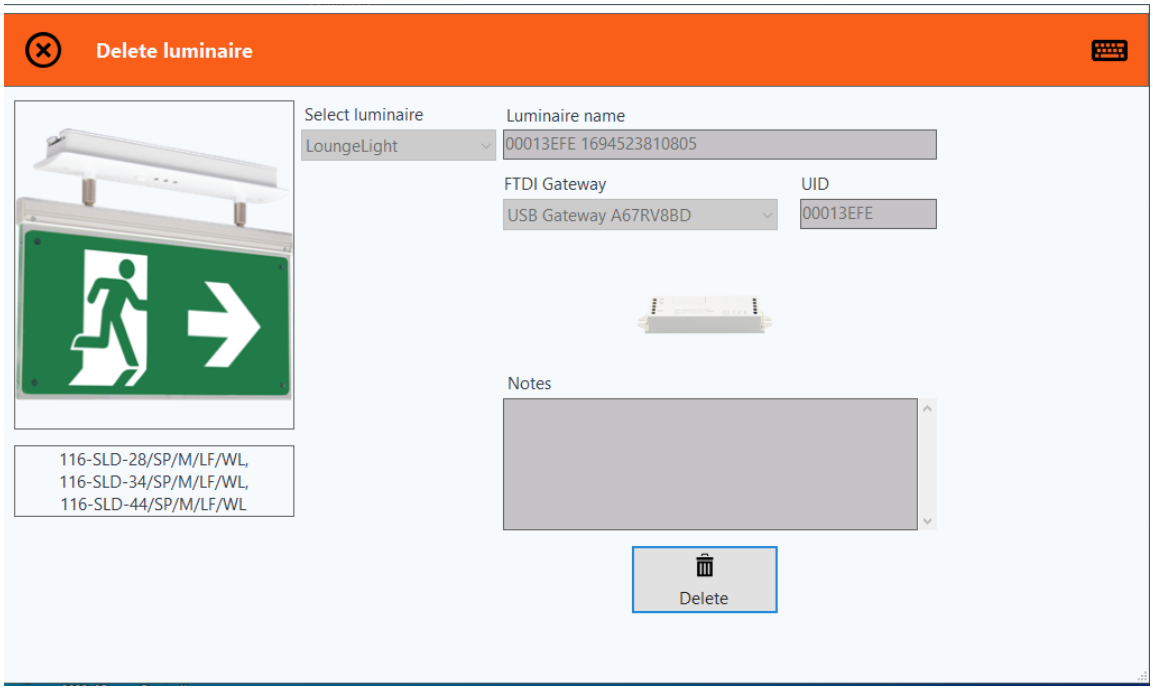
You can search a device by Name, UID and Gateway's SID



The leftmost CRUD action allows the user to edit a selected luminaire. Most fields within the new window are editable, including the **Select luminaire** drop-down menu.

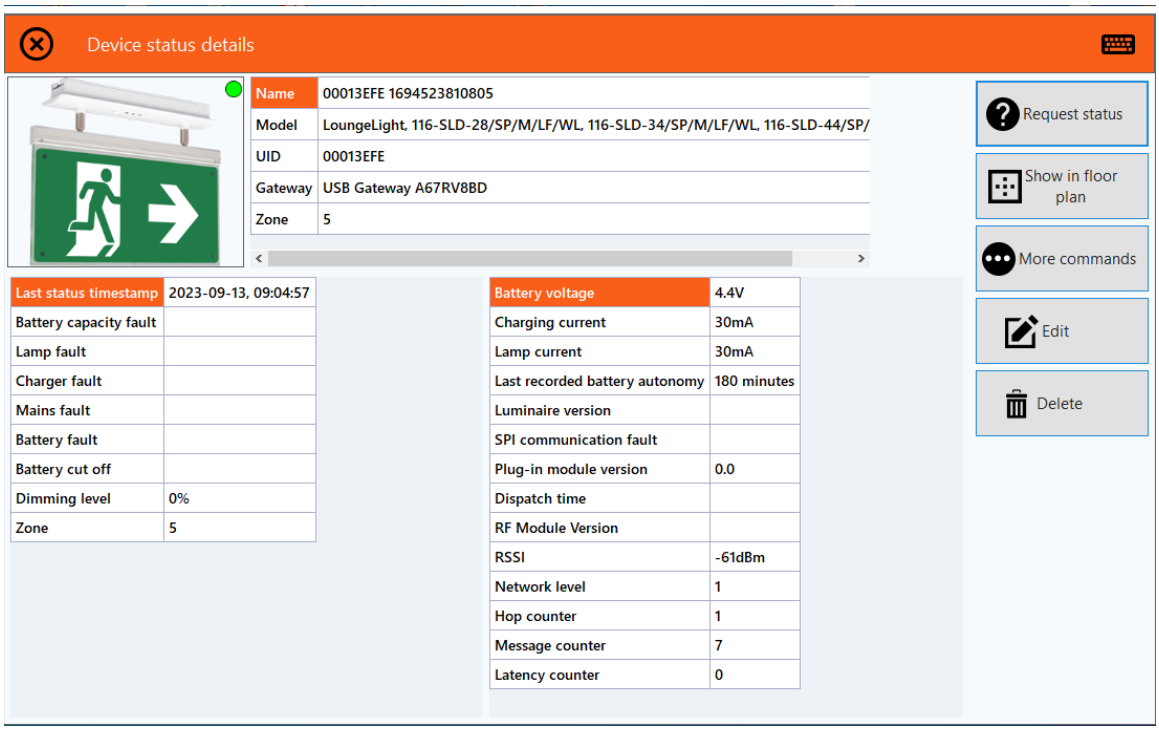

Edit luminaire
Select luminaire
LoungeLight
Luminaire name
00013EFE 1694523810805
FTDI Gateway
USB Gateway A67RV8BD
UID
00013EFE
Notes
116-SLD-28/SP/M/LF/WL,
116-SLD-34/SP/M/LF/WL,
116-SLD-44/SP/M/LF/WL
Save

The next action allows the user to delete a selected luminaire device.



Returning to the Home screen, the user may double click on a device to open **Status** field to access a detailed status array of all connected luminaires.

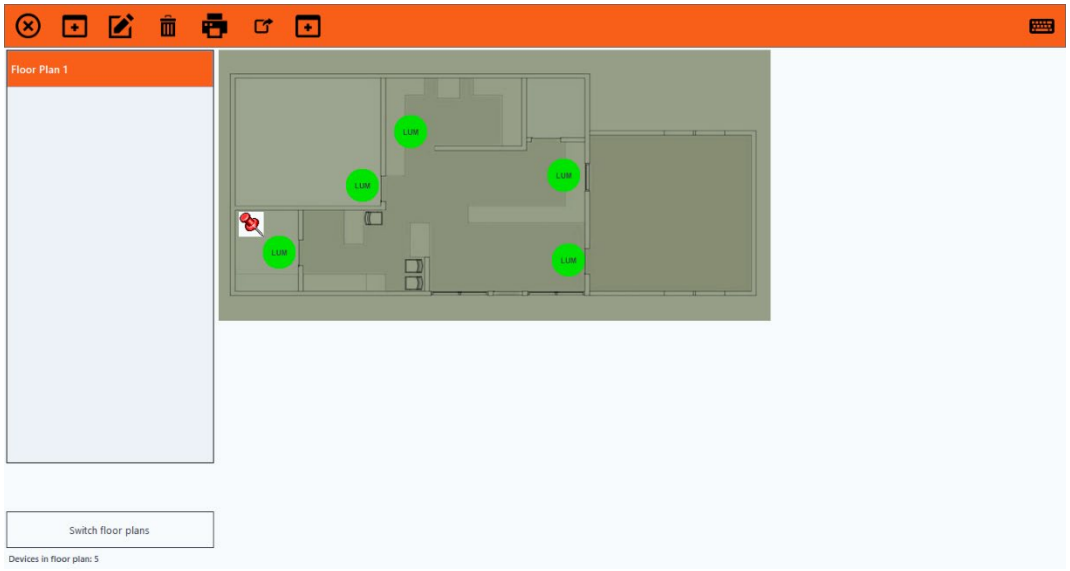
Within the Luminaire status screen, details about a selected device are accessible by clicking on the leftmost icon.



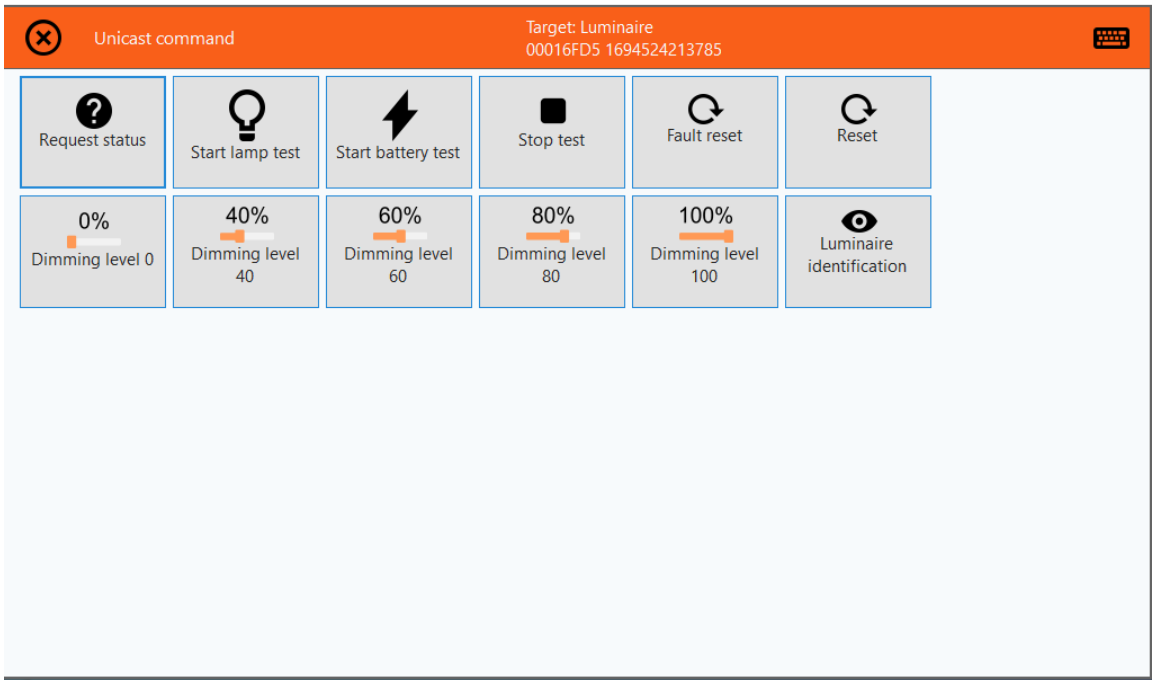
Clicking on the leftmost icon opens a window with several useful commands and controls.

The first button, request new status from the device.

The second button, **Show in floor plan**, is responsible for the following screen.



The “More commands” button opens an array of every available command for the luminaire.



This screen affords the user several commands to send to individual luminaires. Notably, **Request status, Start lamp test**, **Start battery test**, and **Stop test** can be used to command the device to perform a check test on its functions, a durability test on its battery and a halt to its commenced test, respectively.

The **Fault reset** button allows the user to clear the faults of the selected device.

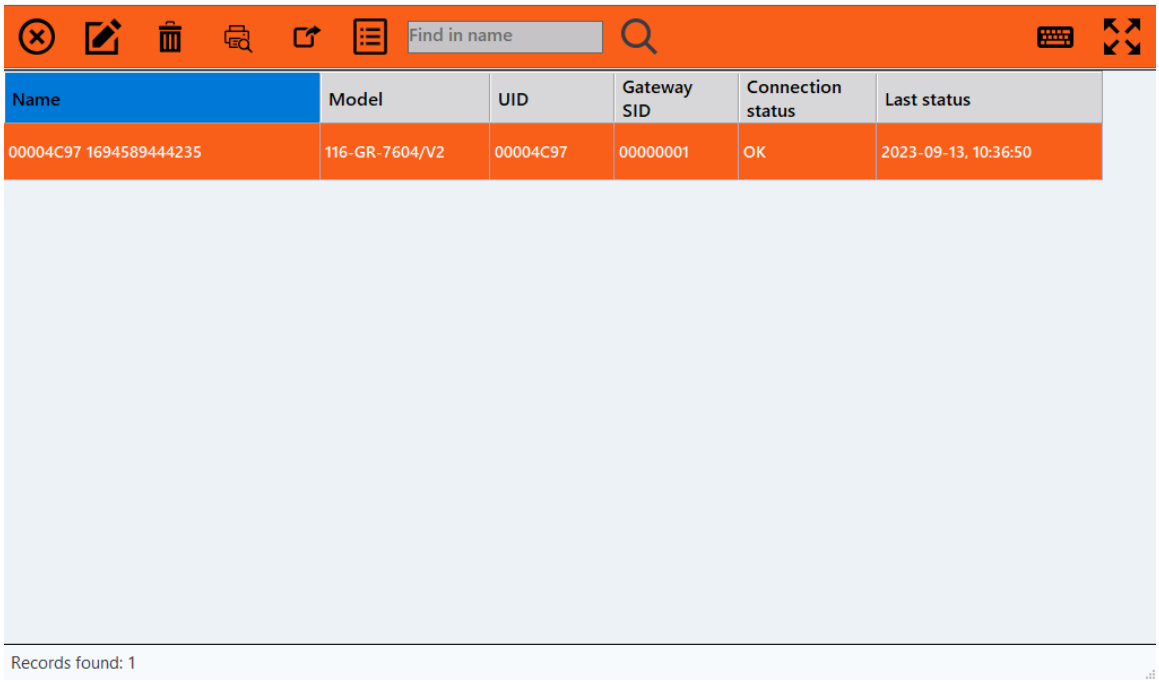
The **Dimming level** buttons instruct the luminaire device to increase or decrease its output to each button's indicative level.

The last two buttons, **Edit device** and **Delete device**, direct the user to the same screens as the CRUD actions that were described earlier.

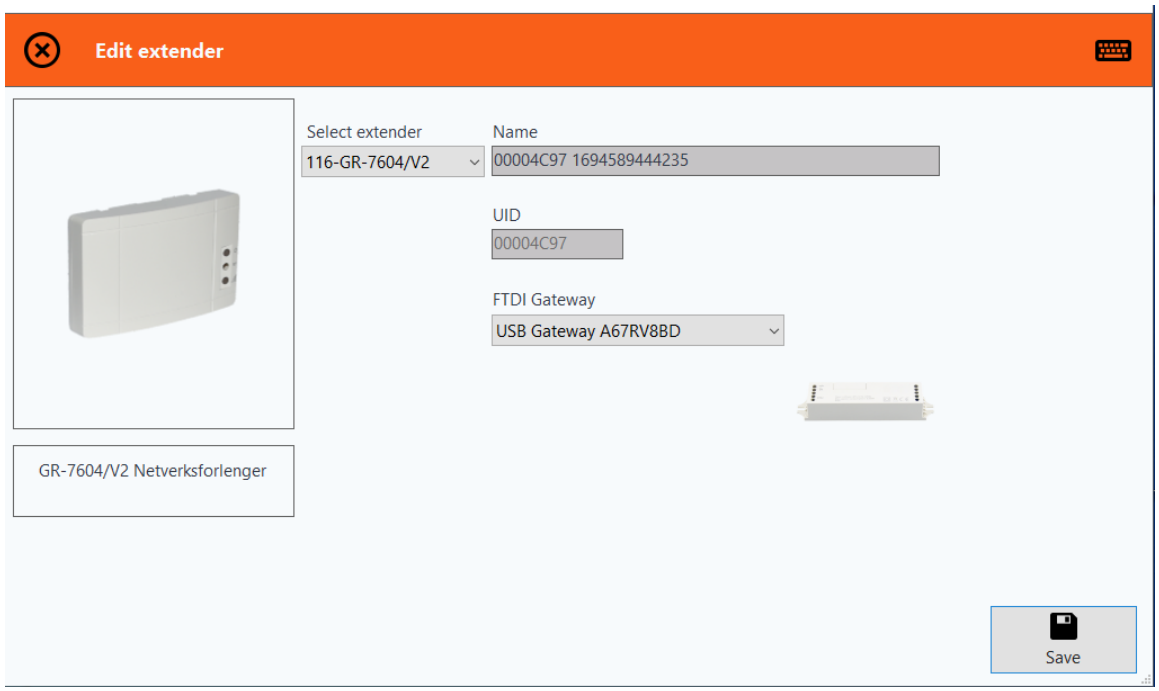
 Deletes all the luminaires from the software.

3.1.1.3. Extenders

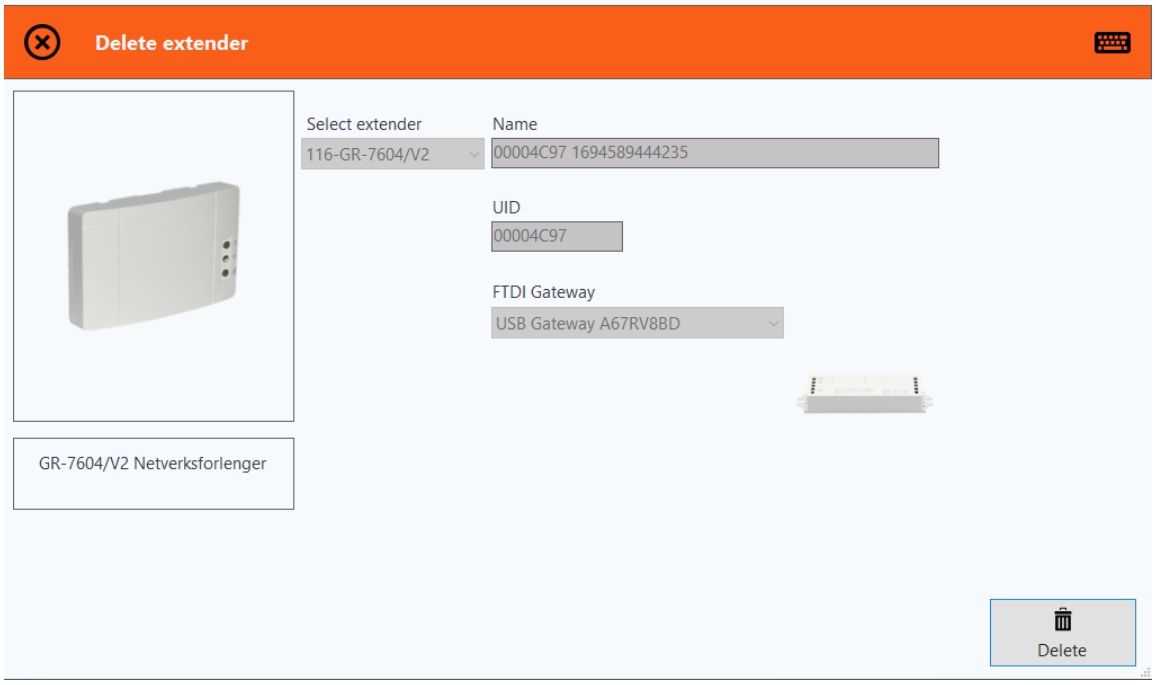
Clicking on the **Extenders** field directs the user to a new window that hosts a table list of every connected extender device. Additionally, through this the user can select to edit or delete a specific device, use the print preview option, use the event export option to locally save an HTML, check the device's status, or search the table for a specific extender.



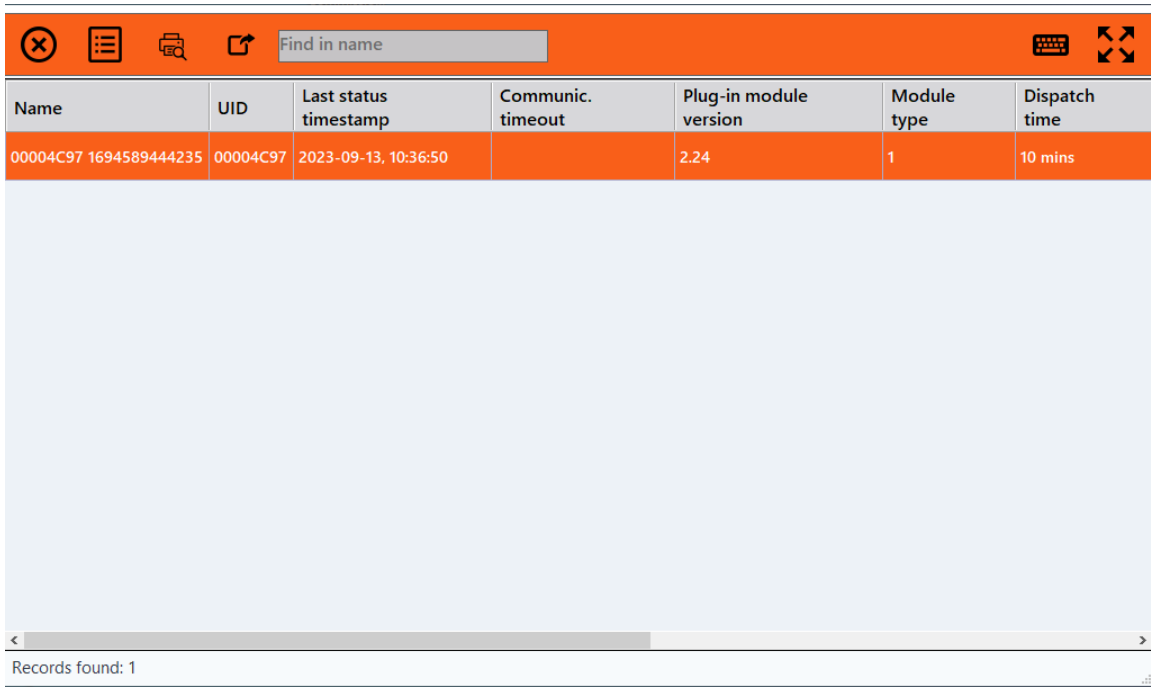
By selecting the "**Edit extender"** option the user is directed within a new window that contains some editable fields regarding the device's information.



By selecting **Delete extender**, the user is directed within a new window that enables them to delete the device in question, after asking them for confirmation.

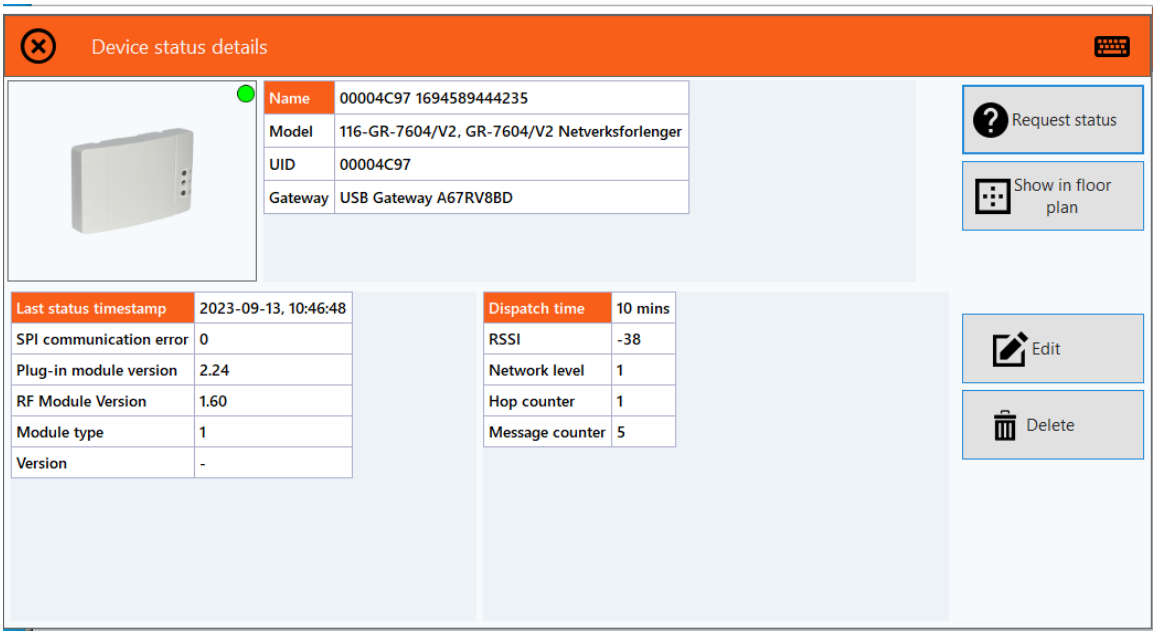


The **Extender status** option redirects them to a new window that is also the same with the screen that is created by clicking on the second interactive field of the Extenders column.

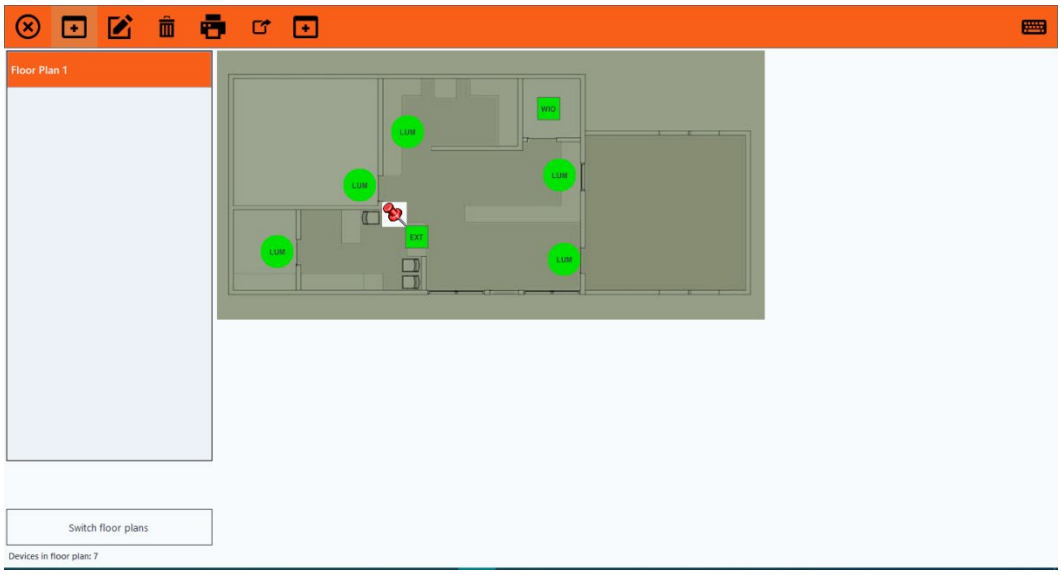


The window above contains information regarding the device's status. Through this the user can select to see additional details about a selected extender, or search for a specific device.

The leftmost option (or double click to the devices raw) redirects the user to the Extender status details, which pertains to a detailed and condensed status report, including new and already explained actions.



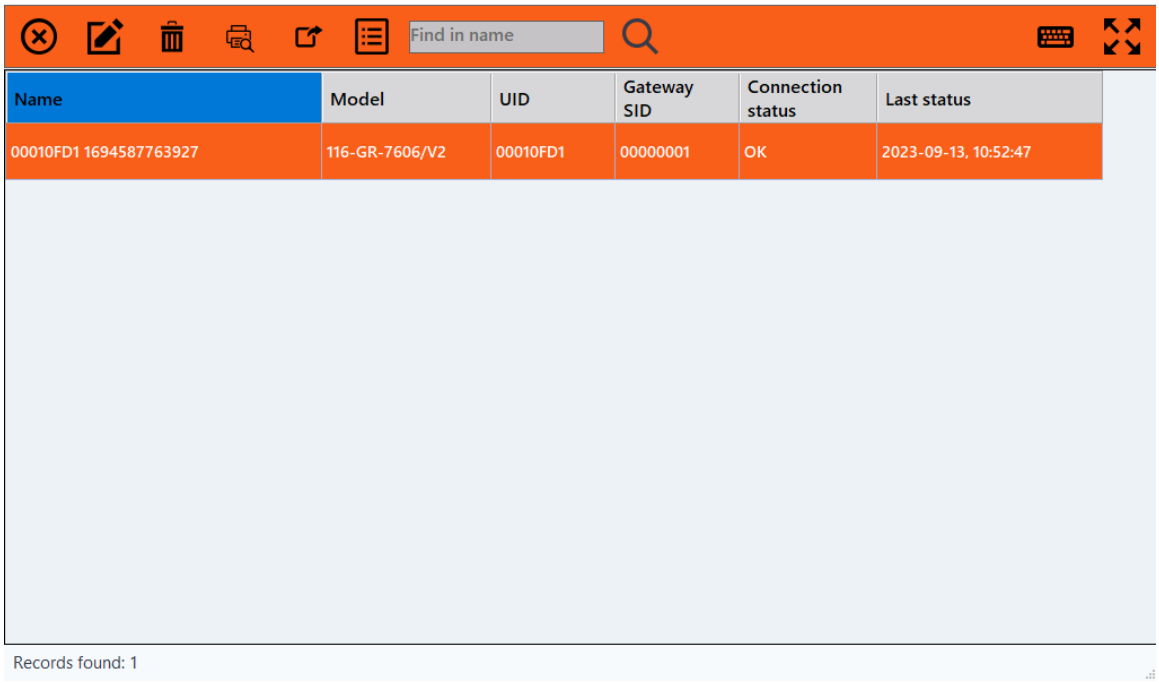
Within the section on the right, the user may find several actions, the first of which being a button that updates the status of the extender. The second button redirects the user to a new window that shows the position of the device, if it has been added within the Floor Plans.



The last two buttons create the same windows as the **Edit extender** and **Delete extender** options found within the Extenders interactive field.

3.1.1.4. Wireless IOs

Clicking on the **Wireless IOs** field directs the user to a new window that hosts a table list of every connected wireless IO device.



The user can select the **Edit wireless IO** option to access a form that enables them to change the desired output and input actions through the detection of certain system procedures.

The outputs can be activated in the following cases:

- Lamp test
- Battery test
- Emergency operation
- Forced emergency
- Fault

The inputs can start/enable the following procedures:

- Lamp test
- Battery test
- Forced emergency
- Dimming level 0
- Dimming level 40
- Dimming level 60
- Dimming level 80
- Dimming level100
- Dimming level ON-100, OFF-80

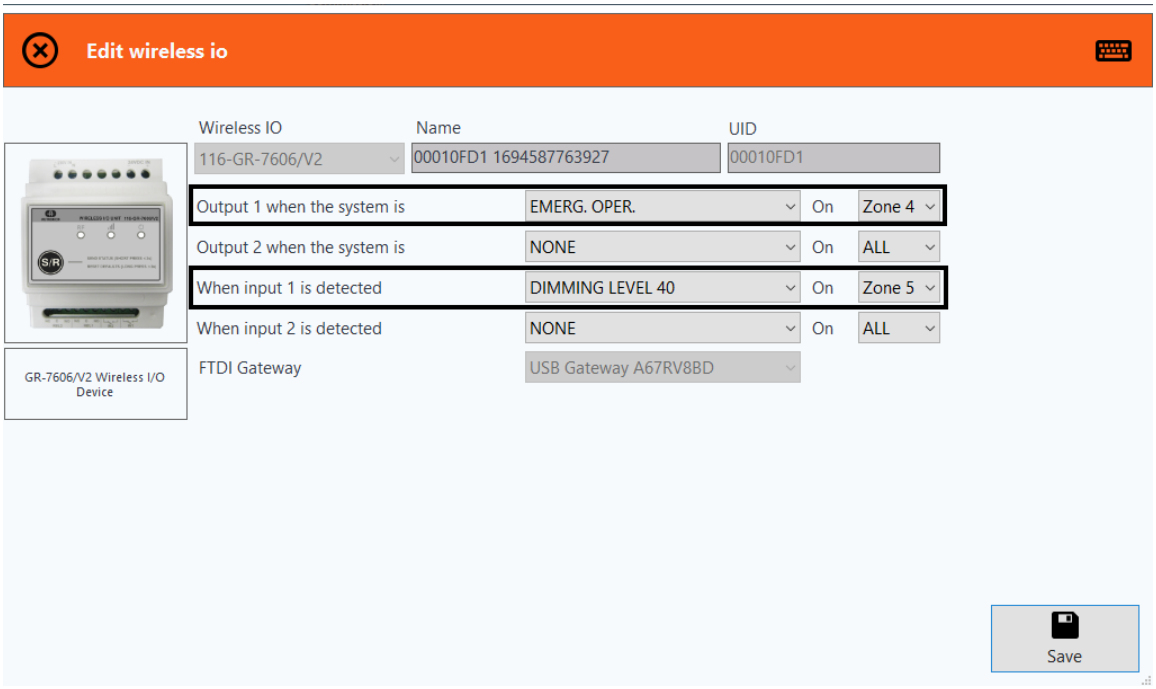
- Dimming level ON-100, OFF-60
- Dimming level ON-100, OFF-40
- Dimming level ON-100, OFF-0
- Dimming level ON-80, OFF-0
- Dimming level ON-80, OFF-60
- Dimming level ON-60, OFF-0
- Dimming level ON-60, OFF-40
- Dimming level ON-40, OFF-0

For example, there are the following **two scenarios**.

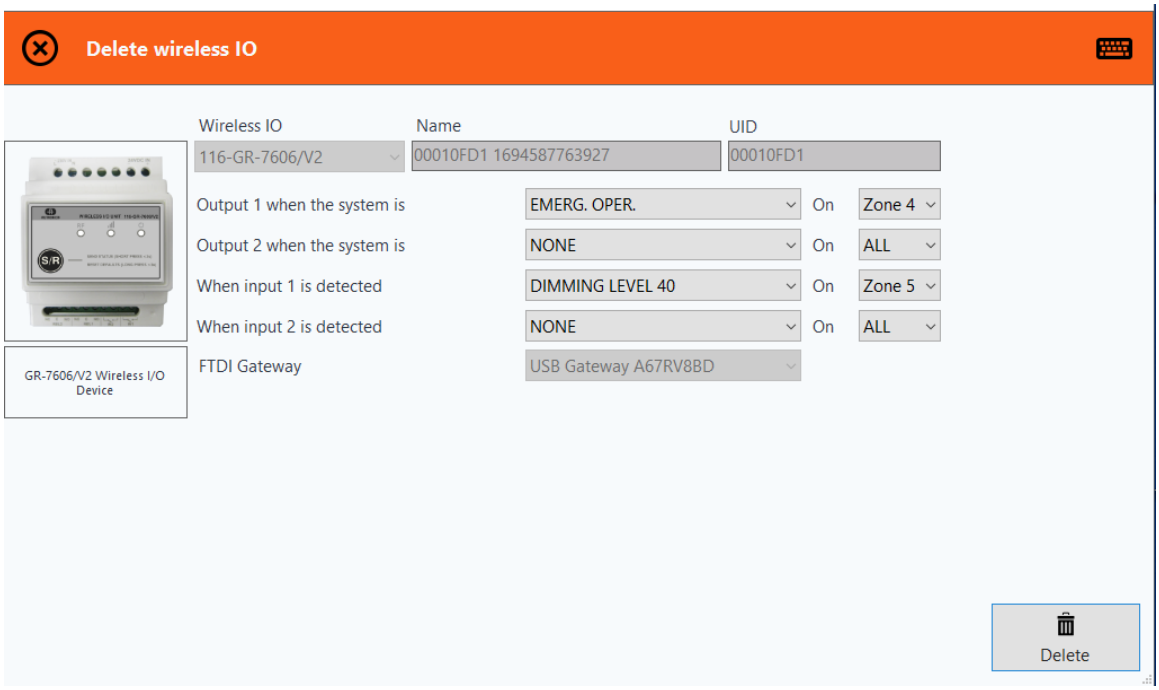
(a) The relay of Output 1 will be activated whenever the system within an assigned zone starts its emergency operation.

(b) Whenever the device's input 1 is detected, e.g., through the user of a switch or a button, the system will change the luminaires' dimming level to 40 within the assigned zone.

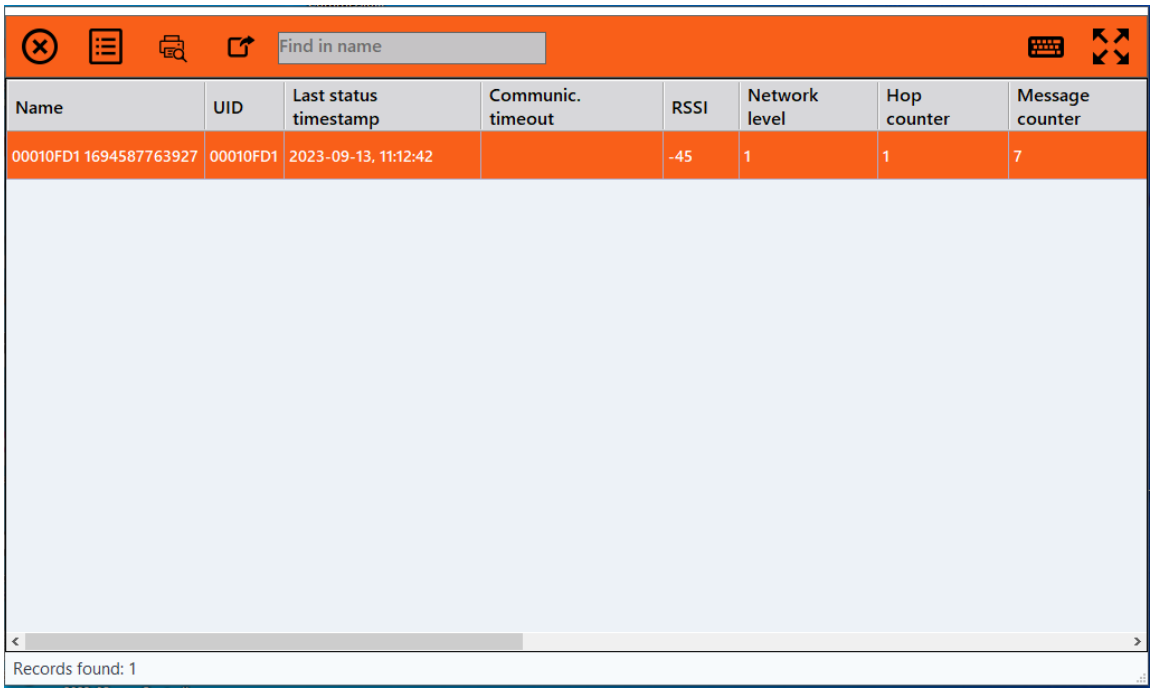
It should be noted that as is common while configuring any element, the user must **Save** configuration by pressing the button on the bottom-right. The view of the table list of the previous screen will be automatically updated, and any changes will be carried on when the user tries to view the specific device.



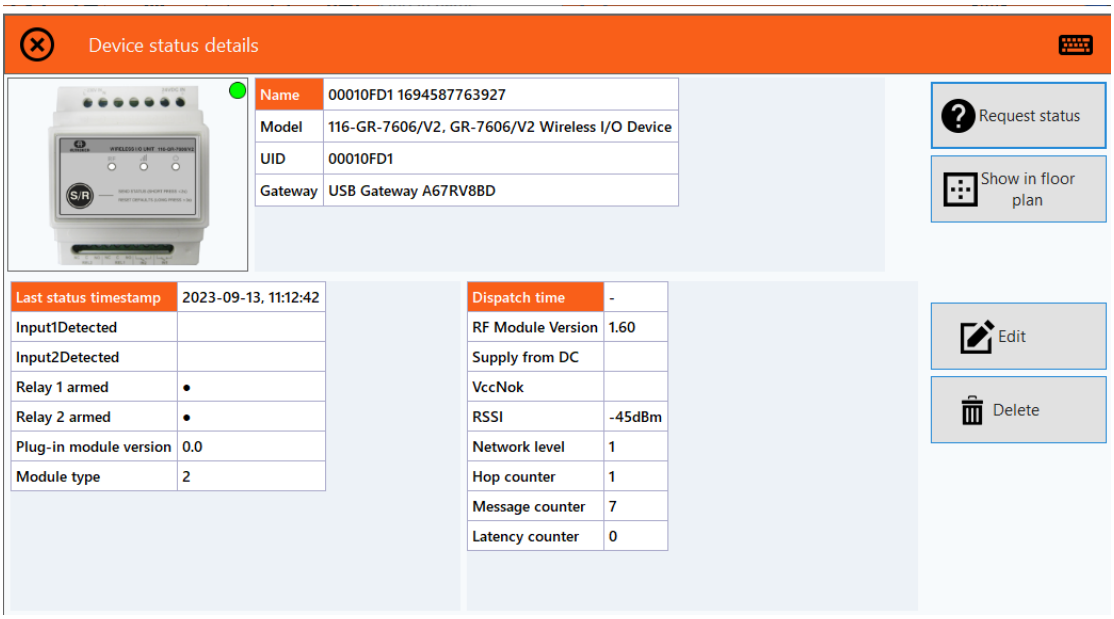
The user can select the **Delete wireless IO** option to delete the selected device.



The **Wireless IO status** window contains basic information regarding the status of every device organized within a table.

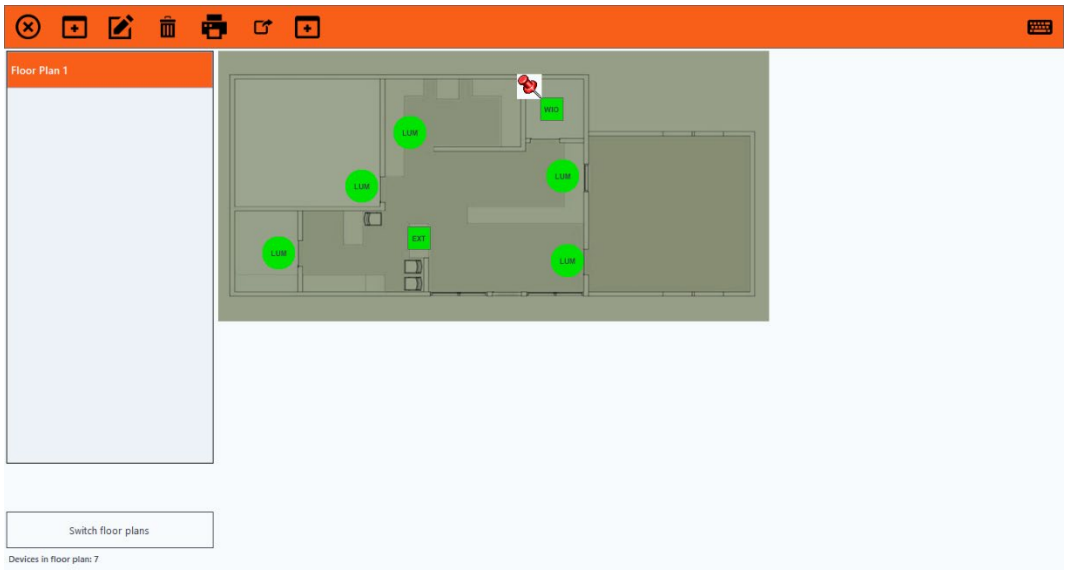


In this window, the user can select the leftmost option of the bar to produce a new screen displaying the details of the selected wireless IO device status. Double-clicking on a table row has the same effect.



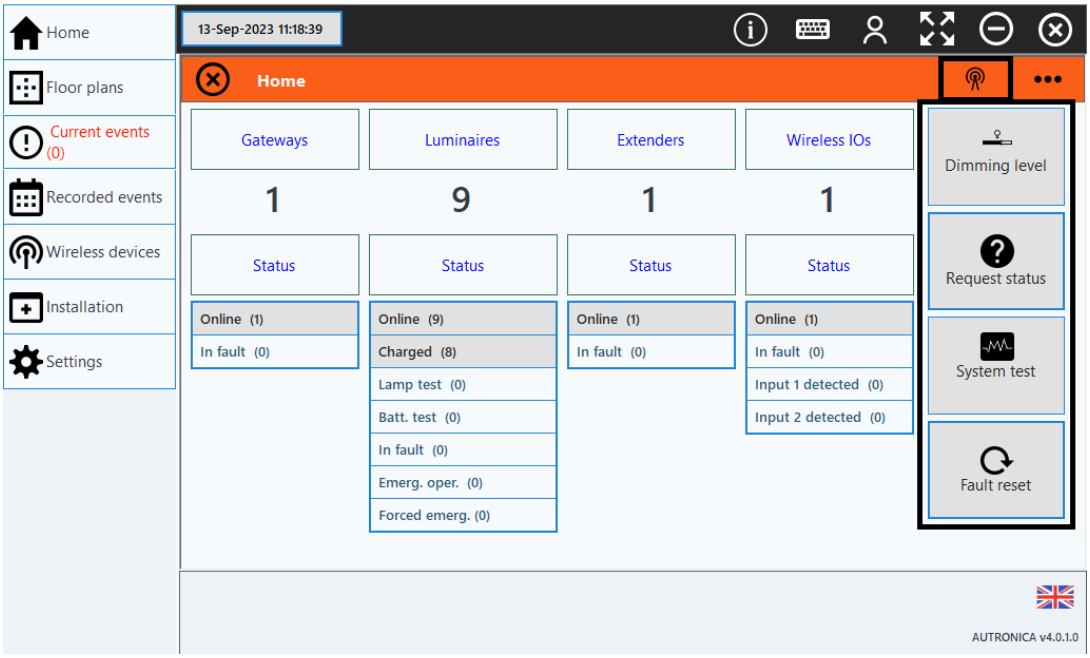
The Wireless IO status details window within the section on the right typically includes the options to update the status of the device with new values, to show the device in the floor plan, and to edit or delete the selected device.

The following image displays the position of the device in the floor plan if the device has been already inserted.

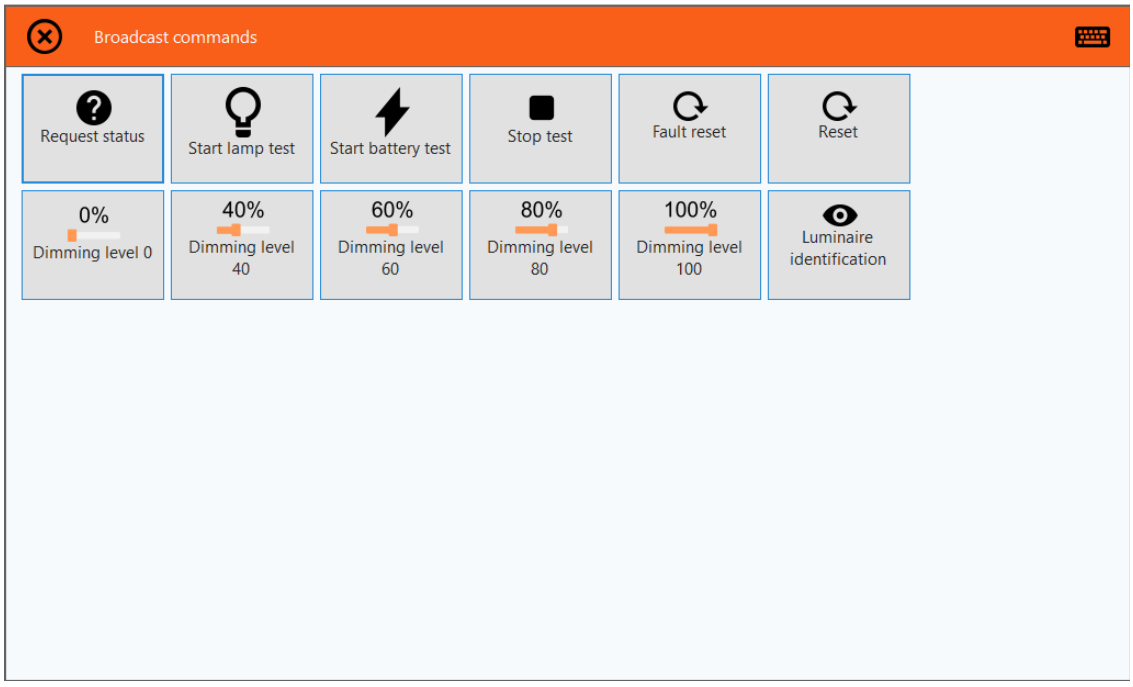


3.1.1.5. Broadcast commands

Returning to the **Home** screen, on the rightmost section of the title bar the user can access the commands that can be broadcast.



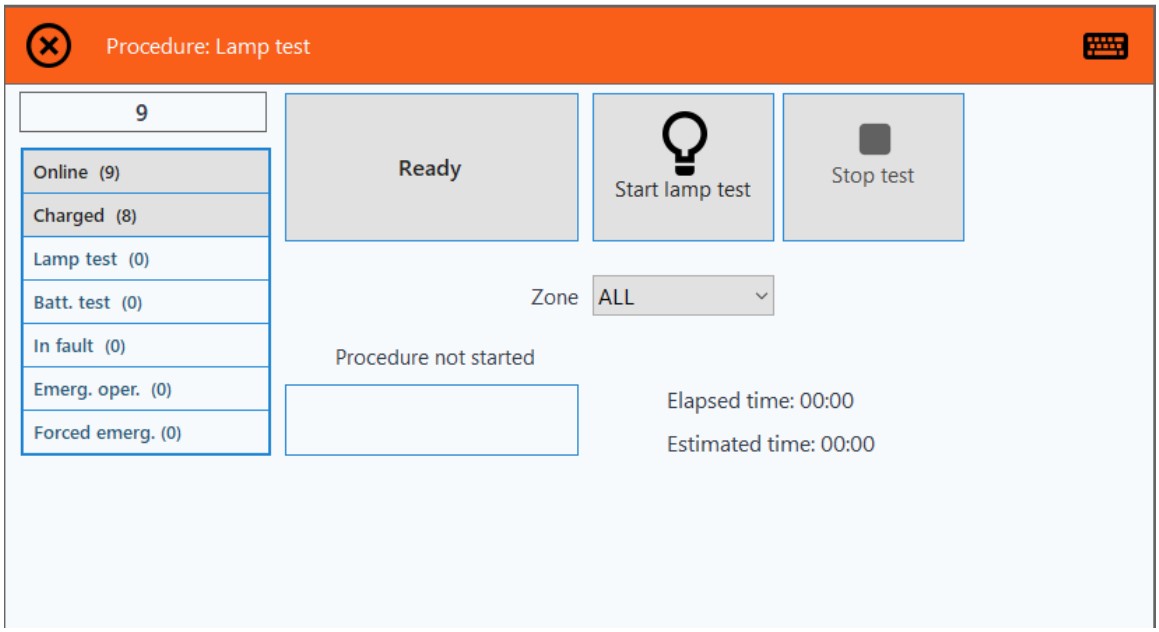
The user can click on the following icon to access the complete list of commands that can be broadcast to every connected luminaire.



This screen contains all available commands that can be broadcast to every connected luminaire device.

Request status updates the status details of the devices.

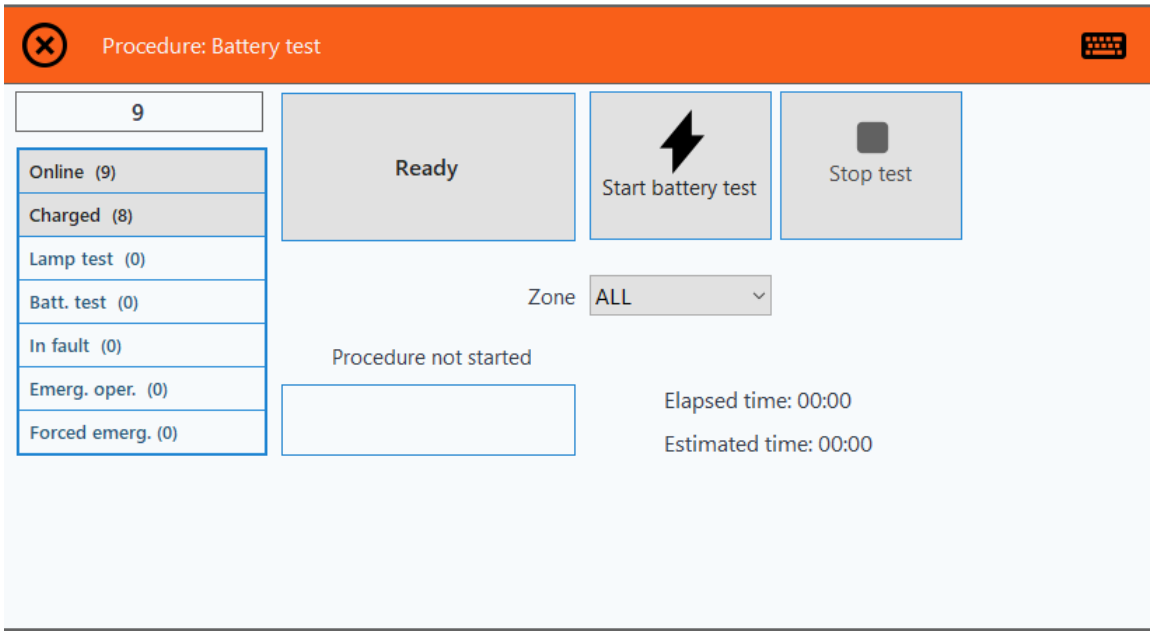
Start lamp test opens a new window that allows the user to initiate the test for all luminaire devices within an assigned zone. The lamp test is a short duration process, depending on the network, that activates the luminaires, which self-record their circuit measurements and register the values in the application. In the case of the existence of faulty measurements, the events are recorded and can be seen within any one of the **In fault** interactive fields of the Home screen.



Once the test has been initiated the user will be able to see its total estimated time and the step in which the procedure is at each moment. The user can stop the test at any time. On completion, the User Interface will notify the user that the procedure has finished.

Start battery test opens a new window that allows the user to initiate the test for all luminaire devices within an assigned zone. The battery test is a long duration process, mainly depending on the type of luminaire model and their batteries, which powers all luminaires. It fundamentally is a duration test that stops when the battery is depleted and records the autonomy of each device. The results of this test are registered in the application.

The following image is similar to the image from the previous test and follows the same principles. The Start test button needs to be pressed to initiate the procedure.



Once the test has been initiated the user will be able to see its total estimated time and the procedure's step. The user can stop the test at any time. On completion, the User Interface will notify the user accordingly.

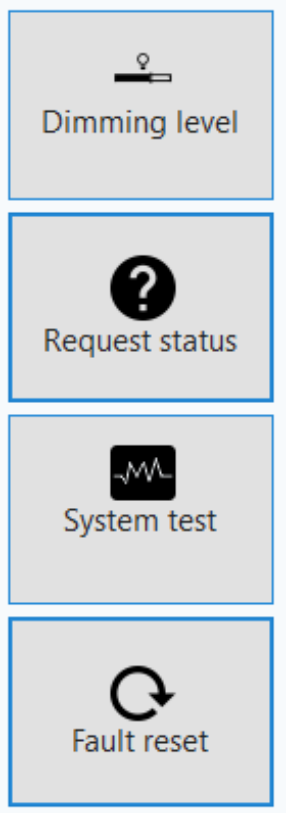
Notice!! This will run for the stated duration of each device individually and it needs a fully charged battery (24h charge-cycle) in order to run. To ensure long battery life do not run the battery test more than 2 times per year (e.g. once every 6 months).

Stop test terminates all tests that are running at the moment. This command is broadcast. Similarly with Request status, the current window's User Interface notifies the user of the process' progress.

Fault reset resets the faults of every connected device and clears the faults table. Similarly with Request status, the current window's User Interface notifies the user of the process' progress.

Dimming level 0/40/60/80/100 increase or decrease the luminaires' light output to each button's indicative level. Similarly with Request status, the current window's User Interface notifies the user of the process' progress.

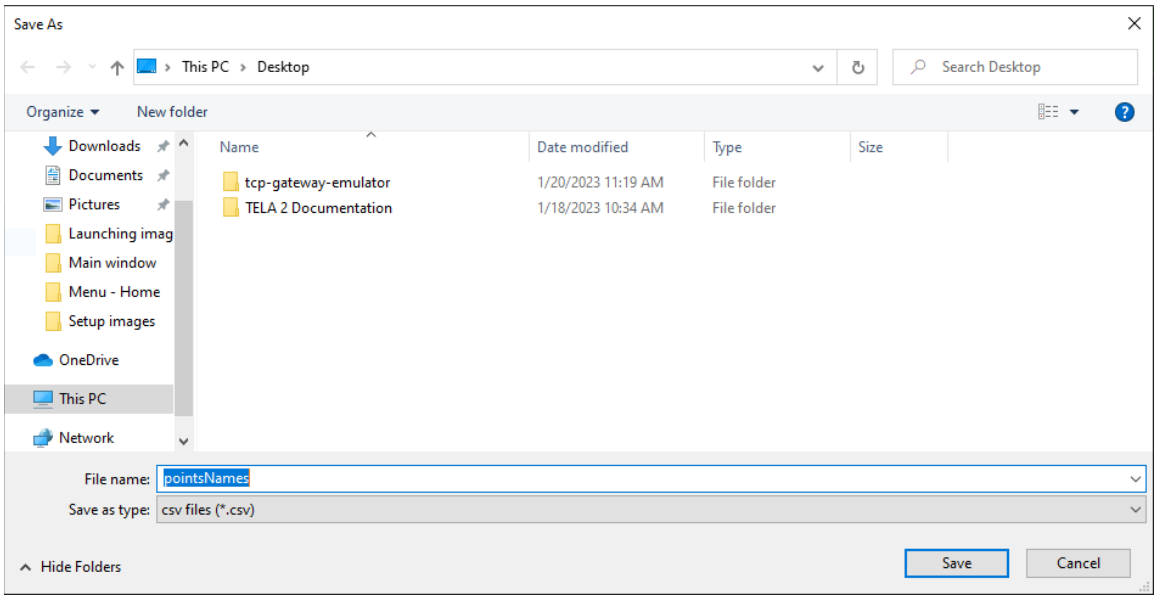
The following image displays the four commands that can be broadcast through the Home screen, without opening the complete list of commands.



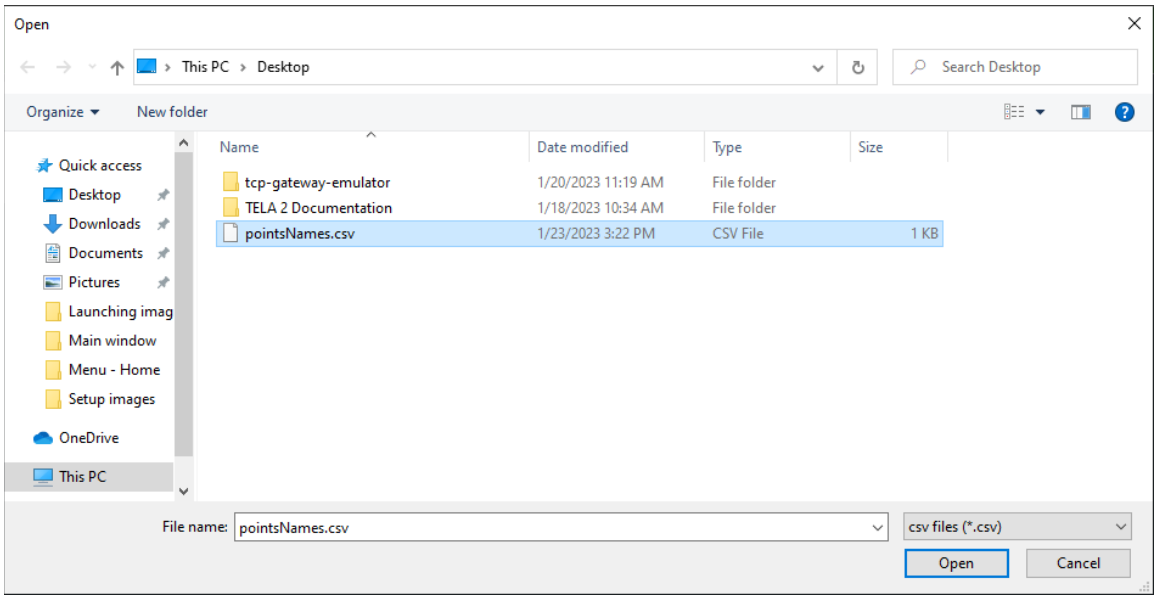
Other options is the last available element within the Home screen is directly next to the Broadcast commands button, on the rightmost of the screen's title bar.

Clicking it opens a window with 2 additional options.

Export names (.csv) exports a file that contains the names of every device, apart from the gateways. A name is automatically assigned to every device, which is derived from that device's hex address. The user can export this file in order to store the names they have already assigned to the devices and use it at a later time. They can also edit the generated file to assign different names more efficiently to the devices. In the case they wanted to change the names of a great number of devices, they would be forced to do so for every device individually, by finding the device, selecting to edit the device, and changing its name within the application.

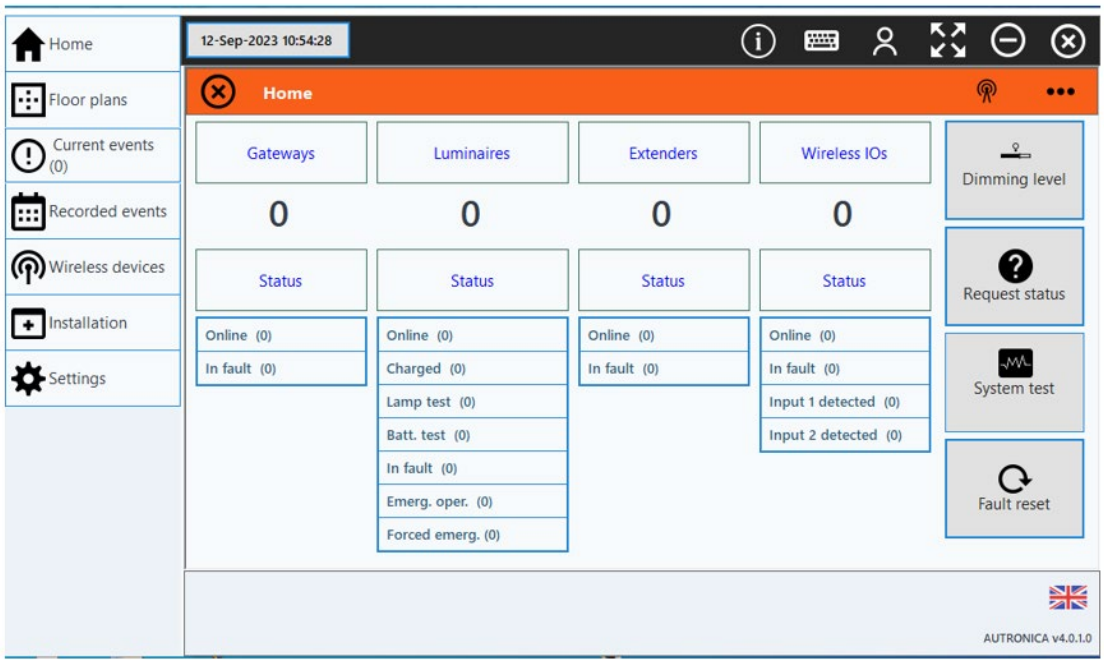


Import names (.csv) allows the user to import a .csv file that contains the hex addresses and names of the devices they want to register in the application. As mentioned previously, this option can be an efficient tool to change the names of every device, apart from the gateways. The user can also add several devices in this file, using a hex address and a name, as shown above. These devices will be read by the system, if the given hex addresses correspond to devices that are already connected to it.



3.1.1.6. Maintenance Notice

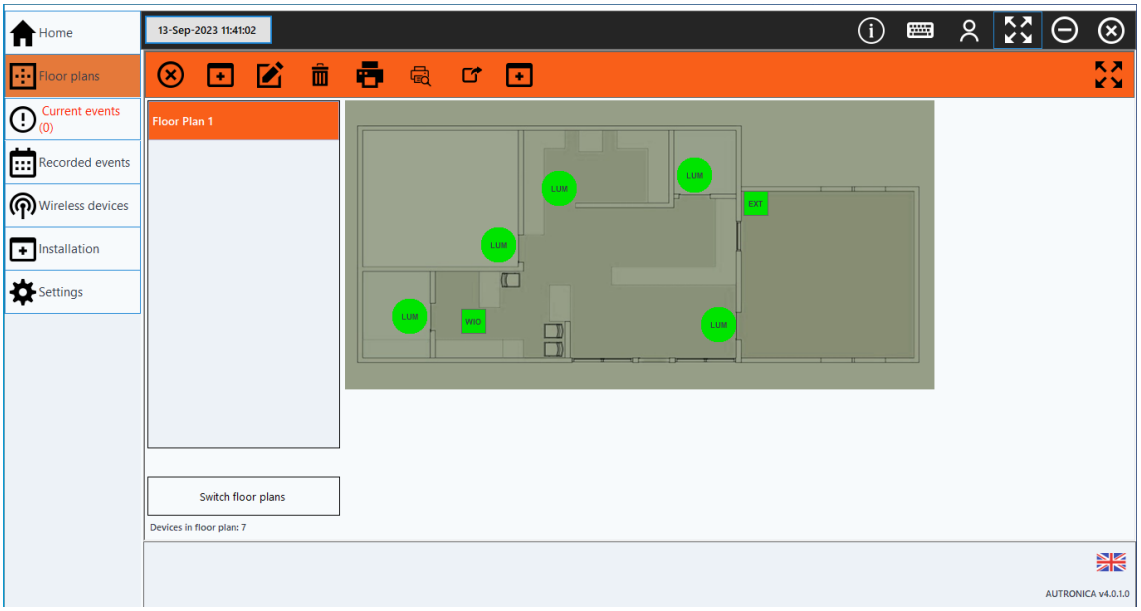
Upon completing the installation of Tela2, the system records the installation date. After one year, Tela2 automatically displays a maintenance message. This process occurs automatically every year and is not affected by whether the computer or tablet is turned on or off.



3.1.2. Floor plans

This chapter provides a thorough overview of the Floor plans menu, its features, configuration capabilities and functionality.

The following image is the User Interface when the Floor plans menu is active and includes all the basic elements that may interest the user.



The top bar contains the following options, from left to right: Add new floor plan, Edit floor plan, Delete floor plan, Print, Print preview, Export image, Place devices. In addition, the user can also switch among the created or already available floor plans and toggle an automatic switch that scrolls through each item of the floor plan list, in carousel fashion.

Add new floor plan, enables the user to add their own floor plan. The first step toward this action is to provide a name for the floor plan in order to create it within the list on the left.

The supported image file are : **.jpg**, **.png**, **.bmp**, **.tiff**, **.gif**.

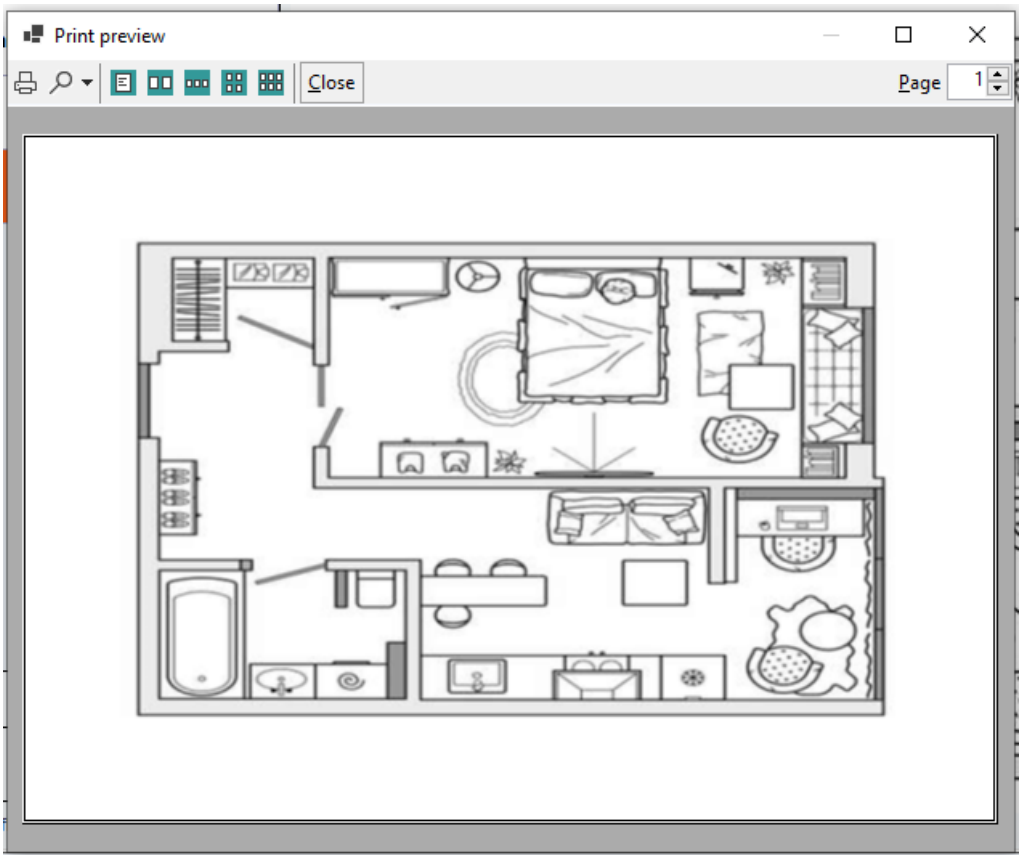
From the left column select “New image” to add your floor plan’s image. You are able to arrange the picture to fit in the software’s screen. There are two ways, manually by the +/- you are able to adjust your image.

You are able to change the adjusting step for the bar below or you can select “Auto”, and the software arrange the picture. In the end press “Save”

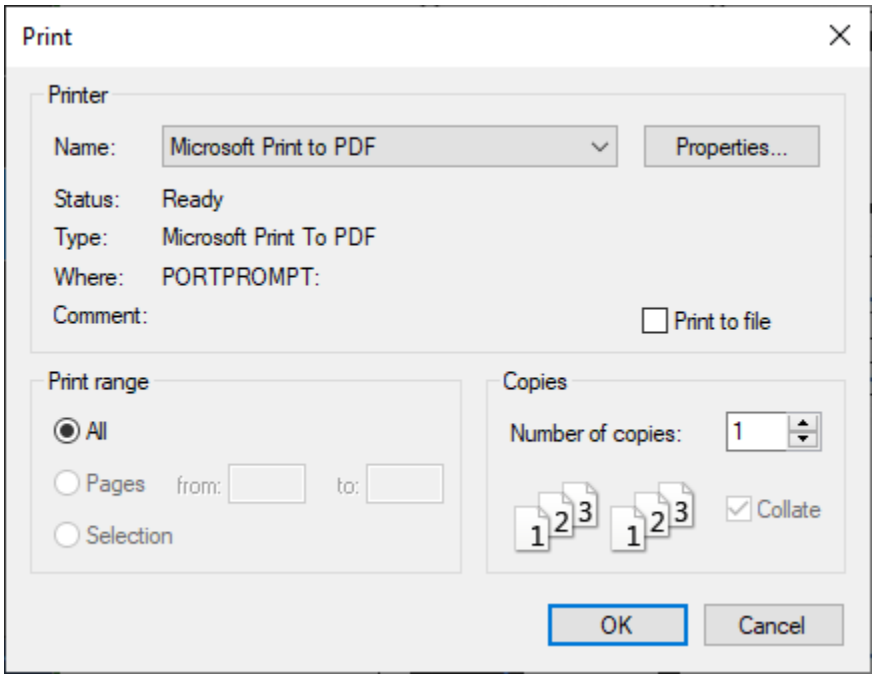
Edit floor plan, this option opens a similar window as the “add new floor plan” but for the selected floor plan and only for editing.

Delete floor plan, select the appropriate plan and click on **Delete floor plan** to remove it.

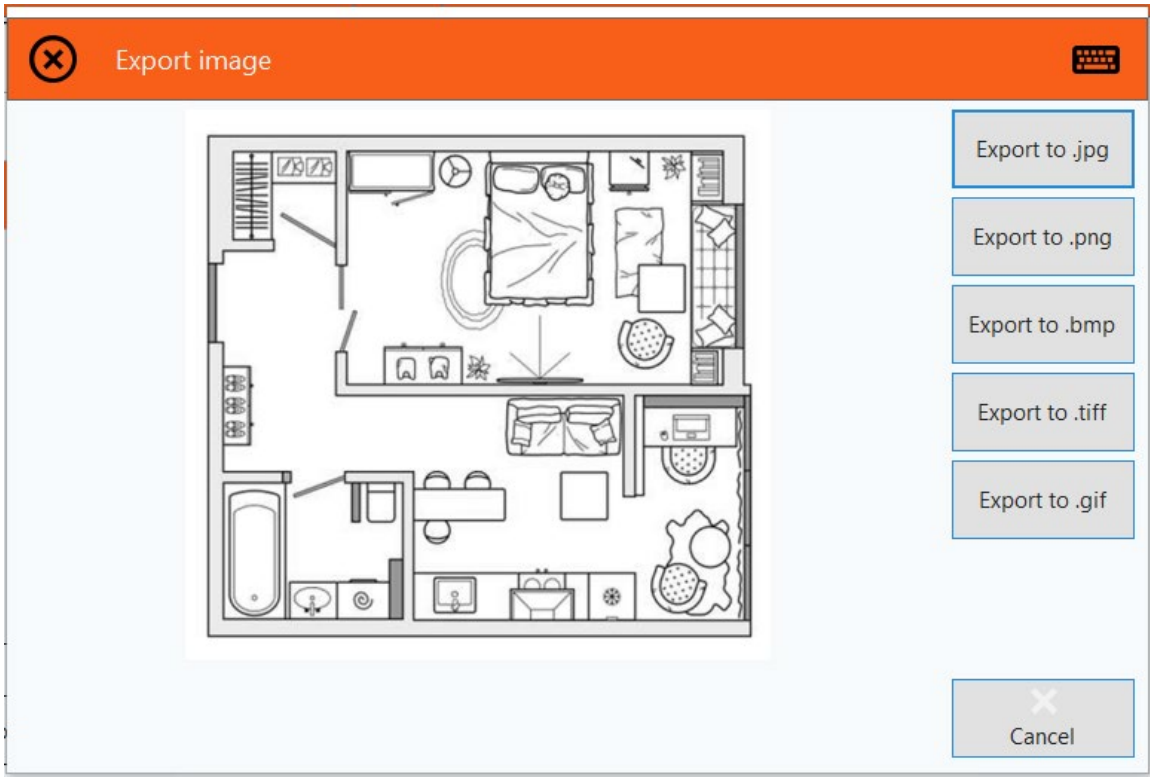
Back within the Floor plans screen, after selecting a plan they may select **Print preview** to produce a window that allows them to view how the plan will be printed.



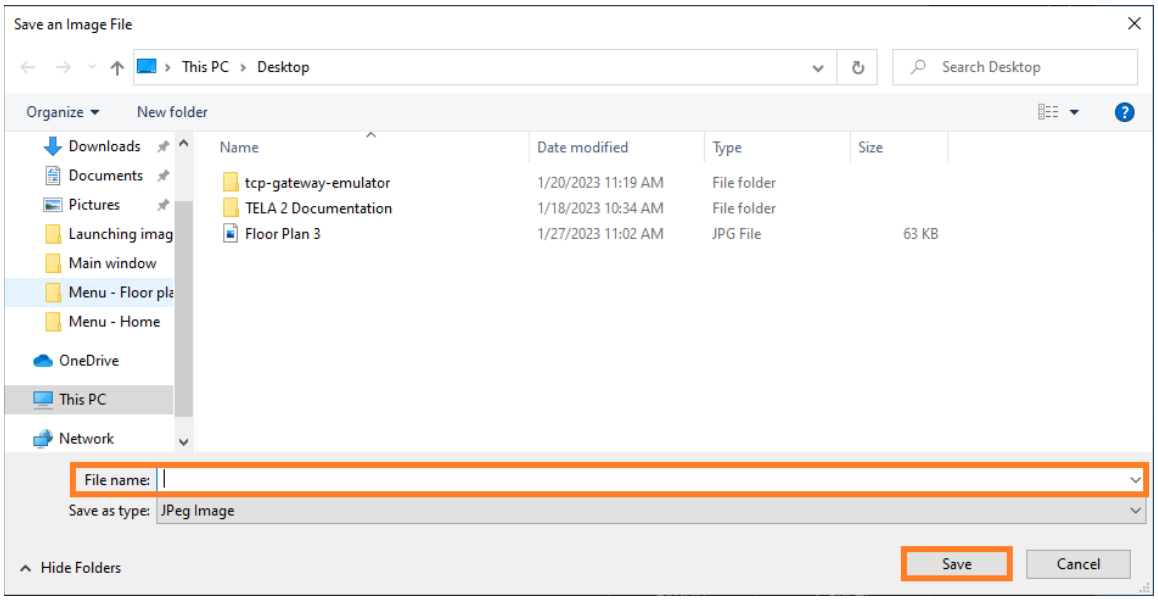
If the preview proves satisfactory, the user can then select to **Print** the floor plan. On click, the appropriate system window will appear.



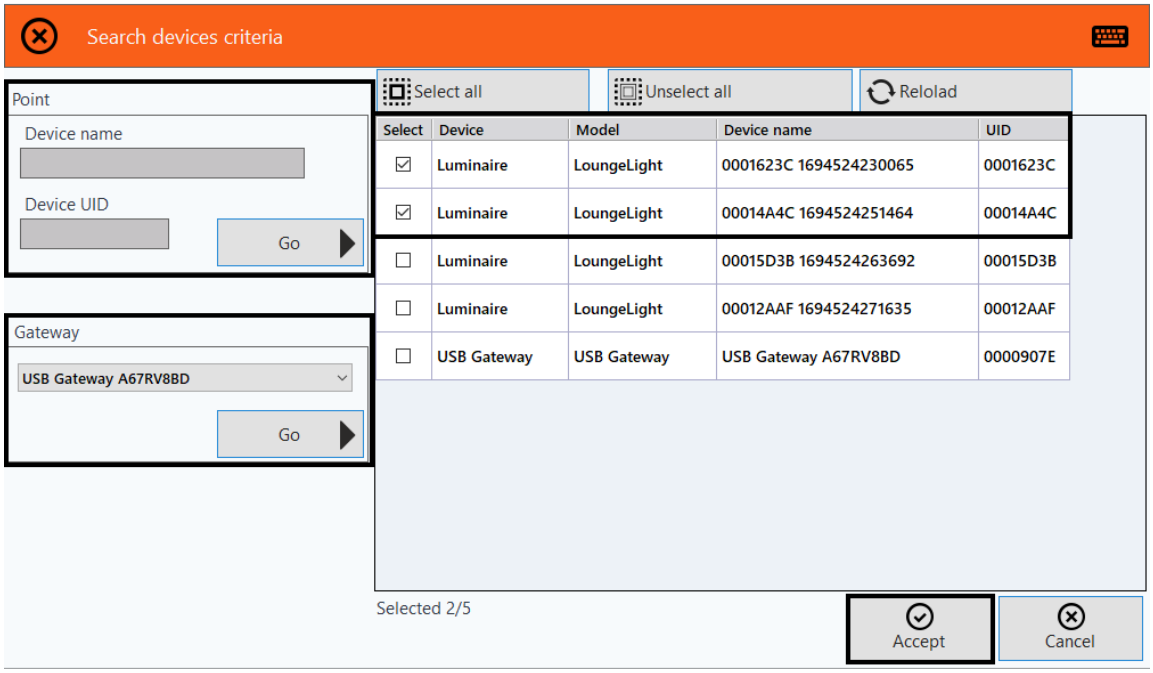
Additionally, the user can select the **Export image** option in order to locally save the image of the floor plan, in one of the types included in the following screenshot.



On **Export** another system window will appear asking the user to select the path within which they want to store the file and a name for the file.



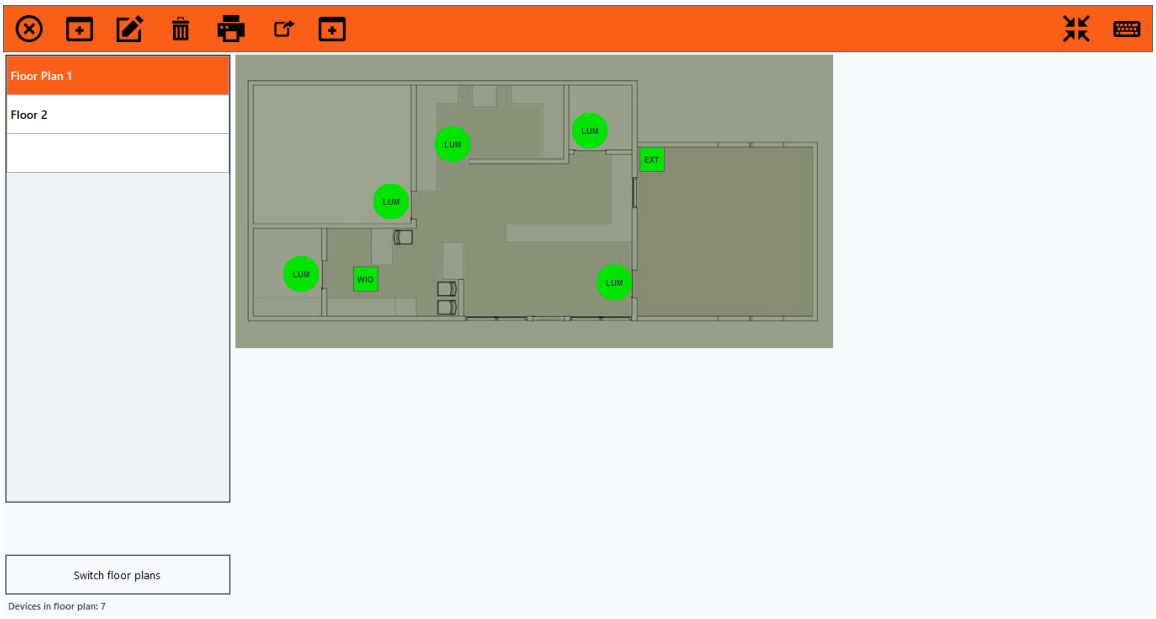
The last element of the Floor plans screen's top bar is the **Place devices** option. This allows the user to select one or multiple devices from a list of every available device, in order to start placing them on the floor plan. It should be noted that the print and export options produce images that correspond to the floor plan's device placement state.



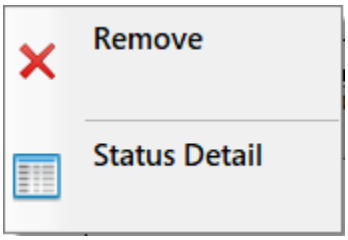
Once the desired devices have been selected, either through the list on the right, or by searching for them using the section on the left, the user may **Accept** this

selection and be redirected back to view the floor plan, which now contains block elements of every inserted device.

The user can change the position of each device by dragging the block to the desired spot.



They can also right click on a device for the option to remove it from the floor plan or view its status details.



The last option within the Floor plans screen is the ability to **Switch floor plans**, which toggles an automatic carousel-like rotation among the available floor plans, in five (5) second intervals.

As each device's block element within the floor plan can change its color, depending on the device's status, e.g., in the case a device is online, offline, faulty, performing a test, etc., this option can prove useful. In a scenario where the user desires to monitor the status of each device in every floor plan that may represent different locations within a building, they may toggle this option to passively view the floor plans.

- Luminaire/device charging (online)

- Luminaire/device in emergency

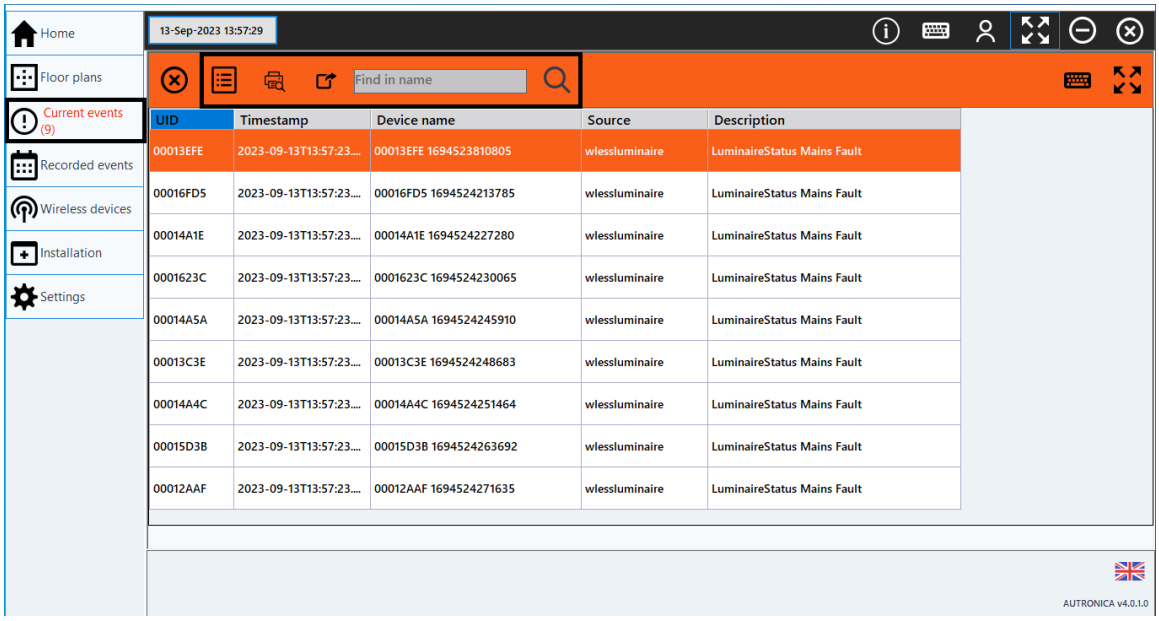
- Luminaire/device with fault

- Luminaire/device disconnect

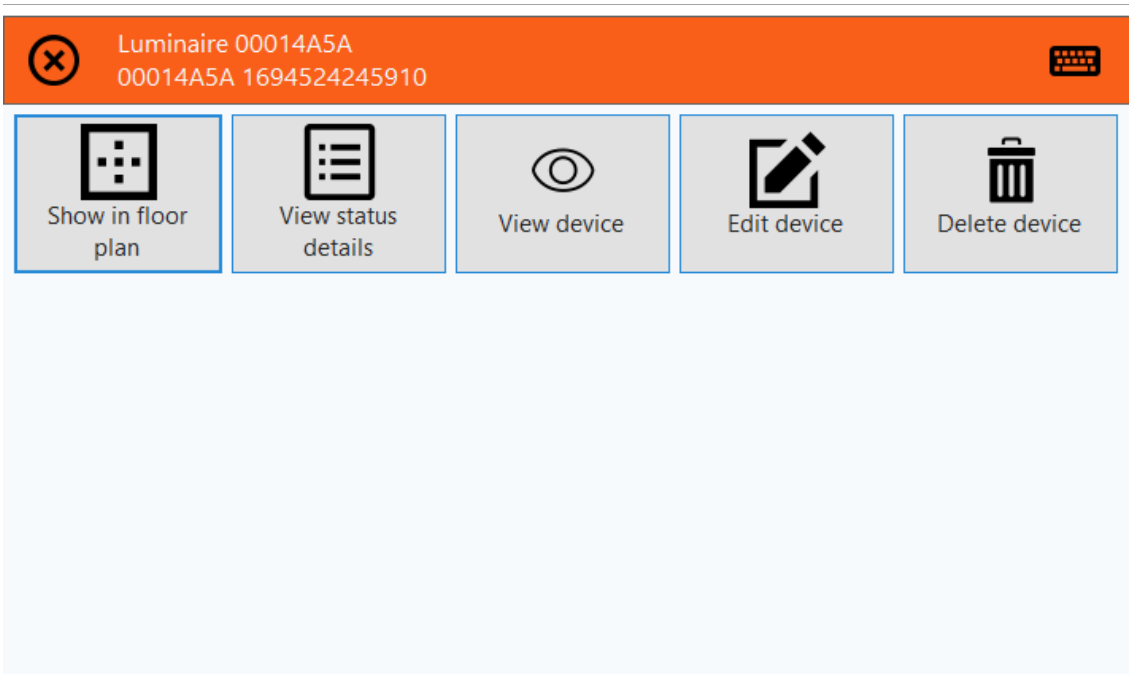
- Luminaire in test

3.1.3. Current events

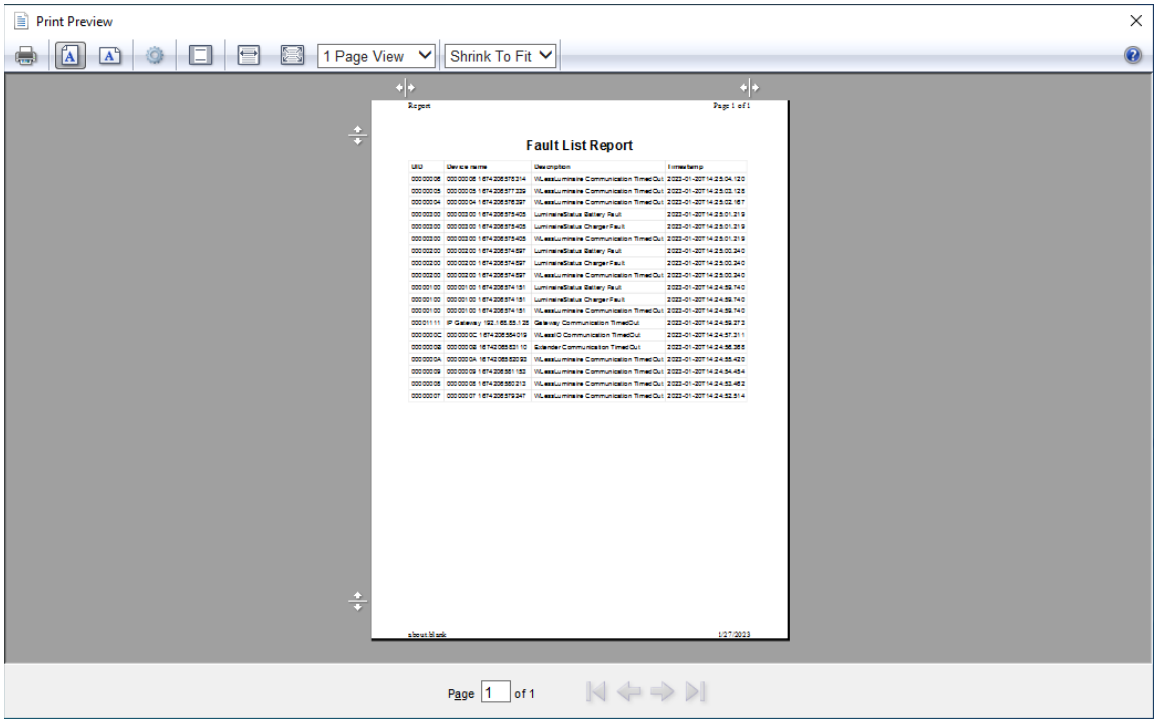
This chapter describes the contents of the Current events menu screen. These include the complete list of the software's current events, such as faults encountered by the system, and a series of options such as printing, exporting, viewing additional options, and searching. The following image shows the menu's basic elements.



Clicking on **Details form**, which is the leftmost icon of the top bar, or double-clicking on a row, opens a window with additional options.

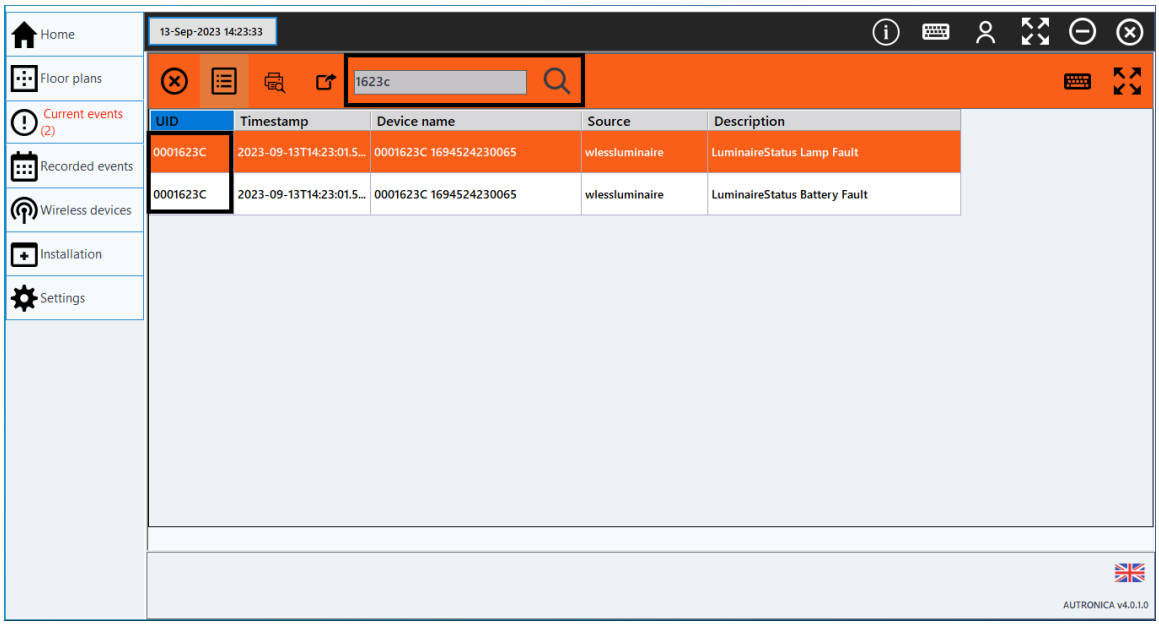


Clicking on **Print preview** opens a window that allows the user to view and slightly configure the way this menu's content will be printed.



Clicking on **Event export** a list in HTML format will export it locally to your pc.

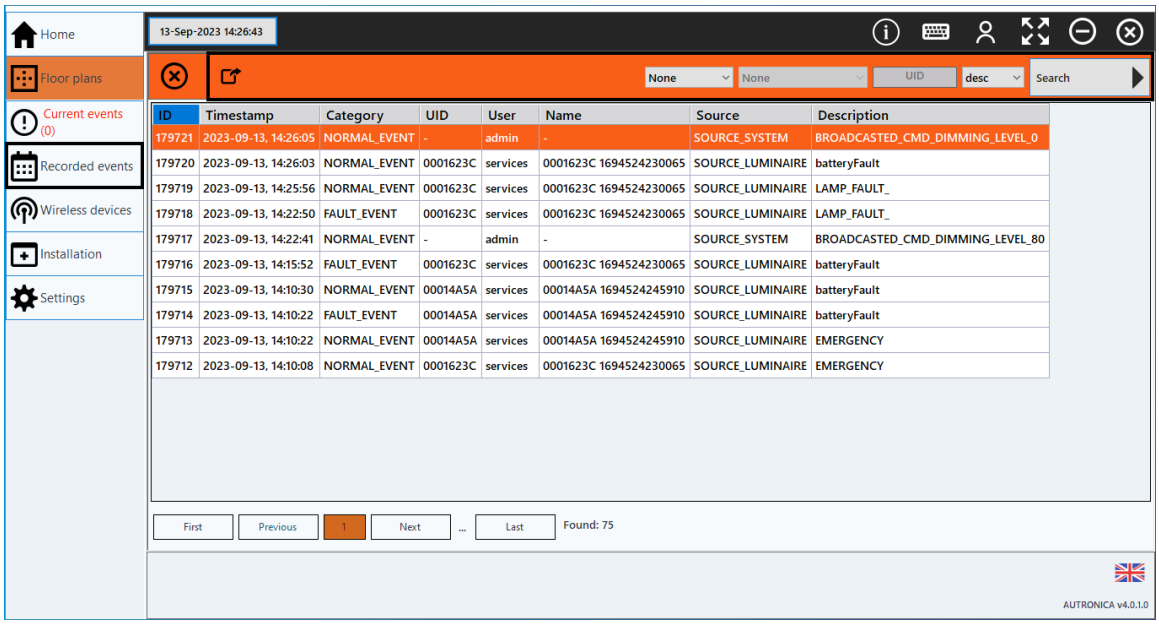
The search field and button, in the following image, allow the user to search the UID list for certain devices. In order for the complete list to be displayed again, the user has to erase the field's contents and press the button.



3.1.4. Recorded events

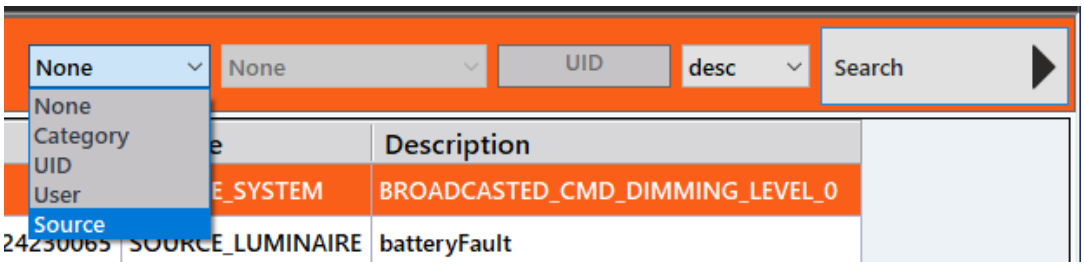
This menu screen allows the user to view the software's recorded events inside a complete or filtered for a more focused results list. The recorded events include user sign-ins, system commencements and shutdowns, encountered faults in the software or hardware, and executed tests among others, since the installation of the application to the present time.

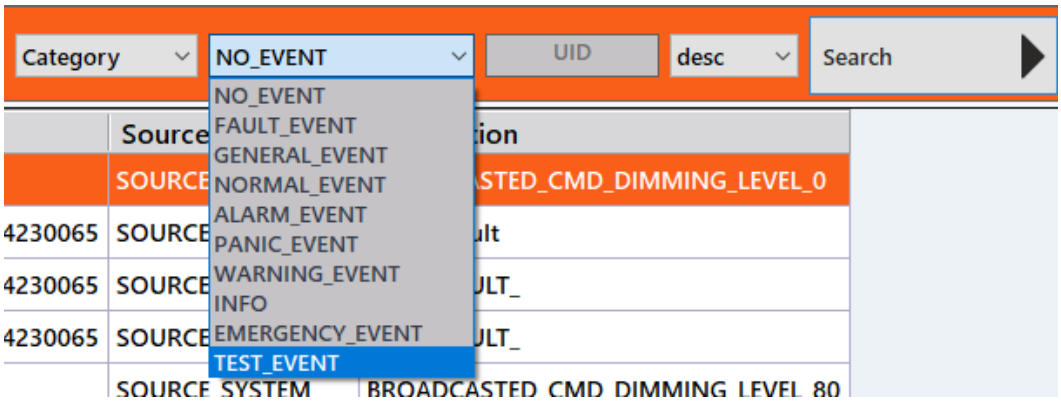
The following screenshot highlights the Recorded events screen's basic elements. The list of events, export in HTML file and filter that can be applied for greater specificity.

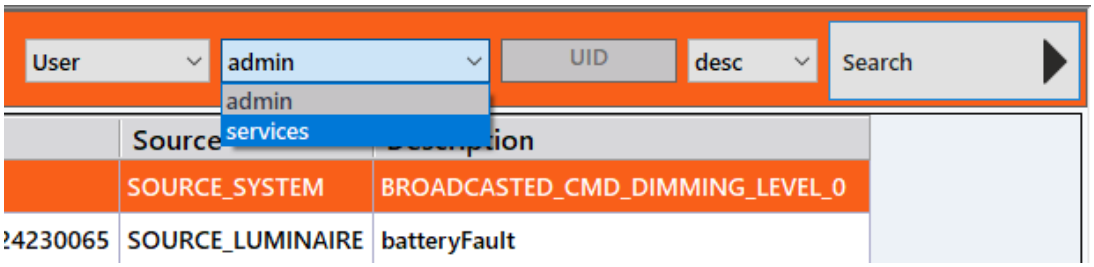


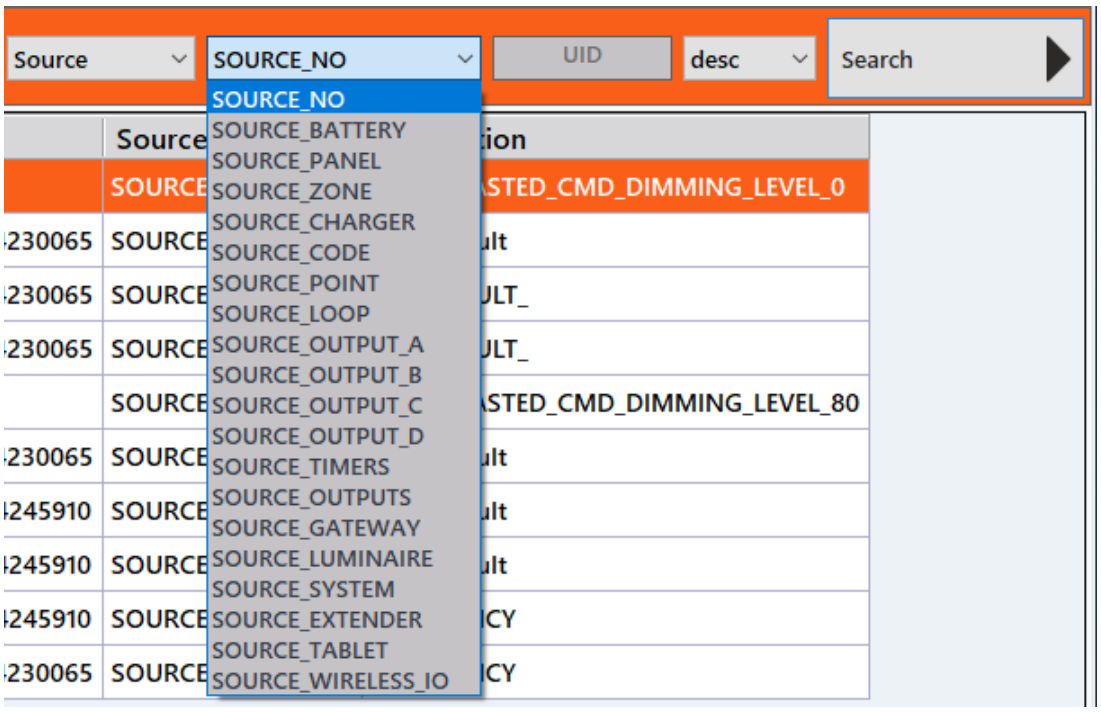
You can sort the events by category, by user or admin, by source or you can search for a specific device by UID.

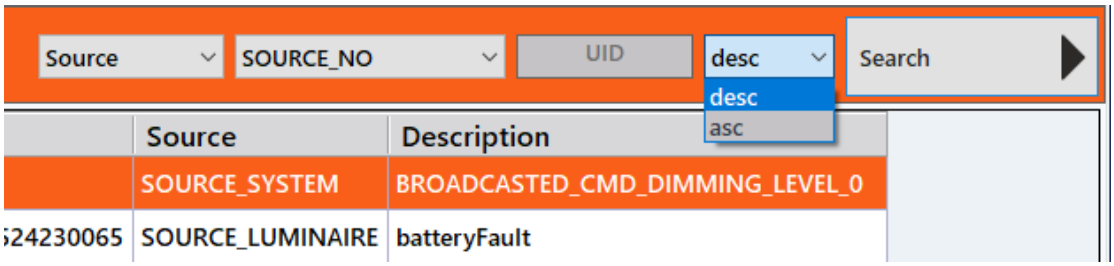
Below are all the available ways to short and search the events.




Category
NO_EVENT
UID
desc
Search
NO_EVENT
FAULT_EVENT
GENERAL_EVENT
NORMAL_EVENT
ALARM_EVENT
PANIC_EVENT
WARNING_EVENT
INFO
EMERGENCY_EVENT
TEST_EVENT
Source
SOURCE
4230065
SOURCE
4230065
SOURCE
4230065
SOURCE
SOURCE_SYSTEM
STED_CMD_DIMMING_LEVEL_0
ult
ULT_
ULT_
BROADCASTED_CMD_DIMMING_LEVEL_80

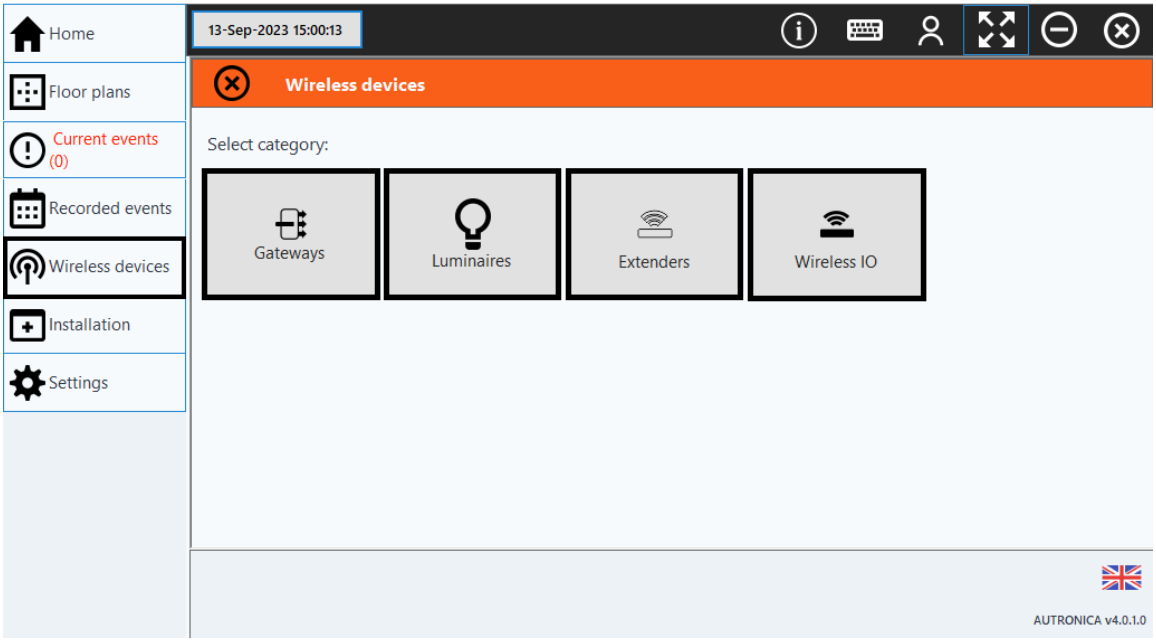

User
admin
UID
desc
Search
admin
services
Source
SOURCE_SYSTEM
BROADCASTED_CMD_DIMMING_LEVEL_0
4230065
SOURCE_LUMINAIRE
batteryFault


Source
SOURCE_NO
UID
desc
Search
SOURCE_NO
SOURCE_BATTERY
SOURCE_PANEL
SOURCE_ZONE
SOURCE_CHARGER
SOURCE_CODE
SOURCE_POINT
SOURCE_LOOP
SOURCE_OUTPUT_A
SOURCE_OUTPUT_B
SOURCE_OUTPUT_C
SOURCE_OUTPUT_D
SOURCE_TIMERS
SOURCE_OUTPUTS
SOURCE_GATEWAY
SOURCE_LUMINAIRE
SOURCE_SYSTEM
SOURCE_EXTENDER
SOURCE_TABLET
SOURCE_WIRELESS_IO
Source
SOURCE
230065
230065
230065
SOURCE
230065
245910
245910
245910
230065
STED_CMD_DIMMING_LEVEL_0
ult
ULT_
ULT_
STED_CMD_DIMMING_LEVEL_80
ult
ult
ult
CY
CY


Source
SOURCE_NO
UID
desc
desc
asc
Search
Source
Description
SOURCE_SYSTEM
BROADCASTED_CMD_DIMMING_LEVEL_0
524230065
SOURCE_LUMINAIRE
batteryFault

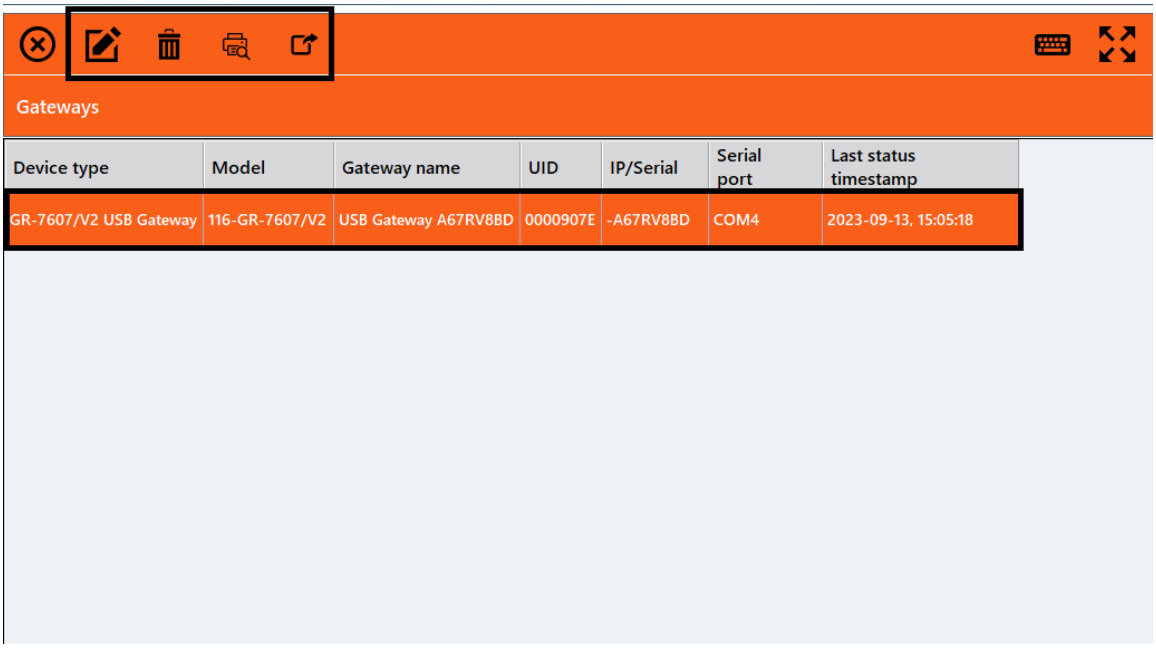
3.1.5. Wireless devices

This menu allows the user to choose from among 4 categories of devices.



These 4 categories represent every wirelessly connected device that can be supported by the software and include gateways, luminaires, extenders and wireless IOs. The previous image displays the basic elements that comprise the menu.

The user may click on any one category to access a list of that specific category's devices that are monitored by the application. The following image depicts the window that lists all the gateway devices. All the other menu is similar.



The user consequently may select a device from the list and access various menus through the options of the top bar.

The leftmost option allows the user to edit the selected gateway, in exactly the same way as described earlier in chapter 3.1.1.1. Gateways.

The next option enables the user to delete the selected gateway by first opening a window that effectively asks for the user's confirmation to delete the device.

The user may also select the **Print preview** option to open a preview window and subsequently print a report of the devices' faults. They may finally choose to export the report within a local file through the **Event export** option.

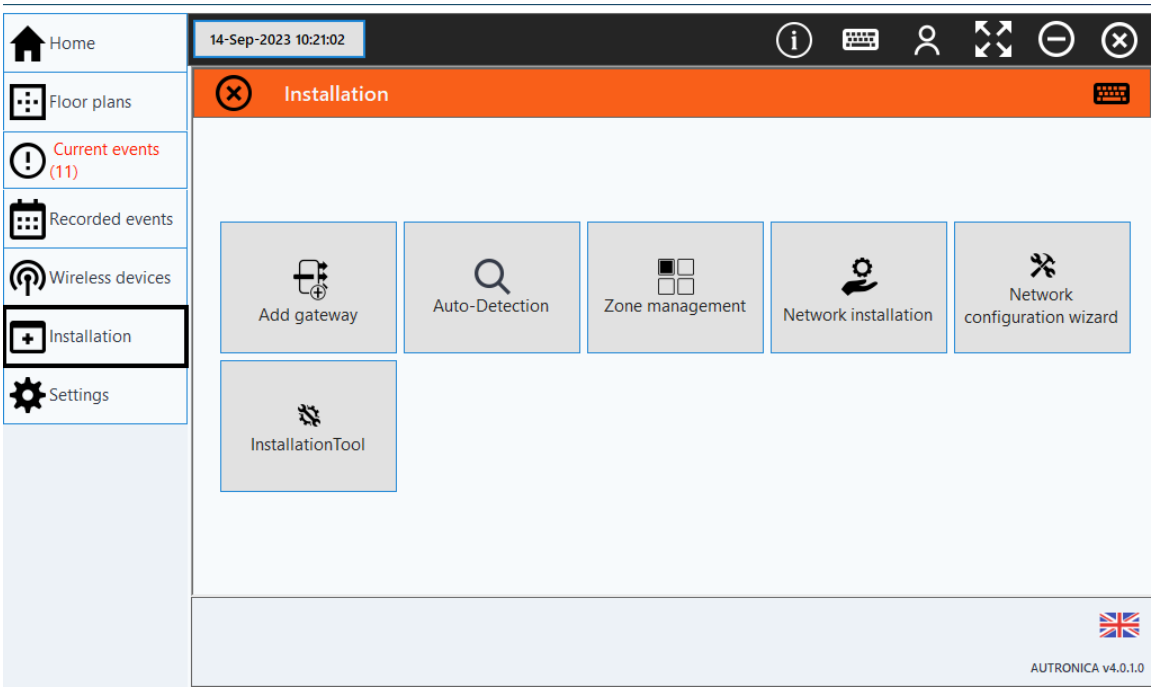
Gateways within the list may also be double-clicked to open a window with details about the status of the device. This window is the same as the one accessed through different menus. Additional options also become available through this window and are discussed at length in chapter 3.1.1.1. Gateways.

Beginning from the leftmost icon of the highlighted top bar seen in the image above, the user can edit a selected device from the list.

3.1.6. Installation

The Installation menu constitutes the most basic step in the initial setup by providing an initial point of reference while configuring the hardware setup for the first time, and also an important tool for any future changes in the networking of the devices. It enables the user to manually add a gateway device, automatically detect all the other connected devices, assign the luminaires to a preferred zone of operation – a zone of operation could represent a dedicated section of the building layout, such as an entire floor – and a separate software **Wireless Installation Tool** that is installed along with the primary application. A detailed guide on how to further operate this tool will be included in sub-chapter 3.1.6.3.

The following image provides an overview of the options within the menu.



There are additional options such as a **Network configuration wizard** and **Network installation**, but the user is advised to only use the **Installation tool** to configure the luminaires and assign them to their own network.

The **Network configuration wizard** can be used in case you have only one gateway to the installation.

3.1.6.1. Add gateway

3.1.6.1.1. Ethernet/Wi-Fi gateway

Gateway devices are used for the connectivity of all wireless devices and serve as the primary bridge between these devices and the server API which in turn

serves as the main communication point among the wireless devices, the UI and the database.

The user may access the **Add gateway** option in order to manually add a gateway device to the system. This option should apply to all gateways that are connected to the system through an ethernet cable or WIFI.

Firstly, specialized technicians must connect the power cables to the gateway. Be careful the power for the gateway is 220-240V AC/50HZ

Secondly, the user should connect the gateway device to a network switch, as it needs to be within the same network as the computer that initiates the configuration.

Thirdly, the user may access this menu, in order to add a gateway to the system.

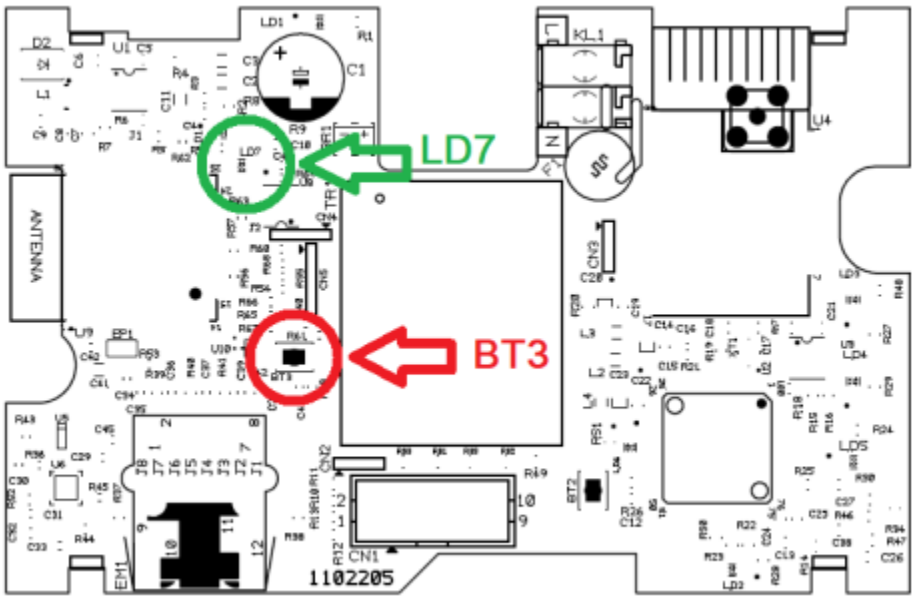
The **Wireless Network Master Ethernet/Wifi** gateway implements both Wi-Fi and Ethernet connectivity capabilities and is compatible both with the standard and the advanced version of this software. The device requires an active network to connect with the main computer, which must be within the same subnet.

This gateway can monitor up to 200 wireless devices, including wireless emergency luminaires, extenders, and input/output units forming a single wireless network. The communication between the gateway and the computer can be established with any one of the following ways: via ethernet – wired connection (DHCP, or static IPv4), via Wi-Fi – WPA2/PSK (DHCP, or static IPv4), and via Wi-Fi – WPS.

After initiation an invitation from the software to enable the gateway, as shown in the previous image, the user needs to configure the device in order to connect to

the local network. The gateway's front cover needs to be opened to expose the main board.

Inside of the front cover there is a sticker with the MAC address. There is a different MAC address for the ethernet and WIFI connection.



The user then needs to press the **BT3 button** located on the left part of the board for ten (10) seconds, while avoiding touching other areas of the circuitry. The **LD7 green LED** will start blinking two (2) times per second, indicating the Wi-Fi access point is running. This indication effectively notifies that the gateway serves as a hotspot for the user to connect to.

In order to connect to the gateway, the user will need a device that supports Wi-Fi, i.e., a smartphone, laptop, or a tablet. They will need to find the point with the following SSID: **WIRELESS_LIGHTING_GATEWAY** and use the following password to connect: **WIRELESSGW**.

When their device is connected to the gateway's access point, they may open a web browser and navigate to the following address: **192.168.1.1**, to reach the webpage depicted in the following image.

Connectivity via Ethernet: In order to connect the **GR-7603/V2** gateway to the local network, the device must first be connected to the local network using a UTP network cable with an RJ45 male connector and to the corresponding RJ45 port located at the bottom of the device.

Within the **IP static** field, a static IPv4 address for this device needs to be entered. If left empty, a dynamic (DHCP) address will be assigned.

Within the **NETMASK** field, the network's desired mask in case of usage Static IP.

Within the **GATEWAY IP** field, the gateway's IP address may optionally be entered.

Next, the main computer's – the computer that is hosting the GR-7600/V2 - WelReceiver service – IPv4 address must be inserted in the **IP Master** field. The rest of the fields may be left empty.

Finally, the user may select the **Ethernet** option from the bottom of the webpage and submit the form.

Connectivity via Wi-Fi (WPA2/PSK): To connect the device with the local network, a Wi-Fi (802.11 b/g/n) network with WPA2/PSK security must be active and within range. The gateway will join the network as a client.

Within the **WiFi SSID** field, the SSID (name) of the Wi-Fi network the gateway will join must be entered. The name is case-sensitive.

Within the **WiFi PSWD** field, the WPA2/PSK password must be entered.

Within the **IP static** field, the IPv4 address for this device needs to be entered. If left empty, a dynamic (DHCP) address will be assigned.

Within the **NETMASK** field, the network's desired mask in case of usage Static IP.

Next, the main computer's – the computer that is hosting the GR-7600/V2 - WelReceiver service – IPv4 address must be inserted in the **IP Master** field.

The user may then select the **WiFi** option from the bottom of the webpage and submit the form.

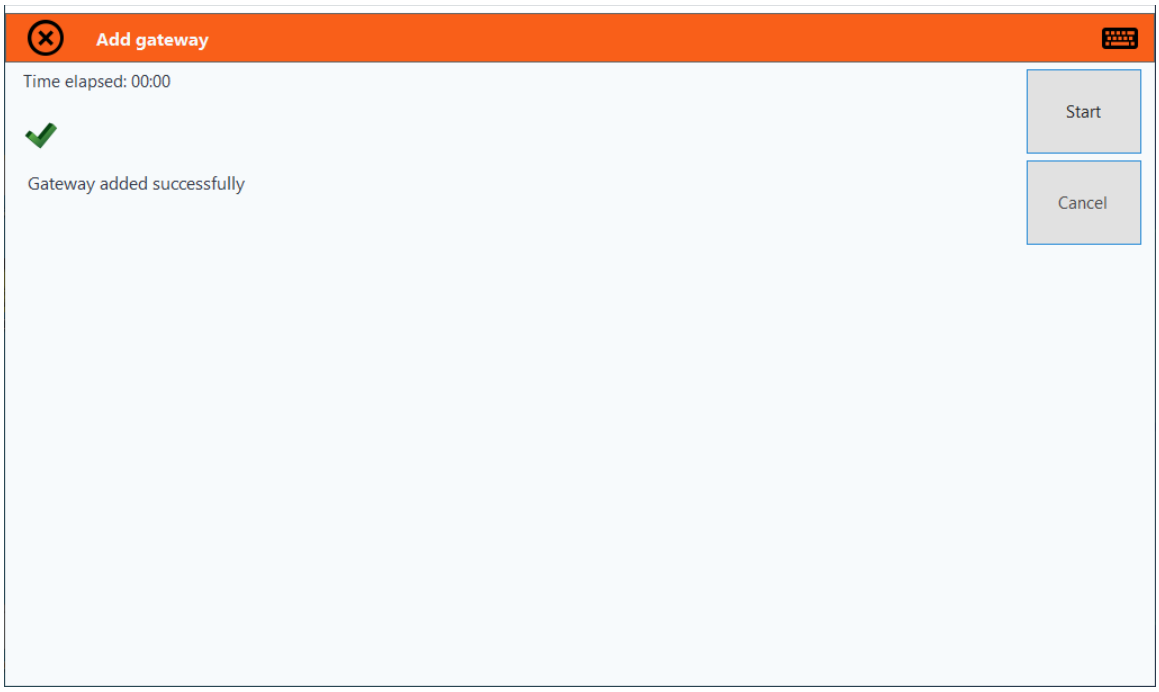
Connectivity via Wi-Fi (WPS): To connect the device with the local network, a Wi-Fi (802.11 b/g/n) network with the WPS feature must be active and within range. The gateway will join the network as a client.

The main computer's – the computer that is hosting the GR-7600/V2 - WelReceiver service – IPv4 address needs to be entered in the **IP Master** field. The rest of the fields may be left empty.

Next, the user must have access to their Wi-Fi router and press the **WPS** button to enable a WPS invitation.

Afterwards, they may select the **WPS** option from the bottom of the webpage to submit the form.

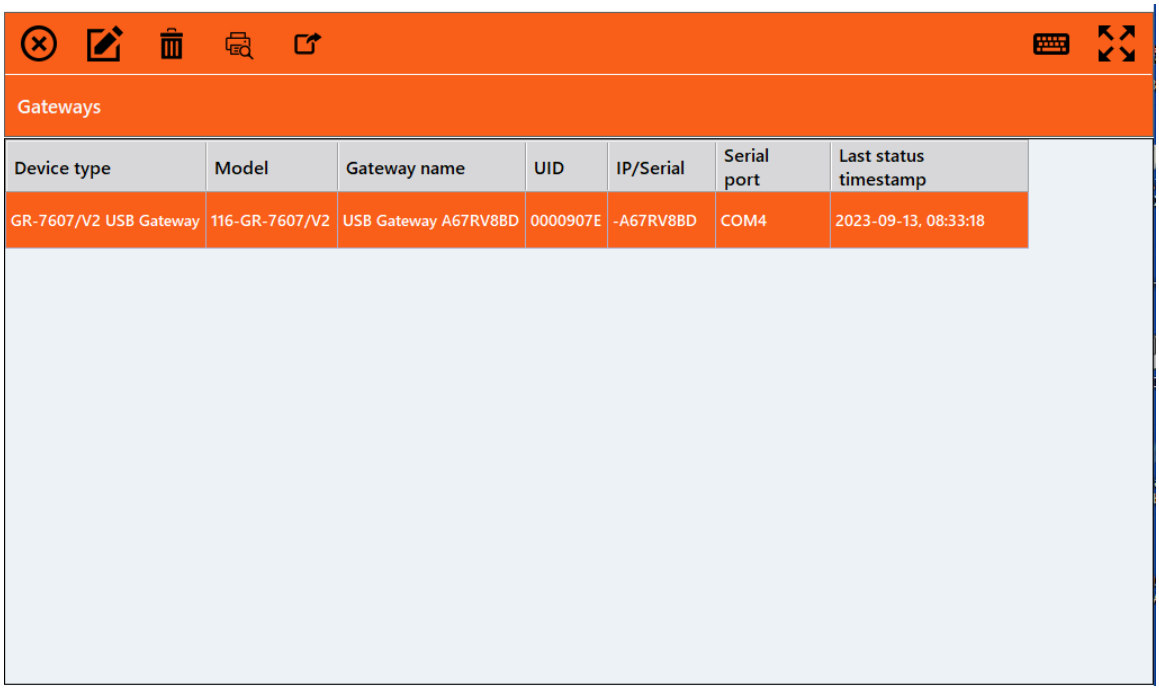
If, after using one of the previous connection methods, the connection is successful, the **LD7 green LED** will start blinking 1 time per second, indicating a successful connection.



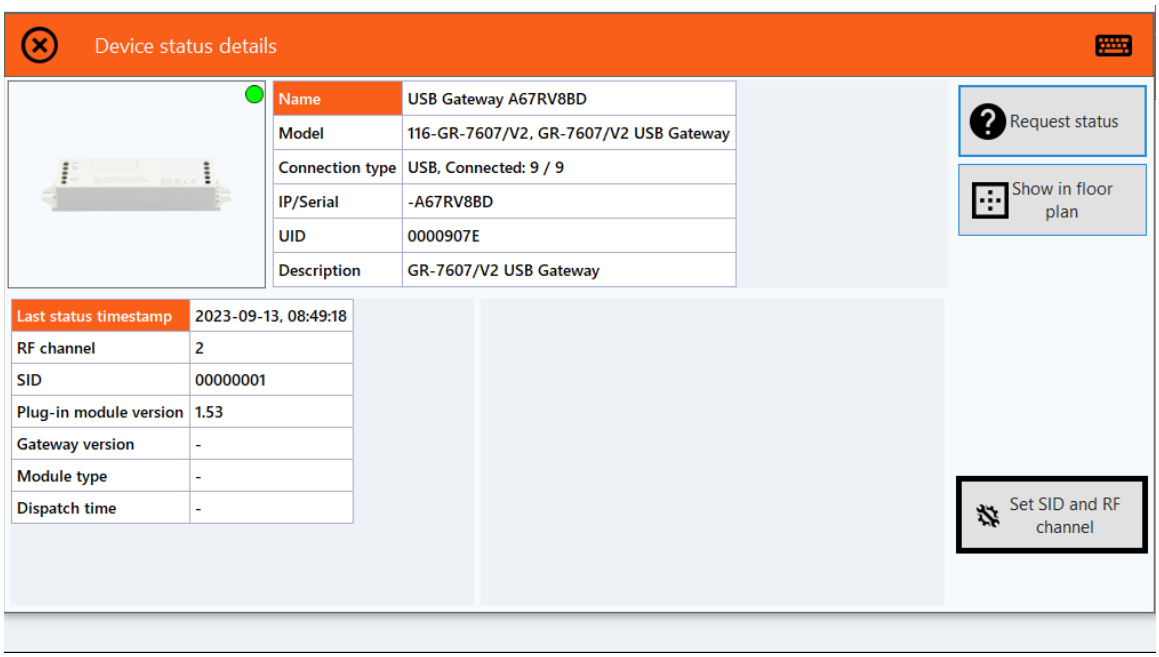
If the LD7 is steady lit, this means that the gateway cannot establish communication with the GR-7600/V2 software.

3.1.6.1.2. USB gateway

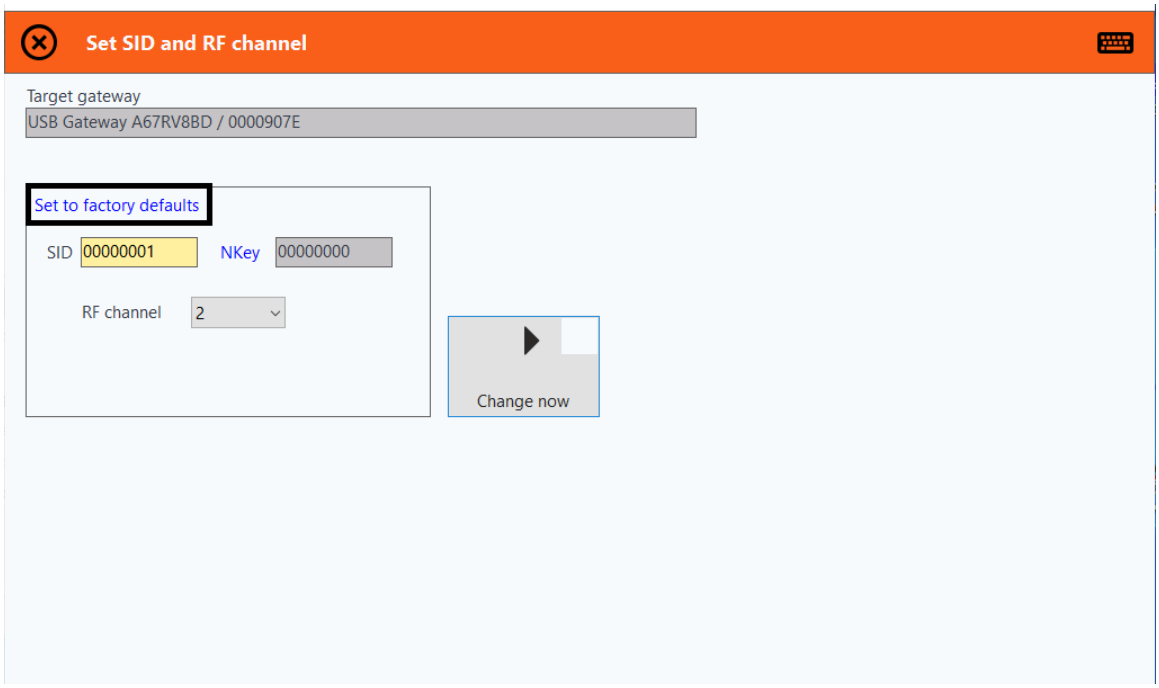
It should be noted that the user can also connect a gateway device through a USB cable. If a gateway is detected through one of the system's USB ports, no action is needed in order to add the gateway, as it is automatically detected and added. The user, however, is advised to navigate to the list of gateways and view the details of the new device's status.



Double-clicking on the new gateway device will display the status details.



If the device has been properly connected and identified by the system, then the user will notice a change in the gateway column of their Home screen, as well as notice the **Online** indication within the device's status details.

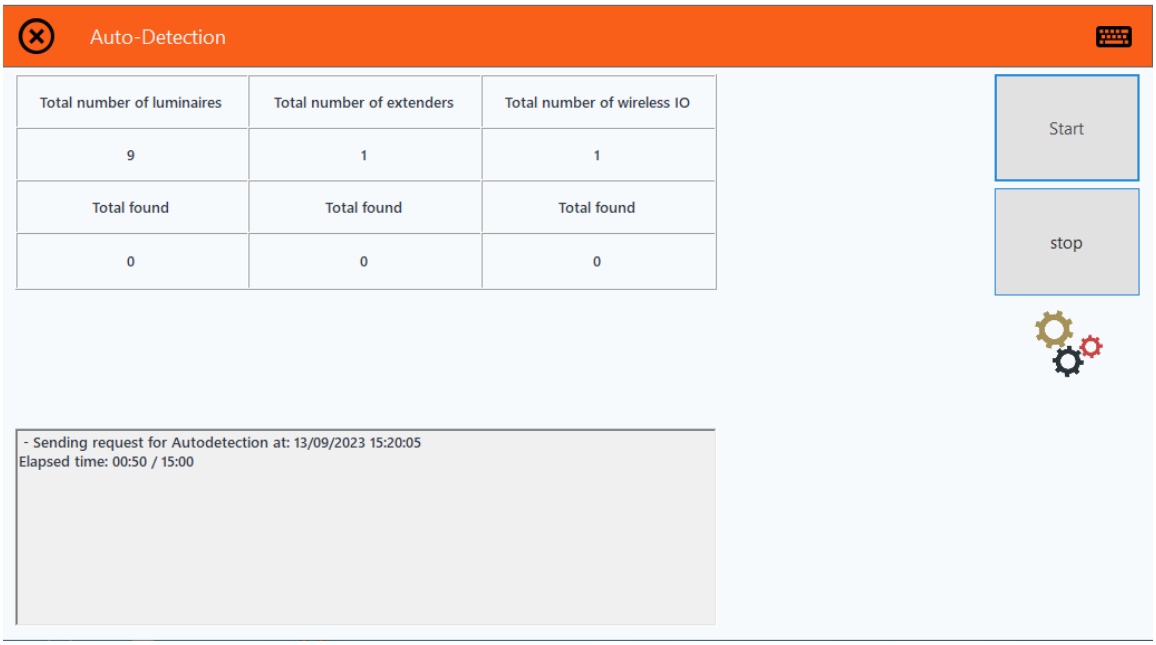


The user can configure the SID and RF channel of the gateway in order to change the network of the device. The initial network of a new, unconfigured gateway is the default network and it is recommended that the user assign the device to a different local network.

3.1.6.2. Auto-detection

The user can access this option automatically detect all of the unregistered connected wireless devices. After the procedure has finished, all unregistered wireless devices will automatically be registered to an available gateway. The devices will be connected to the gateway with the same parameters (SID, Channel, NKEY). This procedure should naturally be initiated only after ensuring that all the wireless devices have been correctly connected to the main power supply network, as per the instructions given the installation guide included in sub-chapter 3.1.6.6.2.

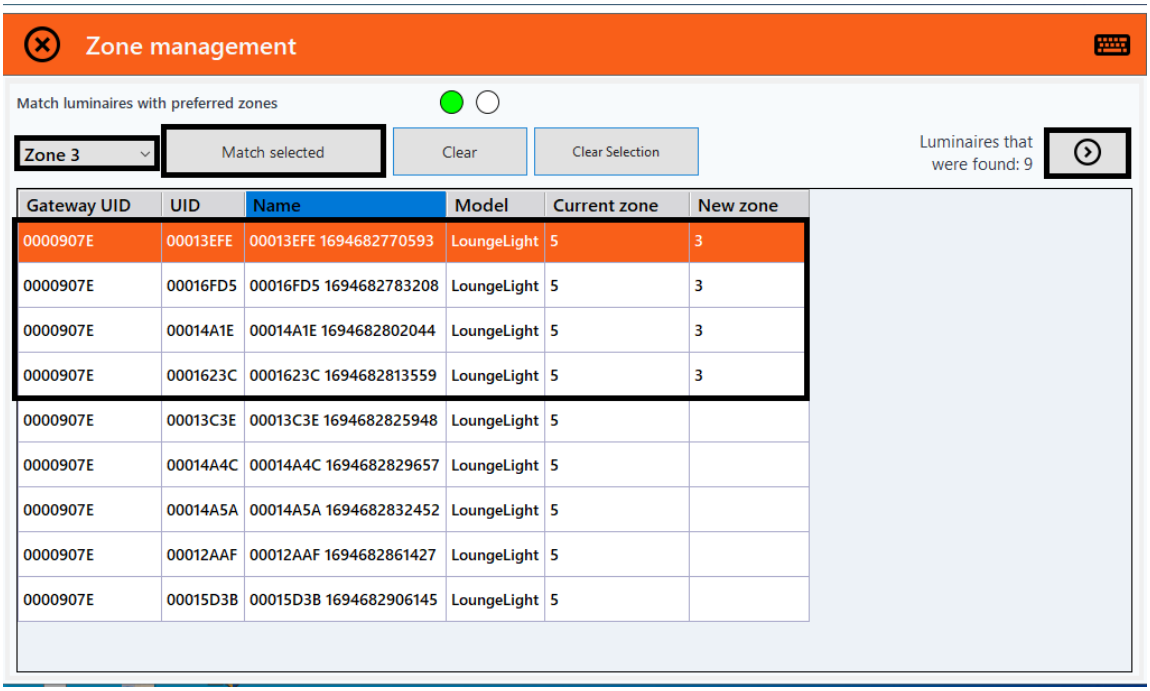
This procedure is recommended if the user does not wish to manually search and register each point independently.

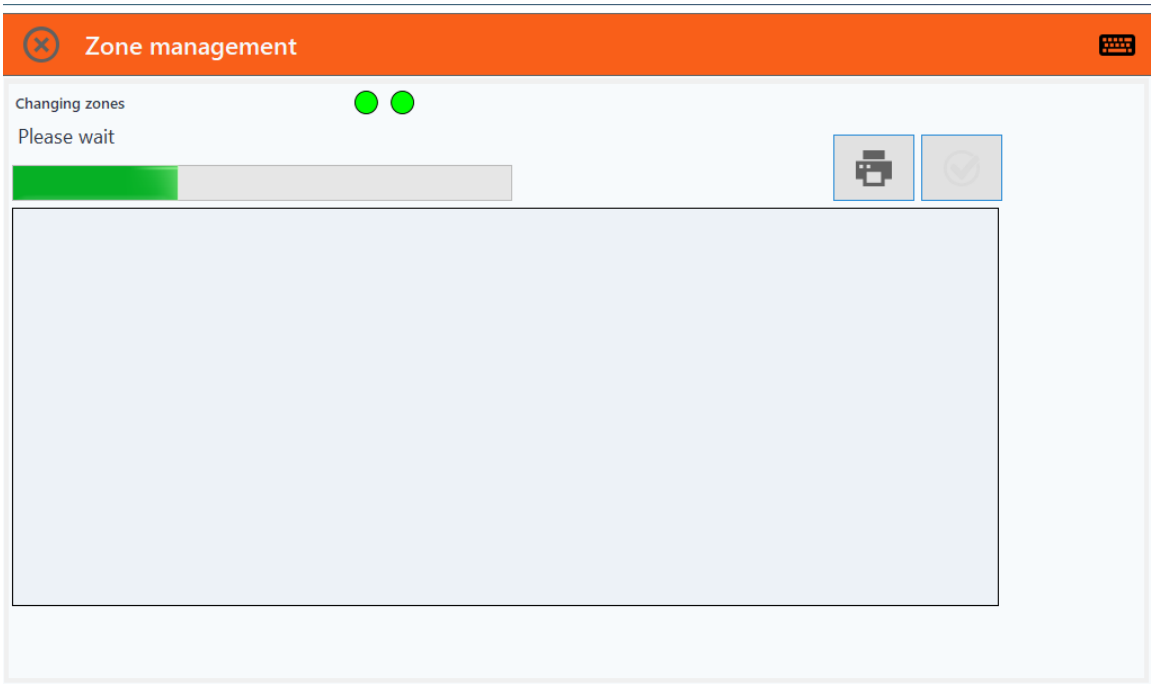


The maximum duration of the procedure is fifteen (15) minutes, after which it will display the number of all the detected wireless devices up to that point. The user may choose to terminate the procedure at any time, if they know the exact number of the wireless devices that need to be detected by the system. Should the user wish to connect additional devices in the future, they can follow the same procedure to detect the new devices.

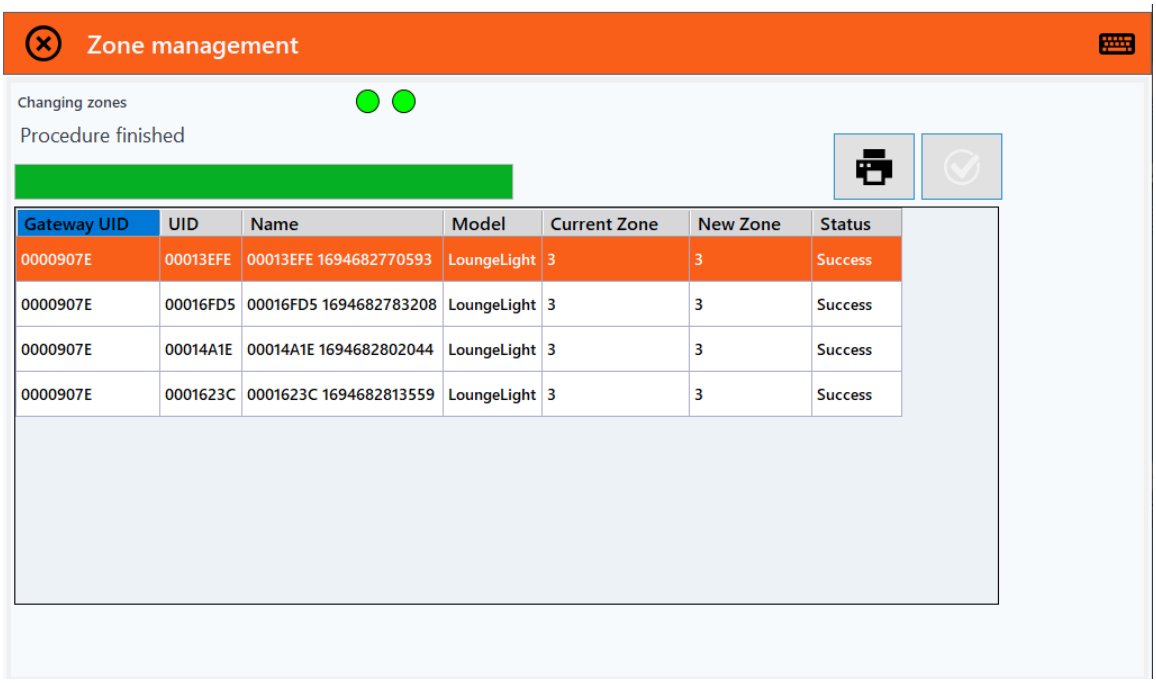
3.1.6.3. Zone management

The user can select this option in order to assign a single or multiple luminaires to a zone of operation. As described earlier, a zone assignment is useful particularly when the user needs to manage and send commands to luminaires that belong to a specific part of the installation site, such as the entire floor of a building.





Once the process finishes, an appropriate message will be displayed along with a list of all the zone changes that were directed by the user.



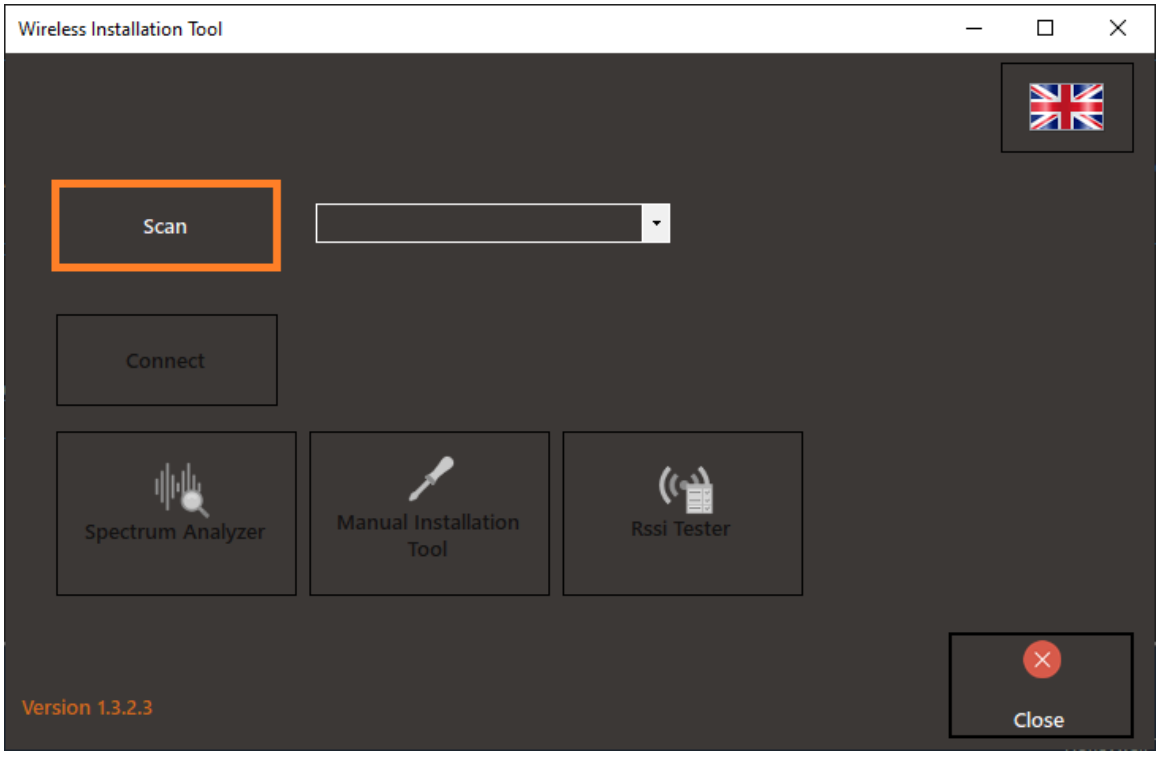
3.1.6.4. Installation tool (intended for USB gateways)

Installation tool is an external application tool that is installed alongside the main software. It is the basic way of configuring all of the installed wireless devices. After all wireless devices have been connected to the main power, in order to configure the network of the wireless devices the user needs to connect a USB gateway.

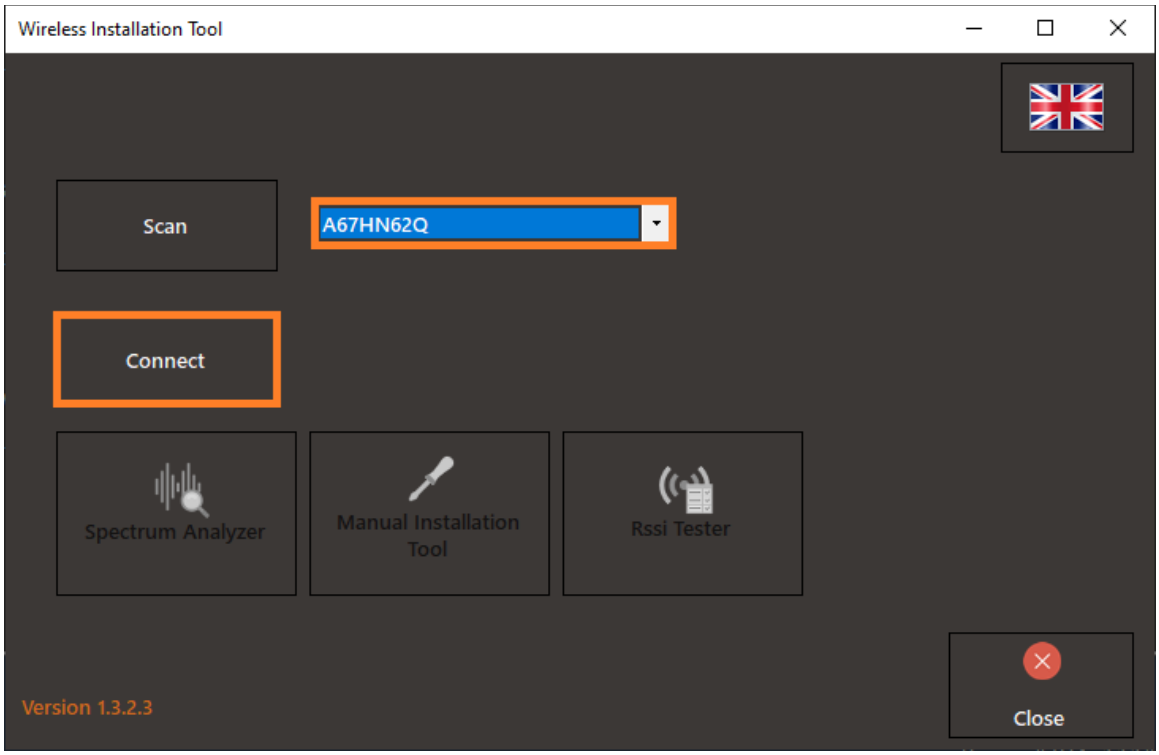
This gateway, once connected, serves as a regular gateway device. Accessing the installation tool ceases its gateway function and the gateway can be used as a Spectrum Analyzer, a Manual Installation Tool, or an RSSI Tester.

If the main computer on which the primary software is installed is stationary and not within range of every powered device, then preferably a laptop computer, running on Windows 10+, needs to be used in order to proceed with the setting up of the devices.

Firstly, the user needs to open the tool from the Installation menu and proceed to scan the network for a list with all available gateways.



When the scanning process is complete, the user may select a gateway and connect to it. It should be noted that while a gateway is connected to this software, it loses its connection with the primary software.

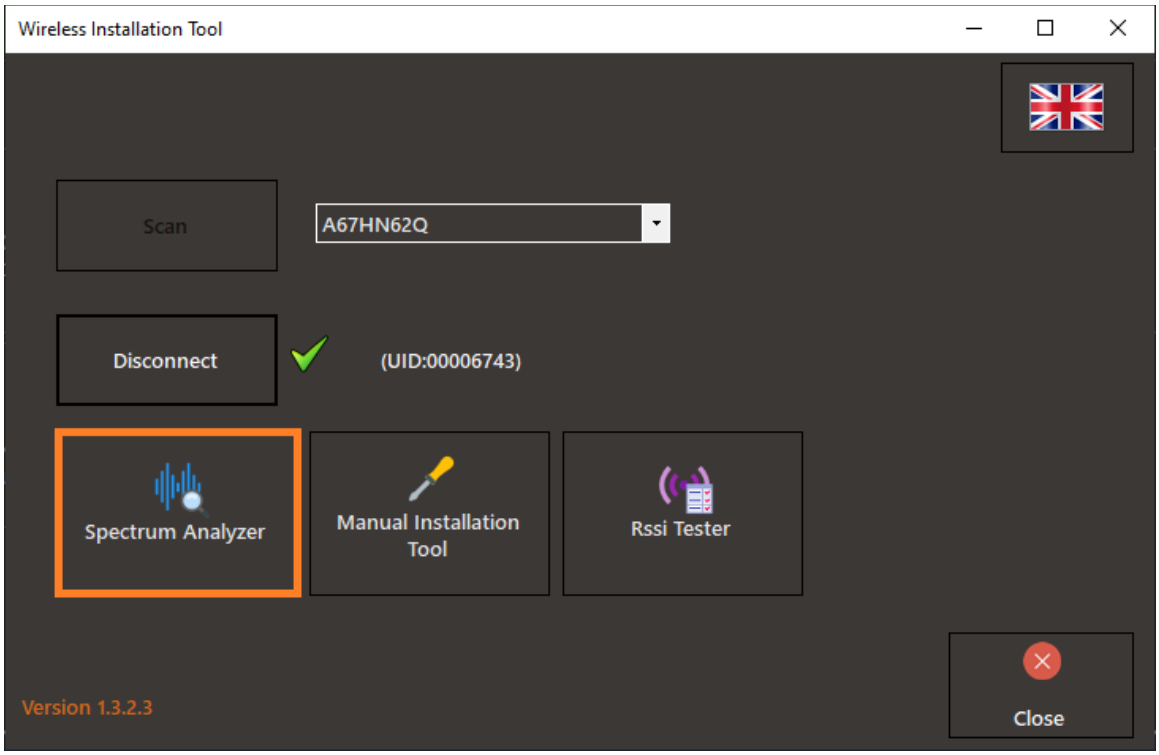


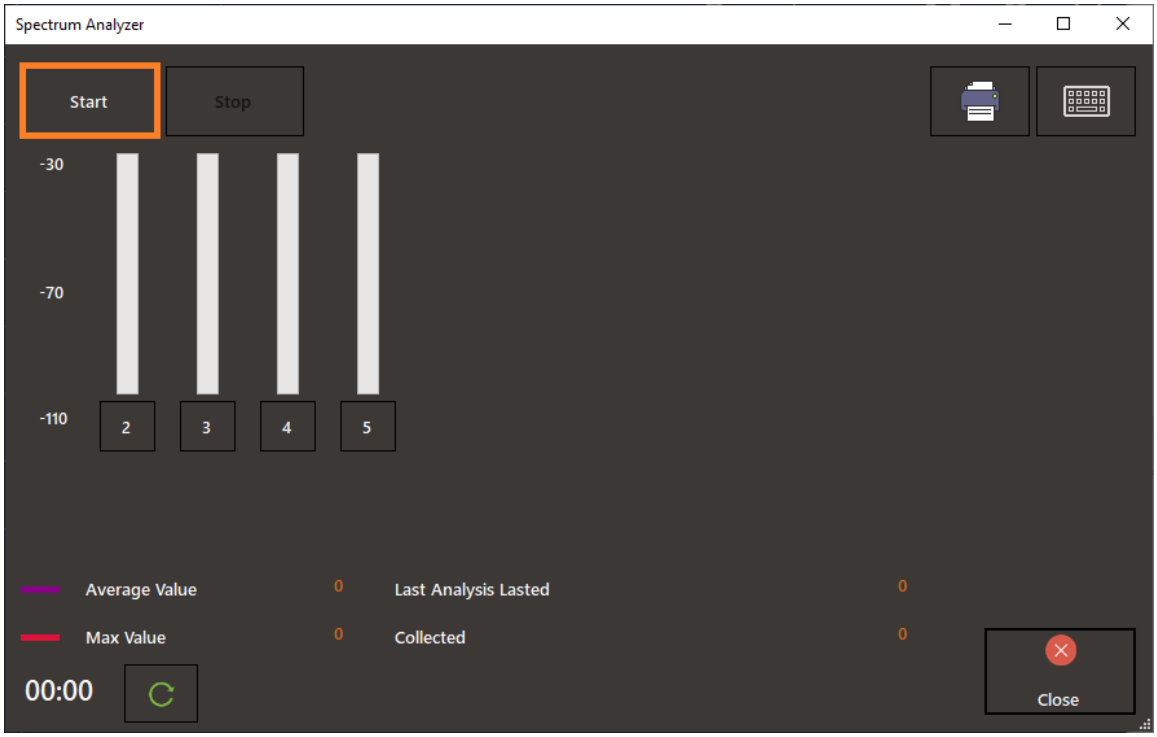
3.1.6.4.1. Spectrum Analyzer

In installation areas where other wireless systems operating at 868 MHz exist nearby, it is recommended to use the **Spectrum Analyzer** tool to scan for traffic on the 4 available RF Channels (frequencies). If there are no other wireless systems at 868 MHz nearby, this step should be skipped.

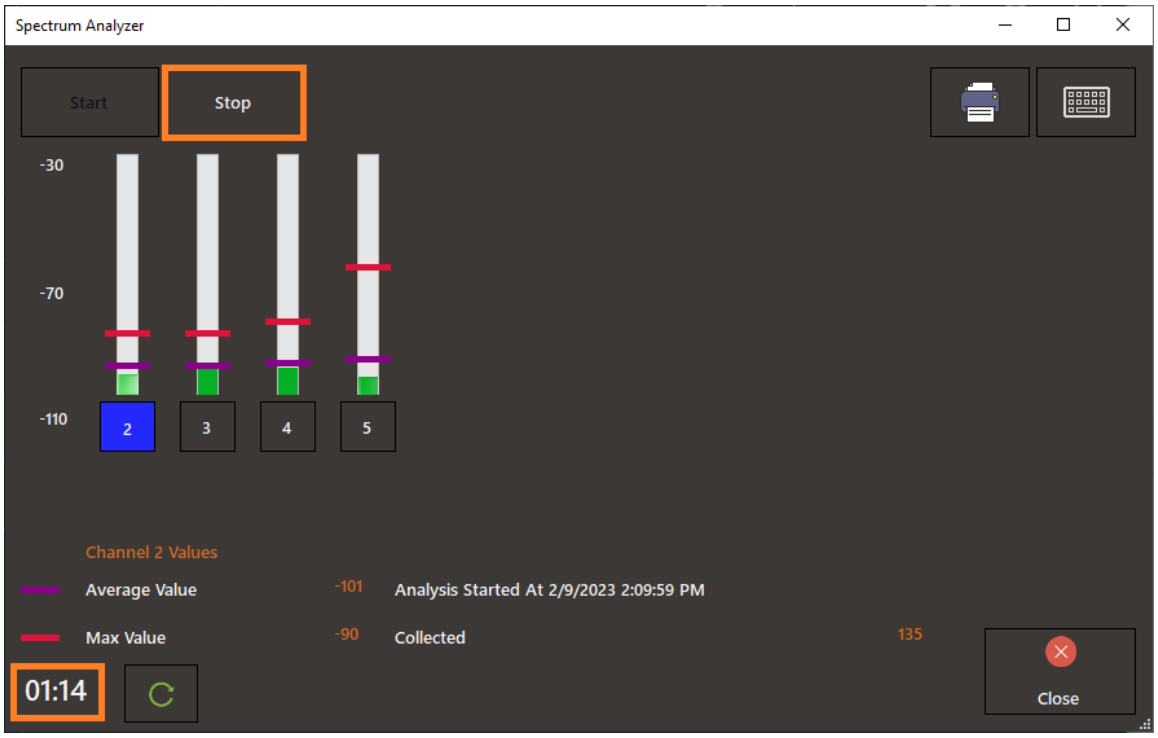
The available channels are 2, 3, 4, and 5, ranging from 868.150 MHz to 868.450 MHz. This tool scans these channels continuously while indicating the maximum and average measurement values for each.

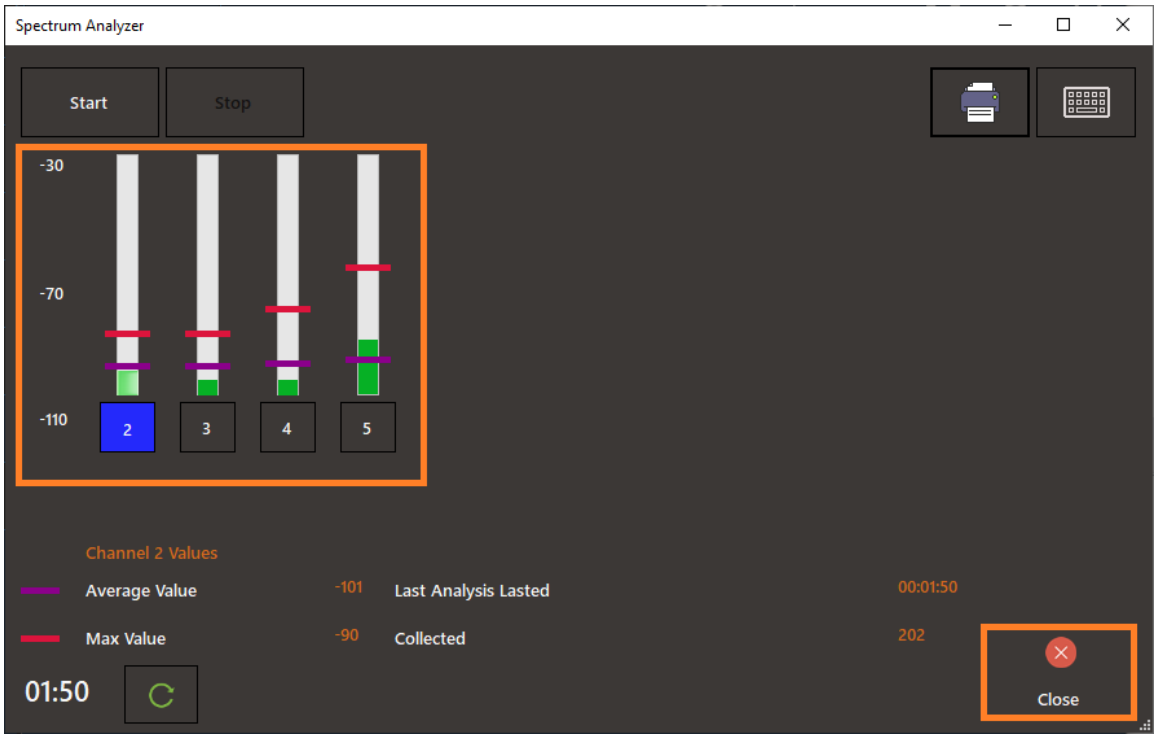
Firstly, the user, after connecting the device with the Installation tool, should select the **Spectrum Analyzer** option. Then, they may press on **Start** to run the procedure.





Each column indicates the measurements of the max and average values in dBm in red and purple colors respectively. The user should allow the procedure to run for at least 1 minute, according to the timer on the bottom-left of the new window.





It is recommended this test be run within various different areas of the installation for better results. For every different area the timer should be reset, and the procedure should run again for at least 1 minute. This process should be repeated until the entire area of a wireless network is covered.

For every installation area that is within an independent wireless network the entire procedure should be run anew, in order for the results to be more accurate about the occupied RF channels by area, and for the RF channels to be separated to avoid excessive channel usage.

It is noted that those RF channels that indicate high max and/or average values should be avoided during the network configuration. In the case of equal average values among channels, those with the lowest max values should be preferred.

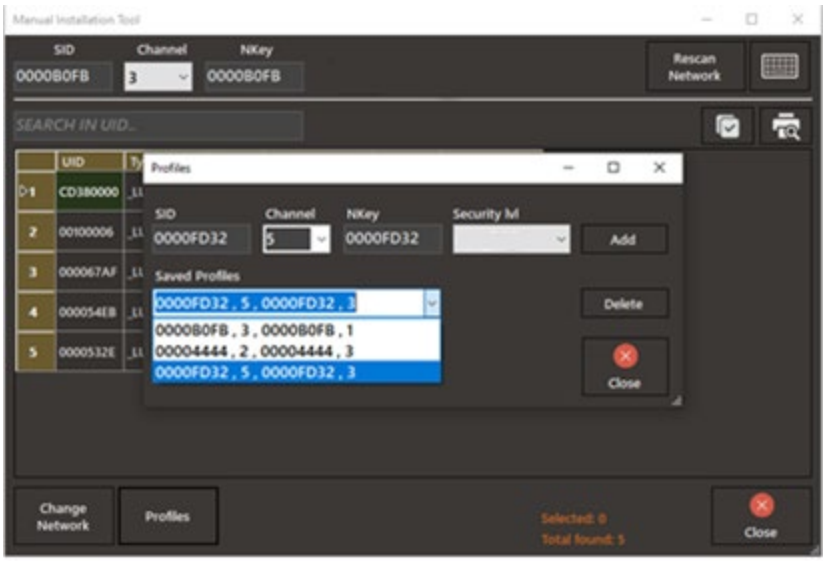
3.1.6.6.2. Manual Installation Tool – Step by step configuration

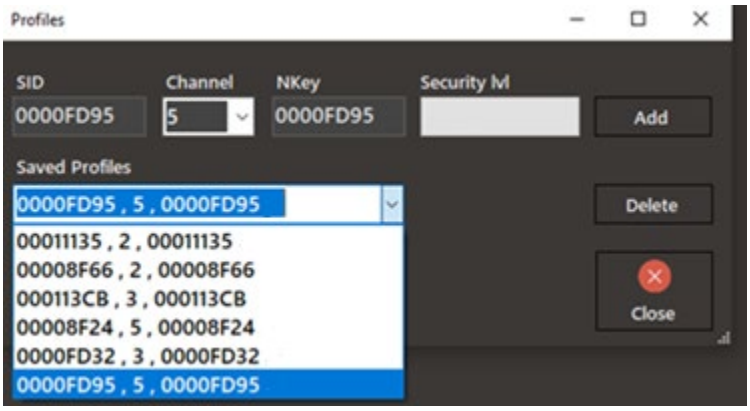
With the **installation tool** and the USB gateway you can separate and change each network's parameters (**SID, Channel, NKEY**) for every device. After the procedure is done, the luminaires will be connected to the proper gateway (**with same SID, Channel, NKEY**).

Power off all the gateways in the installation. Only the usb gateway must be enabled, which will be used with the installation tool for the commissioning.

A. Create a new network profile.

- Input the new **SID, RF channel, Nkey** and press **"Add"**.
  If you want to create more networks (profiles for other gateways) repeat this step. (You can create all the networks for all the gateways now or create them one by one after finishing setting up and connecting the luminaires to each one.)
- Press **"Close"** when you have finished with the new networks.

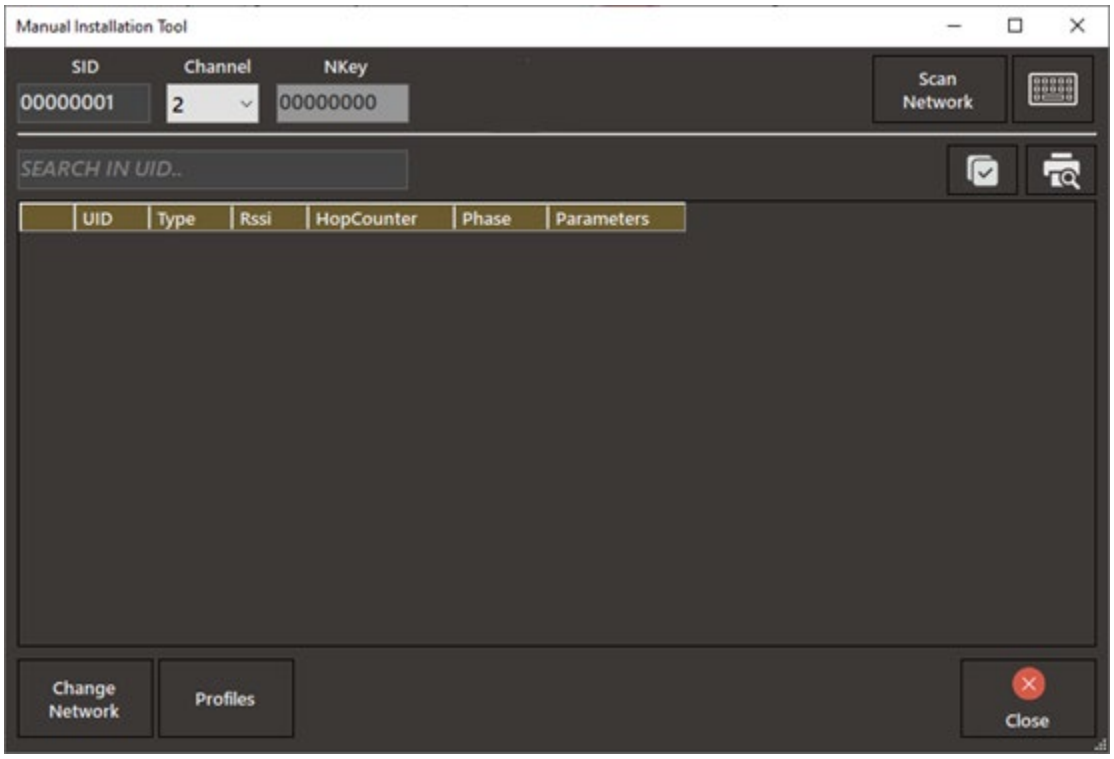

Manual Installation Tool
SID
0000B0FB
Channel
3
NKey
0000B0FB
Rescan Network
SEARCH IN UID..
UID
CD380000
00100006
000067AF
000054EB
0000532E
Profiles
SID
0000FD32
Channel
5
NKey
0000FD32
Security lvl
Add
Saved Profiles
0000FD32 , 5 , 0000FD32 , 3
0000B0FB , 3 , 0000B0FB , 1
00004444 , 2 , 00004444 , 3
0000FD32 , 5 , 0000FD32 , 3
Delete
Close
Change Network
Profiles
Selected: 0
Total found: 5
Close


Profiles
SID
0000FD95
Channel
5
NKey
0000FD95
Security lvl
Add
Saved Profiles
0000FD95 , 5 , 0000FD95
00011135 , 2 , 00011135
00008F66 , 2 , 00008F66
000113CB , 3 , 000113CB
00008F24 , 5 , 00008F24
0000FD32 , 3 , 0000FD32
0000FD95 , 5 , 0000FD95
Delete
Close

B. Scan the (default) devices

By default, your USB gateway will be in **default values (SID:00000001, Channel: 2, NKey:00000000)** which will already be pre-filled. Assuming that this is the first installation, all the lights will also be in the **default values.**

- On the top of the window, input (if not already pre-filled) the default **SID, RF Channel and NKey** values for the wireless network (USB gateway) that will scan the devices with those values (default luminaires).
- Click **'Scan Network'** to run the scan process. The response from all the devices with those network values may take up to 10 minutes.

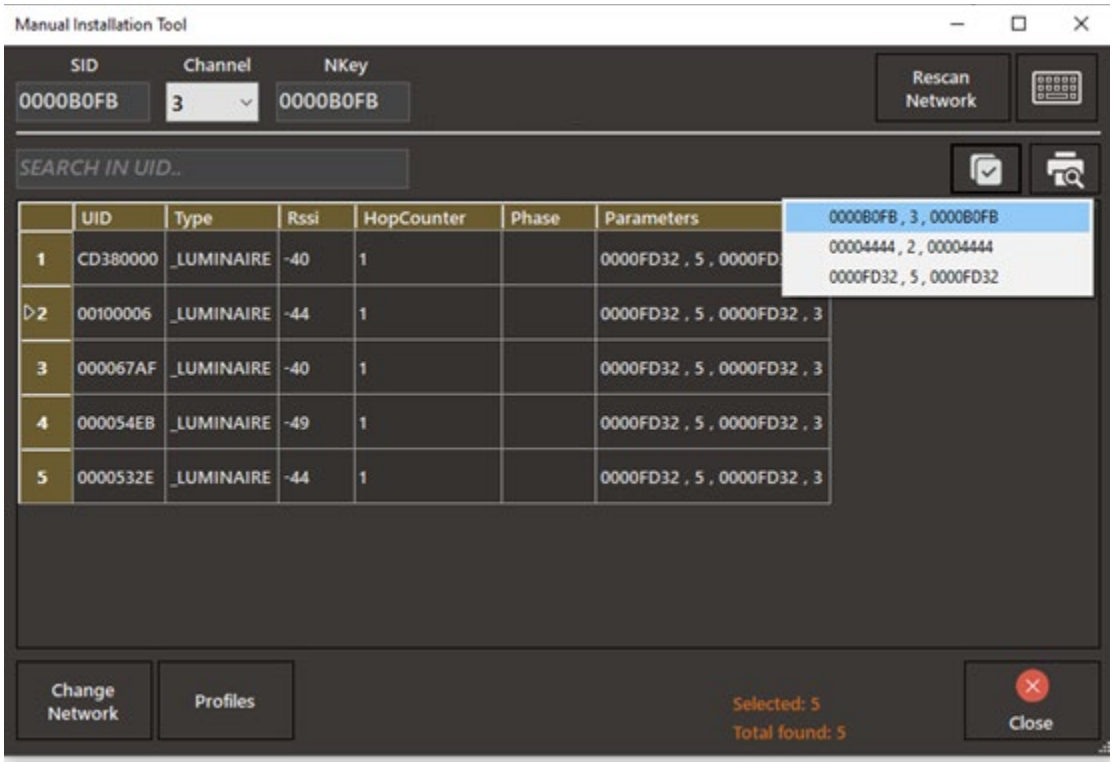


C. Pair the devices (luminaires) to the network (gateway)

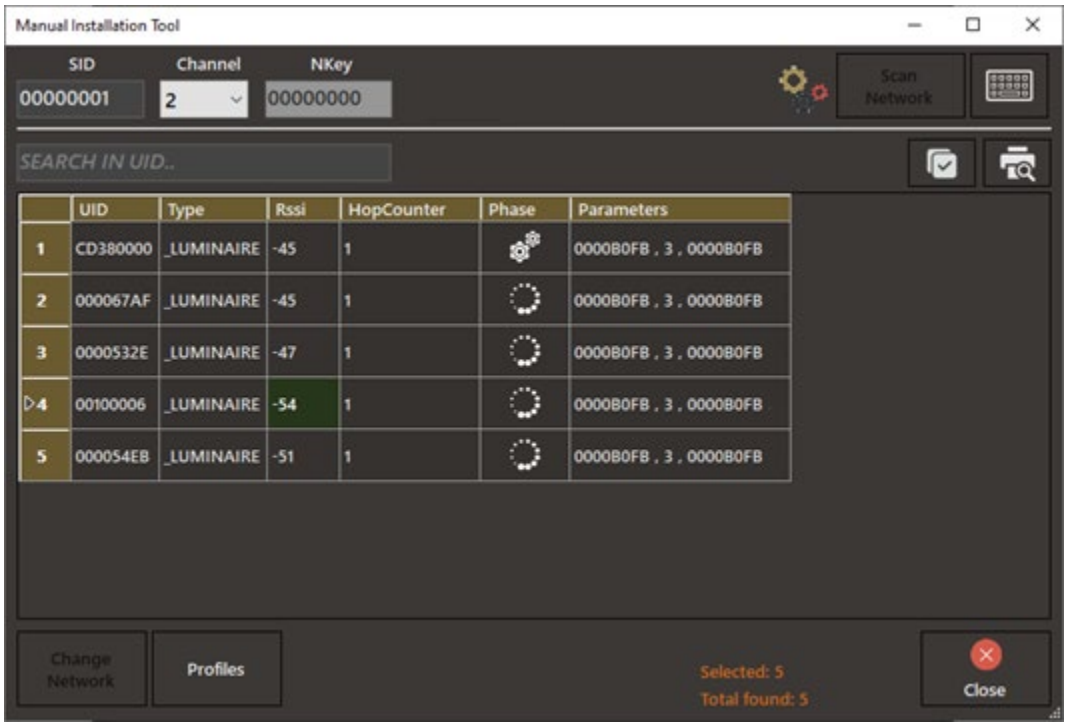
- Select the scanned devices one by one from the list, press right click and select the right profile to be assigned to.

This way you can separate and pair the devices in the correct gateway. In case you want to modify the whole list with the same parameters select the profile you want from the icon:

- **Once you are done selecting the network profiles for each luminaire, press "Change Network" to assign them to selected gateway.**



- Wait while the procedure is running (column “Phase” loading)



D. Pairing results

When the procedure finishes, check the column **“Phase”**.

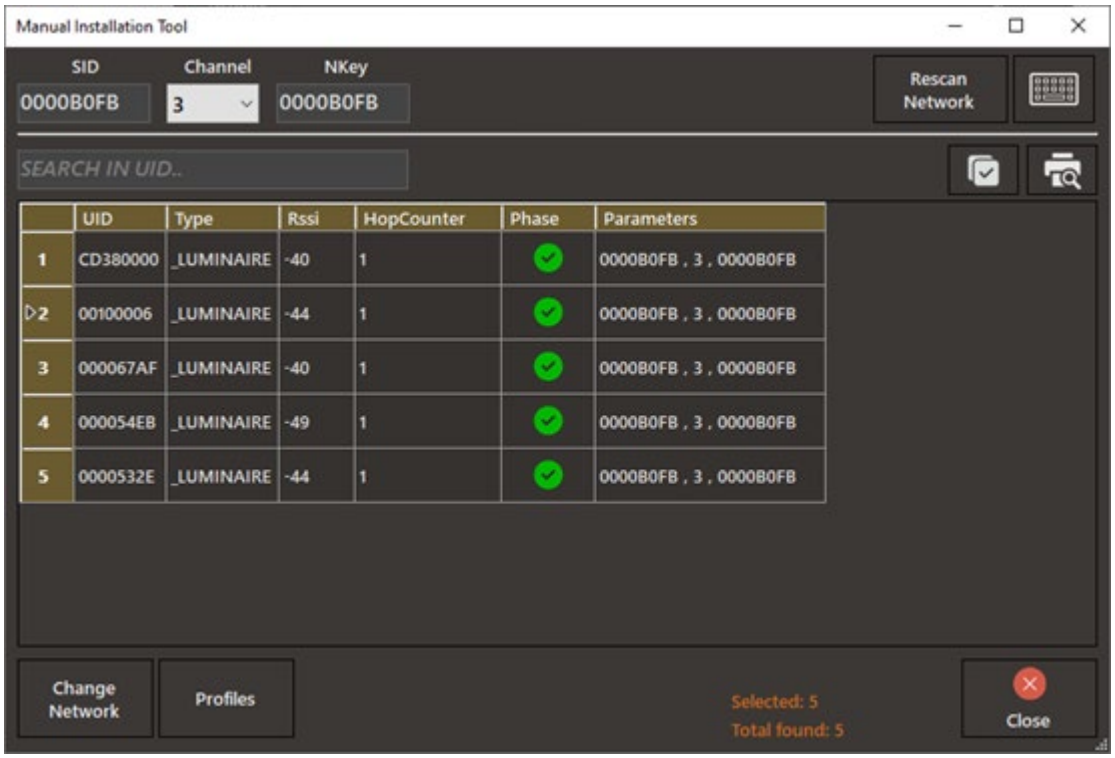
If the device has received the new profile parameters successfully, the icon will turn green.

If the device does not receive the new profile parameters successfully the icon will turn red.

When some of the devices do not receive the new parameters successfully, you can move on to the next step.
Take note of this device in order check it again after you add the gateway in the software.

Usually, some luminaires do not manage to send the response on time and the tool marks them up with red as unsuccessful. After some time, the luminaire will communicate, and you will be able to check its status from the software. If you cannot find them in the software, go and check the luminaire as it may be faulty, disconnected module, powered off, marginal signal.

One you solve any possible issues in the devices, follow the “Pair device” procedure for the unassigned devices.



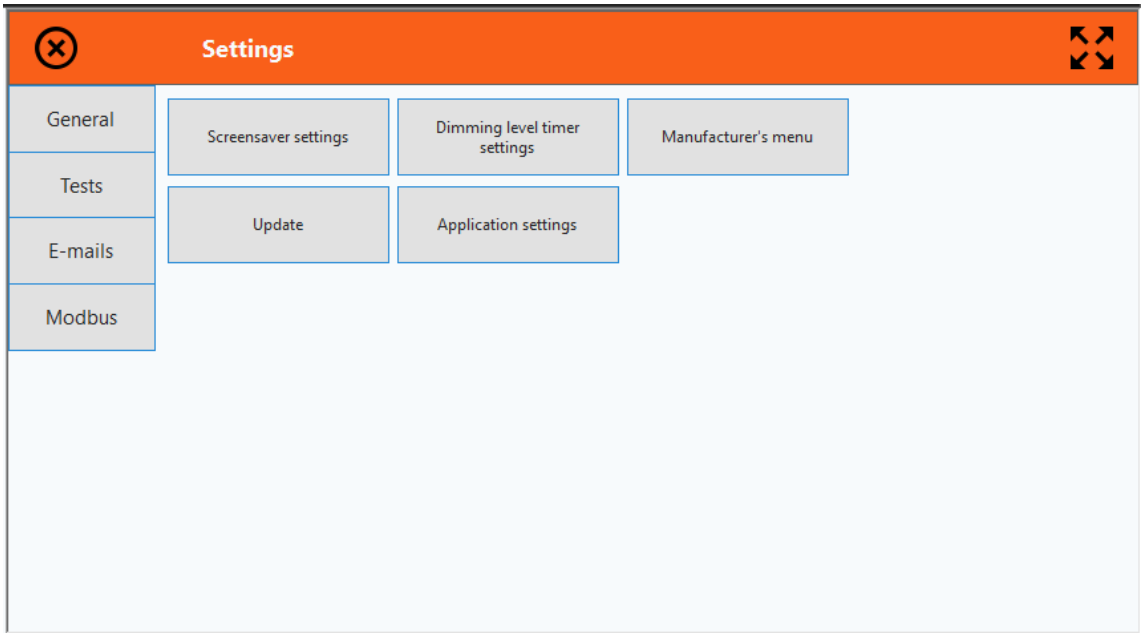
3.1.7. Settings

The settings item is the last element of the application's menu. It contains various options for the user to select, the most important of which regard the configuration of the devices' testing, emailing general and notification reports and the configuration of a Modbus device.

The complete range of options includes general settings, where the user can update the software, open the application settings, enable screen saver and the dimming level timers. Test configuration settings, where the user can set up the date and time for the execution of function and battery tests, e-mail settings, where the user can set up an e-mail account and the sending of automatic reports to all subscribed users, and Modbus settings, displaying the exact mapping of each device to their respective register address.

3.1.7.1. General

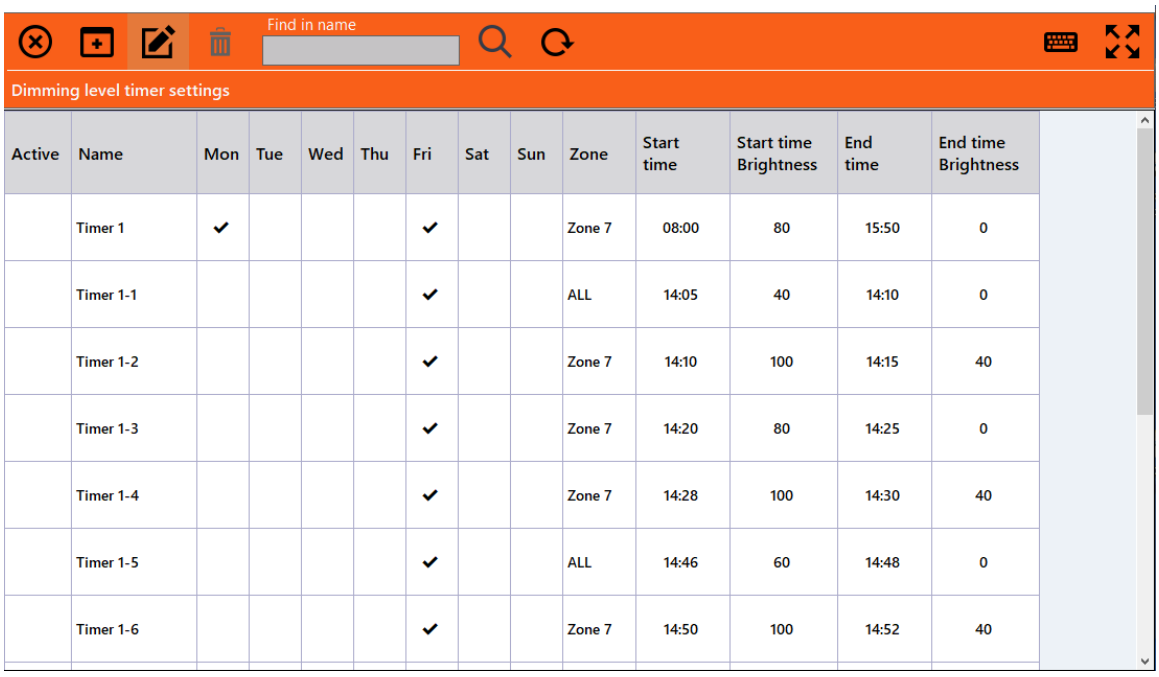
The following image provides an overview of the general settings.



From the General menu you are able to set up the screen saver, perform update to the software and open the application settings.

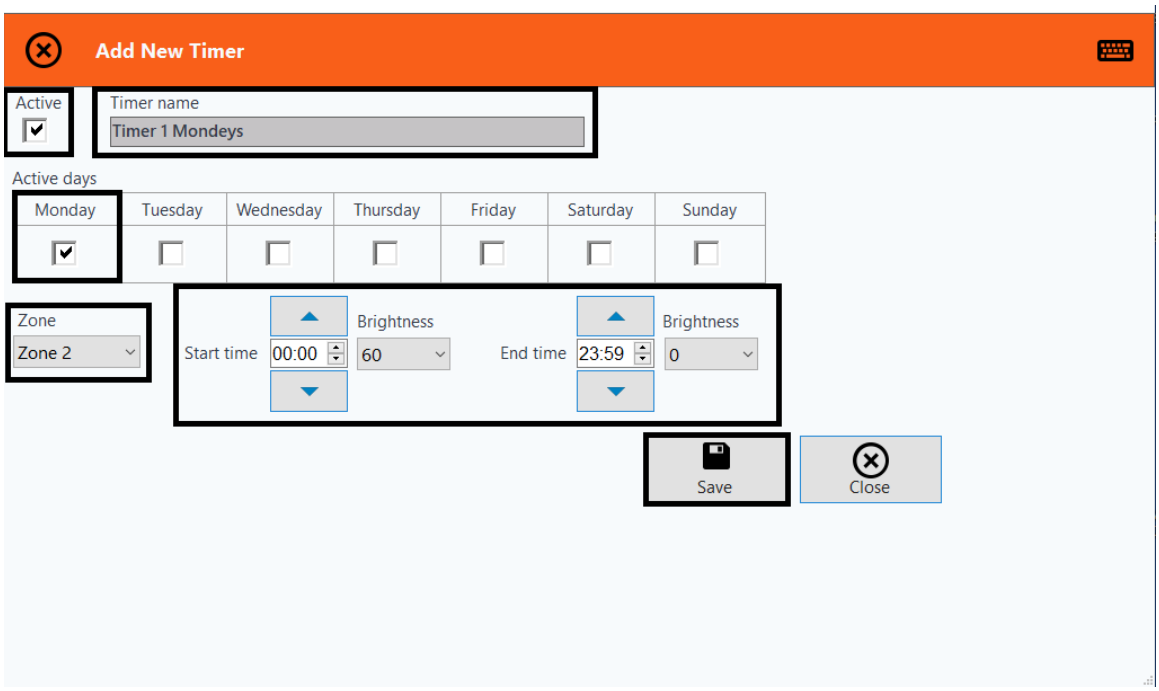
3.1.7.1.1 Dimming Level time settings

Another available option to the user is the ability to set specific timers for the automatic dimming level of the luminaires of a specific zone. There is no limit to the number of timers the user can create, edit, or delete.

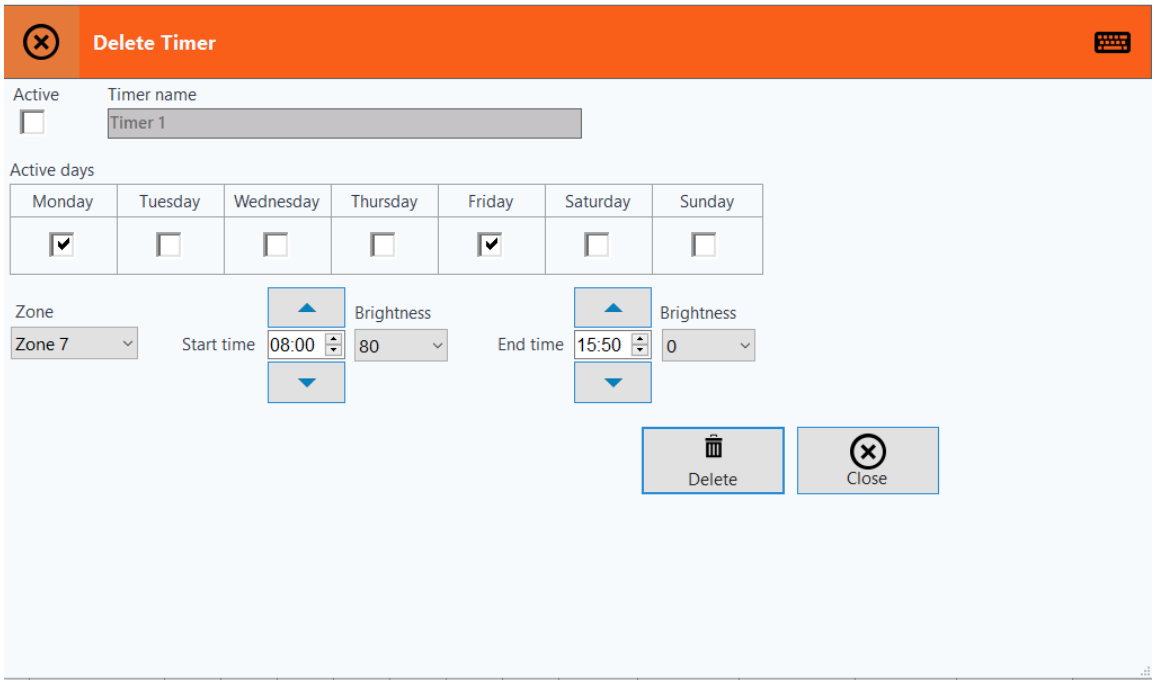


Active	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Zone	Start time	Start time Brightness	End time	End time Brightness
	Timer 1	✔				✔			Zone 7	08:00	80	15:50	0
	Timer 1-1					✔			ALL	14:05	40	14:10	0
	Timer 1-2					✔			Zone 7	14:10	100	14:15	40
	Timer 1-3					✔			Zone 7	14:20	80	14:25	0
	Timer 1-4					✔			Zone 7	14:28	100	14:30	40
	Timer 1-5					✔			ALL	14:46	60	14:48	0
	Timer 1-6					✔			Zone 7	14:50	100	14:52	40

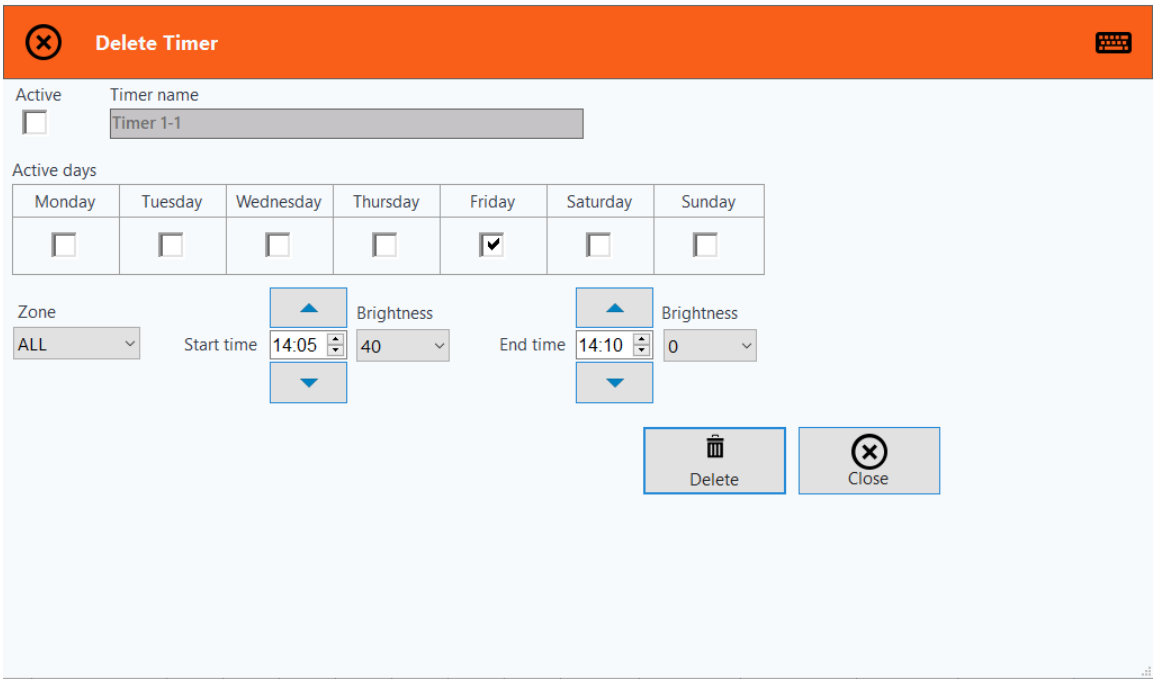
The leftmost option enables the user to add their own timer. They can select the days on which the timer will be active, the zone of luminaires and the brightness levels.



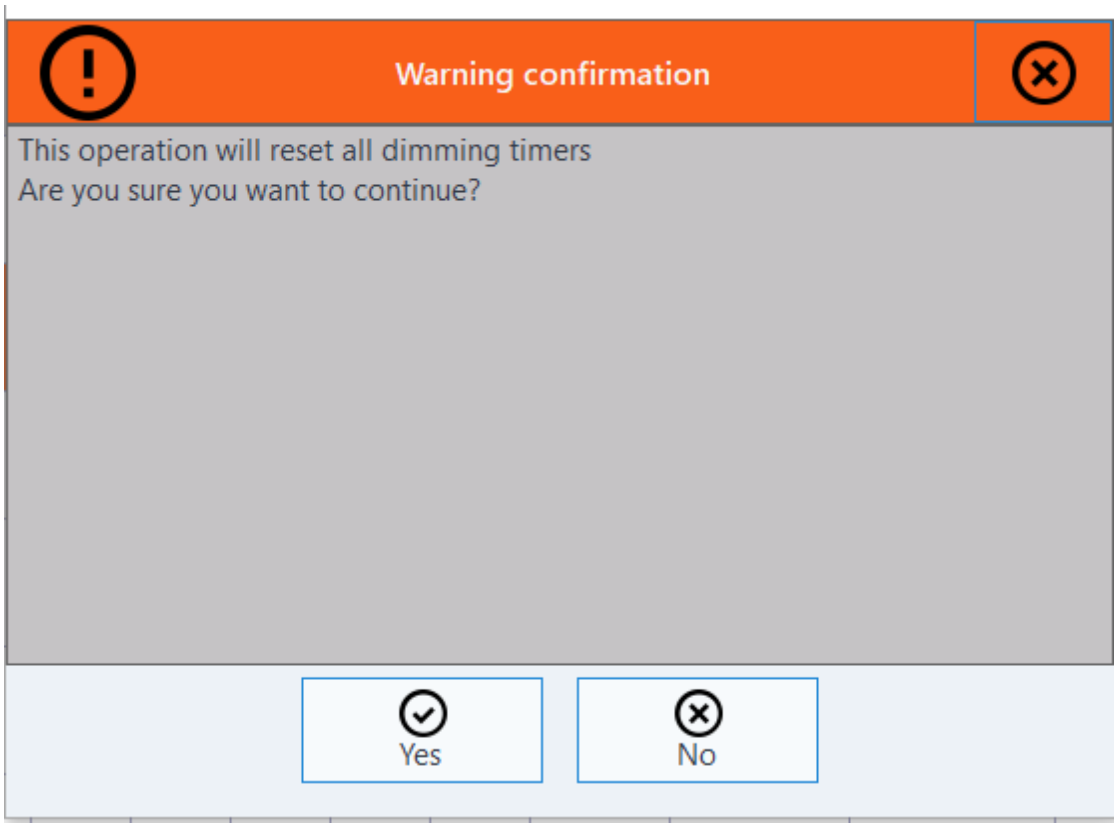
They may also edit an existing timer.



They may also delete a timer and confirm their action.



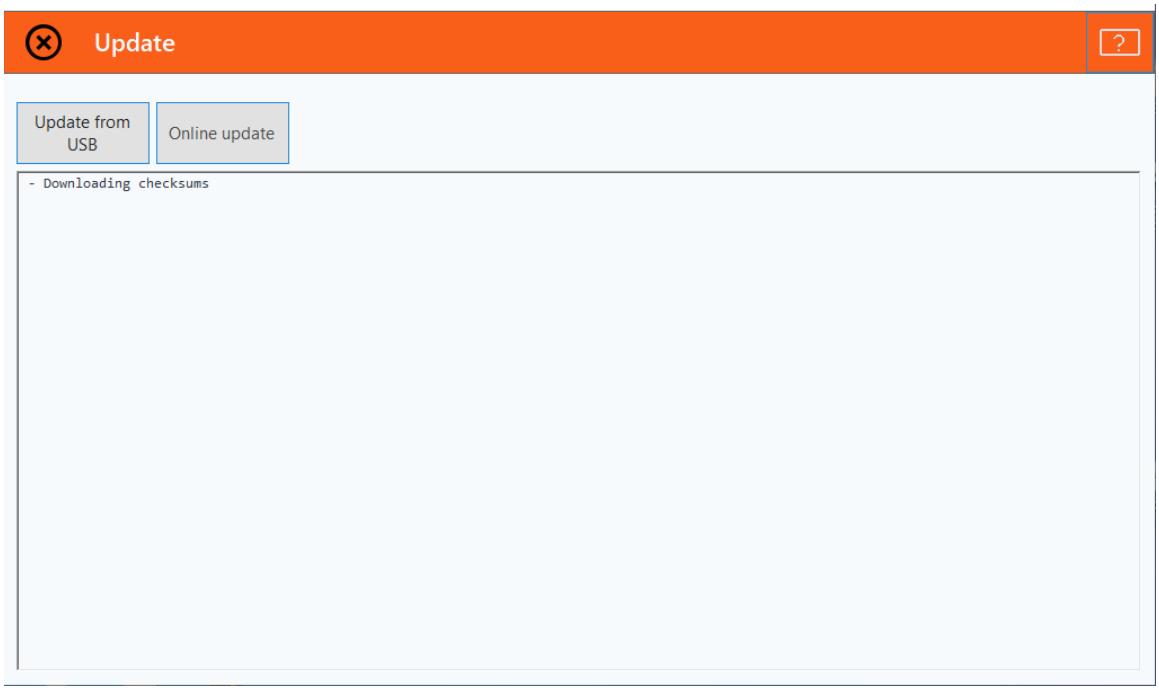
The rightmost option enables the user to reset all timers to the default timers that are available at the time of installation.

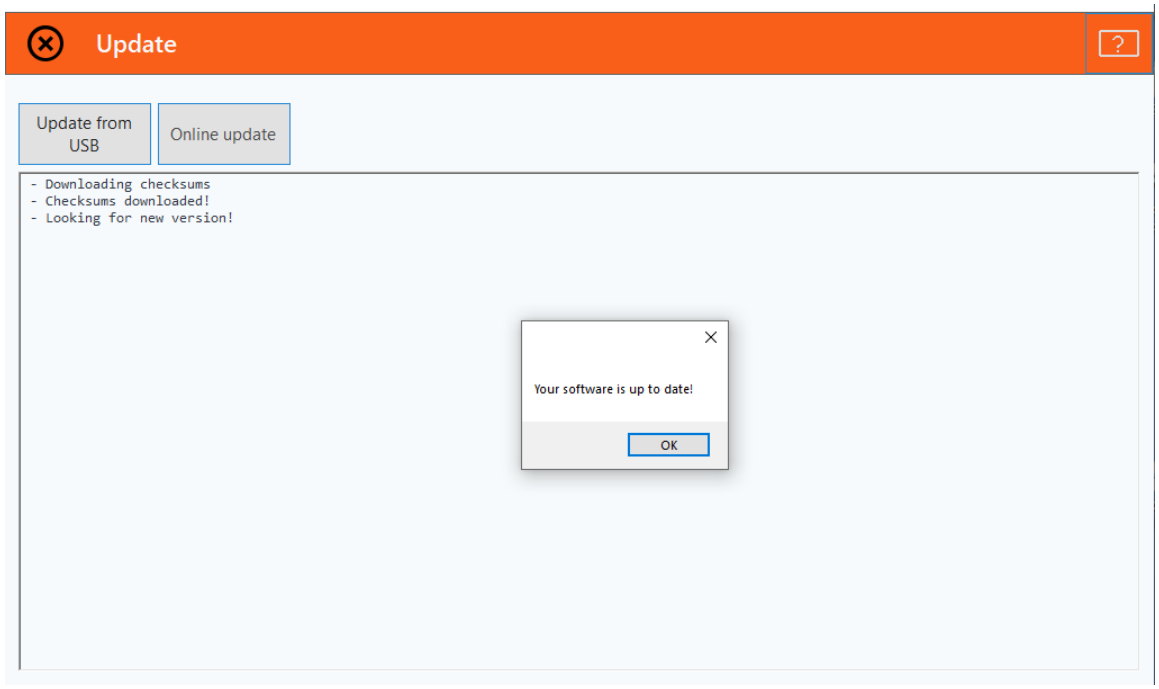


3.1.7.1.2 Software updater

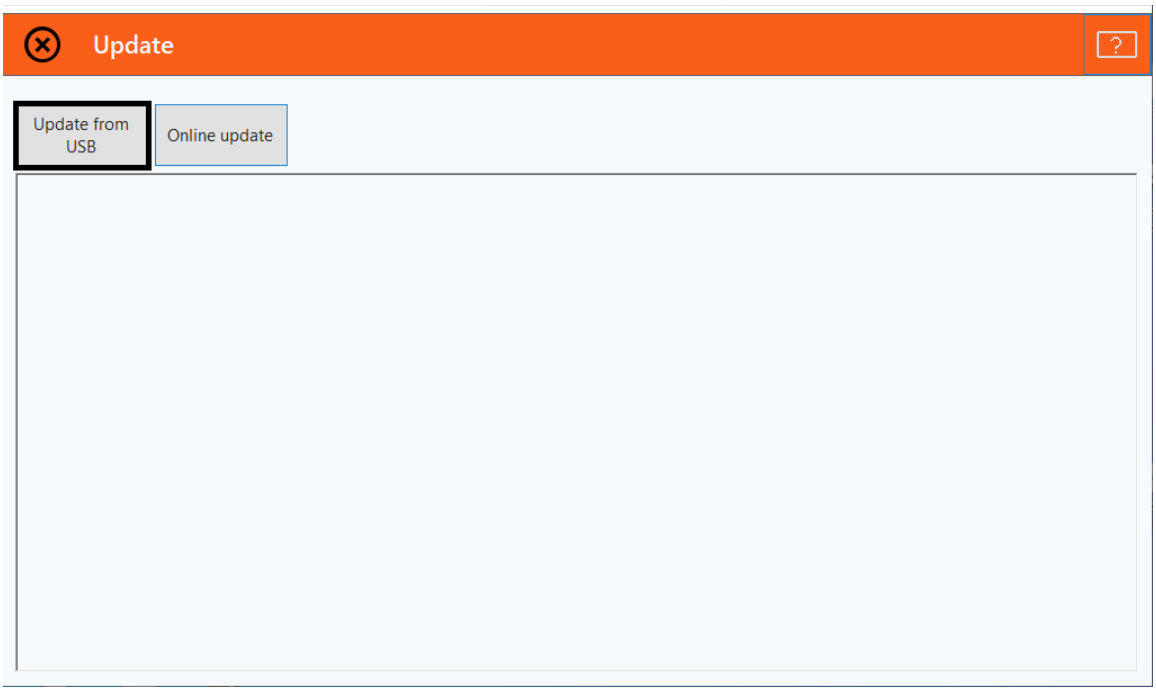
Software updater either automatically via an online source or via USB.

For the former option, the user needs to select the **Online update** tab to start the process. It will automatically be completed, whether an update is found, or the software is already up to date.

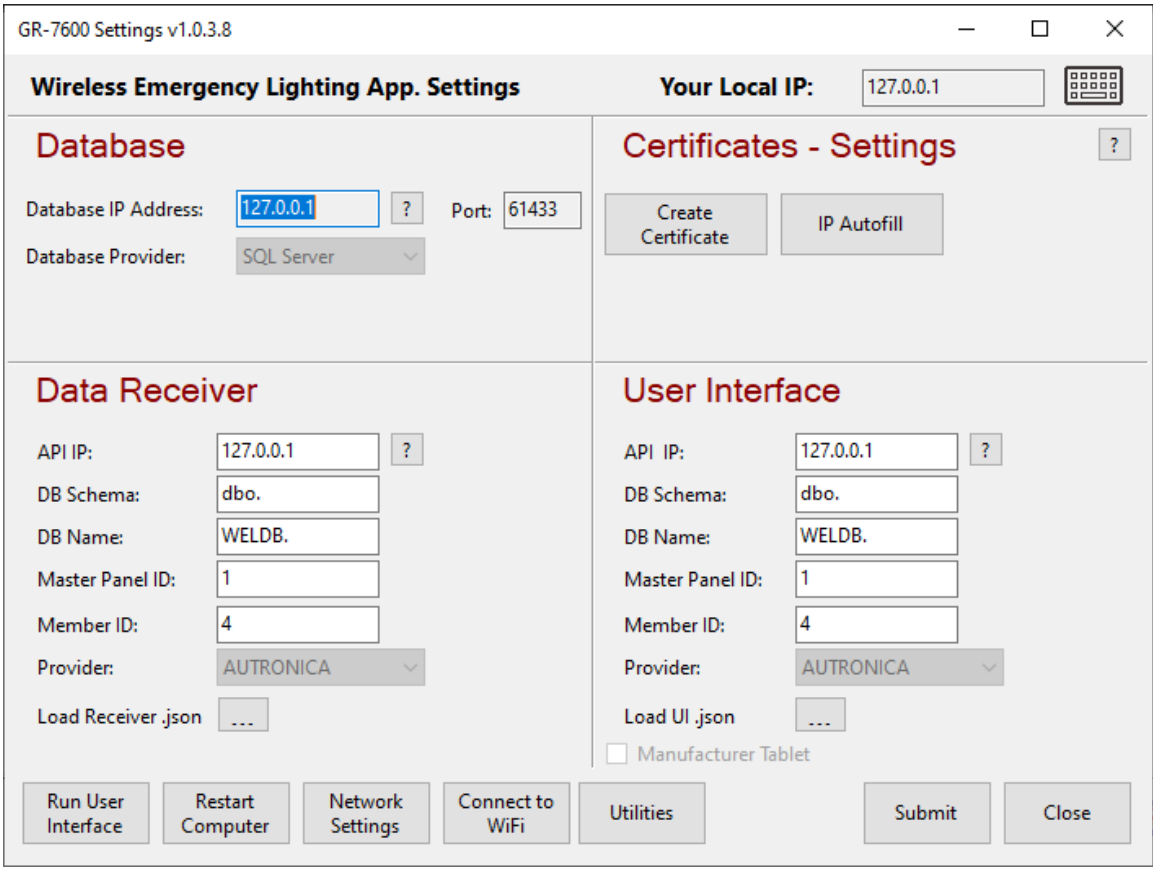




The latter option, through a USB device, allows the user to connect a flash drive for the system to scan for an update file. If the current version is older than the version in the update file, then the application proceeds to update.



Finally, this menu allows the user to also access the networking and certificate creation settings through the **Application settings** option. The same window can also be accessed through the login screen by pressing the gear icon.



3.1.7.2. Tests

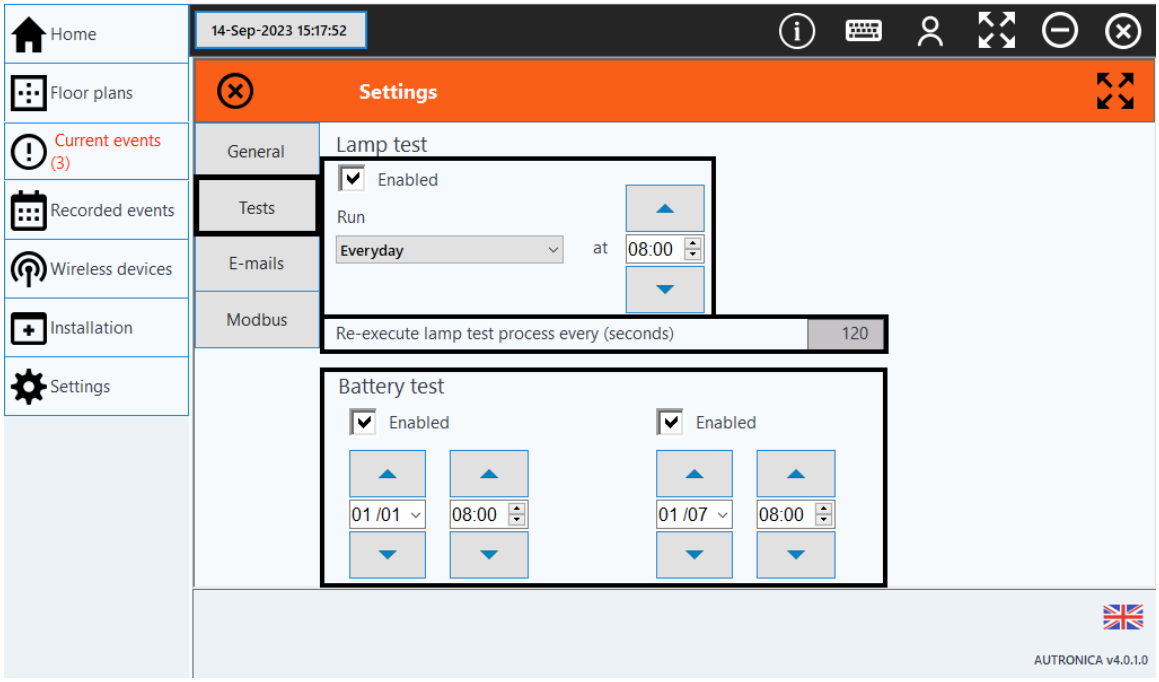
The **Tests** tab allows the user to enable or disable the lamp and battery hardware tests that are available to them.

Through the upper half of the view, the user may choose the frequency with which the luminaires' lamp test will be carried out, the time of day the test will commence, and a test re-execution time interval in seconds, in case the automatic test fails to begin.

The lamp test is a short duration process, depending on the network and the device's model, that activates the luminaires, which self-record their circuit measurements and register the values in the application. In the case of the existence of faulty measurements, the events are recorded and can be seen within any one of the **In fault** interactive fields of the Home screen.

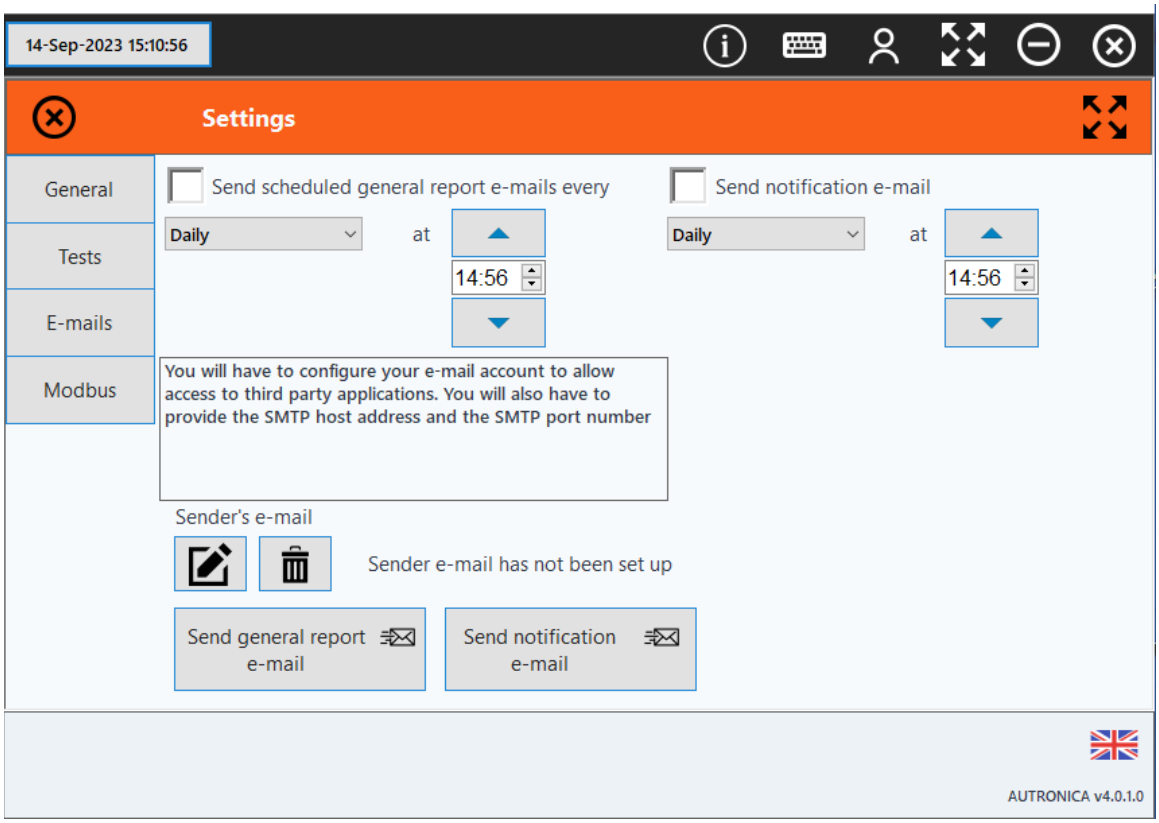
The lower half of the view enables the user to enable up to 2 battery tests and set the dates and times of both. It is recommended that the two tests be set 6 months apart from one another to achieve a more complete image of the luminaires' autonomy.

The battery test is a long duration process, mainly depending on the type of luminaire model and their batteries. It fundamentally is a duration test that stops when the battery is depleted and records the autonomy of each device. The results of this test are registered in the application.

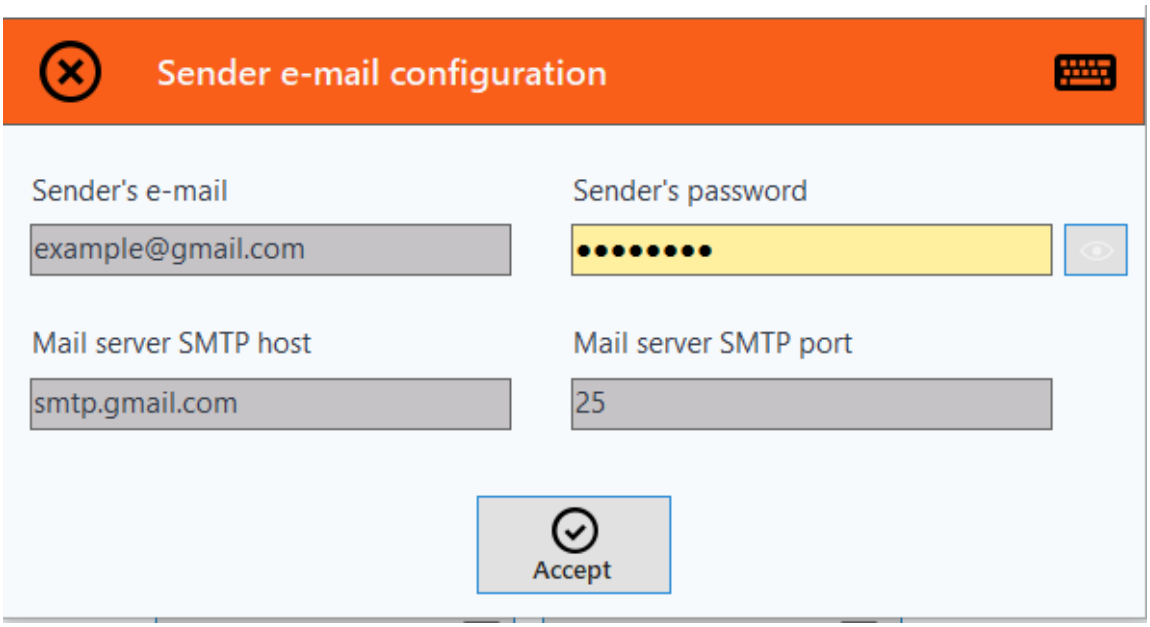


3.1.7.3. E-mails

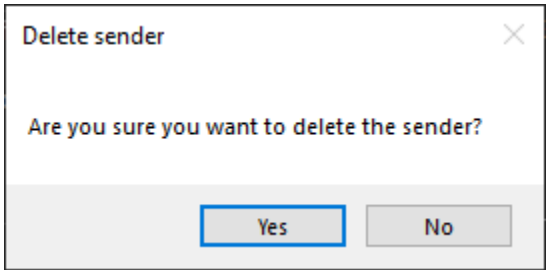
The **E-mails** settings tab allows the user to set up and configure an e-mail account under the address of which e-mails will be sent to all registered users. The e-mails can either be a general report of the system's status, or a notification message also containing the system's events.



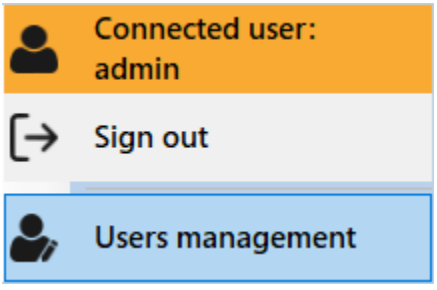
Sender's e-mail, the user may click on the pencil icon to register an address, email's password and mail's server configuration to be able to send out report and notification mail.



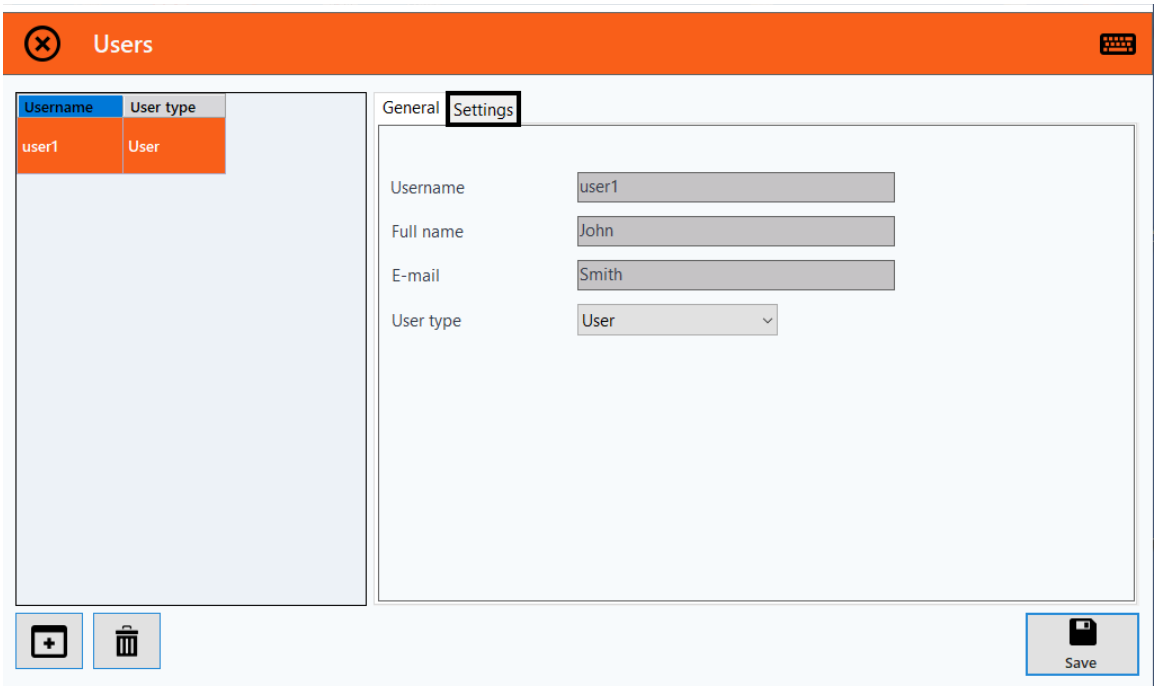
The user may also click on the close icon to delete the registered sender and save the details of another configured e-mail account.



Lastly, the system requires that there is at least 1 recipient to receive the e-mail. Through the top navigation bar of the application window, the user may select the user icon to open a drop-down menu.

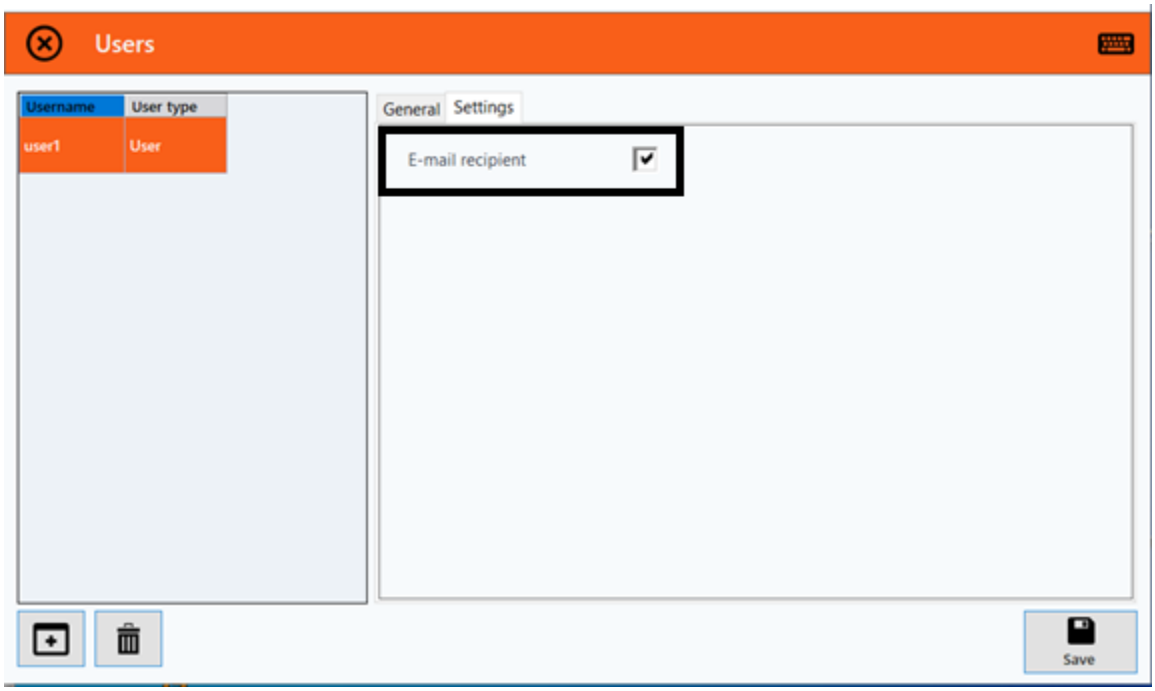


By selecting **Users management,** they gain access to a user management window, where they can create, edit, or delete a user from the system, as described earlier in this manual.



The **General** tab in the above window contains the basic information the system needs to register a new user or edit these fields and save the new information. A user type may also be selected that determines the access level of a user within the software.

The **Settings** tab contains the eligibility of the selected user to receive general report or notification e-mails. By checking the **E-mail recipient** box, the selected user can receive system related e-mails.



3.1.7.5. Modbus

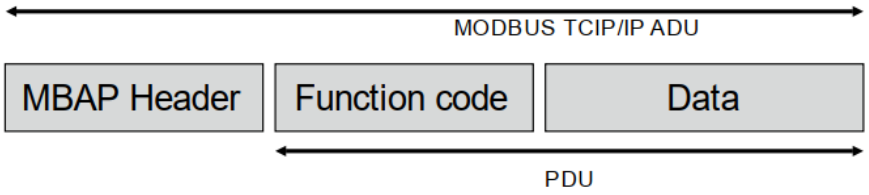
Before delving into the **Modbus** tab of the Settings menu, the Modbus protocol and registry map, and the function codes for status monitoring of the system will be described.

Generally, the Modbus implementation allows the user to have an overview of the system's status, and a detailed view of the status of each device of the system. The Modbus' specifications are based on the Modbus Application Protocol v1.1b and the Modbus Messaging Implementation Guide v1.0b. It should be noted that the system can only operate within the Modbus TCP protocol, supporting the following function codes: 03 Read holding registers.

The following sub-chapters comprise a break-down of the function of the Modbus within the TCP/IP protocol.

3.1.7.5.1. Modbus on TCP/IP Application Data Unit

This section describes the encapsulation of a Modbus request or response when executed within a Modbus TCP/IP network.



The previous image displays a Modbus request/response over a TCP/IP network. A dedicated header is used on TCP/IP to identify the Modbus Application Data Unit. It is called the MBAP Header – Modbus Application Protocol header.

This header is different compared to the Modbus RTU application data unit on the following accounts:

(i) Firstly, The Modbus 'slave address' field that is usually used on the Modbus Serial Line is replaced by a single 'Unit Identifier' Byte within the MBAP Header. The 'Unit Identifier' is used to communicate through devices such as bridges, routers, and gateways that use a single IP address to support multiple independent Modbus end units.

(ii) Secondly, all Modbus requests and responses are designed in such a way that the recipient can verify that a message has finished its transmission. For those function codes, where the Modbus PDU – Protocol Data Unit – has a fixed length, the function code alone suffices. For those codes carrying a variable amount of data in the request correspondence, the data field includes a Byte count.

(iii) Lastly, when the Modbus is carried over the TCP network, additional length information is also carried in the MBAP Header to allow the recipient to recognize

message boundaries even if the message has been split into multiple packets for transmission. The existence of explicit and implicit length rules and the use of a CRC-32 error check code – on Ethernet – results in an infinitesimal chance of undetected corruption within a request or response message.

3.1.7.5.2. MBAP Header

The MBAP Header contains the following fields.

Fields	Length	Description -	Client	Server
Transaction Identifier	2 Bytes	Identification of a MODBUS Request / Response transaction.	Initialized by the client	Recopied by the server from the received request
Protocol Identifier	2 Bytes	0 - MODBUS Protocol	Initialized by the client	Recopied by the server from the received request
Length	2 Bytes	Number of following bytes	Initialized by the client (Request)	Initialized by the server (Response)
Unit Identifier	1 Byte	Identification of a remote slave connected on a serial line or on other buses.	Initialized by the client	Recopied by the server from the received request

The Header is seven (7) Bytes long:

(i) Transaction Identifier – It is used for transaction pairing, where the Modbus server places the transaction identifier of the request inside the response.

(ii) Protocol Identifier – It is used for intra-system multiplexing, where the Modbus protocol is identified by the value 0.

(iii) Length – The length field is a Byte count of the subsequent fields, including the Unit Identifier and data fields.

(iv) Unit Identifier – This field is used for intra-system routing purposes. It is typically used to communicate with a Modbus+ or a Modbus Serial Line slave through a gateway between an Ethernet TCP/IP network and a Modbus Serial Line. This field is set by the Modbus client in the request, where the server must return a response of the same value.

All Modbus/TCP ADUs are sent via TCP to the registered port of 502. It should be noted that all different fields use the Big-endian order for encoding. The Big-endian order of encoding stores the most significant Byte in the sequence first, at the lowest storage address.

3.1.7.5.3. PDU Data

03 (0x03) Read Holding Registers

The above function code is used to read the contents of a contiguous block of holding registers in a remote device. The Request PDU specifies the starting register address and the number of registers. Inside the Protocol Data Unit,

registers are addressed starting at zero. Therefore, registers numbered at 1-16 are addressed as 0-15.

The register data in the response message are packed as two Bytes per register, with the binary contents aligned right within each Byte. For each register, the first Byte contains the high-order bits and the second Byte contains the low-order bits.

Request

Function code	1 Byte	**0x03**
Starting Address	2 Bytes	0x0000 to 0xFFFF
Quantity of Registers	2 Bytes	1 to 125 (0 x 7D)

Response

Function code	1 Byte	**0x03**
Byte Count	2 Bytes	2 x **N***
Register Value	**N*** x 2 Bytes	

***N** = Quantity of registers

Error

Error code	1 Byte	**0x83**
Exception code	1 Byte	01 or 02 or 03 or 04

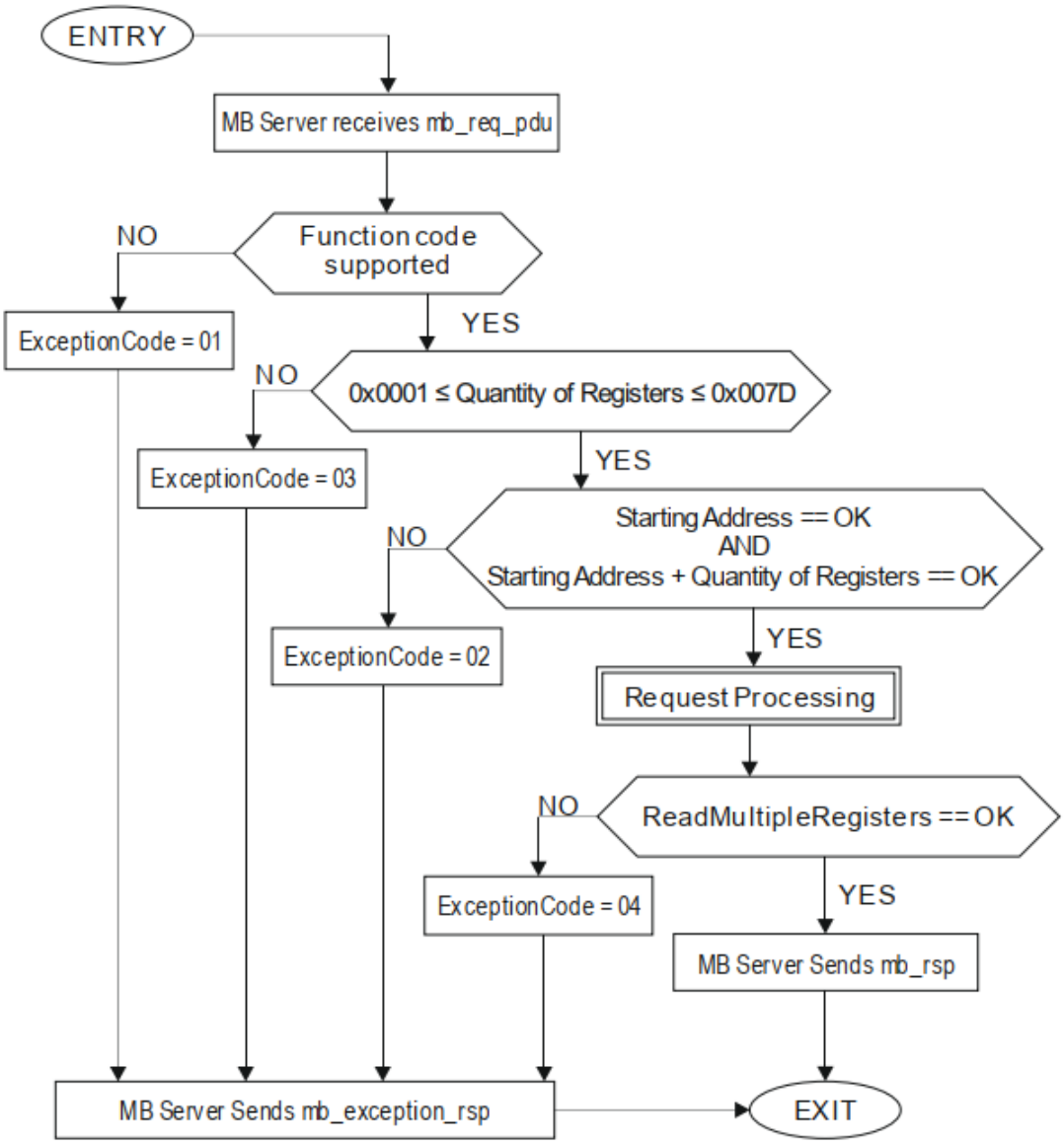
Next, follows an example of a request to read registers numbered at 108-110.

Request	
Field Name	(Hex)
Function	**03**
Starting Address Hi	**00**
Starting Address Lo	**6B**
No. of Registers Hi	**00**
No. of Registers Lo	**03**

Response	
Field Name	(Hex)
Function	**03**
Byte Count	**06**
Register value Hi (108)	**02**
Register Value Lo (108)	**2B**
Register Value Hi (109)	**00**
Register Value Lo (109)	**00**
Register Value Hi (110)	**00**
Register Value Lo (110)	**64**

The contents of register 108 are shown as the two Byte values – high-order and low-order – of 02 2B in hexadecimal, or 555 in decimal, respectively. The contents of registers 109-110 are of a 00 00 and 00 64 hexadecimal value, or a 0 and 100 decimal value, respectively.

The following image displays the flow chart, or state diagram, of the described function code – 03 (0x03) Read Holding Registers.



3.1.7.5.4. Modbus Response Building

Once the request has been processed, the Modbus server has to build the response using the appropriate Modbus server transaction and send it to the TCP management component.

Depending on the result of the processing, two (2) types of response can be built.

(i) A positive Modbus response:

the function code response is equal to the function code request.

(ii) A Modbus exception response:

(a) the objective is to provide the client with relevant information concerning the error detected during the processing,

(b) the function code response is equal to the function code request plus 0x80, and
(c) the exception code is used to indicate the reason for the error.

Exception Code	MODBUS name	Comments
01	Illegal Function Code	The function code is unknown by the server
02	Illegal Data Address	Dependant on the request
03	Illegal Data Value	Dependant on the request
04	Server Failure	The server failed during the execution
05	Acknowledge	The server accepted the service invocation but the server requires a relatively long time to execute. the server therefore returns only an acknowledgement of the service invocation receipt.
06	Server Busy	The server was unable to accept the MB Request PDU. The client application has the responsibility of deciding if and when to re-send the request.
0A	Gateway problem	Gateway paths not available.
0B	Gateway problem	The targeted device failed to respond. The gateway generates this exception.

The Modbus response PDU must be prefixed with the MBAP Header, which is build using data memorized in the transaction context.

(i) Unit Identifier – The Unit Identifier is copied as found within the received Modbus request and subsequently memorized in the transaction context.

(ii) Length – The server calculates the size of the Modbus PDU plus the Unit Identifier Byte. This value is set in the 'Length' field.

(iii) Protocol Identifier – The Protocol Identifier field is set to 0x0000, per Modbus protocol, as found within the received Modbus request.

(iv) Transaction Identifier – This field is assigned the 'Transaction Identifier' value associated with the original request and memorized in the transaction context.

Then, the Modbus response must be returned to the correct Modbus client using the TCP connection that was memorized in the transaction context. When the response is sent, the transaction context must be empty.

3.1.7.5.5. Registers

All the available holding registers that describe the system and device status are presented below, and for the length of the following pages.

Register Addresses

Start Address	End Address	Access	Use
0001	0001	Read (R)	Online Status
0002	0002	Read (R)	Total Faults in system
0003	0003	Read (R)	Luminaires Count
0004	0004	Read (R)	Luminaires With Fault Count
0005	0005	Read (R)	Luminaires In Emergency Count
0006	0006	Read (R)	Luminaires In Test Count
0007	0007	Read (R)	Gateways Count
0008	0008	Read (R)	Gateways With Fault Count
0009	0009	Read (R)	Extenders Count
0010	0010	Read (R)	Extenders With Fault Count
0011	0011	Read (R)	IO Wireless Unit Count
0012	0012	Read (R)	IO Wireless Unit Count With Fault Count
0013	0013	Read (R)	Unregistered Devices Total
0014	0014	Read (R)	Wless Luminaires In Forced Emergency Count
0015	0015	Read (R)	IO Wireless Unit With Input1Detected Count
0016	0016	Read (R)	Last Valid Device Adress

Devices Status

Start Address	End Address	Access	Use
1001	XXXX	Read (R)	Devices Status

Each devices status is 10 addresses long and the total length depends on how many devices are installed in the system. You can view the addresses from the menu modbus -> View Mapping Table

System Overview

Start Address	End Address	Access	Use
0001	0001	R	Online Status

Bit0 = Phos4.0 API Online, Bit1 = Data Receiver Online, Bit2-15 = Not Used

Start Address	End Address	Access	Use
0002	0002	R	Faults Total

The 16 bit read only holding register value is an unsigned integer value and displays the system current Total Faults Count.

Start Address	End Address	Access	Use
0003	0003	R	Luminaires Count

The 16 bit read only holding register value is an unsigned integer value and displays the system current Luminaires Count.

Start Address	End Address	Access	Use
0004	0004	R	Luminaires With Fault Count

The 16 bit read only holding register value is an unsigned integer value and displays the system current Luminaires With Fault Count

Start Address	End Address	Access	Use
0005	0005	R	Luminaires In Emergency Count

The 16 bit read only holding register value is an unsigned integer value and displays the system current Luminaires in Emergency Count

Start Address	End Address	Access	Use
0006	0006	R	Luminaires In Test Count

The 16 bit read only holding register value is an unsigned integer value and displays the system current Luminaires in Test Count.

Start Address	End Address	Access	Use
0007	0007	R	Gateways Count

The 16 bit read only holding register value is an unsigned integer value and displays the system current Gateways Count.

Start Address	End Address	Access	Use
0008	0008	R	Gateways With Fault Count

The 16 bit read only holding register value is an unsigned integer value and displays the system current Gateways With Fault Count.

Start Address	End Address	Access	Use
0009	0009	R	Extenders Count

The 16 bit read only holding register value is an unsigned integer value and displays the system current Extenders Count.

Start Address	End Address	Access	Use
0010	0010	R	Extenders With Fault Count

The 16 bit read only holding register value is an unsigned integer value and displays the system current Extenders With Fault Count.

Start Address	End Address	Access	Use
0011	0011	R	IO Wireless Unit Count

The 16 bit read only holding register value is an unsigned integer value and displays the system current Wireless IO Unit Count.

Start Address	End Address	Access	Use
0012	0012	R	IO Wireless Unit With Fault Count

The 16 bit read only holding register value is an unsigned integer value and displays the system current Wireless IO Unit With Fault Count.

Start Address	End Address	Access	Use
0013	0013	R	Unregistered Devices Total

The 16 bit read only holding register value is an unsigned integer value and displays the system current Unregistered Devices in Total.

Start Address	End Address	Access	Use
0014	0014	R	Wireless Luminaires In Forced Emergency Count

The 16 bit read only holding register value is an unsigned integer value and displays the system current WirelessLuminaires in Forced Emergency Count

Start Address	End Address	Access	Use
0015	0015	R	IO Wireless Unit With Input1 Detected Count

The 16 bit read only holding register value is an unsigned integer value and displays the system current WirelessIO UnitWith Input1Detected Count.

Start Address	End Address	Access	Use
0016	0016	R	Last Valid Device Adress

The 16 bit read only holding register value is an unsigned integer value and displays the system current Last ValidDeviceAddress.

3.1.7.5.6. Device Status

The device status consists of 5 read-only holding registers and its value must be interpreted as bit-fields. Each bit of the 16-bit register value is presented at the following tables.

UID 1	
bit 0-15	**UID (MSB)**

UID 2	
bit 0-15	**UID (LSB)**

*UID = UID (MSB) + UID (LSB)

Device Type/Zone	
bit0 – bit2	Device Type
bit 3 – bit 6	Spare
bit7	Connection Time Out
bit 8 - 15	Zone 8

*Device Type:

0=No Device

1=Wifi Gateway

2=Ethernet Gateway

3=USB Gateway

4=Luminaire

5=Extender

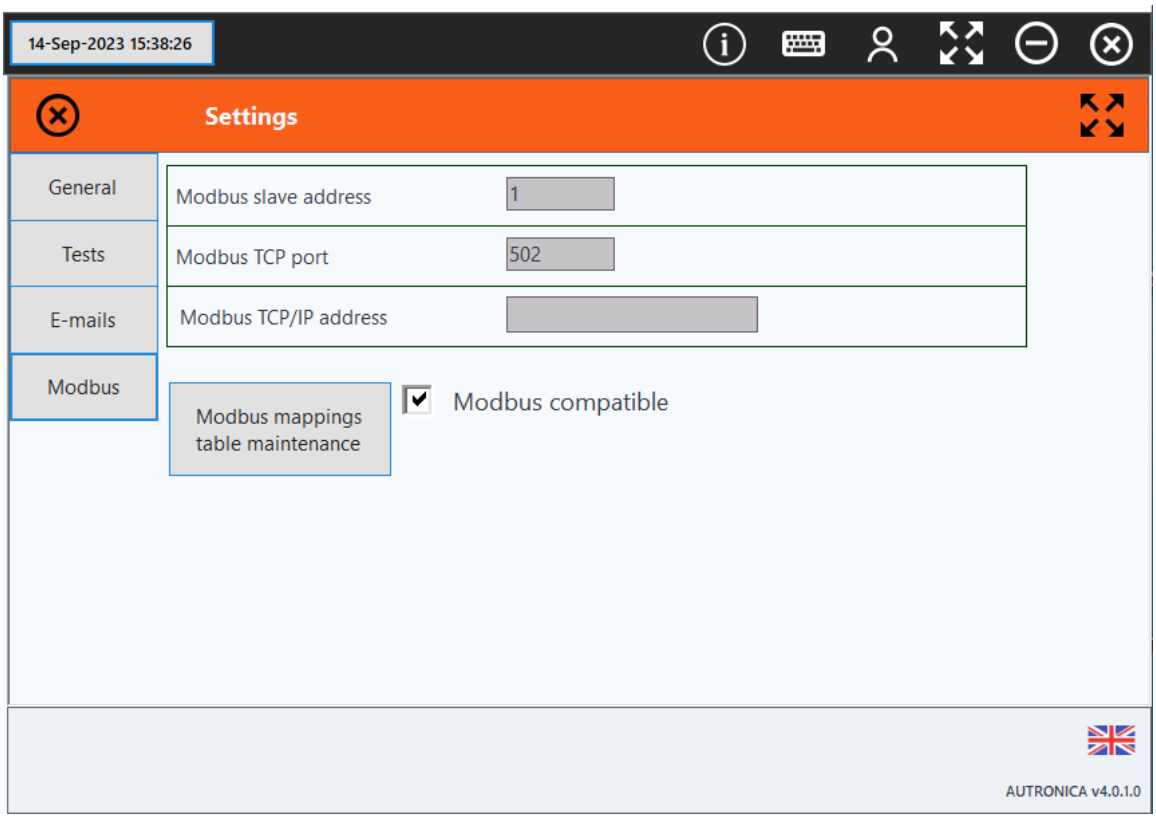
6=IO Unit

Device Status (1)	
bit 0	Spi Comm Error
bit 1	Luminaire Maintained
bit 2	Luminaire Mains Fault
bit 3	Luminaire Battery Charging
bit 4	Luminaire Battery Cut Off Status
bit 5	Luminaire Battery Fault
bit 6	Luminaire Charger Fault
bit 7	Luminaire Lamp Fault
bit 8	Luminaire in battery Capacity Fault
bit 9	Luminaire in Battery Test
bit 10	Luminaire in Lamp Test
bit 11	Luminaire Lamp Test Made
bit 12	Luminaire Forced Emergency
bit 13	Spare
bit 14	Spare
bit 15	Spare

Device Status (2)	
bit 0 – bit 7	Dimming Level (%):8
bit 8	IO Supply From DC
bit 9	IO VccNok
bit 10	IO Input1 Detected
bit 11	IO Input2 Detected
bit 12	IO Relay1 Armed
bit 13	IO Relay 2 Armed
bit 14	Spare
bit 15	Spare

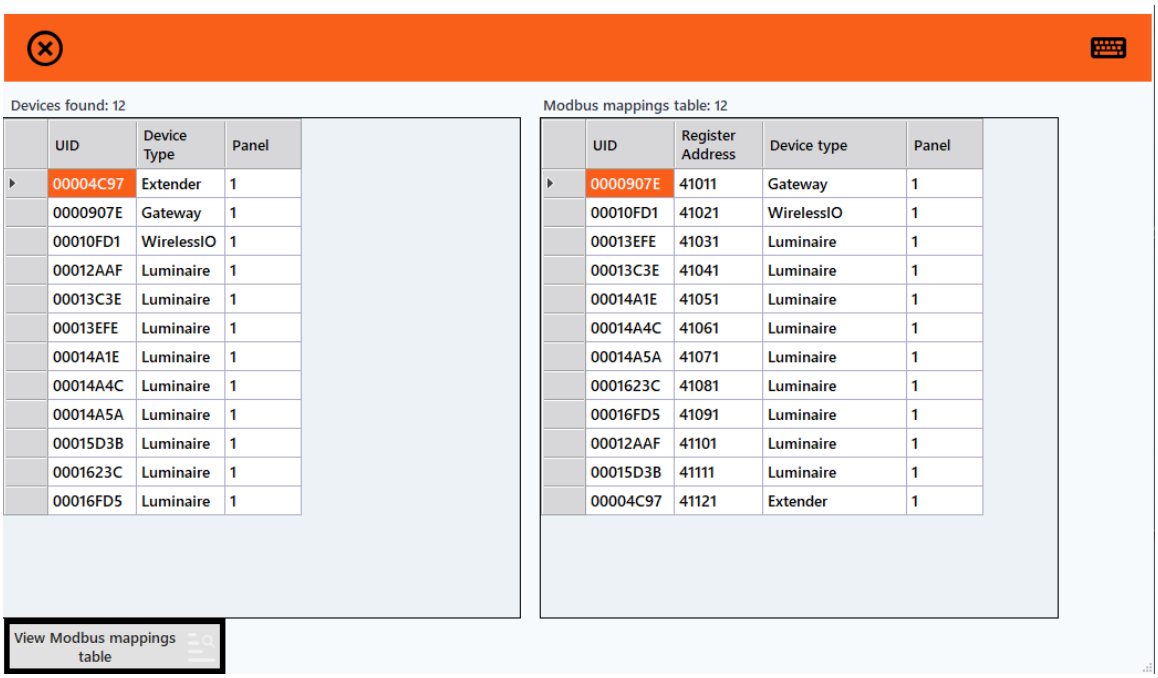
Device Status	Register Address	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
uid1	XXX1	UID (MSB)															
uid2	XXX2	UID (LSB)															
dev type/zone	XXX3	zone : 8								conn timeout	spare				dev type : 3		
Device status (1)	XXX4	spare	spare	spare	Lum in Forced Emergency	Lum Lamp Test Made	Lum In Lamp test	Lum In battery test	Lum Battery Capacity Fault	Lum Lamp Fault	Lum Charger Fault	Lum Battery Fault	Lum Battery CutOff Status	Lum Battery Charging	Lum Mains Fault	Lum Maintained	Spi Comm Error
Device status (2)	XXX5	spare		io Relay2 Armed	io Relay1 Armed	io Input2 Detected	io Input1 Detected	io VccNok	io Supply FromDC	Dimming Level (%) : 8							

Returning to the application and its Settings menu, the user may navigate to the **Modbus** tab from the UI. The following image displays the available options the user has to configure their Modbus.



In the case of multiple Modbus slaves, the user can select the preferred Modbus slave address for the system, while maintaining the value of the **Modbus TCP port** field. The **Modbus TCP/IP address** field must contain the IP address of the computer on which the Modbus service is installed.

The user may also access the **Modbus mappings table maintenance** to create or view the mapping table of the device addresses and status.



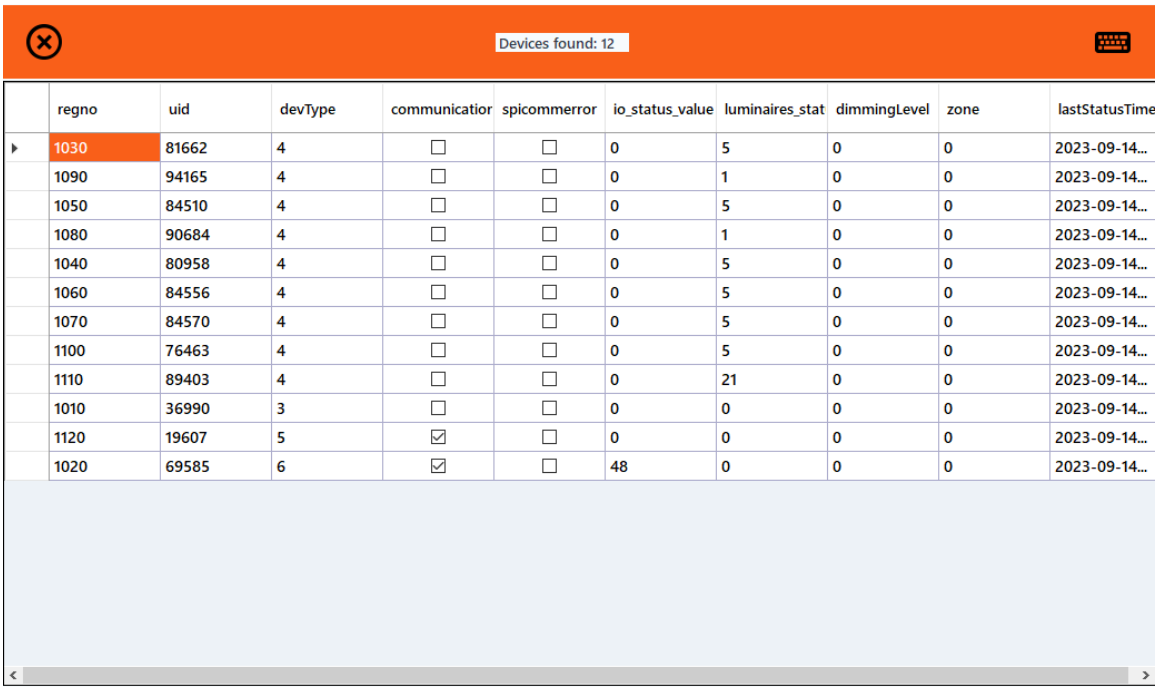
Devices found: 12

	UID	Device Type	Panel
▸	00004C97	Extender	1
	0000907E	Gateway	1
	00010FD1	WirelessIO	1
	00012AAF	Luminaire	1
	00013C3E	Luminaire	1
	00013EFE	Luminaire	1
	00014A1E	Luminaire	1
	00014A4C	Luminaire	1
	00014A5A	Luminaire	1
	00015D3B	Luminaire	1
	0001623C	Luminaire	1
	00016FD5	Luminaire	1

Modbus mappings table: 12

	UID	Register Address	Device type	Panel
▸	0000907E	41011	Gateway	1
	00010FD1	41021	WirelessIO	1
	00013EFE	41031	Luminaire	1
	00013C3E	41041	Luminaire	1
	00014A1E	41051	Luminaire	1
	00014A4C	41061	Luminaire	1
	00014A5A	41071	Luminaire	1
	0001623C	41081	Luminaire	1
	00016FD5	41091	Luminaire	1
	00012AAF	41101	Luminaire	1
	00015D3B	41111	Luminaire	1
	00004C97	41121	Extender	1

View Modbus mappings table



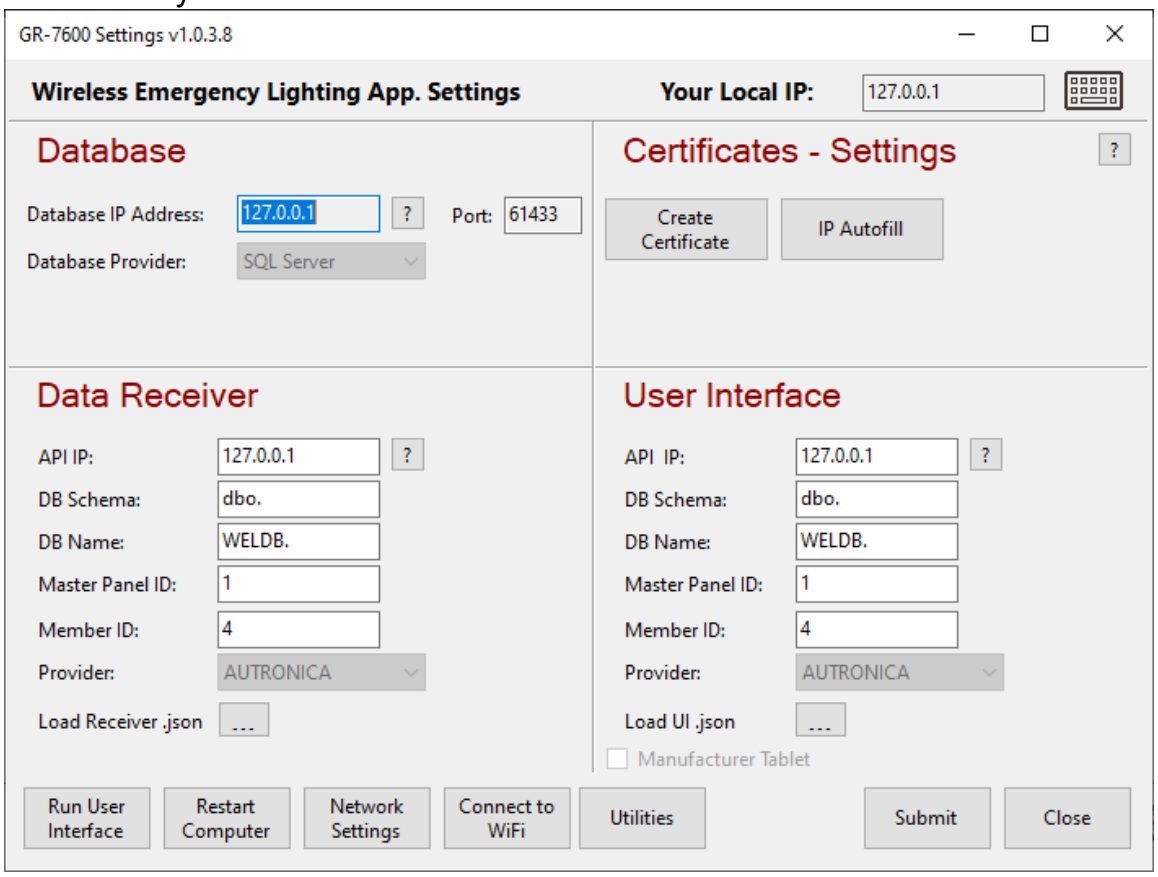
Devices found: 12

	regno	uid	devType	communicatior	spicommerror	io_status_value	luminaires_stat	dimmingLevel	zone	lastStatusTime
▸	1030	81662	4	☐	☐	0	5	0	0	2023-09-14...
	1090	94165	4	☐	☐	0	1	0	0	2023-09-14...
	1050	84510	4	☐	☐	0	5	0	0	2023-09-14...
	1080	90684	4	☐	☐	0	1	0	0	2023-09-14...
	1040	80958	4	☐	☐	0	5	0	0	2023-09-14...
	1060	84556	4	☐	☐	0	5	0	0	2023-09-14...
	1070	84570	4	☐	☐	0	5	0	0	2023-09-14...
	1100	76463	4	☐	☐	0	5	0	0	2023-09-14...
	1110	89403	4	☐	☐	0	21	0	0	2023-09-14...
	1010	36990	3	☐	☐	0	0	0	0	2023-09-14...
	1120	19607	5	☑	☐	0	0	0	0	2023-09-14...
	1020	69585	6	☑	☐	48	0	0	0	2023-09-14...

It should be mentioned that in order to enable the Modbus mapping capabilities of the present software, the user needs to check the **Modbus compatible** box.

4. Application Settings

In the application settings menu, you can find additional configurations about the system.



4.1 Network Settings

Network Settings, opening the windows connection form. From there you are able to configure the system's IP and subnet mask.

4.2 Connect to WiFi

In case you need to connect the system to Wi-Fi network you can open the Connect to Wi-Fi form. The form searches for all the available Wi-Fi networks.

4.3 Utilities

4.3.1 Reset database

In order to reset the database and delete all the users and configurations from the software you can go to Application settings then to the Utilities menu and select Reset database.

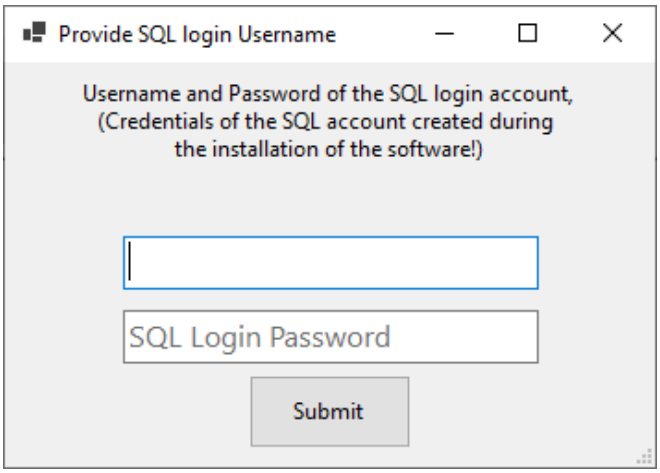
A window will prompt you to add the log in username and password that you have from administrator account.

! The above procedure will perform a factory reset to the software!

4.3.2 Backup & Restore

You are able to take a backup from the entire system and keep it to use in case of

- Backup, from application settings go to Utilities and Backup operation. A prompt window will appear to select the path and the folder you want to save the file.
  When the procedure finished, in the folder will have 2 files
  - GwCertRoot
  - weldb_2023_05_16T12_01_41.bak
- Restore, to restore your configurations and the ethernet gateways continue to work as it is you must keep the same IP address to the software.
  - Select the folder that you gave restored the backup files.
  - You must know your SQL account that you had created during the installation.



4.3.3 Date & Time

From this menu you are able to change the date and time to your system

5. Additional Notes

The wireless network settings – SID, RF Channel, NKey – are stored in the hardware memory of each wireless device individually. In order to restore these to their default values – 00000001, 2, 00000000 – either use the **Network Configuration Wizard**, or in the case of the communication having been lost, each device needs to be reset to its default settings through its dedicated on-board button (see the product manual).

In case of a gateway device failure, it can be replaced with a new one and its settings set to the same values – SID, RF Channel, NKey – manually, without resetting all the connected wireless devices to their factory settings. This option is found within the **Wireless devices** menu, the **Gateways** option and through editing the selected gateway. `Then, after accessing the edit option the user needs to select **Set SID and RF channel** to change the SID and RF Channel values of the gateway.

After the completion of the installation of the connected devices and their networking with their appropriate gateway device, it is recommended that a lamp test be run to ensure the proper communication of the emergency luminaires with the gateway, and the system by extension. If the system includes an interconnection with other security systems, i.e., through a Wireless Input/Output unit, a system event should be simulated by triggering the input to ensure the proper functionality of the Wireless Emergency Lighting system.

6. Epilogue

GR-7600/V2 is fully fledged commissioning and monitoring master software that accompanies or can be installed on a computer unit, capable of controlling the setting up of networks of devices, their installation and command assignment procedures, as well as perpetually monitoring their status and functions in general.

Its built-in functionalities afford the end-user, or the expert responsible for the installation and the setting up of related hardware within this software, complete control over the behavior of all relevant devices throughout multi-faceted, larger installation areas, from one computer. These devices include gateways and wireless devices, such as emergency luminaires, extenders, and input/output units.

***Disclaimer**: The present is a user manual, the usage of which primarily addresses the end-user and/or technicians with the required knowledge to assess the technical parts of this manual, covering most major aspects of the product's general installation process, from physically installing the hardware to the software's inner functionality. Assistance from expert personnel may be required for the completion of the installation and the utilization of all available functions.*