smartDEN Opener

Multifunctional Opener Module
for garage doors, barriers, blinds, awnings, roofs

User Manual
Date: 24 Apr 2018

For firmware version: v1.00 / Apr 2018

Content

1. Features 3
2. Application examples 6
3. Technical parameters 11
4. Internal block diagram 13
5. Connectors, ports and led indicators 14
6. Installation 16
7. Default settings 41
8. Wi-Fi Interface 43
9. Main Controlled Device 44
10. Web access 46
11. HTTP server 97
12. MQTT protocol 103
13. Security considerations 108
14. Mechanical drawing 109
15. Appendix 1. Connecting external controller to smartDEN Opener relays 110
16. Appendix 2. DAE-aModules 111
17. Appendix 3. Char set 117
18. Appendix 4. Dictionary 118
19. Appendix 5. Disclaimer 119

1. Features

smartDEN Opener is multifunctional web enabled Wi-Fi wireless 802.11 b/g/n module for controlling garage doors, barriers, awnings, windows, blinds. Its concept is to combine smart IoT solution for managing your door or window via Internet from computer or smart phone while RF 433 MHz remotes are kept at the same time. Additionally the extra built-in relays can control another two devices and several sensors can be connected as well to provide easy monitoring and sending emails and notifications to smart phone. **smartDEN Opener** supports internal weekly schedule which enables open/close by date and time and even allowing access for second user (guest or neighbor for example). Internal logs are kept into device EEPROM and can be accessed anytime. With the *DAE-aModules* android app it is possible securely to open/close the **smartDEN Opener** from smart phone and to control it via GPS location (for example when approaching your garage door).

For system integrators we provide two communication protocols (MQTT and HTTP/XML/JSON) for embedding in third parity systems (such as home automation servers for example) and lot of software examples.

Motor Control:

- 1 x Motor control channel with maximum load (current): 4A;
- Suitable for garage doors, barriers, awnings, windows;
- Secured with fuse;
- Programmable opening(closing) time;
- "Auto-close" function based on timer and/or sensor;
- Supported types of motors:
  - Reversible AC asynchronous (induction) motors equipped with limit switches;
  - Reversible DC motors equipped with limit switches;

Two independent protection options:

- Via digital input using IR beam sensor;
- Via programmable over-current motor limit;

Relays:

- 2 x SPDT Relays;
- Contacts parameters: 10A / 250VAC, 15A / 120VAC, 10A / 28VDC;

Digital Inputs:

- 3 x optically-isolated;
- Status led for each;
- Input voltage: 3-24VDC;
- Power output: 12VDC or 24VDC for sensors;

Analog Input:

- 1 x analog input (ADC);
- Input voltage: 0-5VDC;
- Power output: 5VDC for sensors;

Temperature Sensor Input:

- 1 x temperature input channel for sensor DALLAS;
- Supported sensors models: DS1820, DS18S20, DS18B20;
- Maximum cable length: 20 meters;
- Power output: 3.3VDC for sensors;
- Software selectable units °C or °F;

RF remote control:

- 2 x pocket remotes for open/close (additional can be purchased separately);
- Working frequency: 433 MHz;
- Working distance: 50 meters open area;
- Encryption: rolling code;
- Programming the opening (closing) time function;
- Maximum number of stored remotes: 20;

Standalone modes:

- Weekly schedule events table for automatic actions: max 20 events;
- Controlling motor and relays based on sensors automatically;
- Timer functions;

Built-in real time clock (RTC):

- Used for schedule (calendar) stand-alone work;
- Option for auto-synchronization via Internet (NTP);
- Daylight savings option;
- Back-up power supply keeps the time for days when power off;

Communication:

- Wireless Wi-Fi 802.11 b/g/n standard;
- External Wi-Fi antenna 3 dBm for better range;
- Supported Wi-Fi modes: Access Point (AP), Station (STA);
- Supported Wi-Fi encryption modes:
  - WEP;
  - WPAPSK-TKIP;
  - WPAPSK-AES;
  - WPA2PSK-TKIP;
  - WPA2PSK-AES;
- Protocols: HTTP, DHCP, DNS, NTP, ICMP (ping), MQTT(QoS 0), XML, JSON, SMTP;

Web Interface:

- System configuration and monitoring;
- Setup and control the motor open/close timings and I/O;
- IP camera embedding option;
- Setup the weekly schedule;
- Backup and restore function of all the parameters;
- Access the logs;
- Secure login authorization;
- Access protection (by IP and MAC address);
- Mobile friendly interface;

Push notifications upon event:

- Emails notifications (no SSL supported, only AUTH PLAIN LOGIN);
- MQTT (Android) notifications - accessible from *DAE-aModules*;

Events log:

- Internal EEPROM memory for events log;
- Minimum 330 (typical 400) I/O events;
- Minimum 270 (typical 400) system events;

TCP/IP Services:

- HTTP server: Access (GET) current measurements in XML/JSON format, download log files in .txt format;

Two types of power supply options selectable during purchase:

- DC power supply: DC12V
- DC power supply: DC24V

Physical and Environment:

- Working temperature range: -25°C ~ +70°C;
- Working humidity range: 40% ~ 85%;

Two types of housing selectable during purchase:

- DIN rail box: 157 x 86 x 58 mm;
- IP65 box: 200 x 155 x 80 mm;

2. Application examples

smartDEN Opener could be used in wide range of home automation and access control applications. Several application examples how **smartDEN Opener** could be used are shown bellow. The examples are only conceptual and an additional equipment/connections should be considered in actual implementations.

2.1. Barriers

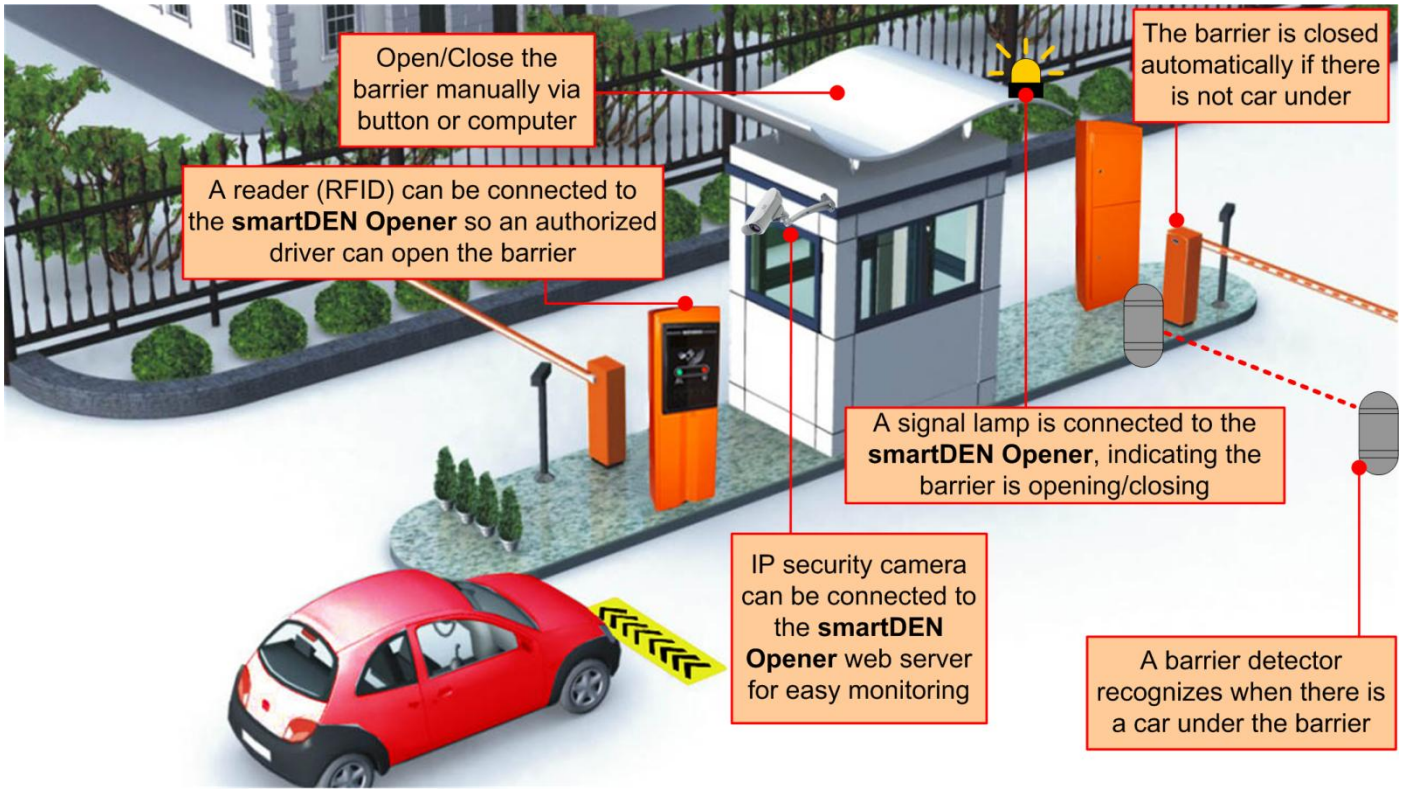

Figure 2.1. Controlling a barrier

smartDEN Opener can be used successfully for opening/closing barrier. Here are the benefits using **smartDEN Opener** for such kind of application:

- Easy set-up of the opening/closing time from web browser, RF remote.
- Open/close from web browser, computer software or mobile smart phone (for example using mobile app *DAE-aModules*);
- Embedding IP camera in the web server, allows integrated solution for monitoring/control the barrier;
- An RFID reader with SPST output can be connected to one of the optically-isolated digital inputs to open the barrier;
- RF remote can open / close the barrier (up to 20 unique RF remotes can work with single **smartDEN Opener** module);
- A barrier IR beam sensor can be used for car detection and barrier strike prevention;
- Auto-closing function when the car has passed;
- **smartDEN Opener** internal log files can be accessed any time;
- External lamp can be controlled by **smartDEN Opener**;

2.2. Garage doors

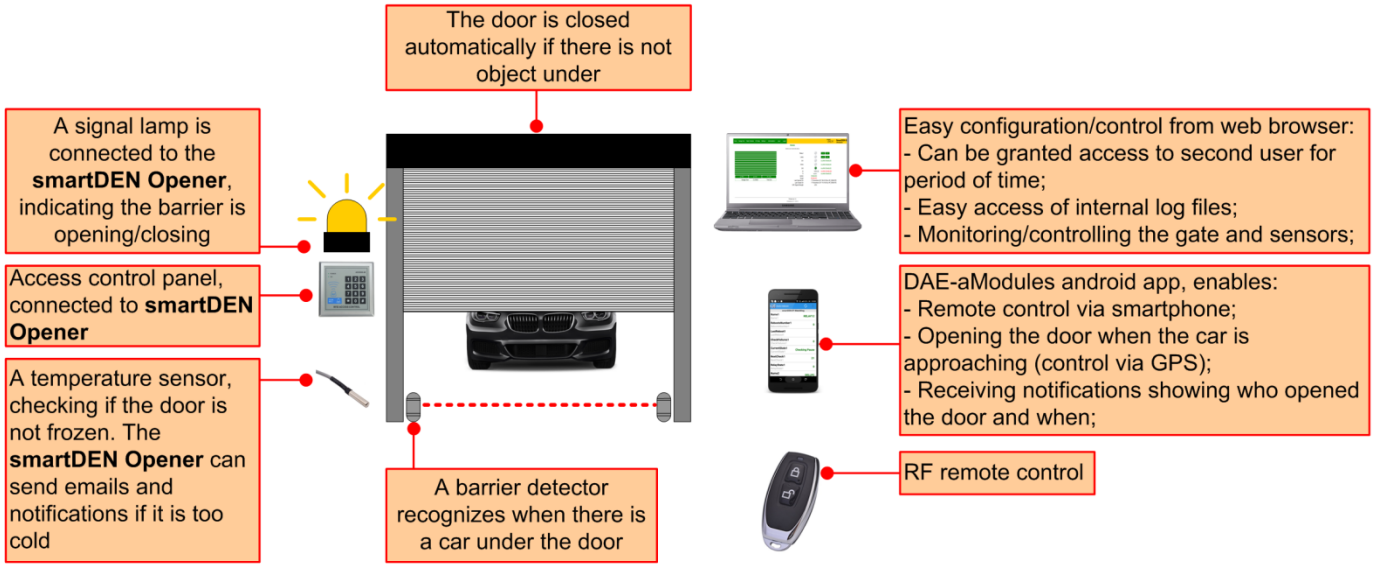

Figure 2.2. Controlling a garage door

smartDEN Opener is also very useful in application requiring garage door control. It provides smart control via mobile phone or internet and open/close via RF remote at the same time.

- Easy set-up of the opening/closing time from web browser, RF remote.
- Open/close from web browser, computer software or mobile smart phone (for example using mobile app *DAE-aModules*);
- Using *DAE-aModules* android app, it is possible to open the door automatically when the car is approaching it (using GPS);
- Embedding IP camera in the web server, allows integrates solution for monitoring/control the door;
- An RFID reader with SPST output can be connected to one of the optically-isolated digital inputs to open the barrier;
- RF remote can open/close the door (up to 20 unique RF remotes can work with single **smartDEN Opener** module);
- A barrier IR beam sensor can be used for car detection and barrier strike prevention;
- Auto-closing function when the car has passed;
- **smartDEN Opener** internal log files can be accessed any time;
- External lamp can be controlled by **smartDEN Opener**;
- A temperature sensor can be connected in order to send notifications if door is frozen;

2.3. Awnings

Figure 2.3. Controlling an awning

Motorized awnings also can be controlled via **smatDEN Opener** with success. Besides the regular open/close function, here the **smartDEN Opener** can provide and function to close the awning if the wind speed is too high. Thanks to its internal schedule the awning can be controlled automatically standalone by date/time or a light sensor can be used as well.

- Easy set-up of the opening/closing time from web browser, RF remote.
- Open/close from web browser, computer software or mobile smart phone (for example using mobile app *DAE-aModules*);
- A light sensor can be used to open/close the awning;
- The internal weekly standalone schedule with RTC can control the awning based on date/time;
- RF remote can open/close the awning (up to 20 unique RF remotes can work with single **smartDEN Opener** module);
- An internal current measurement solution can be used optionally in order to protect the motor from awning hits detecting its consumption in real time.
- **smartDEN Opener** internal log files can be accessed any time;
- A wind sensor can be connected in order to close the awning if storm is coming;
- Sending notifications and emails about weather temperature, light and wind level;

2.4. Roof windows

Figure 2.4. Controlling a roof window

Roof windows can be controlled by **smartDEN Opener** as well. Additionally the rich amount of sensors and the capability of sending notifications make the device ideal for home automation and even security applications.

- Easy set-up of the opening/closing time from web browser, RF remote.
- Open/close from web browser, computer software or mobile smart phone (for example using mobile app *DAE-aModules*);
- Wall switch can be connected to some of the digital inputs for manual open/close;
- RF remote can open/close the door (up to 20 unique RF remotes can work with single **smartDEN Opener** module);
- A sensor can close the window if rain is detected;
- **smartDEN Opener** internal log files can be accessed any time;
- A temperature sensor can be connected in order to send notifications if window is frozen;
- Connecting light sensor for open/close the window during the day/night;
- Scheduled standalone timings for opening/closing the window;
- An internal current measurement solution can be used optionally in order to protect the motor from window hits detecting its consumption in real time.
- A wind sensor can be connected in order to close the window if storm is coming;
- Sending notifications and emails if the window is opened by third parity;

2.5. Window blinds

Figure 2.5. Counting visitors in shop

Motorized window blinds are also possible to be automated via **smartDEN Opener.** Here the benefit is that the module can be scheduled to set up/down the blinds standalone by internal clock (weekly schedule). From the other hand a sunlight sensor can do that as well. Opening via mobile phone (android app *DAE-aModules*), web browser, computer, wall switch, RF remote...

- Easy set-up of the up/down time from web browser, RF remote.
- Set up/down from web browser, computer software or mobile smart phone (for example using android mobile app *DAE-aModules*);
- Wall switch can be connected to some of the digital inputs for manual open/close;
- RF remote can set up/down the blinds (up to 20 unique RF remotes can work with single **smartDEN Opener** module);
- A light sensor can set up/down the blinds;
- **smartDEN Opener** internal log files can be accessed any time;
- Scheduled standalone timings for automatic setting up/down the blinds;

3. Technical parameters

Table 3.1. Physical parameters

Parameter	Value
Size DIN Rail Box (L / W / H), mm	157 x 86 x 58 mm;
Size Distribution Box (L / W / H), mm	200 x 155 x 80 mm;
Operating temperature, °C	-25 to +70

Table 3.2. System parameters

Parameter	Value
Power supply voltage, VDC	12 or 24 (selectable during purchase)
Maximum current consumption, mA	350 @ 12VDC or 250 @ 24VDC
Protection against reverse polarity	Yes
Default settings button	Yes
Reset button	Yes

Table 3.3. Motor control

Parameter	Value
Channels count	1
Maximum controlled motor current, A	4
Supported motor types:	• Reversible AC asynchronous (induction) motors equipped with limit switches; • Reversible DC motors equipped with limit switches;
Programmable opening/closing time	Yes
Over-current motor protection	Yes, software programmable
Second protection against hitting	Yes, using one of the digital inputs

Table 3.4. RF control

Parameter	Value
Communication frequency, MHz	433
Open/close function	Yes
Programming open/close time:	Yes
Maximum distance (opened area), m	50
Maximum stored remotes:	20
Encryption	Rolling code

Table 3.5. Analog Inputs

Parameter	Value
Analog inputs number	1
Analog inputs full scale voltage range, VDC	0 up to 5
Analog inputs absolute maximum non-destructive voltage, VDC	24
Analog inputs resolution, bits	10
Value of LSB, mV	~5
Input impedance, KΩ	68

Sample period, ms	100
	200
Protection against reverse polarity	Yes

Table 3.6. Digital Inputs

Parameter	Value
Digital inputs number	3
Digital inputs voltage range, VDC	0 up to 24
Optical isolation	Yes
High level, VDC	>3.0
Low level, VDC	<3.0
Supported sensor output type	SPST Relay Output (NO, NC)
Sample period, ms	100
	200
Protection against reverse polarity	Yes

Table 3.7. Relays

Parameter	Value
Relays number	2
Relay type	SPDT
Relay contacts parameters:	10A / 250VAC, 15A / 120VAC, 10A / 28VDC
Electrical life expectancy, operations:	100 000
Mechanical life expectancy, operations:	10 000 000

Table 3.8. Temperature Inputs

Parameter	Value
NTC inputs number	1
Sensor type	DALLAS One Wire
Pull-up to 3.3V, kOhm	2.0
Supported sensor models:	DS1820, DS10S20, DS18B20
Sensor working temperature range, °C	From -55 to +125
Maximum cable distance, m	20
Accuracy, °C	±0.1, ±0.5 (depends on the sensor)
Sample period, ms	1000

Table 3.9. Network

Parameter	Value
DHCP	Yes
DNS	Yes
Hardware Real Time Clock (RTC)	Yes
Network parameters	IP/Mask/Default gateway
IP lock (protection)	Yes
MQTT	Yes
Secure HTTP/XML access	Yes
Web server for configuration/access	Yes

4. Internal block diagram

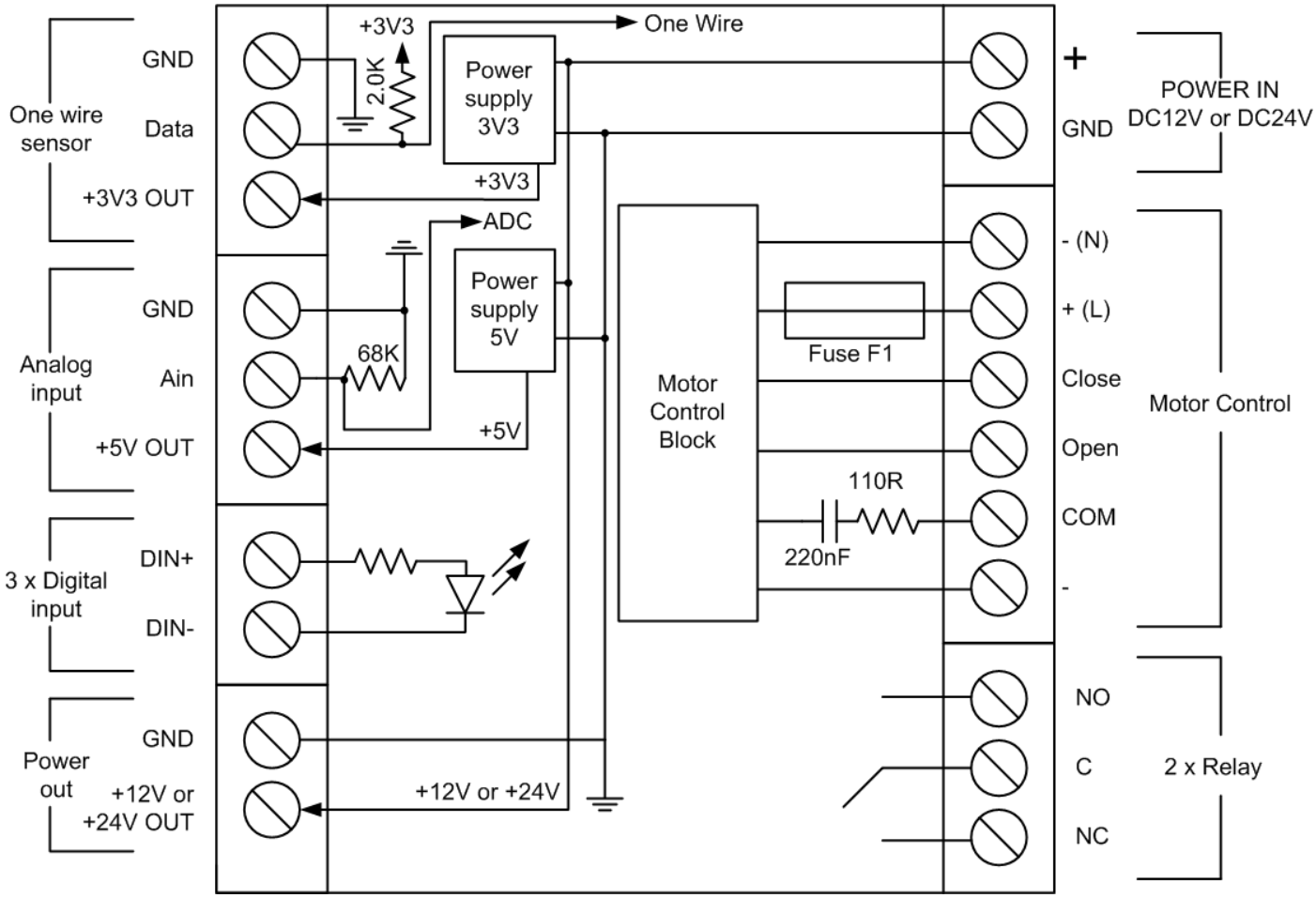

Figure 4.1. Internal block diagram of **smartDEN Opener**

5. Connectors, ports and led indicators

Bellow is shown a picture with the device connectors, ports and led indicators.

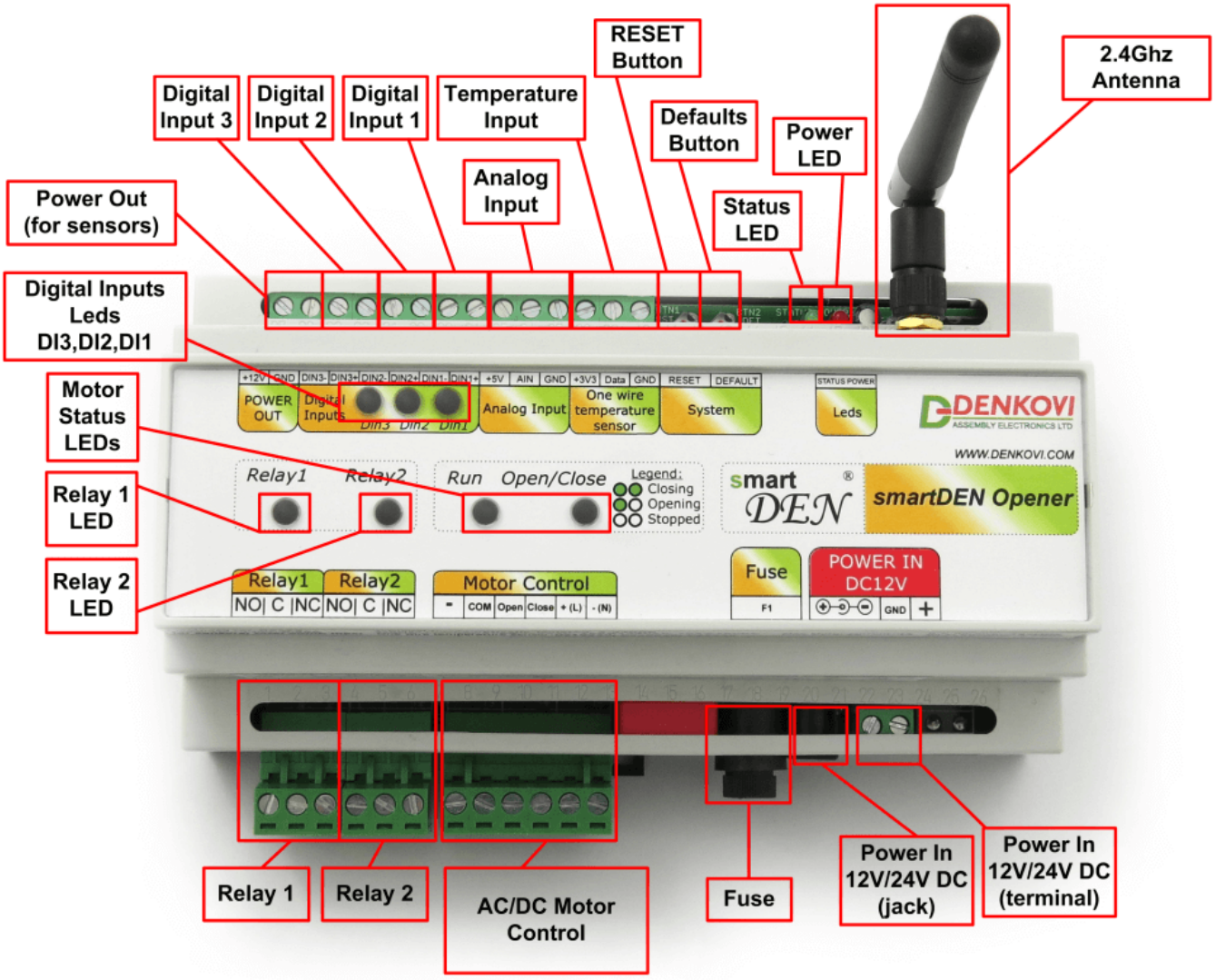

Figure 5.1. DIN rail version overview

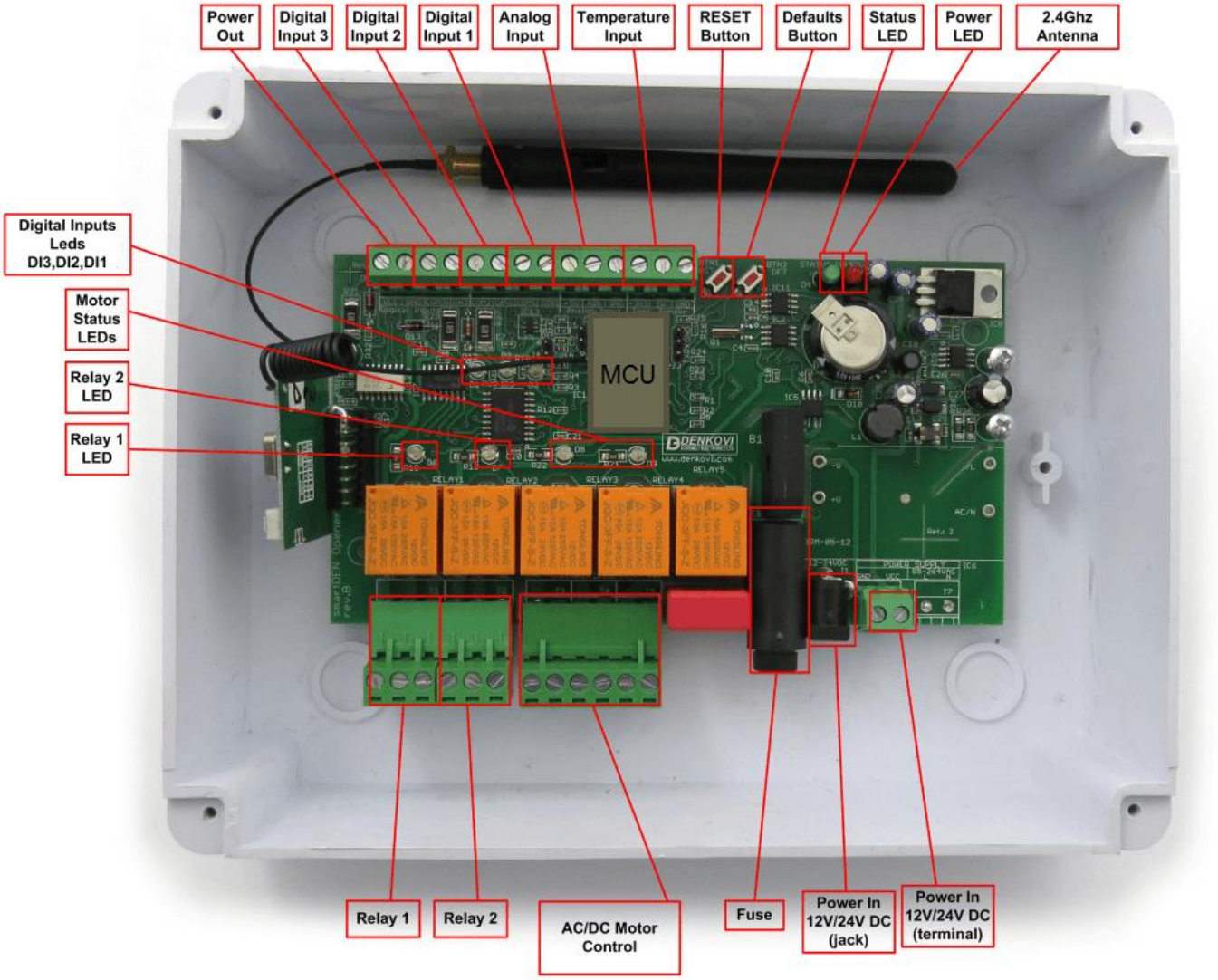

Figure 5.2. Distribution box version overview

6. Installation

- This device must be installed by qualified personnel;
- This device must not be installed directly outdoors;
- Installation consists of:
  - Mounting the device;
  - Connecting motor controlled load, in way described below;
  - Connecting other loads to relays;
  - Providing power;
  - Connecting to an IP network and configuring via a web browser.

6.1. Box mounting

6.1.1. DIN rail box

Figure 6.1. Mounting the device to DIN rail

smartDEN Opener can be mounted to a standard (35mm by 7.55mm) DIN rail. Attach the module to the DIN rail by hooking the hook on the back of the enclosure to the DIN rail and then snap the bottom hook into place.

6.1.2. Distribution box

Figure 6.2. Mounting the device to DIN rail

smartDEN Opener in distribution box could be mounted to wall with at least two dowels.

6.2. Connecting motor

smartDEN Opener is able to control one reversible motor - start/stop and reverse its polarity.

6.2.1. Reversible AC asynchronous (induction) motor (single phase)

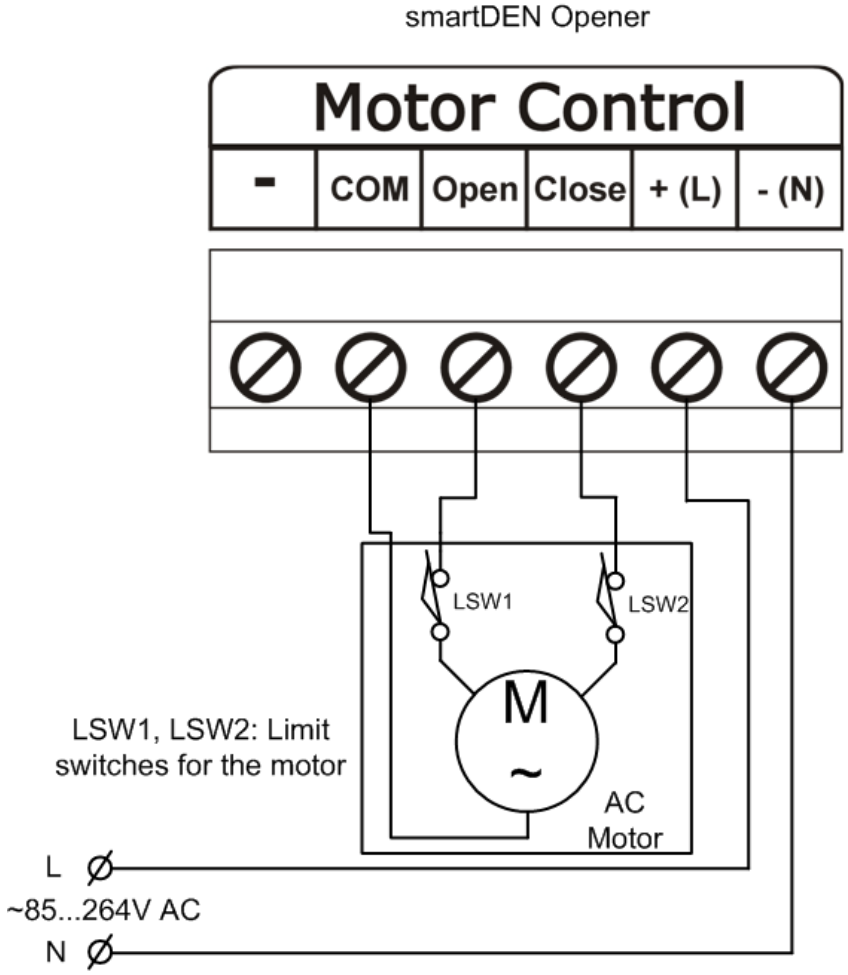

Figure 6.3. Hardware connection of AC motor

The AC Motor is controlled in the following way:

- For open (up) direction, the AC voltage is supplied between **COM** and **Open** terminals;
- For close (down) direction, the AC voltage is supplied between **COM** and **Close** terminals;
- For stop position, no voltage is supplied to the motor;

Please note that:

- LSW1 and LSW2 are limit switched recommend to be installed for the end positions (up/down) of the main controlled device (door, barrier...) in order to protect it;
- The maximum current of the motor should not exceed 4A. For example if the motor working voltage is 220VAC, the maximum controlled power should be no more than 880W. If the motor voltage is 120VAC, the maximum controlled power should be no more than 480W;
- The **Motor Control** channel is secured with fuse (usually 6.3A but can be changed).

6.2.2. Reversible DC motor

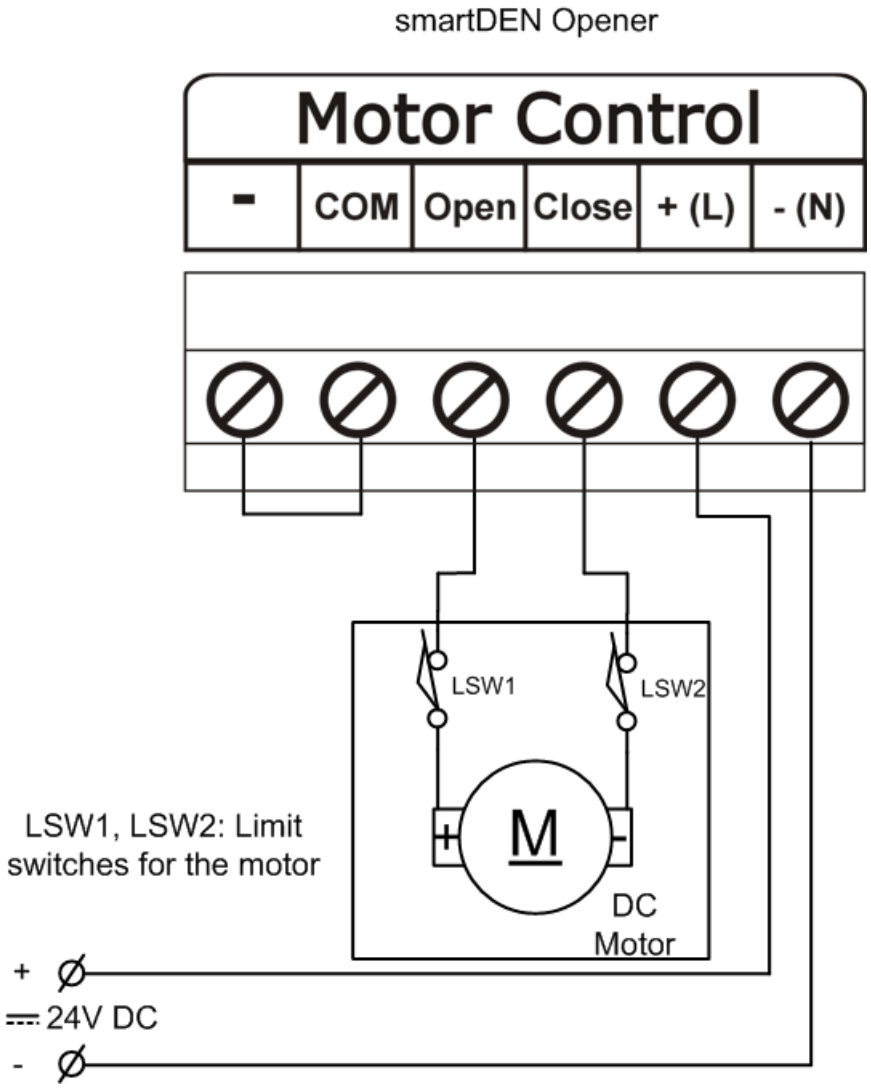

Figure 6.4. Hardware connection of DC motor

The DC Motor is controlled in the following way:

- For open (up) direction, the **Open** terminal is connected with **+VDC (+)** and **Close** is connected to **-VDC (-)**;
- For close (down) direction, the **Open** terminal is connected with **-VDC (-)** and **Close** is connected to **+VDC (+)**;
- For stop position, no voltage is supplied to the motor;

Please note that:

- LSW1 and LSW2 are limit switched recommend to be installed for the end positions (up/down) of the main controlled device (door, barrier...) in order to protect it.
- The maximum current of the motor should not exceed 4A. For example if the motor working voltage is 12VDC, the maximum controlled power should be no more than 48W. If the motor voltage is 24VDC, the maximum controlled power should be no more than 96W.
- The **Motor Control** channel is secured with fuse (usually 6.3A but can be changed);

6.3. Connecting relays

AC or DC loads can be controlled simply by using the **smartDEN Opener** two relays contact outputs to switch the external supply to the external load. **Figure 6.5** and **Figure 6.6** show basic output connections.

6.3.1. Controlling AC load

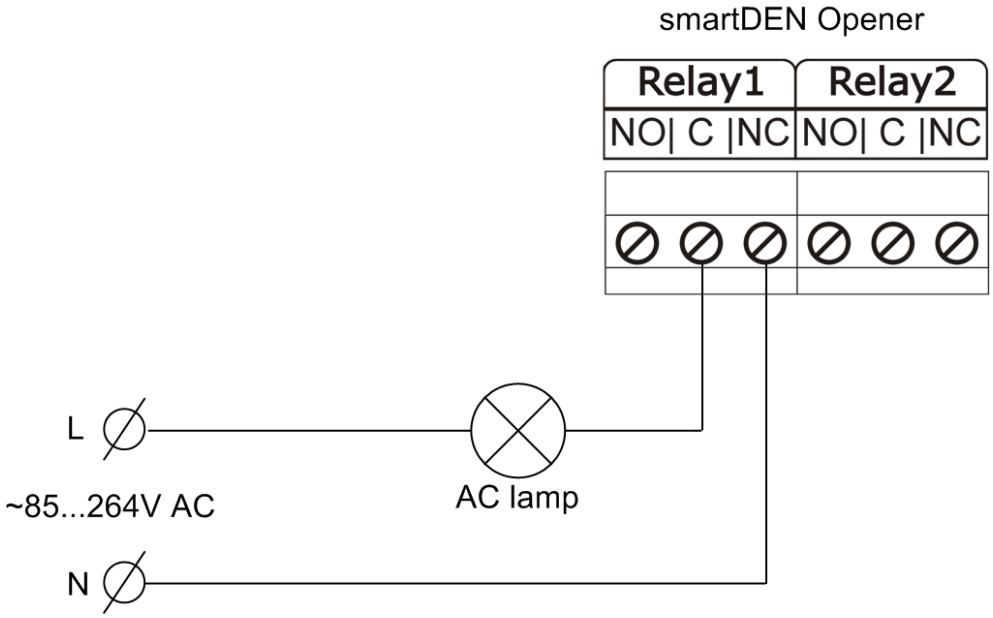

Figure 6.5. Controlling AC load with relay

6.3.2. Controlling DC load

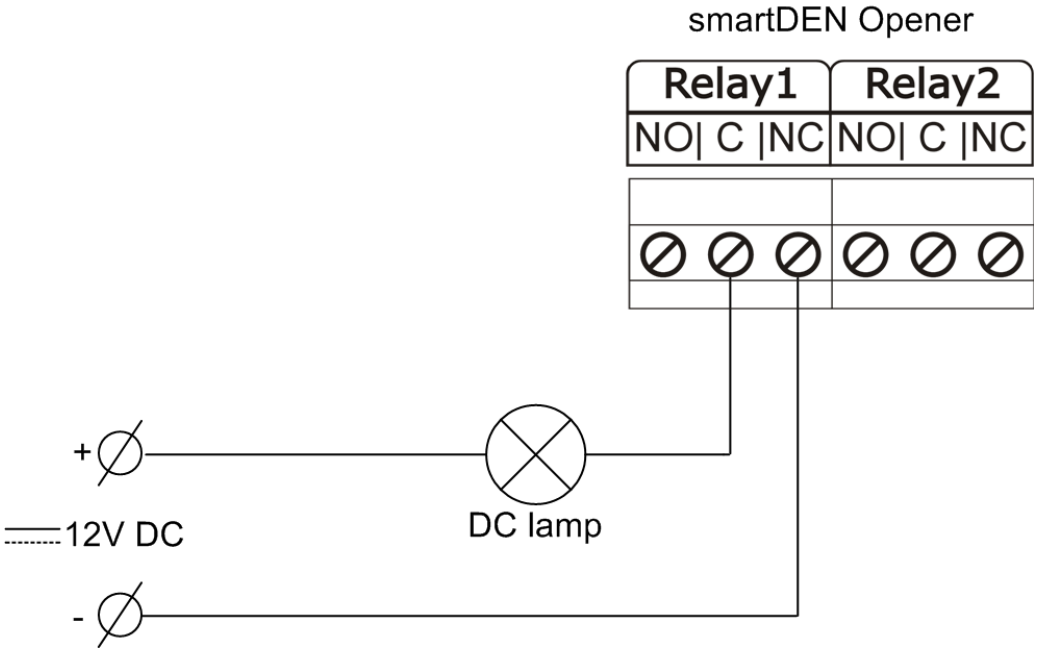

Figure 6.6. Controlling DC load with relay

6.4. Connecting digital inputs

6.4.1. Using the built-in power supply output

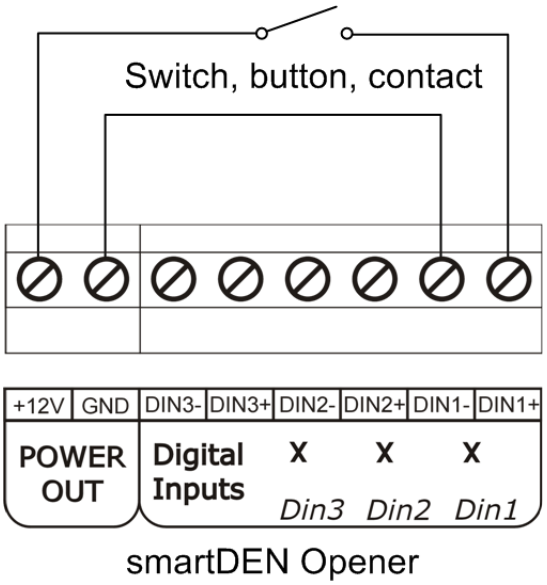

Figure 6.7. Connecting digital inputs using **smartDEN Opener** power out

Dry contact inputs such as PLC contacts or pushbuttons can be connected to the digital inputs using the 12VDC (24VDC) power output of the **smartDEN Opener**. In this case, GND and DIN- are shorted and contacts are connected between VDD and the appropriate digital input (DIN+).

6.4.2. Using external power supply output

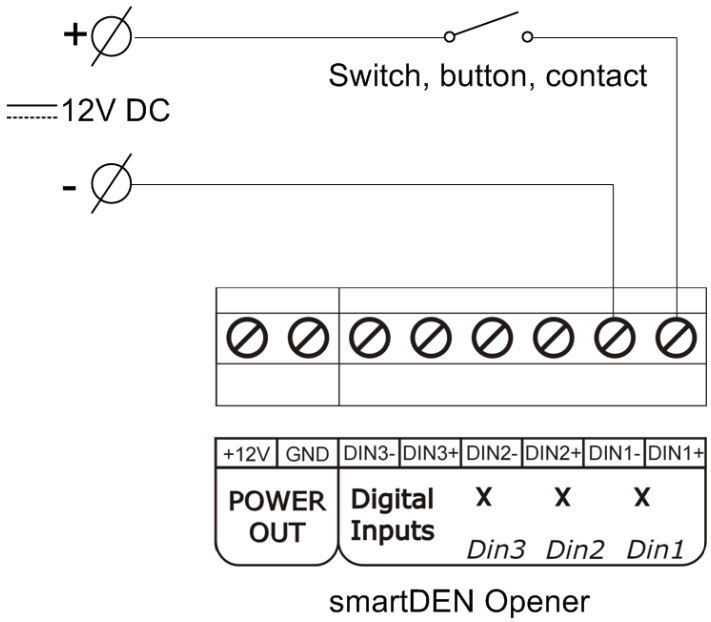

Figure 6.8. Connecting digital inputs using external power out

In this way it is shown how to make connection of the same contact inputs using an external power supply. Note that in this case, no connection is made to the VDD or GND.

6.4.3. Connecting SPST output sensors

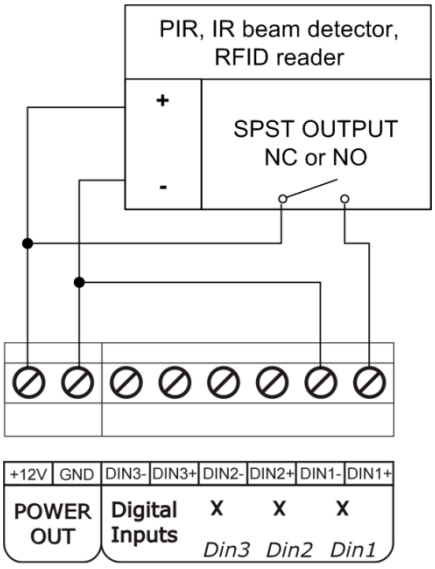

Figure 6.9. Connecting SPST output sensor

6.5. Connecting analog input

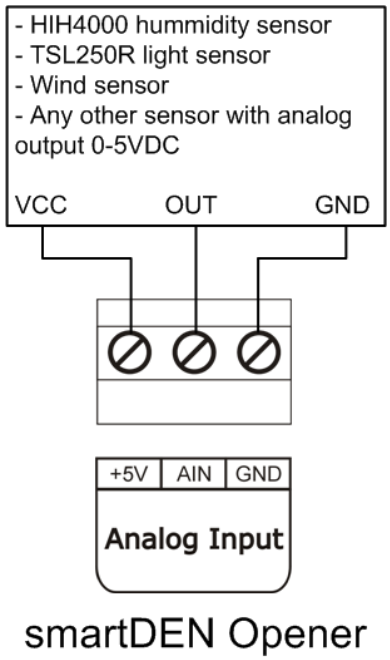

Figure 6.10. Connecting analog output

Any sensor with analog output (preferable linear) should be compatible with the analog input (with range 0-5V). For convince it is provided and additional power out 5VDC for such sensors as usually they are supplied with +5V. If not the other power supply out 12VDC (24VDC) can be used instead. For example compatible sensors models are:

- TSL250R light sensor;
- HIH-4000 humidity sensor;
- Wind speed sensors with 0-5V out;

6.6. Connecting one wire temperature sensor

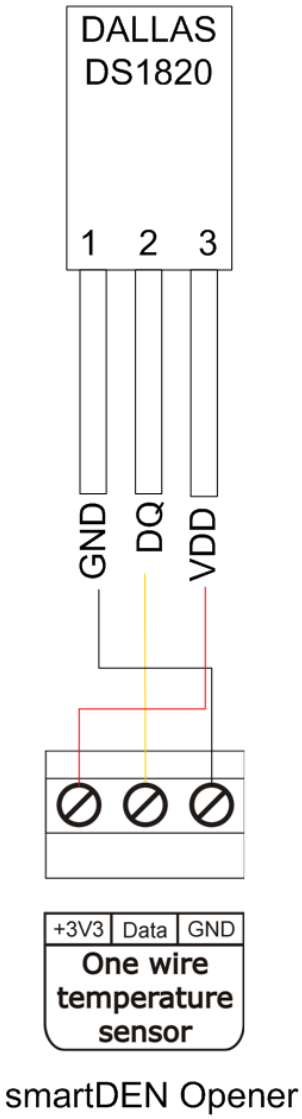

Figure 6.11. Connecting one wire temperature sensor

The temperature input is designed especially for the one wire temperature sensors of company DALLAS. The "Data" line is pulled up with internal resistor (usually with value of 2.0K). The sensors are supplied with +3.3V output power supply from the **smartDEN Opener**. Maximum cable length is about 20 meters. Supported models are:

- DS1820;
- DS18S20;
- SD18B20;

6.7. Power supply

6.7.1. Power supply with DC12V

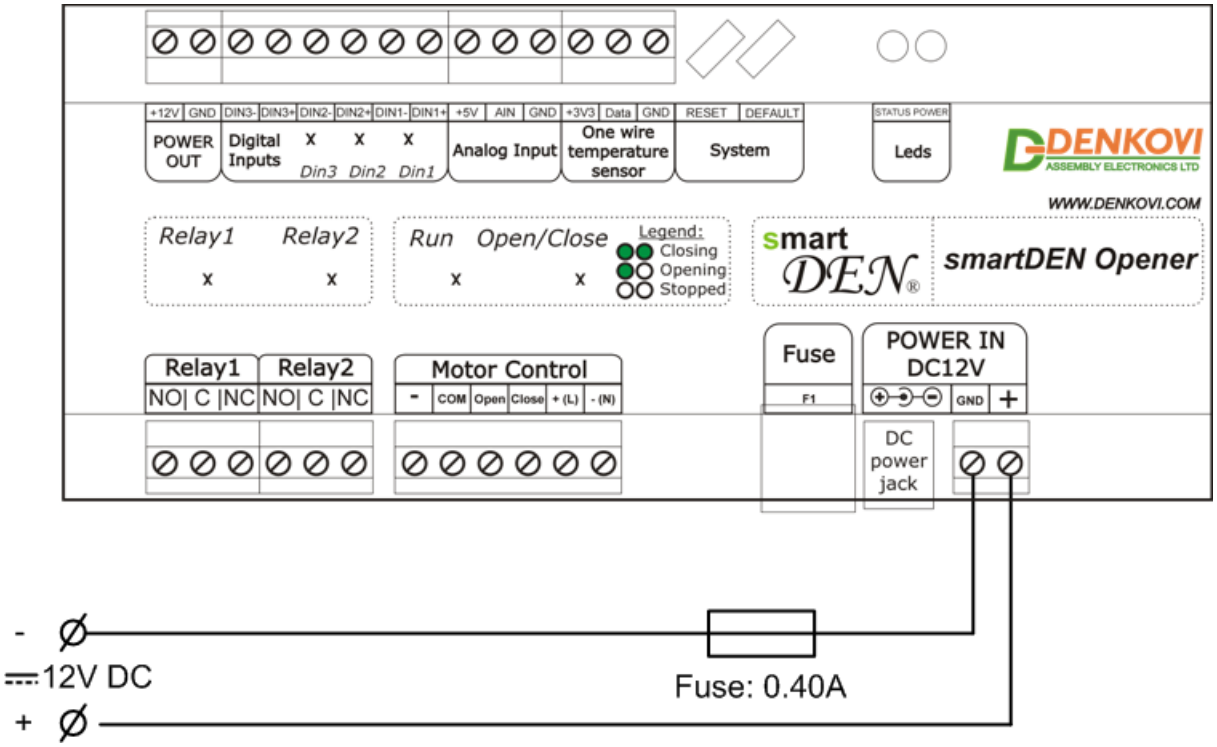

Figure 6.12. 12VDC Power Supply

6.7.1. Power supply with DC24V

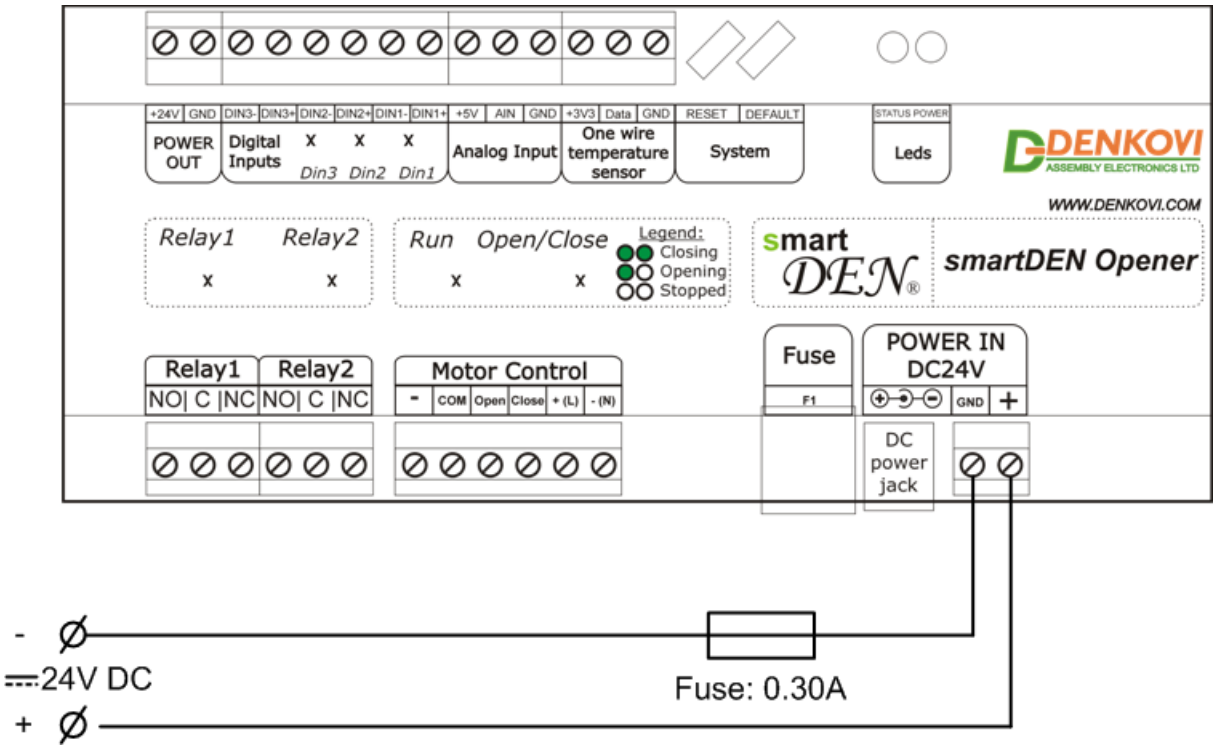

Figure 6.13. 24VDC Power Supply

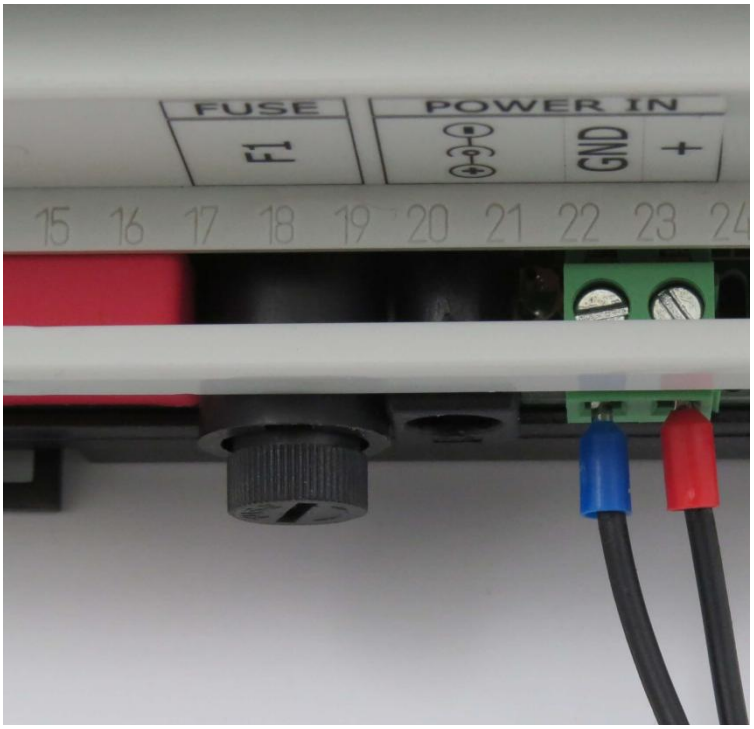

Figure 6.14. smartDEN Opener power supply using terminal wires

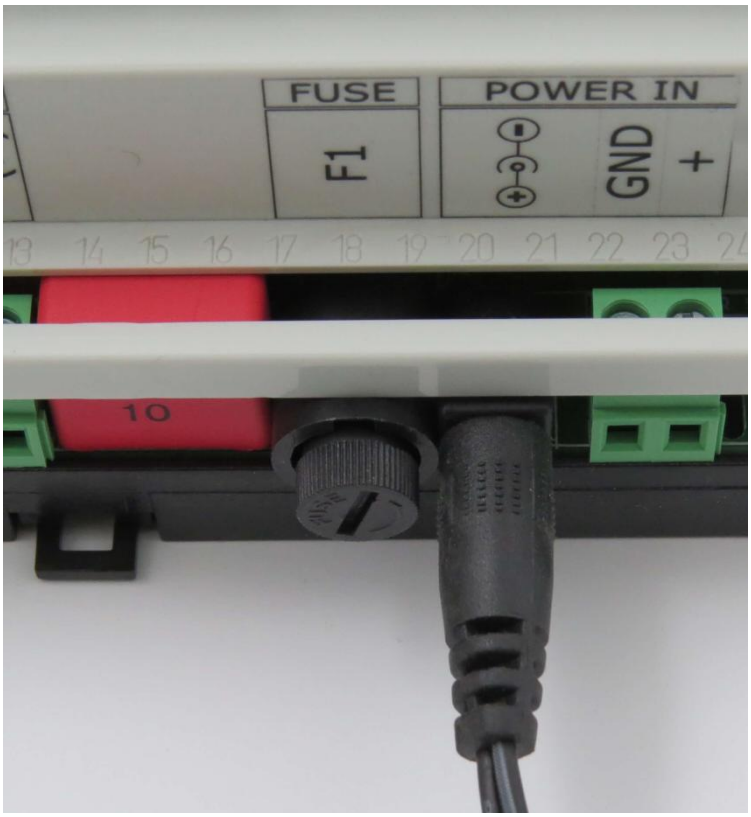

Figure 6.15. smartDEN Opener power supply using 2.5mm DC Jack

smartDEN Opener must be with voltage either **12VDC** or **24VDC** stabilized and filtered. The polarity of the jack must be center positive. After power on, the power led must be on and

STATUS indicator must start blinking in 5 seconds if in Access Point network mode or will flush if in Station network mode.

Figure 6.16. DC jack overview

⚠ Use either only DC jack either only terminal wires at the same time for power supply. Never use both wire and DC jack power supplies together. This may damage **smartDEN Opener**!

⚠ **smartDEN Opener** does not accept AC supply voltage. It is highly recommended to check the power supply source parameters before supply the module.

⚠ The power supply equipment shall be resistant to short circuit and overload in secondary circuit.

⚠ When in use, do not place the equipment so that it is difficult to disconnect the device from the power supply.

⚠ Installation of the board should be made by professional installers. Do not touch/connect/disconnect peripherals while power is turned on. Always disconnect from mains before make any changes.

6.8. RF remote settings

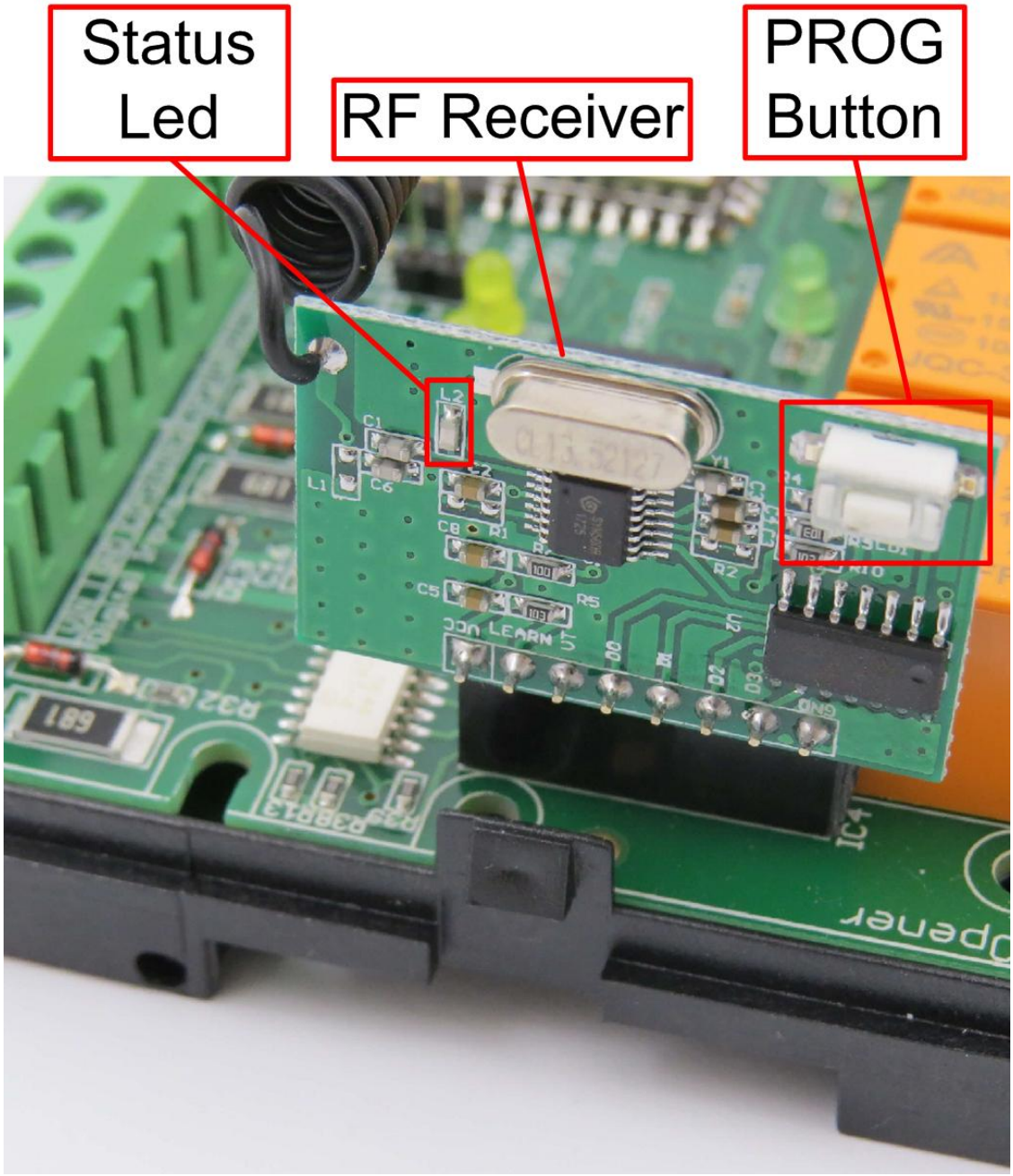

Figure 6.17. smartDEN Opener's RF receiver module

smartDEN Opener is equipped with RF receiver and is shipped with 2 pieces 433MHz RF remotes. However user may prefer to delete or add another remotes.

6.8.1. Delete all the saved RF remotes

1. Open the **smartDEN Opener** box and find IC4 RF receiver module. There are PROG button and status led mounted on it;
2. Press the PROG button while the RF module status led is turned off (usually about 10 sec)
3. Release the PROG button;
4. All the remotes are deleted from the memory.

6.8.2. Adding (saving) new RF remote

1. Open the **smartDEN Opener** box and find IC4 RF receiver module. There are PROG button and status led mounted on it;
2. Press the PROG button for a second, the RF module status led blink at this moment;
3. Release the PROG button;
4. Press some button from the RF remote within 20 seconds after PROG is being released. The RF module status led flashes several times, which means the adding new remote is done;
5. You can store in this way up to 20 remotes.

6.9. Network connection

smartDEN Opener is a Wi-Fi device which makes it mobile and easy to connect. The built in web server makes the configuration easy to set up. **smartDEN Opener** can act in two network modes - Access Point and Station.

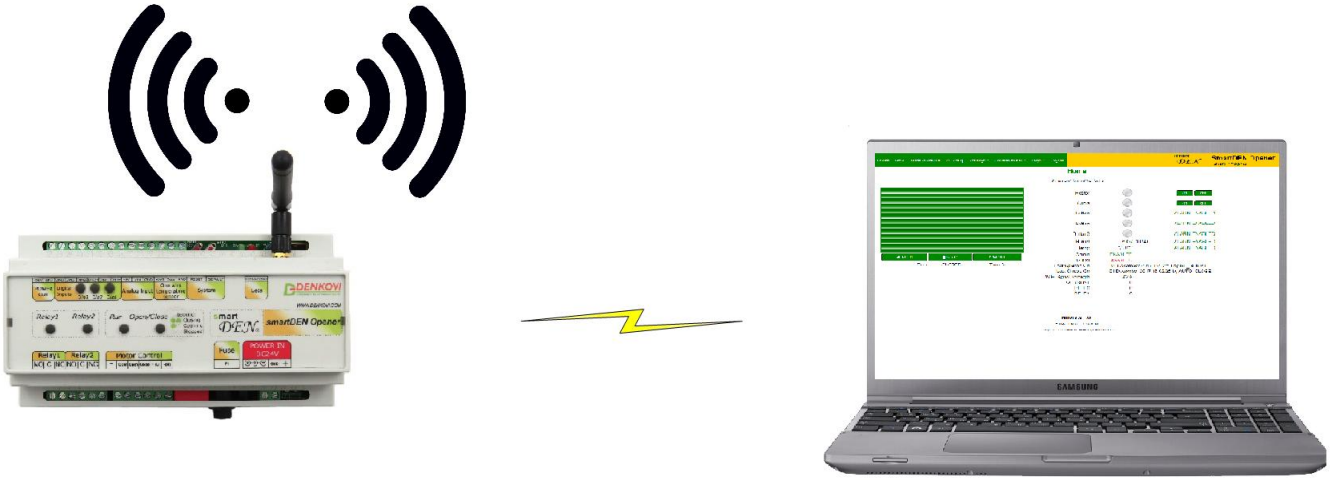

Figure 6.18. Connecting to **smartDEN Opener's** Wi-Fi network. This is the initial connection

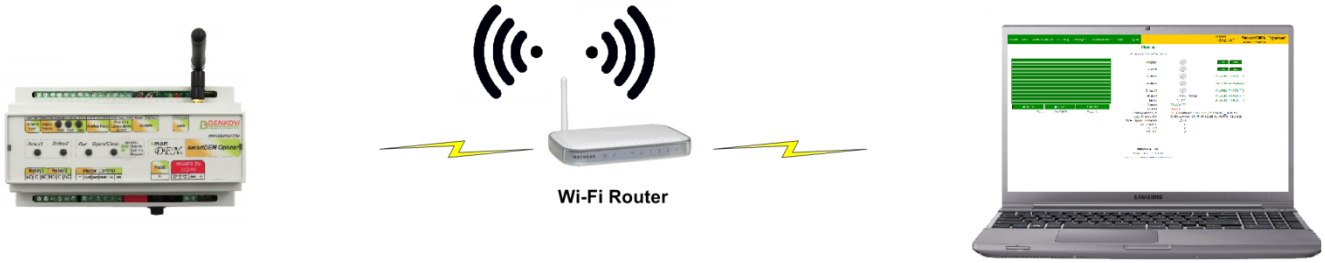

Figure 6.19. Connecting **smartDEN Opener** to a wireless router

6.10. Communication setup

smartDEN Opener is shipped with the following default parameters:

- Network SSID: **SmartDEN_Opener_XXXXXX**
- Network Password: **No Password (Open Network)**
- IP address: **192.168.4.1**
- Subnet mask: **255.255.255.0**
- Gateway: **192.168.4.1**
- Web username: **admin**
- Web password: **admin**

Initially it is recommended to connect a computer to the module's Wi-Fi network. The Wi-Fi network should look like this:

Figure 6.20. **smartDEN Opener** Wi-Fi network

Next you have to change your PC's IP address.

You can "google" how to change computer IP settings.

For Windows 7 OS for example you can do that in the following way:
Navigate to *Control Panel -> Network and Internet -> View network and status tasks -> Change adapter settings*

Then just select the Wireless Network Connection with right click and select *Properties*:

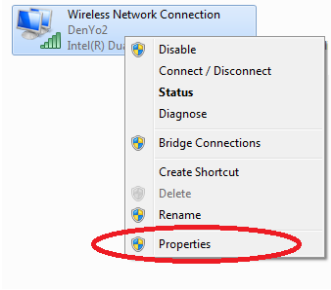

Figure 6.21. Wireless card properties

The next step is to enter into IPv4 properties.

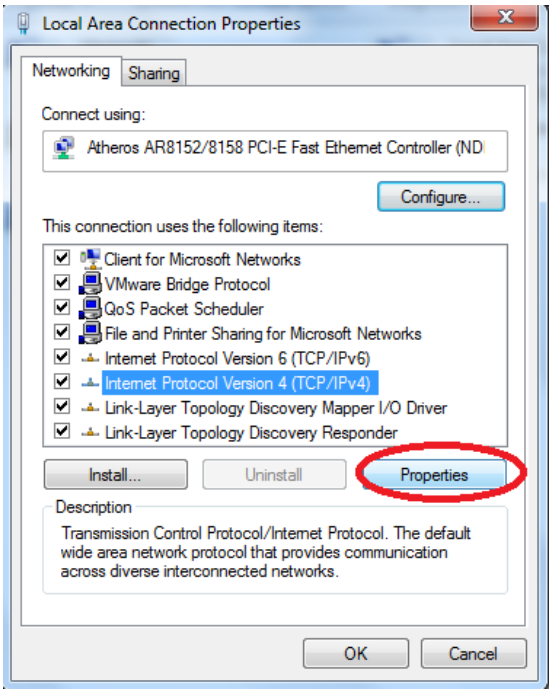

Figure 6.22. Enter in IPv4 properties section

Set the IP address of your PC to be in the same network.

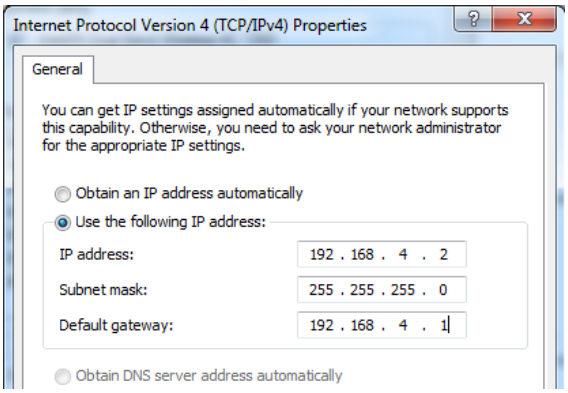

Figure 6.23. Set the IP address

Finally, in order to access **smartDEN Opener** just type in your web browser address bar 192.168.4.1

Figure 6.24. Open the device via browser

If the network settings are O'K, the log-in page should appear:

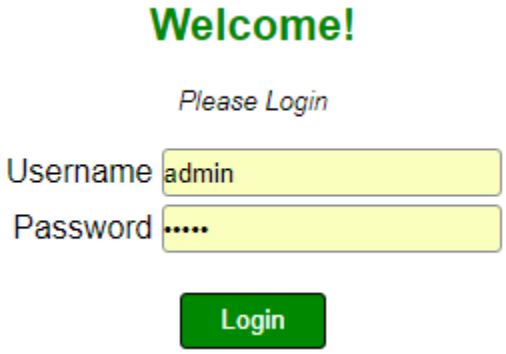

Figure 6.25. Login page

- **smartDEN Opener** modules connected locally can be easily scanned and found via the tool ***Denkovi Finder*** as well.

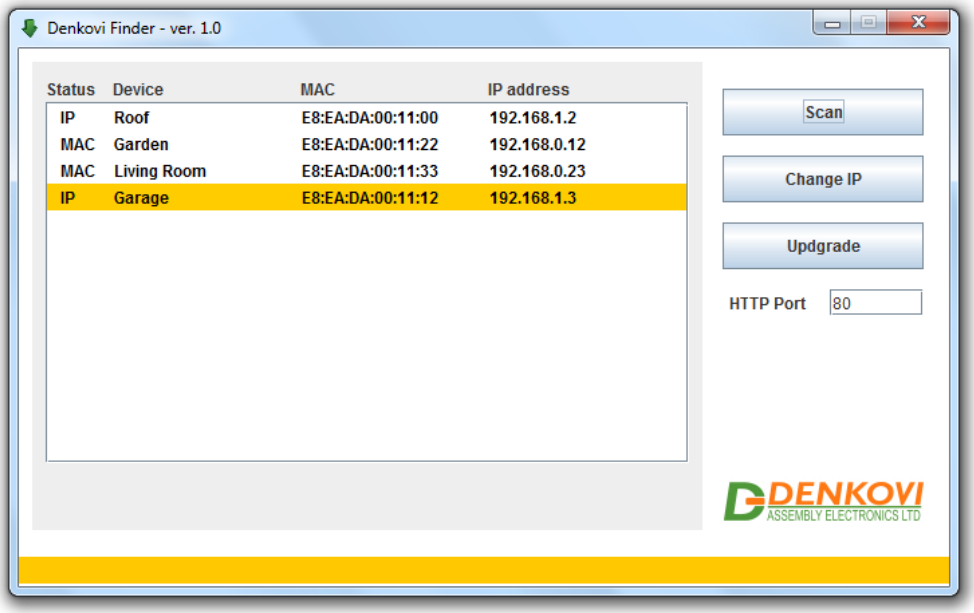

Figure 6.26. Denkovi Finder utility

6.11. DAE-aModules android application

It is possible to use *DAE-aModules* android application with **smartDEN Opener**. There are two types in *DAE-aModules* for **smartDEN Opener** device (board):

- **smartDEN Opener - XML** - this is direct communication with HTTP XML requests.
- **smartDEN Opener - Cloud** - this is cloud communication using MQTT protocol.

6.11.1. smartDEN Opener - XML

This type of added device could be used in both Access Point and Station operating mode. The example below is given in Access Point mode.

⚠ Be sure that **Admin Enable** option is checked from **smartDEN Opener's** web server - General Settings page (see **10. Web Access**).

1. Find **smartDEN Opener** Access Point network and connect to it. It should look like this on the figure below by default.

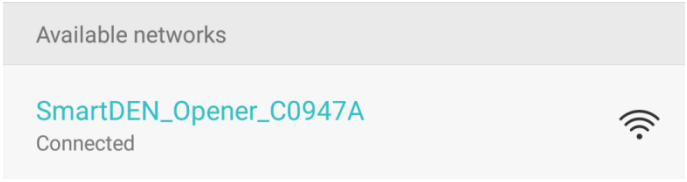

Figure 6.27. smartDEN Opener's Access Point network

2. Open *DAE-aModules* application and click "**Add New Device**" button.
3. Add **smartDEN Opener - XML** device. In this example default settings are used.

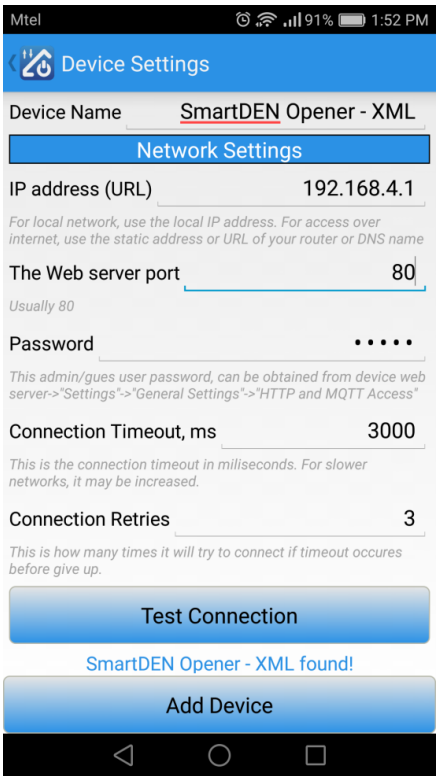

Figure 6.28. smartDEN Opener - XML Settings

- **Device Name** - the name of the device, by default it is "**smartDEN Opener - XML**";

- **IP Address (URL)** - **smartDEN Opener** Access Point's IP address, by default it is 192.168.4.1;
- **The Web server port** - **smartDEN Opener** web server port, by default it is 80;
- **Password** - **smartDEN Opener** admin user's default password, by default it is "admin";
- **Connection Timeout** - the default by *DAE-aModules* is 3000ms;
- **Connection Retries** - the default by *DAE-aModules* - 3;

4. Click "Test Connection" button - if successful connection is obtained "smartDEN Opener - XML found!" message will be visualized. If connection is unsuccessful "smartDEN Opener - XML not found!" message will be visualized.
5. If everything is OK then click **"Add Device**" button on bottom.
6. Now it will be added to list with devices. Click on **smartDEN Opener - XML** device.

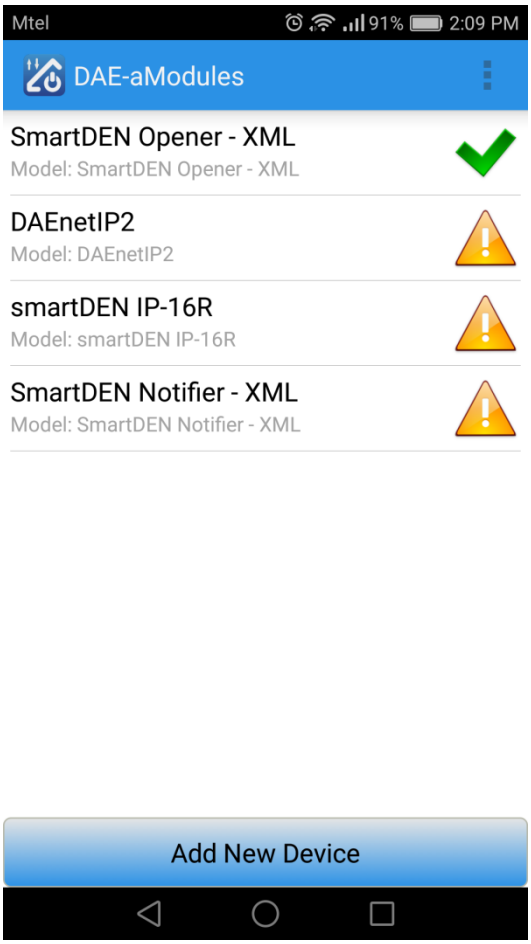

Figure 6.29. *DAE-aModules* list with devices

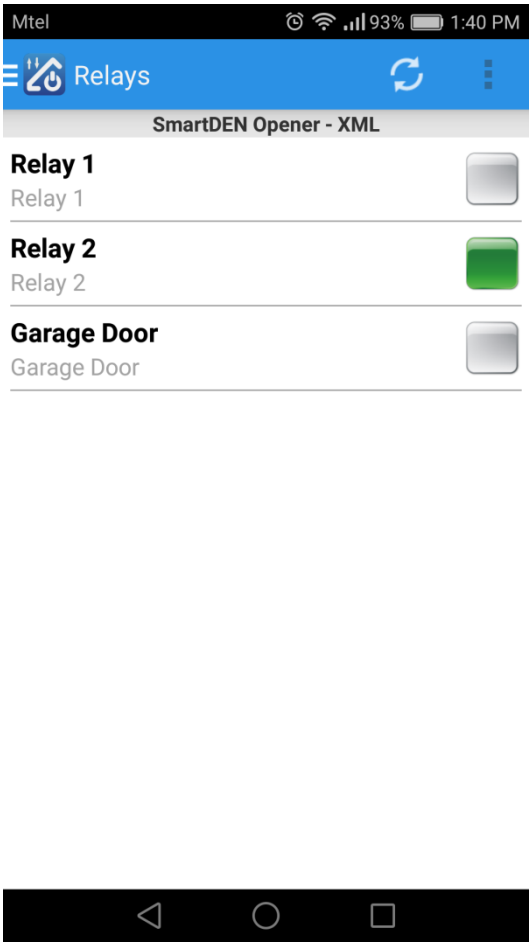

Figure 6.30. Relays tab

7. Control tab will be shown with states of the two relays and Main Controlled Device. In our example on **Figure 6.30** Relay 1 is OFF, Relay 2 is ON and Main Controlled Device ("Garage Door" in our example) is **CLOSED** (or **STOPPED**). By clicking on status buttons the state of the relay will be toggled.
8. When click in upper left corner button another available tabs will be visualized (**Figure 6.29**).
   - **Device List** - will go to home page and show all devices;
   - **Relays** - will go to Relays tab where could be obtained state of relays and Main Controlled Device as well as control them;
   - **Digital Inputs** - will show state of Digital Inputs;
   - **Analog Input** - will show the Analog Input measurement;
   - **Temperature Input** - will show the temperature sensor attached to **smartDEN Opener**;
   - **Settings** - will show screen to edit board settings;

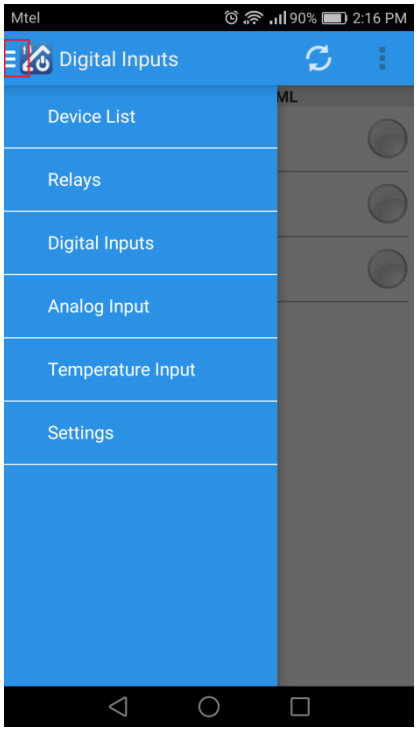

Figure 6.31. *DAE-aModules* additional tabs

When **smartDEN Opener - XML** board is used over Internet, port forwarding might be needed. For more information see this Application Note: http://denkovi.com/access-devices-from-the-internet

6.11.2. smartDEN Opener - Cloud

This communication usually is used in Station operating mode (STA). With such added device notifications could be received (see **16.2. Notifications**). This communication uses Internet and it dependents on third party MQTT brokers (by default).

Be sure that **Admin Enable** option is checked from **smartDEN Opener's** web server and MQTT Client is with state "Connected" (see **10. Web Access)!**

1. Open *DAE-aModules* application and click "**Add New Device**" button.
2. Add **smartDEN Opener** - Cloud board. In this example default settings are used (**Figure 6.32**).
   - **MQTT Server** - in this example is used the default "iot.eclipse.org". There are also other public MQTT Brokers which could be used;
   - **MQTT Server Port** - the default is 1883;
   - **MAC Address** - in this field should be typed **smartDEN Opener**'s Station mode MAC Address (could be found in MQTT page on the web server);
   - **User Name** - there are only two possible choices for this option - "admin" and "guest". In our example Admin user is used so "admin" username will be used. Note that Guest account is **DISABLED** by DEFAULT and could not receive notifications;
   - **Password** - this is user account's password. By default for Admin user it is "admin";
   - **Connection Timeout** - in our example default value is used - 3000ms;
   - **Connection Retries** - again default value is used - 3;

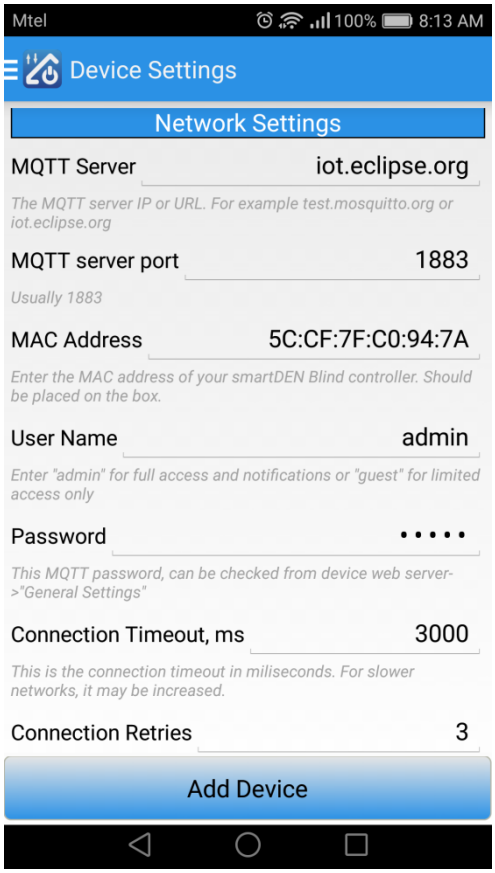

Figure 6.32. smartDEN Opener - Cloud Settings

3. Click "**Test Connection**" button - if successful connection is obtained "smartDEN Opener - Cloud found!" message will be visualized. If connection is unsuccessful "smartDEN Opener - Cloud not found!" message will be visualized.
4. If everything is OK then click "**Add Device**" button on bottom.
5. Each other steps are just same as **smartDEN Opener - XML** (point 6 and 7).

> More information about *DAE-aModules* application could be found on http://denkovi.com/*DAE-aModules*.

6.12. Connecting smartDEN Opener to Wi-Fi network

smartDEN Opener provides more functionality when has Internet access. This could be done by connecting the module to a router. By default **smartDEN Opener** is shipped with default settings which starts the board in Access Point mode (AP). The user must connect to **smartDEN Opener's** Access Point network (described in **6.9. Communication Setup**) and set up the network settings in order to connect the module to a router.

1. When connected to Access Point network of **smartDEN Opener** go to "**Network Settings**" page and change network mode to "**STA**".
2. There is provided "**Scan**" button which will scan the available networks.
3. Next dropdown list will be available with found networks. Now the user could select the desired network from this list or just type network's SSID.
4. Password for the network must be typed if network is protected. If open network is used, leave this field empty.

5. If the router to which is connected provides DHCP server, leave the "**Obtain an IP address automatically**" option enabled else disable this option and type the appropriate addresses.
6. Click "**Save**" button.
7. Changes take effect after restart, so click "**Reboot**" button.

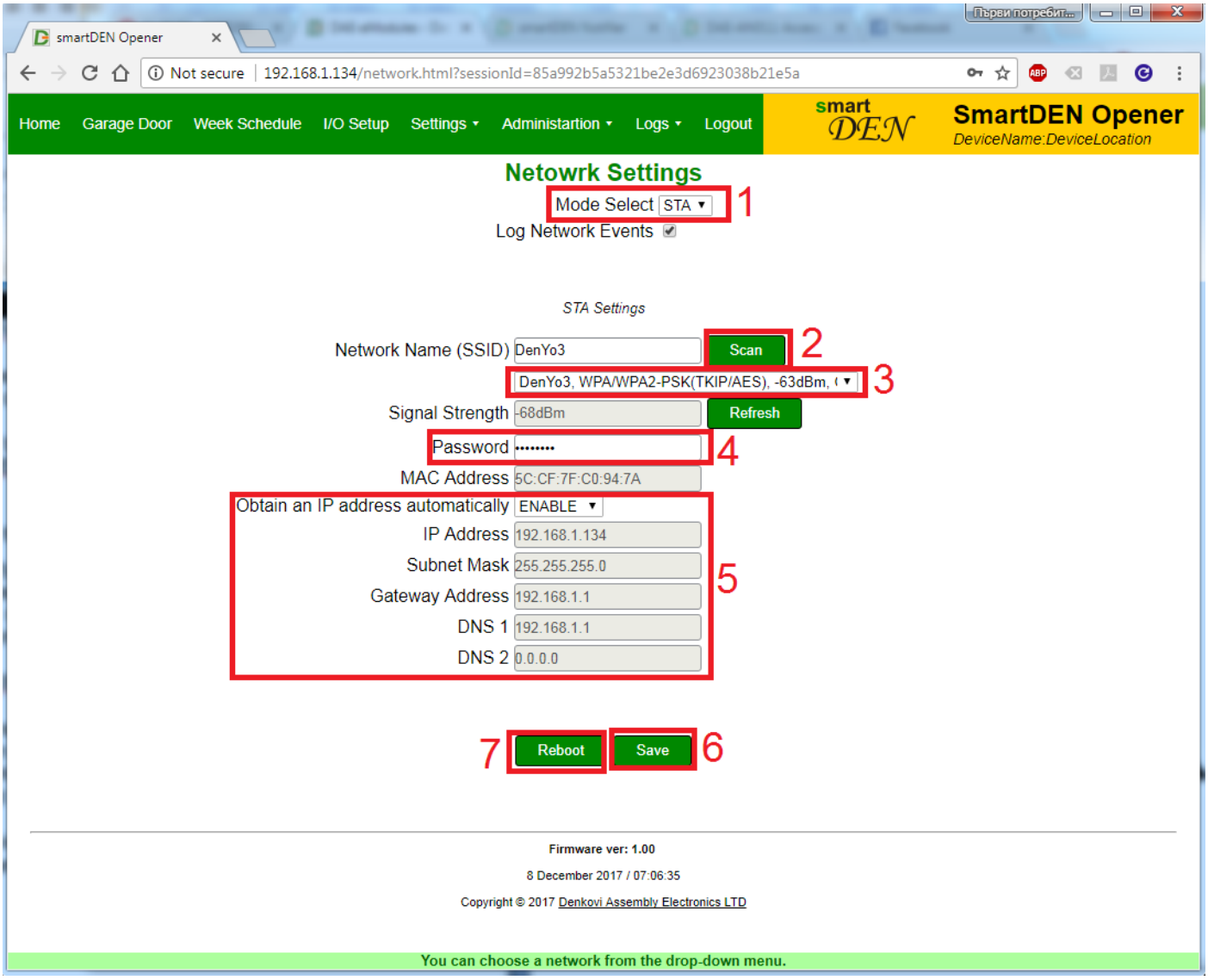

Figure 6.33. Connecting **smartDEN Opener** to Wi-Fi network

After restart **smartDEN Opener** should connect to the router and the user could access it via the local network. If could not connect to the router (because of wrong password for example), **smartDEN Opener** will change to Access Point mode.

6.13. Setting the open/close time

smartDEN Opener provides controlling a Motor Controlled Device. For example this could be a garage door. The provided **Open/Close time** parameter could be set in two ways:

6.13.1. From web server

1. Log into the web server;
2. Go to page "Garage Door" (Main Controlled Device) - the second page after "**Home**" page from menu (see **10.4 Main Controlled Device's page**);
3. Click button "**CLOSE**" and wait until the Main Controlled Device is **CLOSED**;
4. Click "**STOP**" button;
5. Click button "**OPEN**" and wait until the Main Controlled Device is **OPENED**;
6. Click "**STOP**" button;
7. Click "**Save**" button, the settings are saved.

Note that Open/Close time has ±1 second tolerance.

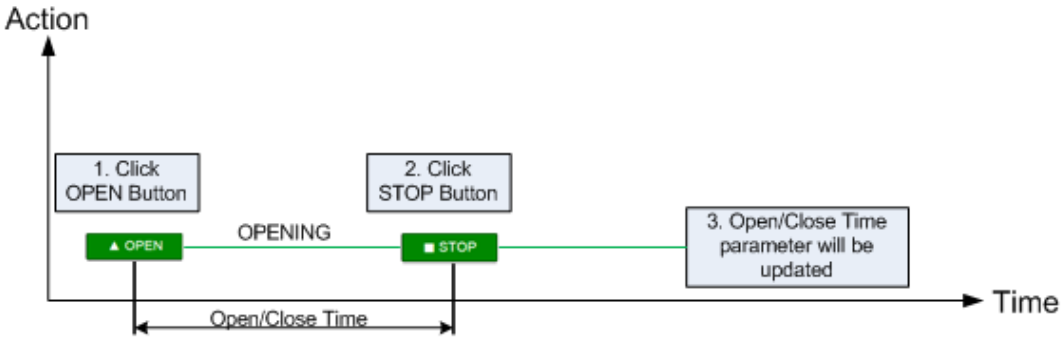

Figure 6.34. Setting **Open/Close time** via web server

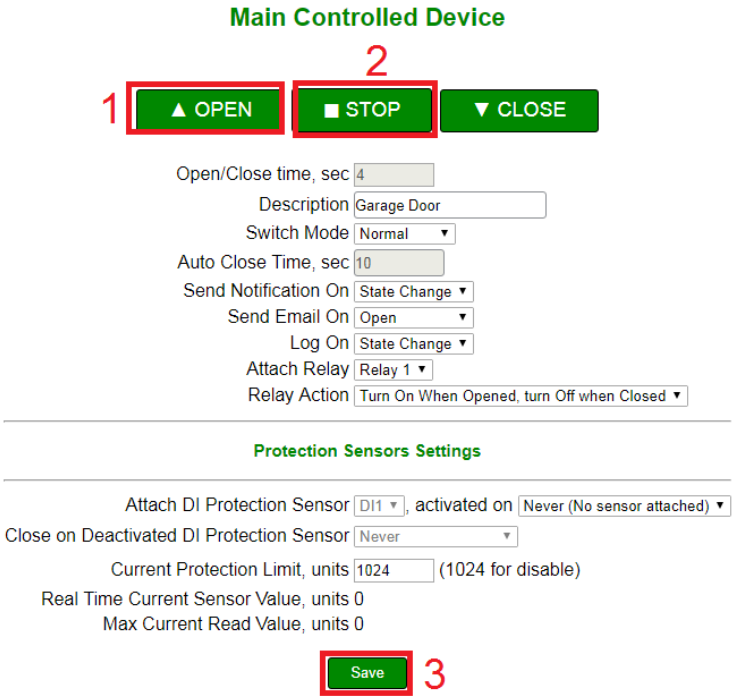

Figure 6.35. Setting the **Open/Close time** via web server

6.13.2. Via RF remote

1. Press the two buttons from the RF remote at the same time. The **smartDEN Opener** status led will start flashing (for about 5 sec);
2. Wait until the status led stop flashing;
3. Release the buttons;
4. Pres RF remote "Open" button so the Main Controlled Device goes to **OPENED** position;
5. Release the RF remote "Open" button;
6. Press the RF remote "Close" button;
7. Wait until the Main Controlled Device goes to **CLOSED** position. The status led will blink with period 0.5 sec during this time;
8. Release the RF remote "Close" button. Now the **Open/Close time** is stored in memory;
9. Press the both RF buttons together. The **smartDEN Opener** status led will become flashing for about 7 sec;
10. Wait until the status led stop flashing;
11. Release the buttons;
12. The **smartDEN Opener** is rebooted with the new opening/closing time.

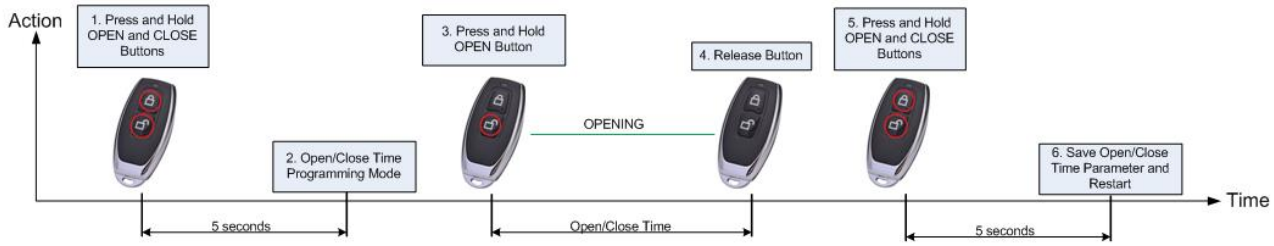

Figure 6.36. Open/Close Time programming via RF Remote Controller

6.14. Setting the protections

6.14.1. Setting the primary current protection

smartDEN Opener provides current protection for Main Controlled Device's motor. It measures the current through Main Controlled Device's motor and if the measured current (consumed by the motor) is more than certain level, the Main Controlled Device stop closing and start opening almost immediately automatically. Such kind of protection is very useful in cases where the Main Controlled Device (garage door, barrier) may hits an object (car for example) and in that moment the motor current consumption is increased. The protection parameters can be set from the web server, in page for the Main Controlled Device:

- **Current Protection Limit, units** - this is the level of measured current which triggers opening the Main Controlled Device. If the current units become higher than this value, the Main Controlled Device will start **OPENING**. It is in ADC raw units. If this parameter is 1024, the current protection is disabled;
- **Real Time Current Sensor Value**, **units** - when closing the Main Controlled Device this parameter show the current motor consumption for reference. It is in ADC raw units;
- **Max Current Sensor Value**, **units** - the maximum measured current while closing the Main Controlled Device. It is in ADC raw units;

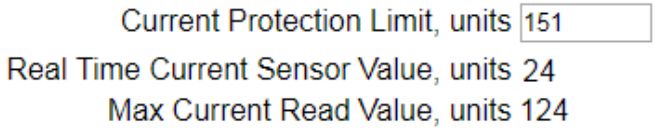

Figure 6.37. Current protection options (Main Controlled Device page)

Steps for setting the current protection:

1. Login to the web server and go to page for the Main Controlled Device.
2. Click the "**Close**" button so the door (barrier, window, tent) will start **CLOSING**;
3. The "**Real Time Current Sensor Value**" will start updating;
4. After the door (barrier, window, tent) is closed the "**Max Current Read Value**" will be updated with the maximum measured value.
5. Set the "**Current Protection Limit**" with higher value than the "**Max Current Read Value**".

⚠ The "**Current Protection Limit**" must be higher than "**Max Current Read Value**" so that there will not be fake detections but it must be also as low as possible so that over-currents will be detected easily

⚠ Use "**Current Protection Limit"** feature only if possible and with HIGH ATTENTION as per the Main Controlled Device manufacturer. It may damage your stuff if not proper tuned.

⚠ **smartDEN Opener** can control motor with maximum consumption 4A or that is about 300 ADC raw units which means when the "**CLOSE**" button is clicked, the "**Real Time Current Sensor Value"** and "**Max Current Sensor Value**" must be less than 300.

⚠ This type of protection is not suitable for all types of applications. Please use it with care! Set up the parameters only as per the Main Controlled Device manufacturer.

6.14.2. Setting the secondary protection via digital input

smartDEN Opener provides additional protection using digital input. In this way it is suitable to use for example barrier detector with SPST output showing when there is human or car under the barrier (door). One digital input could be attached as a DI protection sensor.

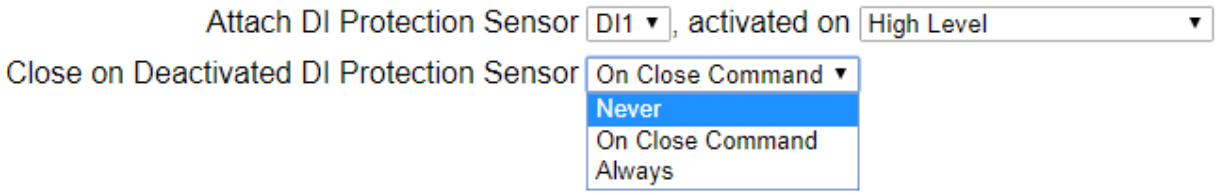

Figure 6.38. DI protection sensor options (Main Controlled Device page)

When this protection type is used the Main Controlled Device may be closed automatically (auto-close) if DI protection sensor is deactivated depending on the settings. When attaching DI protections, the activated level must be selected as well. For example if high level is selected for activation then low level will deactivate the DI protection sensor:

- *Never* - selected digital input does not make **CLOSE** automatically;
- *On Close Command* - CLOSE automatically on deactivated DI protection sensor if only there is a **CLOSE** command. If DI protection sensor is in activated level then **CLOSING** operation is delayed until deactivation level occurs (i.e. car is not under the barrier anymore for example);
- *Always* - **CLOSE** every time when DI protection sensor is deactivated;

7. Default settings

7.1. Table with default settings

The **smartDEN Opener** module is shipped with default (factory) settings shown in the table below. The default settings can be reloaded, if necessary following the steps in **chapter 7.2**.

Table 7.1. Default settings

Settings group	Parameter (according Web pages)	Value
General Settings	Device Name	smartDEN Opener
	Device Location	location
	Username	admin
	Password	admin
Network Settings	Mode	AP
	SSID	SmartDEN_Opener_XXXXXX
	Password	Disabled (Open Network)
	Channel	AUTO
	DHCP	Enabled
	IP Address	192.168.4.1
	Subnet Mask	255.255.255.0
	Output Power	20.5 dBm
HTTP & XML Access	HTTP Port	80
	Access IP Address	0.0.0.0
	Access Mask	0.0.0.0
	Session Timeout, min	5
	Enable Admin XML Access	Yes
	Enable Guest XML Access	No
MQTT Access	MQTT Broker	iot.eclipse.org
	MQTT Port	1883
	Enable Admin MQTT Access	Yes
	Enable Guest MQTT Access	No
Email	Sender Email Address	send@srvden.com
	Sender Email Password	xxxxxx
	SMTP Server	162.241.231.158
	SMTP Port	587
Users	Admin Password	admin
	Admin Enabled	Yes
	Guest Password	guest
	Guest Enabled	No
NTP	NTP Server	pool.ntp.org
	NTP Port	123

7.2. Steps for loading default settings

When necessary, the factory (default settings) may be applied so the module parameters will be returned back as those in **chapter 7.1** from the current document.

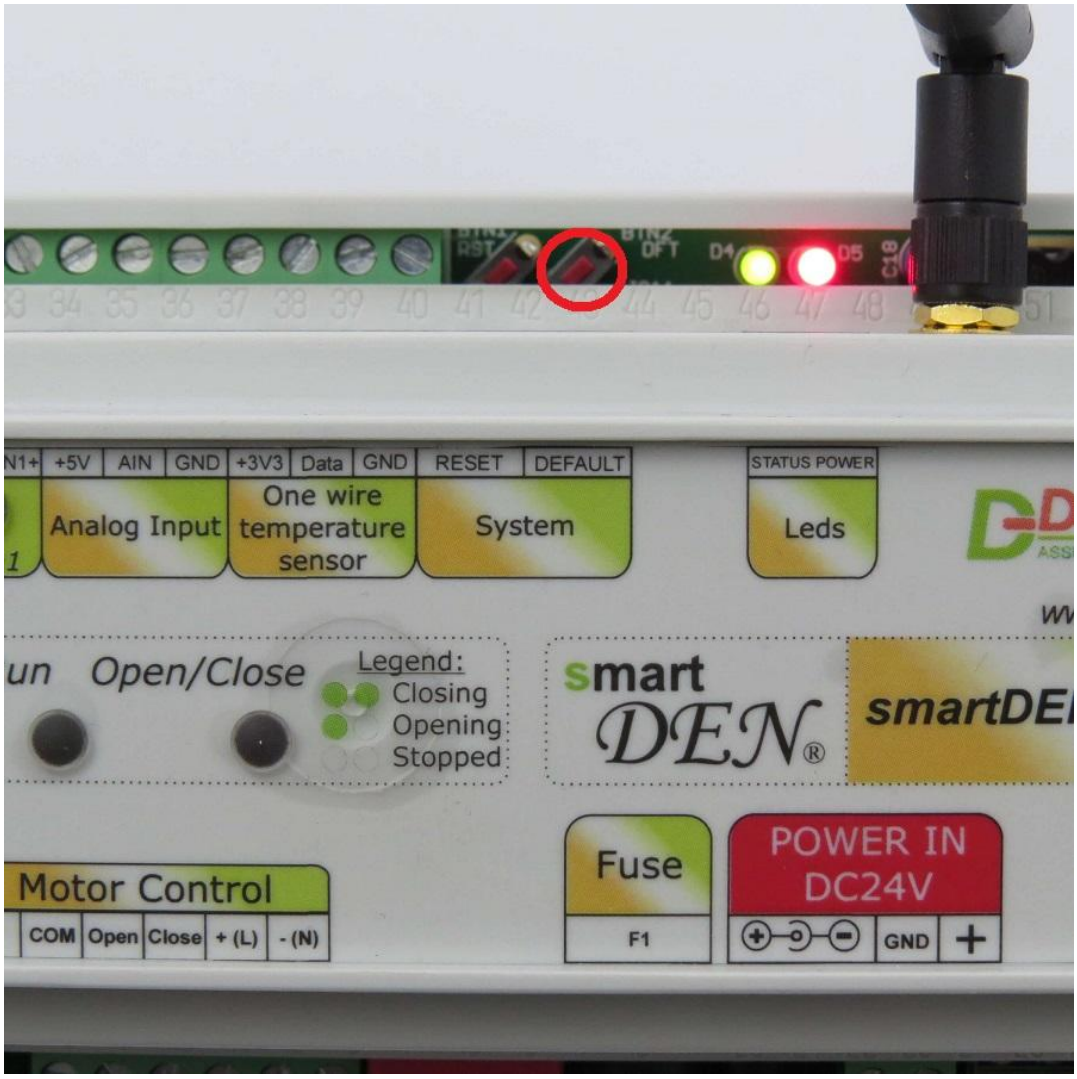

Figure 7.1. Loading the default settings button

1. Turn off the power supply of the device;
2. Press and hold the default button;
3. Turn on the power supply of the device;
4. Wait for until status led indicator become ON (approximately after 5 sec);
5. Release the default button;
6. The module will restart with configured default settings.

8. Wi-Fi Interface

8.1. Access Point Operating Mode (AP)

By default **smartDEN Opener** is shipped in Access Point network mode (AP). In this mode you can connect to **smartDEN Opener** and configure the device to operate in Station network mode. While in Access Point network mode status led will blink once a second.

smartDEN Opener can switch to Access Point network mode if were in Station mode and lost connection to router. This could be recognized by the blinking status led. When this occurs, **smartDEN Opener** will try to reconnect to router on every 2 minutes if the user is not logged in web server.

- Access Point (AP) network mode allows only one user to connect to **smartDEN Opener's** network. All further connections will be rejected.

8.2. Station operating mode (STA)

This is the typical and recommended operating network mode of **smartDEN Opener**. Using the module as a Station network device with Internet access will allow all of the features to operate (such as MQTT access, NTP time synchronization, OTA update, etc.). When using **smartDEN Opener** in Station network mode status led will be constantly switched on. That's how it could be recognized this operating mode. As described above if connection to router is lost **smartDEN Opener** will switch to Access Point network mode and try reconnection on every 2 minutes if user is not logged in web server. **smartDEN Opener** can connect to 2.4Ghz IEEE 802.11 b/g/n networks. The module has 3dBi antenna. The possible encryption of the router's network are:

- Open network (no encryption)
- WEP
- WPA Personal
- WPA2 Personal
- WPA/WPA2 Personal Mixed.

- To use full functionality of **smartDEN Opener** use the module in Station mode (STA) with Internet access. Access Point (AP) is only for configuration.

- For more information see **10.8 Network Page.**

9. Main Controlled Device

smartDEN Opener provides output to control load driven by AC/DC motor. This load is called Main Controlled Device -garage door, blind, awning, window, barrier etc. Main Controlled Device has five states:

9.1. OPENING

OPENING is the state which the Main Controlled Device was in **STOPPED** or **CLOSED** state and **OPEN** command is received (from RF Remote Controlled, web server, etc.). Then voltage is provided between COM and OPEN terminals on motor output terminal. **Open/Close Time** starts decrementing until time elapse. When time elapse motor driven load is stopped and no voltage is provided on motor output terminal. Main Controlled Device is now in **OPENED** state.

If during **OPENING** state **OPEN** command is received Main Controlled Device will continue **OPENING**.

If during **OPENING** state **CLOSE** command is received Main Controlled Device will go to **STOPPED** state.

If during **OPENING** state **STOP** command is received Main Controlled Device will go to **STOPPED** state.

9.2. CLOSING

CLOSING is the state which the Main Controlled Device was in **STOPPED** or **OPENED** state and **CLOSE** command is received (from RF remote, web server, etc.). Then voltage is provided between COM and CLOSE terminals on motor output terminal. **Open/Close Time** starts decrementing until time elapse. When time elapse motor driven load is stopped and no voltage is provided on motor output terminal. Main Controlled Device is now in **CLOSED** state.

If during **CLOSING** state **CLOSE** command is received Main Controlled Device will continue **CLOSING**.

If during **CLOSING** state **OPEN** command is received Main Controlled Device will go to **STOPPED** state.

If during **CLOSING** state **STOP** command is received Main Controlled Device will go to **STOPPED** state.

9.3. OPENED

OPENED is the state which the Main Controlled Device was reached one of its end position. Then no voltage is provided on motor output terminal.

If during **OPENED** state **CLOSE** command is received Main Controlled Device will start **CLOSING**.

If during **OPENED** state **OPEN** command is received Main Controlled Device will take no action.

If during **OPENED** state **STOP** command is received Main Controlled Device will go to **STOPPED** state.

9.4. CLOSED

CLOSED is the state which the Main Controlled Device was reached one of its end position. Then no voltage is provided on motor output terminal.

If during **CLOSED** state **OPEN** command is received Main Controlled Device will start **OPENING**.

If during **CLOSED** state **CLOSE** command is received Main Controlled Device will take no action.

If during **CLOSED** state **STOP** command is received Main Controlled Device will go to **STOPPED** state.

9.5. STOPPED

STOPPED is the state which the Main Controlled Device was interrupted during **OPENING** or **CLOSING** or **STOP** command was received during any state. Then no voltage is provided on motor output terminal.

If during **STOPPED** state **OPEN** command is received Main Controlled Device will start **OPENING**.

If during **STOPPED** state **CLOSE** command is received Main Controlled Device will start **CLOSING**.

If during **STOPPED** state **STOP** command is received Main Controlled Device will take no effect.

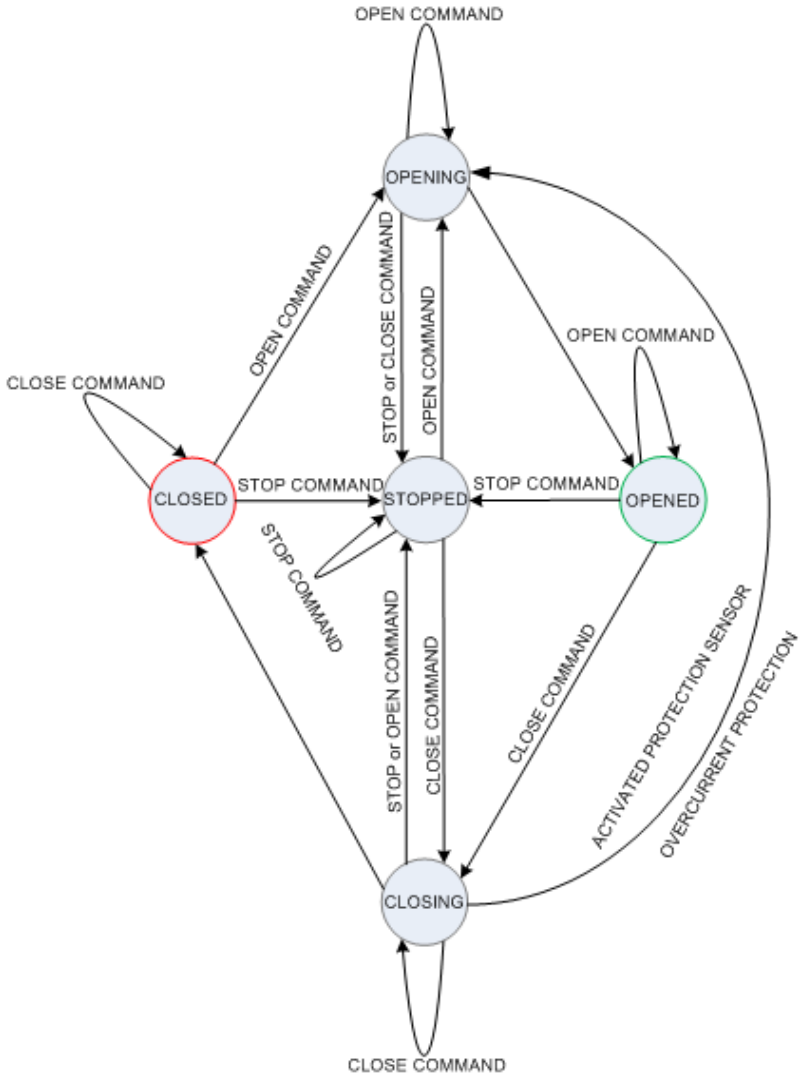

Figure 9.1. Graph of Main Controlled Device's states

10. Web access

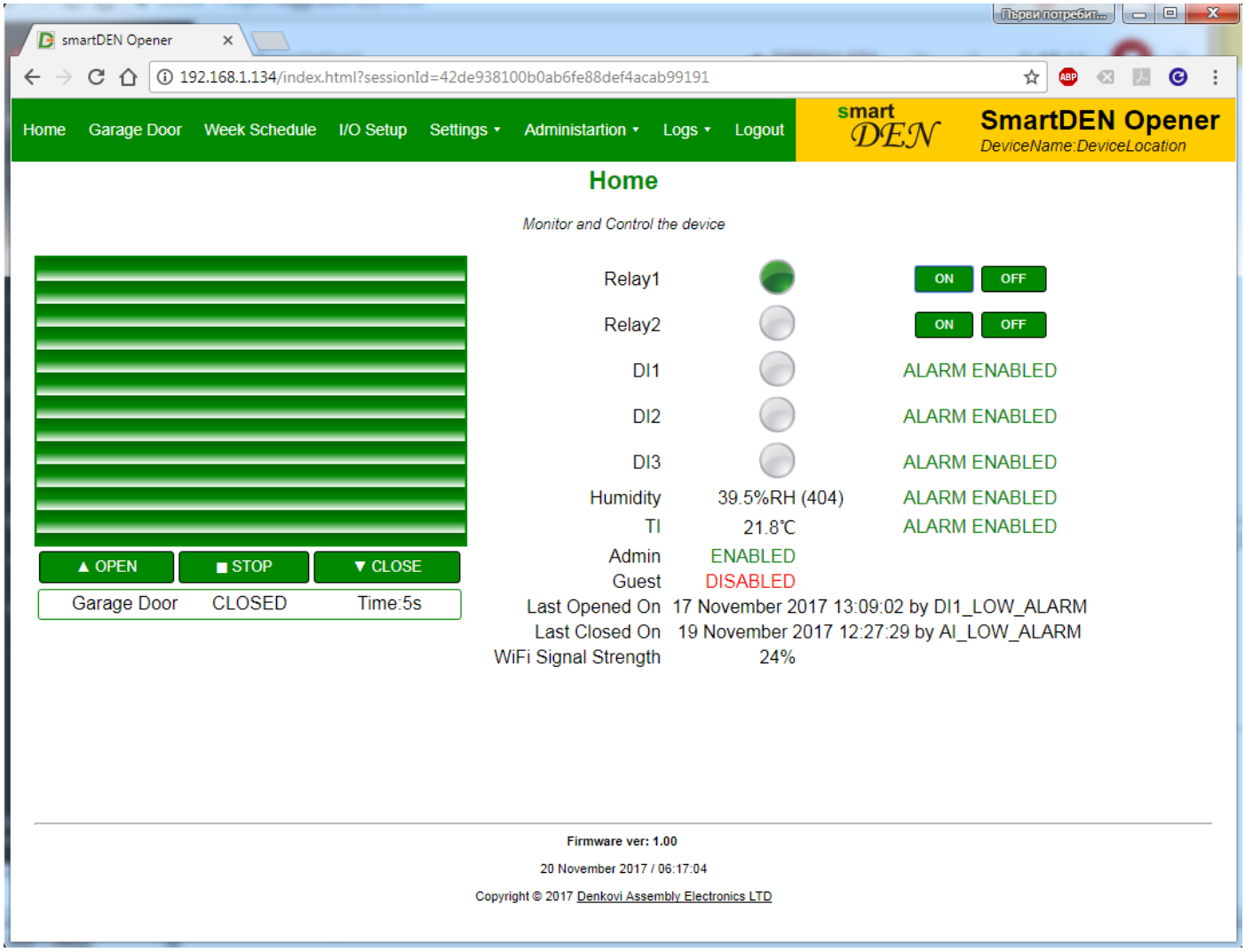

Figure 10.1. Web Access

To access the setup pages, run a web browser (Google Chrome, Mozilla Firefox or similar), and enter the **smartDEN Opener** IP address, for example: http://192.168.4.1

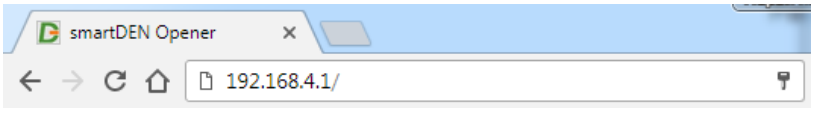

Figure 10.2. Open via browser

Note: Browser must have JavaScript enabled!

10.1. Login

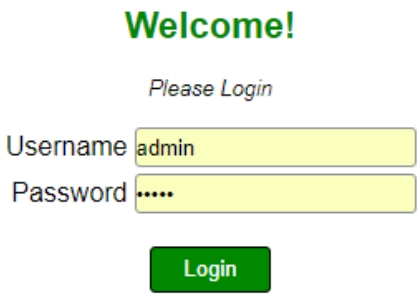

Figure 10.3. Login page

Enter the username and password and click "**Login**" button. This will bring you to the **smartDEN Opener** home page which contains details for the current status of the device.

Note: The default username and password are **admin / admin** (usernames and passwords are case sensitive).

Note: When the username and password are entered, they are transmitted across the network in encrypted form, so eavesdropping on the data transmission will not reveal the password.

Note: In order to prevent setup/control conflicts, at any given moment, only one user can be logged in.

Note: If there is no data traffic between the Web-browser and the **smartDEN Opener** for time, specified by **Session Timeout** parameter, the session "times out" and a new login is required.

10.2. Menu

The main menu consists of the following items, located on the top of the window frame. There are seven main menu buttons and three of them have submenus. The screenshot on **Figure 10.4** illustrates the menu bar on wide screen and **Figure 10.5** same menu on mobile screen. A short description of menu is given below:

- **Home** - this is monitoring and control page. All peripherals state is shown in real time at this page;
- **Garage Door** - this is Main Controlled Device's page. It consist of settings for times of opening/closing, protection sensor settings, etc.
- **Week Schedule** - this page allows creating events that will repeat weekly;
- **I/O Setup** - consist of settings for the digital inputs, analog input, temperature input and relays;
- **Settings** - there are five submenus for different settings:
  - **General Settings** - settings for HTTP& MQTT access, web server access, device settings, IP camera settings;
  - **Network** - settings for the network (IP addresses, MAC address, DHCP settings, etc.);
  - **Date/Time** - settings for date and time (NTP server, auto synchronization, Time zones, etc.);
  - **Email** - settings for email notifications (enable/disable emails, email addresses, etc.);
  - **MQTT** - settings for MQTT access (MQTT Broker and Port);
- **Administration** - this menu consist of four submenus:
  - **Firmware Update** - this page provides remote firmware update;
  - **Backup** - page for backups and restore settings from .cfg file;
  - **Factory Defaults** - when pressed this submenu button a dialog will open and ask for confirmation. Use this with attention;
  - **Reboot** - when pressed a confirmation dialog will be opened;
- **Logs** - this menu has two submenus:
  - **System Log** - contains log messages (boot time, network connection, date/time synchronization, etc.);
  - **Events Log** - text file containing log information for I/O state changes;
- **Logout** - clicking this button will end current session and redirect to login page;

Figure 10.4. Navigation menu (wide screen)

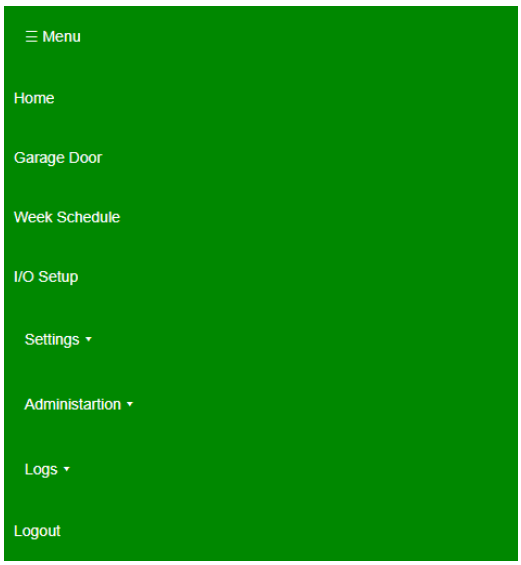

Figure 10.5. Navigation menu (mobile screen)

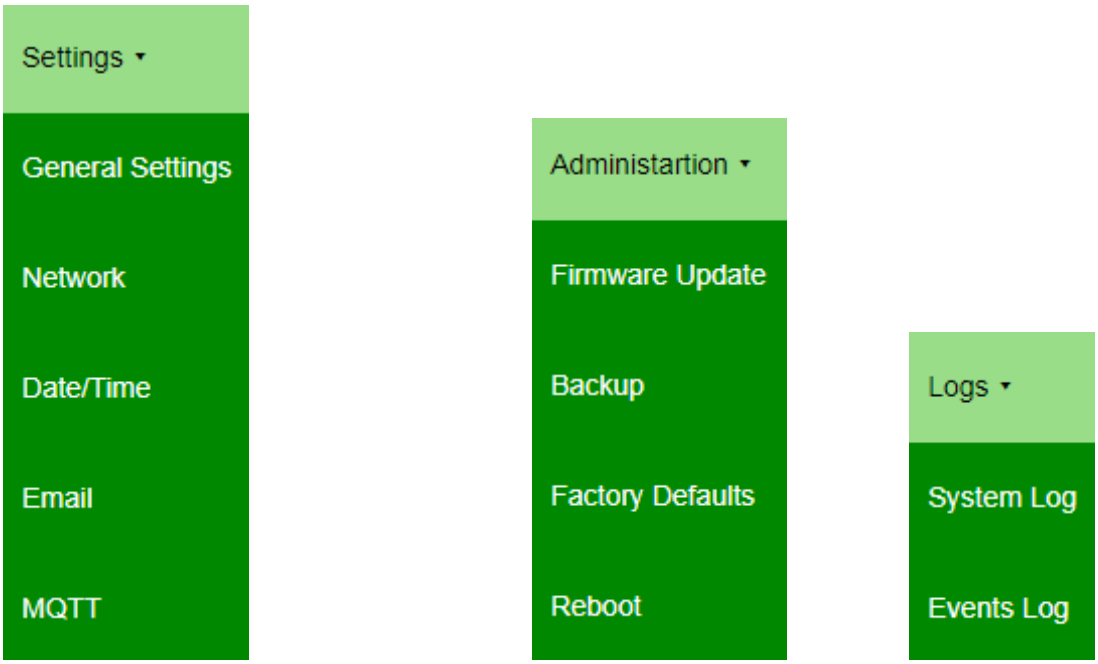

Figure 10.6. Settings, administration and logs submenus

10.3. Home page

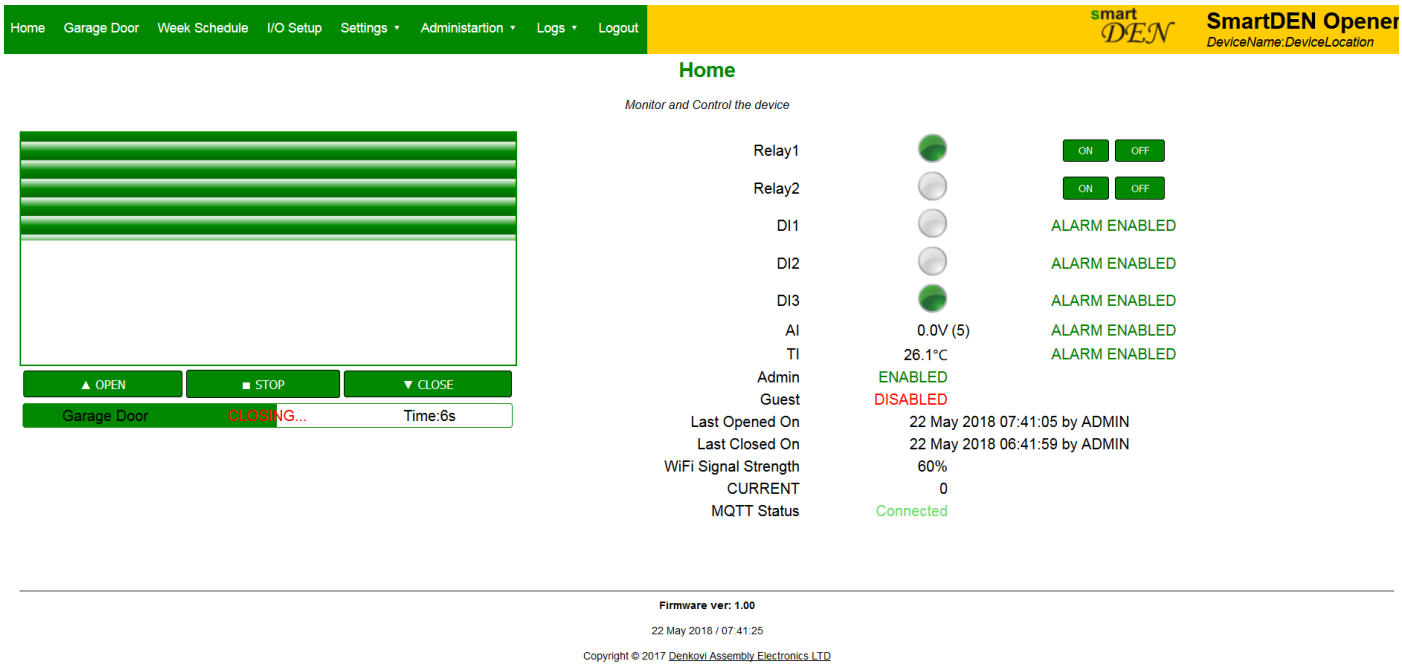

Figure 10.7. Home Page

This page contains real time information for the status of the inputs, relays, Main Controlled Device and additional information. Here it is detailed explanation of the page:

- **Animation** - there is an animation showing the movement of the Main Controlled Device. This animation will not be shown if IP camera is enabled;
- **OPEN / STOP / CLOSE** - these buttons control the movement of the Main Controlled Device;
- **Progress bar** - below the buttons is located progress bar containing information about the Main Controlled Device. For example on **Figure 10.7** the device is named "Garage Door", its state is **OPENING** and the time to fully Open is 5 seconds;
- **Relay1** - shows the state (ON is green and OFF is gray) and control buttons of Relay 1;
- **Relay2** - shows the state (ON is green and OFF is gray) and control buttons of Relay 2;
- **DI1** - shows the state (High is green and Low is gray) of the Digital Input 1 and its alarm (ENABLED / DISABLED);
- **DI2** - shows the state (High is green and Low is gray) of the Digital Input 2 and its alarm (ENABLED / DISABLED);

- **DI3** - shows the state (High is green and Low is gray) of the Digital Input 3 and its alarm (ENABLED / DISABLED);
- **AI** - shows the value (First shown is scaled value and then (raw ADC value)) of the Analog Input and its alarm (ENABLED / DISABLED);
- **TI** - shows the value of the Temperature Input and its alarm (ENABLED / DISABLED).
- **Admin** - shows the state (ENABLED / DISABLED) of Administrator's MQTT and HTTP access;
- **Guest** - shows the state (ENABLED / DISABLED) of Guest's MQTT and HTTP access.
- **Last Opened On** - shows the last time and reason (user) that opened the Main Controlled Device;
- **Last Closed On** - shows the last time and reason (user) that closed the Main Controlled Device;
- **Wi-Fi Signal Strength** - shows the signal strength of the Wi-Fi signal;
- **DeviceName** - name of the device.
- **DeviceLocation** - location of the device.
- **Firmware ver** - firmware version of the **smartDEN Opener**;
- At the row before last is located the date and time from **smartDEN Opener** real time clock.

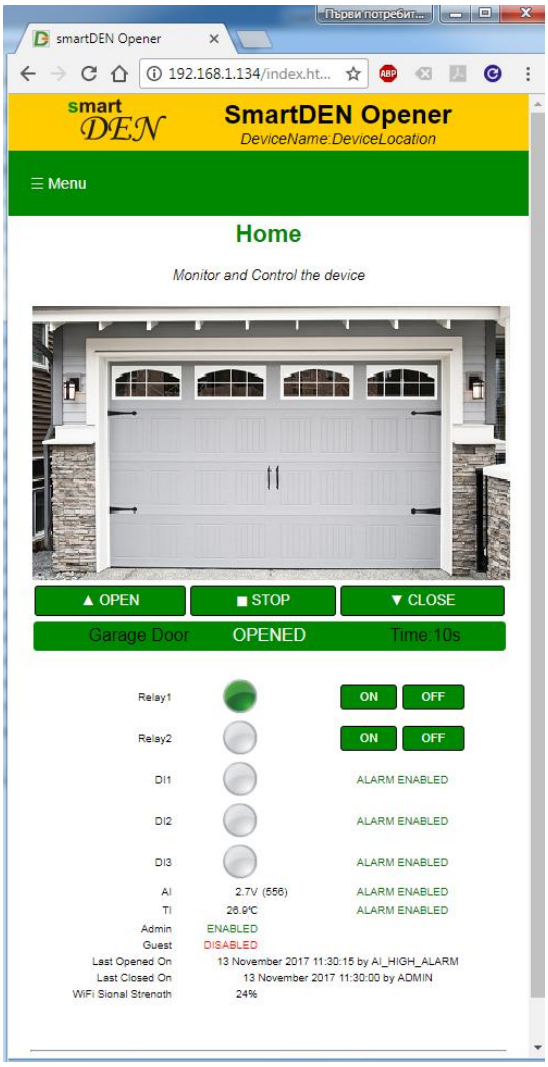

Figure 10.8. Home page (mobile view)

10.4. Main Controlled Device

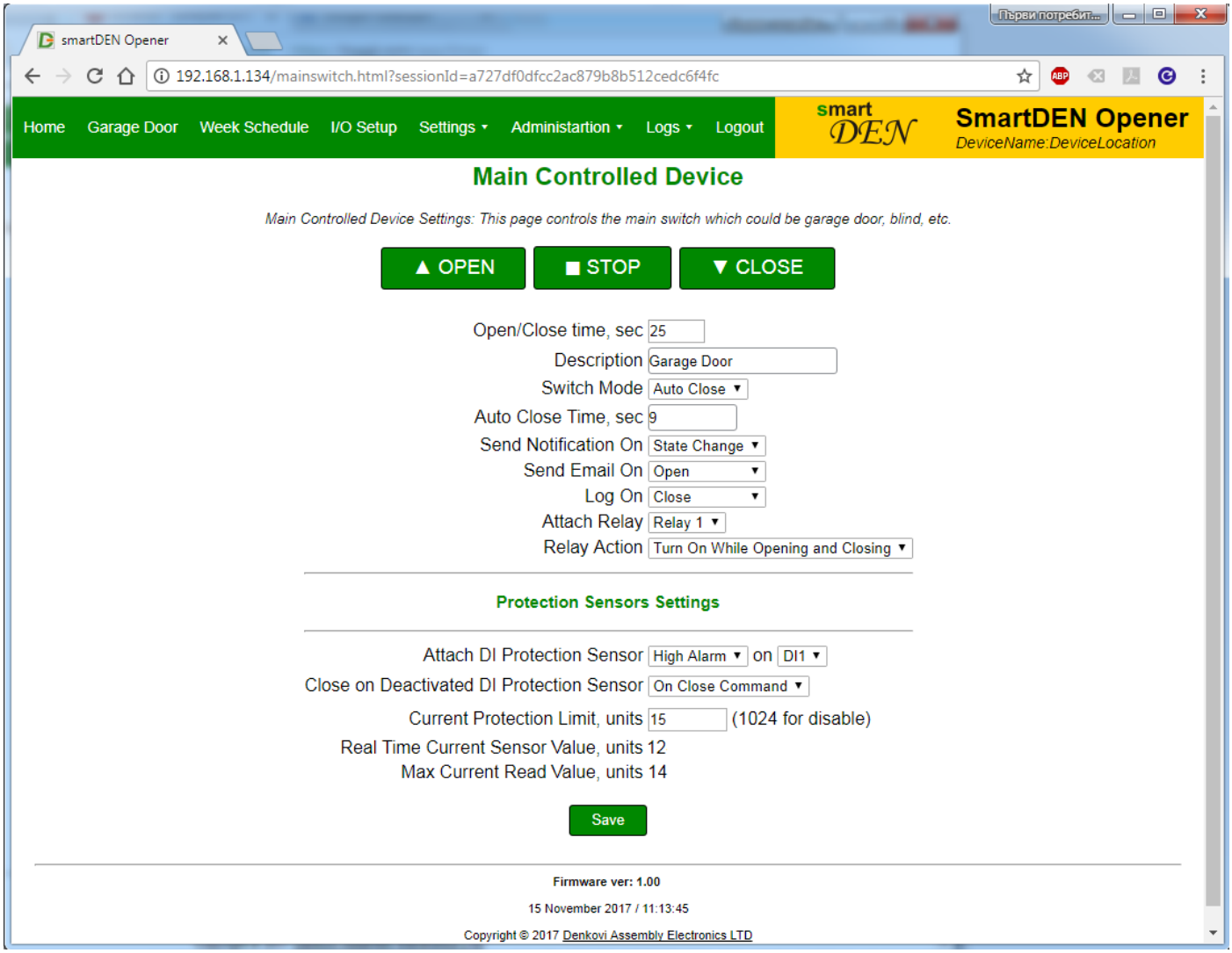

Figure 10.9. Main Controlled Device Page

This page describes the functionality and parameters of the Main Controlled Device. You can program the time for opening/closing time from here. There are additional options such as when to log and send different kind of notifications, attach protection sensor (for example to prevent closing when a person is under a garage door), "auto close" function, current protection, secondary protection, etc. Here is detailed explanation of the page.

- **OPEN/STOP/CLOSE** buttons - with these buttons you can program the time for opening/closing of the Main Controlled Device;
- **Open/Close Time** - This is the time that the Main Controlled Device's motor is turned on. Note that this time has tolerance ±1 second;
- **Description** - this text field allows naming the Main Controlled Device (by default it is "Garage Door"). There are up to 12 allowed symbols (see **Appendix 3**);
- **Switch Mode** - this parameter determines the working mode of the Main Controlled Device. There are two available options:
  - *Normal* - in this mode the Main Controlled Device is opened and closed by alarm or user;

- *Auto Close* - this parameter closes the Main Controlled Device after the time in seconds, specified by the **Auto Close time** parameter. This time can be from 1 to 65535 seconds;

- **Send notification On** - this parameter allows sending notification on specified state of the Main Controlled Device. There are several available options:
  - *Never* - this option will not send notifications about Main Controlled Device;
  - *State Change* - this will send notifications on **OPENED** and **CLOSED** states;
  - *Open* - this option will send you notifications on **OPENED** state;
  - *Close* - this option will send you notifications on **CLOSED** state;

Note: **Admin User** must be enabled and proper MQTT settings applied.

- **Send Email On** - This parameter allows sending emails on specified state of the Main Controlled Device. There are several available options:
  - *Never* - this option will not send emails about Main Controlled Device;
  - *State Change* - this will send email on **OPENED** and **CLOSED** states;
  - *Open* - this option will send you email on **OPENED** state;
  - *Close* - this option will send you email on **CLOSED** state;

Note: Emails must be enabled with proper settings applied.

- **Log On** - This parameter allows logging Main Controlled Device's states. There are several available options:
  - *Never* - this option will not log Main Controlled Device's state changes;
  - *State Change* - this will log OPENED, CLOSED and STOPPED states;
  - *Open* - this option will log OPENED state;
  - *Close* - this option will log CLOSED state;

Note: **Enable Writing to Logs** options must be enabled.

- **Attach Relay** - allows you to control one of the onboard relays depend on the state of the Main Controlled Device. There are three available options:
  - **Nothing** - no relay is attached;
  - *Relay 1* - if you select this option Relay 1 will be controlled by the Main Controlled Device. Relay action will be determined from **Relay Action** option;
  - *Relay 2* - this option will attach Relay 2 to Main Controlled Device. Relay action will be determined from **Relay Action** option;
- **Relay Action** - if you attach relay to Main Controlled Device, you can choose its action from these several options:
  - *Turn On While Opening and Closing* - this option will turn on the relay during the time the Main Controlled Device opens and closes. This option is suitable for Warning Lamps;
  - *Turn Off While Opening and Closing* - this option will turn off the relay during the time the Main Controlled Device opens and closes;
  - *Turn On When Opened* - this option will turn on the relay when the Main Controlled Device is **OPENED**. Suitable for lamps;
  - *Turn Off When Opened* - this option will turn off the relay when the Main Controlled Device is **OPENED**. Suitable for heaters in the winter;

- *Turn On When Closed* - this option will turn on the relay when the Main Controlled Device is **CLOSED**. Suitable for heaters in the winter;
- *Turn Off When Closed* - this option will turn on the relay when the Main Controlled Device is **CLOSED**. Suitable for heaters in the lamps;

- **Attach DI Protection Sensor** - you can "attach" a digital input which will prevent the door from closing when an object is detected and auto-close when the object is gone. For proper use of this parameter it is needed to be a digital input with constant output (not pulse). For example barrier sensor mounted under the door/barrier is a proper choice:
  - *No sensor* - will not "attach" a Digital Input to the Main Controlled Device;
  - *Low Level* - will "attach" the selected Digital Input and will be **ACTIVATED** when the level on the selected Digital Input is LOW;
    High Level - will "attach" the selected Digital Input and will be **ACTIVATED** when the level on the selected Digital Input is HIGH;

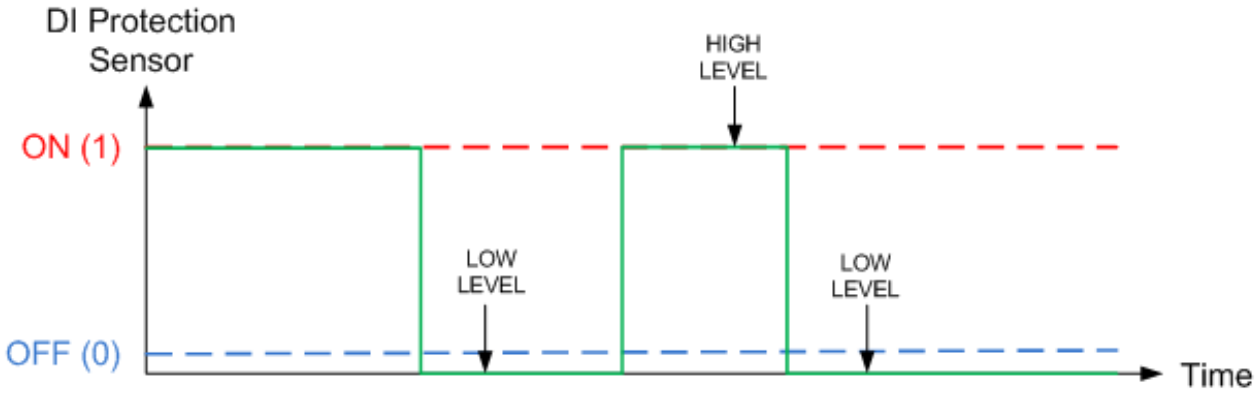

Figure 10.10. DI Protection Sensor Levels

- **Close on Deactivated DI Protection Sensor** - this parameter is used to close the Main Controlled Device by the DI protection sensor. When object is entering in the zone of sensor, it is called **ACTIVATED** state and when leaving it is **DEACTIVATED** state. The condition for **CLOSING** is that DI protection sensor must be **ACTIVATED** first and then **DEACTIVATED**:
  - *Never* - the Main Controlled Device will never be closed by DI protection sensor;
  - *On Close Command* - the Main Controlled Device will be closed only if **CLOSE** command is received during **OPENING** or in **OPENED** state and only if the DI protection sensor is **DEACTIVATED** in the way described above;
  - *Always* - the Main Controlled Device will be closed every time when the DI Protection sensor is **DEACTIVATED**;

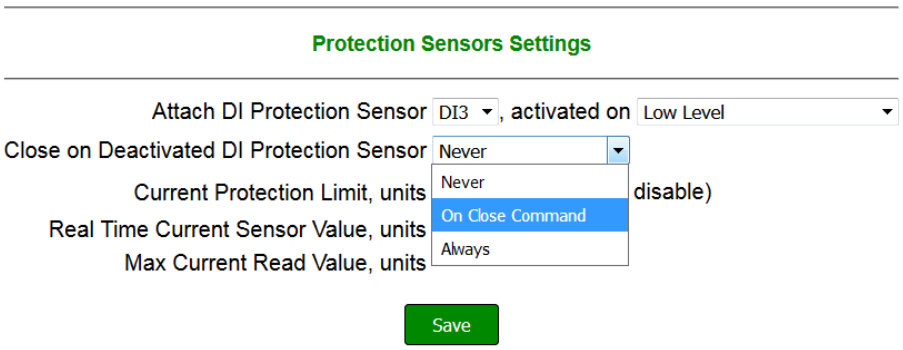

Figure 10.11. **Close on Deactivated DI Protection Sensor** options

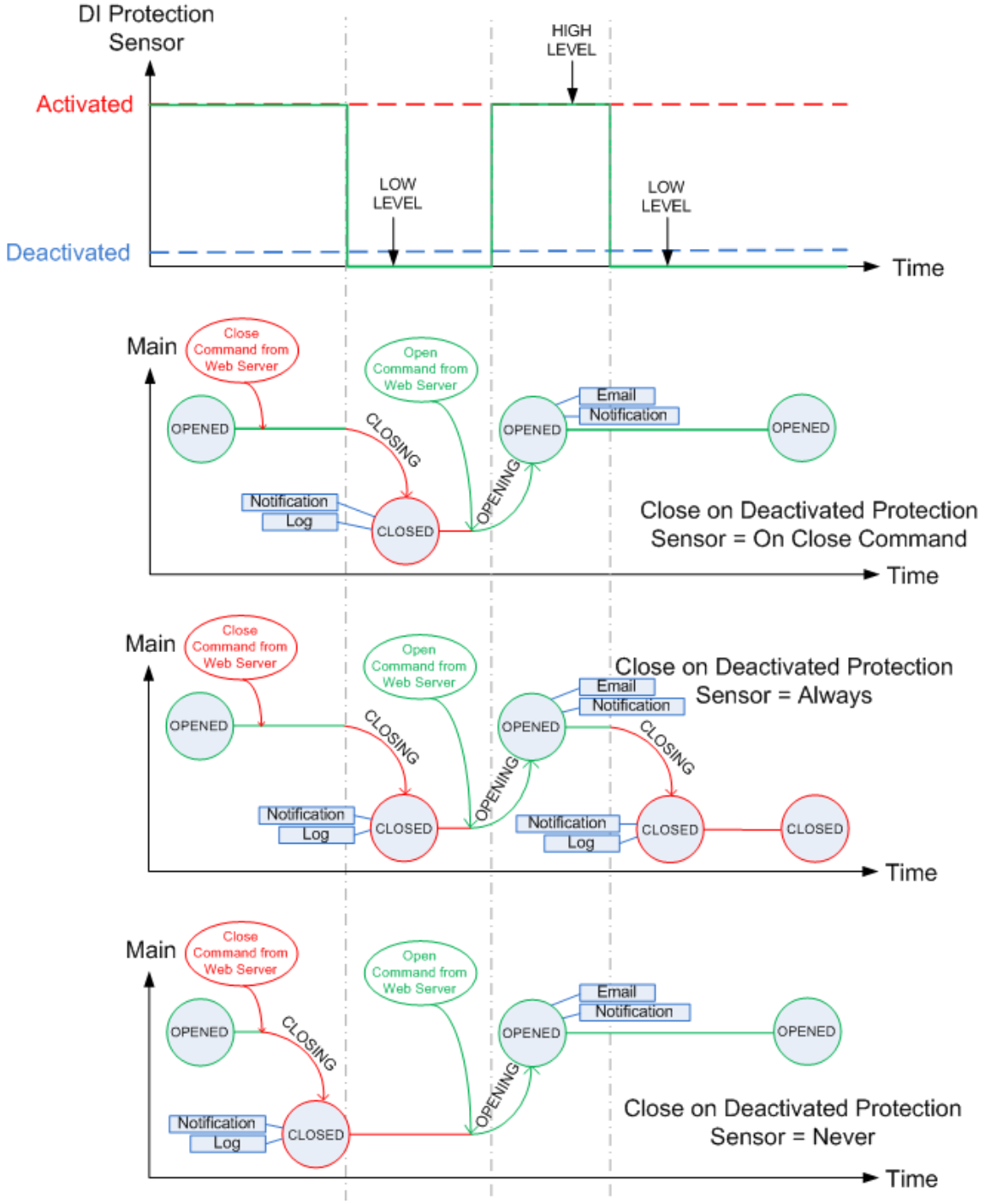

Figure 10.12. Close on Deactivated DI Protection Sensor options behavior

⚠ When using **DI Protection Sensor** for proper working be sure that nothing will DISABLE its alarm (for example week schedule could make it malfunction if DISABLE event occurs).

Current Protection Limit - This value is used when Main Controlled Device is **CLOSING**. If the current units become higher than this value, the Main Controlled Device will start **OPENING**. If this parameter is 1024, the current protection is disabled. If current protection is desired, make sure that this value is more than **Max Current Read Value** to prevent unwanted **OPENING** during **CLOSING**. If Main Controlled Device is **OPENED** by **Current**

Protection Limit, it will stay **OPENED** until some other input (DI, AI, TI, Auto Close, etc.) or user send **CLOSE** command;

- **Real Time Current Sensor Value, units**: when closing the Main Controlled Device this parameter show the current motor consumption. It is in ADC raw units;
- **Max Current Sensor Value, units**: the maximum measured current while closing the Main Controlled Device. It is in ADC raw units;
- **Save** - should be clicked every time when made changes before leaving this page.

On the figure below it is illustrated an example with garage door and a car. Firstly the garage door (Main) is **OPENED** by web server. Then accidently a car is parked below the garage door. A **CLOSE** command is received from the web server and **smartDEN Opener** starts **CLOSING** the garage door. At given moment the door reaches the car and motor's current increases above the **Current Protection Limit** which changes Main direction and garage door starts **OPENING**.

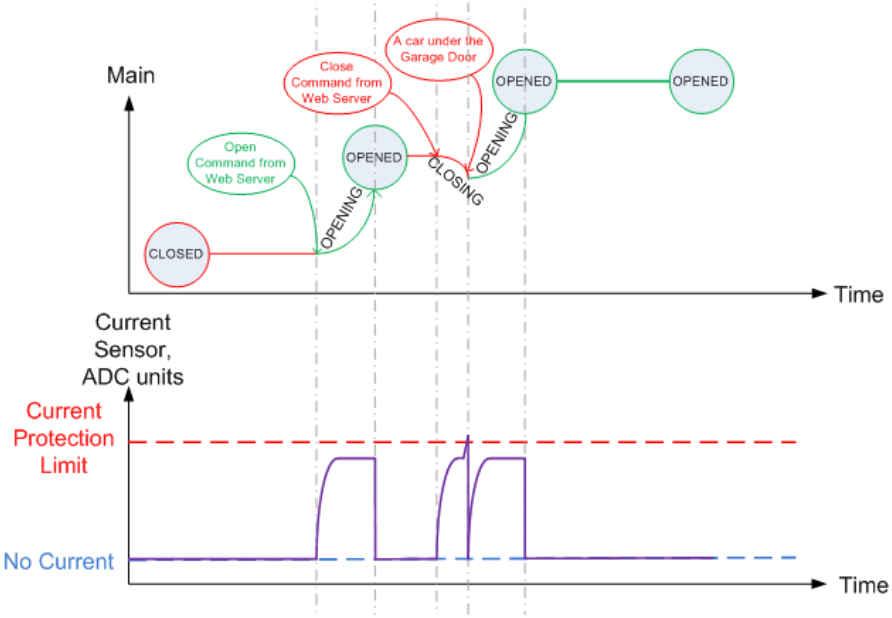

Figure 10.13. Current protection usage example

⚠ Use **Current Protection Limit** feature only if possible and with HIGH ATTENTION as per the Main Controlled Device producer. It may damage your stuff if not proper tuned.

⚠ **smartDEN Opener** can control motor with maximum consumption 4A or that is about 300 ADC raw units which means when the **CLOSE** button is clicked, the "**Real Time Current Sensor Value"** and "**Max Current Sensor Value**" must be less than 300.

⚠ This type of protection is not suitable for all types of applications. Please use it with care! Set up the parameters only as per the Main Controlled Device manufacturer.

⚠ The **Current Protection Limit** must be set as lower as possible in order to be sensitive but still higher than **Max Current Sensor Value** in order to avoid fake detections.

10.5. Week Schedule

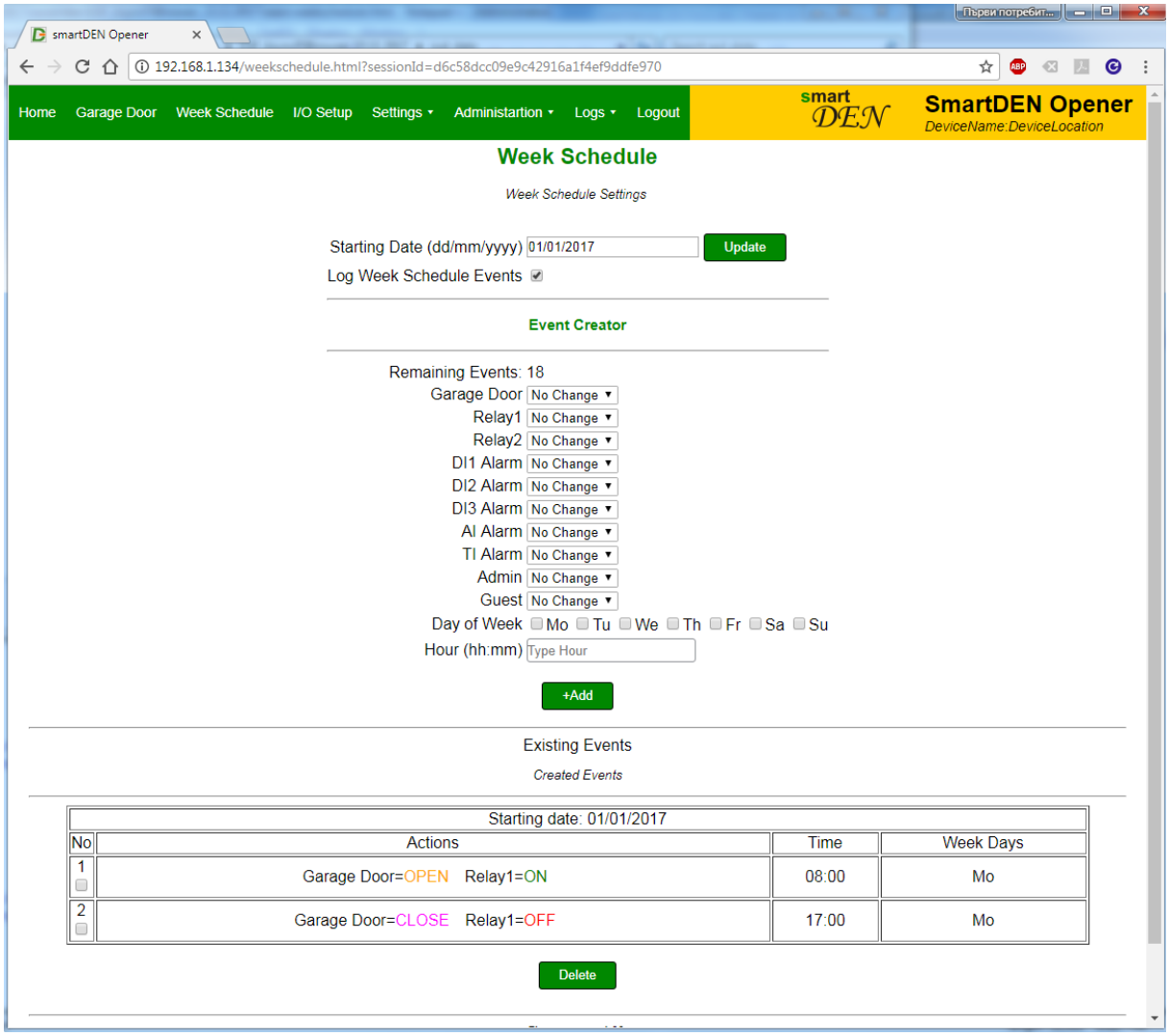

Figure 10.14. Week Schedule Page Overview

This page provides creating of events (up to 20) that will repeat weekly standalone without need of constant computer or smart phone connection.

- **Starting Date** - executing created events will start from this date. As shown in the page the format is date/month/year. Update button can change this date;
- **Log Week Schedule Events** - this checkbox allows enabling/disabling logs for events;
- **Remaining Events** - the number of remaining events that can be created. Maximum allowed events are 20;
- **Garage Door*** - specifies the state of the Main Controlled Device. There are three options:
  - *No Change* - will not affect state of the Main Controlled Device;
  - *OPEN* - will start opening Main Controlled Device if it is not;
  - *CLOSE* - will start closing Main Controlled Device if it is not;
- **Relay1*** - specifies the state of the Relay 1. There are three options:
  - *No Change* - will not affect state of the Relay 1;
  - *ON* - will turn on Relay 1 if it is off;
  - *OFF* - will turn off Relay 1 if it is on;
- **Relay2*** - specifies the state of the Relay 2. There are three options:

  - *No Change* - will not affect state of the Relay 2;
  - *ON* - will turn on Relay 2 if it is off;
  - *OFF* - will turn off Relay 2 if it is on;
- **DI1* Alarm** - specifies the state of Digital Input 1 alarm. There are three options:
  - *No Change* - will not affect state of the Digital Input 1 alarm;
  - *ENABLED* - will enabled Digital Input 1 alarm;
  - *DISABLED* - will disable Digital Input 1 alarm;
- **DI2* Alarm** - specifies the state of Digital Input 2 alarm. There are three options:
  - *No Change* - will not affect state of the Digital Input 2 alarm;
  - *ENABLED* - will enabled Digital Input 2 alarm;
  - *DISABLED* - will disable Digital Input 2 alarm;
- **DI3* Alarm** - specifies the state of DI3 alarm. There are three options:
  - *No Change* - will not affect state of the Digital Input 3 alarm;
  - *ENABLED* - will enabled Digital Input 3 alarm;
  - *DISABLED* - will disable Digital Input 3 alarm;
- **AI* Alarm** - Specifies the state of Analog Input alarm. There are three options:
  - *No Change* - will not affect state of the analog Input alarm;
  - *ENABLED* - will enabled Analog Input alarm;
  - *DISABLED* - will disable Analog Input alarm;
- **TI* Alarm** - Specifies the state of Temperature Input alarm. There are three options:
  - *No Change* - will not affect state of the Temperature Input alarm;
  - *ENABLED* - will enabled Temperature Input alarm;
  - *DISABLED* - will disable Temperature Input alarm;
- **Admin** - Specifies the state of **Admin User** HTTP and MQTT access. There are three options:
  - *No Change* - will not affect **Admin User** access;
  - *ENABLED* - will enabled **Admin User** access;
  - *DISABLED* - will disable **Admin User** access;
- **Guest** - Specifies the state of **Guest User** HTTP and MQTT access. There are three options:
  - *No Change* - will not affect **Guest User** access;
  - *ENABLED* - will enabled **Guest User** access;
  - *DISABLED* - will disable **Guest User** access;
- **Day of Week** - specifies the days in which this event will be executed;
- **Hour -** specifies the time in which this event will be executed. Format is hour:minutes;
- **Add** - with this button an event is created and will be shown in "**Existing Events**" section;
- **Existing Events** - a table containing all existing events. Every event in the table has a serial number, actions (that are executed when occur), time (when occurs) and week days (which days in week is executed);
- **Delete** - button which deletes selected events from the Existing Events' table.

⚠ ***These names are default descriptions of the I/O peripherals. When changing description of peripherals, the new descriptions will be displayed.

⚠ After deleting an event, the next added event will has the serial number of the smallest event number that has been deleted.

10.6. I/O Setup

10.6.1. Digital Inputs

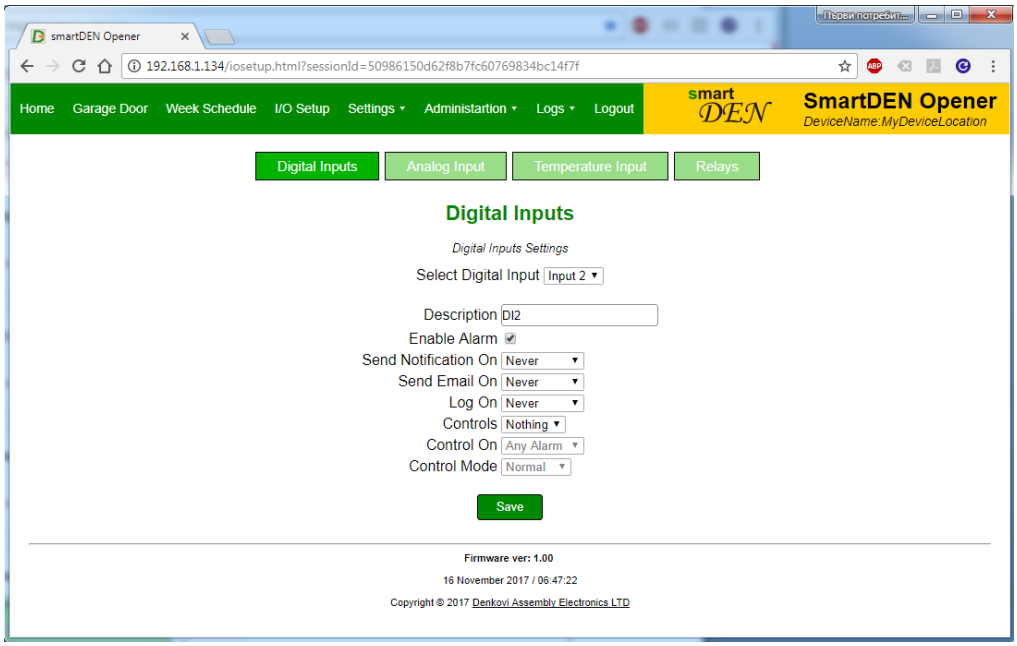

Figure 10.15. Digital Inputs page

smartDEN Opener has three digital inputs, which can control different or same peripheral (Main Controlled Device or some relay). Every digital input has these parameter:

- **Select Digital Input** - dropdown menu to select one of the digital inputs;
- **Description** - specifies the name of the digital input (for example "Button"). There are up 10 allowed symbols for description (see **Appendix 3**);
- **Enable Alarm** - this will allow the digital input to control its peripheral (if desired) or just write to log, send notifications or emails (if enabled). For example on below alarm is enabled but **Controls**, **Send notification On**, **Log On** and **Send Email On** are not desired, so nothing will happen on "Any Alarm". LOW ALARM EVENT is generated on HIGH (ON) to LOW (OFF) transition of the digital input. HIGH ALARM event is generated on LOW (OFF) to HIGH (ON) transition.

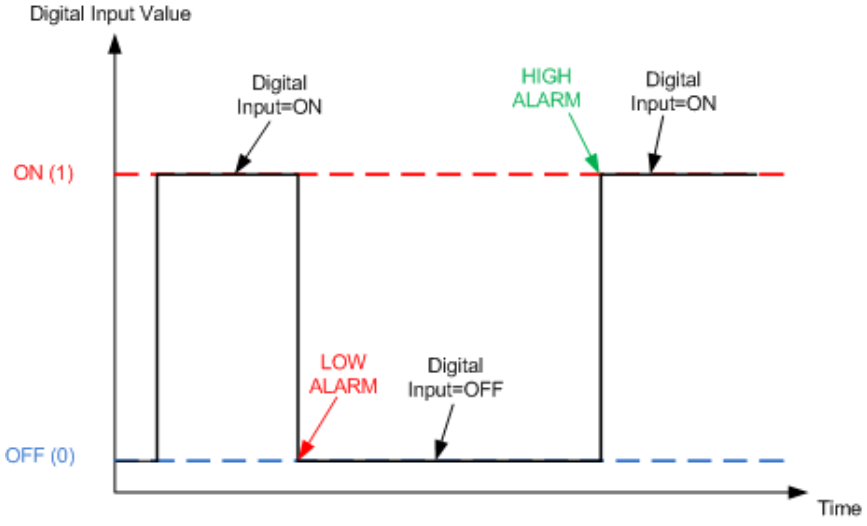

Figure 10.16. Digital Inputs alarms

- **Send notification On** - this parameter allows sending MQTT notifications on specified alarm:
  - *Never* - **smartDEN Opener** will not send any notifications about selected digital input;
  - *Low Alarm* - controller will send notifications only on high to low transition of the digital input (falling edge);
  - *High Alarm* - controller will send notifications only on low to high transition of the digital input (rising edge);
  - *Any Alarm* - will send notifications on both LOW ALARM event and HIGH ALARM event;

  In order to use this parameter MQTT settings should be set properly and **Admin/Guest User** accounts should be enabled in the way desired. Note that notifications are available in *DAE-aModules* App with MQTT enabled.

- **Send Email On** - this parameter allows sending emails on specified alarm:
  - *Never* - **smartDEN Opener** will not send any emails about selected digital input;
  - *Low Alarm* - controller will send emails only on high to low transition of the digital input (falling edge);
  - *High Alarm* - controller will send emails only on low to high transition of the digital input (rising edge);
  - *Any Alarm* - will send emails on both LOW ALARM event and HIGH ALARM event;
- **Log On** - this parameter allows writing to Events Log only on specified alarm:
  - *Never* - **smartDEN Opener** will not write log messages about selected digital input;
  - *Low Alarm* - controller will write logs only on high to low transition of the digital input (falling edge);
  - *High Alarm* - controller will write logs only on low to high transition of the digital input (rising edge);
  - *Any Alarm* - will write logs on both LOW ALARM event and HIGH ALARM event;
- **Controls** - this parameters specifies which output is controlled by this digital input:
  - *Nothing* - this digital input will not control any output. If some of the previous settings are set it will be used for monitoring some process (for example if used barrier sensor it may send notification when it is crossed through);
  - *Relay 1* - this digital input will control Relay 1;
  - *Relay 2* - this digital input will control Relay 2;
  - *Main* - this digital input will control Main Controlled Device;
- **Control On** - specifies on which alarm the digital input will control the selected output:
  - *Low Alarm* - the digital input will control selected output only on high to low transition (falling edge);
  - *High Alarm* - the digital input will control selected output only on low to high transition (rising edge);
  - *Any Alarm* - the digital input will control selected output on both LOW and HIGH ALARM events;
- **Control Mode** (**Controls** is selected to be "Relay1" or "Relay2"):
  - *Normal* - in this mode the selected relay will turn on when digital input generates HIGH ALARM and will turn off when LOW ALARM event is generated;
  - *Inversed* - in this mode the selected relay will turn on when digital input generates LOW ALARM event and will turn off when HIGH ALARM event is generated;
  - *Toggle* - in this mode, depending on the selected **Control On** value, the state of the relay will be inversed (toggled).
- **Control Mode** (**Controls** is selected to be "Main"):

- *Open* - in this mode the Main Controlled Device will start **OPENING** on selected alarm (alarm selected in **Control On**);
- *Stop* - in this mode the Main Controlled Device will **STOP** on selected alarm (alarm selected **in Control On**);
- *Close* - in this mode the Main Controlled Device will start **CLOSING** on selected alarm (alarm selected in **Control On**);
- *Toggle* - in this mode the Main Controlled Device will start **CLOSING** if it is **OPENED** or will start **OPENING** if is **CLOSED** or **STOPPED** on selected alarm (alarm selected in **Control On**);
- *NO Sensor* - in this mode the Main Controlled Device will start **OPENING** if **Control On** option is set to "Low Alarm". If **Control On** option is set to "High Alarm" the Main Controlled Device will start **CLOSING**. If "Any Alarm" is selected in **Control On** option, then the Main Controlled Device will **OPEN** on LOW ALARM event and **CLOSE** on HIGH ALARM event.
- *NC Sensor* - in this mode the Main Controlled Device will start **CLOSING** if **Control On** option is set to "Low Alarm". If **Control On** option is set to "High Alarm" the Main Controlled Device will start **OPENING**. If "Any Alarm" is selected in **Control On** option then the Main Controlled Device will **CLOSE** on LOW ALARM event and **OPEN** on HIGH ALARM event.
- *Protection* - in this mode the Main Controlled Device will prevent **CLOSING** if the level on the selected digital input is equal to selected alarm in **Control On** option. For example if **Control On** is set to "High Alarm", the Main Controlled Device will not **CLOSE** if the level on the digital input is HIGH (1). Usually this option must not be set by the user manually.

The next example describes the behavior of controlling relays by digital input. On **Figure 10.17** is shown configuration of the **smartDEN Opener** and on **Figure 10.18** is given timing diagram how the relay is reflected depend on the digital input.

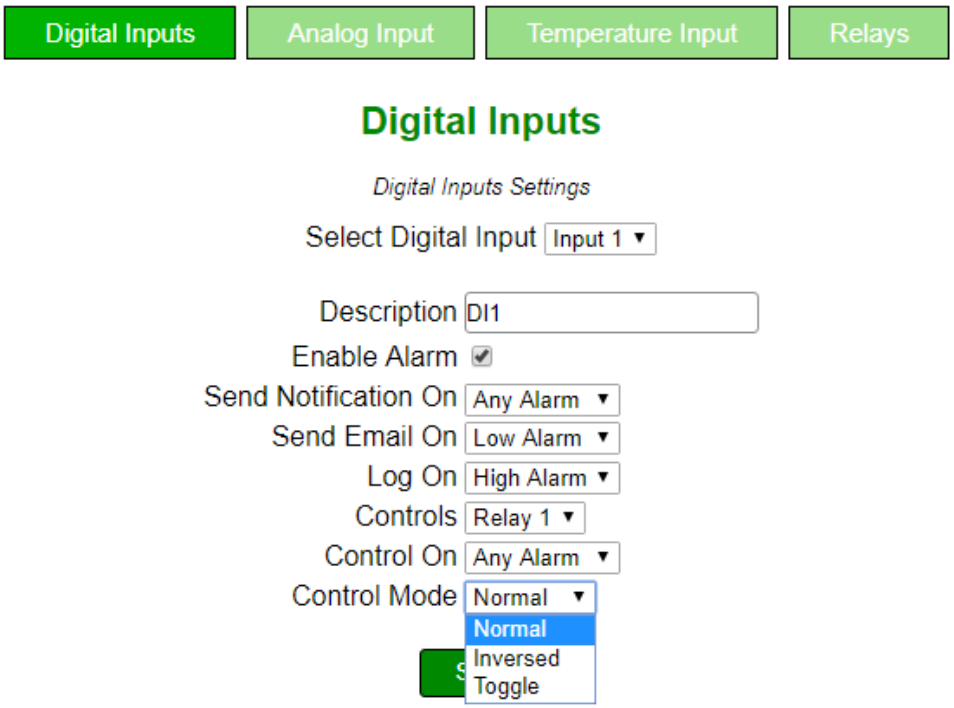

Figure 10.17. Digital input controlling relay settings

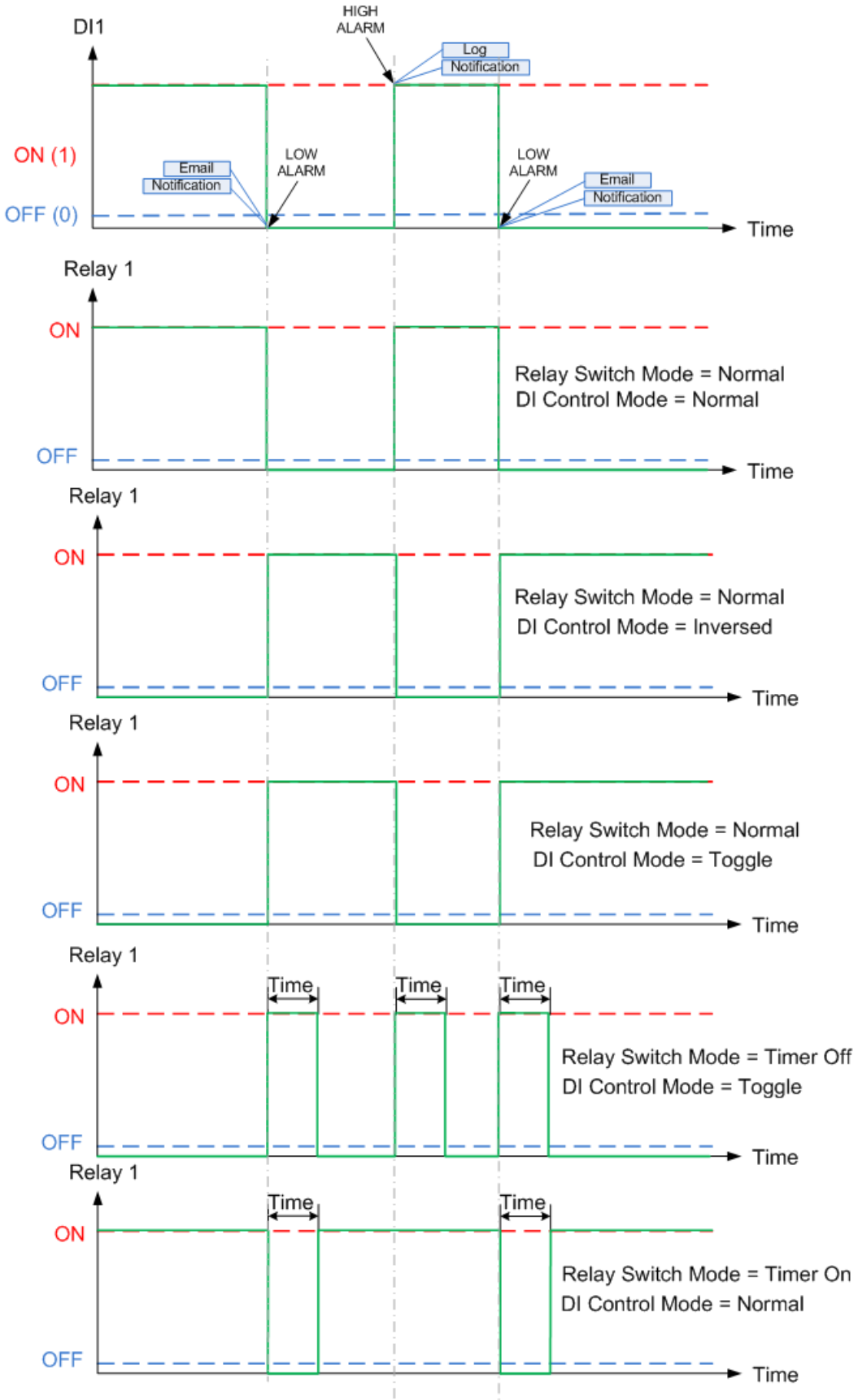

Figure 10.18. Digital input controlling relay examples

On the figure above, Digital Input 1 (named "DI1") controls Relay 1 on "Any Alarm" (LOW ALARM EVENT and HIGH ALARM event respectively). First three graphics are captured with Relay 1 working in "Normal" **Relay Switch Mode**.

As shown on the graphics DI1 first makes transition from HIGH to LOW level and generates LOW ALARM EVENT. In "Normal" **Control Mode** if the Relay 1 was turned on then it turns off. In "Inversed" **Control Mode** if the Relay 1 was turned off then it turns on. In "Toggle" **Control Mode** if the Relay 1 was turned off then it turns on. On this point an email is sent.

The next transition generates HIGH ALARM. In "Normal" **Control Mode** if the Relay 1 was turned off then it turns on. In "Inversed" **Control Mode** if the Relay 1 was turned on then it turns off. In "Toggle" **Control Mode** if the Relay 1 was turned on then it turns off. On this point a log message is written to events log.

The last transition on generates LOW ALARM EVENT again. The states are identical to the first LOW ALARM EVENT.

Last two graphics show "Toggle" and "Normal" **Control Mode** but with Relay 1 configured to work in "Timer On" and "Timer Off" **Relay Switch Mode**. As shown on graphics, Relay 1 turns on or off automatically after time specified by the Relay 1 **Time** parameter.

The next examples are about controlling Main Controlled Device from digital input.

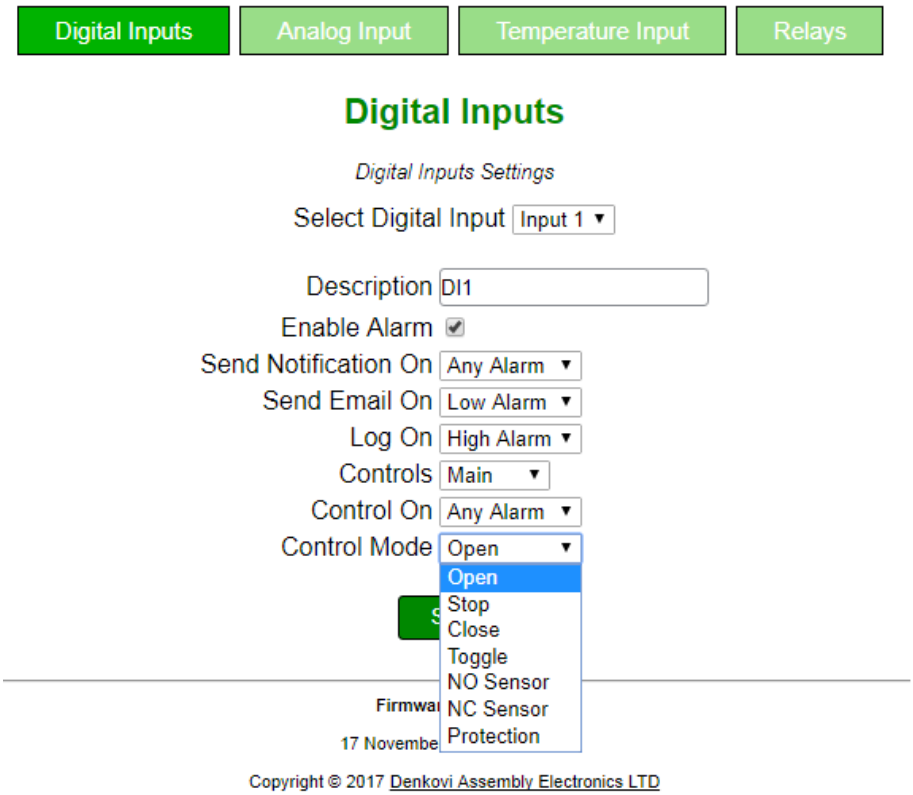

Figure 10.19. Digital Input controlling Main Controlled Device settings

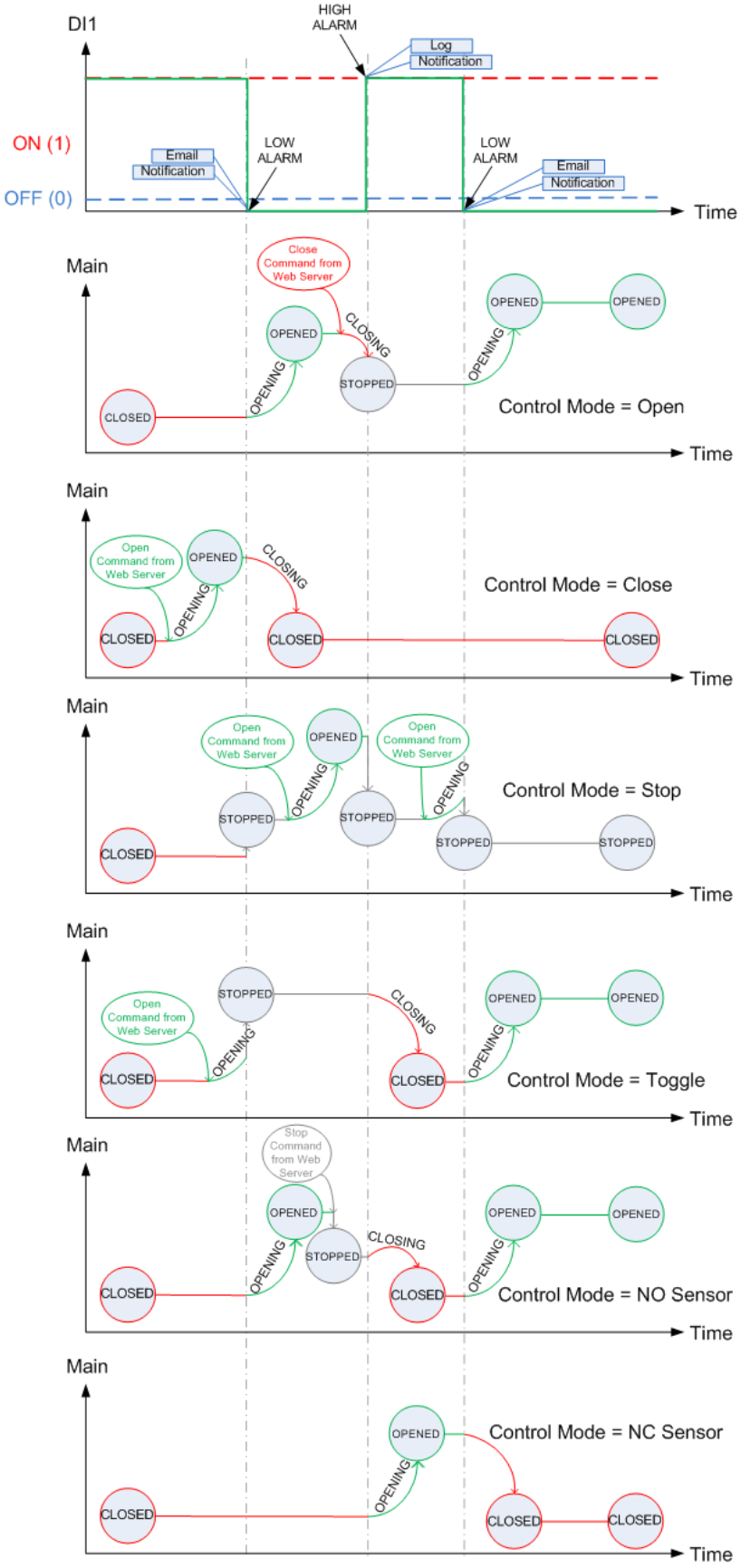

Figure 10.20. Digital Input controlling Main Controlled Device examples

On the **Figure 10.20** example, Digital Input 1 named "DI1" controls Main Controlled Device (Main) on Any Alarm (LOW ALARM EVENT and HIGH ALARM respectively). On each alarm notification is sent and emails are sent on LOW ALARM EVENT and log messages are written on HIGH ALARM.

As shown on the graphics DI1, first makes transition from HIGH to LOW level and then generates LOW ALARM EVENT. In "Open" **Control Mode,** when the Main Controlled Device was closed, it starts **OPENING** and reaches **OPENED** state. Before the next alarm occurs, **smartDEN Opener** receives **CLOSE** command from the web server and starts **CLOSING**. When high alarm is generated, Main Controlled Device stops and goes to **STOPPED** state. On the next LOW ALARM EVENT, it starts **OPENING** again.

If "Close" **Control Mode is** chosen, when the **Main Controlled Device** was **CLOSED,** it receives **OPEN** command and starts **OPENING**. Then goes to state **OPENED** after **Open/Close time** expires. On next alarm, it starts **CLOSING**. When **CLOSED,** it receives another alarm which should **CLOSE** it, but does not take effect because it is already **CLOSED**.

If **Control Mode** is "Stop", then on **Any Alarm** (in our example) the Main Controlled Device will go to **STOPPED** state. As shown on **Figure 10.20,** Main is **CLOSED** and receives **STOP** command and then it changes its state to **STOPPED**. Then an **OPEN** command is sent and the Main Controlled Device starts **OPENING**. When reaches **OPENED** state, HIGH ALARM is generated and Main goes to **STOPPED** state again. A new **OPEN** command is received and Main starts **OPENING**. Before **Open/Close time** expires, a new alarm is generated and the Main Controlled Device goes to **STOPPED** state.

If "Toggle" **Control Mode** is selected, the Main Controlled Device will switch over **OPENED** and **CLOSED** state on **Any Alarm** (in our example). The Main Controlled Device is in **CLOSED** state and receives an **OPEN** command from the web server. Main starts **OPENING** and then a **CLOSE** (the opposite of **OPEN**) command is generated on LOW ALARM EVENT. This makes the state of the Main Controlled Device **STOPPED**. On next generated HIGH ALARM, a **CLOSE** command is sent (because the state before **STOPPED** was **OPENING**) and Main Controlled Device starts **CLOSING**. It reaches **CLOSED** state and after a while, a LOW ALARM EVENT is generated again. Then an **OPEN** command is sent and Main start **OPENING**.

In "NO Sensor" **Control Mode** as described earlier LOW ALARM EVENT will **OPEN** the Main Controlled Device and HIGH ALARM will **CLOSE** it. On first LOW ALARM EVENT an **OPEN** command is sent and Main starts **OPENING**. After a while, when reached **OPENED** state, a **STOP** command is sent from the web server and Main goes to **STOPPED** state. On the HIGH ALARM the Main Controlled Device starts **CLOSING** and goes to **CLOSED** state. On the next LOW ALARM EVENT, again an **OPEN** command is sent and Main starts **OPENING**.

In "NC Sensor" **Control Mode** as described earlier LOW ALARM EVENT will **CLOSE** the Main Controlled Device and HIGH ALARM will **OPEN** it. On first LOW ALARM a **CLOSE** command is sent, but Main is already in **CLOSED** state. On the HIGH ALARM an **OPEN** command is sent and the Main Controlled Device starts **OPENING**. On next LOW ALARM EVENT again a **CLOSE** command is sent and Main starts **CLOSING**.

10.6.2. Analog Input

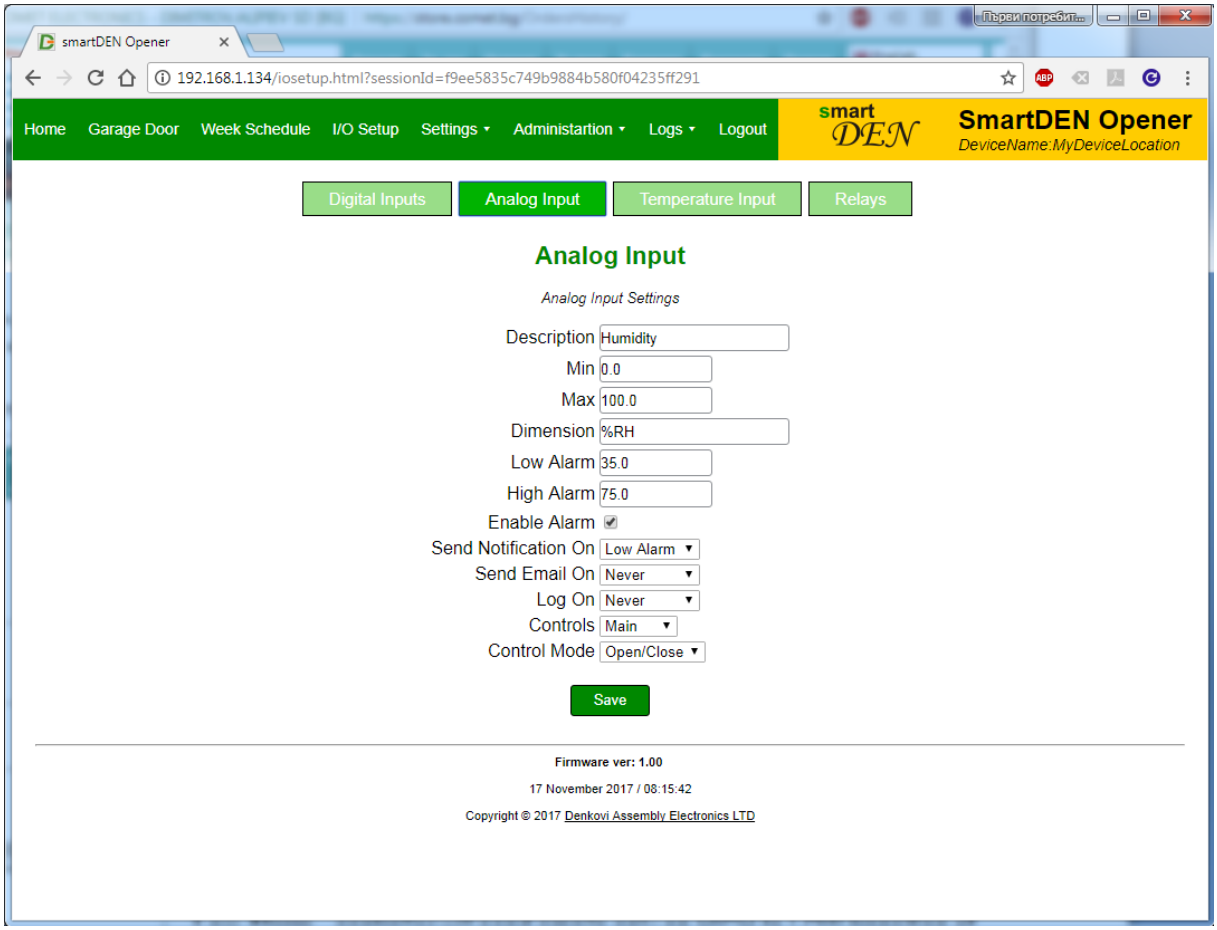

Figure 10.21. Analog Input page

smartDEN Opener provides one analog input (with 0-5V input range usually) for sensors with analog outputs (linear preferable):

- **Description** - name of the analog input. There are 10 allowed symbols reserved for description (see **Appendix 3**);
- **Min** - this value is the minimum value of the linear scaled voltage on analog input. Its value should be in range -32768.0 to 32767.0;
- **Max** - this value is the maximum value of the linear scaled voltage on analog input. Its value should be in range -32768.0 to 32767.0;
  Equations of scaled value of Analog Input is given below. There are two possibilities:
  - **Min** is higher number than **Max**:

$$AIScaledValue = Min - \frac{ADCValue}{\frac{1024}{Min-Max}}$$

  - **Max** is higher number than **Min**:

$$AIScaledValue = Min + \frac{ADCValue}{\frac{1024}{Max-Min}}$$

- **Dimension** - this is the dimension of the scaled value. There are 5 allowed symbols reserved for this parameter (see **Appendix 3**);
- **Low Alarm** - sets the scaled value on which LOW ALARM event will be generated. LOW ALARM event is generated when the scaled value of the Analog Input is higher than **High Alarm** parameter value and then falls below **Low Alarm** parameter value;

- **High Alarm** - sets the scaled value on which HIGH ALARM event will be generated. HIGH ALARM event is generated when the scaled value of the Analog Input is lower than **Low Alarm** parameter value and then exceeds **High Alarm** parameter value;
- **Enable Alarm** - if this option is checked alarms will be generated for the analog input;
- **Send notification On** - this parameter allows sending notifications on specified alarm. There are four choices:
  - *Never* - **smartDEN Opener** will not send any notifications about analog input;
  - *Low Alarm* - controller will send notifications only on LOW ALARM event;
  - *High Alarm* - controller will send notifications only on HIGH ALARM event;
  - *Any Alarm* - will send notifications on both LOW ALARM and HIGH ALARM events;

  In order to use this parameter MQTT settings should be set properly and Admin/Guest accounts should be enabled in the way desired.

- **Send Email On** - this parameter allows sending emails on specified alarm. There are three identical to notifications choices:
  - *Never* - **smartDEN Opener** will not send any emails about analog input;
  - *Low Alarm* - controller will send emails only on LOW ALARM event;
  - *High Alarm* - controller will send emails only on HIGH ALARM event;
  - *Any Alarm* - will send emails on both LOW ALARM and HIGH ALARM events;
- **Log On** - this parameter allows writing to events log only on specified alarm. There are same choices as emails and notifications:
  - *Never* - **smartDEN Opener** will not write any logs about analog input;
  - *Low Alarm* - controller will write logs only on LOW ALARM event;
  - *High Alarm* - controller will write logs only on HIGH ALARM event;
  - *Any Alarm* - will write logs on both LOW ALARM and HIGH ALARM events;
- **Controls** - this parameter specifies which output is controlled by the analog input. There are four choices:
  - *Nothing* - this analog input will not control any output. If some of the previous settings are set it will be used for monitoring some process (for example if used humidity sensor it may send notification when it reaches selected alarm);
  - *Relay 1* - the analog input will control Relay 1;
  - *Relay 2* - the analog input will control Relay 2;
  - *Main* - the analog input will control Main Controlled Device;
- **Control Mode** (**Controls** is selected to be "Relay1" or "Relay2"):
  - *Normal* - in this mode the selected relay will turn on when analog input generates HIGH ALARM event and will turn off when LOW ALARM event is generated;
  - *Inversed* - in this mode the selected relay will turn on when analog input generates LOW ALARM event and will turn off when HIGH ALARM event is generated;
- **Control Mode** (**Controls** is selected to be "Main"):
  - *Open* - in this mode Main Controlled Device will start **OPENING** on HIGH ALARM event if not **OPENED**;
  - *Close* - in this mode Main Controlled Device will start **CLOSING** on LOW ALARM event if not **CLOSED**;
  - *Open/Close* - in this mode Main Controlled Device will start **CLOSING** on LOW ALARM event and will start **OPENING** on HIGH ALARM event;
  - *Close/Open* - in this mode Main Controlled Device will start **OPENING** on LOW ALARM event and will start **CLOSING** on HIGH ALARM event;
- **Save** - before leaving this tab or page click this button to changes take effect.

The next example situation shows how the analog input controls the Main Controlled Device.

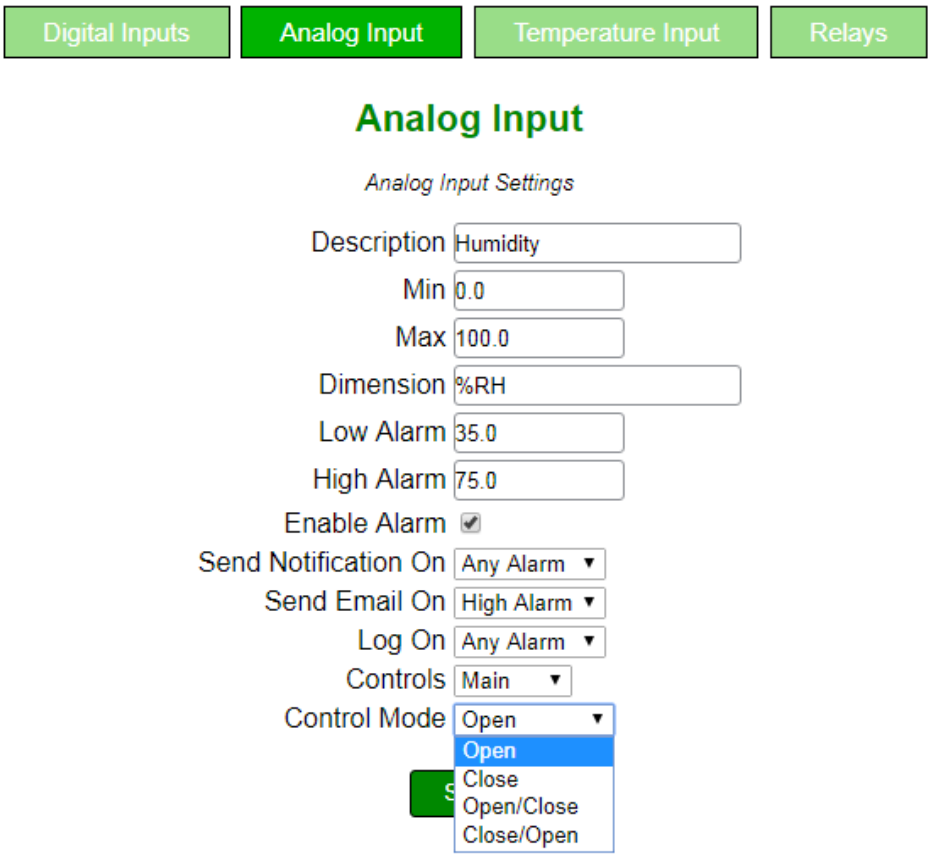

Figure 10.22. Analog Input controlling Main Controlled Device settings

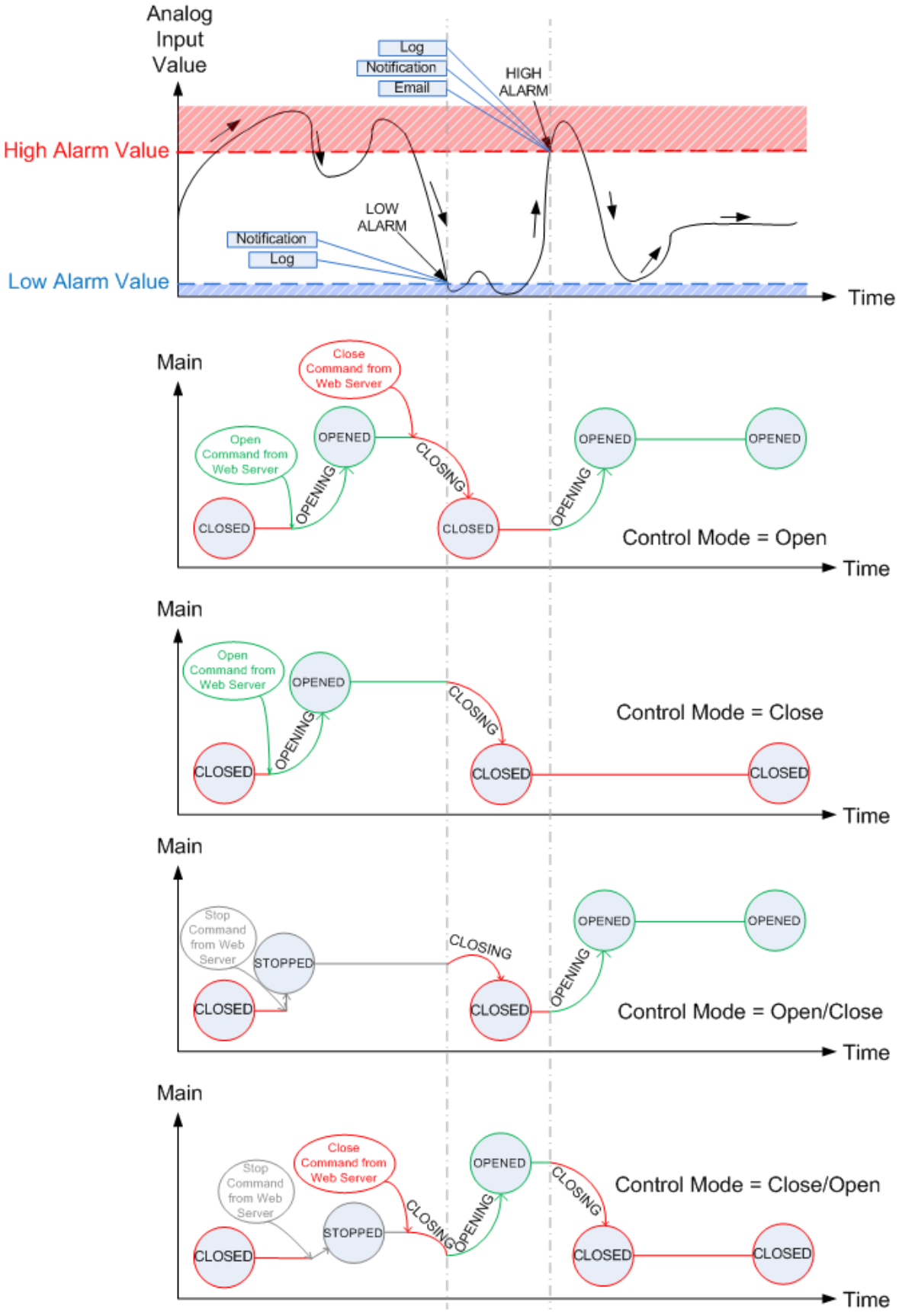

Figure 10.23. Analog Input controlling Main Controlled Device examples

On **Figure 10.23** is illustrated how Analog Input changes reflect Main Controlled Device with settings from **Figure 10.22**. MQTT notifications are sent and log messages are written on "Any Alarm" (LOW ALARM event and HIGH ALARM event respectively) but emails are sent only on HIGH ALARM event.

When **Control Mode** is set to "Open" the Main Controlled Device will start **OPENING** on every generated HIGH ALARM event. It is shown that Main is in **CLOSED** state first. Then an **OPEN** command is sent from the web server and Main Controlled Device starts **OPENING**. It reaches **OPENED** state and accepts another **CLOSE** command. Main starts **CLOSING** and LOW ALARM event is generated but this does not affect this **Control Mode** so Main Controlled Device continuous **CLOSING** and goes to **CLOSED** state. When it is in state **CLOSED,** the Analog Input generates HIGH ALARM event which starts **OPENING** the Main Controlled Device and it goes to **OPENED** state. No more alarms are generated after that.

In "Close" Control Mode the Main Controlled Device starts CLOSING on every LOW ALARM event generated. In our example when the Main Controlled Device is in **CLOSED** state, **OPEN** command is sent from web server. The Main Controlled Device starts **OPENING** and goes to **OPENED** state. Lately, LOW ALARM event is generated and Main starts **CLOSING** and goes to **CLOSED** state. The next HIGH ALARM event generated will not affect the state in this mode.

In "Open/Close" Control Mode the Main Controlled Device is OPENED on every HIGH ALARM event and **CLOSED** on every LOW ALARM event. As shown on **Figure 10.23**, Main Controlled Device is **CLOSED** and **STOP** command is received from web server, which makes Main Controlled Device to go in **STOPPED** state. When LOW ALARM event generated by the Analog Input, Main Controlled Device starts **CLOSING** and goes to **CLOSED** state. Then a HIGH ALARM event is generated and Main Controlled Device starts **OPENING** and goes to **OPENED** state.

In "Close/Open" Control Mode the Main Controlled Device is OPENED on every LOW ALARM event and **CLOSED** on every HIGH ALARM event. Main Controlled Device is **CLOSED** and **STOP** command is received from web server which makes Main Controlled Device to go in **STOPPED** state. Then a **CLOSE** command is received from the web server and Main starts **CLOSING**. At this moment, before Main Controlled Device's **Open/Close Time** expires, LOW ALARM event is generated, Main Controlled Device starts **OPENING** and goes to **OPENED** state. Lately HIGH ALARM event is generated and Main Controlled Device starts **CLOSING** which makes it **CLOSED**.

The next example situation shows how the analog input controls Relay1.

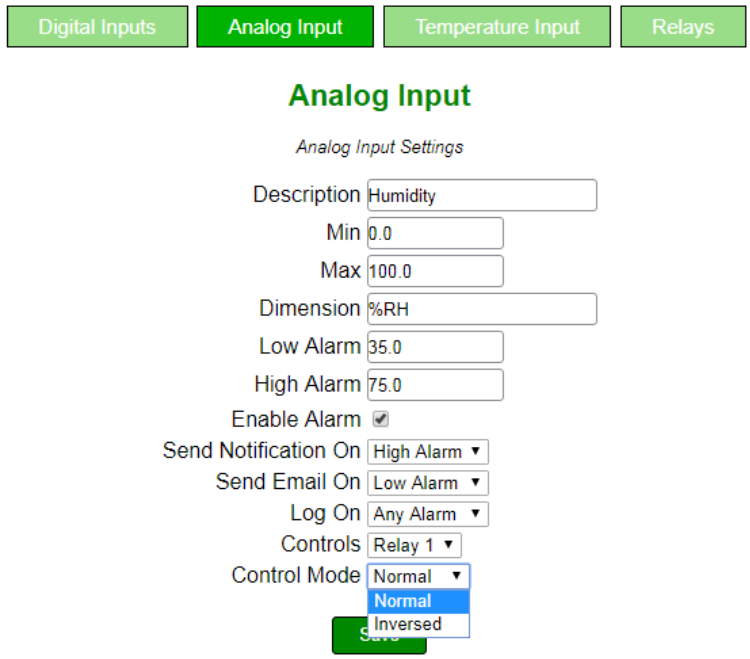

Figure 10.24. Analog Input controlling Relay 1

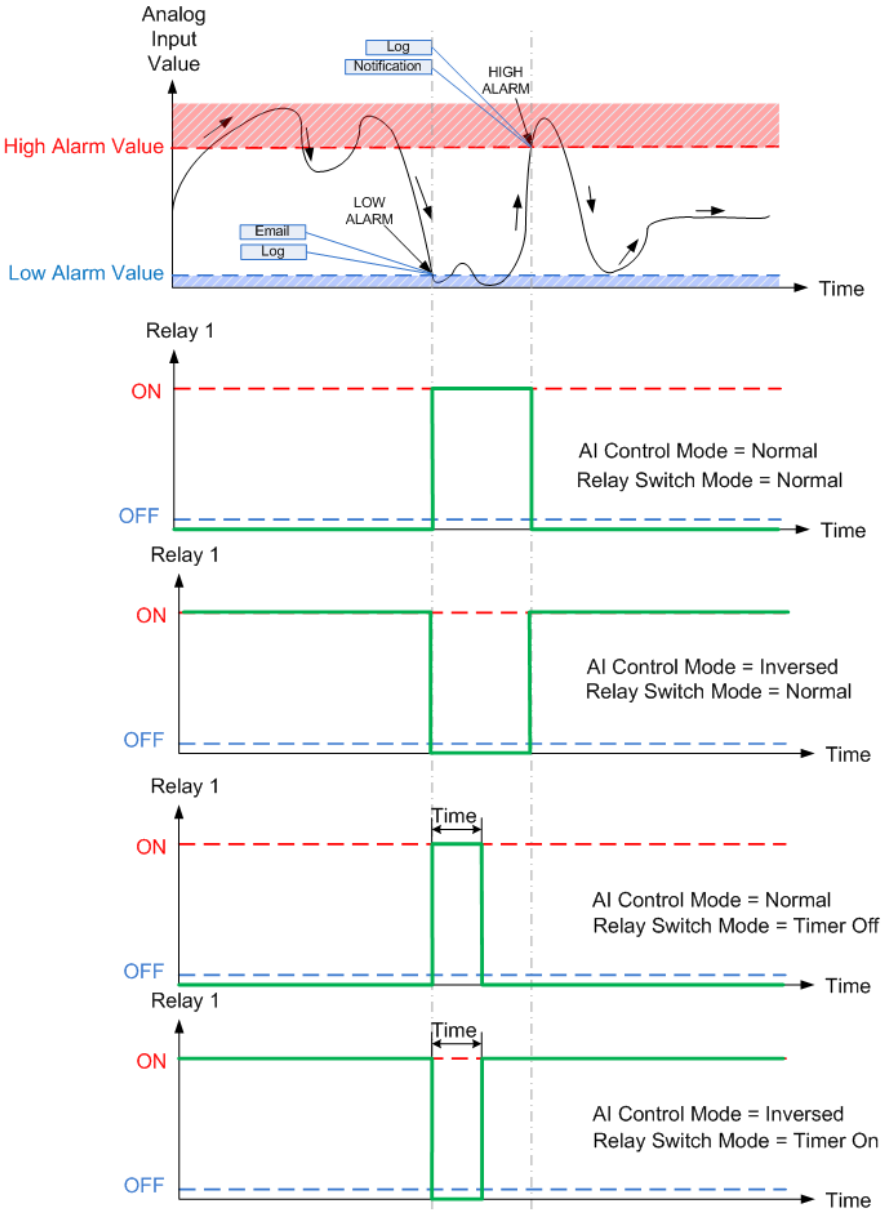

Figure 10.25. Analog Input controlling "Relay 1" examples

On the figure above, it is illustrated how Analog Input changes reflect to Relay 1 with settings from **Figure 10.24**. The log messages are written on any alarm event (LOW ALARM event and HIGH ALARM event respectively) but emails are sent only on HIGH ALARM event and MQTT notifications are sent on HIGH ALARM event as well. The first two examples are captured with Relay 1 configured to operate in "Normal" **Relay Switch Mode** (see **10.6.4 Relays**).

In "Normal" **Control Mode** Relay 1 (in our example) will be turned on when LOW ALARM event is generated and will be turned off when HIGH ALARM event is generated.

In "Inversed" **Control Mode** Relay 1 will be turned on when HIGH ALARM event is generated and will be turned off when LOW ALARM event is generated.

Last two graphics shows "Normal" and "Inversed" **Control Mode** of the analog input combined with Relay 1 operating in "Timer On" and "Timer Off" **Relay Switch Mode**. As seen in "Normal" **Control Mode** of the analog Input when **Relay Switch Mode** is "Timer Off", the relay turns on

when LOW ALARM event is generated and turns off after time specified in Relay 1 **Time** parameter.

10.6.3. Temperature Input

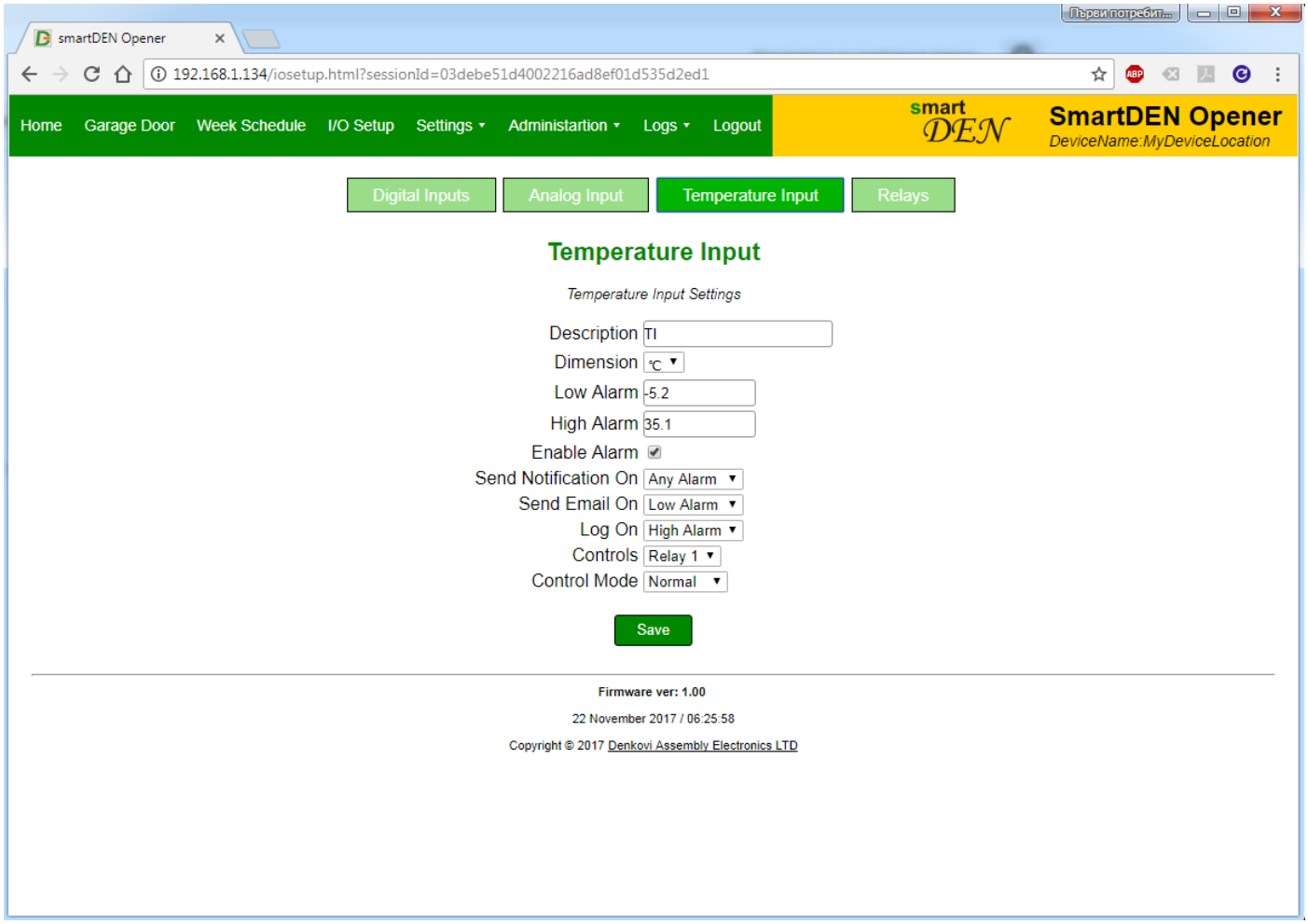

Figure 10.26. Temperature Input page

smartDEN Opener provides one temperature input for Dallas One Wire Temperature Sensor (for example DS18S20):

- **Description** - allows naming the temperature input. There are 10 allowed symbols reserved for description (see **Appendix 3**);
- **Dimension** - this is the dimension of measured temperature. There are two choices - Celsius (^{o}C) and Fahrenheit (^{o}F);
- **Low Alarm** - sets the value on which LOW ALARM event will be generated. LOW ALARM event is generated when the temperature has been higher than **High Alarm** parameter value and then falls below **Low Alarm** parameter value;
- **High Alarm** - sets the value on which HIGH ALARM event will be generated. HIGH ALARM event is generated when the temperature has been lower than **Low Alarm** parameter value and then exceeds **High Alarm** parameter value;
- **Enable Alarm** - if this option is checked alarms will be generated for the temperature input;
- **Send notification On** - this parameter allows sending notifications on specified alarm. There are four choices:
  - *Never* - **smartDEN Opener** will not send any notifications about temperature input;

  - *Low Alarm* - controller will send notifications only on LOW ALARM event generated by temperature input;
  - *High Alarm* - controller will send notifications only on HIGH ALARM event generated by temperature input;
  - *Any Alarm* - will send notifications on both LOW and HIGH ALARM events;
- **Send Email On** - this parameter allows sending emails on specified alarm. There are four identical to notifications choices:
  - *Never* - **smartDEN Opener** will not send any notifications about temperature input;
  - *Low Alarm* - controller will send emails only on LOW ALARM event generated by temperature input;
  - *High Alarm* - controller will send emails only on HIGH ALARM event generated by temperature input;
  - *Any Alarm* - will send emails on both LOW and HIGH ALARM events;
- **Log On** - this parameter allows writing to events log only on specified alarm. There are same choices as emails and notifications:
  - *Never* - **smartDEN Opener** will not write log messages about temperature input;
  - *Low Alarm* - controller will write log messages only on LOW ALARM event generated by temperature input;
  - *High Alarm* - controller will write log messages only on HIGH ALARM event generated by temperature input;
  - *Any Alarm* - will write log messages on both LOW and HIGH ALARM events;
- **Controls** - This parameter specifies which output is controlled by the temperature input. There are four choices:
  - *Nothing* - this analog input will not control any output. If some of the previous settings are set it will be used for monitoring some process;
  - *Relay 1* - the temperature input will control Relay 1;
  - *Relay 2* - the temperature input will control Relay 2;
  - *Main* - the temperature input will control Main Controlled Device;
- **Control Mode** (**Controls** is set to "Relay 1" or "Relay 2"):
  - *Normal* - in this mode the selected relay will turn on when temperature input generates HIGH ALARM event and will turn off when LOW ALARM event is generated;
  - *Inversed* - in this mode the selected relay will turn on when temperature input generates LOW ALARM event and will turn off when HIGH ALARM event is generated;
- **Control Mode** (**Controls** is set to "Main"):
  - *Open* - in this mode Main Controlled Device will start **OPENING** on HIGH ALARM event if not **OPENED**;
  - *Close* - in this mode Main Controlled Device will start **CLOSING** on LOW ALARM event if not **CLOSED**;
  - *Open/Close* - in this mode Main Controlled Device will start **CLOSING** on LOW ALARM event and will start **OPENING** on HIGH ALARM event;
  - *Close/Open* - in this mode Main Controlled Device will start **OPENING** on LOW ALARM event and will start **CLOSING** on HIGH ALARM event;
- **Save** - before leaving this tab or page click this button to changes take effect.

Next figures illustrate **Control Mode** parameter examples. The principle of control mode is the same as Analog Input. That's why the examples given below are same as Analog Input's.

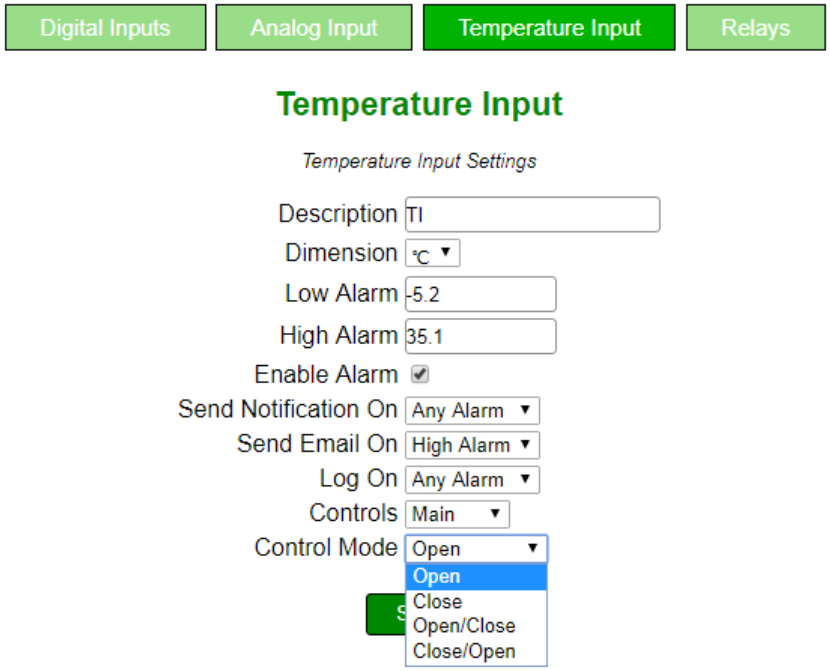

Figure 10.27. Temperature Input controlling Main Controlled Device settings

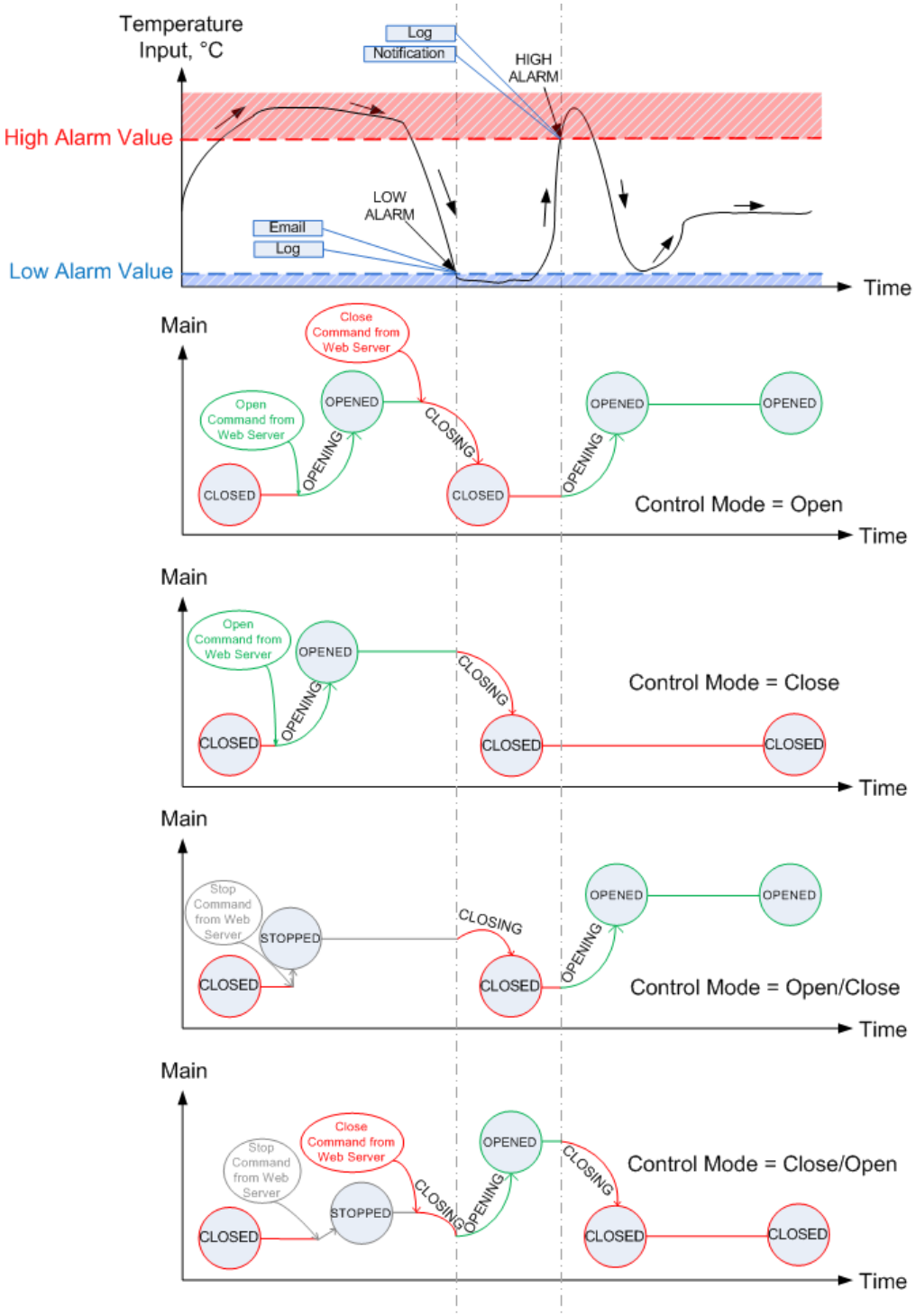

Figure 10.28. Temperature Input Controlling Main Examples

On **Figure 10.28** is illustrated how Temperature Input changes reflect to Main Controlled Device with settings from **Figure 10.27**. MQTT notifications are sent and log messages are written on any alarm (LOW ALARM event and HIGH ALARM event respectively) but emails are sent only on HIGH ALARM event.

When **Control Mode** is set to "Open" the Main Controlled Device will start **OPENING** on every generated HIGH ALARM event. On **Figure 10.28** is shown that Main Controlled Device is in **CLOSED** state first. Then an **OPEN** command is sent from the web server and Main Controlled Device starts **OPENING**. It reaches **OPENED** state and accepts another **CLOSE** command. Main

Controlled Device starts **CLOSING** and LOW ALARM event is generated but this does not affect this **Control Mode** so Main Controlled Device continuous **CLOSING** and goes to **CLOSED** state. When **CLOSED** the Temperature Input generates HIGH ALARM event, this starts **OPENING** the Main Controlled Device and it goes to **OPENED** state. No more alarms are generated.

In "Close" Control Mode the Main Controlled Device starts CLOSING on every LOW ALARM event generated. In our example on **Figure 10.28** the Main Controlled Device is in **CLOSED** state and **OPEN** command is sent from web server. The Main Controlled Device starts **OPENING** and goes to **OPENED** state. Lately LOW ALARM event is generated and Main starts **CLOSING** and goes to **CLOSED** state. The next HIGH ALARM event generated will not affect the state in this mode.

In "Open/Close" Control Mode the Main Controlled Device is OPENED on every HIGH ALARM event and **CLOSED** on every LOW ALARM event. The Main Controlled Device is **CLOSED** and **STOP** command is received from web server which makes Main Controlled Device to go in **STOPPED** state. On the LOW ALARM event generated by the Temperature Input, Main Controlled Device starts **CLOSING** and goes to **CLOSED** state. Then a HIGH ALARM event is generated and Main starts **OPENING** and goes to **OPENED** state.

In "Close/Open" Control Mode the Main Controlled Device is OPENED on every LOW ALARM event and **CLOSED** on every HIGH ALARM event. The Main Controlled Device is **CLOSED** and **STOP** command is received from web server which makes Main Controlled Device to go in **STOPPED** state. Then a **CLOSE** command is received from the web server and Main Controlled Device starts **CLOSING**. At this moment before Main Controlled Device's **Open/Close Time** expires**,** LOW ALARM event is generated, Main Controlled Device starts **OPENING** and goes to **OPENED** state. Lately HIGH ALARM event is generated and Main Controlled Device starts **CLOSING** which makes it in **CLOSED** state.

10.6.4. Relays

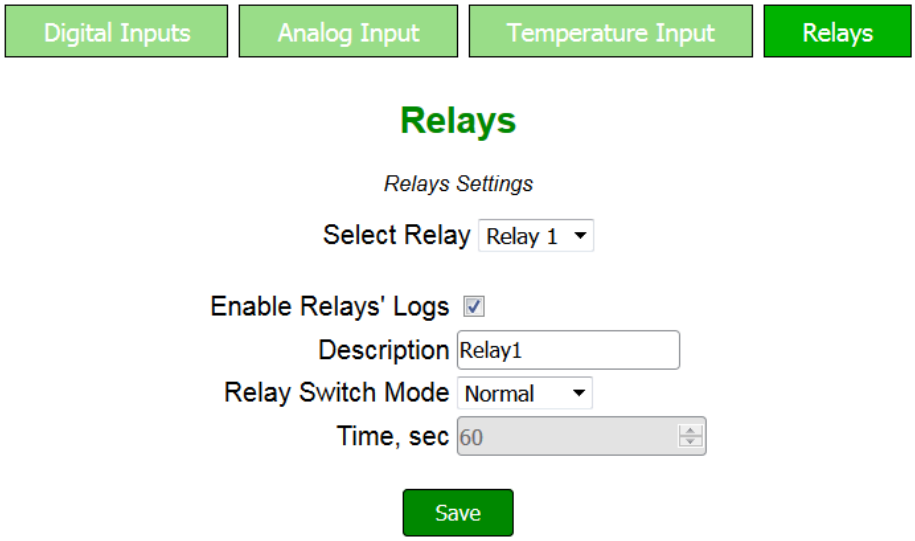

Figure 10.29. Relays Tab Overview

smartDEN Opener provides two relay outputs:

- **Enable Relays' Logs** - enables/disables writing to logs when there is relay state change.
- **Description** - allows naming the relay output. There are 10 allowed symbols reserved for description (see **Appendix 3**).
- **Relay Switch Mode** - this parameter sets the principle of relay switching. There are three possible choices:
  - *Normal* - in this switching mode relay will be turned on when **ON** command is send and will turned off when **OFF** command is send (no matter who/what sends the command);
  - *Timer On* - in this mode the relay could be turned on with **ON** command, but when turned off it will turn on again after defined interval by the **Time** parameter;
  - *Timer Off* - in this mode the relay could be turned off with **OFF** command, but when turned on it will turn off again after defined interval by the **Time** parameter;
- *Time, sec* - this is the time for **Timer On** and **Timer Off** switching modes. The time is set in seconds and has ±1 second tolerance. This value could be in range 0 ÷ 65535 seconds.

Below is given an example of **Relay Switch Mode** parameter. Note that commands could be received from **Digital Inputs**, **Analog Input**, **Temperature Input**, **web server**, **Mobile Application**, **communication protocols**, etc.

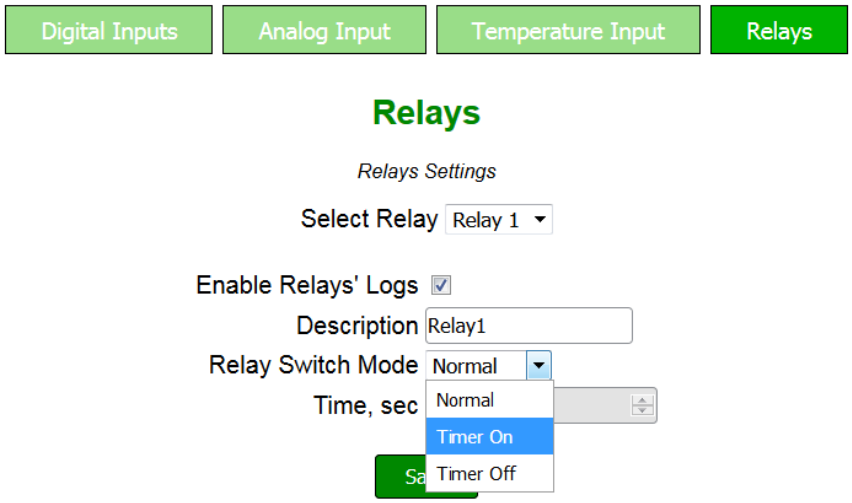

Figure 10.30. Relay Switch Mode settings

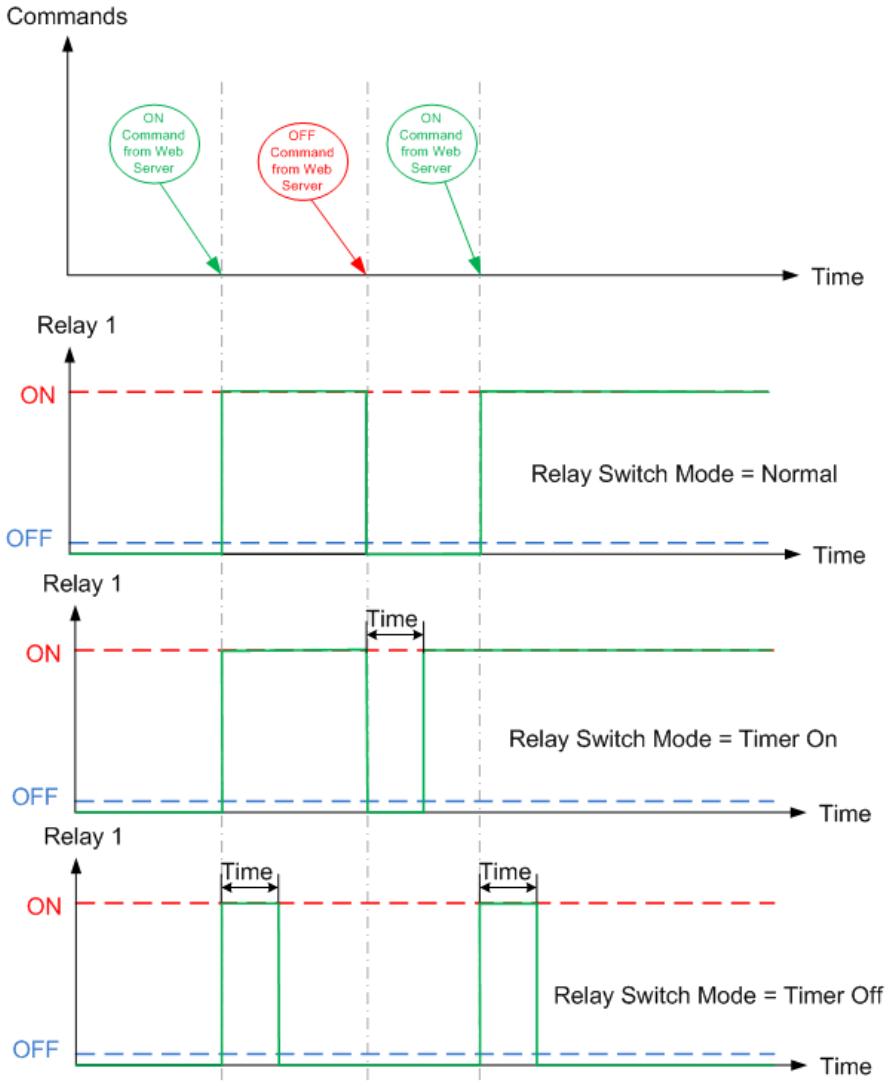

Figure 10.31. Relay Switch Mode examples

10.7. General Settings

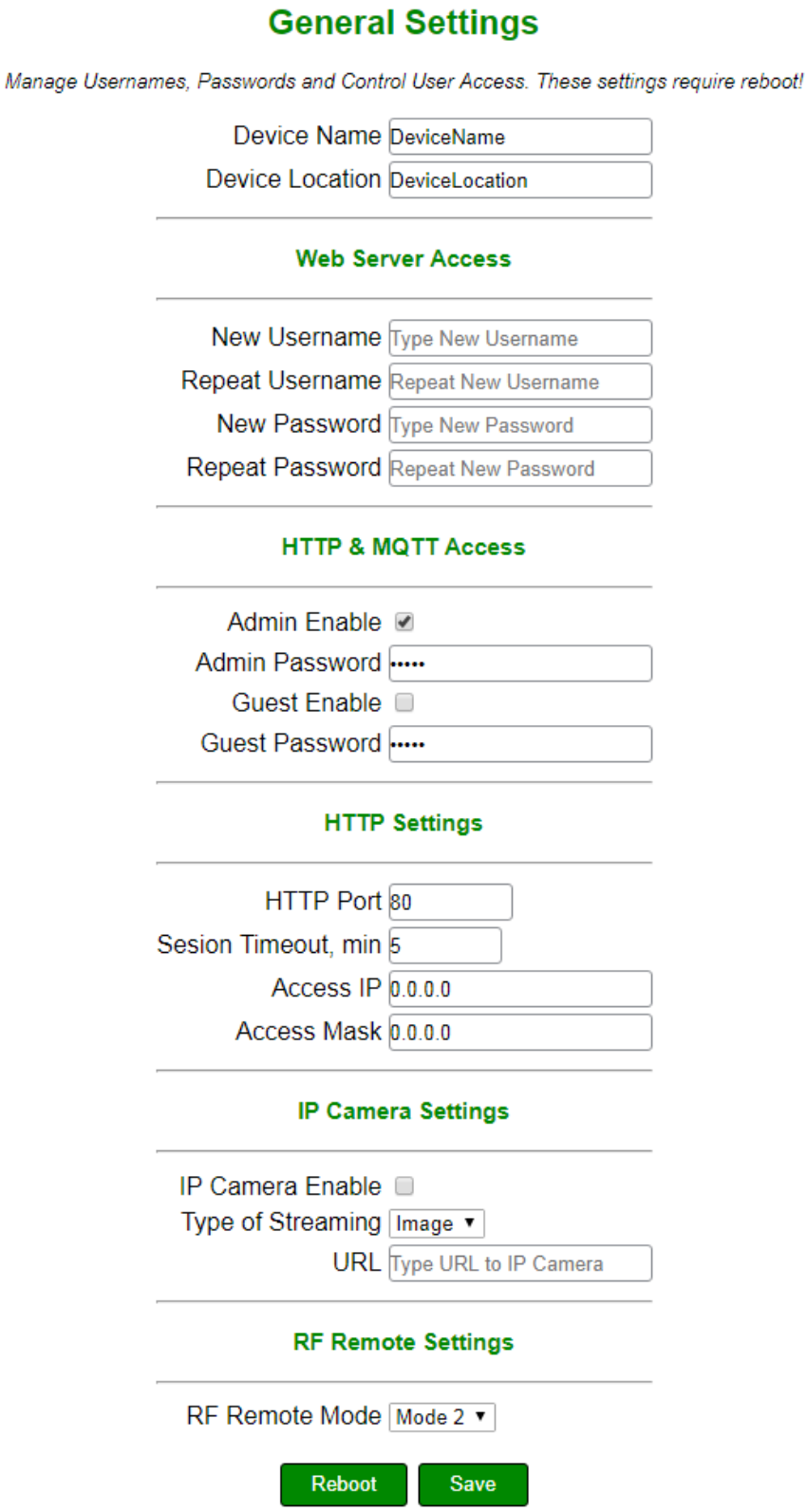

Figure 10.32. General Settings page

This page provides settings about **smartDEN Opener**'s device name and location, username and passwords, MQTT and HTTP access, HTTP settings, IP camera settings and RF remote settings. Parameters in this page are given below:

- **Device Name** - this parameter is used for naming **smartDEN Opener**. On each page in the web server in the upper right corner is shown **Device Name** parameter. When MQTT notifications and emails are desired each notification and email will contain this **Device Name**. There are 15 allowed symbols reserved for this parameter (see **Appendix 3**);
- **Device Location** - this parameter is used to tell **smartDEN Opener**'s location. Useful parameter when more than one device is used from one user (for example when several garage doors in different cities are owned by one user). When MQTT notifications and emails are desired each notification and email will consist of **Device Location**. There are 15 allowed symbols reserved for this parameter (see **Appendix 3**);
- **New Username** - this parameter is used for changing the username used to log in to web server. The new username should be minimum 5 symbols and maximum 15 symbols.
- **Repeat Username** - this parameter must be equal to **New Username** that was entered if username change is desired;
- **New Password** - this parameter is used for changing the password used to log in to web server. The new password should be minimum 5 symbols and maximum 15 symbols.
- **Repeat Password** - this parameter must be equal to **New Password** that was entered if password change is desired;

  💡 **Username** and **Password** for the web server could be changed only both together. If only username change is desired for example, you must enter the old password in **New Password** field.

- **Admin Enable** - this parameter allows **Admin** access for HTTP and MQTT resources. With this option enabled Admin could use the *DAE-aModules* Mobile Application in both XML and Cloud versions of **smartDEN Opener**. If Cloud version is used then notifications could be received by Admin. This parameter also allows using HTTP Protocol in both XML and JSON versions as well as MQTT Protocol *(see* **12. smartDEN Opener's MQTT Protocol**). **Admin** is the higher priority user. **Admin** can disable/enable **Guest** access, but **Guest** could not make such changes. **Admin** is also the only one user who could receive notifications. By default this parameter is Enabled;
- **Admin Password** - in order to use both MQTT and HTTP protocols as well as *DAE-aModules* Mobile Application this password must be used for identification. By default **Admin Password** is "admin". There are 15 allowed symbols reserved for this parameter *(see* **Appendix 3 Table 17.1**);
- **Guest Enable** - this parameter allows **Guest** access for HTTP and MQTT resources. With this option enabled Guest could use the *DAE-aModules* Mobile Application in both XML and Cloud versions of **smartDEN Opener**. This parameter also allows using HTTP Protocol in both XML and JSON versions as well as MQTT Protocol *(see* **12. smartDEN Opener's MQTT Protocol**). **Guest** has the same rights as **Admin** with the difference that can not disable **Admin**'s access. By default this parameter is Disabled;
- **Guest Password** - in order to use both MQTT and HTTP protocols as well as *DAE-aModules* Mobile Application this password must be used for identification. By default **Guest Password** is "guest". There are 15 allowed symbols reserved for this parameter (see **Appendix 3**);

  💡 **Admin User** has higher priority than **Guest User**.

- **HTTP Port** - this is the port on which web server and HTTP Protocol will respond. By default its value is 80. Note that changes on this parameter will take effect after reboot;
- **Session Timeout** - web server will need new login if there was no activity for more than this time. **Session Timeout** is in minutes and by default is 5 minutes;
- **Access IP** - this parameter allows restricting access to web server and HTTP Protocol. Note that setting **Access IP** is not enough to restrict access. **Access Mask** should be properly set to use this feature as appropriate;
  Access Mask - Used to restrict access to selected range of IP addresses. If not properly set connection to web server might be lost!

  💡 You can allow the HTTP/XML/JSON access to a range of IP addresses by setting an appropriate value for **Access Mask**. For example setting the **Access IP Address** to 192.168.1.0 and **Access Mask** to 255.255.255.0 allows the access from IP addresses in range from 192.168.1.0 to 192.168.1.255.

  💡 If you don't want to restrict the HTTP/XML access by IP address, set the **Access Mask** to 0.0.0.0.

  💡 Setting the **Access Mask** to 255.255.255.255 allows the HTTP/XML access only from the exactly specified **Access IP Address**.

  ⚠ Use **Access IP** and **Access Mask** with attention. If not properly configured, connection to web server might be lost. In such case use default settings button.

- **IP Camera Enable** - this parameter enables displaying IP camera on **Home Page**. If enabled animation will be hide and IP camera view will be available. By default this value is disabled;
- **Type of Streaming** - this parameter gives two choices:
  - *Image* - with this **Type of Streaming** you should enter a valid **URL** to image of IP camera. Most IP cameras provide such **URL** which contains picture in real time. The camera should be public or **URL** have to contain authorization information (might not work with every browser). Principle of working with this **Type of Streaming** is that picture is refreshed when previous picture is received (might be fast when good internet connection is used and slow when the internet connection is slow);
  - *Video* - this **Type of Streaming** allows streaming video from a valid **URL** of IP camera (it might be video from another website, too). The camera should be public or **URL** have to contain authorization information (might not work with every browser);
- **URL** - this parameter sets the **URL** to the IP camera. It must start with "http://". If non public camera are used this **URL** should contain authorization information (might not work with all browsers). If invalid **URL** is typed then in **Home Page** blank frame will be shown in place of the animation. There are 120 symbols reserved for this parameter;
- **RF Remote Mode** - this option is provided because of different RF remotes on the market. There are two modes - Mode 1 and Mode 2, specifying which button on RF remote opens and which closes the Main Controlled Device. Experiment with this option to find best mode for your RF remote. By default **RF Remote Mode** is Mode 1, which meets RF remotes shipped with **smartDEN Opener**.

10.8. Network page

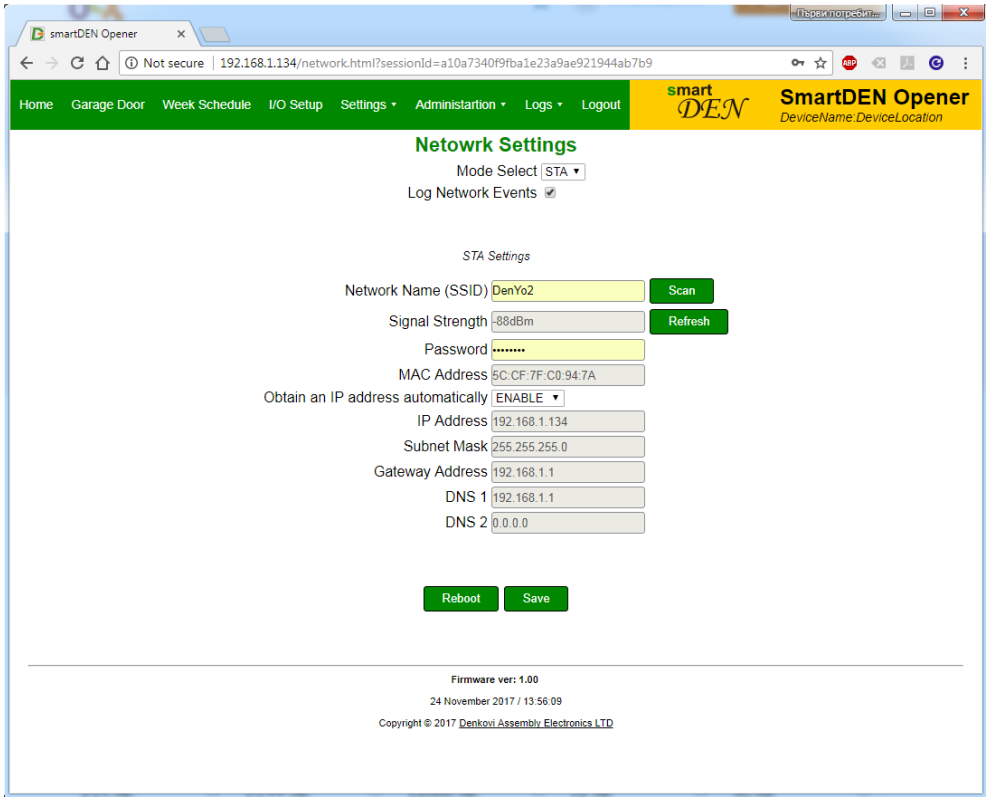

Figure 10.33. Network page

Network page provides all settings about network configuration of **smartDEN Opener**. **smartDEN Opener** could work in two network modes - Access Point (AP) and Station (STA). Default (factory) mode is Access Point (AP) which is just for initial settings.

When "AP" mode select parameter is selected then AP settings will be loaded. **Figure 10.34** illustrates AP network settings:

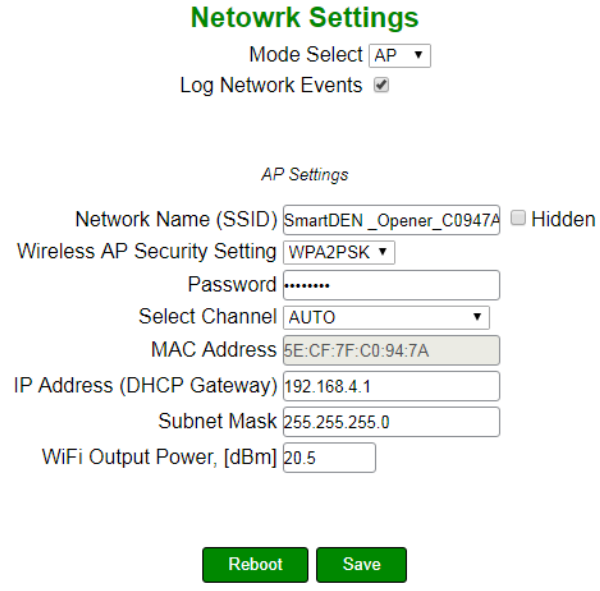

Figure 10.34. Access Point (AP) network mode

- **Mode Select** - this parameter is common for both modes - when AP is selected Access Point settings will be shown;
- **Log Network Events** - this parameter again is common for both network modes. It is used to write to system log messages about Network;
- **Network Name** (SSID) - this is the SSID of AP network. By default it is SmartDEN_Opener_XXXXXX where XXXXXX are the last six symbols from AP's **MAC Address**. There are 30 allowed symbols reserved for this parameter (see **Appendix 3**);
- **Hidden** - if checked, it will make SSID hidden;
- **Wireless AP Security Setting** - there are two security options for the AP network:
  - *DISABLE* - AP network will be opened and everyone could connect to it;
  - *WPA2PSK* - AP network will be secured with WPA2PSK encryption;
- **MAC Address** - this is Access Point's **MAC Address**;
- **IP Address** (**DHCP Gateway**) - this is the IP address of the Access Point. When a device connects to this AP, this address will be its gateway;
- **Subnet Mask** - this is AP's subnet mask;
- **Wi-Fi Output Power** - this is Access Point's Wi-Fi output power. Its value could be in range 0 ÷ 20.5 dBm. As higher value set longer distance will be covered by AP network. By default this value is set to 20.5dBm;
- **Save** - this button is used to save AP network configuration. When clicked, the above AP settings will be applied on next reboot;
- **Reboot** - reboot the device.

When "STA" **Mode Select** parameter is selected then STA Settings will be loaded. **smartDEN Opener** can connect to IEEE 802.11 b/g/n Wi-Fi networks. In this mode the device is connected to router most often. **Figure 10.35** illustrates STA network settings and detailed explanation of parameters is given below:

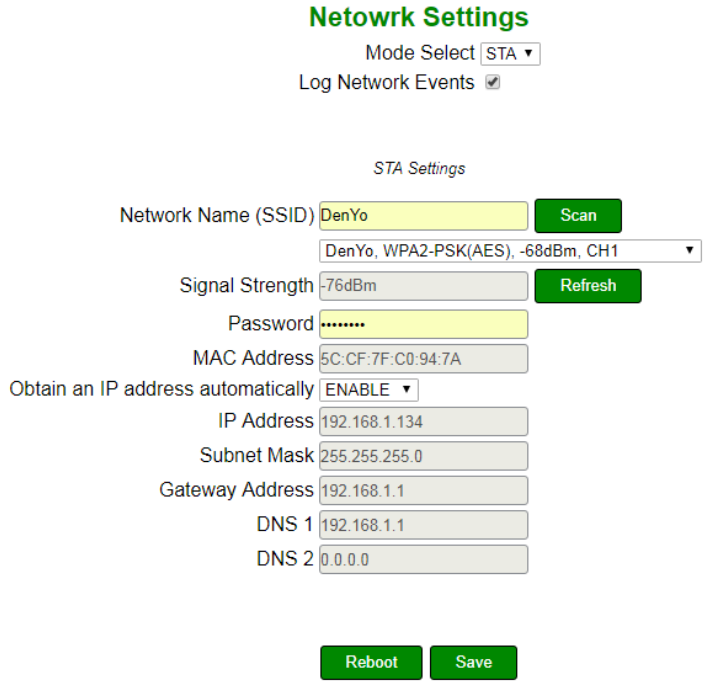

Figure 10.35. Station (STA) network mode

- **Mode Select** - this parameter is common for both modes - when **STA** is selected Station settings will be shown;

- **Log Network Events** - this parameter again is common for both network modes. It is used to write to system log messages about Network;
- **Network Name** (SSID) - this is the SSID of network that **smartDEN Opener** will try to connect to. There is "Scan" button provided to scan for available networks. When clicked **smartDEN Opener** will scan networks around and will report them in a dropdown select box. When click on some of the choices in the dropdown select box, **Network Name** will automatically equal to selected network. In scan report there are shown settings like SSID (name), type of encryption, signal strength and channel of the network. If a network is hidden it may not exist in scan report. There are 30 allowed symbols reserved for this parameter (see **Appendix 3**);

  💡 **smartDEN Opener** can connect to network with following network encryption types:
  - Open Network (No Encryption)
  - WEP
  - WPA Personal
  - WPA2 Personal
  - WPA/WPA2 Personal Mixed

- **Signal Strength** - this parameters visualize signal strength of the network which **smartDEN Opener** is currently connected. With the "**Refresh**" button this value will be refreshed. Useful parameter especially when moving the device;
- **MAC Address** - this is **smartDEN Opener's** Station **MAC Address**;
- **Obtain an IP Address Automatically** - this is DHCP option of the Station configuration. If set to "ENABLE" then **smartDEN Opener** will get address from router's DHCP server automatically. When "DISABLE" option is selected then the user should configure the IP addresses of **smartDEN Opener** manually.

  💡 If incorrect settings are set, **smartDEN Opener** may not connect to the desired network. Use this parameter with attention and double check before saving!

- **IP Address** - IP address of the device;
- **Subnet Mask** - subnet mask;
- **Gateway Address** - network gateway;
- **DNS1** - DNS1 address;
- **DNS2** - DNS2 address;

  💡 **IP Address, Subnet Mask, Gateway Address, DNS1** and **DNS2** should be in format x.x.x.x where x is number from 0 ÷ 255.

- **Save** - this button is used to save STA network configuration. When clicked, the above STA settings will be applied on next reboot;
- **Reboot** - reboot the device.

  ⚠ You have to reboot the device for these settings to apply.

10.9. Date/Time

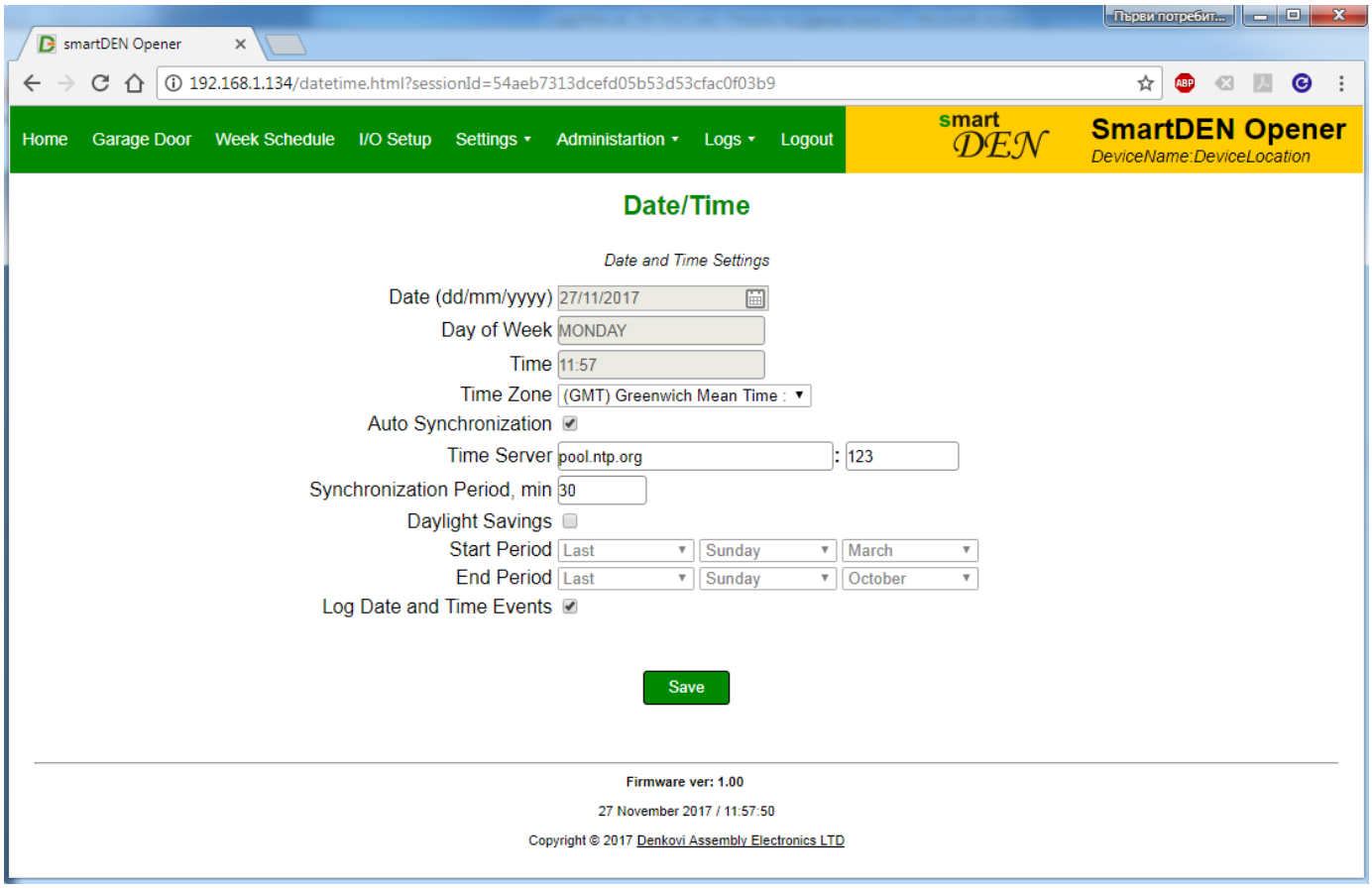

Figure 10.36. Date/Time page

"Date/Time" page consist of settings about the onboard RTC module and automatic synchronization with NTP time server or manual date and time settings:

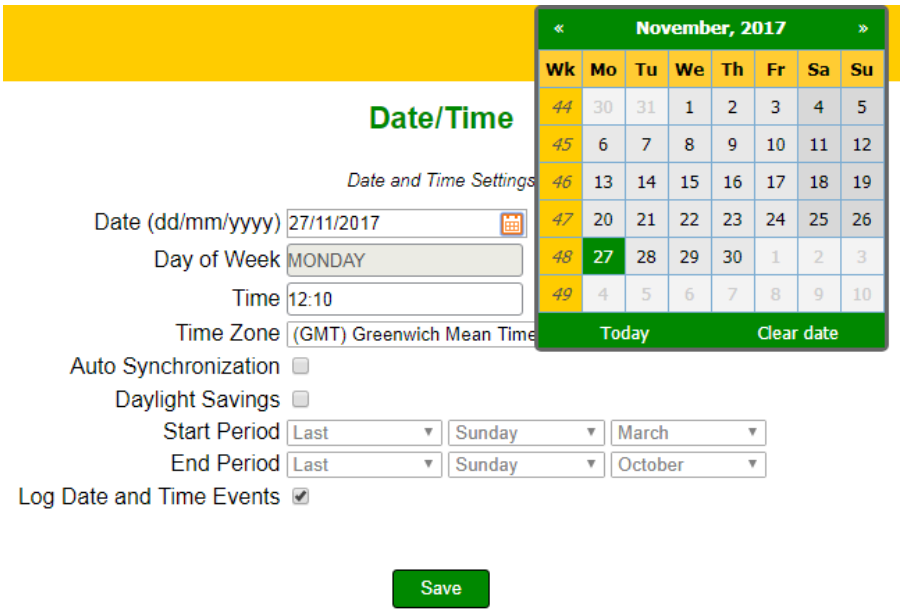

Figure 10.37. Date Selection with Pop-up Calendar

- **Date** - sets the date of the onboard RTC module. Format is (dd/mm/yyyy). Date can be selected when clicked on the text field when **Auto Synchronization** option is not checked. Calendar will pop-up and date selection can be made (**Figure 10.37**).
- **Day of Week** - shows current day of week stored in **smartDEN Opener's** onboard RTC module. This parameter is read only;
- **Time** - sets the time of the onboard RTC module. Format is (hh/mm). Time can be set when **Auto Synchronization** option is not checked;
- **Time Zone** - time zone selection drop-down list.
- **Auto Synchronization** - enables **Date** and **Time** auto synchronization from ntp server. When checked **Time Server** and **Synchronization Period** fields are shown. Time got from NTP server will be Greenwich Mean Time (GMT).

  💡 This parameter will work only in STA network mode.

- **Time Server** - this could be any public or private NTP server. On the right is located port number. There are 30 allowed symbols reserved for this parameter (see **Appendix 3**);
- **Synchronization Period** - this is the time in which **Date/Time** will be updated from NTP server. Its could be in range 10 ÷ 1440 minutes;
- **Daylight Savings** - daylight savings time can be defined from this option. In the period defined one hour will be added to current time;
- **Start Period** - this is the start period of **Daylight Savings Time**. On this day at 03:00 am, time shifts forward to 04:00 am;
- **End Period** - this is the end period of **Daylight Savings Time**. On this day at 04:00 am, time returns back to 03:00 am;
- **Log Date and Time Events** - used to write messages to system log file about NTP server successful / unsuccessful synchronization events;

10.10.Emails (SMTP)

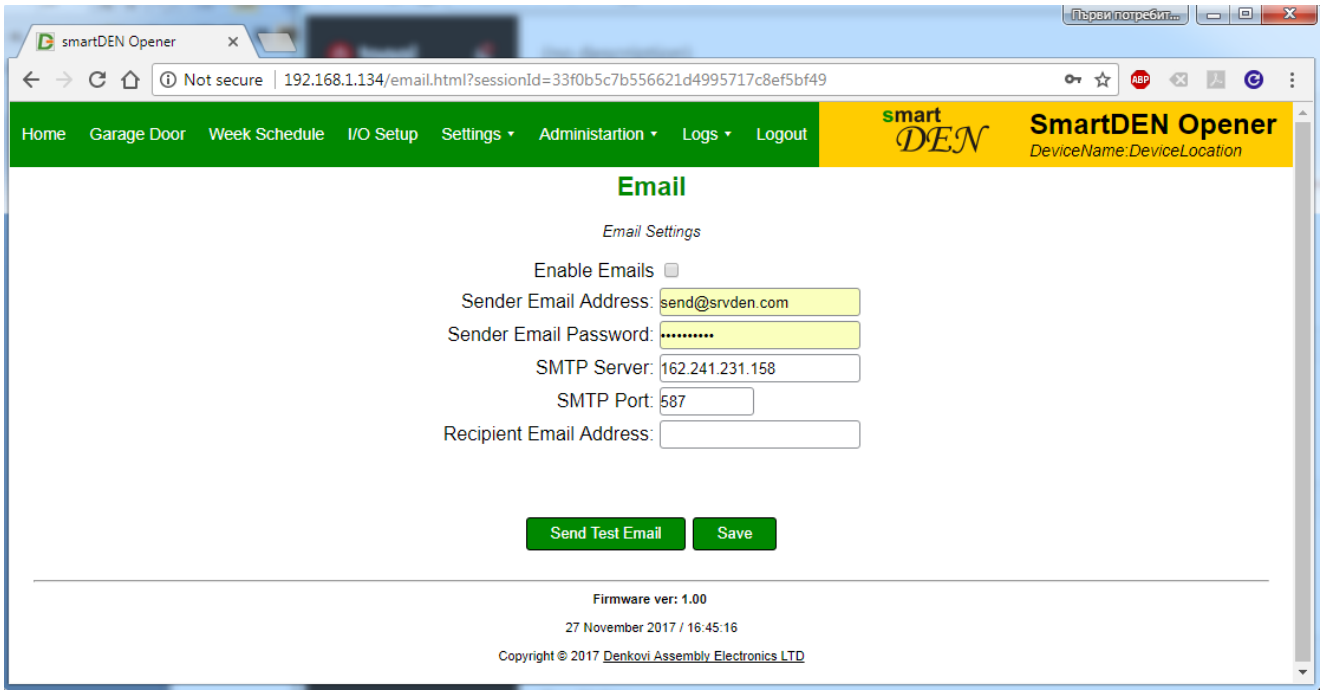

Figure 10.38. Email page

Emails page provides settings for configuring email sending via SMTP protocol. Emails are sent non encrypted over network as plain text (no SSL - via plain auth login). The parameters of the page are described below:

- **Enable Emails** - global option to enable **smartDEN Opener** to send emails;
- **Sender Email Address** - the email address from which **smartDEN Opener** will send emails. There are 25 allowed symbols reserved for this parameter (see **Appendix 3**);
- **Sender Email Password** - this is the password for the **Sender Email Address** used by **smartDEN Opener** to send emails. There are 15 allowed symbols reserved for this parameter (see **Appendix 3**);
- **SMTP Server** - this is sender's SMTP server for sending emails. There are 20 allowed symbols reserved for this parameter (see **Appendix 3**);
- **SMTP Port** - this is sender's **SMTP Port** for sending emails. **SMTP Port** could be a number from 1 ÷ 65 535;
- **Recipient Email Address** - this is recipient's email address to which **smartDEN Opener** will send emails. There are 25 allowed symbols reserved for this parameter (see **Appendix 3**);
- **Send Test Email** - used to check settings. When clicked on this button **smartDEN Opener** will send test email message;
- **Save** - used to save email configuration **of smartDEN Opener**;

⚠ **smartDEN Opener** uses SMTP plain authentification which means that email address and password is send as plain text over network and no SSL is used.

10.11.MQTT Page

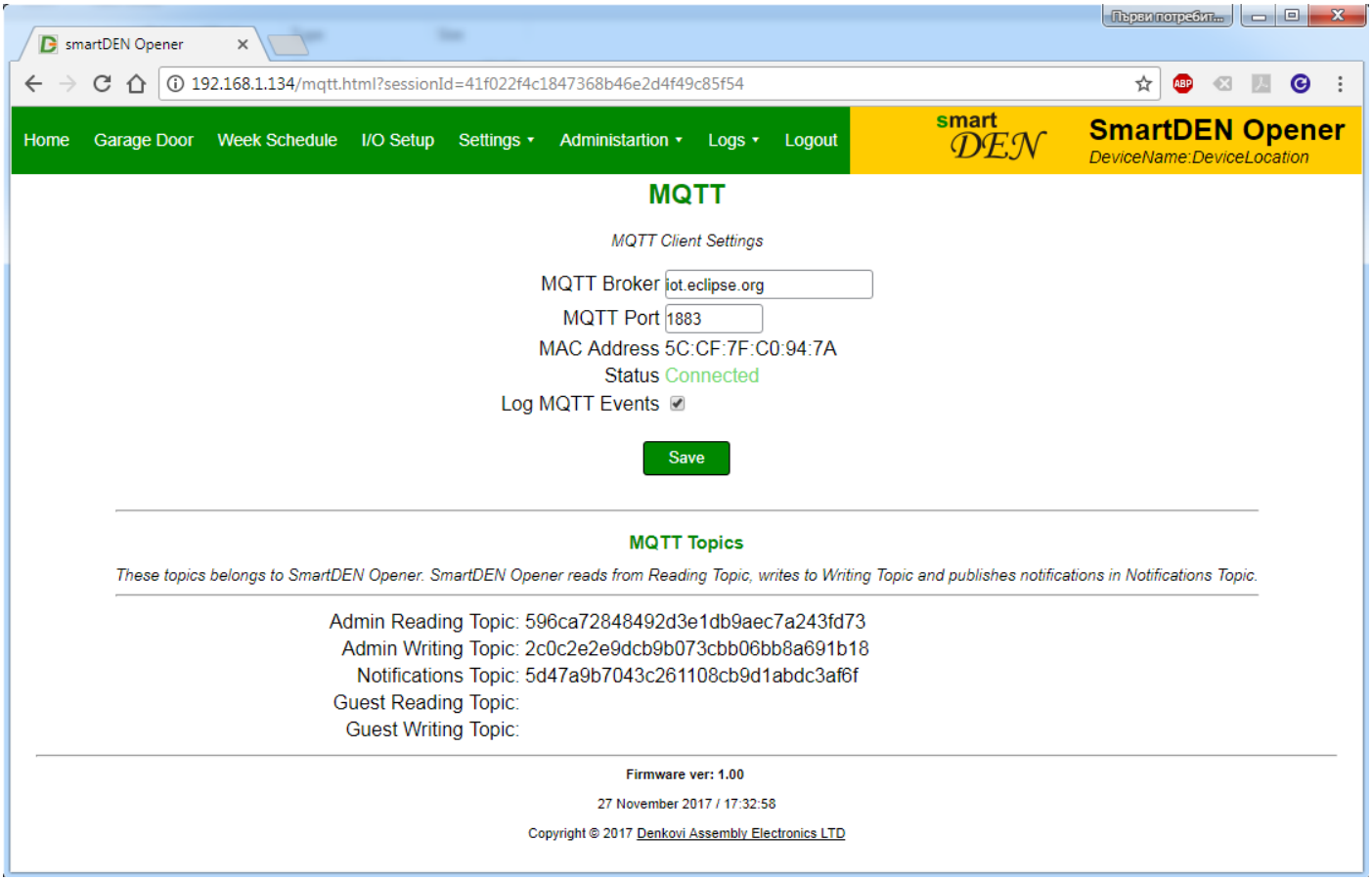

Figure 10.39. MQTT Page Overview

This page provides settings for configuring MQTT client. The MQTT communication requires broker and usually Internet connection. MQTT protocol is used in order to be sent push notifications. *DAE-aModules* is able to receive such notifications, but third parity apps also could be able to do that.

- **MQTT Broker** - this is the broker used for MQTT client. For example "iot.eclipse.org" or "test.mosquitto.org" works good. There are 30 allowed symbols reserved for this parameter (see **Appendix 3**);
- **MQTT Port** - this is **MQTT Broker's** port. It could be a number from 1 ÷ 65535;
- **MAC Address** - read only field. It will be necessary when setting up **smartDEN Opener** as Cloud Device in *DAE-aModules* application. **MAC Address** is used to form subscription topics;
- **Status** - shows the current status of **smartDEN Opener's** MQTT client;
- **Log MQTT Events** - this parameter is used to write messages to system log about MQTT client connections;
- **Save** - used to save configuration of **smartDEN Opener**'s MQTT client;

MQTT topics are created when **smartDEN Opener** is connected to the **MQTT Broker**. There are five topics depend on **Admin User** and **Guest User** access:

- **Admin Reading Topic** - this is the topic from which **smartDEN Opener** reads **Admin User**'s commands;

- **Admin Writing Topic** - this is the topic to which **smartDEN Opener** responds to **Admin User**'s commands;
- **notifications Topic** - notifications are pushed to this topic;
- **Guest Reading Topic** - this is the topic from which **smartDEN Opener** reads **Guest** user's commands;
- **Guest Writing Topic** - this is the topic to which **smartDEN Opener** responds to **Guest's** commands.

10.12.Firmware update

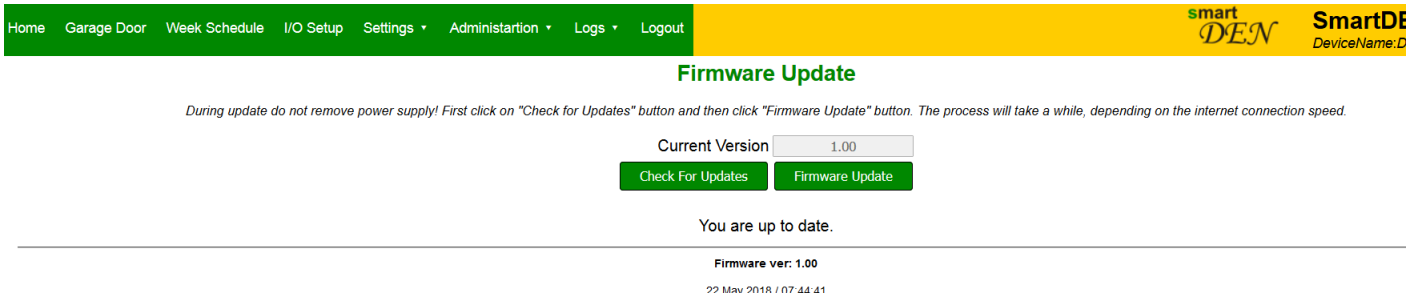

Figure 10.40. Firmware update page

This page provides settings for remote update over the air (OTA). Note that internet connection might be necessary. The parameters of the page are described below:

- **URL to Firmware Download Page** - this parameter contains the path to firmware files. It should contain everything after "http://". By default this value points to Denkovi Assembly Electronics' **smartDEN Opener** firmware update page. There are 50 allowed symbols reserved for this parameter (see **Appendix 3**);
- **Current Version** - read only field containing the current firmware version of **smartDEN Opener**;
- **Check For Updates** - a button which will check for new updates. If the **URL to Firmware Download Page** is correctly typed then a message will be shown and **Firmware Update** button will be visible;
- **Firmware Update** - a button which will be shown when correct path to firmware update page is typed;

During Firmware Update **STATUS** led is switched off. When firmware update procedure is finished **smartDEN Opener** will reboot. Note that **smartDEN Opener** will reboot no matter whether update is successful or not.

⚠ During firmware update process it is recommend **to not interrupt** the power supply and be sure the Internet connection is stable otherwise a malfunction of device can occur.

There are three possible situations, which are described below:

- Wrong URL to firmware update page message:

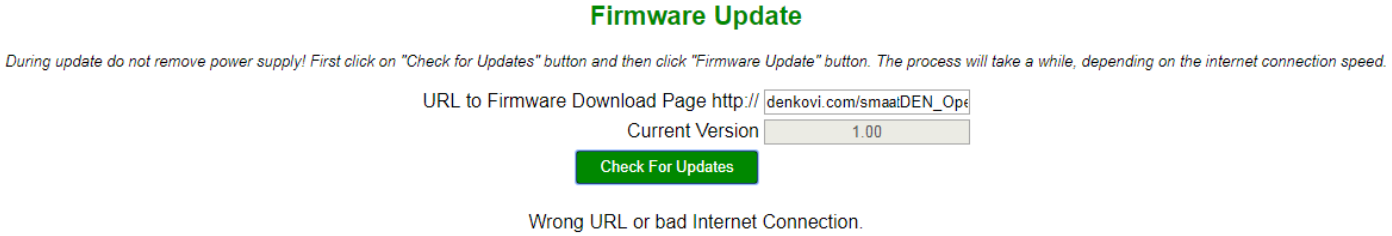

Figure 10.41. Wrong URL or bad Internet connection message

In this situation **Firmware Update** button is hidden. **Firmware Update** process could not be started.

- Up to date message:

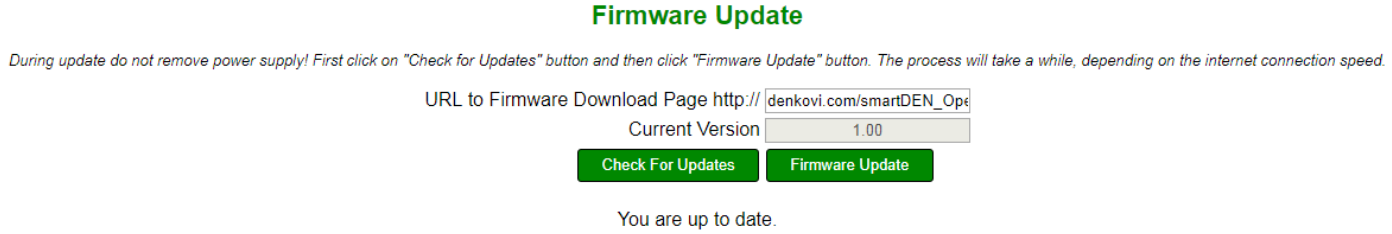

Figure 10.42. You are up to date message

In this situation **Firmware Update** button is shown and firmware update could be done but new version is not available.

- New version available message:

Figure 10.43. New version available message

In this situation **Firmware Update** button is shown and firmware update could be done to a newer version.

Please note it is quite possible after firmware update the module to be returned with the default settings!

10.13.Backup and restore configuration settings

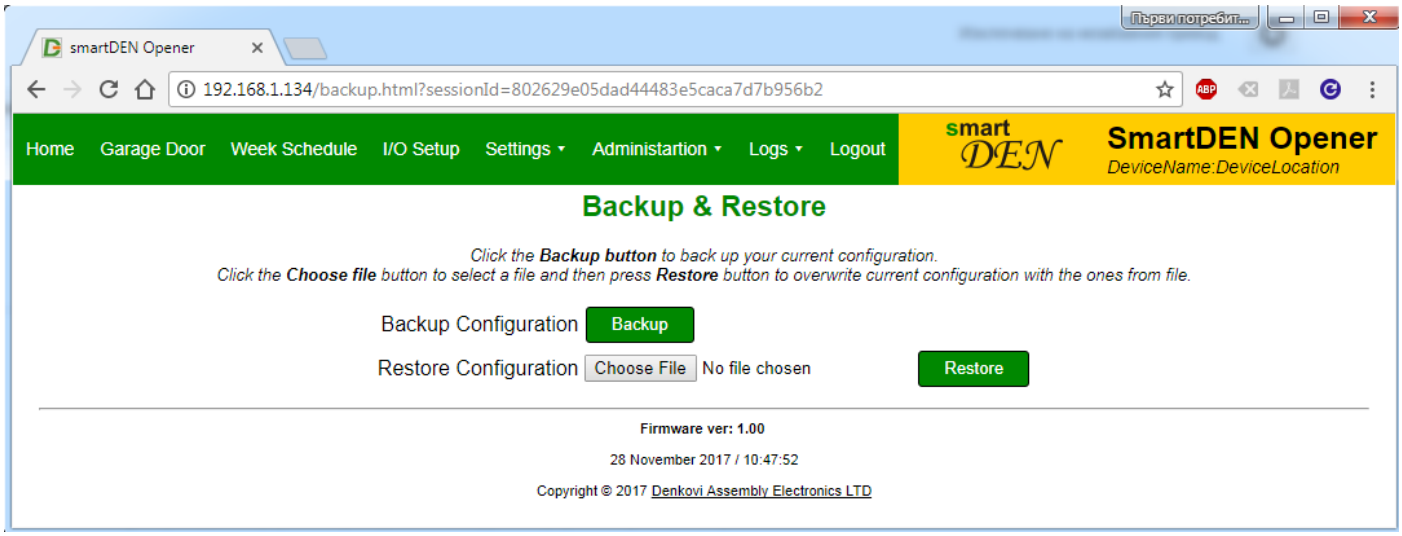

Figure 10.44. Backup Page Overview

This page provides backup and restore functions of **smartDEN Opener's** configuration. Parameters on this page are described below:

- **Backup Configuration** - provides button which when clicked will open prompt to save a **smartDEN Opener** configuration file. **smartDEN Opener's** configuration file is named "smartDENconfig.cfg". This file could be used later to restore configuration.
- **Restore Configuration** - this parameter gives a possibility to restore previous configuration of **smartDEN Opener**. When clicked "**Choose File**" a dialog will be opened and configuration file should be selected. After file selection using "**Restore**" button will restore **smartDEN Opener** configuration from selected file.

It is recommended to make **Restore Configuration** from personal computer or laptop. This feature works best with Mozilla Firefox and Google Chrome browsers.

10.14.Software factory defaults

When clicked this button will show a dialog box for confirmation. If confirmed the default settings will be loaded. See **7. Default Settings**.

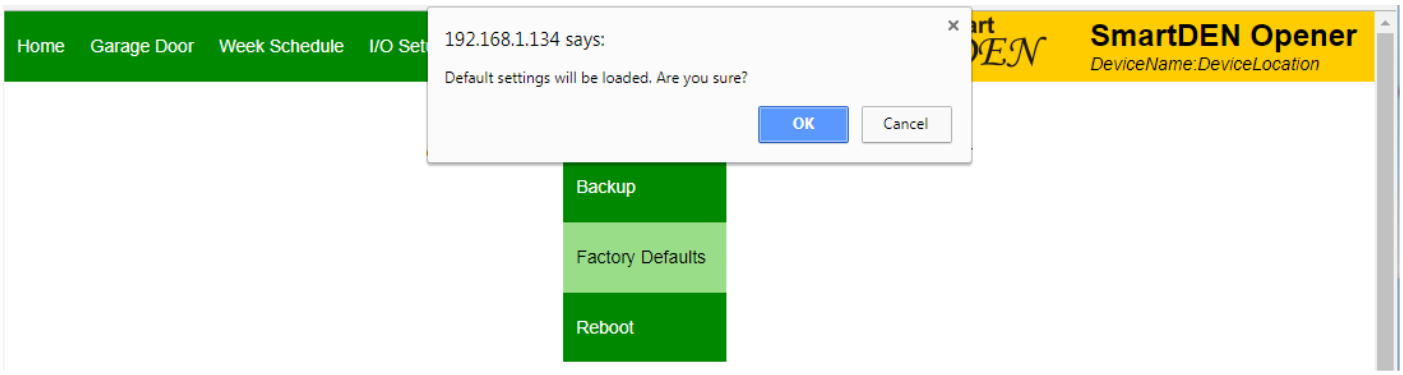

Figure 10.45. Factory defaults button

10.15.Software reboot

When clicked on this button a dialog box will be shown for confirmation. If confirmed **smartDEN Opener** will reboot.

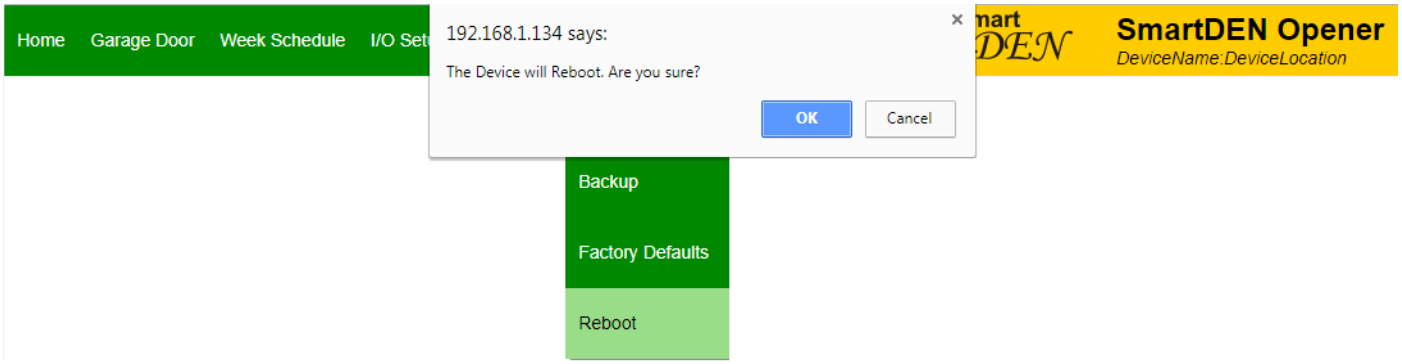

Figure 10.46. Reboot Button

10.16.System log

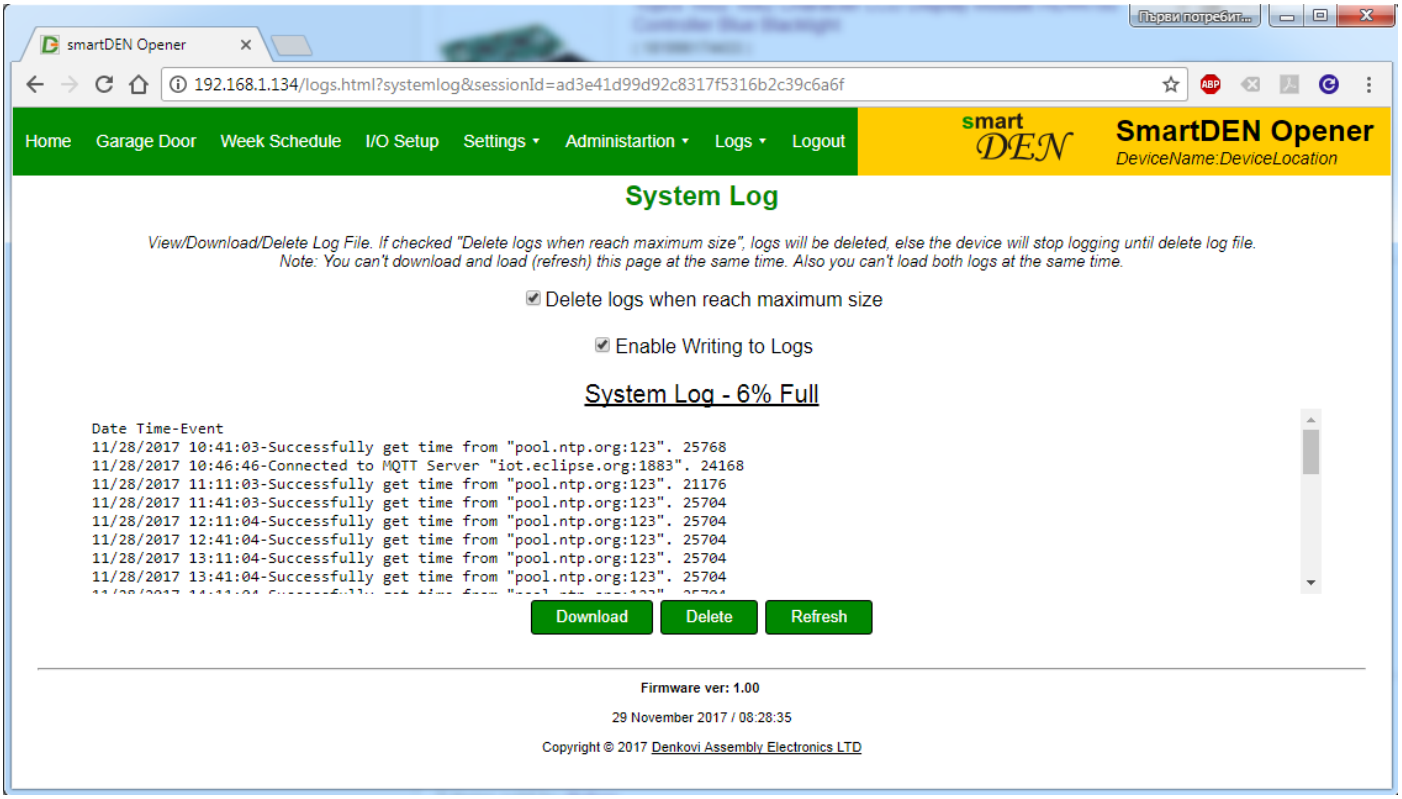

Figure 10.47. System log

"**System Log**" page visualizes log messages written in system log file with size approximately 30KB:

- **Delete logs when reach maximum size** - this checkbox is used to enable/disable deleting logs;

- **Enable Writing to Logs** - this is global checkbox for writing to logs. When checked log messages will be written to logs else log messages will be not written no matter what is set to be logged;
- **Download** - a button which on click will open a dialog for saving "systemlog.txt" file;
- **Delete** - button which will delete **System Log** file from **smartDEN Opener**;
- **Refresh** - button which will reload page.

Next to "**System Log**" caption is written the current size of the log. On **Figure 10.47** system log file is 6% full. Clicking on this caption will open system log file in new tab.

Format of system log file is: "Date Time-Event. Heap". There are several possible system log events indicated with the following message type:

- "Boot up" message - it is written every time device boots up;
- "Network status" messages - they are written on any network change, connection or disconnection;
- "MQTT status" messages - written on change in MQTT settings, connection and disconnection from MQTT Broker;
- "Date and time" messages - written on successful/ unsuccessful connection to NTP server or getting date and time from onboard RTC;

"**Delete logs when reach maximum size**" checkbox is reflecting both system and events logs.

"**Enable Writing to Logs** " checkbox is reflecting both system log and events log.

During loading or downloading "**System Log**" page other pages may not respond because of downloading file. It is recommended to wait until whole log file is downloaded and then switch to other page.

10.17.Events log

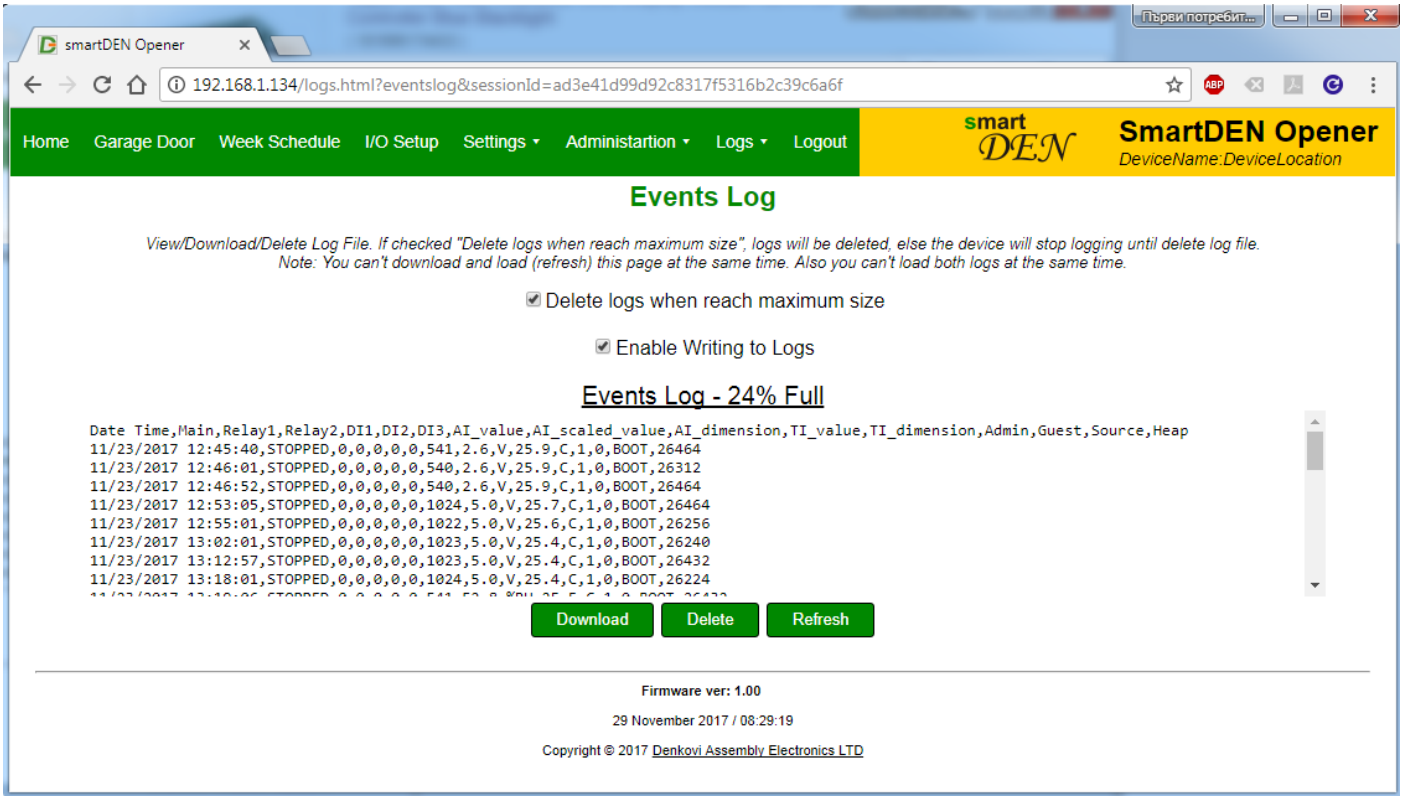

Figure 10.48. Events log

"**Events Log**" page visualizes log messages written in events log file. Size of events log file is about 30KB and it is only for messages when an I/O event occur. Every log message consist of all inputs and outputs state. Events log messages are written in .csv (comma separated value) format:

- **Delete logs when reach maximum size** - this checkbox is used to enable/disable deleting logs;
- **Enable Writing to Logs** - this is global checkbox for writing to logs. When checked log messages will be written to logs else log messages will be not written no matter what is set to be logged;
- **Download** - a button which on click will open a dialog for saving "eventslog.txt" file;
- **Delete** - button which will delete events log file from **smartDEN Opener**;
- **Refresh** - button which will reload page.

Next to "**Events Log"** caption it is written the current size of the log. On the figure above events log file is 24% full. Clicking on this caption will open the events log file in new tab.

Format of events log file is:

"Date Time, Main, Relay1, Relay2, DI1, DI2, DI3, AI_value, AI_scaled_value,AI_dimension,TI_value,TI_dimension,Admin,Guest,Source,Heap".

Example row of events log:

11/23/2017 12:45:40,STOPPED,0,0,0,0,0,541,2.6,V,25.9,C,1,0,BOOT,26464

This means:

Event date/time: 23 November 2017 at 12:45:40h
Main Controlled Device is **STOPPED**
Relay1 is turned off
Relay2 is turned off
Digital Input 1 is off
Digital Input 2 is off
Digital Input 3 is off
Analog Input raw value is 541
Analog Input scaled value is 2.6
Analog Input dimension is V
Temperature Input value is 25.9
Temperature Input dimension is Celsius
Admin User access is enabled
Guest User access is disabled
Reason (source) for writing this line of log is that **smartDEN Opener** booted up
System Heap is 26464 bytes

- "**Delete logs when reach maximum size**" checkbox is reflecting both system and events logs.
- "**Enable Writing to Logs** " checkbox is reflecting both system log and events log.
- During loading or downloading "**Events Log**" page other pages may not respond because of the file downloading. It is recommended to wait until whole log file is downloaded and then switch to other page.

10.18.Logout

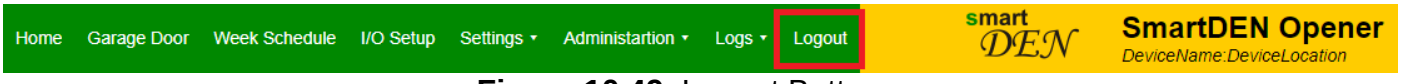

Figure 10.49. Logout Button

"Logout" button is used to end current session. After logging off, new login will be required.

11. HTTP server

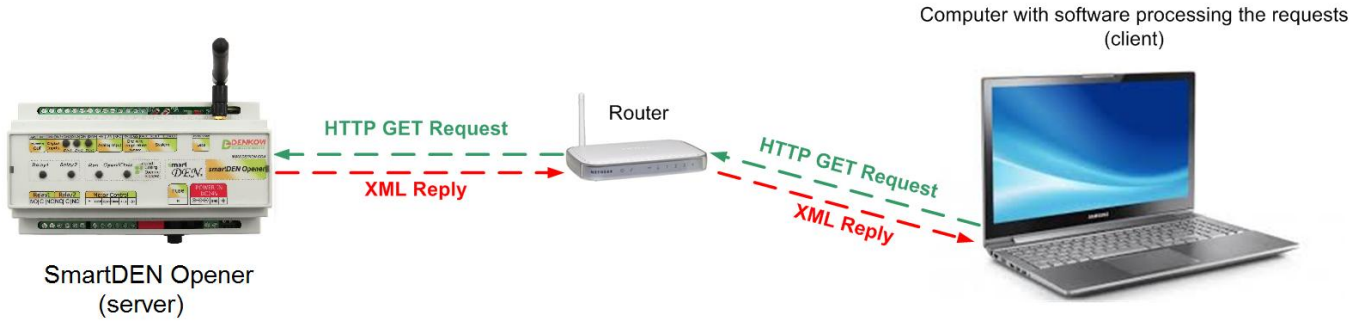

Figure 11.1. smartDEN Opener works as HTTP server

This operation mode allows custom applications to obtain I/O values and other information from **smartDEN Opener** without using a Web-browser. The custom application acts as a HTTP client, sending HTTP GET requests to **smartDEN Opener**. There are two formats of response provided by **smartDEN Opener** - XML and JSON. To receive the current state of the **smartDEN Opener,** the application requests the page *current_state.xml or current_state.json*, for example:

http://192.168.1.134/current_state.xml&pw=<password>

http://192.168.1.134/current_state.json&pw=<password>

11.1. Authentification (non-encrypted password)

The password is passed as non-encrypted parameter with the request. For example:

http://192.168.1.134/current_state.xml?pw=admin

http://192.168.1.134/current_state.json?pw=admin

- On each HTTP request the password must be sent for authentication. It can be used either **Admin User**'s password either **Guest User**'s password.
- Please note that the both users can be disabled and enabled any time which may cause enable / disable this type of requests.
- **Session Timeout** parameter does not reflect this request.

11.2. Retrieving smartDEN Opener current state

smartDEN Opener provides two type of response to obtain current state depend on request - XML or JSON.

11.2.1. XML response

To get XML response the request should look like this for example:

http://192.168.1.134/current_state.xml?pw=admin

Example response from **smartDEN Opener** is given below:

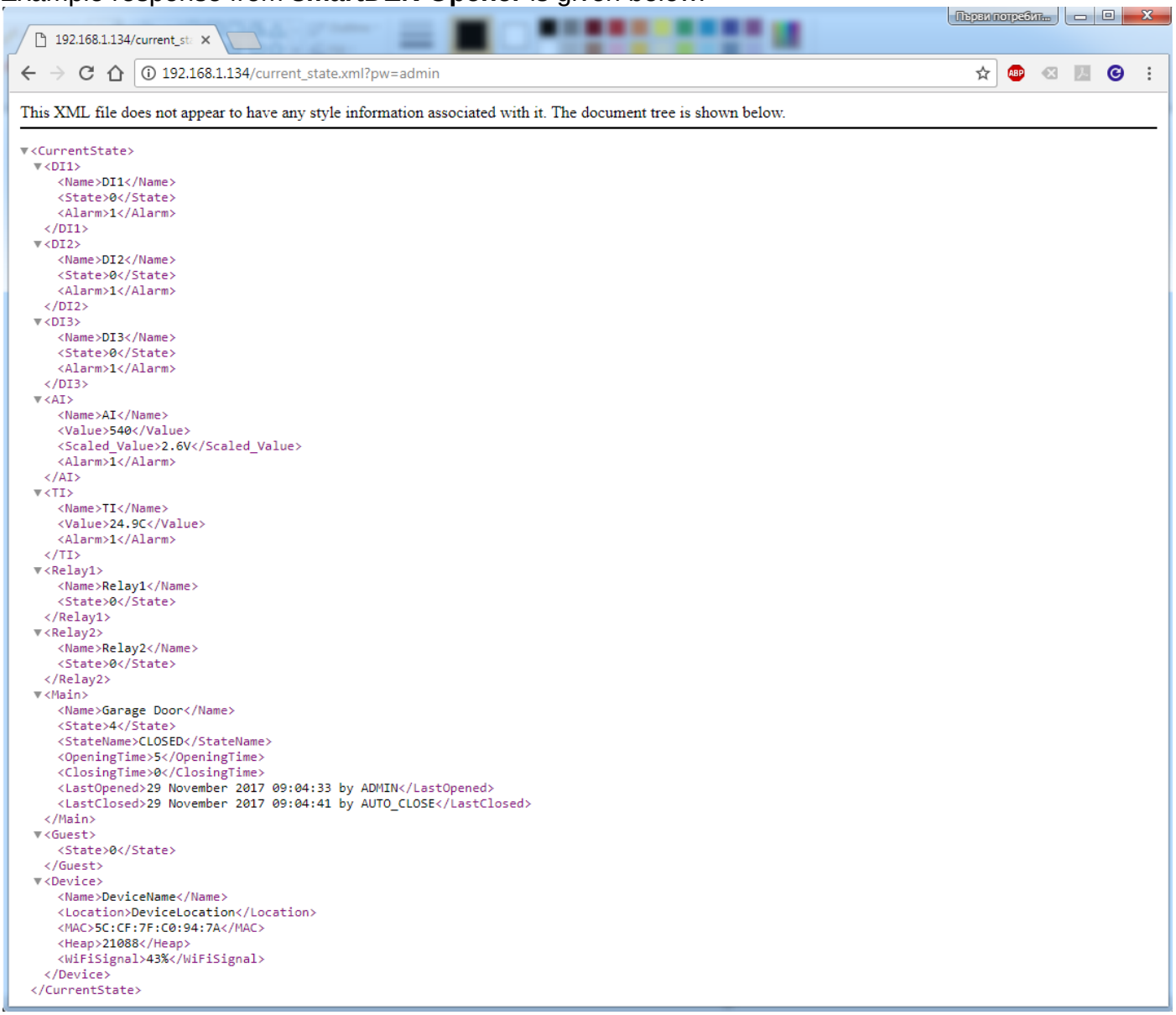

Figure 11.2. XML response from **smartDEN Opener**

11.2.2. JSON response

To get JSON response the request should look like this for example:

http://192.168.1.134/current_state.json?pw=admin

Example response from **smartDEN Opener** is given below:

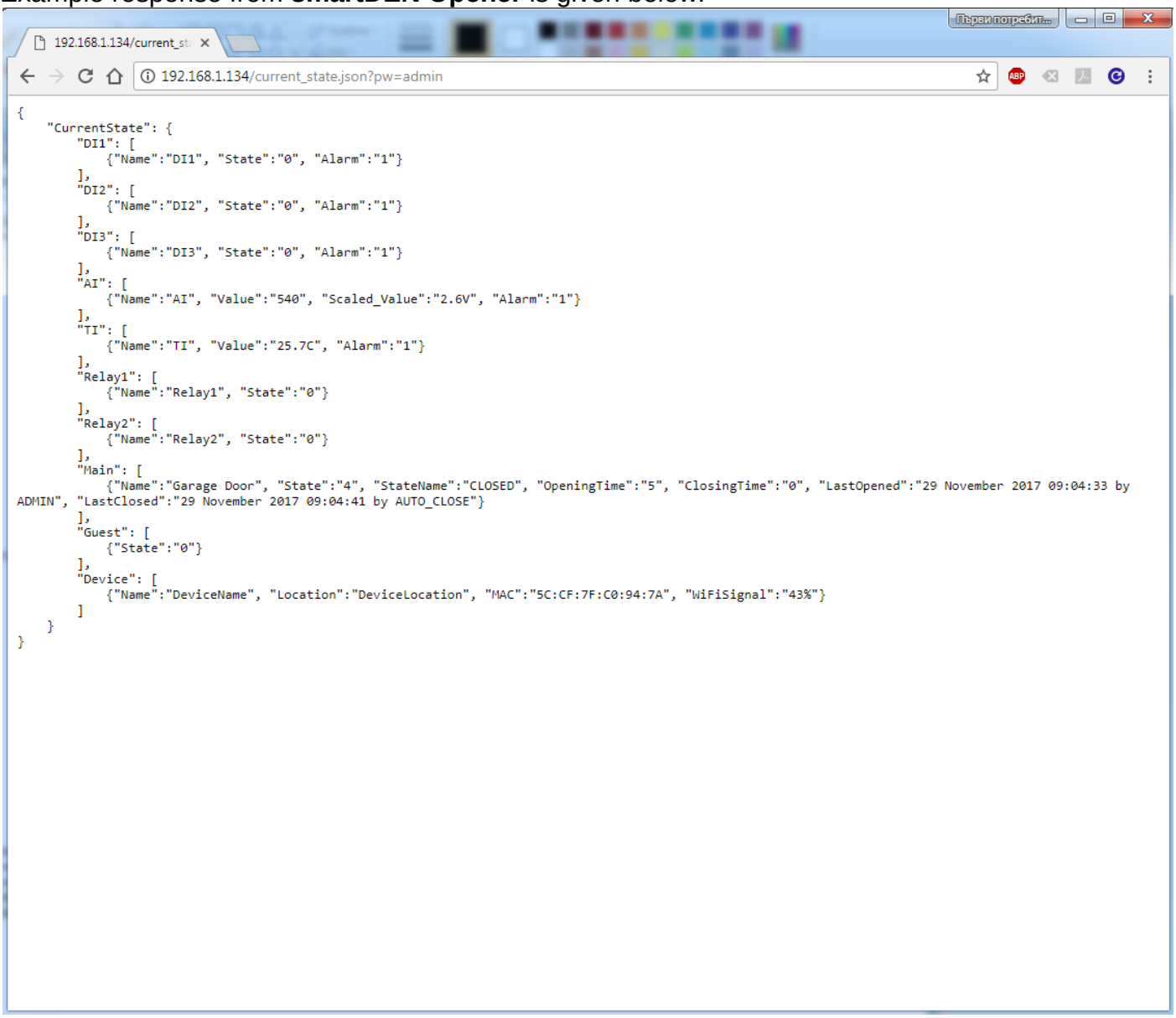

Figure 11.3. JSON response from **smartDEN Opener**

11.3. Multiple HTTP XML/JSON access

When HTTP XML and JSON requests are desired, there is no limitation of connections which can obtain the current state. **Session Timeout** parameter is not reflecting this type of access.

11.4. HTTP XML/JSON commands

smartDEN Opener I/O can be accessed via HTTP requests. Request parameters given below could be used both with XML and JSON format. Controlling inputs and outputs might be combined in one request, for example:

http://192.168.1.134/current_state.xml?pw=admin&R1=1&R2NAME=Heater

http://192.168.1.134/current_state.json?pw=admin&R1=1&R2NAME=Heater

11.4.1. Single relays control

Example requests:

http://192.168.1.134/current_state.xml?pw=admin&R1=0&R2=1

http://192.168.1.134/current_state.json?pw=admin&R1=1&R2=0

Possible values for R1 and R2 are 0 (turn off) and 1 (turn on).

11.4.2. Control all the relays via single command

Example requests:

http://192.168.1.134/current_state.xml?pw=admin&R=1

http://192.168.1.134/current_state.json?pw=admin&R=3

Possible values for R are:

Table 11.1. Relays control table

R	Relay 1	Relay 2
R=0	OFF	OFF
R=1	ON	OFF
R=2	OFF	ON
R=3	ON	ON

11.4.3. Control Main Controlled Device

Example requests:

http://192.168.1.134/current_state.xml?pw=admin&MS=1

http://192.168.1.134/current_state.jsonl?pw=admin&MS=1

Possible values for MS are 0 (CLOSE), 1 (OPEN) and 2 (STOP).

11.4.4. Control relays and Main Controlled Device via single command

Example requests:

http://192.168.1.134/current_state.xml?pw=admin&SETALL=1

http://192.168.1.134/current_state.json?pw=admin& SETALL=3

Possible values for SETALL are:

Table 11.2. SETALL control table

SETALL	Relay 1	Relay 2	Main Controlled Device
SETALL=0	OFF	OFF	CLOSE
SETALL=1	ON	OFF	CLOSE
SETALL=2	OFF	ON	CLOSE
SETALL=3	ON	ON	CLOSE
SETALL=4	OFF	OFF	OPEN
SETALL=5	ON	OFF	OPEN
SETALL=6	OFF	ON	OPEN
SETALL=7	ON	ON	OPEN

11.4.5. Control inputs alarms

Table 11.3. Alarms control table

Parameter	Example requests	Possible values
DI1ALARM	*http://192.168.1.134/current_state.xml?pw=admin&DI1ALARM=1*	1 (ENABLED) 0 (DISABLED)
DI2ALARM	*http://192.168.1.134/current_state.xml?pw=admin&DI2ALARM=1*	
DI3ALARM	*http://192.168.1.134/current_state.xml?pw=admin&DI3ALARM=0*	
AIALARM	*http://192.168.1.134/current_state.xml?pw=admin&AIALARM=1*	
TIALARM	*http://192.168.1.134/current_state.xml?pw=admin&TIALARM=0*	

11.4.6. Change descriptions of inputs, outputs and device

Table 11.4. Descriptions control table

Parameter	Description	Example request	Max allowed length	Possible values
DI1NAME	Digital Input 1 Description	*http://192.168.1.134/current_state.xml?pw=admin&DI1NAME=Button*	10	see **Appendix 3.**
DI2NAME	Digital Input 2 Description	*http://192.168.1.134/current_state.xml?pw=admin&DI2NAME=Button*	10	
DI3NAME	Digital Input 3 Description	*http://192.168.1.134/current_state.xml?pw=admin&DI3NAME=Button*	10	
AINAME	Analog Input Description	*http://192.168.1.134/current_state.xml?pw=admin&AINAME=Rain*	10	
TINAME	Temperature Input Description	*http://192.168.1.134/current_state.xml?pw=admin&TINAME=Temp*	10	
R1NAME	Relay 1 Description	*http://192.168.1.134/current_state.xml?pw=admin&R1NAME=Heater*	10	
R2NAME	Relay 2 Description	*http://192.168.1.134/current_state.xml?pw=admin&R2NAME=Clima*	10	
MSNAME	MCD Name	*http://192.168.1.134/current_state.xml?pw=admin&MSNAME=Door*	12	

DEVNAME	Device Name	http://192.168.1.134/current_state.xml?pw=admin&DEVNAME=Garage	15	
DEVLOC	Device Location	http://192.168.1.134/current_state.xml?pw=admin&DEVLOC=Bulgaria	15	

11.4.7. Grant Guest user access

This request could be made only by **Admin User**. Request should look like this:

http://192.168.1.134/current_state.xml?pw=admin&GUEST=1

http://192.168.1.134/current_state.json?pw=admin&GUEST=0

Possible values for **Guest User** are 0 (DISABLE) and 1 (ENABLE).

- If wrong password is sent via HTTP XML/JSON request, "Bad Arguments!" message will be received from **smartDEN Opener**. If incorrect parameters are sent, they will not take effect!

12. MQTT protocol

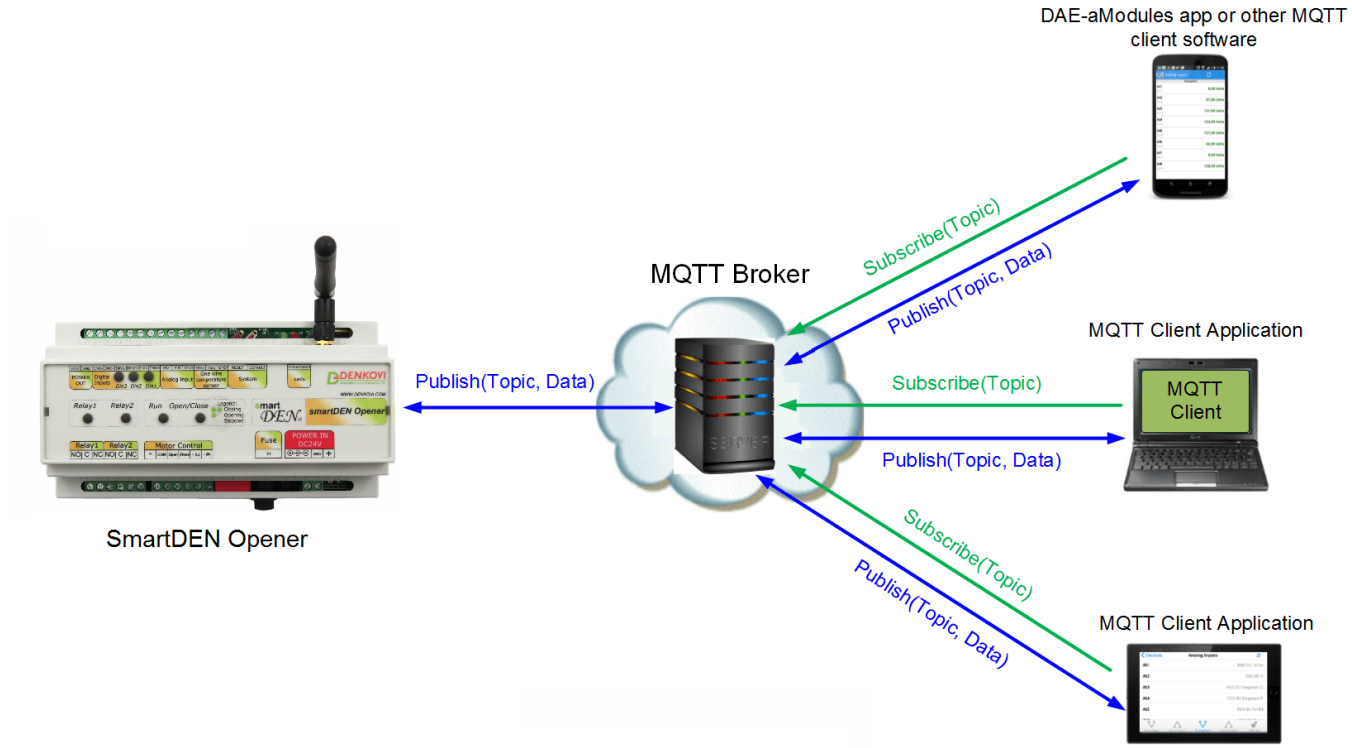

Figure 12.1. MQTT communication Overview

smartDEN Opener has MQTT client for cloud access to the state of the module and control the **I/O** lines. Adding **smartDEN Opener** as cloud device via *DAE-aModules* application will use this protocol for communication. It is possible to create third party application based on this information.

12.1. MQTT topics generating

- MQTT topics generating encryption algorithm to be implemented in custom application is available upon request.

12.2. MQTT protocol commands

smartDEN Opener uses MQTT QoS 0 subscription. The communication is not secured and messages are sent over network in plain text. **smartDEN Opener's** default MQTT Broker is *iot.eclipse.org*, but some other free public brokers are also available like *test.mosquitto.org*. Keep in mind that public brokers might be unavailable due to server overload or other problems.

Here it is described how to get current state of **smartDEN Opener** and how to change I/O's states, alarms, descriptions, etc. The functionality is the same as HTTP Protocol. Both **Admin** and **Guest** users can obtain this information when access is enabled. Command requests are created in this way:

MQTT_COMMAND?<command>; Example: *MQTT_COMMAND?R1=1;*

MQTT_COMMAND?<command1>&<command2>; Example: *MQTT_COMMAND?R1=1&R2=1;*

More commands separated by '*&*' combined in one request. As seen *MQTT_COMMAND* is the keyword of the request. Next is '*?*' sign which notes that the commands start from this symbol. Each command is separated by '*&*' sign. At end of the request '*;*' sign should be applied. If this principle is not observer a "Bad Arguments!" message will be received.

- Maximum request length is 100 symbols starting from MQTT_COMMAND and ending with last ";".

12.2.1. Getting current state of smartDEN Opener

Getting the current state as each other command should be posted in **Admin Reading Topic**.

MQTT_COMMAND?GETSTATUS;

When command is sent, response will be received in admin writing topic. The response of all successful commands is the same and is given on **Figure 12.2**.

12.2.2. Relays control

MQTT_COMMAND?R1=1;

MQTT_COMMAND?R2=0;

Possible values for R1 and R2:

- *0* - turn off;
- *1* - turn on.

12.2.3. Control relays via single command

MQTT_COMMAND?R=3;

Possible values for R are shown in table below:

Table 12.1. Relays control table

R	Relay 1	Relay 2
R=0	OFF	OFF
R=1	ON	OFF
R=2	OFF	ON
R=3	ON	ON

12.2.4. Control Main Controlled Device

MQTT_COMMAND?MS=2;

Possible values for MS are 0 (CLOSE), 1 (OPEN) and 2 (STOP).

12.2.5. Control relays and Main Controlled Device via single command

MQTT_COMMAND?SETALL=7;

Table 12.2. SETALL control table

SETALL	Relay 1	Relay 2	Main Controlled Device
SETALL=0	OFF	OFF	CLOSE
SETALL=1	ON	OFF	CLOSE
SETALL=2	OFF	ON	CLOSE
SETALL=3	ON	ON	CLOSE
SETALL=4	OFF	OFF	OPEN
SETALL=5	ON	OFF	OPEN
SETALL=6	OFF	ON	OPEN
SETALL=7	ON	ON	OPEN

12.2.6. Enable/disable inputs alarms

MQTT_COMMAND?SETALL=7;

Table 12.3. Inputs alarms table

Parameter	Example Request	Possible Values
DI1ALARM	*MQTT_COMMAND?DI1ALARM=1;*	1 (ENABLED) 0 (DISABLED)
DI2ALARM	*MQTT_COMMAND?DI2ALARM=0;*	
DI3ALARM	*MQTT_COMMAND?DI3ALARM=1;*	
AIALARM	*MQTT_COMMAND?AIALARM=1;*	
TIALARM	*MQTT_COMMAND?TIALARM=0;*	

12.2.7. Change descriptions

Table 12.4. Descriptions commands table

Parameter	Description	Example Request	Max allowed length	Possible Values
DI1NAME	Digital Input 1 Description	*MQTT_COMMAND?DI1NAME=Button1;*	10	see **Appendix 3.**
DI2NAME	Digital Input 2 Description	*MQTT_COMMAND?DI2NAME=Button2;*	10	
DI3NAME	Digital Input 3 Description	*MQTT_COMMAND?DI3NAME=Button3;*	10	
AINAME	Analog Input Description	*MQTT_COMMAND?AINAME=Humid;*	10	
TINAME	Temperature Input Description	*MQTT_COMMAND?TINAME=Temp;*	10	
R1NAME	Relay 1 Description	*MQTT_COMMAND?R1NAME=Heater;*	10	
R2NAME	Relay 2 Description	*MQTT_COMMAND?R2NAME=Clima;*	10	
MSNAME	MCD Name	*MQTT_COMMAND?MSNAME=Door;*	12	
DEVNAME	Device Name	*MQTT_COMMAND?DEVNAME=Garage;*	15	

DEVLOC	Device Location	*MQTT_COMMAND?DEVLOC=Bulgaria;*	15	

12.2.8. Grant Guest user access

This request could be made only by **Admin User**. Request should look like this:

MQTT_COMMAND?GUEST=1;

Possible values for **Guest User** command:

- *0* - **DISABLE**;
- *1* - **ENABLE**.

12.2.9. MQTT command reply

```
<CurrentState>
<DI1>
  <Name>DI1</Name>
  <State>0</State>
  <Alarm>1</Alarm>
</DI1>
<DI2>
  <Name>DI2</Name>
  <State>0</State>
  <Alarm>1</Alarm>
</DI2>
<DI3>
  <Name>DI3</Name>
  <State>0</State>
  <Alarm>1</Alarm>
</DI3>
<AI>
  <Name>temp</Name>
  <Value>540</Value>
  <Scaled_Value>2.6V</Scaled_Value>
  <Alarm>1</Alarm>
</AI>
<TI>
  <Name>TI</Name>
  <Value>25.1C</Value>
  <Alarm>1</Alarm>
</TI>
<Relay1>
  <Name>ass</Name>
  <State>1</State>
</Relay1>
<Relay2>
  <Name>dss</Name>
  <State>1</State>
</Relay2>
<Main>
  <Name>Garage Door</Name>
  <State>4</State>
  <StateName>CLOSED</StateName>
  <OpeningTime>5</OpeningTime>
  <ClosingTime>0</ClosingTime>
  <LastOpened>29 November 2017 09:51:57 by ADMIN_HTTP</LastOpened>
  <LastClosed>29 November 2017 09:52:04 by AUTO_CLOSE</LastClosed>
</Main>
<Guest>
  <State>1</State>
</Guest>
<Device>
  <Name>DeviceName</Name>
  <Location>BULGARIA</Location>
  <MAC>5C:CF:7F:C0:94:7A</MAC>
  <Heap>25688</Heap>
  <WiFiSignal>47%</WiFiSignal>
</Device>
</CurrentState>
```

Figure 12.2. MQTT successful response

13. Security considerations

There are no extraneous IP services found on general-purpose operating systems (e.g. fingerd, tcp_wrapper, etc.) that can possibly be exploited by an unauthorized agent. In particular, the **smartDEN Opener** does not run protocols such as Telnet and FTP which may have the potential for security breech.

Web-browser access

A challenge-response authentication is used in login process. When the password is entered, it is transmitted across the network in encrypted form, so eavesdropping on the data transmission will not reveal the password. Subsequent transmissions of the password to "login" onto the device are encrypted and "safe". The only case when the password is transmitted across the network "in the open", is when it is being changed and submitted in **General Settings** form. Therefore, you must set passwords in the secure environment where you can make sure that no one is "eavesdropping".

MQTT operation

MQTT protocol uses encrypted topics subscription. However when MQTT operation is used on public brokers, messages could be eavesdropped. **smartDEN Opener** does NOT use SSL communication and each messages are transmitted in plain text. For more security own private MQTT broker could be used.

XML operation

XML operation uses open authentication so the requests are sent over the network in plain text and could be eavesdropped. Use it on your own risk.

- Web server and HTTP XML and JSON requests access can be restricted by IP Address (range of IP Addresses) as additional security.

RF remote

RF remote controller uses "rolling code" encryption which is considered safe enough. The RF remote controllers with **smartDEN Opener** are just the same as cars' RF remote controllers.

14. Mechanical drawing

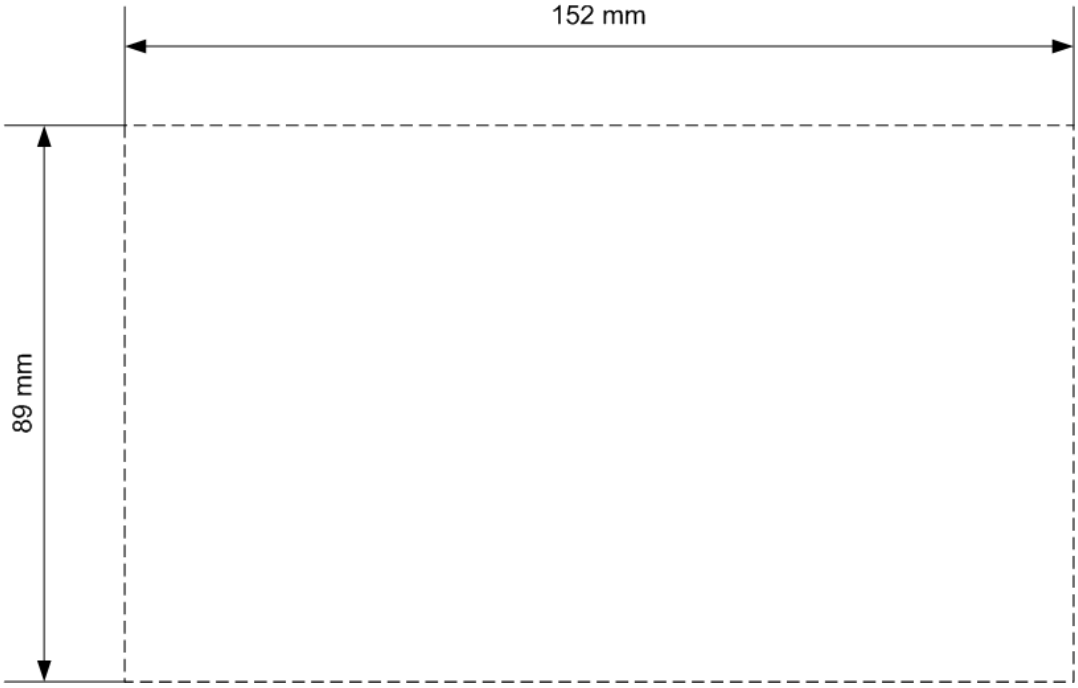

Figure 14.1. DIN Rail device size

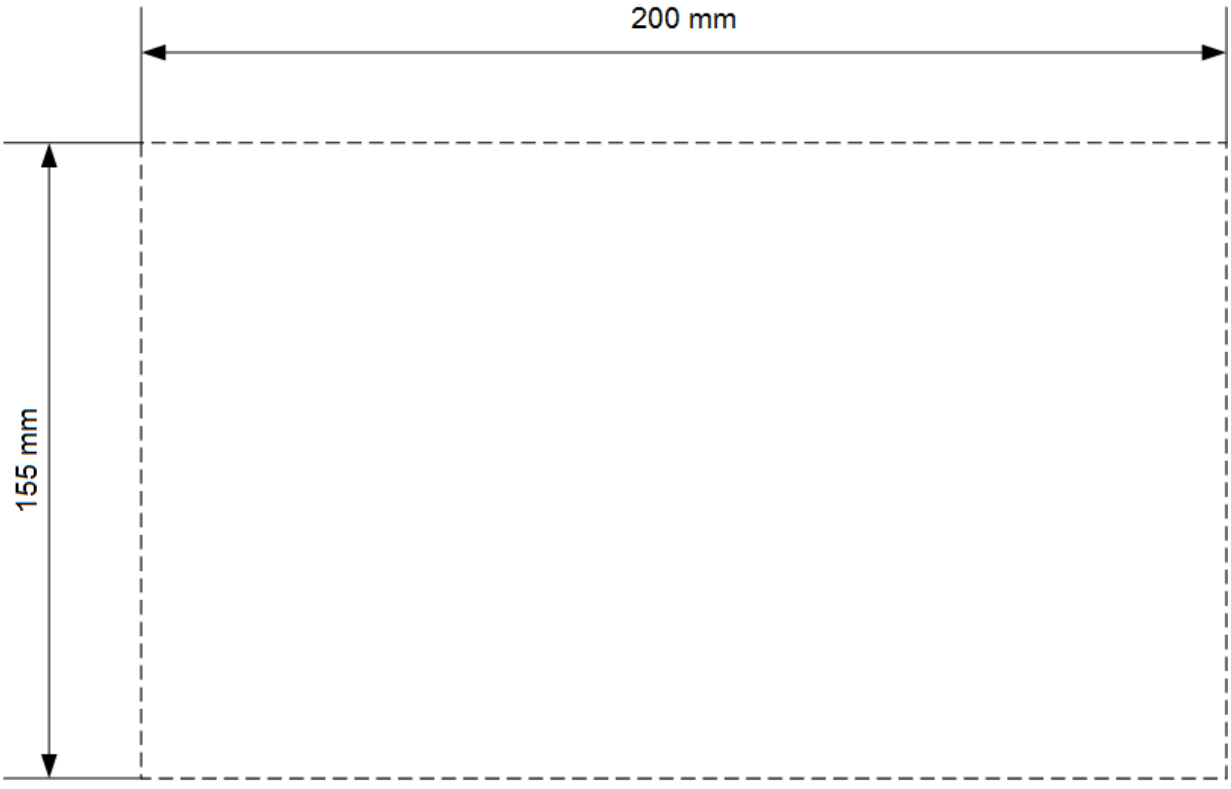

Figure 14.2. Distribution box device size

15. Appendix 1. Connecting external controller to smartDEN Opener relays

Controlling barriers (or other devices with built-in controller) using **smartDEN Opener's** dry output contact is easy. Just attach relay to Main Controlled Device and control barriers. An example of hardware connection is given on **Figure 15.1** and configuration is given on **Figure 15.2.** In this example is assumed that barrier is opened on short circuit on the dry contact digital input and closed on open circuit. Controlling is made by OPEN and CLOSE buttons (commands) and could be controlled by web server, HTTP XML and JSON requests, MQTT commands and RF Remote Controller.

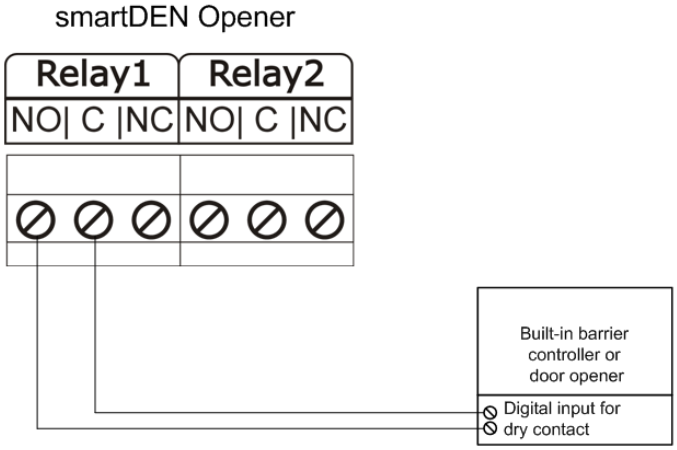

Figure 15.1. Hardware Connection to **smartDEN Opener**

In our example Relay1 is controlling the barrier. Relay 1 is attached to Main Controlled Device. So when click OPEN button (send OPEN command) the barrier will open and when click CLOSE (send CLOSE command) the barrier will close. Additional features like Attach DI Protection Sensor or timer "auto close" function could be used too for fully automation (see **10.4. Main Controlled Device Page**).

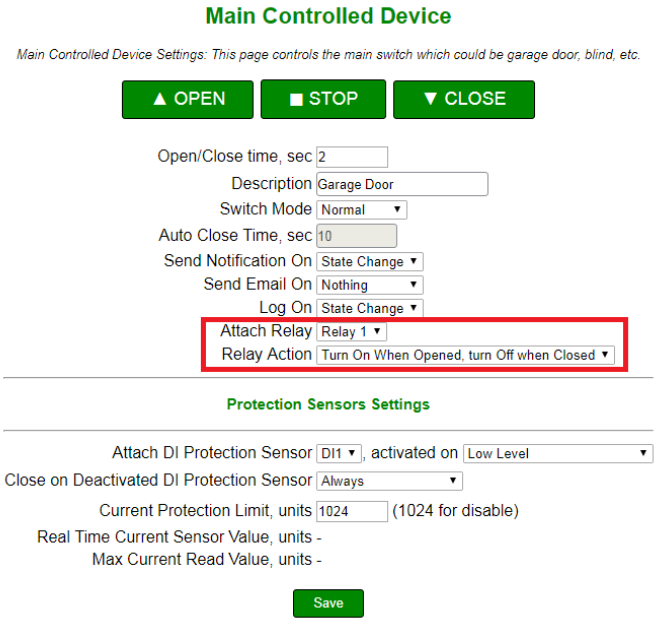

Figure 15.2. Configuration of Main Controlled Device

16. Appendix 2. DAE-aModules

DAE-aModules application provides some unique features. One of them is notification receiving and the other is GPS controlling of the Main Controlled Device.

16.1. Notifications

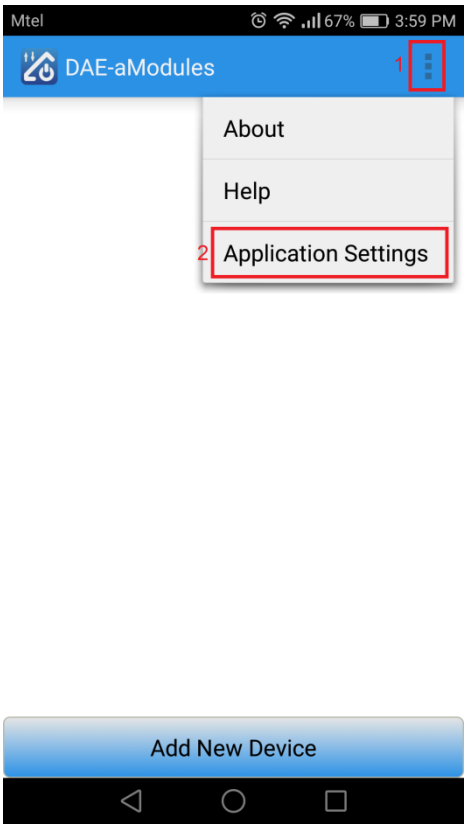

Figure 16.1. *DAE-aModules* configuration

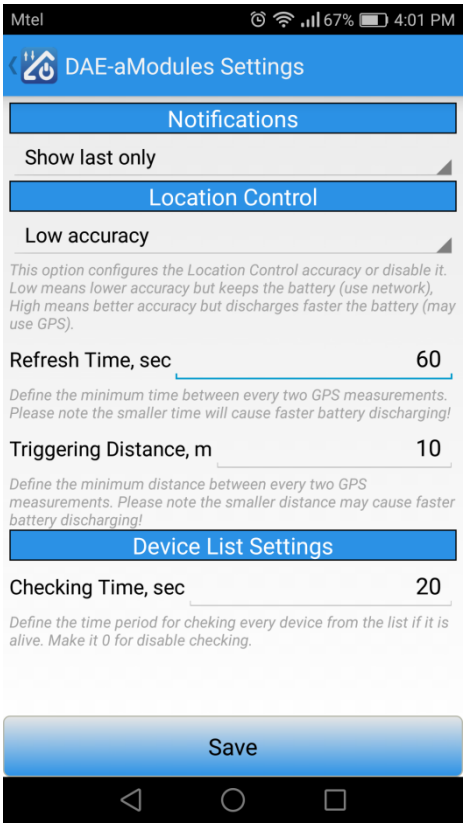

Figure 16.2. *DAE-aModules* application settings

1. Go to upper right corner and click the button (**Figure 16.1**);
2. Click application settings. New window will be loaded showing these settings (**Figure 16.2**).

There are several options for notifications reception:

- **Disabled** - *DAE-aModules* will not show any notifications;
- **Show few** - *DAE-aModules* will show the last notification from last added device in device list which sends notifications. If **smartDEN Opener** sent the last notification and is last in the device list its notification will be shown;
- **Show last only** - *DAE-aModules* will show the last notification received (from all devices in device list). If **smartDEN Opener** sent the last notification its notification will be shown;
- **Show all** - *DAE-aModules* will show every message received from **smartDEN Opener** (Cloud) and all other added devices.

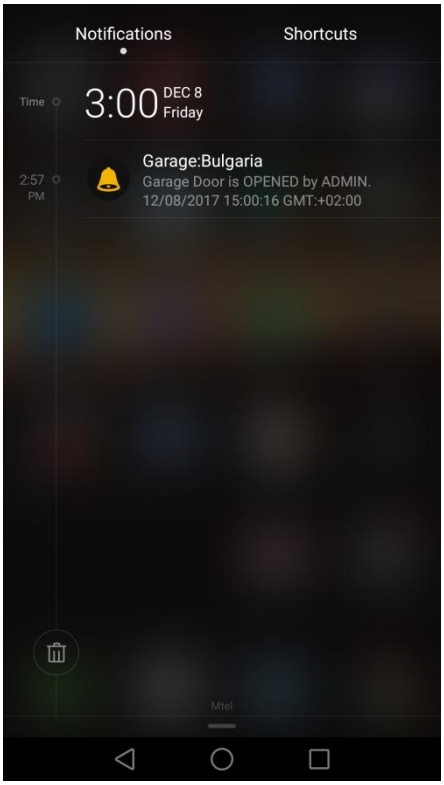

Figure 16.3. Notification Preview

16.2. Location Control

This option could be used to control **smartDEN Opener's** Main Controlled Device via GPS coordinates. Useful feature especially for garage doors. There are several settings to configure:

- **Accuracy** - provides three options:
  - *Disable - DAE-aModules* will disable **Location Control**;
  - *Low Accuracy* - this option will use location from network and will keep battery charge;
  - *High Accuracy* - this option may use GPS location for higher accuracy. Note that battery could discharge faster.
- **Refresh Time** - this option defines the minimum time between two GPS measurements. Note that smaller **Refresh Time** will cause faster battery discharging;
- **Triggering Distance** - this option defines the minimum distance between every two GPS measurements. Note that smaller **Triggering Distance** will cause faster battery discharge.

16.3. Control a Relay or Main Controlled Device by GPS location

There are two available options to control a relay or the Main Controlled Device by location - **GPS Inside** (set relay/door on/open while entering the perimeter) or **GPS Outside** (set relay/door on/open while leaving the perimeter):

1. In "**Control**" tab of *DAE-aModules* click on the button in the upper right corner.
2. Click on the appeared "Settings" button.
3. Then select the desired relay or Main Controlled Device and click on it. A pop-up window will appear. From this window the name of the relay could be changed as well as special mode could be selected.

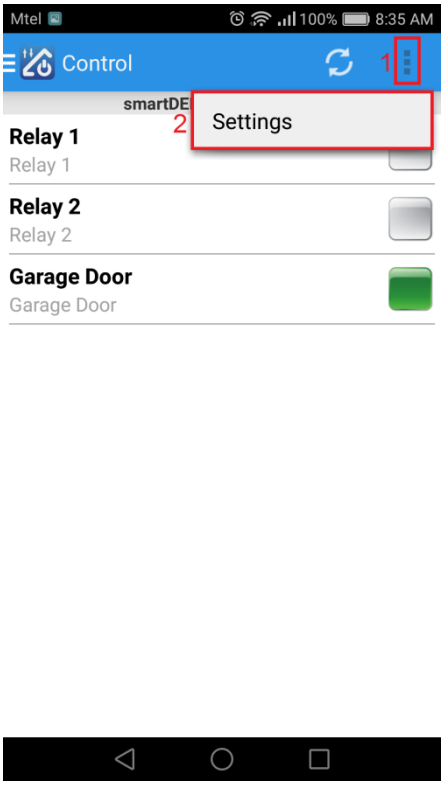

Figure 16.4. Relays Tab

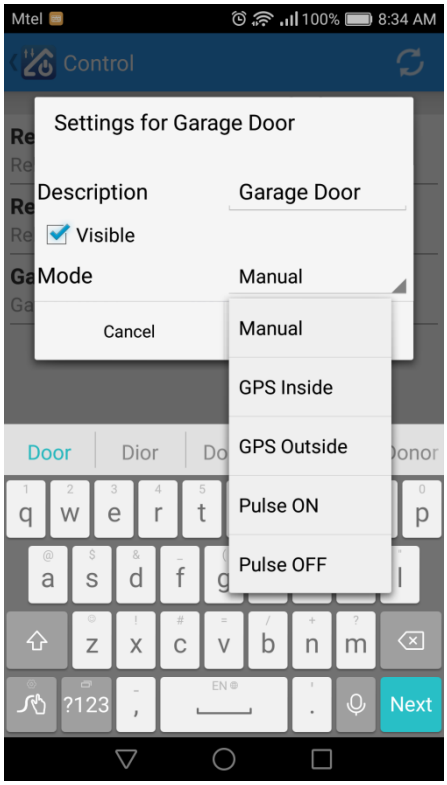

Figure 16.5. Main Controlled Device's modes

Location control could be done with these two modes:

- **GPS Inside** - In this mode the output (relay) will be set ON when the user crosses the set radius entering the perimeter. This is suitable for example when the user approach his house and want to open some garage door automatically. Please note an internet connection is required for this command otherwise it won't be executed.

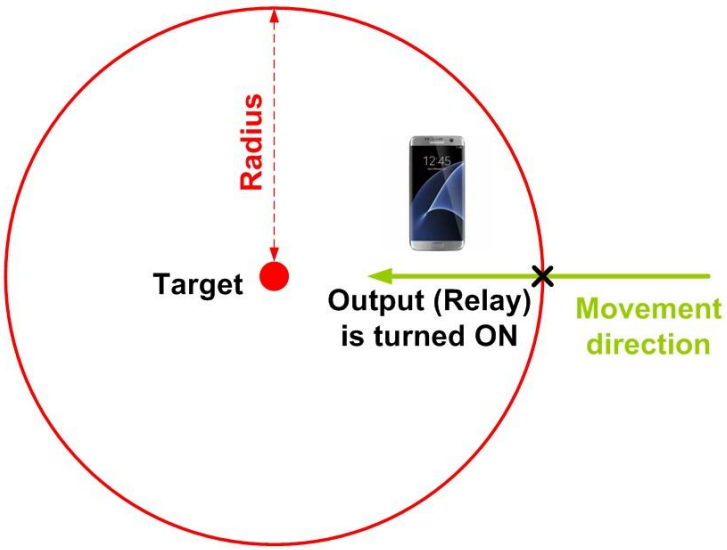

Figure 16.6. GPS Inside control by location

- **GPS Outside** - In this mode the output (relay) will be set ON when the user crosses the set radius leaving the perimeter. This is suitable for example when the user leaves his work place and going home an electrical device must be switched ON automatically. Please note an internet connection is required for this command otherwise it won't be executed.

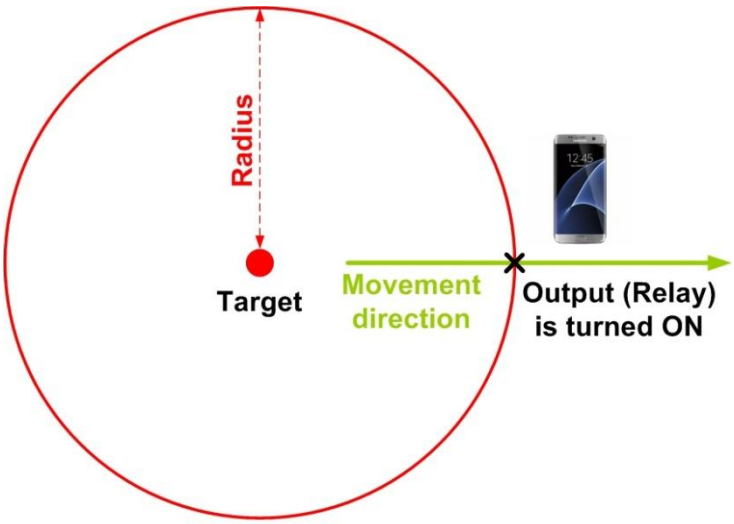

Figure 16.7. GPS Outside control by location

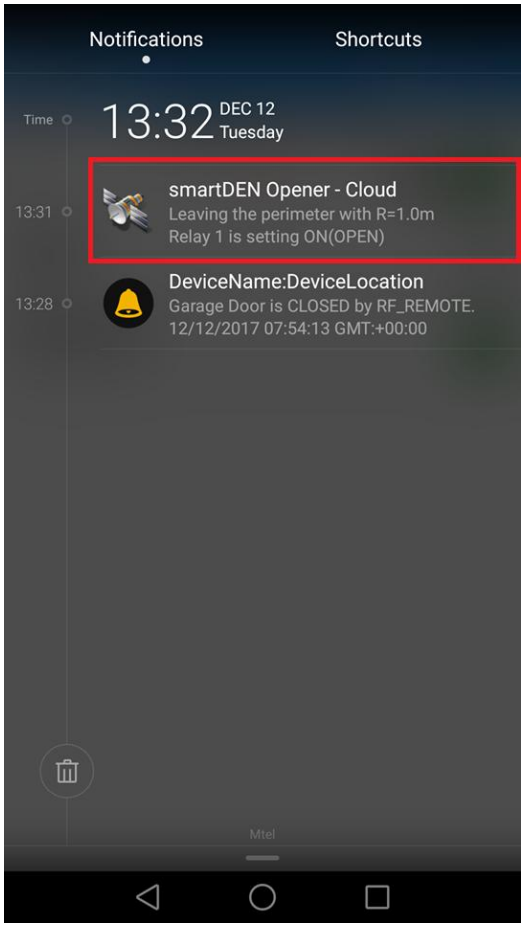

Figure 16.8. GPS outside mode notification

17. Appendix 3. Char set

smartDEN Opener has a set of characters (char set) which are allowed when typing descriptions, names, etc. They are given in the table below.

Table 17.1. Char set

Character	Description
A-Z	Capital letters (English Alphabet)
a-z	Small letters (English Alphabet)
0-9	Numbers (zero to nine)
-	Minus sign
+	Plus sign
	Space character
%	Percent sign
_	Underscore sign
,	Comma sign
.	Dot sign
****	Backslash sign
/	Forward slash sign
?	Question mark sign
:	Colon sign
@	At symbol
=	Equal sign
$	Dollar sign
#	Sharp sign
!	Exclamation mark sign
^	Caret sign
*****	Asterisk sign

18. Appendix 4. Dictionary

AI - Analog Input
TI - Temperature Input
DI - Digital Input
MCD - Main Controlled Device (means the motor controlled device - barrier, door, window, awning).
Main - Main Controlled Device (means the motor controlled device - barrier, door, window, awning).
MQTT - MQ Telemetry Transport or Message Queuing Telemetry Transport
XML - Extensible Markup Language
JSON - JavaScript Object Notation
HTTP - Hyper Text Transfer Protocol
DHCP - Dynamic Host Configuration Protocol
IP - Internet Protocol
SMTP - Simple Mail Transfer Protocol
RTC - Real Time Clock

19. Appendix 5. Disclaimer

Denkovi Assembly Electronics LTD products are not designed, authorized or warranted to be suitable for use in space, nautical, space, military, medical, life-critical or safety-critical devices or equipment.

Denkovi Assembly Electronics LTD products are not designed, authorized or warranted to be suitable for use in applications where failure or malfunction of an Denkovi Assembly Electronics LTD product can result in personal injury, death, property damage or environmental damage.

Denkovi Assembly Electronics LTD accepts no liability for inclusion or use of Denkovi Assembly Electronics LTD products in such applications and such inclusion or use is at the customer's own risk. Should the customer use Denkovi Assembly Electronics LTD products for such application, the customer shall indemnify and hold Denkovi Assembly Electronics LTD harmless against all claims and damages.