Commissioning Guide

Wireless Emergency Lighting

GR-7600/V2

AUTRONICA

CE

1. INTRODUCTION 5
2. INSTALLING SOFTWARE APPLICATION 116-GR-7600/V2 5
3. SPECIFICATIONS AND TERMS 11
4. USER MANAGEMENT 13
5. COMMISSIONING 14
5.1 Before starting 14
5.2 Spectrum Analyzer 16
5.3 Connecting 116-GR-7603/V2 Ethernet + Wifi Gateway 18
For Ethernet connectivity: 20
For Wi-Fi (WPA2/PSK) connectivity: 20
For Wi-Fi (WPS) connectivity: s21
5.4 Connecting a 116-GR-7607/V2 or 116-GR-7605/V2 as USB Gateway 22
5.5 Network detection and configurations 22
5.5.1 Network configuration wizard (single network) 23
5.5.2 Easy Commissioning (multiple networks) 26
5.5.3 Easy Commissioning (adding new devices) 28
5.6 Edit Names 29
5.6.1 Edit Gateway name 29
5.6.2 Edit name of a wireless device 29
5.7 Creating Floor Plans 30
5.8 Setting Zones for emergency luminaires 32
5.9 Configuring Wireless In/Out units triggers 33
6. RESET SYSTEM STATUS / CLEAR EVENTS 34
7. SYSTEM SETTINGS 35
7.1 General page 35
7.2 Test page (schedule Lamp & Battery test) 36
7.3 Notifications page 36
7.4 E-mails page 37
7.5 Tablet page 37
7.6 Modbus page 38

8. BROADCAST COMMANDS / RUN TESTS 39

9. IMPORTANT NOTES 41

1. INTRODUCTION

This guide provides instructions regarding commissioning **wireless emergency lighting system 116-GR-7600/V2** – by **Autronica**. Prior to commissioning, the installation of the wireless emergency lighting shall be fulfilled in accordance with the corresponding Quick Installation Guide.

IMPORTANT: Before commissioning the wireless emergency system there must be an existing running network. The commissioning requires a high degree of network competence.

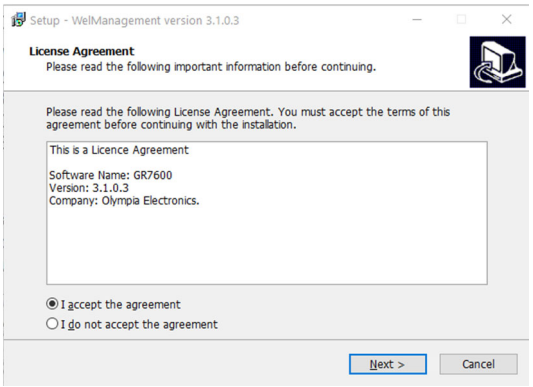
2. INSTALLING SOFTWARE APPLICATION 116-GR-7600/V2

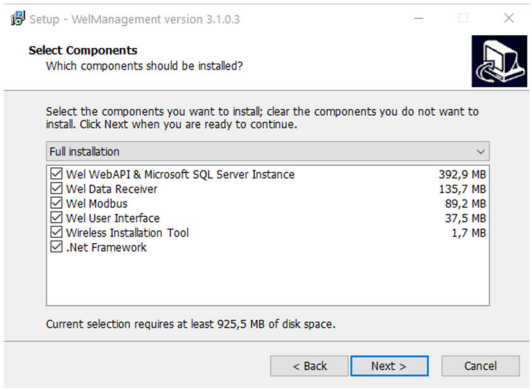
In order to use a Windows PC as the master PC of the wireless emergency lighting system, start by installing the software application.

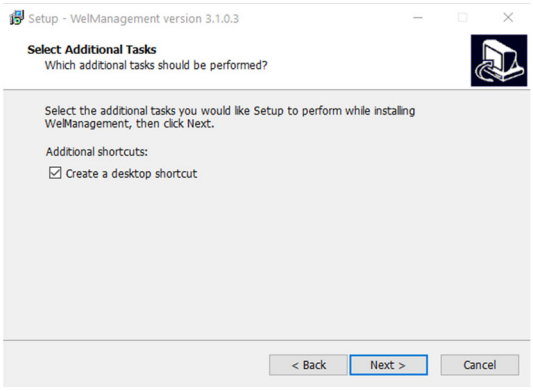
116-GR-7600/V2 software minimum PC requirements:

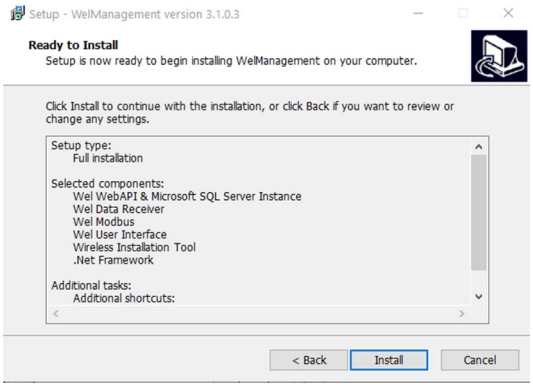
- Windows 10 64bit
- 3GB RAM
- 8GB free storage space
- CPU dual core 1,3GHz
- Ethernet or Wi-Fi connectivity

For the master PC, which is responsible of monitoring and controlling wireless network traffic and holding the system database, please do install all pre-selected packages (full installation).

1. 

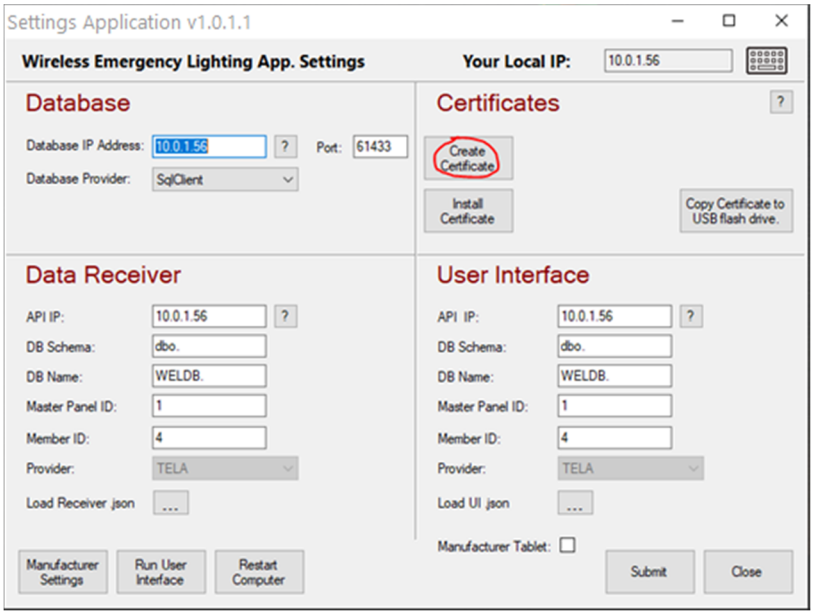
2. 

3. 

4. 

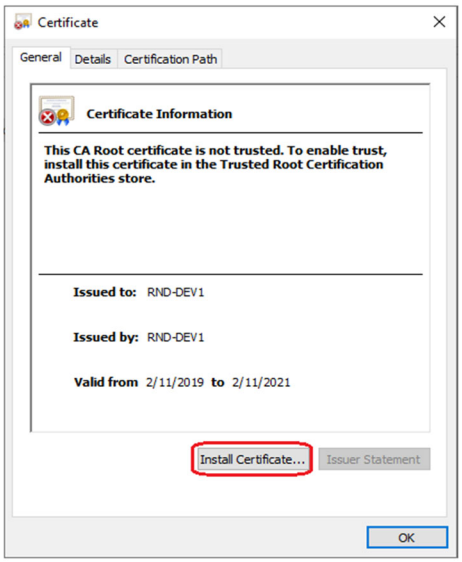
***Note**: for client PCs that their purpose is to monitor the wireless installation remotely, install only the "WEL User Interface" and ".NET Framework", as all other packages are needed for the master PC only.*

Launch "**WelManagement**" from the desktop shortcut. At first launch, the application settings window will show up. A certificate is needed to be created in order to provide safe communication of the "API" service. If there was no previous certificate installed on this master PC, press the "**Create Certificate**" button.

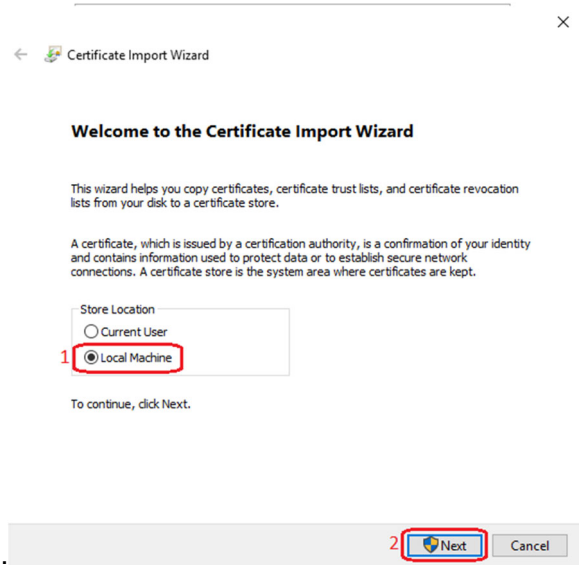


Then follow the steps as shown below:

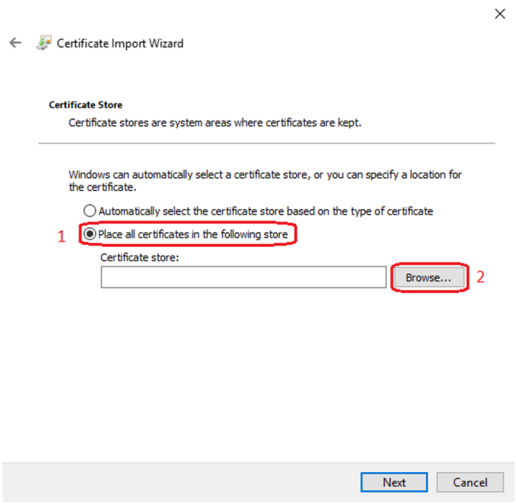
1.


Certificate
General
Details
Certification Path
Certificate Information
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.
Issued to: RND-DEV1
Issued by: RND-DEV1
Valid from 2/11/2019 to 2/11/2021
Install Certificate...
Issuer Statement
OK

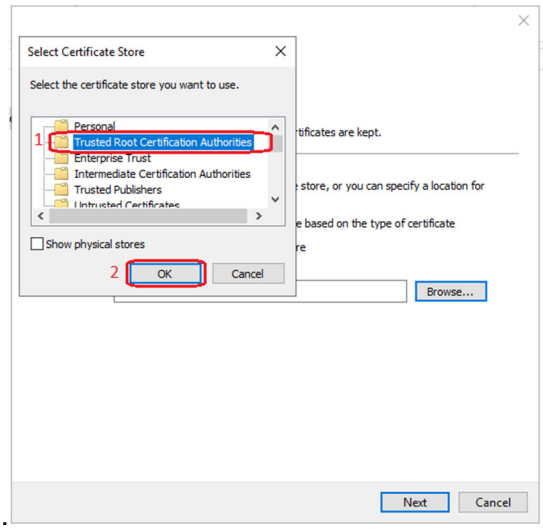
2.


Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
Store Location
Current User
Local Machine
1
To continue, click Next.
2
Next
Cancel

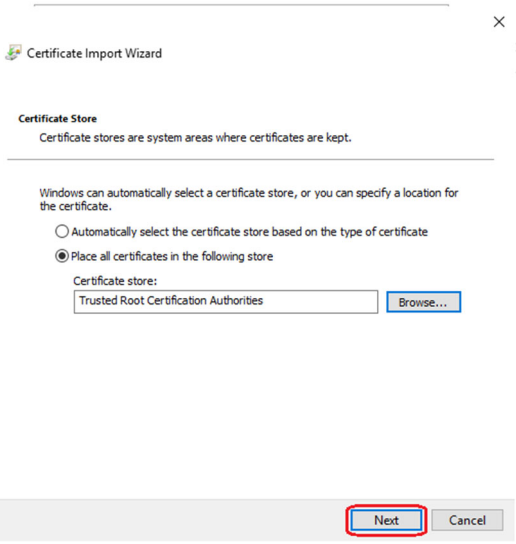
3.


Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
1
Place all certificates in the following store
Certificate store:
Browse...
2
Next
Cancel

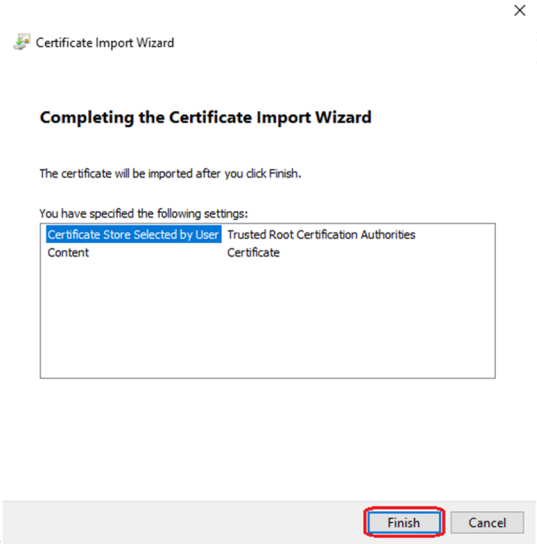
4.

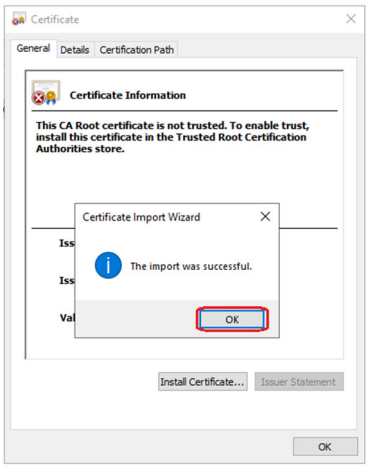

Select Certificate Store
Select the certificate store you want to use.
Personal
1
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Show physical stores
2
OK
Cancel
Browse...
Next
Cancel

5.


Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Trusted Root Certification Authorities
Browse...
Next
Cancel

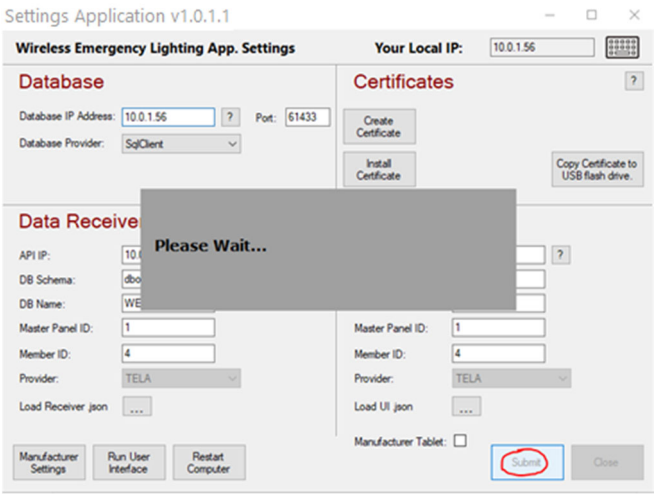
6.


Certificate Import Wizard
Completing the Certificate Import Wizard
The certificate will be imported after you click Finish.
You have specified the following settings:
Certificate Store Selected by User
Trusted Root Certification Authorities
Content
Certificate
Finish
Cancel

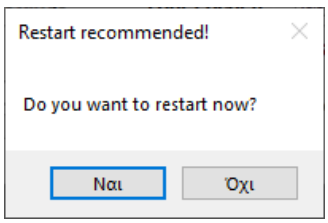
7. 

The same certificate (which you can copy on a USB flash drive) can be used to other client devices for remote access. For remote access, choose "**Install Certificate**" and import the certificate from the USB flash drive. On the application settings for the remote access PC, the target IP for the Database and the Data Receiver must be the IP of the master PC, while the "**User Interface**" IP must be the remote PC's IPv4 address.

After installation of the certificate, click on "**Submit**".



Then you will be prompted to restart the PC.



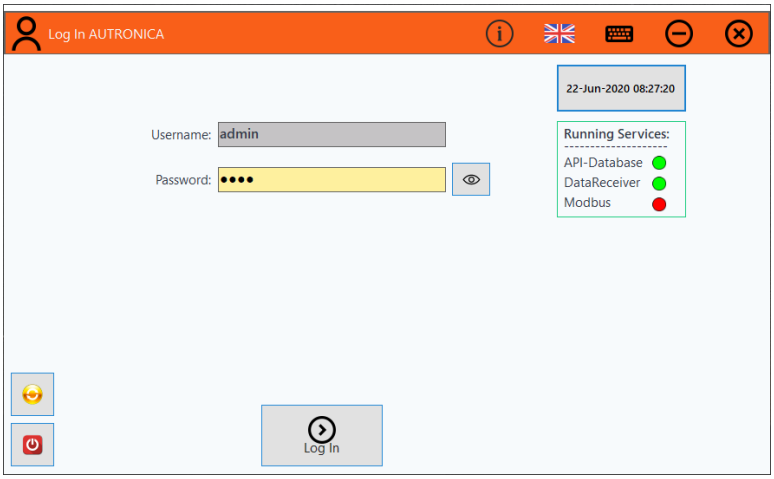
After restarting, all processes needed for the wireless lighting system will run on the background in real time, even when you are not using User Interface.

Important Notes:

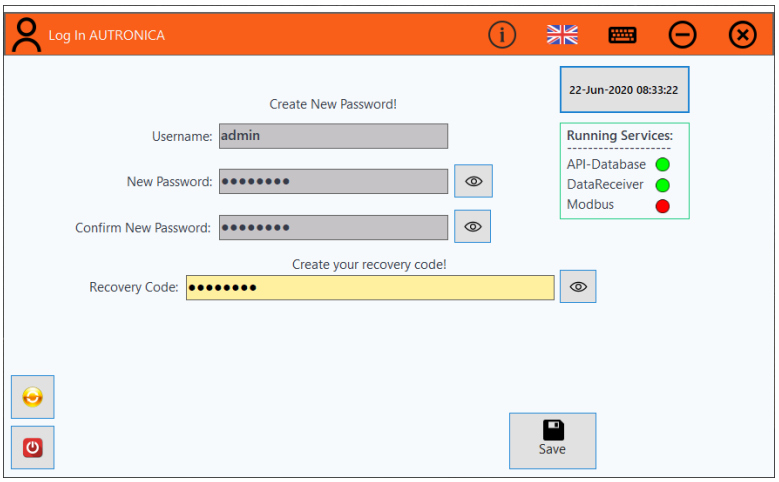
- **The master PC which runs the "116-GR-7600/V2" software application must be operating uninterruptedly (energy saving plan disabled).**
- **To maintain communication when mains power is down, connect this master PC and the "116-GR-7603/V2" Gateways to a UPS.**
- **The IPs' that are used for, "Receiver" and "Database" must be static IPv4. Therefore the master PC must use a static IP permanently.**
- **"WelAPI", "WelDbmaker", "WelReceiver" and "WelModbus" are 4 essential services running in the background. Do not block or stop these services by any means.**
- **Consult an IT technician for local network addressing if needed.**

Now, when launching the "WelManagement" icon, the user login screen will appear (User Interface).

- Default administrator username: **admin**
- Default administrator password: **1000**



After the first login you are prompted to enter new "**Password**" and "**Recovery Code**". These login credentials must be kept safe, as they are used only by the administrator. Use at least an 8-digit password and also avoid using the same value for the recovery code, as the system will reject it.



After this you can login with your new password.

The system administrator has all privileges required to add, delete, monitor and control every segment of the system (users, gateways, devices, settings, etc).

Use this account, or create a new one with “administrator” privileges to continue with the commissioning procedure.

(see: 4. User Management for more information)

3. SPECIFICATIONS AND TERMS

A wireless network consists of a Wireless Gateway (master) and a group of wireless devices (emergency luminaires, network extenders, input/output units, etc), all connected to the Gateway, which is the master device of the wireless network.

Multiple wireless networks can co-exist in an installation simultaneously and be monitored via a single master PC (Autronica 116-GR-7600/V2 PC software application). Each system can support up to 16 Gateways (Network Masters) and up to 200 wireless devices per Gateway.

As an alternative solution for smaller scale installations, the “116-GR-7610/V2” can operate as a standalone control panel, capable of control and monitoring of 2 USB Gateways, thus 2 wireless networks in parallel.

The most common terms of a wireless network are described below:

- **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 the data to the master PC. Available models with Ethernet/Wi-Fi or USB connectivity.

- **Wireless device**: may be any type of wireless device (emergency luminaires, network extenders, I/O units) that connects to a wireless network.

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

- **SID**[1]: (System ID) represents the wireless network’s name. All wireless devices in a wireless network must share the same SID to achieve connection. The default SID is ‘00000001’. *(8-digit hexadecimal form)*

- **NKey**[2]: (Network key) is a key used to encrypt all transmitted communications, providing a high security level and preventing “attacks” on your wireless network(s). The default NKey is ‘00000000’. *(8-digit hexadecimal form)*

- **RF Channel**[3]: is the operating frequency of the wireless network. There are 4 available channels (2, 3, 4 and 5) within the 868,150 – 868,450 MHz frequency range, to be used for your network(s), which can be switched during commissioning procedure. Where wireless networks operate nearby, a different RF Channel should be used on each network to avoid data traffic. The default channel is 2.

- **Hop level**: The hopping functionality is the fundamental feature of a mesh wireless network. Thanks to this, there is no need for direct connection between Network Master (Gateway) and every wireless device (luminaires, etc), as the message can be re-transmitted by any wireless device located between the Gateway and the target device, until it reached the end, as long as they belong to the same network and are in range. Therefore each wireless device is also a repeater (as shown in 'Figure 1'). The 'level' value indicates how many times the message was repeated (hopped) in order to reach the Gateway. Normally, a wireless network is able to perform up to 16 hops.

- **Network level**: Identical to Hop level, indicates the number of repeaters between the Gateway and a wireless device.

- **Self-Healing**: If a wireless device (e.g. a luminaire) which connects to the Gateway via hopping (network level 2 and above) loses connection with its link, it will automatically search for a new available route (if available) and reconnect. This function is quick and does not require human interaction.

- **Listen-before-talk**: Prior to transmitting any messages, a wireless device checks the communication

- **Master PC**: is the Windows PC running the "Advanced" version of "116-GR-7600/V2" software application and its services. Alternatively, a "116-GR-7610/V2" can be used instead, which runs the "Standard" version of the "116-GR-7600/V2" software application that works exclusively with USB Gateway models.

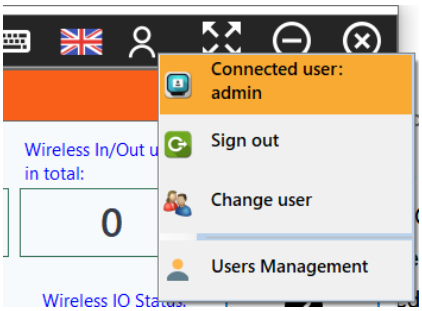
  ***1,2,3**: in order for Gateway and a group of wireless devices to form a network and connect with each other, they must all share the same **SID**, **NKey** and **RF Channel** values.*

  *When the **SID** and **RF Channel** between two devices **match**, but the **NKey differs**, there will be a wireless connection but the transmitted data will not be able to be decrypted, thus no valid data are received.*

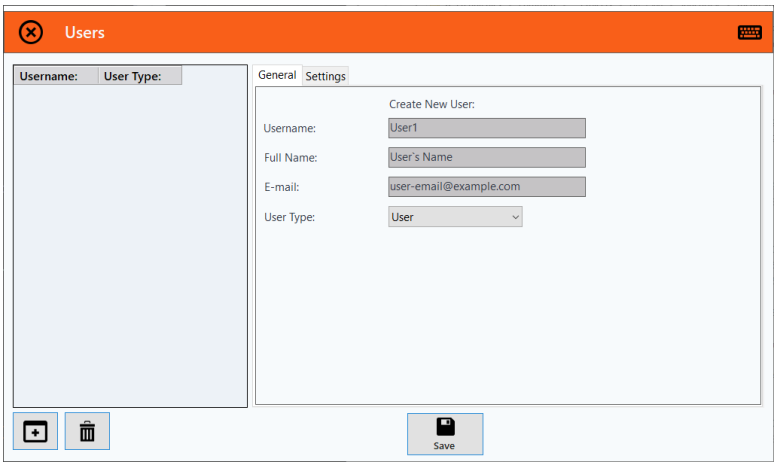
  *When the **SID** or the **RF Channel** between two devices **differ**, there will be no connection between those two devices and they are considered to belong to different networks.*

4. USER MANAGEMENT

After first login as “**Admin**”, you can create new users with “administrator” or basic “user” privileges. Go to “**Users Management**” option by selecting the user avatar icon on top bar.



In the form that is appearing, write the user’s username, full name, e-mail (optional) and then select the user type: “**administrator**” **type** grants full access for editing, adding, or deleting registered devices, apply settings regarding system behavior and initiate test procedures, “**user**” **type** grants limited access, where the user is able to monitor the status of the system and send light dimming commands, but the access to add, edit or delete is denied.



On the “**Settings**” tab, you can enable e-mail notifications for the current user. When done click “**Save**” and the new entry appears on the list on the left side.

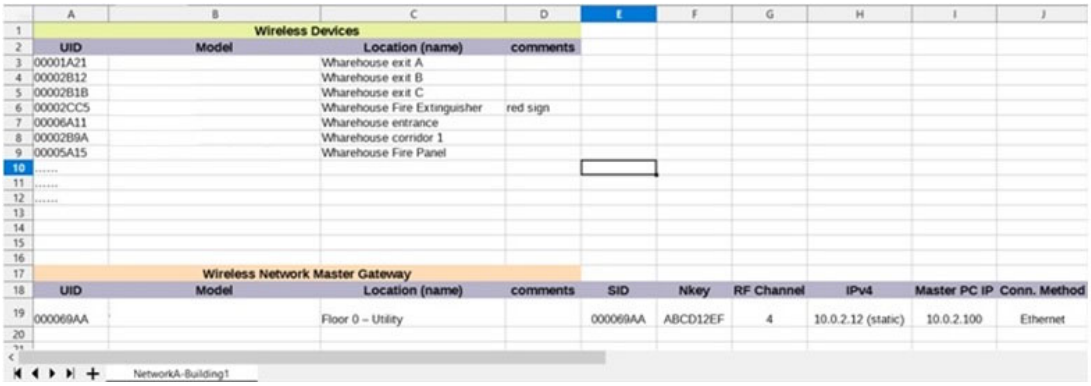
You can continue with “**Commissioning**” using the default “**Admin**” account, or you can create a new “**administrator**” **type** account for this purpose (recommended).

The system will ask for a new password on first login of the new created profile.

5. COMMISSIONING

5.1 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. Therefore you are advised to create at least a spreadsheet document, where you write down every aspect of the wireless emergency lighting installation. Create a new page 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		Wharehouse exit A							
4	00002B12		Wharehouse exit B							
5	00002B1B		Wharehouse exit C							
6	00002CC5		Wharehouse Fire Extinguisher	red sign						
7	00006A11		Wharehouse entrance							
8	00002B9A		Wharehouse corridor 1							
9	00005A15		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		Floor 0 – Utility		000069AA	ABCD12EF	4	10.0.2.12 (static)	10.0.2.100	Ethernet
20										

NetworkA-Building1

There is not any standard 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.

There are some network parameters that require consideration before proceeding into applying changes on wireless networks:

(For Advanced version): Regarding the IPv4 network parameters prefer 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 “116-GR-7600/V2” application, the IPv4 has to be static permanently.

The “**SID**” for a network can be any value that is in 8-digit hexadecimal form and has to be unique for each separate wireless network. Therefore, it is recommended to use the “**UID**” value of the Gateway, for the “**SID**” of the wireless network as well. Those two values will not conflict and are certainly unique.

The “**NKey**” value is a pass key that is used to encrypt wireless data, to prevent unwanted interaction from unauthorized acts. Once written to a wireless device cannot be retrieved for security reasons. Therefore, if the “NKey” value is written in the spreadsheet, it should be accessible only to authorized personnel.

The “**RF Channel**” is the operating frequency of the wireless network. The available RF Channels are 2, 3, 4 and 5 (868,150 – 868,450MHz range). Do not reuse RF Channels in neighbor networks, to avoid traffic. Optionally, you may use “Spectrum Analyzer” tool to check network traffic from other wireless systems on 868MHz, before assigning RF channels to each wireless network. You can re-use same RF Channels on networks whose distance is at least 80 meters apart between their closest devices.

5.2 Spectrum Analyzer

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

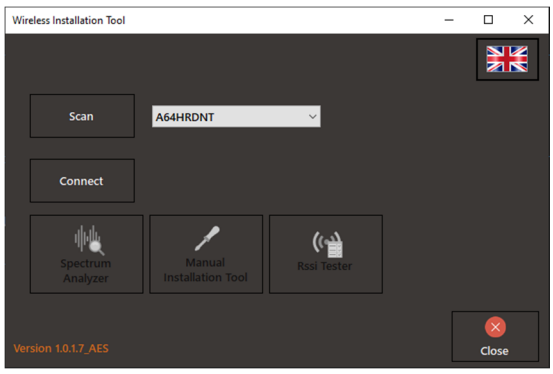
To use "**Spectrum Analyzer**" a USB device (116-GR-7605/V2 or 116-GR-7603/V2) is required.

The "Spectrum Analyzer" tool is included within the "**Wireless Installation Tool**" utility menu. The "Wireless Installation Tool" is implemented in "116-GR-7600/V2" application and is also available as a standalone version that can run on Windows 10. (Contact supplier for more information).

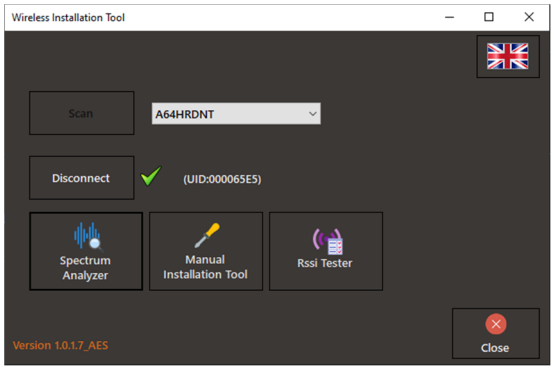
The "RF Channel" is the operating frequency of the wireless network. The available RF Channels are **2**, **3**, **4** and **5** (from 868,150 to 868,450MHz). The "Spectrum Analyzer" tool scans those 4 RF channels continuously, indicating maximum and average measurement values per each.

How to:

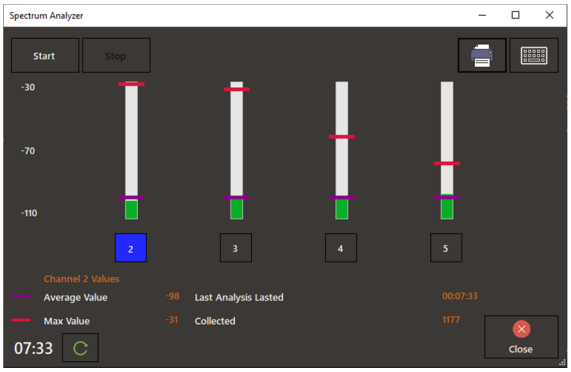
First, connect a "116-GR-7605/V2 RSSI Tester / USB Gateway" to an available USB port. Then, go to "**Installation** > **Wireless Installation Tool**" and on the window form appearing select "**Scan**". You will see the serial number of the USB device appearing in the list.



Select "**Connect**" and wait until you see the "**UID**" of the USB device appearing in the middle.



Now select "**Spectrum Analyzer**" option to run it. In the new window, click "**Start**" to run the procedure.



The columns are indicating the measurements in "**Average**" and "**Max**" values (dBm) in purple and red color respectively. Let the procedure run at least a minute (according to the timer bottom left). It is recommended to run the test into many areas of the installation for better results; reset the timer on each new position and count at **least 1 minute of scanning**, until you cover the area of a wireless network. In areas that another independent wireless network will be installed, run a new measurement by stopping the previous first. Then you will have more detailed results about occupied RF channels by area, so that you can use separate RF channels for each wireless network to avoid high RF channel usage.

Upon result, the RF channels that have high average and (or) high maximum values are ought to be avoided (later during network configuration). When average values between are almost equal, the RF channels with lower maximum value are better for usage. In the example picture above, RF channel number 5 is first in preference and 2 is last.

***IMPORTANT**: Note that the scale is in negative range, therefore -50dBm is higher than -100dBm, therefore, in average, a channel with -100dBm is considered to have less traffic than a channel with -50dBm.*

5.3 Connecting 116-GR-7603/V2 Ethernet + Wifi Gateway

The "**116-GR-7603/V2 Ethernet + Wifi Gateway"** which implements both Wi-Fi & Ethernet connectivity is compatible only with "**Advanced**" version of "**116-GR-7600/V2**" software application and needs an active **Ethernet** or **Wi-Fi** network in order to connect with the master PC, which must be within the same subnet.

The "116-GR-7603/V2" Gateway is capable of monitoring up to 200 wireless devices, consisted of wireless emergency luminaires, extenders, and input/output units, all forming a single wireless network.

You can establish communication between the "116-GR-7603/V2" and the master PC with the following ways:

- Ethernet – wired (DHCP or Static IPv4)
- Wi-Fi – WPA2/PSK (DHCP or Static IPv4)
- Wi-Fi – WPS

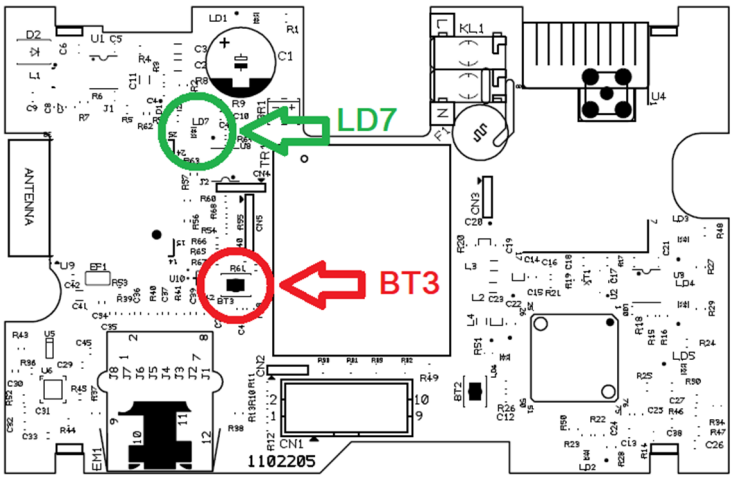
***IMPORTANT**: To continue with further configurations, a Wi-Fi device (DHCP) will be required (i.e. a smartphone, a laptop or a tablet)*

STEP 1 – ENABLE GATEWAY INVITATION VIA 116-GR-7600/V2 SOFTWARE

First, via the "116-GR-7600/V2" software user interface, go to "**Installation** > **Add IP Gateway**" and click "**Start**". The software will enter a mode to accept a new Gateway connection.

STEP 2 – CONFIGURE THE GATEWAY TO CONNECT TO LOCAL NETWORK AND 116-GR-7600/V2

While the device is active, open the front cover and press the "**BT3**" button located in the left part, inside of the device, for **3 seconds**. Avoid touching other areas of the device electronics. The "**LD7**" green LED will start blinking **2 times per second**, indicating the **Wi-Fi Access Point** running.

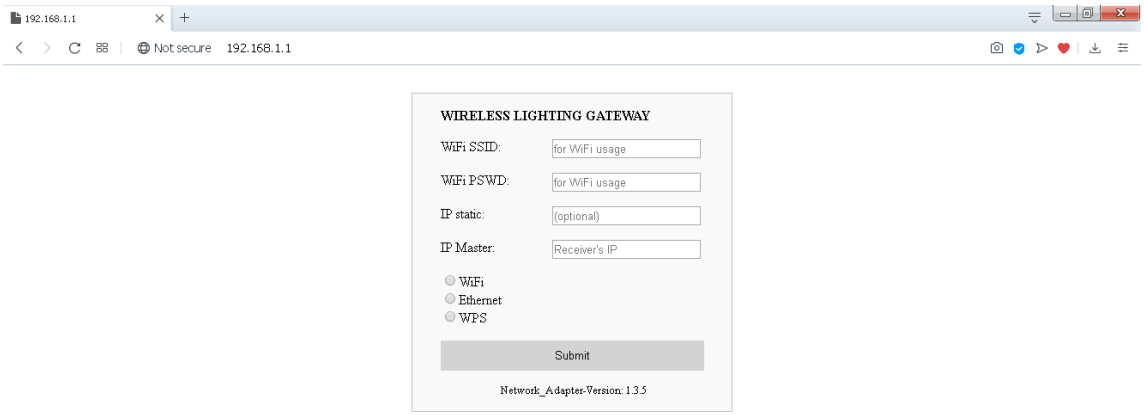


"BT3" button and "LD7" LED positions

Use your Wi-Fi device (laptop, smartphone) in order to connect to the Wi-Fi Access Point with the SSID (name):

"**WIRELESS_LIGHTING_GATEWAY**"
Use the following password when asked:
"**WIRELESSGW**"

Open a web browser via your Wi-Fi device and in the browser's URL area type the address "**192.168.1.1**" and then press "Enter". The following webpage appears:



Use your preferred connection method:

FOR ETHERNET CONNECTIVITY:

In order to connect the “116-GR-7603/V2” Gateway with the local network, using **Ethernet** connectivity, first the device must be connected to the local network using a UTP network cable with RJ45 male connector, to the corresponding **RJ45 port** on the bottom of the device.

In the “**IP static**” field write the static IPv4 address for this Gateway device, or leave empty for dynamic addressing (DHCP option).

Next, write the IPv4 address of the master PC (that is hosting the WelReceiver service), in the “**IP Master**” field. This value is required. Leave the rest of the fields empty.

Then, select the “**Ethernet**” option below and click “**Submit**” to apply changes.

FOR WI-FI (WPA2/PSK) CONNECTIVITY:

In order to connect the “116-GR-7603/V2” Gateway with the local network, using **Wi-Fi** connectivity, a Wi-Fi (802.11 b/g/n) network with WPA2/PSK security must be active and within range. The Gateway will join the Wi-Fi network **as a client**.

In the “**WiFi SSID**” field write the SSID (name) of the Wi-Fi network that the Gateway will join. The name is case sensitive.

In the “**WiFi PSWD**” field write the WPA2/PSK password of the Wi-Fi network.

In the "**IP static**" field write the static IPv4 address for this Gateway device, or leave empty for dynamic addressing (empty → DHCP).

Next, write the IPv4 address of the master PC (that is hosting the WelReceiver service) in the "IP Master" field. This value is required.

Then, select the "**WiFi**" option below and click "Submit" to apply changes.

FOR WI-FI (WPS) CONNECTIVITY:

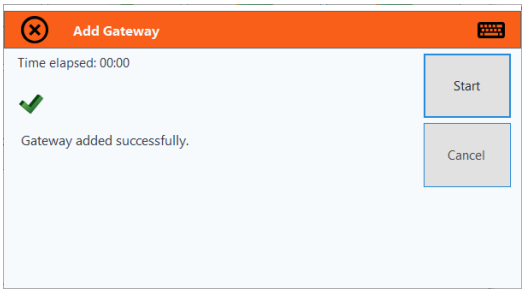
In order to connect the "116-GR-7603/V2" Gateway with the local network, using **Wi-Fi - WPS** connectivity, a Wi-Fi (802.11 b/g/n) network with WPS must be active and within range (use your laptop or smartphone to ensure signal level). The Gateway will join the Wi-Fi network as a client.

Write the IPv4 address of the Master PC (that is hosting the WelReceiver service), in the "**IP Master**" field. This value is required. Leave the rest empty.

Now, on your Wi-Fi router, click the "**WPS**" button to enable WPS invitation.

Then, back on the webpage select the "**WPS**" option below and click "**Submit**" to apply changes.

If your connection method succeeds, the "**LD7**" green LED will start blinking **1 time per second**, indicating successful connection.



On the "116-GR-7600/V2" software "**Add IP Gateway**" window, you will see a confirmation message "**Gateway added successfully**". Close the window and proceed into auto-detecting or easy-commissioning procedure.

5.4 Connecting a 116-GR-7607/V2 or 116-GR-7605/V2 as USB Gateway

The connection of a “116-GR-7607/V2” or “116-GR-7605/V2” as USB Gateway is simple. Connect the device to an available USB port of the master PC. Within a few seconds a new “Gateway” entry will appear. Now you can move into detecting devices and network configurations.

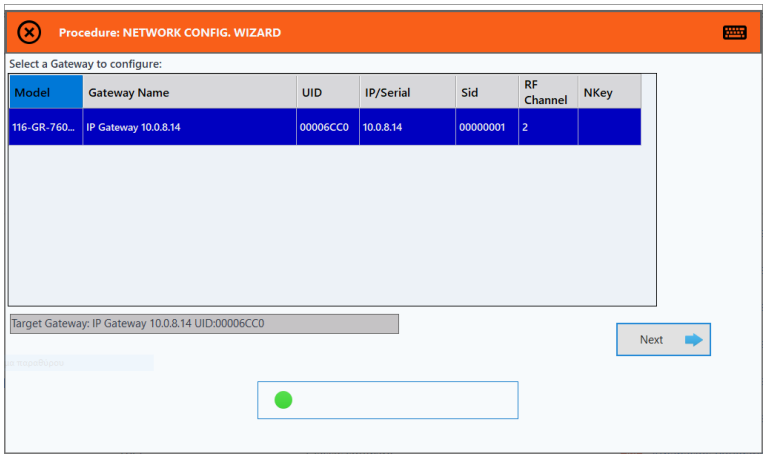
5.5 Network detection and configurations

When only one wireless network is installed, it is recommended to use the “**Network Configuration Wizard**” in “**Installation**” menu. This tool performs a quick network configuration to all connected devices simultaneously, by broadcasting configuration commands. Therefore it is intended to be used when only one wireless network exists, or when the neighbor networks are isolated by each other, using at least a different SID.

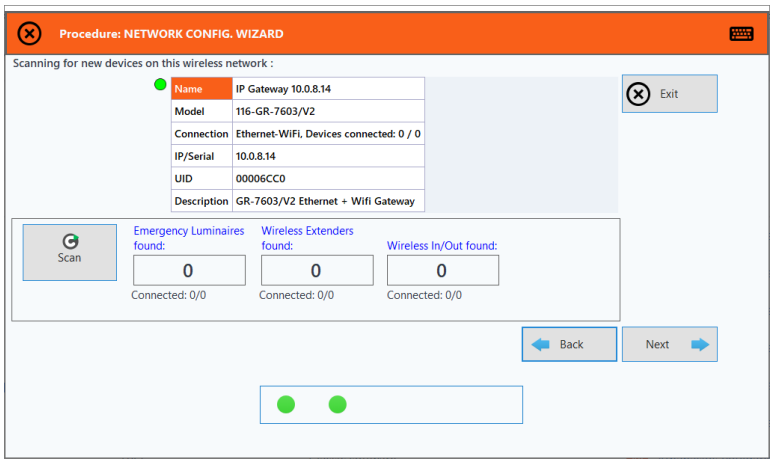
When multiple wireless networks are installed (≥2 Gateways), use the “**Easy Commissioning**” procedure in “**Installation**” menu. This commissioning procedure normally takes more time to complete and requires a good planning from before (spreadsheet document of wireless network details). It is designed to work when all wireless devices have been activated simultaneously without proper network formation and is transmitting configuration commands to each wireless device individually. Therefore it takes some more time to complete, yet it saves time from activating and performing configurations at one network at a time.

5.5.1 **Network configuration wizard** (single network)

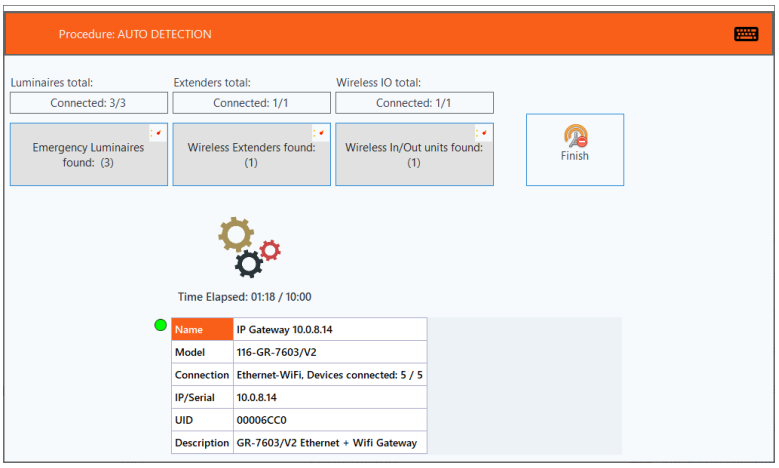
Go to “**Installation**” and select “**Network Configuration Wizard**”.



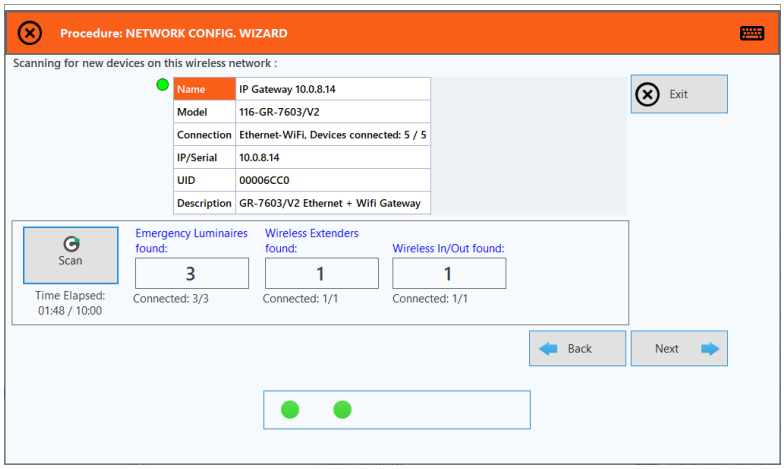
On the next window, you are prompted to select network (by Gateway). Click “**Next**”.

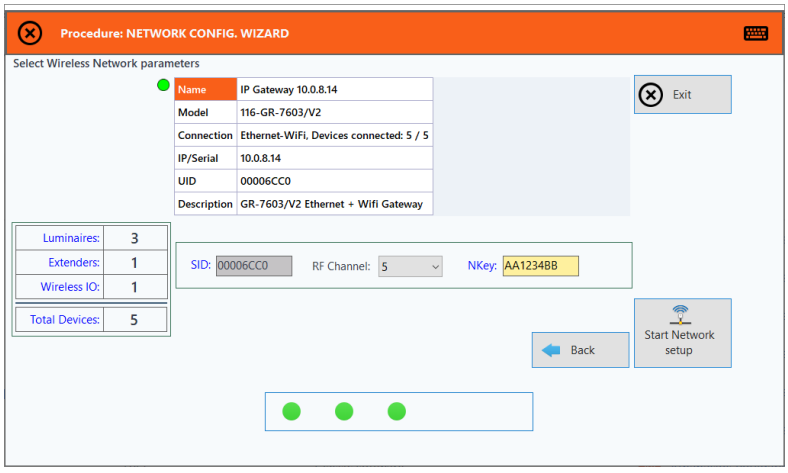


On the next window appearing, the network’s details and configurations are shown. If the network has no registered wireless devices (from previous “**Autodetection**”) then you can use “**Scan**” button to start “**Autodetection**” procedure, to find and register all available devices in the area.

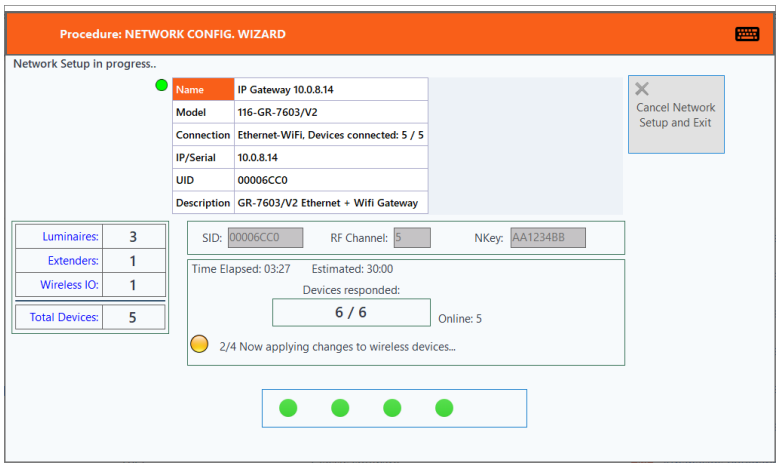


Once the system has detected all devices, click "**Finish**".

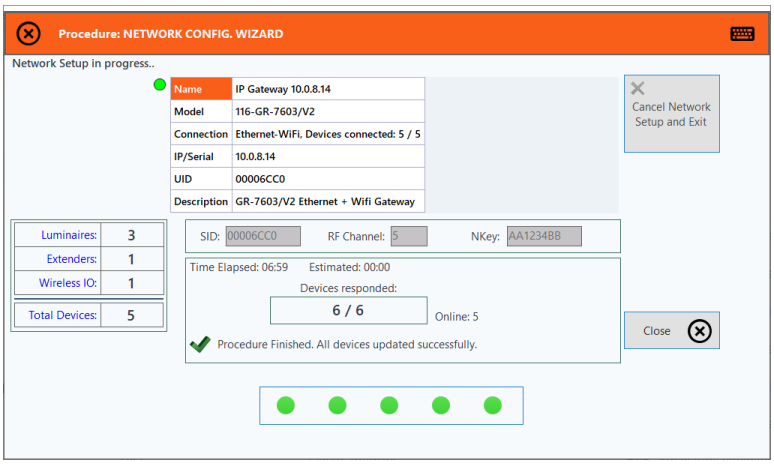




On the network details windows again, you have to provide "**SID**", "**RF Channel**" and "**NKey**" values for new network configurations. To avoid unwanted interference, use the recommended SID (which matches the UID of the selected Gateway). For "**RF Channel**" select a free channel, not occupied by other neighbor networks or other systems (see "**Spectrum Analyzer**" tool). For "**NKey**" use a password of your choice. The "**NKey**" must be also an 8-digit number of hexadecimal form (A – F & 0 -9). Then select "**Start Network Setup**".



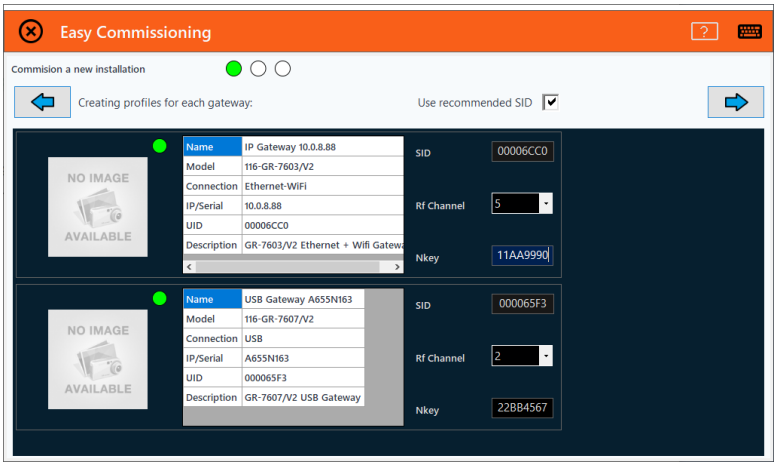
When all devices have responded to the network configuration request, the system will apply new settings to all wireless devices of this network and to its Gateway as well.



On end, click “**Close**” to exit the wizard.

5.5.2 **Easy Commissioning** (multiple networks)

Go to “Installation” and select “**Easy Commissioning**”. Select “**Commission a new installation**”.

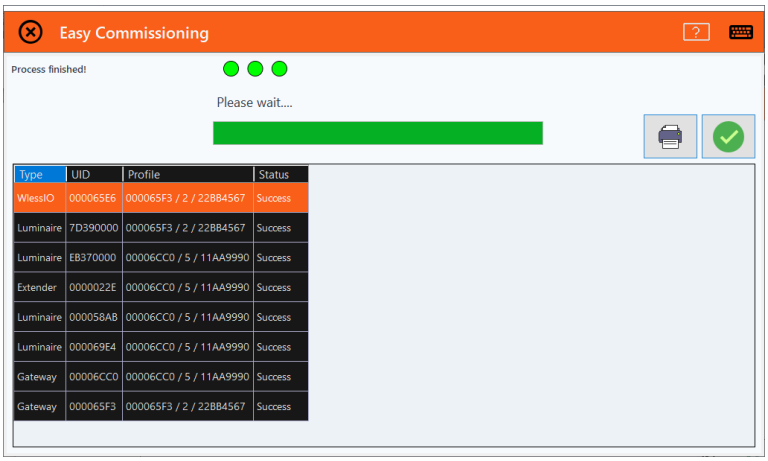


On the following window that appears, the registered Gateways are depicted. On the right side of each Gateway there are the network parameters. Select an “**RF Channel**” (different for neighbor networks), then enter an “**NKey**” of your choice, as a password (you may enter the same NKey to all networks or use a separate one). For the “**SID**”, use the recommended (must differ among networks). Then click “**Next**” to proceed.

Next, the main configuration window appears. Here you can select individual configurations for each detected wireless device. The “profile” of each network is depicted on the left side, while on the right side there is a list of the detected wireless devices. Wait a few minutes until the system detects all installed units (according to the installation plan).

Now, by identifying each device (luminaire or other) by its UID, using the installation plan (e.g. the spreadsheet document), select the corresponding network “profile” that his device should join. Select one row (or multiple by using “Ctrl” key) and then select “**Match Selected**” to apply

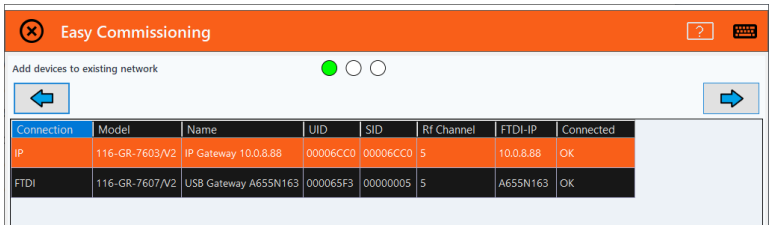
a network profile. Continue until you have assigned a network profile for each device and then click “**Next**” button.



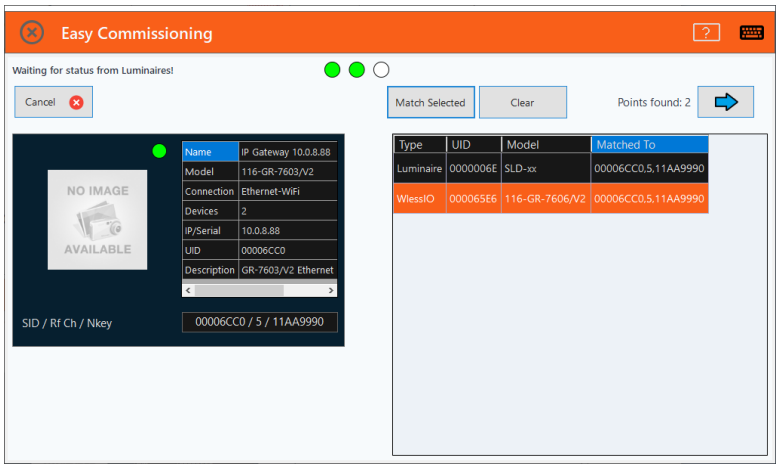
The system now is going through a procedure that sends unique commands to each selected wireless device to apply individual settings, so this may take a while. As a reference, for each Gateway and 100 wireless devices, it takes 20 minutes approximately. In the end, a full report of the procedure appears. You can print this report before exiting if there are failures, to review later.

5.5.3 **Easy Commissioning** (adding new devices)

When new wireless devices need to be added in an existing network, which has custom network parameters, the "**Easy Commissioning**" tool can provide a solution. By selecting "**Add devices to existing network**", the system temporarily switches the selected Gateway to factory default SID, RF Channel and NKey (00000001, 2 and 00000000) in order to **invite** new devices **to join** the specific network. This solution can also be used after one or more devices have failed to respond during commissioning and are considered "lost".



On the window that appears select the Gateway – network, in which the devices must join and click "**Next**" button.



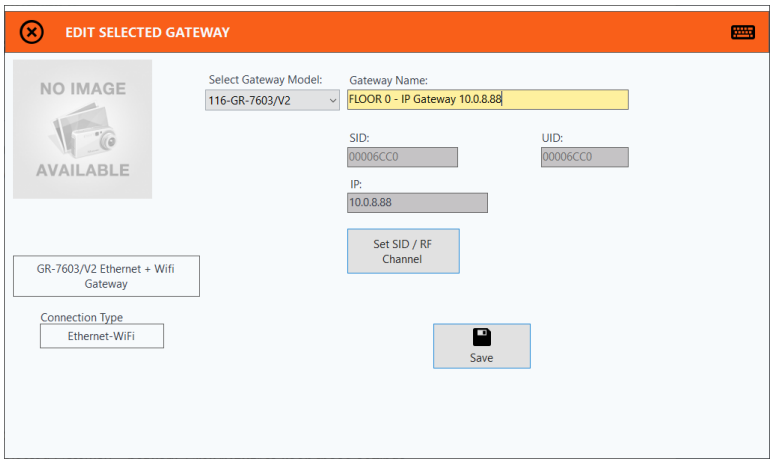
The following window is displaying the selected network on the left and on the right side there is a list with the detected devices (in default network parameters).

Select which of the devices you want to join this network (use "Ctrl" key to select multiple) and then select "**Match Selected**" to apply the parameters of this network profile. Click "**Next**" button when done to apply.

5.6 Edit Names

5.6.1 Edit Gateway name

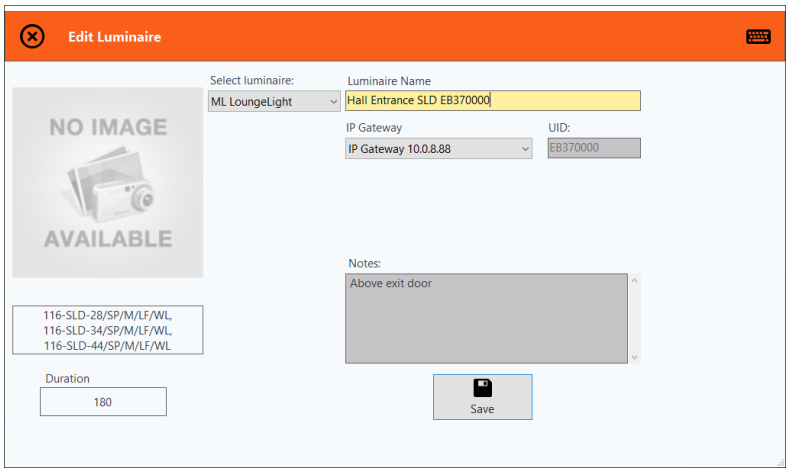
You can edit the name of a Gateway (thus the name of the network) by going in "**Wireless Devices** > **Gateways**" and then click on "**Edit Selected Gateway**" button at the top of the window.



On the form that appears, you can edit the field "**Gateway Name**" to change the name of the selected Gateway – network. Click "**Save**" to keep these settings.

5.6.2 Edit name of a wireless device

Similar to the Gateway, you can change the name of a wireless device, by going to "**Wireless Devices**" and selecting the device category (emergency luminaire, extender, Wireless In/Out units). Then click on the "**Edit**" button on top.

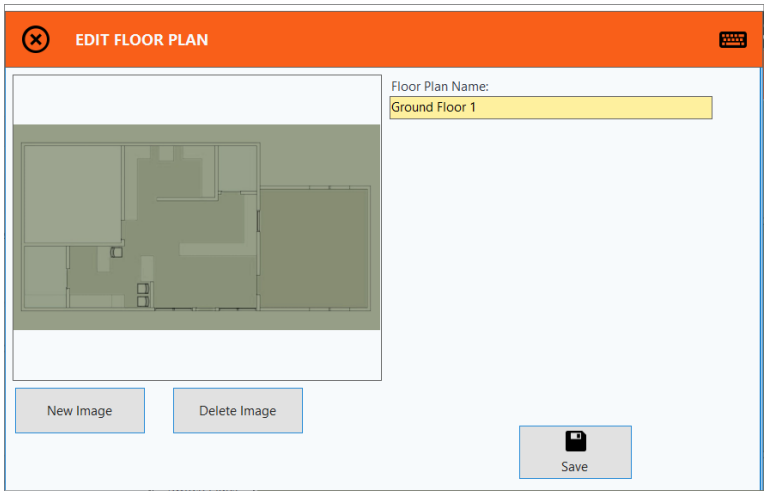


You can change the name of each device, by changing the field “**Name**” and then click “**Save**”. In addition, you can add extra notes in the “Notes” field below.

5.7 Creating Floor Plans

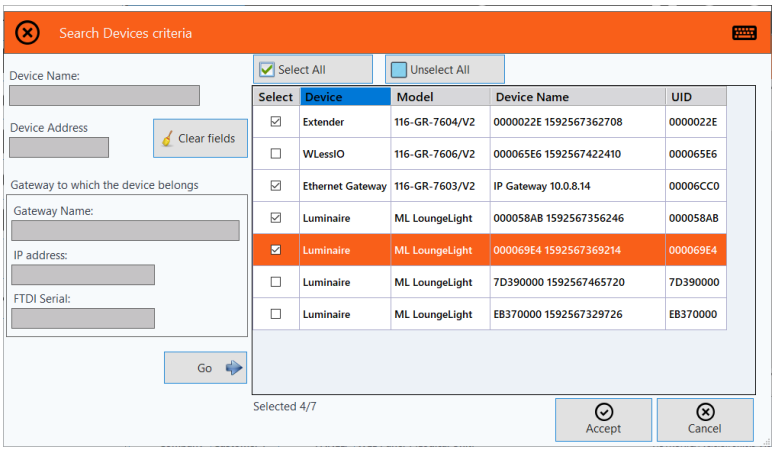
The “116-GR-7600/V2” software is equipped with “Floor Plans” tab, which is displaying a graphical view of the installation, with live icons which alter color according to state (emergency, fault, test, etc). This gives the user a better view of the operating state of the installation at a certain area (e.g. a floor).

To add a new floor, go to “Floor Plans” tab and select “Add New Floor Plan” button on top, write a name (e.g. Ground Floor 1) and save.



Then, load an image for this floor, by selecting “**Edit Floor Plan**” and then “**New Image**”. Select the location of the floor image and “**Open**”. You can open images directly from an external USB flash drive, which will be stored in the database upon opening. The image format must be “.jpg”, “.bmp” or “.png” and the resolution must be equal or a bit lower than the resolution of the monitor, to avoid “hidden” areas and scrolling for viewing. “**Save**” when done.

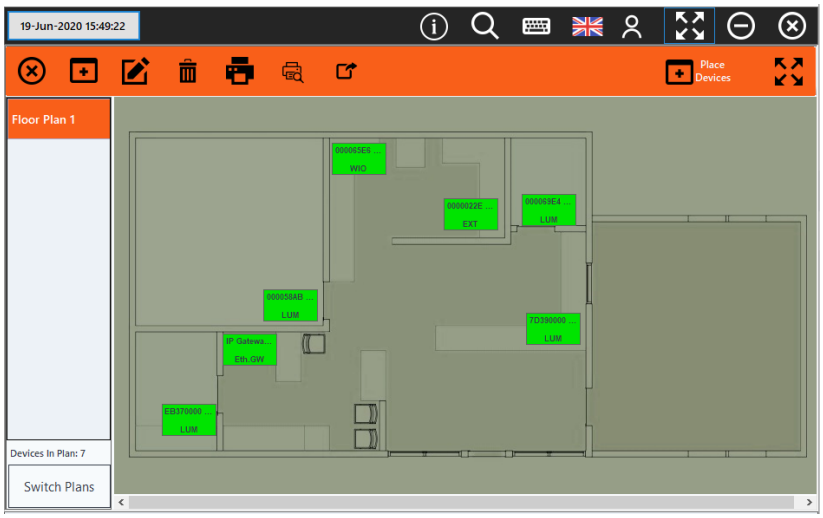
Now, in order to place wireless devices into place, clock on “**Place Devices**” button on top right.



The form that appears can work with filter criteria for faster finding. Select the devices that belong to this floor and then "**Accept**" to place.

All selected devices are placed into origin position (0,0) on top left of the image. Use drag'n'drop method to move each device into its location, according to the installation plan (use the "UID" to identify).

Continue with the rest of the floors and devices. An example is depicted below:



The icons are colored according to their current state:

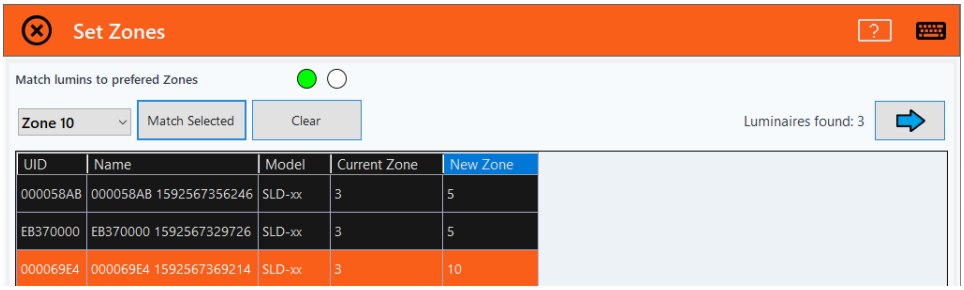
- Green → Normal mode (charging)
- Red → In Fault
- White → Disconnected
- Yellow → In Emergency mode
- Light Blue → In Test (lamp or battery)

In order to delete an icon, right click on it and select "**Delete**". In order to view details of an icon, right click on it and select "**Status Detail**".

5.8 Setting Zones for emergency luminaires

By setting a zone to each emergency luminaire, you can group devices together, even by different wireless networks, in order to perform lamp/battery tests by group. The default zone is **Zone 1** and there are **16 zones available**.

In order to assign zones to the registered emergency luminaires go to "**Installation** > **Set Zones**". On the list below, all register emergency luminaires are appearing. Select, one or multiple devices (using "Ctrl" key) and then select a zone from the drop down menu above. Then click "**Match Selected**" to match the selected zone to the selected emergency luminaires below. Continue until you assign a zone for each device, or leave empty to keep the old setting. "**Clear**" button resets selections.

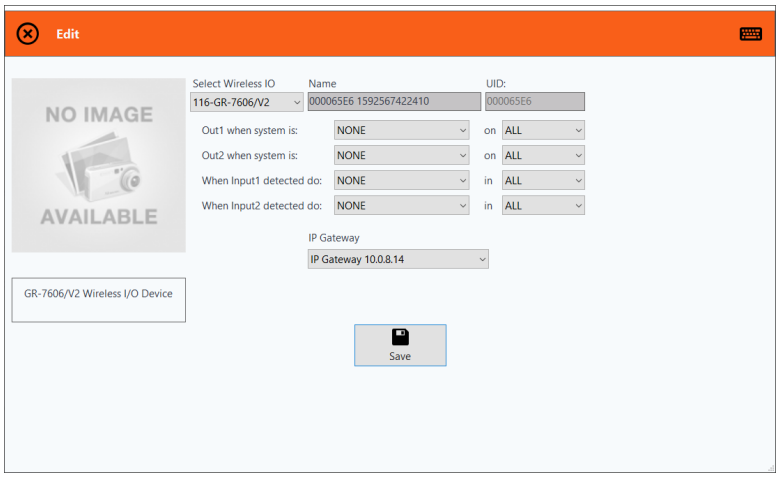


When you have finished assigning zones to emergency luminaires click "**Next**" key on the right sight to proceed. The procedure will take a few minutes to complete, according to the number of selected changes.

5.9 Configuring Wireless In/Out units triggers

The "**116-GR-7606/V2 Wireless In/Out Unit**" is a device that acts as a connection bridge between other informative or security equipment by providing 2 dry-contact relays which are used to inform about wireless emergency lighting status and 2 inputs that can initiate a lamp or battery test.

In order to configure a Wireless In/Out unit's triggers, go to "Wireless In/Out units" list, directly from the "Home" tab by clicking on the respective title, or via the "Wireless Devices" tab.
Then double-click on the entry you want to configure. A new information page opens up. On the right side, click on the icon "Edit" to open name and trigger configuration page.



From this page you can set Output relay 1 and Output relay 2 to be armed in case of lamp test, battery test, emergency mode or active test and by targeting a specific zone.

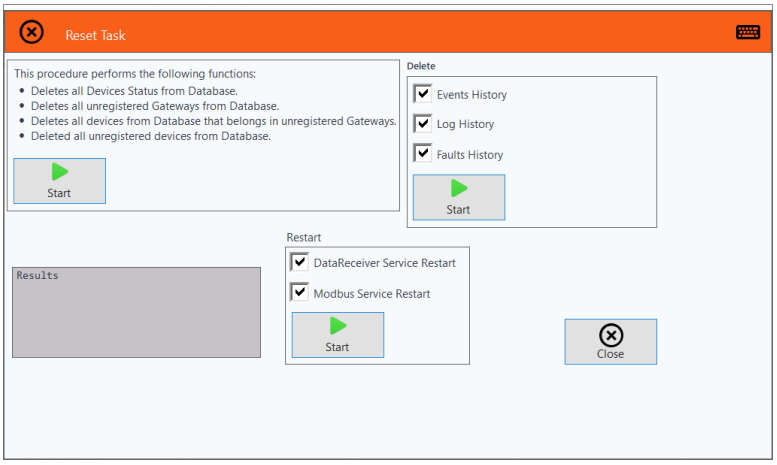
You can also set the 2 Inputs behavior separately, to initiate a lamp test or a battery test procedure when triggered and more specifically to a single zone.

6. RESET SYSTEM STATUS / CLEAR EVENTS

After commissioning, in order to clear the recorded events list of the events that were logged during network configurations, go to "**Home**" tab and select "**Other options**" icon on top right.

And then select "**Reset**" option.

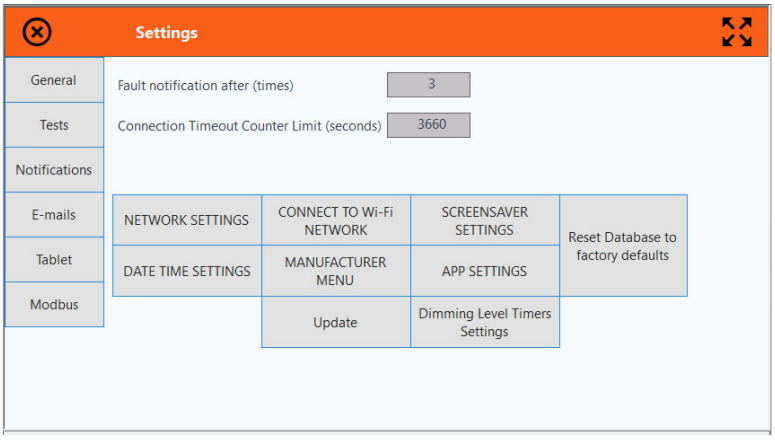
Here you have the options to delete events, faults and log, restart services and also delete all temporary status, unregistered devices, etc. The options are also explained in the picture below. Select which parts you need to delete and click "**Start**" to perform.



7. SYSTEM SETTINGS

In the "**Settings**" tab there are a series of options for system configurations.

7.1 General page



Fault notification after (times): this option defines the repeats of a fault that the system needs to confirm a valid fault. It is recommended to leave this value at default (3).

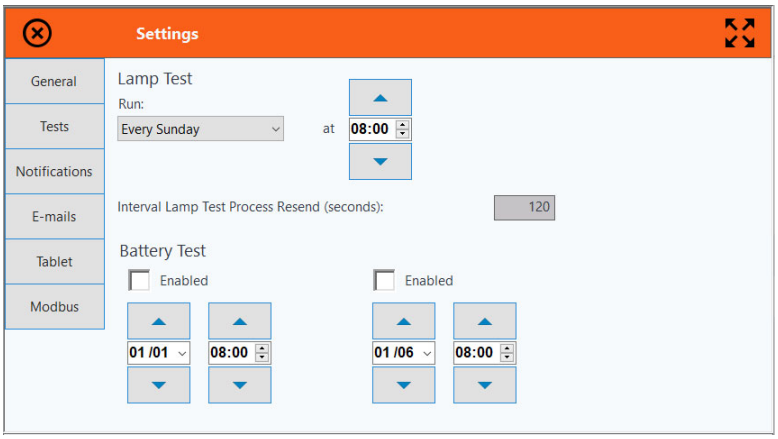
Connection Timeout Counter Limit (seconds): this option defines the time in which a wireless device is declared as "disconnected", if there is no status message within this time. It is recommended to leave this value at default (3660).

The rest of the options open following settings, according to their description.

7.2 Test page (schedule Lamp & Battery test)

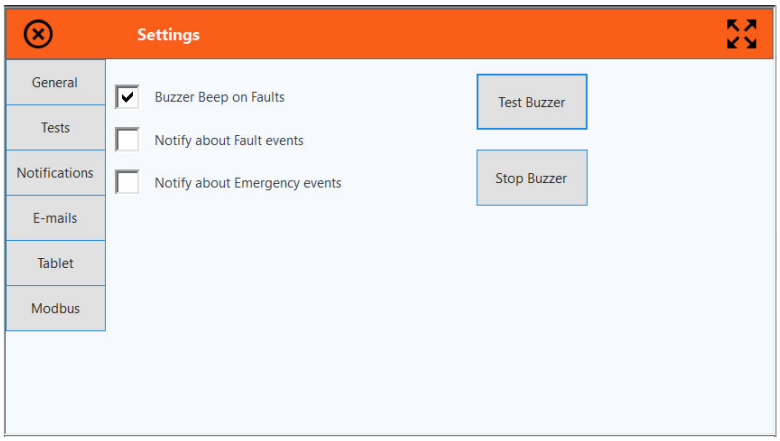
Via this page you can **schedule Lamp and Battery test** to run **automatically**.

Interval Lamp Test Process Resend (seconds): 120 – defines the time in seconds that the lamp-test commands will be resend. Do not alter this value.



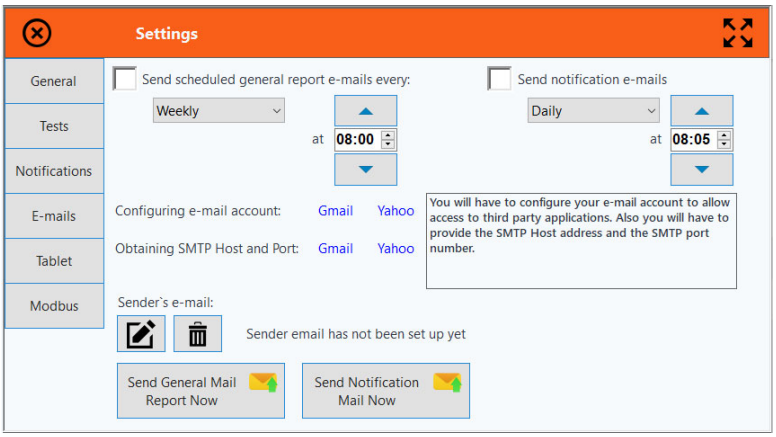
7.3 Notifications page

Via this page you can enable or disable certain types of notifications and test system buzzer.



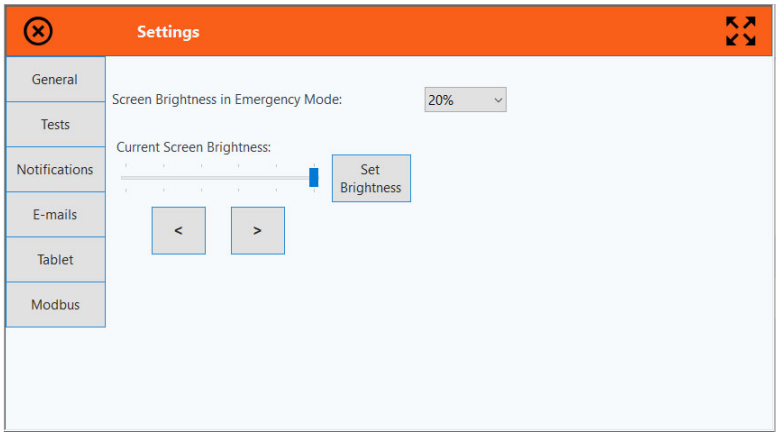
7.4 E-mails page

Via this page you can configure e-mail notifications and reports.



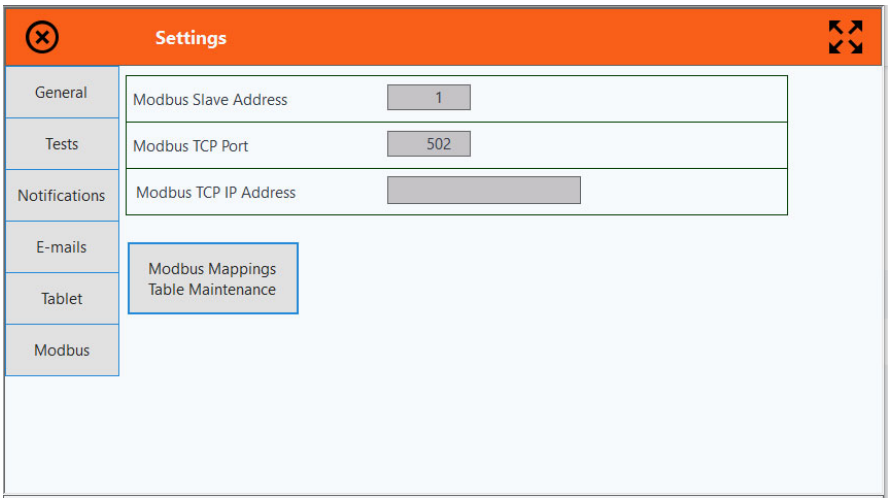
7.5 Tablet page

When using a “116-GR-7610/V2” as a master PC, via this page you can configure screen brightness levels.



7.6 Modbus page

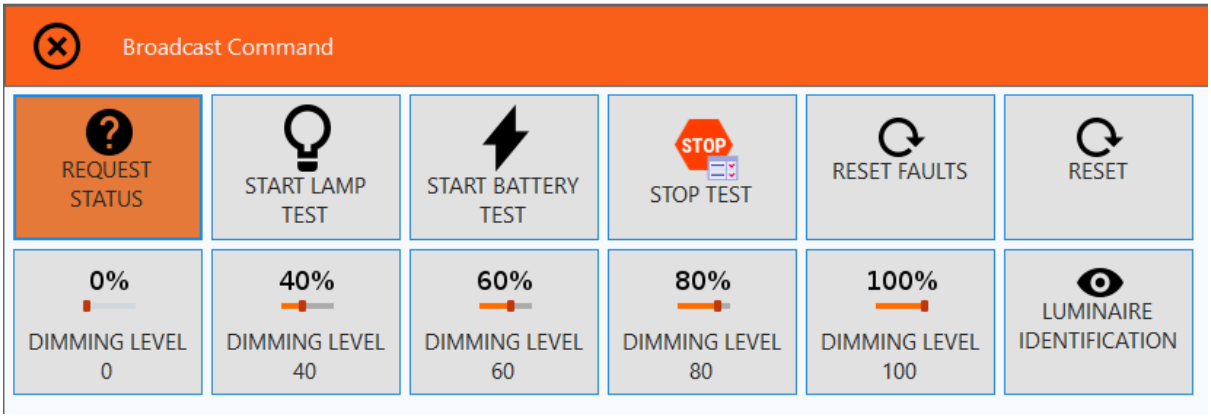
Via this page you can configure modbus service IPv4 address (TCP), port and modbus address. The "**Modbus Mappings Table Maintenance**" generates a new mapping table according to the registered devices in the system.



8. BROADCAST COMMANDS / RUN TESTS

Under this menu, there is a set of commands regarding emergency lighting. Broadcast commands are applied to all connected devices (or to selected zones where applicable). To open broadcast command menu, select the "**Broadcast Command**" icon located in "**Home**" tab.

This will show the menu form below:



The "**Request Status**", sends a command to all connected devices to respond with their current operating status back to the ystem. This is normally done automatically by every wireless device every 10', but this command will force for response. The response from each device might take up to 5'.

The "**Start Lamp Test**" initiates a procedure where every connected emergency luminaire will run a lamp test and respond back to the system with a result. Failed lamp tests will be reported in events list.

The "**Start Battery Test**" option, similar to the lamp test, runs a procedure where every connected emergency luminaire enters battery test mode. 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).

The "**Stop Test**" option stops all running tests.

The “**Reset Faults**” option sends a command to all connected emergency luminaires to clear faults currently recorded in their memory. Note that faults that are still valid will re-appear, until the fault is fixed.

The “**Reset**” command sends a message to all emergency luminaires to perform a system reset and clear all device faults. Use this option wisely and only when necessary.

Each “**Dimming Level**” option sets the light output of the connected emergency luminaires to the selected level.

The “**Luminaire Identification**” option initiates a flashing sequence on the function indicator LEDs of the emergency luminaires (green-red-yellow). As broadcasted has no significant usage, but it is useful when you need to identify a unit which has no markings on it (such as a written “UID” or name), by sending it to a single device at a time (go to “Wireless Devices > Luminaires > *double click on the entry* > More Commands > Luminaire Identification”.

9. IMPORTANT NOTES

Wireless Network settings (SID, RF Channel & NKey) are stored in the hardware memory of each wireless device individually. In order to restore these values back to defaults (00000001, 2, 00000000) either use the "Network Configuration Wizard", or in case the communication has been lost perform reset-to-defaults to each one device via the dedicated on-board button (see product manual).

In case of a Gateway failure, you can replace it with a new one and set the same wireless network settings (SID, RF Channel and NKey) manually, without resetting all connected wireless devices to factory defaults. This option can be found under "WIRELESS DEVICES > GATEWAYS > EDIT SELECTED GATEWAY > SET SID & RF CHANNEL". This option only changes the SID and RF Channel values of the Gateway and not in the connected wireless devices.

After the completion of the commissioning procedure, it is recommended to run a lamp test to ensure proper communication with the emergency luminaires. If your system includes interconnection with other security systems (e.g. via a Wireless Input/Output unit), simulate a system event by triggering the input to ensure proper functionality of the Wireless Emergency Lighting.

Our vision

Zero loss of lives

no injuries or damages caused by fire and gas

www.autronicafire.com

Carrier

Autronica Fire and Security AS

A Carrier Company

www.autronicafire.com