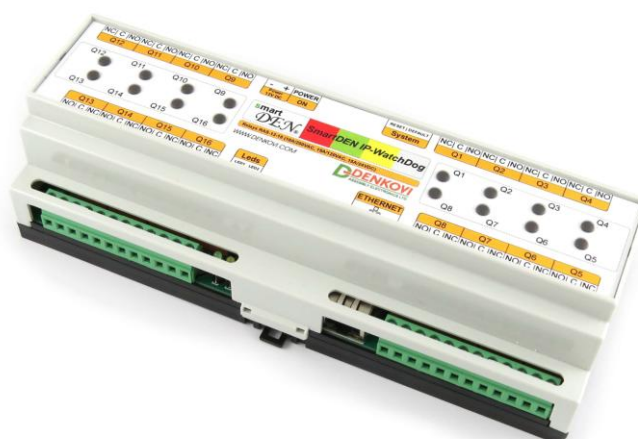


smartDEN IP-WatchDog

PING Restarter and Auto-Rebooter

User Manual
Date: 06 Aug 2017

For firmware version: v1.21 / May 2017



Content

1.	Features	3
2.	Application examples.....	4
3.	Technical parameters	7
4.	Connectors, ports and led indicators	8
5.	Installation	8
6.	Default Settings	17
7.	Web access.....	19
8.	HTTP/XML/JSON access	31
9.	Auto-Reboot mode specifics.....	37
10.	Security considerations.....	38
11.	Appendix 1. Settings for different hardware connection modes.....	39
12.	Appendix 2. Dimensions	41

1. Features

smartDEN IP-WatchDog is network (LAN/WAN) device which can monitor up to 16 remote hosts' (PC, routers, switches, cameras...) availability. If an unresponsive host is detected, the module reboots it automatically.

- 10 Mb Ethernet interface with Link/Activity Led;
- Auto-MDIX;
- 16 independent channels;
- SPDT Relay for every channel (NO,C,NC);
- Led for each relay;
- Four testing modes available for each channel:
 - Incoming PING;
 - Outgoing PING;
 - Incoming HTTP;
 - Outgoing HTTP;
- Three possible hardware connection ways:
 - In parallel of the device "Reset" button;
 - In parallel of the device "Power ON/OFF" button;
 - In sequence of the device power supply cable;
- Fully configurable sequence of testing and rebooting;
- Two modes for every channel:
 - Auto-Reboot mode;
 - General Purpose mode (ON/OFF);
- Built-in hardware Real Time Clock (RTC);
- Web server with secure login authorization;
- Secure HTTP/XML/JSON API protocols for integration;
- Supported protocols: ARP, IP, ICMP (ping), DHCP, DNS;
- Access protection (by IP and MAC address);
- Option for relays states saving and loading on reset;
- Free Android application for monitoring and control.

2. Application examples

2.1. Monitoring / restarting computer (PC) farms

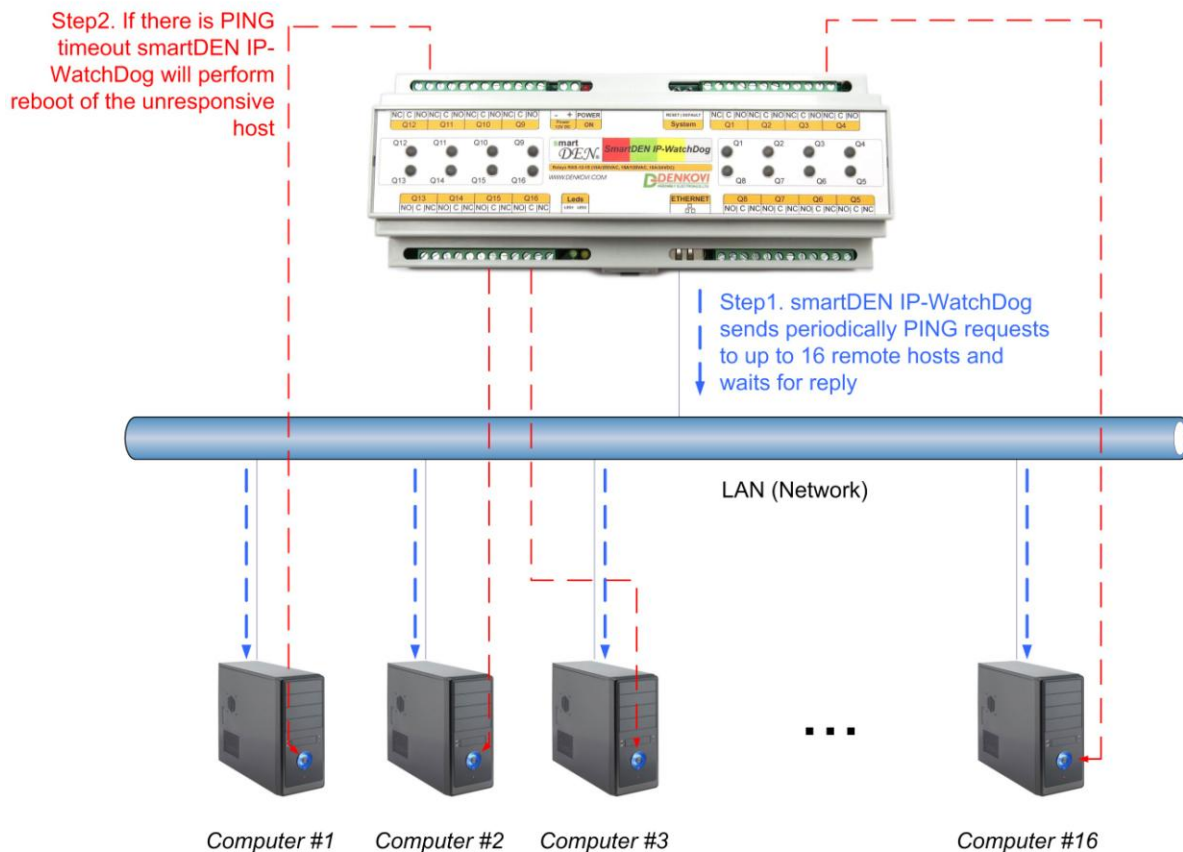


Figure 1. Monitoring / restarting computer (PC) farms

- **smartDEN IP-WatchDog** sends PING request to up to 16 computers periodically;
- If a reply is not received within the stated timeframe a reboot will be performed;
- The procedure is fully automated and no additional software/hardware/human action is needed;
- Operator can monitor computer state and perform reboot sequence at any time manually as well.

2.2. Monitoring / restarting network equipment

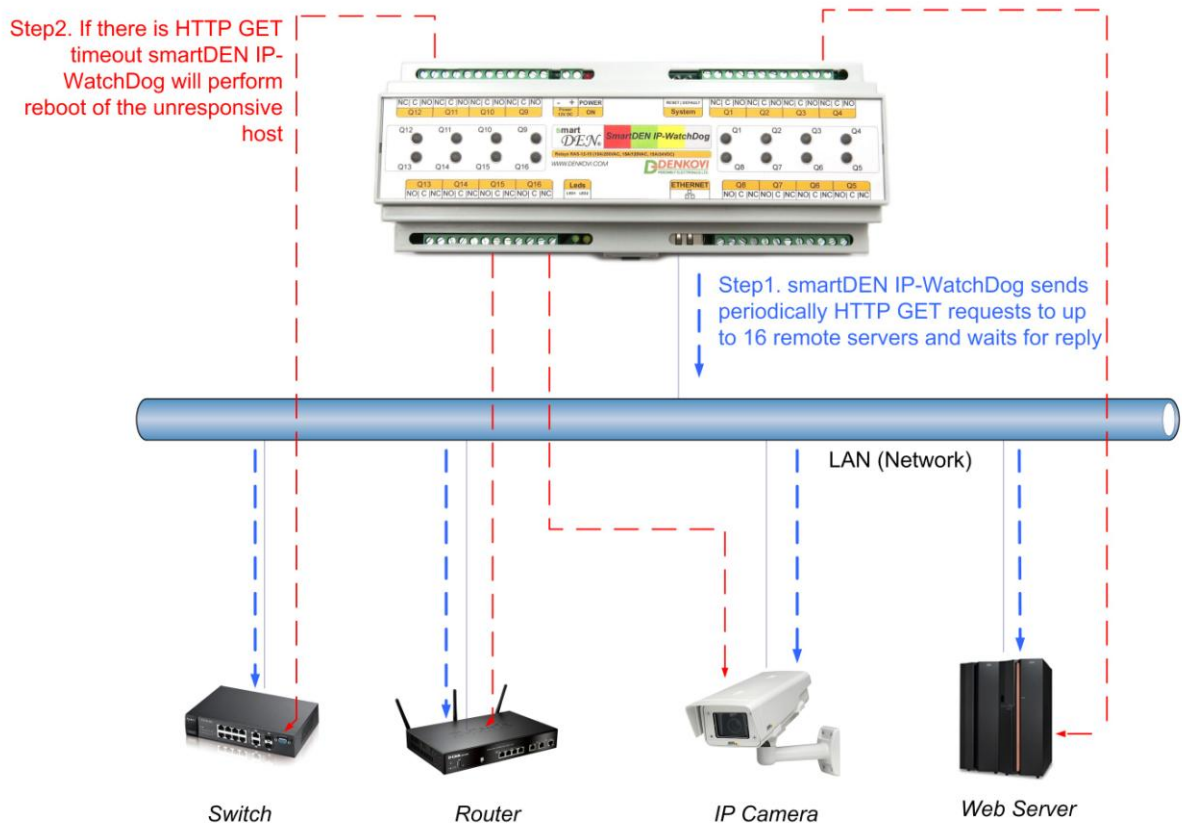


Figure 2. Monitoring / restarting network equipment

- **smartDEN IP-WatchDog** monitors the webserver of the remote host (IP Camera for example) via sending HTTP GET requests periodically;
- If a reply is not received within the stated timeframe a reboot will be performed;
- The procedure is fully automated and no additional software/hardware/human action is needed;
- Operator can monitor computer state and perform reboot sequence at any time manually as well;
- Up to 16 network devices can be monitored and rebooted.

2.3. Internet connection checking

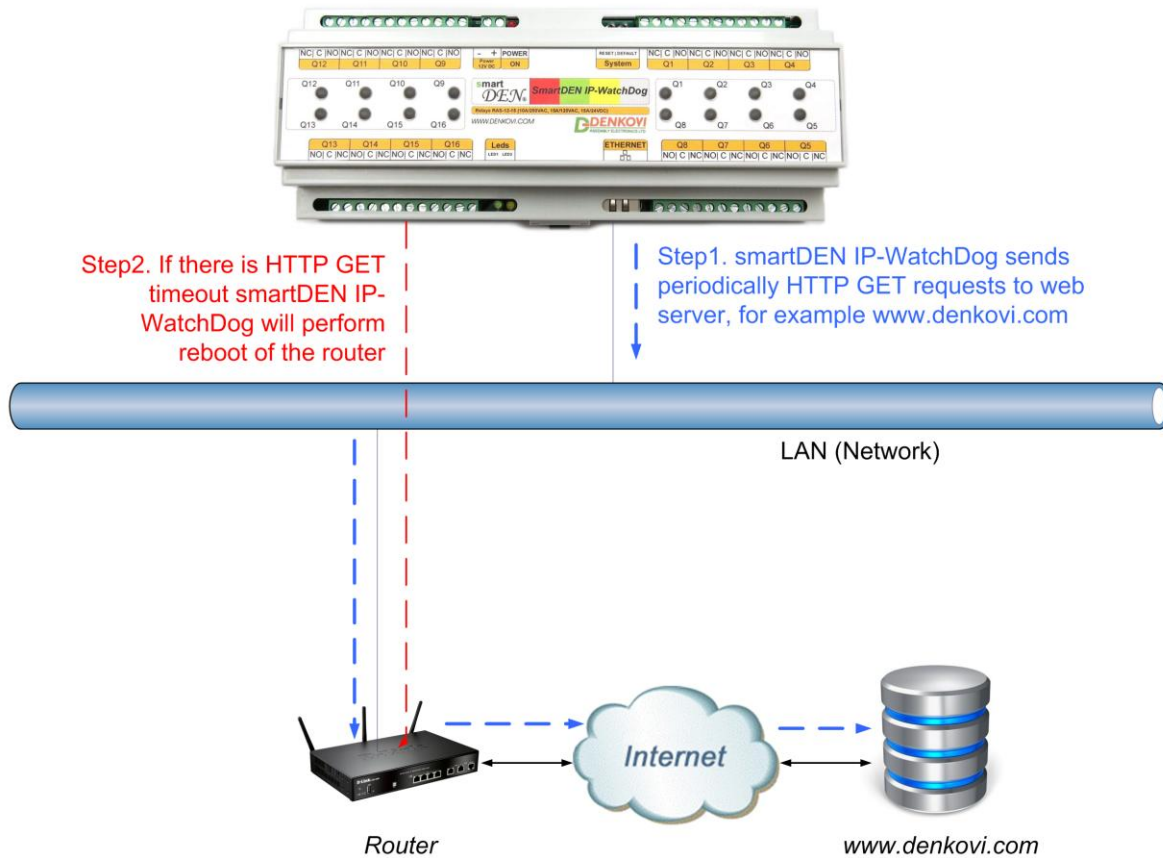


Figure 3. Internet connection checking

- **smartDEN IP-WatchDog** sends HTTP GET request to web server;
- If a reply is not received within the stated timeframe a reboot of the router will be performed;
- The procedure is fully automated and no additional software/hardware/human action is needed;
- Operator can monitor computer state and perform reboot sequence at any time manually as well.

3. Technical parameters

Table 1. Technical parameters

Parameter	Value
Box size, mm	210 x 85 x 58
Box weight, g	420
Power supply voltage,VDC	12 or 24 (depends on the model) ± 2
Maximum current consumption at 12VDC (when all relays are ON), mA	600
Maximum current consumption at 24VDC (when all relays are ON), mA	400
Operating temperature, °C	0 to 70
Relays maximum switchable current / voltage	10A / 250VAC, 15A / 120VAC, 10A / 28VDC

4. Connectors, ports and led indicators

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

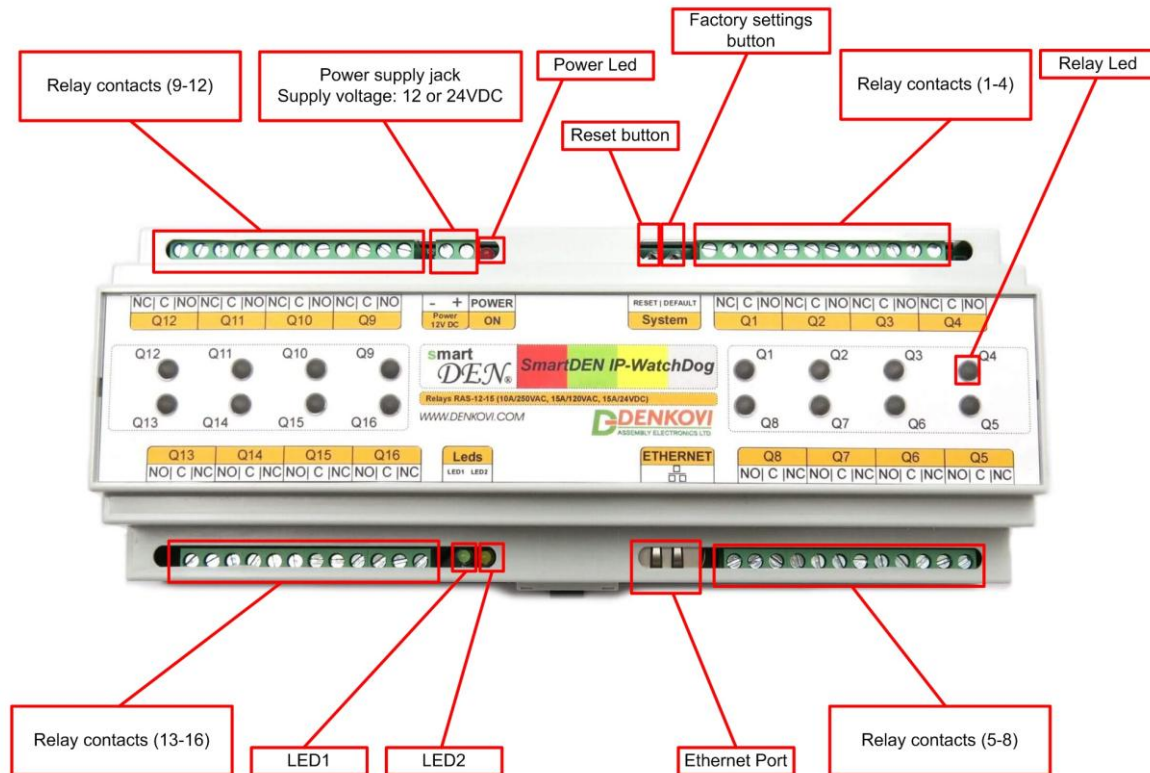


Figure 4. Device overview

5. Installation

- This device must be installed by qualified personnel;
- This device must not be installed directly outdoors;
- Installation consists of mounting the device, connecting to an IP network, connecting the relays, providing power and configuring via a web browser.

5.1. Box mounting



Figure 5. Mounting the device to DIN rail

smartDEN IP-WatchDog 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.

5.2. Power supply

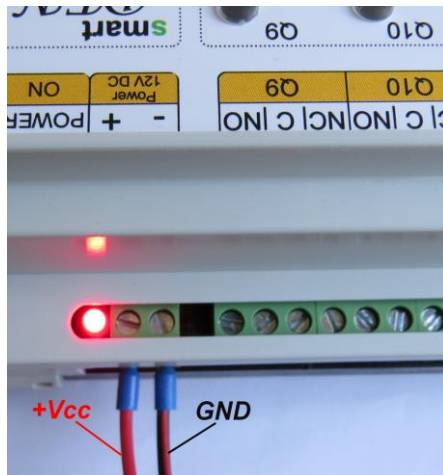


Figure 6. smartDEN IP-WatchDog power supply

Depending on the selected model during purchase the power supply source for **smartDEN IP-WatchDog** must be with voltage either **12VDC** or **24VDC** stabilized and filtered. After power on, the power led must be on and **Led1 indicator** must start blinking in 5 seconds which means the controller is running normally.



Figure 7. Connecting a LAN cable

- ❗ Please keep the polarity and supply voltage range!
- ❗ **smartDEN IP-WatchDog** 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.

5.3. Connection with the monitored device

smartDEN IP-WatchDog has 16 SPDT relays channels with parameters specified in the technical parameters section. Every relay channel has normally open (NO) and normally closed (NC) contacts connected directly to the terminals. Please refer to Appendix 1 for settings.

5.3.1. In parallel of the device "Reset" button

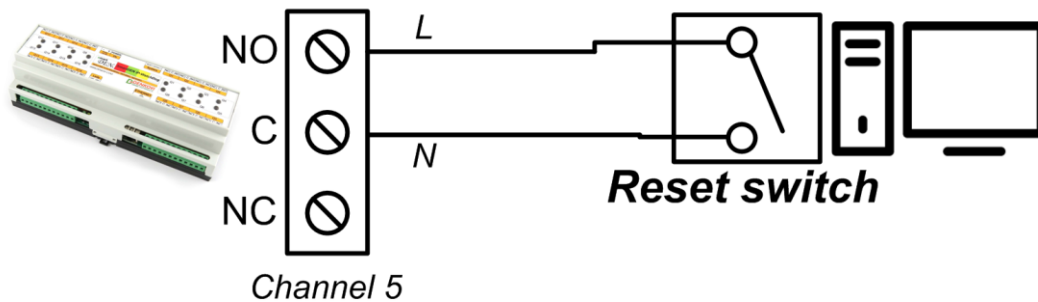


Figure 8. Connection with "Reset" button

5.3.2. In parallel of the device "Power ON/OFF" button

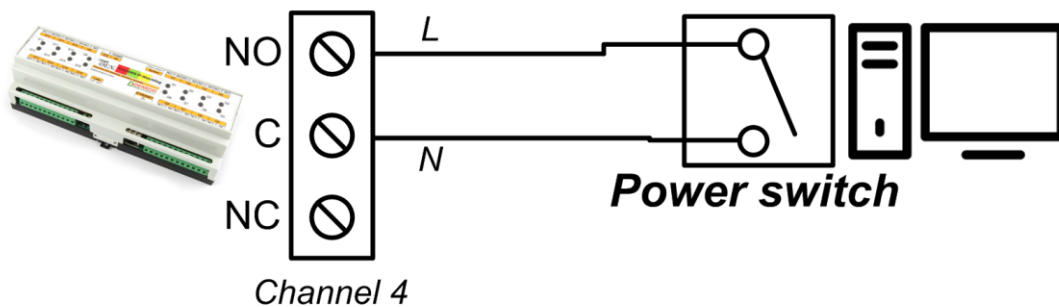


Figure 9. Connection with "Power" button

5.3.3. In sequence of the device power supply cable

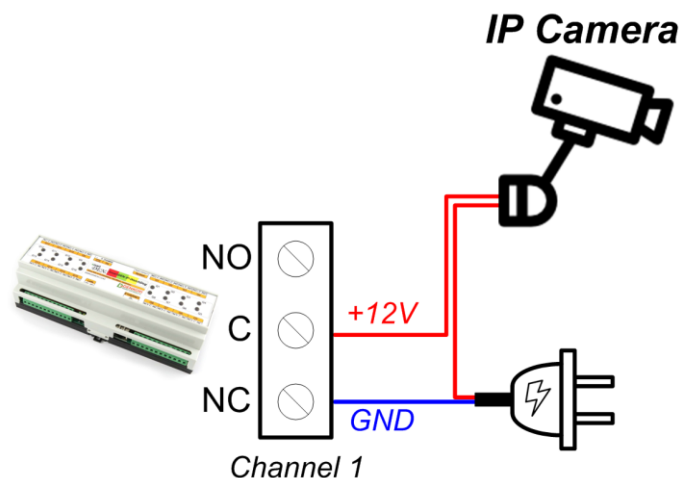


Figure 10. Connection with ip camera power supply

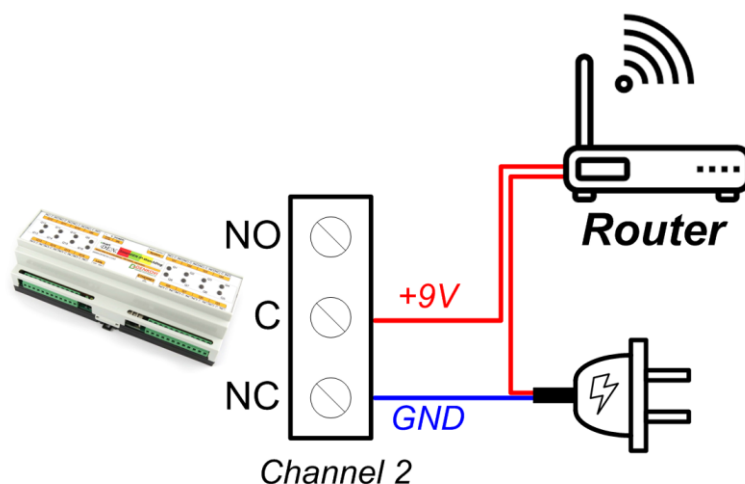


Figure 11. Connection with router power supply

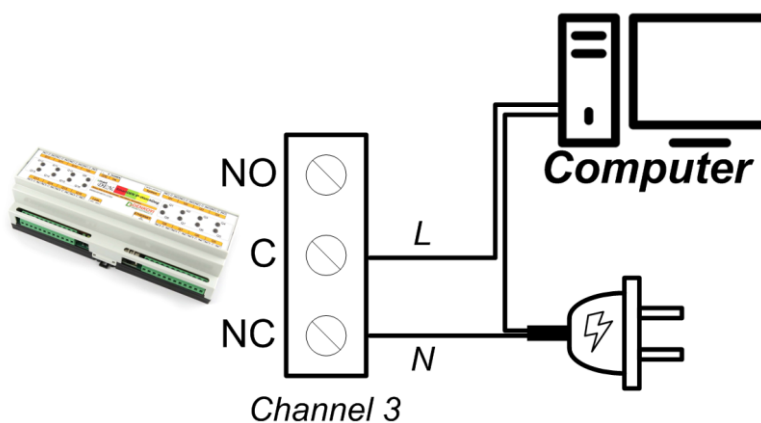


Figure 12. Connection with computer power supply

5.4. Network connection

smartDEN IP-WatchDog supports AUTO-MDIX so either "crossover" or "straight-through" network cable can be used.

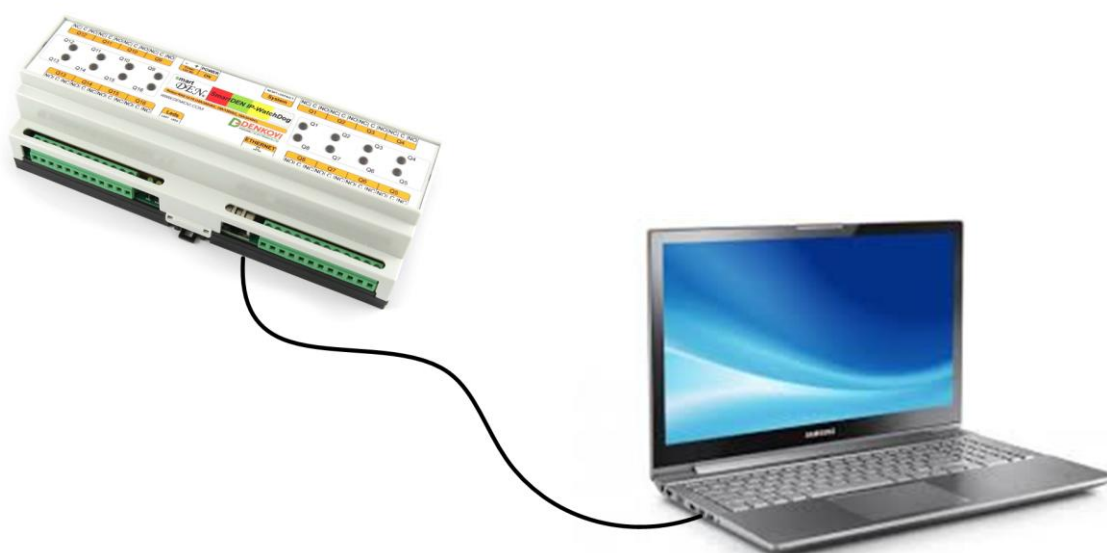


Figure 13. Connecting **smartDEN IP-WatchDog** to a computer directly. This is the recommend initial connection.



Figure 14. Connecting **smartDEN IP-WatchDog** to a wireless router.

5.5. Communication setup

smartDEN IP-WatchDog is shipped with the following default parameters:

- IP address: **192.168.1.100**
- Subnet mask: **255.255.255.0**
- Gateway: **192.168.1.1**
- Web password: **admin**

Initially it is recommended to connect the module directly to the computer.

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



You can google how to change you computer IP settings or just visit this web page: <http://www.howtochangeipaddress.com/changeip.php>

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 local area connection with right click and select *Properties*:

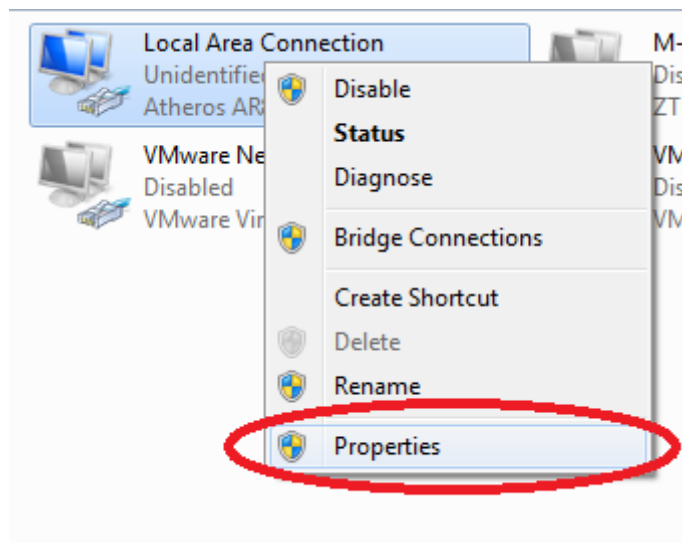


Figure 15. LAN card properties

The next step is to enter into IPv4 properties.

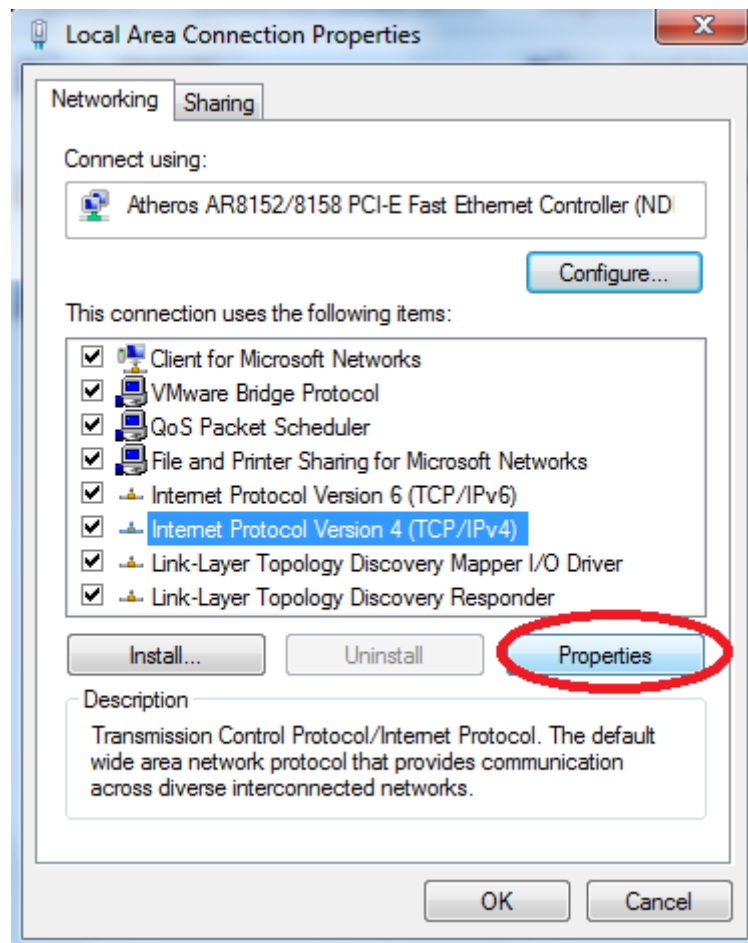


Figure 16 Enter in IPv4 properties section

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

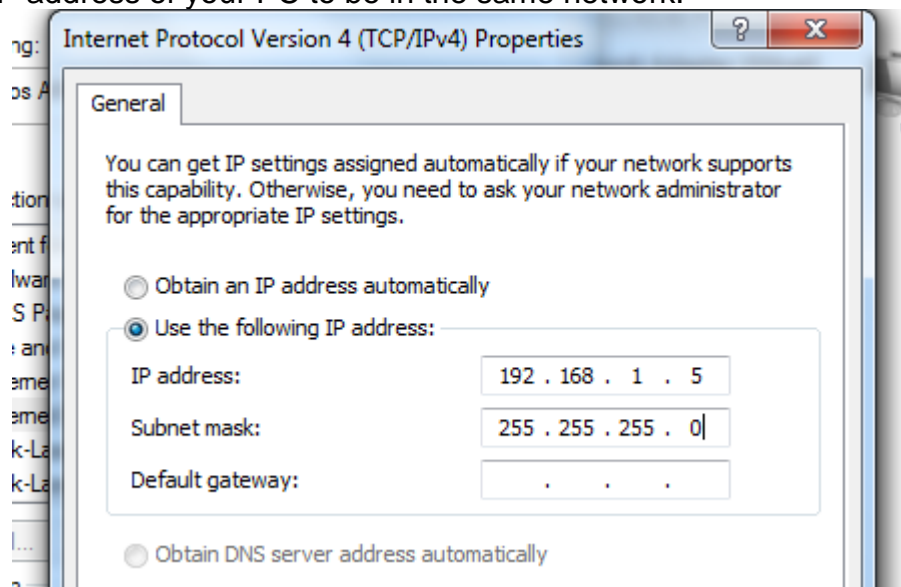


Figure 17. Set the IP address

Finally, in order to access **smartDEN IP-WatchDog** just type in your browser 192.168.1.100

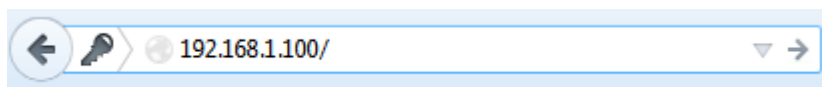
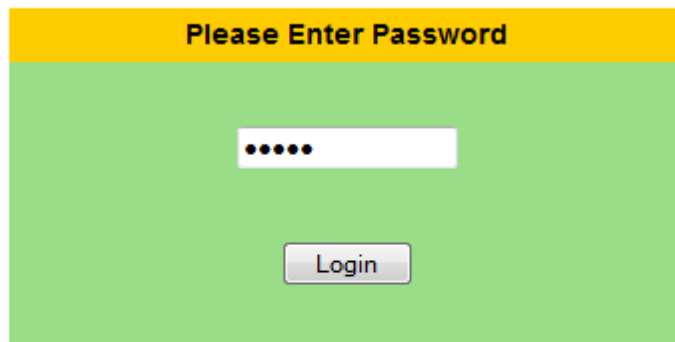


Figure 18. Open the device via browser

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



Logged out

Figure 19. Login page



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

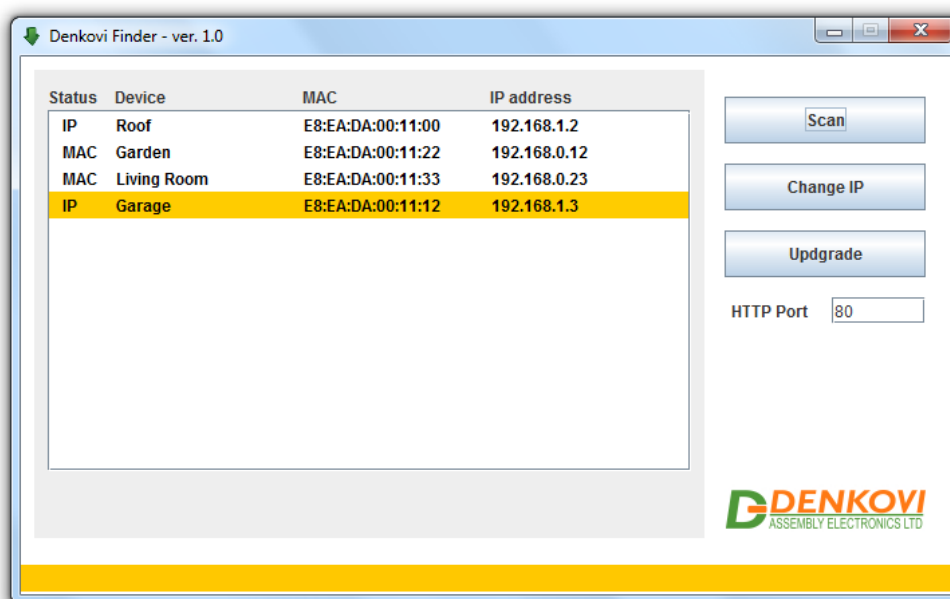


Figure 20. Denkovi Finder

6. Default Settings

6.1. Table with default settings

The **smartDEN IP-WatchDog** module is shipped with default (factory) settings shown in Table 2. The default settings can be reloaded, if necessary (see **point 6.2**).

Table 2. Default settings

Settings group	Parameter (according Web pages)	Value
General Settings	Device Name	SMARTDEN_IP-WD
	Password	admin
Network Settings	DHCP	Disabled
	IP Address	192.168.1.100
	Gateway	192.168.1.1
	Subnet Mask	255.255.255.0
	Primary DNS	192.168.1.1
	Secondary DNS	0.0.0.0
HTTP/XML/JSON Access	HTTP Port	80
	AutoReboot HTTP Port	90
	Access IP Address	192.168.1.0
	Access Mask	0.0.0.0
	Access MAC Address	00:00:00:00:00:00
	Session Timeout, min	3
	Enable Access	Yes
	Encrypt Password	No
	Multiple Access	Yes

6.2. 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 **point 6.1** from the current document.

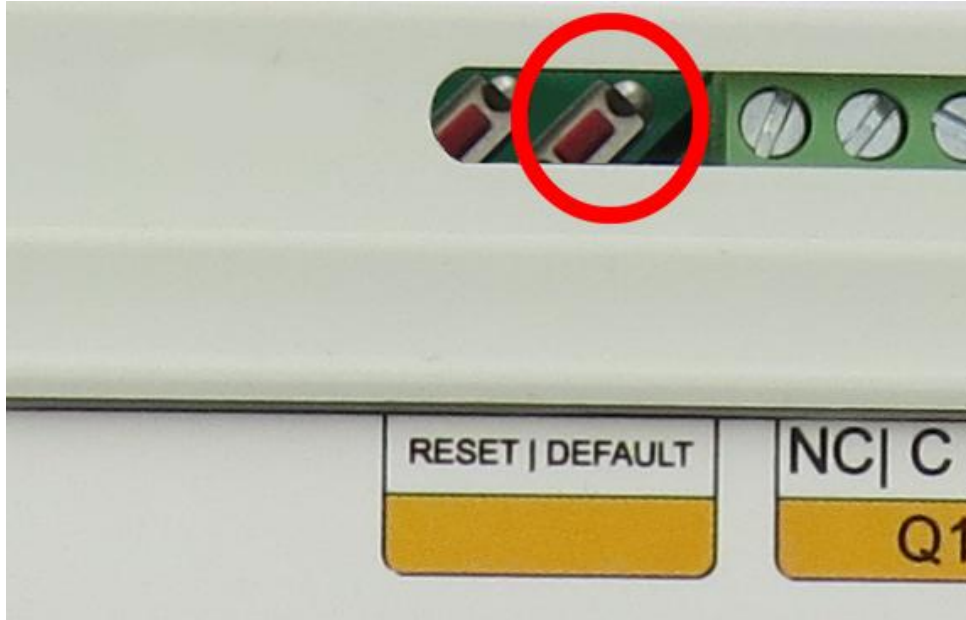


Figure 21. Loading the default settings

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 both led indicators (led1 and led2) become ON (approximately 10 sec);
5. Release the default button;
6. The module is configured with default settings.

7. Web access

smartDEN IP-WatchDog Info	
smartDEN IP-WatchDog Version	v1.21
Build Date	Jun 12 2017 00:08:00
Documentation	User Manual

Figure 22. Web access

To access the setup pages, run a web browser (Internet Explorer, Mozilla Firefox or similar), and enter the **smartDEN IP-WatchDog** IP address, for example:
<http://192.168.1.100>

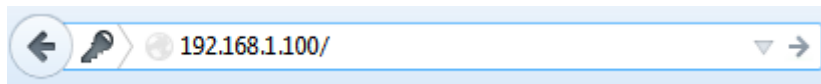
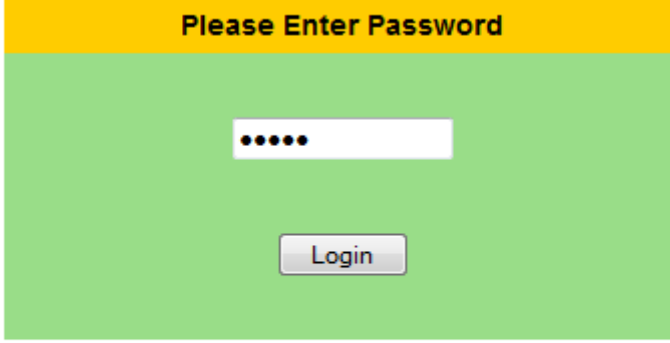


Figure 16. Open via browser

Note: You will need to have JavaScript enabled in your browser.

7.1. Login



The screenshot shows a login interface. At the top, a yellow banner contains the text "Please Enter Password". Below this, on a light green background, is a white password input field with five black dots. Underneath the input field is a grey button with the text "Login". Below the entire green area, the text "Logged out" is displayed in a light blue font.

Figure 23. Login page

Enter the password and click "Login" button. This will bring you to the **smartDEN IP-WatchDog** main configuration page which contains details for the current firmware version and build date and provides buttons and links to obtain further details.

Note: The default password is admin (passwords are case sensitive).

Note: 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.

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 IP-WatchDog** for time, specified by **Session Timeout** parameter, the session "times out" and a new login is required.

7.2. Menu

The main menu consists of the following items, located in the left window frame:

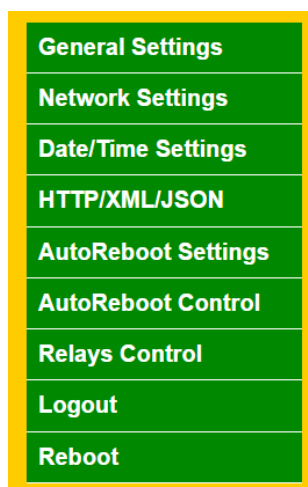


Figure 24. Navigation menu

7.3. General Settings

General Settings

General Settings	
Device Name	SMARTDEN_IP-WD
Password	*****
<input type="button" value="Save"/> <input type="button" value="Reload"/>	

Figure 25. General settings

- **Device Name:** The name of the module (max 15 symbols). Every module can have different name in your network so they can be distinguished;
- **Password:** The password used for logging into the web admin and XML operation (max. 10 chars);



When typed, the password in this screen is not hidden. Only in this case, when the password is being changed, it is transmitted across the network "in the open". Therefore, set passwords in a secure environment where you can make sure that no one is "eavesdropping". Subsequent transmissions of the password to "login" onto the device are encrypted and "safe".

- **Save button:** Once you have changed the settings as required, click this button.

7.4. Network settings

Network Configuration

Network Configuration	
MAC Address	E8:EA:DA:00:1B:18
Enable DHCP	<input type="checkbox"/>
IP Address	192.168.1.74
Gateway	192.168.1.1
Subnet Mask	255.255.255.0
Primary DNS	8.8.8.8
Secondary DNS	192.168.1.1

Figure 26. Network settings

This menu lets you configure the network settings of **smartDEN IP-WatchDog** relay module:

- **Enable DHCP:** This option allows DHCP to be enabled or disabled. If DHCP is set to Enabled, the Network page must be saved and **smartDEN IP-WatchDog** must be rebooted before obtaining an IP address;
- **IP address:** This is the IP address of the **smartDEN IP-WatchDog**. It needs to be manually assigned only if DHCP is disabled. With DHCP enabled, this field displays the currently assigned address;
- **Gateway:** This specifies the IP address of the gateway router. It is used for accessing public time servers for automatic time synchronization;
- **Subnet Mask:** This is the subnet mask for the network on which the **smartDEN IP-WatchDog** is installed;
- **Primary DNS:** Primary DNS (Domain Name Service) address;
- **Secondary DNS:** Secondary DNS address;
- **Save button:** Once you have changed the settings as required, click this button.



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

7.5. Date and Time Settings

Date/Time Settings

Date/Time Settings	
Date (dd/mm/yyyy)	<input type="text" value="08/09/2014"/>
Day of Week	<input type="text" value="Mon"/>
Time (hh:mm)	<input type="text" value="12:58"/>
Time Zone	<input type="text" value="(GMT)"/>
Auto Synchronization	<input checked="" type="checkbox"/>
Time Server	<input type="text" value="pool.ntp.org"/>
Server Port	<input type="text" value="123"/>
Synchronization Period, min	<input type="text" value="30"/>

Figure 27. Date/Time settings

This page lets you configure the following parameters related with the real time clock built-in the module:

- **Date (dd/mm/yyyy):** Enter the current date here in specified format;
- **Time (hh:mm):** Enter the current time here in 24-hour format;
- **Time Zone:** Select the time zone for your geographic location.
- **Auto Synchronization:** This option enables or disables automatic synchronization with the SNTP (Simple Network Time Protocol) server with period specified by **Synchronization Period**;
- **Time Server:** This is the SNTP server, used for synchronizing the time automatically;
- **Server Port:** SNTP server port;
- **Synchronization Period, min:** This option sets the period in which automatic synchronization will take place, if enabled;
- **Save button:** Once you have changed the settings as needed, click "**Save**". These settings apply immediately and do not require a reboot.

7.6. HTTP/XML/JSON Settings

HTTP/XML/JSON Settings

HTTP Access	
Web HTTP Port	<input type="text" value="80"/>
AutoReboot HTTP Port	<input type="text" value="90"/>
Access IP Address	<input type="text" value="192.168.1.0"/>
Access Mask	<input type="text" value="0.0.0.0"/>
Access MAC Address	<input type="text" value="00:00:00:00:00:00"/>
Session Timeout, min	<input type="text" value="3"/>
XML/JSON Access	
Enable Access	<input checked="" type="checkbox"/>
Encrypt Password	<input type="checkbox"/>
Multiple Access	<input checked="" type="checkbox"/>

Figure 28. HTTP/XML/JSON Settings

These settings let you configure the HTTP, XML and JSON access parameters of smartDEN IP-WatchDog:









- **HTTP Port:** Port that the Web server listens for HTTP requests (default port is 80). You have to reboot the device for a new port setting to apply;
- **AutoReboot HTTP Port:** HTTP port for incoming HTTP requests.
- **Access IP Address/Access Mask:** These fields can be used to restrict the HTTP/XML/JSON access by specifying the IP address and subnet mask of the HTTP client;
- **Access MAC Address:** This field can be used to restrict the HTTP/XML/JSON access by specifying the MAC address of the HTTP client;
- **Session Timeout, min:** Specifies the timeout period for HTTP, XML and JSON sessions in minutes;
- **Enable Access:** This option enables or disables XML/JSON access to the smartDEN IP-WatchDog;
- **Encrypt Password:** When XML/JSON access is enabled, this option adds additional security level by encrypting the login password;

- **Multiple Access:** This option enables simultaneous access from several HTTP/JSON clients;
- **Save button:** Once you have changed the settings as required, click this button.

Note: When **Encrypt Password** mode is enabled, the **Multiple Access** option is not taken into account and, at any given moment, only one user can be logged-in.

Note: When **Multiple Access** mode is enabled, any XML/JSON request will always reset the current HTTP session.

Note: When **Multiple Access** mode is disabled, whether **Encrypt Password** is enabled or not, it is possible to access the module via XML/JSON only after login for the specified session timeout.

-  You have to reboot the device for these settings to apply.
-  It is highly recommended to log out from the web server after finishing the parameters setup.
-  It is recommend to use different HTTP ports. In that case **AutoReboot HTTP Port** can be accessed only via index.htm, and **Web HTTP Port** all the rest pages excepting index.htm.
-  If you don't want to restrict the HTTP/XML/JSON access by IP address, set the **Access Mask** to 0.0.0.0.
-  If you don't want to restrict the HTTP/XML/JSON access by MAC address, set the **MAC Address** to 00:00:00:00:00:00.
-  Setting the **Access Mask** to 255.255.255.255 allows the HTTP/XML/JSON access only from the exactly specified **Access IP Address**.
-  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.
-  There is connection timeout for the HTTP ports. After connecting, if there is not data transmission after certain timeout the connection will be terminated. The timeout for **Web HTTP Port** is 20 sec and for the **AutoReboot HTTP Port** - 5 sec.

7.7. Auto-reboot Settings

smartDEN IP-WatchDog main feature is to be used for auto-rebooting of IP devices (servers, PC hosts, switches, cameras etc.). **smartDEN IP-WatchDog** checks the working state of the device at regular intervals by sending ping requests. After preset number of successive ping failures **smartDEN IP-WatchDog** performs a predefined reset/reboot sequence of the monitored device connected to one of the 16 relays.

AutoReboot Settings

Channel 3 Info: Reboots number: 142, Last reboot: 13/06/2017 10:12

AutoReboot Channel	3 (RELAY3) ▼	
Auto-reboot Parameters		
Description	RELAY3	
AutoReboot Enable	<input checked="" type="checkbox"/>	
Mode	Outgoing Ping ▼	
Host Address	192.168.1.191	<input type="button" value="Test"/>
Host HTTP Port	80	
Check Interval, sec	5	
Check Timeout, sec	4	
Check Failures Before Reboot	5	
Check Delay After Reboot, sec	10	
Reboot Sequence		
<input checked="" type="checkbox"/>	Power-up Pulse, sec	1
<input checked="" type="checkbox"/>	Reboot Pulse1, sec	1
<input checked="" type="checkbox"/>	Pulse1 To Pulse2 Delay, sec	1
<input checked="" type="checkbox"/>	Reboot Pulse2, sec	1

Figure 29. Auto-reboot configuration page

- **AutoReboot Channel** - select the channel (1 to 16);
- **Description** - name of the channel (max. 7 symbols);
- **AutoReboot Enable** - activate this mode;
- **Mode** - testing mode (Outgoing Ping, Incoming Ping, Outgoing HTTP, Incoming HTTP);
- **Host Address** - the address of the tested device (max 24 symbols);
- **Test** - button for host manual test in modes Outgoing Ping and Outgoing HTTP;
- **Host HTTP Port** – HTTP server port of the remote host (this makes sense only for Outgoing HTTP mode);
- **Check Interval, sec** – testing interval (period) (from 1 to 3600 seconds);
- **Check Timeout, sec** – timeout for reply receiving for modes Outgoing Ping and Outgoing HTTP (from 1 to 100 seconds);
- **Check Failures Before Reboot** – the number of consecutive failures before reboot;
- **Check Delay After Reboot, sec** – the waiting period after reboot that should pass before the device is checked again (from 1 to 3600 seconds);
- **Power-up Pulse, sec** – if checked, the **smartDEN IP-WatchDog** will generate a pulse at power-up. This, for example can be used to switch on the device. This parameter can be set from 1 to 3600 seconds;
- **Reboot Pulse1, sec** - if checked, the **smartDEN IP-WatchDog** will generate a pulse when the reboot condition is detected. This can be used to switch off or reset the device. Range is from 1 to 3600 seconds;
- **Pulse1 To Pulse2 Delay, sec** - if the device is switched off by Pulse1, the **smartDEN IP-WatchDog** will wait before generating Pulse2 to switch it on. This delay can be set from 1 to 3600 seconds;
- **Reboot Pulse2, sec** - if checked, the **smartDEN IP-WatchDog** will generate a second pulse to switch it on the device.



The reboot circuit can be wired to common (C) and normally open (NO) or normally closed (NC) contacts. Relay state “ON” means that the NO contacts are closed and the NC contacts are open. Relay state “OFF” means that the NO contacts are open and the NC contacts are closed.



When the relay is wired in series with the power circuit of the device, the C and NC contacts should be used.



When the relay is wired in parallel with the “reset” or “power on/off” button the device, the C and NO contacts should be used.



When the associated relay is working in auto-reboot mode, when it is set ON via web browser, XML, JSON, SNMP it will perform the reboot sequence.



“Pulse” means that the relay switches ON for defined time and then switches OFF.



If the reboot circuit is wired in parallel to “reset” button of the device, only **Reboot Pulse1** option can be checked.



If the relay is wired in series with the power circuit of the device, only **Reboot Pulse1** option can be checked (the device is switched off when the relay is ON).



If the reboot circuit is wired in parallel to “power on/off” button of the device, **Reboot Pulse1**, **Pulse1 To Pulse2 Delay** and **Reboot Pulse2**, options can be checked.



If certain channel is working in outgoing mode and at the moment it is performing request (it is waiting timeout of the reply) the disabling via **AutoReboot Enable** will not be executed.

7.7.1. Outgoing Ping Mode

It is possible the **Host Address** to be IP address (192.168.1.1 for example) or name (using DNS, for example www.google.com).

smartDEN IP-WatchDog sends PING requests to the target host during some interval (Check Interval). For every request it is waiting **Check Timeout** before failure to be recorded. When they are detected **Check Failures Before Reboot** consecutive failures, it is preformed reboot procedure.

7.7.2. Incoming Ping Mode

It is possible the **Host Address** to be IP address only (192.168.1.1 for example).

smartDEN IP-WatchDog expects PING requests from the target host. If there aren't incoming requests during the period given by **Check Interval** a failure is detected. When they are detected **Check Failures Before Reboot** consecutive failures, it is preformed reboot procedure.

7.7.3. Outgoing HTTP Mode

It is possible the **Host Address** to be IP address (192.168.1.1 for example) or name (using DNS, for example www.google.com).

smartDEN IP-WatchDog sends HTTP GET requests to index.html during the period (**Check Interval**). For every request it is waiting **Check Timeout** before failure to be recorded. When they are detected **Check Failures Before Reboot** consecutive failures, it is preformed reboot procedure.

7.7.4. Incoming HTTP Mode

It is possible the **Host Address** to be IP address only (192.168.1.1 for example).

smartDEN IP-WatchDog expects HTTP GET requests from the target host to page index.html. If there aren't incoming requests during the period given by **Check**

Interval a failure is detected. When they are detected **Check Failures Before Reboot** consecutive failures, it is preformed reboot procedure.

7.8. AutoReboot Control

From this page it is possible to monitor and control the channels working in Autoreboot mode.

AutoReboot Control

No	Description	Mode	Host Address	Reboots Number	Last Reboot	Check Failures	Current State	Next Check, sec	Reboot now
1	RELAY12	Outgoing Ping	www.abv.bg	0		0	Checking Pause	6	Reboot
2	DELLPC	Disabled	192.168.1.43	0		0	Idle	-	Reboot
3	RELAY3	Outgoing Ping	192.168.1.191	183	13/06/2017 10:40	3	Checking...	-	Reboot
4	RELAY4	Disabled	0.0.0.0	0		0	Idle	-	Reboot
5	RELAY5	Disabled	0.0.0.0	0		0	Idle	-	Reboot
6	RELAY6	Disabled	0.0.0.0	0		0	Idle	-	Reboot
7	R.Ping	Disabled	192.168.1.1	0		0	Idle	-	Reboot
8	RELAY8	Disabled	192.168.1.28	0		0	Idle	-	Reboot
9	R.HTTP	Outgoing HTTP	192.168.1.1	0		0	Checking Pause	6	Reboot
10	RELAY10	Disabled	0.0.0.0	0		0	Idle	-	Reboot
11	RELAY11	Disabled	0.0.0.0	0		0	Idle	-	Reboot
12	RELAY12	Incoming Ping	192.168.1.137	17	13/06/2017 10:35	0	Delay After Reboot	13	Reboot
13	RELAY13	Incoming HTTP	192.168.1.137	73	13/06/2017 10:40	0	Reboot Pulse1	-	Reboot
14	RELAY14	Outgoing Ping	1.2.3.4	12	13/06/2017 10:31	4	Checking Pause	49	Reboot
15	den.htt	Outgoing HTTP	www.denkovi.com	0		0	Checking Pause	8	Reboot
16	DELLPC	Outgoing Ping	192.168.1.43	0		0	Checking Pause	7	Reboot

Color Legend

OK	Rebooted at least once	Current check failures	Channel is disabled
----	------------------------	------------------------	---------------------

Figure 30. AutoReboot Control

- **Description** – name and shortcut to the configuration page;
- **Reboots Number** – reboots number;
- **Check Failures** – current consecutive failures number;
- **Current State:**
 - Idle – channel is not used;
 - Power-up Pulse – it is performed Power-up Pulse;
 - Delay After Reboot – in waiting state after the previous reboot;
 - Checking Pause – pause (interval) between checks;
 - Checking... – checking, it is waiting for reply for the outgoing modes;
 - Wait for request... – it is waiting request for the incoming modes;
 - Reboot Pulse1 - it is performed Reboot Pulse1;
 - Pulse1/Pulse2 Pause – pause between Pulse1 and Pulse2;
 - Reboot Pulse2 - it is performed Reboot Pulse2;
- **Next Check, sec** – seconds until the next check (they are displayed only for states Delay After Reboot, Checking Pause and Wait for request);
- **Reboot now** – command for manual reboot with the given pulse sequence;

They are used the following colors:

- **green** – the device is not rebooted (Reboots Number = 0), there are not any current consecutive failures (Check Failures = 0);

- **yellow** – the device is rebooted (Reboots Number > 0), there are not any current consecutive failures (Check Failures = 0);
- **red** – there are current consecutive failures (Check Failures = 0);
- **gray** – Autoreboot mode is disabled.

7.9. Monitoring and control

Relays Control

Relays (1..8)							
RELAY1	RELAY2	RELAY3	RELAY4	RELAY5	RELAY6	RELAY7	RELAY8
Off ▾	On ▾	Off ▾	Off ▾	On ▾	Off ▾	Off ▾	Off ▾
Relays (9..16)							
RELAY9	RELAY10	RELAY11	RELAY12	RELAY13	RELAY14	RELAY15	RELAY16
Off ▾	Off ▾	Off ▾	Off ▾	Off ▾	Off ▾	Off ▾	Off ▾

Figure 31. Monitoring and control

This page provides monitoring and control of the **smartDEN IP-WatchDog** relays. From here you can control/monitor the relays (only those one who are in manual mode).

7.10. Logout

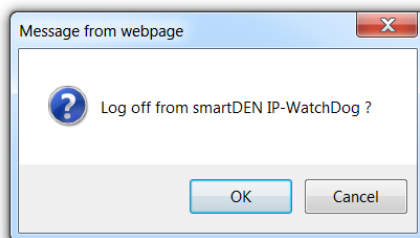


Figure 32. Log off

7.11. Reboot

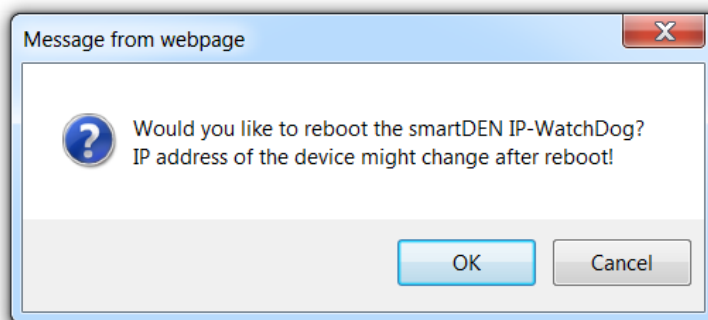


Figure 33. Reboot

8. HTTP/XML/JSON access

This operation mode allows custom applications to control the **smartDEN IP-WatchDog** without using a Web-browser. The custom application acts as a HTTP client, sending HTTP GET requests to the **smartDEN IP-WatchDog**.

To receive the current state of the **smartDEN IP-WatchDog**, the application requests the page *current_state.xml* (*current_state.json*), for example:

http://192.168.1.100/current_state.xml

http://192.168.1.100/current_state.json

The custom application can also control the **smartDEN IP-WatchDog** by sending parameters (name/value pairs) with the HTTP/XML/JSON GET request, for example:

http://192.168.1.100/current_state.xml?Relay=1&Relay2=0&Relay3=1

http://192.168.1.100/current_state.json?Relay=1&Relay2=0&Relay3=1

The XML/JSON login process differs depending on the selected **Encrypt Password** option.

8.1. Login (Encrypted Password)

In this mode a two-step login sequence is provided as a protection against unauthorized access. The first time the custom application requests the page *current_state.xml* / *current_state.json*, a random login key is issued in the reply. Next the custom application uses this key to encrypt the password. The encrypted password is sent as a parameter with the next request to the page *current_state.xml* / *current_state.json*.

Bellow is an example of login process:

Step 1:

Request

http://192.168.1.100/current_state.xml

Reply (login required):

```
<CurrentState>  
<LoginKey>65156</LoginKey>  
</CurrentState>
```

http://192.168.1.100/current_state.json

Reply (login required):

```
{"CurrentState": {"LoginKey": "65156"}}
```

Step 2:

Request (password is sent as a parameter)

http://192.168.1.100/current_state.xml?pw=28237099263eabfd88626124a822c64c

Reply (password is O'K, login accepted):

```

- <CurrentState>
  + <Channel1></Channel1>
  + <Channel2></Channel2>
  + <Channel3></Channel3>
  + <Channel4></Channel4>
  + <Channel5></Channel5>
  + <Channel6></Channel6>
  + <Channel7></Channel7>
  + <Channel8></Channel8>
  + <Channel9></Channel9>
  + <Channel10></Channel10>
  + <Channel11></Channel11>
  + <Channel12></Channel12>
  + <Channel13></Channel13>
  + <Channel14></Channel14>
  + <Channel15></Channel15>
- <Channel16>
  <Name>DELLPC</Name>
  <Mode>Outgoing Ping</Mode>
  <HostAddress>192.168.1.43</HostAddress>
  <RebootsNumber>0</RebootsNumber>
  <LastReboot> </LastReboot>
  <CheckFailures>0</CheckFailures>
  <CurrentState>Checking Pause</CurrentState>
  <NextCheck>20</NextCheck>
  <RelayState>0</RelayState>
  </Channel16>
+ <Device></Device>
</CurrentState>

```

or

http://192.168.1.100/current_state.json?pw=28237099263eabfd88626124a822c64c

```
{
  "CurrentState": {
    "Channel": [
      {
        "Name": "RELAY12", "Mode": "Outgoing Ping", "HostAddress": "www.abv.bg", "RebootsNumber": "0", "LastReboot": " ", "CheckFailures": "0",
        "Name": "DELLPC", "Mode": "Disabled", "HostAddress": "192.168.1.43", "RebootsNumber": "0", "LastReboot": " ", "CheckFailures": "0", "Current!": "0",
        "Name": "RELAY3", "Mode": "Outgoing Ping", "HostAddress": "192.168.1.191", "RebootsNumber": "257", "LastReboot": "13/06/2017 11:31", "Current!": "0",
        "Name": "RELAY4", "Mode": "Disabled", "HostAddress": "0.0.0.0", "RebootsNumber": "0", "LastReboot": " ", "CheckFailures": "0", "Current!": "0",
        "Name": "RELAY5", "Mode": "Disabled", "HostAddress": "0.0.0.0", "RebootsNumber": "0", "LastReboot": " ", "CheckFailures": "0", "Current!": "0",
        "Name": "RELAY6", "Mode": "Disabled", "HostAddress": "0.0.0.0", "RebootsNumber": "0", "LastReboot": " ", "CheckFailures": "0", "Current!": "0",
        "Name": "R.Ping", "Mode": "Disabled", "HostAddress": "192.168.1.1", "RebootsNumber": "0", "LastReboot": " ", "CheckFailures": "0", "Current!": "0",
        "Name": "RELAY8", "Mode": "Disabled", "HostAddress": "192.168.1.28", "RebootsNumber": "0", "LastReboot": " ", "CheckFailures": "0", "Current!": "0",
        "Name": "R.HTTP", "Mode": "Outgoing HTTP", "HostAddress": "192.168.1.1", "RebootsNumber": "0", "LastReboot": " ", "CheckFailures": "0", "Current!": "0",
        "Name": "RELAY10", "Mode": "Disabled", "HostAddress": "0.0.0.0", "RebootsNumber": "0", "LastReboot": " ", "CheckFailures": "0", "Current!": "0",
        "Name": "RELAY11", "Mode": "Disabled", "HostAddress": "0.0.0.0", "RebootsNumber": "0", "LastReboot": " ", "CheckFailures": "0", "Current!": "0",
        "Name": "RELAY12", "Mode": "Incoming Ping", "HostAddress": "192.168.1.137", "RebootsNumber": "24", "LastReboot": "13/06/2017 11:27", "Current!": "0",
        "Name": "RELAY13", "Mode": "Incoming HTTP", "HostAddress": "192.168.1.137", "RebootsNumber": "102", "LastReboot": "13/06/2017 11:31", "Current!": "0",
        "Name": "RELAY14", "Mode": "Outgoing Ping", "HostAddress": "1.2.3.4", "RebootsNumber": "17", "LastReboot": "13/06/2017 11:22", "CheckFailures": "0",
        "Name": "den.htt", "Mode": "Outgoing HTTP", "HostAddress": "www.denkovi.com", "RebootsNumber": "0", "LastReboot": " ", "CheckFailures": "0",
        "Name": "DELLPC", "Mode": "Outgoing Ping", "HostAddress": "192.168.1.43", "RebootsNumber": "0", "LastReboot": " ", "CheckFailures": "0"
      ]
    ],
    "Device": {
      "Name": "SMARTDEN_IP-WD",
      "MAC": "E8:EA:DA:00:18:18",
      "sysUpTime": "169636"
    }
  }
}
```



Password encryption algorithm to be implemented in custom application is available upon request.

8.2. Login (Non-Encrypted Password)

In this mode the password is passed as non-encrypted parameter with the request:

http://192.168.1.100/current_state.xml?pw=admin

http://192.168.1.100/current_state.json?pw=admin

Getting the <LoginKey> in the answer in this mode means only that the provided password is wrong or the login session has been expired.



If there is no data traffic between the custom application and the **smartDEN IP-WatchDog** for time, specified by **Session Timeout** parameter, the session "times out" and a new login is required.

8.3. Getting the current state

After a login the custom application can obtain the **smartDEN IP-WatchDog** current state by a request to the page *current_state.xml* / *current_state.json* :

http://192.168.1.100/current_state.xml

The reply contains page in XML format:

```
- <CurrentState>
  + <Channel1></Channel1>
  + <Channel2></Channel2>
  + <Channel3></Channel3>
  + <Channel4></Channel4>
  + <Channel5></Channel5>
  + <Channel6></Channel6>
  + <Channel7></Channel7>
  + <Channel8></Channel8>
  + <Channel9></Channel9>
  + <Channel10></Channel10>
  + <Channel11></Channel11>
  + <Channel12></Channel12>
  + <Channel13></Channel13>
  + <Channel14></Channel14>
  + <Channel15></Channel15>
- <Channel16>
  <Name>DELLPC</Name>
  <Mode>Outgoing Ping</Mode>
  <HostAddress>192.168.1.43</HostAddress>
  <RebootsNumber>0</RebootsNumber>
  <LastReboot> </LastReboot>
  <CheckFailures>0</CheckFailures>
  <CurrentState>Checking Pause</CurrentState>
  <NextCheck>20</NextCheck>
  <RelayState>0</RelayState>
</Channel16>
+ <Device></Device>
</CurrentState>
```

http://192.168.1.100/current_state.json

The reply contains page in JSON format:

```
{
  "CurrentState": {
    "Channel": [
      {"Name": "RELAY12", "Mode": "Outgoing Ping", "HostAddress": "www.abv.bg", "RebootsNumber": "0", "LastReboot": " ", "CheckFailures": "0", "Current!": "0"},
      {"Name": "DELLPC", "Mode": "Disabled", "HostAddress": "192.168.1.43", "RebootsNumber": "0", "LastReboot": " ", "CheckFailures": "0", "Current!": "0"},
      {"Name": "RELAY3", "Mode": "Outgoing Ping", "HostAddress": "192.168.1.191", "RebootsNumber": "257", "LastReboot": "13/06/2017 11:31", "CheckFailures": "0", "Current!": "0"},
      {"Name": "RELAY4", "Mode": "Disabled", "HostAddress": "0.0.0.0", "RebootsNumber": "0", "LastReboot": " ", "CheckFailures": "0", "Current!": "0"},
      {"Name": "RELAY5", "Mode": "Disabled", "HostAddress": "0.0.0.0", "RebootsNumber": "0", "LastReboot": " ", "CheckFailures": "0", "Current!": "0"},
      {"Name": "RELAY6", "Mode": "Disabled", "HostAddress": "0.0.0.0", "RebootsNumber": "0", "LastReboot": " ", "CheckFailures": "0", "Current!": "0"},
      {"Name": "R.Ping", "Mode": "Disabled", "HostAddress": "192.168.1.1", "RebootsNumber": "0", "LastReboot": " ", "CheckFailures": "0", "Current!": "0"},
      {"Name": "RELAY8", "Mode": "Disabled", "HostAddress": "192.168.1.28", "RebootsNumber": "0", "LastReboot": " ", "CheckFailures": "0", "Current!": "0"},
      {"Name": "R.HTTP", "Mode": "Outgoing HTTP", "HostAddress": "192.168.1.1", "RebootsNumber": "0", "LastReboot": " ", "CheckFailures": "0", "Current!": "0"},
      {"Name": "RELAY10", "Mode": "Disabled", "HostAddress": "0.0.0.0", "RebootsNumber": "0", "LastReboot": " ", "CheckFailures": "0", "Current!": "0"},
      {"Name": "RELAY11", "Mode": "Disabled", "HostAddress": "0.0.0.0", "RebootsNumber": "0", "LastReboot": " ", "CheckFailures": "0", "Current!": "0"},
      {"Name": "RELAY12", "Mode": "Incoming Ping", "HostAddress": "192.168.1.137", "RebootsNumber": "24", "LastReboot": "13/06/2017 11:27", "CheckFailures": "0", "Current!": "0"},
      {"Name": "RELAY13", "Mode": "Incoming HTTP", "HostAddress": "192.168.1.137", "RebootsNumber": "102", "LastReboot": "13/06/2017 11:31", "CheckFailures": "0", "Current!": "0"},
      {"Name": "RELAY14", "Mode": "Outgoing Ping", "HostAddress": "1.2.3.4", "RebootsNumber": "17", "LastReboot": "13/06/2017 11:22", "CheckFailures": "0", "Current!": "0"},
      {"Name": "den.htt", "Mode": "Outgoing HTTP", "HostAddress": "www.denkovi.com", "RebootsNumber": "0", "LastReboot": " ", "CheckFailures": "0", "Current!": "0"},
      {"Name": "DELLPC", "Mode": "Outgoing Ping", "HostAddress": "192.168.1.43", "RebootsNumber": "0", "LastReboot": " ", "CheckFailures": "0", "Current!": "0"}
    ],
    "Device": {
      "Name": "SMARTDEN_IP-WD",
      "MAC": "E8:EA:DA:00:18:18",
      "sysUpTime": "169636"
    }
  }
}
```

8.4. Multiple XML Access

In this mode the password should be passed as non-encrypted parameter with each request:

http://192.168.1.100/current_state.xml?pw=admin&Relay1=1

http://192.168.1.100/current_state.json?pw=admin&Relay1=1



Multiple XML/JSON Access is not allowed when **Encrypt Password** option is enabled.

8.5. Parameters

After a login the custom application can also control the **smartDEN IP-WatchDog** by sending parameters (name/value pairs) with the HTTP GET request.

Valid parameters and values are shown in the bellow table.

Table 3. Valid HTTP parameters

Name	Value	Description
Relay <i>i</i>	0...1	Relay <i>i</i> value (<i>i</i> =1...16)
SetAll	0...65535	Set all the relays with single command
pw	password	Required at login



If the channel is in Autoreboot, with 'Relay*i*=1' it will be started the sequence of reboot. In this mode 'Relay*i*=0' does not lead to turning off the relay (it will be turned off after the sequence is finished).
 If the Autoreboot mode is disabled for this channel, the relay can be turned on/off with 1/0.

9. Auto-Reboot mode specifics

There is only one "socket" for outgoing PING, which is used sequentially for all channels, configured in this mode. This means if some channel waits for timeout from unresponsive device and in this moment the next channel has to perform outgoing PING, then the timeout will be waited.

There are 7 "sockets" for outgoing HTTP requests, which are used by all channels, configured in this mode. If all the sockets are busy, the next channel will have to wait for free socket.

The incoming PING and HTTP requests are processed in parallel.



It is recommend the Web HTTP server port and outgoing HTTP testing to be separated, which means they must be on different ports.

10. Security considerations

The **smartDEN IP-WatchDog** runs a special firmware and do not have a general-purpose operating system. 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 IP-WatchDog** does not run protocols such as Telnet and FTP which may have the potential for security breach. The only exception from this is the SNMPv1 protocol, that can be disabled.

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 Setting** form. Therefore, you must set passwords in the secure environment where you can make sure that no one is "eavesdropping".

SNMP communication

SNMPv1 does not implement encryption. Authentication of clients is performed only by a "community string", which is transmitted in clear text. SNMP communication should be used in trusted networks and disabled if not used.

XML/JSON operation

A challenge-response authentication can be used in login process. The password can be transmitted by custom application across the network in encrypted form.



Web and XML/JSON access can be restricted by IP Address (range of IP Addresses) or by MAC Address.

11. Appendix 1. Settings for different hardware connection modes

11.1. Settings for connection "In parallel of the PC reset switch"

It is used NO and C of the relay channel. In this mode upon relay activation, it is imitated "Reset" button pressing. It is necessary to set only **Reboot Pulse1** or **Reboot Pulse2**.

Reboot Sequence		
<input type="checkbox"/>	Power-up Pulse, sec	10
<input type="checkbox"/>	Reboot Pulse1, sec	20
<input type="checkbox"/>	Pulse1 To Pulse2 Delay, sec	10
<input checked="" type="checkbox"/>	Reboot Pulse2, sec	5

Figure 34. Settings for "in parallel of "PC" reset switch"

11.2. Settings for connection "In parallel of the PC power ON/OFF switch"

It is used NO and C of the relay channel. In this mode upon relay activation, it is imitated "Power ON/OFF" button pressing. It is necessary to set only **Reboot Pulse1**, **Pulse1 to Pulse2 Delay** and **Reboot Pulse2**. In that case Reboot Pulse1 imitate pressing the "Power OFF" button and after pause with **Reboot Pulse2** it is imitating Power ON pressing.

If **smartDEN IP-WatchDog** and the tested device are with common power supply, then it is necessary to set and **Power-up Pulse** for initial turn-on of the device (Power ON) after supplying.

Reboot Sequence		
<input type="checkbox"/>	Power-up Pulse, sec	10
<input type="checkbox"/>	Reboot Pulse1, sec	20
<input type="checkbox"/>	Pulse1 To Pulse2 Delay, sec	10
<input checked="" type="checkbox"/>	Reboot Pulse2, sec	5

Figure 35. Settings for "in parallel of "PC" reset switch"

11.3. Settings for connection "In sequence of the power supply cable"

It is used NC and C of the relay channel. When the relay is activated, the power supply is turned off. It is necessary to set only **Reboot Pulse1** or **Reboot Pulse2**.

Reboot Sequence		
<input type="checkbox"/>	Power-up Pulse, sec	10
<input checked="" type="checkbox"/>	Reboot Pulse1, sec	10
<input type="checkbox"/>	Pulse1 To Pulse2 Delay, sec	10
<input type="checkbox"/>	Reboot Pulse2, sec	5

Figure 36. Settings for "in sequence of the power supply cable"

12. Appendix 2. Dimensions

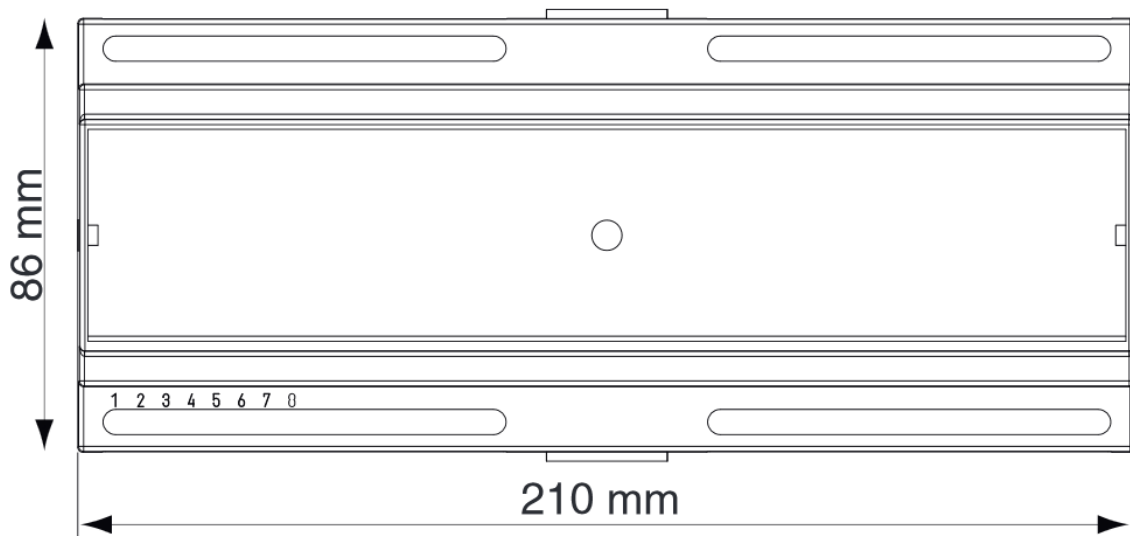


Figure 37. Dimensions