1. [Docs] UniPing server solution v4/SMS & UniPing server solution v3 . . . 3
1.1 [ENG] UniPing server solution v4/SMS & UniPing server solution v3, User guide . . . 4
1.1.1 [USS] Introduction . . . 5
1.1.2 [USS] Copyright and Disclaimer . . . 6
1.1.3 [USS] A Device Overview . . . 7
1.1.4 [USS] Sockets and Indication Elements . . . 9
1.1.5 [USS] Installing and Removing a SIM Card . . . 17
1.1.6 [USS] Using IO Lines to Control External Devices (in the «Output» Mode) . . . 20
1.1.7 [USS] Sensors Plugin . . . 22
1.1.8 [USS] Setting Parameters to Default Values (to the Factory Settings) . . . 28
1.1.9 [USS] Shipping Kit . . . 29
1.1.10 [USS] Warranty . . . 31
1.1.11 [USS] Operating and Storage Conditions . . . 32
1.1.12 [USS] Safety Precautions . . . 33
1.1.13 [USS] Where to Get a Document of a Firmware Description? . . . 34
1.1.14 [USS] Additional Documents and Links . . . 35
1.2 [ENG] [DKSF 70/71.7 IU] UniPing server solution v4/SMS & UniPing server solution v3, Firmware description . . . 36
1.2.1 [ENG] 1. [DKSF 70/71.7 IU] Introduction . . . 37
1.2.2 [ENG] 2. [DKSF 70/71.7 IU] Getting Basic Information about a Device . . . 38
1.2.2.1 [ENG] 2.1. [DKSF 70/71.7 IU] How to Know a Default IP Address and a MAC Address of a Device? . . . 39
1.2.2.2 [ENG] 2.2. [DKSF 70/71.7 IU] Default User Name and Password . . . 41
1.2.2.3 [ENG] 2.3. [DKSF 70/71.7 IU] Connecting to the Web Interface of a Device with a Default Authentication . . . 42
1.2.2.4 [ENG] 2.4. [DKSF 70/71.7 IU] I Need to Know the Firmware and Hardware Versions, and a Serial Number of a Device . . . 43
1.2.2.5 [ENG] 2.5. [DKSF 70/71.7 IU] How to See the Uptime? . . . 44
1.2.2.6 [ENG] 2.6 [DKSF 70/71.7 IU] Where Can I see the Hostname, Location, and Contacts of a Device? . . . 45
1.2.2.7 [ENG] 2.7. [DKSF 70/71.7 IU] How to Restart the Firmware of a Device? . . . 46
1.2.3 [ENG] 3. [DKSF 70/71.7 IU] Basic Configuration . . . 47
1.2.3.1 [ENG] 3.1. [DKSF 70/71.7 IU] How to Set up a Hostname, Location, and Contacts of a Device? . . . 48
1.2.3.2 [ENG] 3.2. [DKSF 70/71.7 IU] Where Can I Change the Settings of the Network Interface? . . . 49
1.2.3.3 [ENG] 3.3. [DKSF 70/71.7 IU] Changing a Username and a Password . . . 50
1.2.3.4 [ENG] 3.4. [DKSF 70/71.7 IU] How to Set the Community for SNMP? . . . 51
1.2.3.5 [ENG] 3.5. [DKSF 70/71.7 IU] How to Restrict the Access to a Device? . . . 52
1.2.3.6 [ENG] 3.6. [DKSF 70/71.7 IU] There Is a Need to Send SNMP Trap-Notifications. How Can I Configure This? 53 53
1.2.3.7 [ENG] 3.7. [DKSF 70/71.7 IU] How to Set the Clock? . . . 54
1.2.3.8 [ENG] 3.8. [DKSF 70/71.7 IU] I Want to Configure SYSLOG. How Can I Do This? . . . 56
1.2.3.9 [ENG] 3.9. [DKSF 70/71.7 IU] How to Receive Notifications and Reports via Email? . . . 57
1.2.3.10 [ENG] 3.10. [DKSF 70/71.7 IU] How to Update the Firmware of the Device? . . . 59
1.2.3.11 [ENG] 3.11. [DKSF 70/71.7 IU] The Log of a Device . . . 60
1.2.3.12 [ENG] 3.12. [DKSF 70/71.7 IU] How to Disable All Notifications Quickly? . . . 62
1.2.3.13 [ENG] 3.13. [DKSF 70/71.7 IU] Backing up and Restoring a Device Configuration . . . 63
1.2.4 [ENG] 4. [DKSF 70/71.7 IU] Working with Temperature Sensors . . . 64
1.2.4.1 [ENG] 4.1. [DKSF 70/71.7 IU] Which Temperature Sensors Are Supported by a Device? . . . 65
1.2.4.2 [ENG] 4.2. [DKSF 70/71.7 IU] How to Detect a Unique Id Number of a 1-Wire Temperature Sensor? . . . 66
1.2.4.3 [ENG] 4.3. [DKSF 70/71.7 IU] Where to See the Current Temperature? . . . 67
1.2.4.4 [ENG] 4.4. [DKSF 70/71.7 IU] Is It Possible to Set a Description for Temperature Sensors? . . . 68
1.2.4.5 [ENG] 4.5. [DKSF 70/71.7 IU] Setting Up the Top and the Bottom Margins of the Norm for the Temperature Sensor . . . 69
1.2.4.6 [ENG] 4.6. [DKSF 70/71.7 IU] I Want to Configure Sending the Notifications When a Status of a Temperature Sensor Is Changed. How to Do This? . . . 70
1.2.5 [ENG] 5. [DKSF 70/71.7 IU] Working with Humidity Sensors . . . 71
1.2.5.1 [ENG] 5.1. [DKSF 70/71.7 IU] Which Humidity Sensors Are Supported by a Device? . . . 72
1.2.5.2 [ENG] 5.2. [DKSF 70/71.7 IU] How to Determine a Unique Id of a 1-Wire Humidity Sensor? . . . 73
1.2.5.3 [ENG] 5.3. [DKSF 70/71.7 IU] Initial Configuration of Humidity Sensors . . . 74
1.2.5.4 [ENG] 5.4. [DKSF 70/71.7 IU] Viewing Readings and Configuring Parameters of Humidity Sensors in a Web Interface . . . 75
1.2.5.5 [ENG] 5.5. [DKSF 70/71.7 IU] Is It Possible to Set Up a Description for Humidity Sensors? . . . 76
1.2.5.6 [ENG] 5.6. [DKSF 70/71.7 IU] I Want to Configure Sending Notifications When a Status of a Humidity Sensor Is Changed. How Can I Do That? . . . 77
1.2.6 [ENG] 6. [DKSF 70/71.7 IU] Working with a Built-In Relay . . . 79
1.2.6.1 [ENG] 6.1. [DKSF 70/71.7 IU] Manual Relay Management Using a Web Interface . . . 80
1.2.6.2 [ENG] 6.2. [DKSF 70/71.7 IU] I Want to Configure Sending Notifications about Events when a Relay Is Switched. How Can I Do This? . . . 81
1.2.6.3 [ENG] 6.3. [DKSF 70/71.7 IU] What Is «Watchdog» and How Can It Be Configured? . . . 83
1.2.6.4 [ENG] 6.4. [DKSF 70/71.7 IU] What Is a «Schedule» and How to Configure It? . . . 85
1.2.7 [ENG] 7. [DKSF 70/71.7 IU] Working with the Channels of the Discrete Input-Output . . . 87
1.2.7.1 [ENG] 7.1. [DKSF 70/71.7 IU] How to Avoid the Necessity to Remember Numbers of Input-Output Lines in Notifications? . . . 88
1.2.7.2 [ENG] 7.2. [DKSF 70/71.7 IU] Configuring an Operation Mode for an Input-Output Line . . . 89
1.2.7.3 [ENG] 7.3. [DKSF 70/71.7 IU] How to Determine a Current Logic Level of an Input-Output Line? . . . 90
1.2.7.4 [ENG] 7.4. [DKSF 70/71.7 IU] How to Control an Input-Output Line in an «Output» Mode? . . . 91

1.2.7.5 [ENG] 7.5. [DKSF 70/71.7 IU] I Want to Configure Sending Notifications when a Logic Level of an IO Line Is Changed. How to Do This? . . . 92
1.2.7.6 [ENG] 7.6. [DKSF 70/71.7 IU] What do I need a Filter out short noise pulses in DISCRETE IO Line Settings for? . . . 94
1.2.8 [ENG] 8. [DKSF 70/71.7 IU] Work with an analog smoke sensor (current sensor) . . . 95
1.2.8.1 [ENG] 8.1. [DKSF 70/71.7 IU] The View of a Sensor Status . . . 96
1.2.8.2 [ENG] 8.2. [DKSF 70/71.7 IU] MONITORING SETUP: Alert, Broken Loop, Short in the Loop . . . 97
1.2.8.3 [ENG] 8.3. [DKSF 70/71.7 IU] I want to configure Notification on Status Change for the Smoke Sensor. How can I do it? . . . 98
1.2.8.4 [ENG] 8.4. [DKSF 70/71.7 IU] The Configuration of Loop Power . . . 99
1.2.9 [ENG] 9. [DKSF 70/71.7 IU] Work with 1-Wire Smore Sensors . . . 100
1.2.10 [ENG] 10. [DKSF 70/71.7 IU] Work with the NetPing Power Quality Monitoring Sensor 1-Wire . . . 101
1.2.11 [ENG] 11. [DKSF 70/71.7 IU] Work With SMS-Messages and Built-In GSM-Modem . . . 102
1.2.11.1 [ENG] 11.1. [DKSF 70/71.7 IU] How to Find Out a USSD Balance on a SIM-Card? . . . 103
1.2.11.2 [ENG] 11.2. [DKSF 70/71.7 IU] I Need to Configure the Numbers to Send SMS-Notifications. How Can I do This? . . . 104
1.2.11.3 [ENG] 11.3. [DKSF 70/71.7 IU] How Can I Enable an Extended Log for a GSM-Modem? . . . 105
1.2.11.4 [ENG] 11.4. [DKSF 70/71.7 IU] The GSM-Signal Strength Checking . . . 106
1.2.11.5 [ENG] 11.5. [DKSF 70/71.7 IU] The Receiving of SMS-Notifications by Watchdog Events . . . 107
1.2.11.6 [ENG] 11.6. [DKSF 70/71.7 IU] GSM Modem Troubleshooting . . . 108
1.2.11.7 [ENG] 11.7. [DKSF 70/71.7 IU] What kinds of SMS Notifications can this Device Send? . . . 109
1.2.11.8 [ENG] 11.8. [DKSF 70/71.7 IU] How Can I Control the Device using SMS Commands? . . . 112
1.2.11.9 [ENG] 11.9. [DKSF 70/71.7 IU] Setting the Time for Sending a Summary Report About the Status of Sensors, IO Lines and Relays in the Form of SMS Messages . . . 116
1.2.11.10 [ENG] 11.10. [DKSF 70/71.7 IU] How to Find Out IMEI of the Built-in GSM Modem? . . . 117
1.2.11.11 [ENG] 11.11. [DKSF 70/71.7 IU] How to Send Arbitrary SMS? . . . 118
1.2.11.12 [ENG] 11.12. [DKSF 70/71.7 IU] How can I Configure the Forwarding of Incoming Unrecognized SMS As a Command? . . . 121
1.2.12 [ENG] 12. [DKSF 70/71.7 IU] Work with IR Command Module . . . 122
1.2.12.1 [ENG] 12.1. [DKSF 70/71.7 IU] How Can I Record IR Commands Corectly? . . . 123
1.2.12.2 [ENG] 12.2. [DKSF 70/71.7 IU] Playback of IR Commands Via the Web Interface . . . 124
1.2.12.3 [ENG] 12.3. [DKSF 70/71.7 IU] Can I Play Back the IR Commands via SNMP? . . . 125
1.2.12.4 [ENG] 12.4. [DKSF 70/71.7 IU] How Can I Determine the Version of a Built-In Firmware of IR module? . . . 126
1.2.12.5 [ENG] 12.5. [DKSF 70/71.7 IU] Recommendations . . . 127
1.2.13 [ENG] 13. [DKSF 70/71.7 IU] Work with the "LOGIC" module . . . 128
1.2.13.1 [ENG] 13.1. [DKSF 70/71.7 IU] What is "LOGIC"? . . . 129
1.2.13.2 [ENG] 13.2. [DKSF 70/71.7 IU] How Can I Use the "LOGIC" module? . . . 130
1.2.13.3 [ENG] 13.3. [DKSF 70/71.7 IU] How Can I Configure the Pinger in the "LOGIC" Module? . . . 133
1.2.13.4 [ENG] 13.4. [DKSF 70/71.7 IU] What is SNMP SETTER? . . . 134
1.2.13.5 [ENG] 13.5. [DKSF 70/71.7 IU] Initial Reset and Initial Output Status . . . 135
1.2.13.6 [ENG]13.6. [DKSF 70/71.7 IU] IR Commands . . . 136
1.2.13.7 [ENG] 13.7. [DKSF 70/71.7 IU] The Examples of the "LOGIC" Module Configuration . . . 137
1.2.14 [ENG] 14. [DKSF 70/71.7 IU] Device Support for Custom Notifications . . . 138
1.2.15 [ENG] 15. [DKSF 70/71.7 IU] SNMP Protocole Device Support . . . 142
1.2.15.1 [ENG] 15.1. [DKSF 70/71.7 IU] Can I Control The Device be Means of SNMP? . . . 143
1.2.15.2 [ENG] 15.2. [DKSF 70/71.7 IU] Configuration of Sending SNMP TRAP Messages . . . 144
1.2.15.3 [ENG] 15.3. [DKSF 70/71.7 IU] Which OID are Supported By the Device? . . . 148
1.2.15.4 [ENG] 15.4. [DKSF 70/71.7 IU] SNMP TRAP Support . . . 153
1.2.16 [ENG] 16. [DKSF 70/71.7 IU] The Support via the device NetPing HTTP API . . . 159
1.2.16.1 [ENG] 16.1. [DKSF 70/71.7 IU] The IO Lines Control . . . 160
1.2.16.2 [ENG] 16.2. [DKSF 70/71.7 IU] The Control of The Relay . . . 163
1.2.16.3 [ENG] 16.3. [DKSF 70/71.7 IU] Control of Temperature Sensors . . . 165
1.2.16.4 [ENG] 16.4. [DKSF 70/71.7 IU] The Control of Smoke Sensor (Current in the Loop) . . . 166
1.2.16.5 [ENG] 16.5. [DKSF 70/71.7 IU] The Control of the 1-wire Smoke Sensors . . . 167
1.2.16.6 [ENG] 16.6. [DKSF 70/71.7 IU] The Control of the Transceiver of the IR Commands . . . 169
1.2.16.7 [ENG] 16.7. [DKSF 70/71.7 IU] Control of the Humidity Sensors . . . 170
1.2.16.8 [ENG] 16.8. [DKSF 70/71.7 IU] Control of The GSM Modem . . . 172
1.2.17 [ENG] 17. [DKSF 70/71.7 IU] Documentation and Files . . . 174

[Docs] UniPing server solution v4/SMS & UniPing server solution v3

[ENG] UniPing server solution v4/SMS & UniPing server solution v3, User guide

[USS] Introduction

This user guide helps to become familiar with an operation of a Uniping server solution v3/SMS device and get an idea about its functionality and technical specifications as well as prepare a device for an operation.

A User Guide is designed for network administrators and users, who set up or operate a device. To work with a device properly, a user must have an idea about the principles of building and functioning of local networks as well as possess the next knowledge and skills:

- Basic knowledge in the area of local and global networks;
- Basic knowledge in the area of architecture and principles of work of TCP/IP networks;
- Basic knowledge in the area of architecture and principles of work of Ethernet networks.

[USS] Copyright and Disclaimer

Developer and manufacturer:

NetPing east Co Ltd.

[USS] A Device Overview

In this section, a function, an appearance and sensors that can be connected to a device are described.

Function of a Device

UniPing server solution v3/SMS and UniPing server solution v3 are devices for monitoring the operation environment of equipment in a server room.

A device helps to remotely track:

- temperature;
- humidity;
- access control to a room, to closets and servers;
- presence of smoke;
- water leakage;
- presence of 220V;
- presence of motion in a room;
- presence of shocks and vibrations

In addition, a device allows:

- notifying about events in a server room through SNMP TRAP, SYSLOG, e-mail and SMS (for a UniPing server solution v3/SMS device with a built-in GSM modem);
- building a system of sound and light alerting using a siren alarm AS-10, light beacons and other indication elements.

A monitoring device allows connecting a large number of various sensors. Readings of sensors may be taken through SNMP, HTTP protocols, and using URL-encoded commands and SMS commands (for a UniPing server solution v3/SMS device with a built-in GSM modem).

A device can be powered from an ordinary 220 V AC socket (internal battery) or from external power supply unit 5V DC (1,5A).

> Important! It is prohibited to supply the power to a device from two power sources (internal and external) simultaneously. This can lead to a failure of a device.

Appearance of a UniPing server solution v3/SMS Device

A device has a standard size to be mounted in a 19' rack. A height of a device is 1U. The appearance is shown below:

Picture 1 – Front panel

Picture 2 – Back panel

Appearance of a UniPing server solution v3 Device

A device has a standard size to be mounted in a 19' rack. A height of a device is 1U. Appearance is shown below:

Picture 3 – Front panel

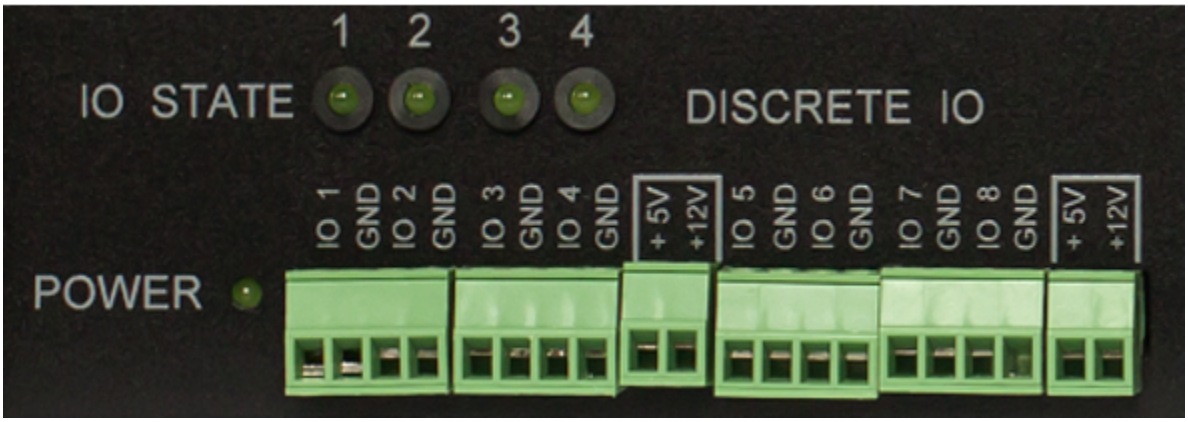
Picture 4 – Back panel

[USS] Sockets and Indication Elements

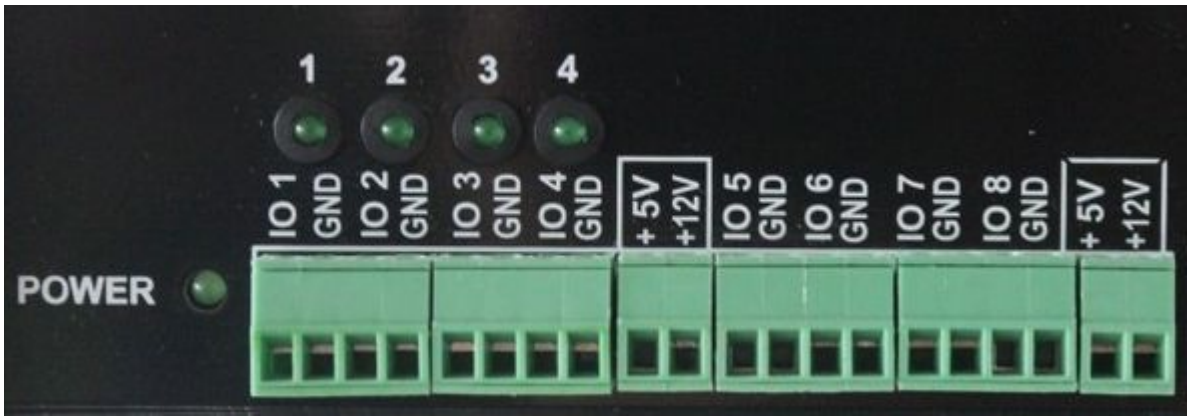
POWER LED

A POWER LED (see picture 1 and picture 2), when turned on, means a device works.

IO Lines Connection Terminals



Picture 1 – A terminal block for connecting IO lines (UniPing server solution v3/SMS device)



Picture 2 – A terminal block for connecting IO lines (UniPing server solution v3 device)

DISCRETE IO terminal block is used to connect universal IO lines.

There are eight IO lines in a block. For each line, there are two contacts: IO and GND. To make connecting sensors convenient, there are terminals +5 V and +12 V in a DISCRETE IO block. A maximum summed current on +5V and +12V terminals is 200mA, it is limited by a self-resetting fuse. To recover a terminal operation after a reboot, there is a need to deenergize a device completely for 30 minutes.

Electrical specifications of IO lines in the "output" mode:

Voltage of the logic "1": 4V, maximal current is: 0.3 mA

Voltage of the logic "0": 0,1V, maximal current is: 0.8 A

Electrical specifications of IO lines in the "input" mode:

Voltage of the logic "1": >2.1V

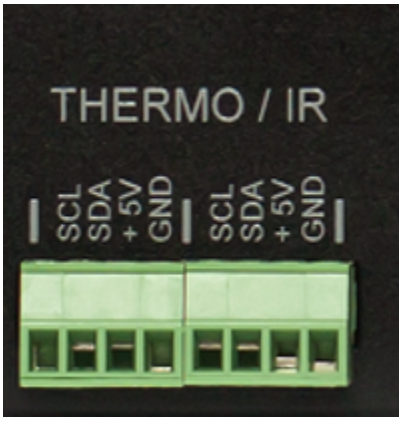
Voltage of the logic "0": <0,9V

It is possible to plug relay coils to UniPing Server Solution v3/SMS IO lines directly. A voltage of triggering a relay should be either 12 V or 5 V, and a triggering current - no more than 200mA. Control relay contacts are connected to an IO terminal and to the terminal +12 V or 12 V relay or a +5 V terminal for a 5 V relay. A corresponding IO line should be set to an output mode. When connecting several relays, there is a need to take into consideration that their summed maximum triggering current should not exceed 200mA.

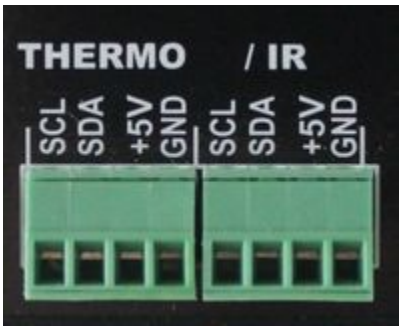
IO STATE LEDs

IO STATE LEDs (see picture 1 and picture 2) signal about a status of the first four IO lines. When a LED is turned on, a corresponding IO line is in a status logic 1, and a turned off LED means a logic status 0.

Thermo / IR Terminals



Picture 3 – Terminals «Thermo / IR» (UniPing server solution v3/SMS device)



Picture 4 – Terminals «Thermo / IR» (UniPing server solution v3 device)

A THERMO/IR terminal block is used to plug temperature sensors and an IR-transceiver. To make plugging sensors convenient, connecting terminals are output to a front panel twice. Temperature sensors can be plugged into a left terminal block as well as into a right one. An IR transceiver is plugged in parallel to temperature sensors into the same terminals.

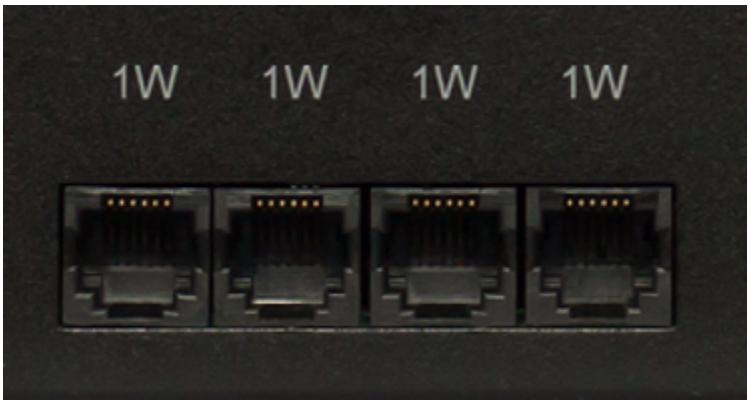
Smoke Terminals

Picture 5 – Terminals «Smoke» (UniPing server solution v3/SMS device)

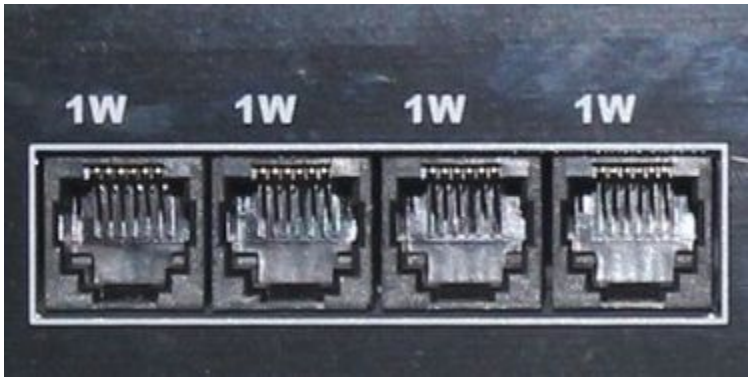
Picture 6 – Terminals «Smoke» (UniPing server solution v3 device)

A SMOKE terminal block is used to plug in a smoke sensor.

1W Sockets



Picture 7 – «1W» sockets (UniPing server solution v3/SMS device)

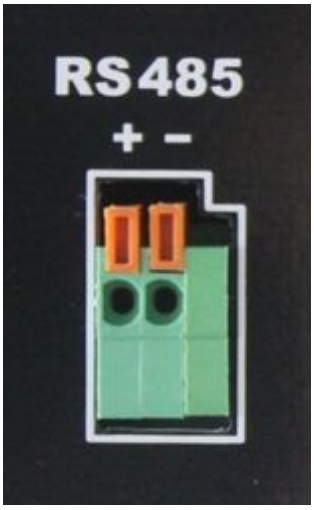


Picture 8 – «1W» sockets (UniPing server solution v3 device)

1W sockets are used to plug in sensors of a model line 1-Wire, that are built using a 1Wire technology. To make sensors plugin more convenient, there are four sockets on a body of a device. It is possible to plug in more than four sensors of a model line 1-Wire, using splitters and extenders.

RS232 / RS485 Sockets

Picture 9 – «RS232 / RS485» sockets (UniPing server solution v3/SMS device)



Picture 10 – «RS485» sockets (UniPing server solution v3 device)

RS232/RS485 socket is used to plug in RS232/RS485 devices. A port RS232/RS485 can work in the mode of converting interfaces RS232/RS485 – Ethernet via TCP protocol.

> Important! Ports RS232 and RS485 use one bus inside a device. It is prohibited to plug in devices to the ports RS232 and RS485 simultaneously.

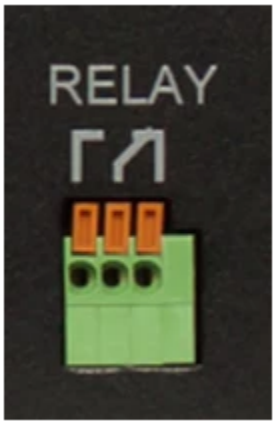
> There is no «RS232» socket in a UniPing server solution v3 device.

Functions of contacts of a RS232 socket are represented in a table:

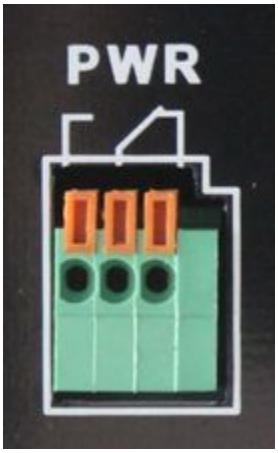
Contact Number	Function
1 (left upper one)	DCD(I)
2	RX(I)
3	TX(O)
4	DTR(0), always HIGH
5	GND
6	DSR(I)
7	RTS(O)

8	CTS(I)
9	RING(I)

Relay Socket (PWR)



Picture 11 – Socket «Relay» (UniPing server solution v3/SMS device)



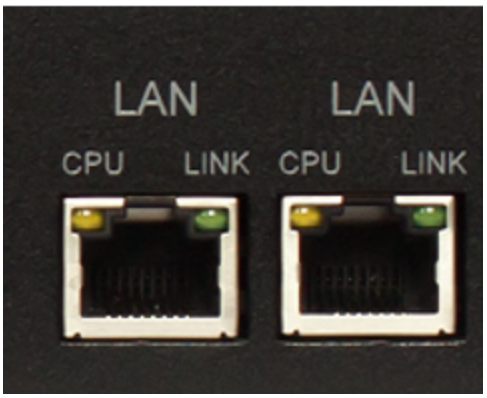
Picture 12 – Socket «PWR» (UniPing server solution v3 device)

Contacts of a relay, built into a body of a device, are output normally opened and normally closed. A relay can be used for managing a Reset button of a computer as well as for connecting an Alarm AC-10.

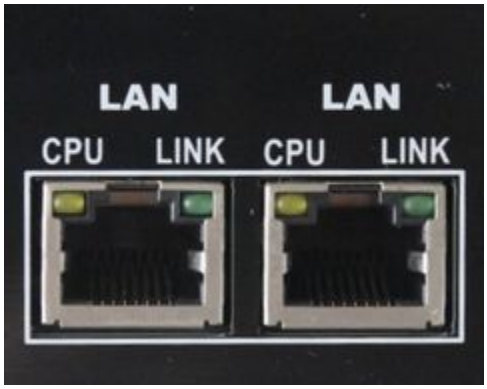
Electrical parameters of power management channel RELAY are as follows:

- The maximum permissible voltage on the relay contacts is 50V;
- The maximum allowable current through the relay contacts is 2A

LAN Sockets



Picture 13 – LAN sockets (UniPing server solution v3/SMS device)



Picture 14 – LAN sockets (UniPing server solution v3 device)

Ethernet 10/100 BASE-T ports form together a two-port Ethernet switch. One port is used to connect to a network, and the other one - to connect an additional equipment (another NetPing device, an administrator's laptop, etc.), which gives a possibility not to install an additional switch on a remote land. These ports are equal, and any of them can be used to connect to a network.

> Important! Connecting both ports to an Ethernet switch with turned off STP protocol will lead to creating a loop in an Ethernet segment.

Ethernet ports have two LEDs. The left one is CPU, and when it is lighting, it means a device is turned on. It blinks when packages are transferred to a network. The right one is Link, when it is lighting, it means having a link on this port. It blinks when receiving packages from a network.

GSM Sockets

Picture 15 – GSM modem sockets (UniPing server solution v3/SMS device)

A GSM ANT socket is designed for plugging in an external antenna, which is included into a shipping kit. A SIM Card slot is designed for installing a SIM card.

Important! Before installing a SIM card into a device, disable PIN code verification on it, using an ordinary cell phone.

Reset Button

A Reset button is designed for resetting parameters to default values. To reset the parameters, press a Reset button with a sharp object and hold it during a device is turning on.

Power Supply Inputs

There are two power supply inputs on a back panel. One of them is used to feed a device from an external power supply unit 5 V DC (1,5A). Another one is used to feed a device from an internal power supply unit 220 V AC.

Important! It is prohibited to power a device from two power sources (an external and an internal one) simultaneously. It can damage a device.

Picture 16 – 5V DC Input (UniPing server solution v3/SMS device)

Picture 17 – 5V DC Input (UniPing server solution v3 device)

Picture 18 – 220V AC Input (UniPing server solution v3/SMS device)

Picture 19 – 220V AC Input (UniPing server solution v3 device)

[USS] Installing and Removing a SIM Card

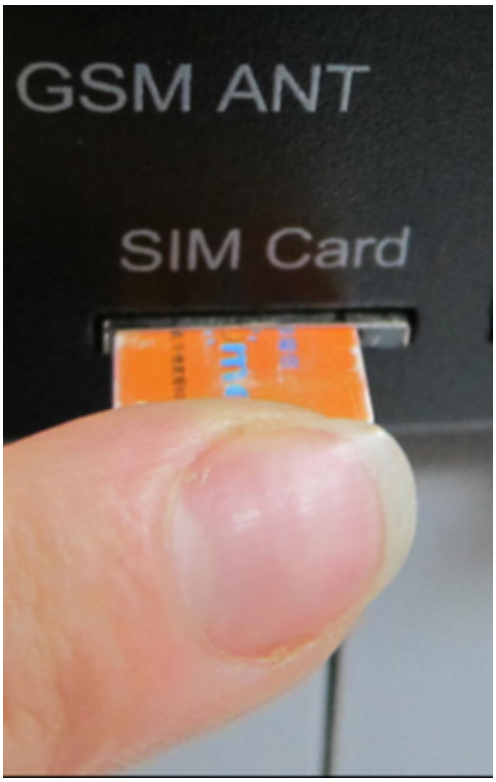
> Information in the section applies to a UniPing server solution v3/SMS device with a built-in GSM modem.

INSTALLING A SIM CARD

> Install and remove a SIM card when a device is de-energized!

Install a SIM card in the next way:

With a slight touch of a finger, install a SIM card until it clicks:

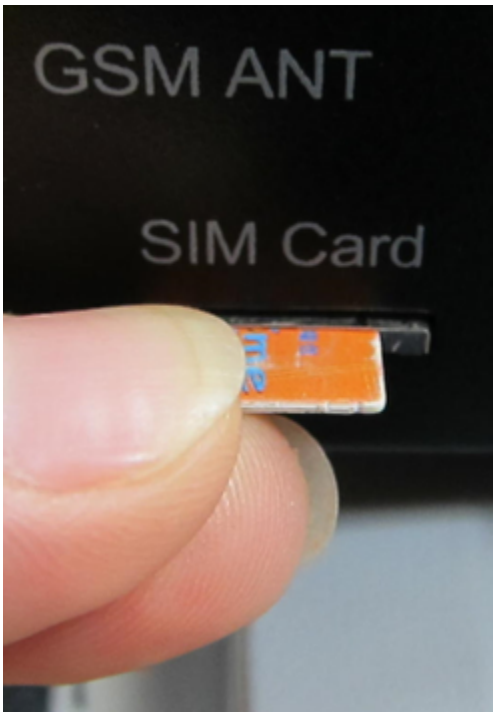


A SIM card is installed:

REMOVING A SIM CARD

To remove a SIM card, click a protruding part of a SIM card with a finger until it clicks

Remove a SIM card from a holder



[USS] Using IO Lines to Control External Devices (in the «Output» Mode)

Input-Output (IO) lines of a device can be used for an input work as well as in an output mode for managing external devices.

A device has eight IO lines that correspond to IO 1 - IO 8 contacts of a terminal block. Lines are configured for work for input or output through a controlling web-interface of a device or using URL-encoded commands. All eight IO lines can be customized independently.

Lines management can be done by SNMP commands, URL-encoded commands, via a web-interface or using SMS-commands (for devices with built-in GSM modem).

Such device functions as a watchdog and scheduled load management are NOT AVAILABLE for IO in an output mode.

Examples of using:

- Remote servers reboot – an imitation of pressing “reset”;
- Remote management of an alarm, a light, a fan;
- Management of an electric lock, electric gates on a remote object;
- Management of smart home elements - watering flowers, opening-closing louvers, water pump, heating boiler, heaters, etc.
- Remote management of a power installation (diesel generator, gasoline).

> Important! Correct electrical coordination of IO lines is required when connecting external executive devices.

> Important! IO lines do not have galvanic isolation with a device! Remember about electrical safety when using relays that commutate 220 V circuits. All work must be done by specialists with a correspondent qualification who have a permit to work with such a voltage!

It is acceptable to use intermediate relays with a power supply voltage of 12 V from an external source. A ready socket can be used for IO lines connection NetPing AC/DIN socket. In addition, we can advise ready assembly relays of other manufacturers, which can be connected to our devices:

- BM8070D a power relay 16A/250V for DIN-rail (check out the compatibility of this relay with the NetPing device model on the relay web page on the site);
- MP701 a power module switch (4 independent channels, 2 kW 10A each) (check out the compatibility of this relay with the NetPing device model on the relay web page on the site);

For more detailed information, please contact a technical support support@netpingdevice.com.

Electric parameters of IO lines

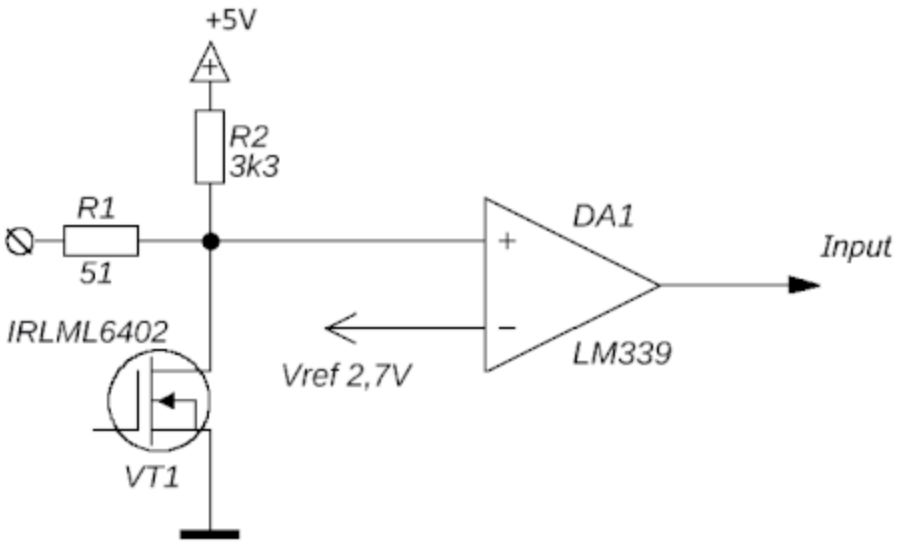
In the «output» mode:

- the voltage of logic «1»: +5 V, resistance: 3,3 kOhm;
- the voltage of logic «0»: 0 V, resistance: 51 Ohm.

In the «input» mode:

- voltage of logic «1»: > 2.7 V;
- voltage of logic «0»: < 2,7 V.

Equivalent Circuit



[USS] Sensors Plugin

> It is prohibited to plug sensors and external modules into NetPing devices when a power supply is on!

> Configuring a device and receiving notifications from sensors are described in the document «Firmware Description».

Sensors of 1-Wire Model Line

Sensors of a 1-Wire model line (Temperature 1-wire, (THS), 2m and Humidity sensor 1-wire (HS), 2m) are plugged into 1W sockets by RJ12 plugs. It is allowed to use extenders and splitters. A maximum loop length of the 1-Wire network is limited to 50 meters. It is possible to plug up to eight temperature sensors and up to four humidity sensors to a device simultaneously.

Latest firmware work only with sensors with a 1-Wire interface (THS temperature sensor, HS humidity sensor, etc.). Outdated firmware versions also supported temperature sensors of TS, WT series as well, using the i2c interface.

IR Transceiver IRC-TRv2

An IR transceiver is connected by a four-line wire according to the table below:

Sensor Flex	Sensor Flex	UniPing server solution v4/SMS, UniPing server solution v3 Terminal Block
Yellow	Labeled wire (red).	SCL
Green	Second wire after a labeled one	SDA
Red	Third wire after a labeled one	+5V
Black	Fourth wire after a labeled one	GND

A sensor is shipped with an inseparable cable with connectors at the ends. A cable length can be extended using RC-4 sensor cable extenders, which are consequentially plugged one into another using any wire with a section no less than 0,4 mm^2. A maximum loop length is 10 meters from each sensor to a device (a «star» topology).

Sensors of Dry Contact Type

Dry contact sensors are door opening sensors, buttons and other sensors with a mechanism of work based on opening/closing a conductor. A sensor is connected with two wires to an IO line of a device according to the table. An order of plugging wires does not matter.

Sensor Flex	UniPing server solution v4/SMS, UniPing server solution v3 Terminal Block
First wire	One of IO lines – 1 - 8
Second Wire	GND

> Important! Sensors of a dry contact type, a supply voltage sensor, a leakage sensor, and others are plugged to IO lines of a device. You can plug any eight sensors out of this set.
>
> Important! A corresponding IO line should be set to an input mode in settings of a device.

A maximum allowable loop length is 100 meters.

H2O Leakage Sensor

A leakage sensor is plugged by a four-line wire according to the table:

Sensor Flex	UniPing server solution v4/SMS, UniPing server solution v3 Terminal Block
Green	One of IO lines – 1 - 8
Yellow	GND

Brown	+5V
White	GND

> Important! Sensors of a dry contact type, a supply voltage sensor, a leakage sensor, and others are plugged to IO lines of a device. You can plug up to eight sensors of this set.
>
> Important! A correspondent IO line should be set to an input mode in settings of a device.

A sensor is packaged with an inseparable cable, with connectors on the ends. A cable length can be increased with the help of flat cable extenders of RC-4 sensor, which are sequentially plugged one into another. Or it can be done independently with the help of any wire with a minimum cross section of 0,4 mm^2. Maximum allowable length of a flat cable is 100 m.

Leakage Sensors, model 2605

A leakage sensor is plugged by a four-line wire according to the table:

Sensor Flex	UniPing server solution v4/SMS, UniPing server solution v3 Terminal Block
Green	One of IO lines – 1 - 8
Yellow (White)	GND
Red	+5V
Black	GND

> Important! Sensors of a dry contact type, a supply voltage sensor, a leakage sensor, and others are plugged to IO lines of a device. You can plug up to eight sensors of this set.
>
> Important! A correspondent IO line should be set to an input mode in settings of a device.

A sensor is shipped with an inseparable cable with connectors at the end. A cable length can be extended using RC-4 sensor cable extenders, that are consequentially plugged one into another or independently using any wire with a section no less than 0,4 mm^2. A maximum allowable loop length is 100 m.

Supply Voltage Sensor

A supply voltage sensor is plugged by a two-line wire according to the table. An order of plugging wires does not matter.

Sensor Flex	UniPing server solution v4/SMS, UniPing server solution v3 Terminal Block
First wire	One of IO lines – 1 - 8
Second wire	GND

> Important! Sensors of a dry contact type, a supply voltage sensor, a leakage sensor, and others are plugged to IO lines of a device. You can plug up to eight sensors of this set.
>
> Important! A correspondent IO line should be set to an input mode in settings of a device.

A sensor is packaged with an inseparable cable, with connectors on the ends. A cable length can be increased with the help of flat cable extenders of RC-4 sensor, which are sequentially plugged one into another. Or it can be done independently with the help of any wire with a minimum cross section of 0,4 mm^2. Maximum allowable length of a flat cable is 100 m.

Glass Breakage Sensors

A glass breakage sensor is plugged by a four-line wire according to the table:

Sensor Flex	UniPing server solution v4/SMS, UniPing server solution v3 Terminal Block
Red wire (labeled)	+12V

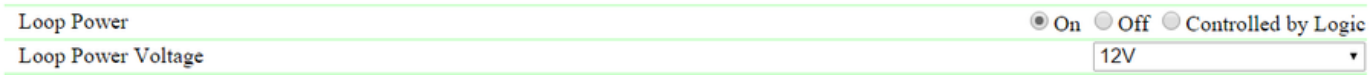
Second wire after a labeled one	GND
Third wire after a labeled one	GND
Fourth wire after a labeled one	One of IO lines – 1 - 8

Important! Sensors of a dry contact type, a supply voltage sensor, a leakage sensor, and others are plugged to IO lines of a device. You can plug up to eight sensors of this set.

Important! A correspondent IO line should be set to an input mode in settings of a device.

Important! For the operation of a glass breakage sensor, there is a need to power a 12-V loop on the page of a smoke sensor (current sensor) of a device web interface.

LOOP POWER



A sensor is packaged with an inseparable cable, with connectors on the ends. A cable length can be increased with the help of flat cable extenders of RC-4 sensor, which are sequentially plugged one into another. Or it can be done independently with the help of any wire with a minimum cross section of 0,4 mm^2. Maximum allowable length of a flat cable is 100 m.

Shock Sensors

A shock sensor is plugged by a four-line wire according to the table:

Sensor Flex	UniPing server solution v4/SMS, UniPing server solution v3 Terminal Block
Blue wire	One of IO lines – 1 - 8
Green wire	One of IO lines – 1 - 8
Red wire	+12V
Black wire	GND

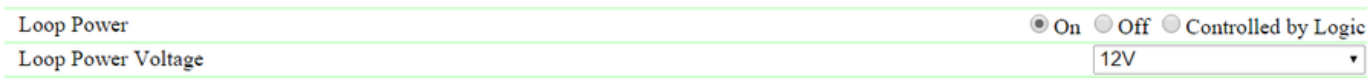
A shock sensor takes two IO lines. You can plug no more than four such sensors.

Important! Sensors of a dry contact type, a supply voltage sensor, a leakage sensor, and others are plugged to IO lines of a device. You can plug up to eight sensors of this set.

Important! A correspondent IO line should be set to an input mode in settings of a device.

Important! For the operation of a shock sensor, there is a need to power a 12-V loop on the page of a smoke sensor (current sensor) of a device web interface.

LOOP POWER



A sensor is packaged with an inseparable cable, with connectors on the ends. A cable length can be increased with the help of flat cable extenders of RC-4 sensor, which are sequentially plugged one into another. Or it can be done independently with the help of any wire with a minimum cross section of 0,4 mm^2. Maximum allowable length of a flat cable is 100 m.

Motion Sensors

A motion sensor is plugged by a four-line wire according to the table:

Sensor Flex	UniPing server solution v4/SMS, UniPing server solution v3 Terminal Block

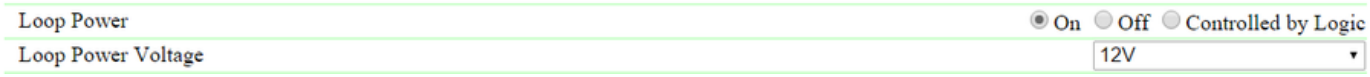
Red wire (labeled)	One of IO lines – 1 - 8
Second wire after a labeled one	GND
Third wire after a labeled one	GND
Fourth wire after a labeled one	+12V

Important! Sensors of a dry contact type, a supply voltage sensor, a leakage sensor, and others are plugged to IO lines of a device. You can plug up to eight sensors of this set.

Important! A correspondent IO line should be set to an input mode in settings of a device.

Important! It is necessary to turn on a power supply for a 12 V loop at the page of a smoke sensor (current sensor) of a device web interface for a motion sensor to operate.

LOOP POWER



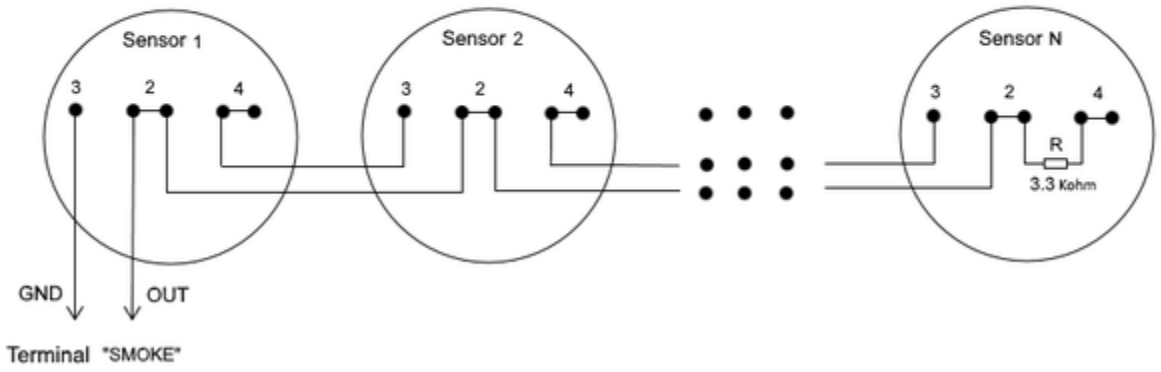
A sensor is packaged with an inseparable cable, with connectors on the ends. A cable length can be increased with the help of flat cable extenders of RC-4 sensor, which are sequentially plugged one into another. Or it can be done independently with the help of any wire with a minimum cross section of 0,4 mm^2. Maximum allowable length of a flat cable is 100 m.

Smoke detector (mod. M206-5E)

A smoke sensor is plugged by a two-line wire according to the table:

Sensor Flex Type 1	Sensor Flex Type 2	Sensor Flex Type 3	UniPing server solution v4/SMS, UniPing server solution v3 Terminal Block
Red+Black	Black	Black	GND
Yellow+Green	Red+Black	Red	OUT

UniPing server solution v3-SMS, UniPing server solution v3, NetPing Connection board v2



Theoretically, a number of sensors in a circuit is not limited. The main requirement is to maintain a loop resistance in a standby mode at 3.3 kOhm (determined by a resistor at the end of a circuit). I.e. sensors can be added to a circuit until a loop resistance is not increased because of resistance of connecting wires.

A sensor is packaged with an inseparable cable, with connectors on the ends. A cable length can be increased with the help of flat cable extenders of RC-4 sensor, which are sequentially plugged one into another. Or it can be done independently with the help of any wire with a minimum cross section of 0,4 mm^2. Maximum allowable length of a flat cable is 100 m.

NetPing AC/DIN External Sockets

The amount of plugged in NetPing AC/DIN sockets is limited by the amount of available IO lines only.

All wires are used to plug a socket into a device except a brown one (a white one). The IO line, where a socket AC/DIN is connected, needs to be switched to an output mode. When a status of an IO line is a logic level 0, there will be 220V on a socket, a voltage will be turned on. When its status is a logic level 1, a socket will be de-energized, a voltage off.

> Important! The brown wire is not used and must stay unplugged!

Controlling through an IO line:

Sensor Flex	UniPing server solution v4/SMS, UniPing server solution v3 Terminal Block
Red	+5V
Black	GND
Blue (green)	One of IO lines – 1 - 8

Controlling through RELAY (NO is normally opened contact, NC is a normally closed contact):

Sensor Flex	UniPing server solution v4/SMS, UniPing server solution v3 Terminal Block
Red	+5V
Black	GND
Blue (Green)	Middle contact of a «Relay» terminal
	«+5V» terminal is plugged to a normally opened relay contact (a left terminal in «Relay») by an auxiliary wire

> When plugging NetPing AC/DIN to a relay:
>
> - RELAY "On" there is no voltage in a socket;
> - RELAY "Off" there is voltage in a socket

A relay with normally closed contacts is used for a load commutation in a NetPing AC/DIN. This means having 220 V on a socket and a voltage turned on when a control wire is not plugged in.

A sensor is packaged with an inseparable cable, with connectors on the ends. A cable length can be increased with the help of flat cable extenders of RC-4 sensor, which are sequentially plugged one into another. Or it can be done independently with the help of any wire with a minimum cross section of 0,4 mm^2. Maximum allowable length of a flat cable is 100 m.

Electricity Meter "Energy Meter CE102"

An electricity meter is connected by a two-wire line according to the table:

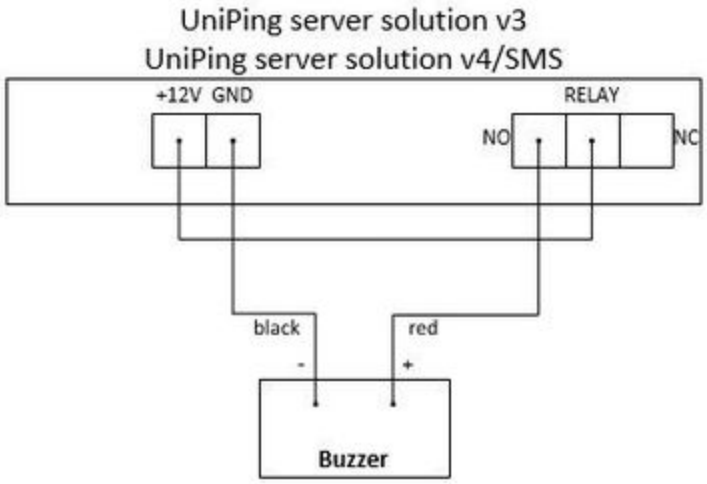
Meter Socket	UniPing server solution v4/SMS Terminal Block
11 (B)	RS485-
12 (A)	RS485+

Buzzer (mod.STD-3025)

Connecting the buzzer to the RELAY (NO - is normally opened contact, NC - is normally closed contact) with using +12V:

Loop Color	UniPing server solution v4/SMS, UniPing server solution v3 Terminal Block
Black	GND

Red	NO (RELAY)
	+12V ↔ Middle contact (RELAY)



A sensor is packaged with an inseparable cable, with connectors on the ends. A cable length can be increased with the help of flat cable extenders of RC-4 sensor, which are sequentially plugged one into another. Or it can be done independently with the help of any wire with a minimum cross section of 0,4 mm^2. Maximum allowable length of a flat cable is 100 m.

[USS] Setting Parameters to Default Values (to the Factory Settings)

Resetting parameters to the factory settings is necessary in the following cases :

- A loss of a login and/or password to a web interface of a device;
- A lack of information about current IP address of a device;
- In some cases after a device software update.

A procedure of resetting parameters to the factory settings changes all customizable parameters of a device to the default ones. (IP and MAC addresses, access filters, a user name, a password, etc.).

To reset parameters to default settings, fulfill the next actions sequentially:

- Turn off a power supply of a device;
- Press the Reset button (a button Set for a UniPing v3 monitoring unit);
- Turn on a power supply of a device, continuing to hold Reset button pressed for 15-20 seconds;
- Release the button. All parameters of a device are set to default settings.

> On default, the next parameters of a device are set:
>
> User name: visor
>
> Password: ping
>
> IP address: 192.168.0.100
>
> Subnetwork mask: 255.255.255.0
>
> Gateway: not set
>
> SNMPcommunity: SWITCH
>
> MAC-address: 00 a2 xx xx xx xx
>
> Here xx xx xx xx corresponds to a serial number of a device. Thus, all devices after being manufactured have unique MAC-addresses.

After resetting parameters to default settings there is a need to do an initial configuration of a device.

[USS] Shipping Kit

Shipping kit of a UniPing server solution v3/SMS device

A shipping kit includes:

- UniPing server solution v3/SMS device – 1 pc.;
- GSM antenna – 1 pc.;
- computer power cable 1,8 meters – 1 pc.;
- mounting ears – 2 pcs.;
- fasteners for ears – 4 pcs.;
- mating terminals – 9 pcs.
- screwdriver – 1 pc.;
- zip bag – 1 pc.;
- memo – 1 pc.;
- packaging box – 1 pc.

Shipping kit of a UniPing server solution v3 device

A shipping kit includes:

- UniPing server solution v3 device – 1 pc.;
- computer power cable 1,8 meters – 1 pc.;
- mating terminals – 9 pcs.
- screwdriver – 1 pc.;
- memo – 1 pc.;
- packagng box – 1 pc.

[USS] Warranty

The manufacturer guarantees normal operation of the product within 24 months from the date specified on the warranty sticker if a buyer follows operating and storage conditions. Manufacturer warranty applies only to failure of a device which occurred because of defects in manufacturing process of products and components used. If during a warranty period the manufacturer receives a notice of such defects, it will repair or exchange the product (by its own discretion). If the manufacturer is unable to repair or replace a flawed item during a period of time determined by the current legislation, the manufacturer according to a customer's wish can return the amount paid for the product at the time of purchase. The manufacturer provides a limited warranty on firmware and device configuration software. In case of detecting any errors in the software which became known to the manufacturer on its own or from a customer, the manufacturer will fix these errors within a reasonable time and provide an update for the customer. Only the errors that block normal use of the device at conditions and for performing functions described in this User Guide are a subject to mandatory fix. This warranty does not apply to cases when defects appear because of: a misuse of a device, any modifications of a device without a written permission of the manufacturer, opening up a device (a warranty sticker on the case of a device is damaged) except cases foreseen by this description; repairing by unauthorized personnel, using or storing a device out of the range of allowable temperature and humidity, pressure, a software modification, and the reasons, listed below:

- A device failed because of the problems in a public electric network, plugging a device into power supply networks with invalid parameters, absence of grounding, etc. (power fluctuations and surges, overloading, etc.);
- A device failed because of having liquid inside;
- A device failed as a result of extreme temperatures;
- A device failed because of mechanical damage;
- A device failed because of connecting a power supply unit with invalid output voltage or a defective power supply unit;
- There are foreign objects, insects, etc inside the enclosure;
- During operation a voltage bigger than an allowable voltage range by the Ethernet standard has been supplied to the ports of a device.

[USS] Operating and Storage Conditions

A device is designed for continuous round the clock operation indoors. In operating conditions of use, a device is resistant to an environment with temperature in a range of 0°C - +40°C (32 – 104 degrees Fahrenheit) and relative humidity in a range of 5% - 95 % at 25°C (77 degrees Fahrenheit) without moisture condensation. A device should be protected from direct moisture and direct sun light.

A construction of a device provides a reliable uninterrupted work during a long period of time without maintenance. Highly developed functionality of remote setting and configuration of a device allows changing any parameters remotely and centrally for the most of the devices.

Devices should be stored in a temperature range between - 40°C and +70°C.

In rooms for keeping a device, a content of dust, acid and alkali gases, aggressive gases and other harmful impurities causing corrosion, should not exceed a content of corrosion-active agents for atmosphere of type 1.

> Important! A device must be connected to a power supply socket with a grounding contact or a hole, where a contact, located at an outlet and connected to a ground wire, is inserted. Grounding must be performed according to the State Standard P 50571.21-2000. An infraction of this rule is a violation of a device operation conditions and may be dangerous to human lives as well as damage other devices!

[USS] Safety Precautions

The next information will allow users to avoid both injuries and damaging a device as well as connected equipment.

- A device must be plugged to a power supply socket with a ground or a hole, where a contact is inserted. A contact must be located at a plug and be connected to a ground wire. Grounding must be implemented according to ГОСТ Р 50571.21-2000;
- A device must be used only in a power supply network, indicated by a manufacturer. Using any other power supply types may lead to damaging a device;
- Do not use damaged power cords as well as insecurely fixed wall sockets;
- An electric equipment with electricity consumption of more than 1500 W must be grounded;
- It is prohibited to open the case of a device;
- Do not drop a device and avoid impact of force on it;
- Protect a device from high humidity levels. It is prohibited to touch a device and a connected equipment with wet hands;
- Use devices only indoors;
- Do not place a device at a surface or inside heating devices, such as microwaves, stoves and heaters;
- Do not use a device in locations marked as potentially explosive, with a possibility of an explosion and a ban on the use of wireless devices (works for devices with a built-in GSM modem);
- Protect a device against fire and extreme temperatures;
- Avoid impact of direct sunlight on a device;
- Do not allow children to use a device.

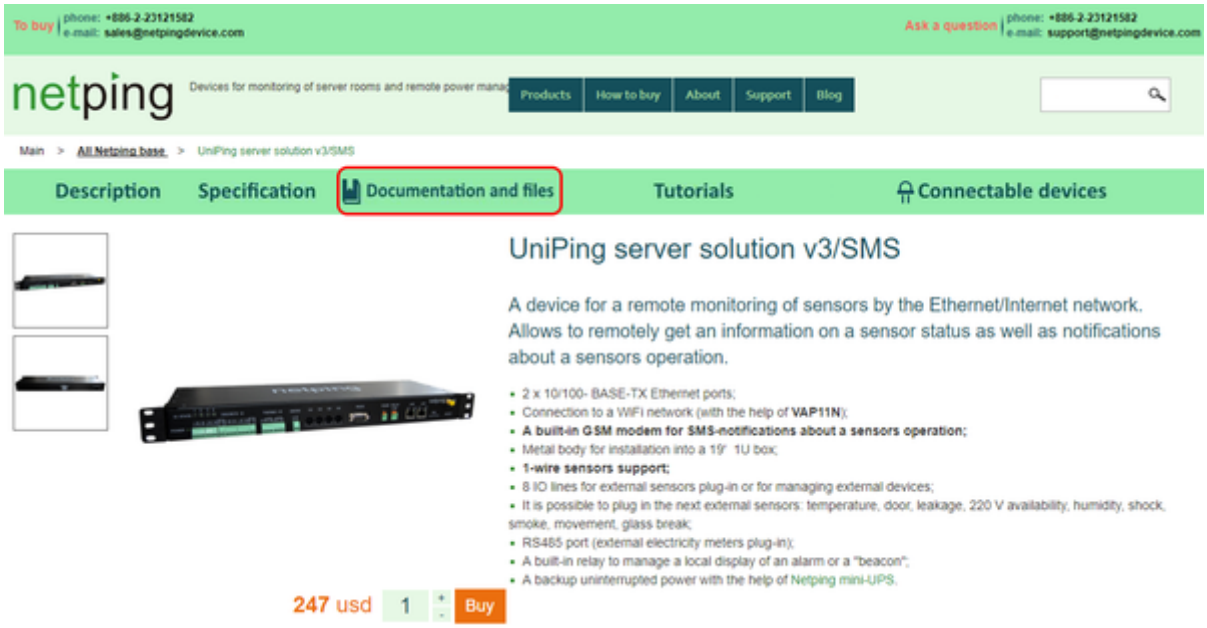
Attention! Failure to comply with these conditions is a violation of the operating conditions of a device.

[USS] Where to Get a Document of a Firmware Description?

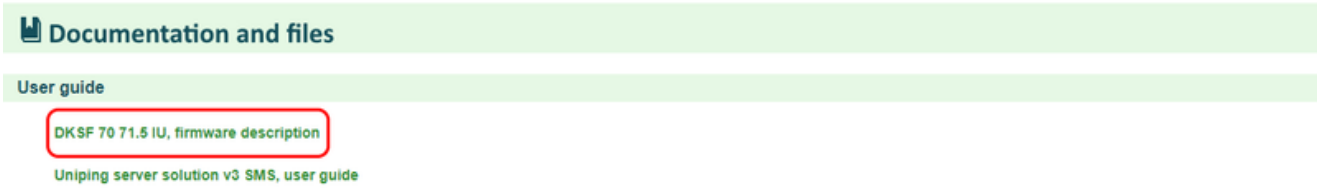
A configuration and operation order with management interfaces of a device are provided in the document «Firmware Description». The documentation is updated according to the changes made to the firmware.

To find an actual version of «Firmware Description» on the manufacturer's web site, there is a need to:

1. Go to the page of a description of a necessary device:
   - UniPing server solution v3/SMS
   - UniPing server solution v3
2. Go to the section «Documentation and Files»:



3. Go to the link «Firmware description DKSF 70.5 IU»:



> A version in the document «Firmware Description» must coincide with a firmware version of your device, i.e. the first two digits in the name of a document with a firmware description must be the same as the first two digits in a firmware name of your device.

[USS] Additional Documents and Links

Technical support for Netping devices

Manufacturer's website: http://www.netpingdevice.com/

Kindly see our blog for articles with examples of using the devices and news on issuing new firmware versions.

If any problems arise when using a device or there is a need for additional information, contact a technical support by the address support@netpingdevice.com.

Pages of devices on a manufacturer's website:

- UniPing server solution v3/SMS
- UniPing server solution v3

Information about a functionality of a device and its configuration using a web interface is available from the document «Firmware Description». Where to Get a Document of a Firmware Description?

[ENG] [DKSF 70/71.7 IU] UniPing server solution v4/SMS & UniPing server solution v3, Firmware description

[ENG] 1. [DKSF 70/71.7 IU] Introduction

What This Document Is About?

This document describes the functionality of the DKSF 70/71.7.X firmware for the next devices: UniPing server solution v4/SMS, UniPing server solution v3.

The devices UniPing server solution v4/SMS, UniPing server solution v3 with the firmware of the DKSF 70/71.7.X version support the next management interfaces:

- HTTP (web-interface);
- SNMP v1;
- URL encoded HTTP commands;
- SMS-commands (for the models UniPing server solution v4/SMS with a built-in GSM-modem).

Description of configurations an operating order for these management interfaces is provided in this document.

Description of physical specifications of the device, its controls, and indicators, a connection order of a device nad external sensors are given in the user guide for the devices UniPing server solution v4/SMS, UniPing server solution v3.

A user guide can be explored at the link: UniPing server solution v3(4)/SMS & UniPing server solution v3, User Guide.

Developer and manufacturer:

NetPing east Co Ltd.

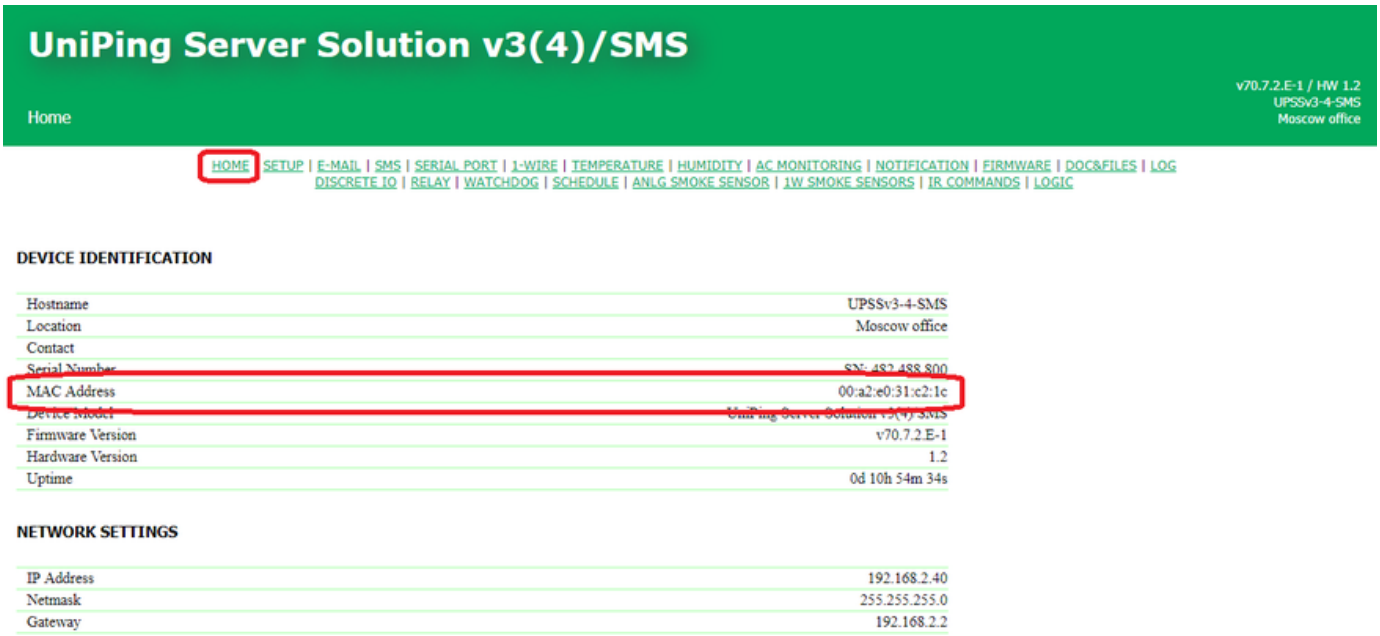
[ENG] 2. [DKSF 70/71.7 IU] Getting Basic Information about a Device

[ENG] 2.1. [DKSF 70/71.7 IU] How to Know a Default IP Address and a MAC Address of a Device?

A default IP address is specified at the backside of the UniPing server solution v4/SMS, UniPing Server Solution v3/SMS and UniPing server solution v3:

> A default IP address is 192.168.0.100

A MAC address can be found on the home page of a web interface of a device:



[ENG] 2.2. [DKSF 70/71.7 IU] Default User Name and Password

Default user name and password for connecting to a device web interface are:

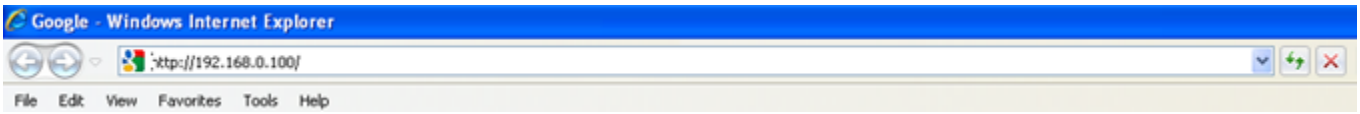
- Login: visor
- Password: ping

This information is given at the backside of UniPing server solution v4/SMS and UniPing server solution v3:

[ENG] 2.3. [DKSF 70/71.7 IU] Connecting to the Web Interface of a Device with a Default Authentication

Web Interface

A web interface is used to manage a device. To connect to a device and configure its parameters, there is a need to enter and IP address of a device in the address bar of a browser:



> When working in Internet Explorer, web interface operation speed can be decreased. It is recommended to use the latest version of Google Chrome.

Use a command ping from a command line to check a connection with a device:

ping 192.168.0.100

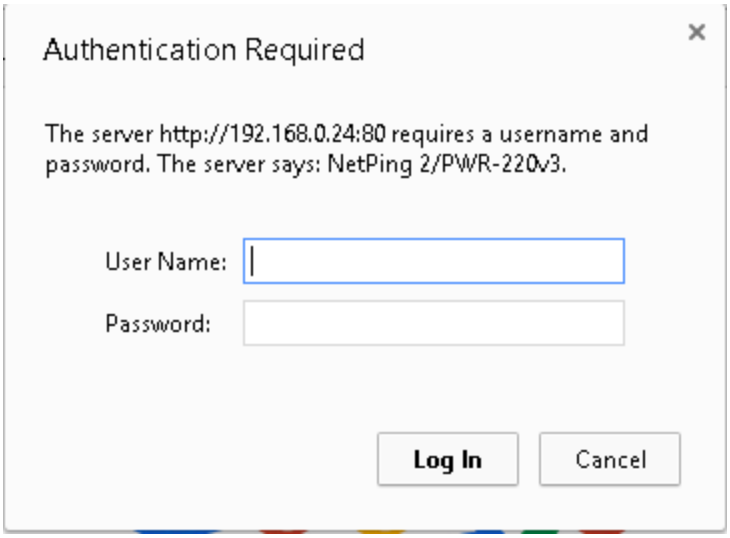
> IP address of a computer should be in the same subnetwork with an IP address of a device! For example, if a device has an IP address 192.168.0.100, then a computer should have address 192.168.0.11 mask 255.255.255.0

AUTHENTICATION

While connecting, a device will request authentication by entering login and password.

On default:

- Address for connecting to a device: http://192.168.0.100/;
- User: visor;
- Password: ping

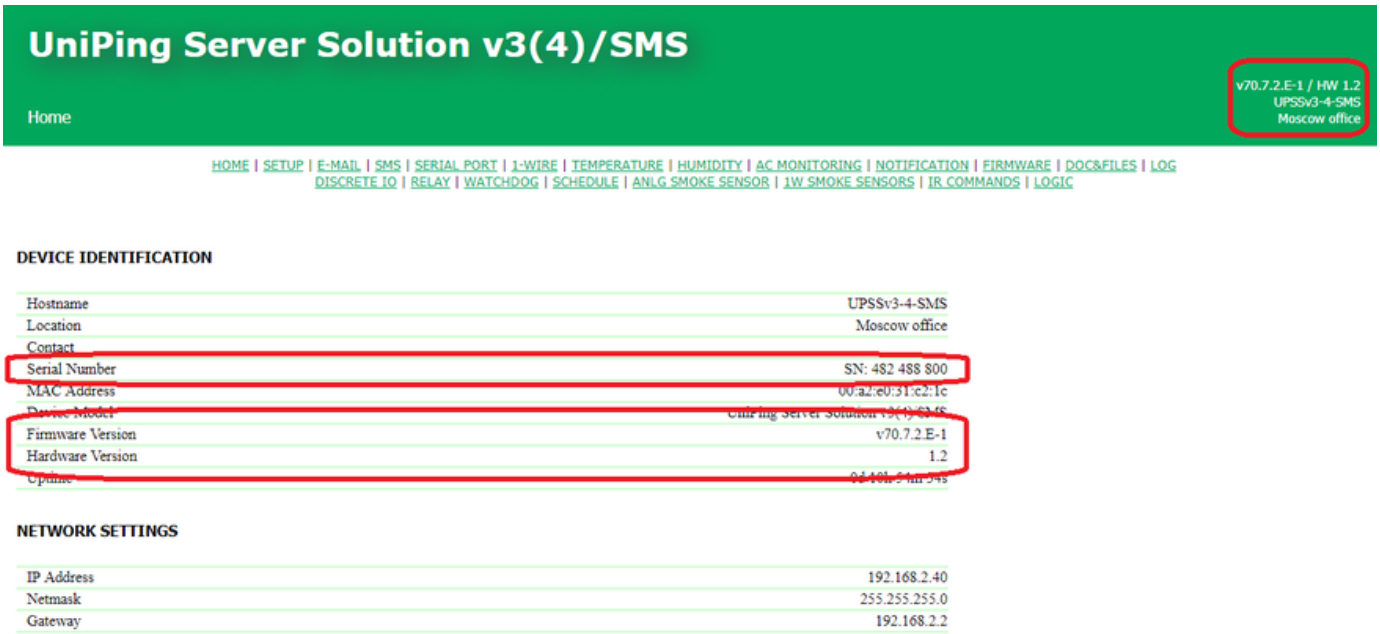


> Make sure that a device responds to ping 192.168.0.100 after the first device activation as well as after resetting its parameters.

> It is prohibited to use non-ASCII characters ("№", "®", "«" and others, as well as any Cyrillic character) in a username and a password. Otherwise, authentication issues may arise in a web interface in browsers except Google Chrome.

[ENG] 2.4. [DKSF 70/71.7 IU] I Need to Know the Firmware and Hardware Versions, and a Serial Number of a Device

The information about the firmware and hardware versions and a serial number of a device can be found at the home page of a device web interface. Otherwise, it can be found in the heading of all pages of a web interface, a name and a location of a device are represented there as well.



where:

Firmware Version — is a current firmware version installed on the device.

The firmware version looks like DKSF PPP.VV.SS.C-M (for example, DKSF 70.6.3.A-1), where:

- DKSF — is a specific prefix for all firmware versions of the company NetPing East Ltd.;
- PPP — is a number of the device model for which the firmware version is designed.

Usually but not necessarily, the numbers of projects coincide with the project number of the hardware of the device.

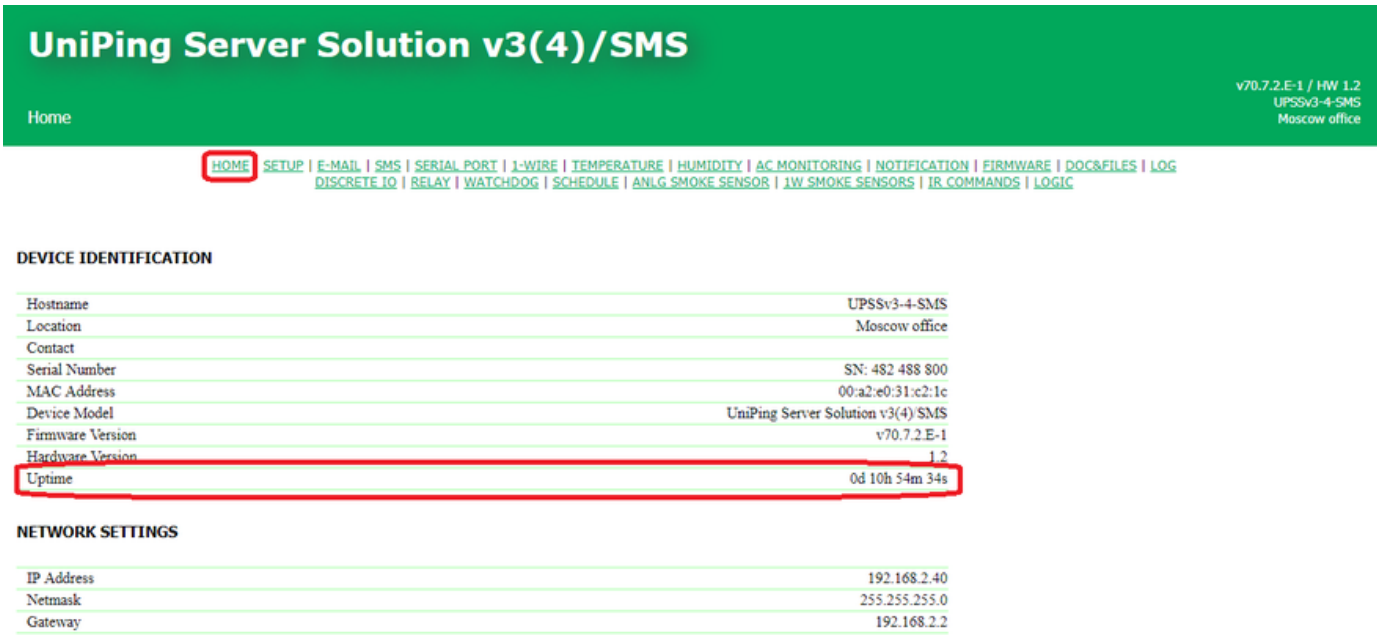
- VV — is a version number. Versions are numbered starting from 1. The version number is changed to the next one if, during the development, there is an extensive expansion or change in functionality функциональности;
- SS — is a subversion number. The subversion number is changed at any firmware update, including bug fixes, updating new modules, optimization;
- C — is a symbol that shows the type of this firmware version. R or A — mean a stable Russian firmware version, B — is a testing version or the first version of the new firmware and E — is a stable English firmware version;
- M — is a numeric suffix that shows the modification (variant) of the device model, for which the firmware is designed.

Hardware Version — is a version of the circuit board and/or equipment of the device.

Serial Number — is a unique ID number of a device. It should coincide with the number on the sticker on the device. A serial number of a device cannot be changed.

[ENG] 2.5. [DKSF 70/71.7 IU] How to See the Uptime?

The uptime of a device is displayed at the home page of a device web interface:



where:

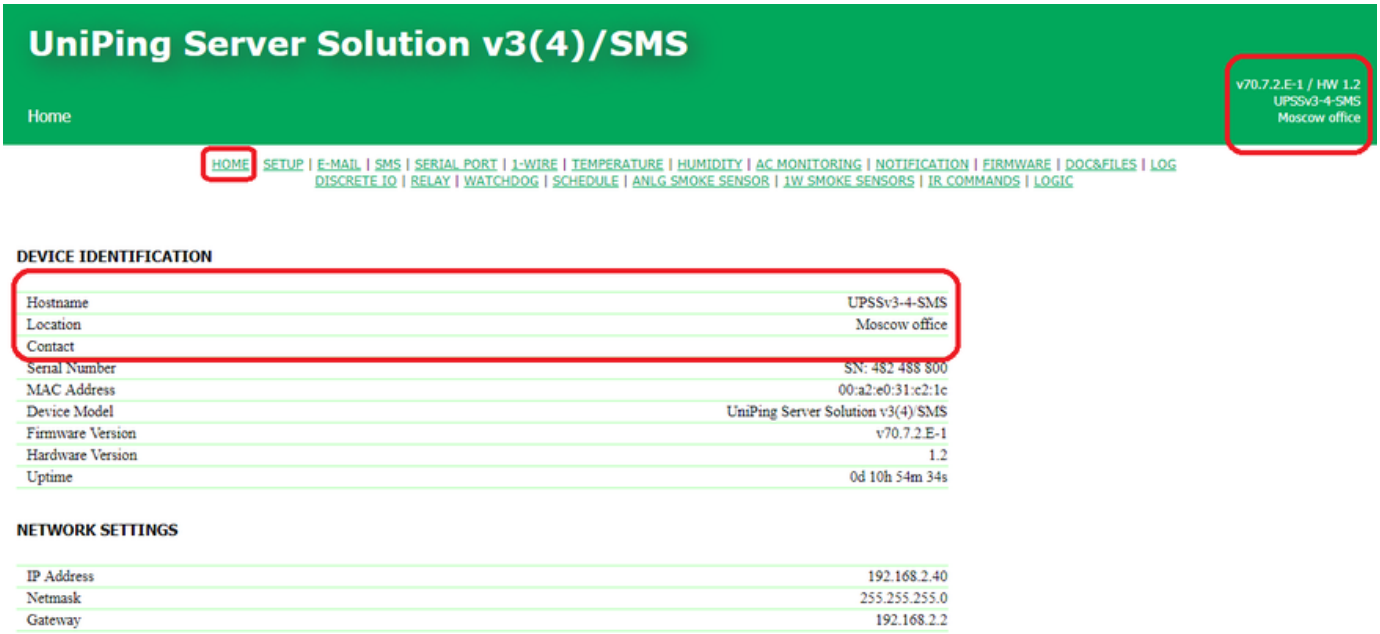
Uptime — is the uptime of a device since the last switching on or rebooting.

An alternative variant for advanced users is using SNMP v1 protocol to read the OID value using the command Get:

OID	Name	Type	Access	Description
.1.3.6.1.2.1.1.3.0	sysUpTime	TIMETICKS	READ	The uptime since the last switching on or rebooting.

[ENG] 2.6 [DKSF 70/71.7 IU] Where Can I see the Hostname, Location, and Contacts of a Device?

A hostname of a device, its location, and the owner's contacts are represented at the home page of a device web interface. In addition, there is a hostname and a location of a device shown on the right of all pages.



where:

Hostname — is the name of a device. It allows distinguishing between several NetPing devices of one type according to their hostnames. A hostname is represented at the home page and in a heading of a web interface and is sent in the notifications and available via SNMP.

Location — is a description of the location of the installation of a NetPing device. It is represented at the homepage and in a heading of a web interface, is available via SNMP.

Contact — is contact data (usually an email) of an administrator. It is represented at the homepage and is available via SNMP.

All three variables can be set (change) on the SETUP page of a web interface.

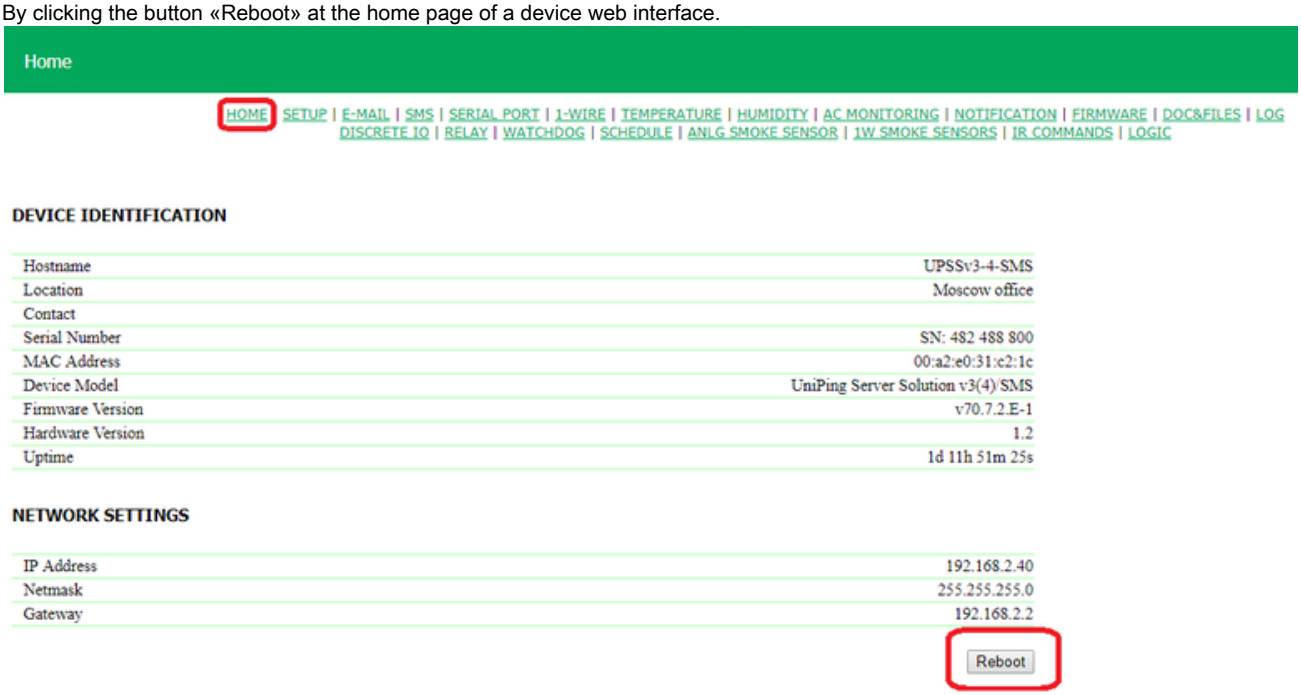
For advanced users, a primary access option is using SNMP v1 protocol by reading corresponding OIDs using a command Get:

OID	Name	Type	Access	Description
.1.3.6.1.2.1.1.5.0	sysName	DISPLAYSTRING (SIZE (0..255))	READ/WRITE	The domain name of a device
.1.3.6.1.2.1.1.6.0	sysLocation	DISPLAYSTRING (SIZE (0..255))	READ/WRITE	Location of a device
.1.3.6.1.2.1.1.4.0	sysContact	DISPLAYSTRING (SIZE (0..255))	READ/WRITE	Contact data

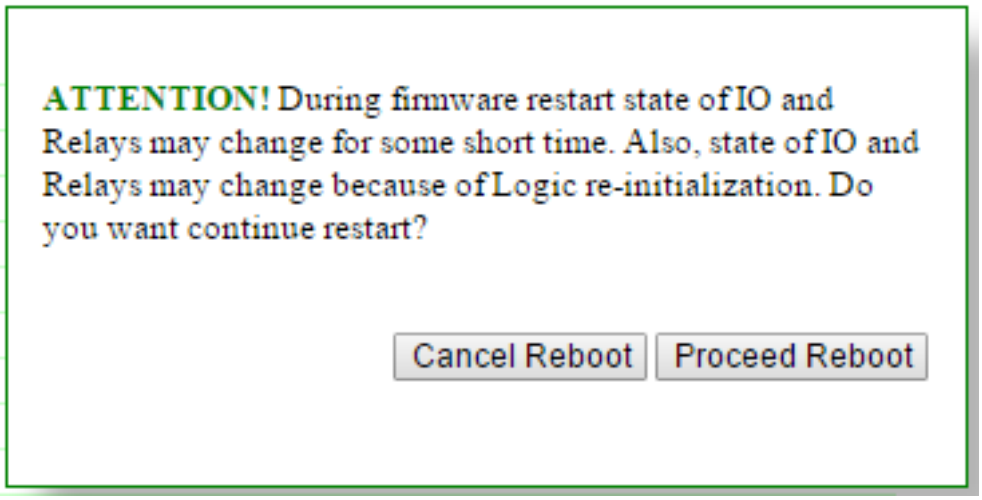
[ENG] 2.7. [DKSF 70/71.7 IU] How to Restart the Firmware of a Device?

The firmware can be restarted in two ways:

1. By clicking the button «Reboot» at the home page of a device web interface.



After this, the system is going to show the informational notification with the confirmation of the firmware restart.



When clicking the button «Proceed Reboot», yellow CPU LEDs at Ethernet ports are going to blink several times, and the firmware is going to restart. The uptime of a device is going to reset to 0d 0h 0m 0s.

2. Using an SNMP v1 protocol by setting OID values by the command Set:

OID	Name	Type	Access	Description
.1.3.6.1.4.1.25728.911.1.0	npSoftReboot	Integer	READ/WRITE	Software reboot of the firmware when writing the value «1» (analog to the rebooting of a device through a web interface).
.1.3.6.1.4.1.25728.911.3.0	npForceReboot	Integer	READ/WRITE	An immediate forced restart of the firmware when writing the value «1» (resetting a processor, the same as when switching power on).

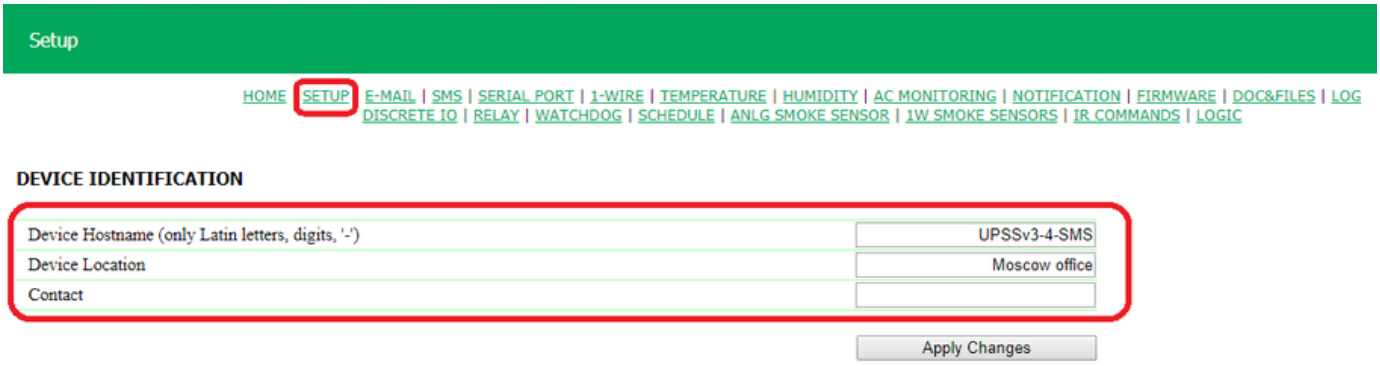
3. SMS-командой «RB20», A general view of the restart command (details are given in the section «11.8. [DKSF 70/71.6 IU] How to Control a Device via SMS Commands?») is as follows:

```
NETPING RB20 community_w kkkkk
```

[ENG] 3. [DKSF 70/71.7 IU] Basic Configuration

[ENG] 3.1. [DKSF 70/71.7 IU] How to Set up a Hostname, Location, and Contacts of a Device?

To configure a name and a location of a device as well as the contact data, there is a need to go to the page «SETUP» of a device web interface:



In the section «Device identification», it is possible to configure:

Device Hostname — is the name of a device. It allows distinguishing between several NetPing devices of one type according to their hostnames. A hostname is displayed at the main page and in the heading of the web interface, in the email notification in the field «From:», in other notifications and is available via SNMP — sysName. On default: empty line.

Device Location — is a description of the installation place of a NetPing device. It is displayed on the home page and in the heading of the web interface. It is also available by SNMP. On default: empty line.

Contact — is contact data (usually, an email) of an administrator. It is displayed on the home page and is available via SNMP. On default: empty line.

After setting up all necessary parameters, click the button «Apply changes».

In addition, it is possible to configure these parameters using a SNMP v1 protocol by setting the OID values using the command Set:

OID	Name	Type	Access	Description
.1.3.6.1.2.1.1.5.0	sysName	DISPLAYSTRING (SIZE (0..255))	READ/WRITE	Name of a device
.1.3.6.1.2.1.1.6.0	sysLocation	DISPLAYSTRING (SIZE (0..255))	READ/WRITE	Location of a device
.1.3.6.1.2.1.1.4.0	sysContact	DISPLAYSTRING (SIZE (0..255))	READ/WRITE	Contact data

[ENG] 3.2. [DKSF 70/71.7 IU] Where Can I Change the Settings of the Network Interface?

To change network interface parameters, such as an HTTP port, a server and an SNMP agent, there is a need to go to the page «Setup» of a device web interface:

In the section «Network Settings» it is possible to configure:

IP Address – is a field for setting up or changing an IP address of a device. On default: 192.168.0.100

Netmask – is a field for setting up or changing a subnet mask, where the devices are. On default: 255.255.255.0

Gateway – is a field for setting up or changing an IP address of a gateway. The value 0.0.0.0 means a gateway is not specified and packages for other subnetworks will not be sent by a device. On default: 0.0.0.0

> A device will send any outgoing packages to a gateway address. Therefore, there is a need to specify an IP address of a gateway properly if there is a need to work with a device from other subnetworks.

DNS server – is a DNS server address. The value 0.0.0.0 means a DNS server is not specified, and a device will not send DNS requests. On default: 0.0.0.0

> A DNS server must use a recursive method. Cyrillic domain names are not supported. Domain names longer than 62 symbols are not supported either.

A DNS module works independently from other firmware modules. A DNS module saves responses from a DNS server into a DNS-cache of a device. Other firmware modules use this cache to determine an IP address, where a package needs to be sent. A request is not sent directly before sending a DNS package. If there is no correspondent entry in a DNS-cache in the moment of sending a package, then an outgoing package is discarded. A DNS cache size coincides with the number of hostnames (IP addresses) specified in the settings of a device.

Domain names are resolved and renewed in the next cases:

- Firmware start and restart;
- Saving settings through a web interface (if a domain name is changed);
- A life timeout of a DNS record, specified in the response from a DNS server

When a lifetime of a cache entry is expired, the entry is not removed from a cache. A device updates an expired entry from time to time. Other firmware modules use an outdated information until the entry is successfully updated.

If a DNS server does not respond, a device repeats its request three times. Afterwards, it repeats the request periodically nearly once a minute if there is still no response from a server. The requests are repeated when there is no server response and if there is an error in a server response, including the error «no such hostname».

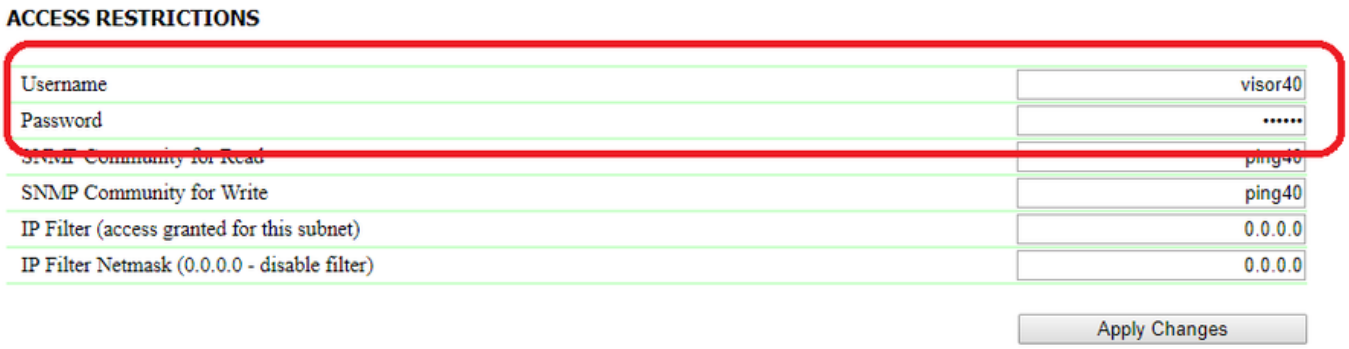
HTTP Server Port – is a field for configuring a port number, through which an embedded web interface operates. When connecting through a web browser to a device with a port number different from 80, there is a need to indicate the URL of the following appearance: http://x.x.x.x:nn, where x.x.x.x – is an IP address of a device, nn – is a port number, specified in settings of a device. On default: 80

SNMP Agent Port – is a field for configuring a UDP port number, which an SNMP agent listens to. On default: 161

After setting all necessary parameters, click the button «Apply changes».

[ENG] 3.3. [DKSF 70/71.7 IU] Changing a Username and a Password

To change the username and a password, there is a need to go to the page «SETUP» of a device web interface:



In the section «Access Restrictions», it is possible to configure:

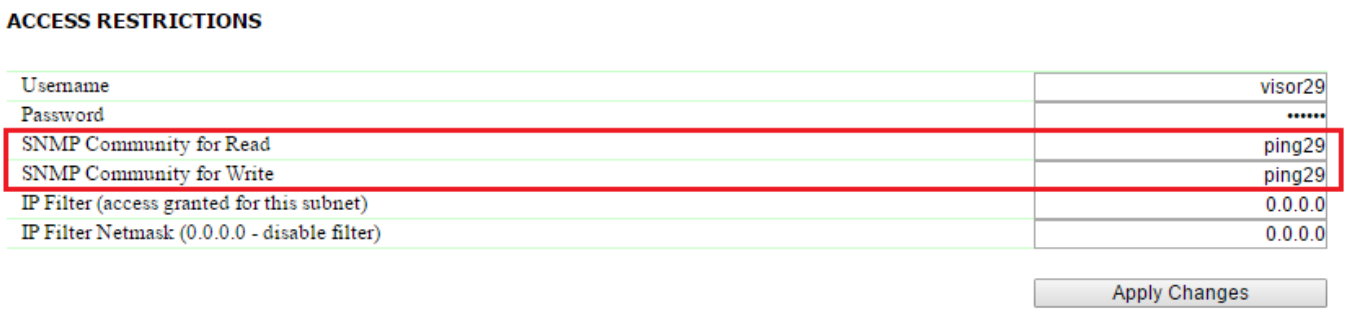
Username — is a field for setting up or changing a username when accessing a device using a web interface. Latin and Cyrillic letters, digits, and certain special characters are allowed. A maximum size if 16 characters. On default: visor.

Password — is a field for setting up or changing a user's password when accessing a device using a web interface. Latin and Cyrillic letters, digits, and certain special characters are allowed. A maximum size if 16 characters. On default: ping.

After setting all necessary parameters, click the button «Apply changes».

[ENG] 3.4. [DKSF 70/71.7 IU] How to Set the Community for SNMP?

To configure Community, there is a need to go to the web page «Setup» of a device web interface:



In the section «Access Restrictions» it is possible to configure:

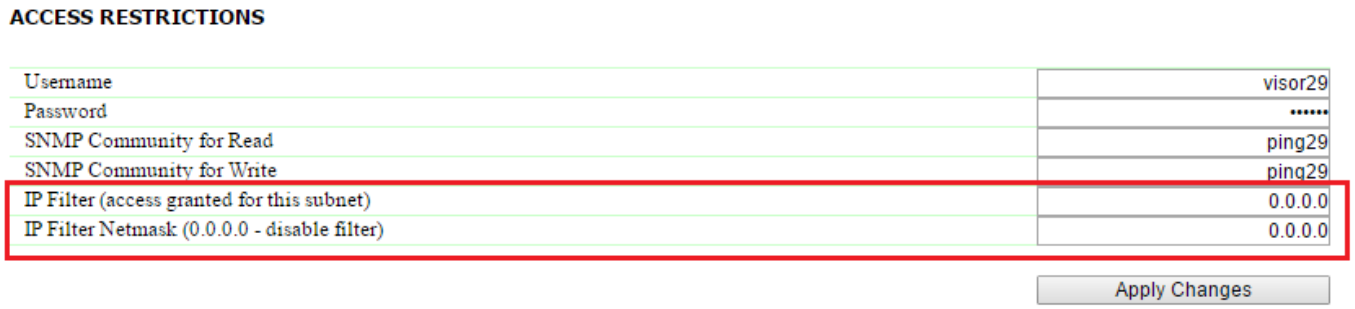
Community for Read – is a field for setting up or changing Community for read parameters of a device when accessing a device via an SNMP protocol. Its maximum size is 16 characters. On default: SWITCH

Community for Write – is a field for setting up or changing Community for write parameters of a device when accessing a device via an SNMP protocol. Its maximum size is 16 characters. On default: SWITCH

After setting up all necessary parameters, click the button «Apply changes».

[ENG] 3.5. [DKSF 70/71.7 IU] How to Restrict the Access to a Device?

To restrict the access to a device via HTTP and SNMP protocols, there is a need to go to the web page «Setup» of a device web interface:



In the section «Access Restrictions» it is possible to configure the following:

IP Filter – is a field determining an IP address or a subnetwork, from which it is allowed to configure and view parameters of a device via HTTP, SNMP protocols. A subnet mask specified in the field «IP Filter Netmask» is applied to the address indicated in the field «IP filter». As a result, there is a subnetwork, from which is it allowed to control a device. To allow the access for one IP address, there is a need to specify a mask 255.2 55.255.255 in the field «IP Filter Netmask». On default: 0.0.0.0

IP Filter Netmask – is a field for setting up or changing an IP filter netmask to access a device. Its value 0.0.0.0 means an access filter is disabled. On default: 0.0.0.0

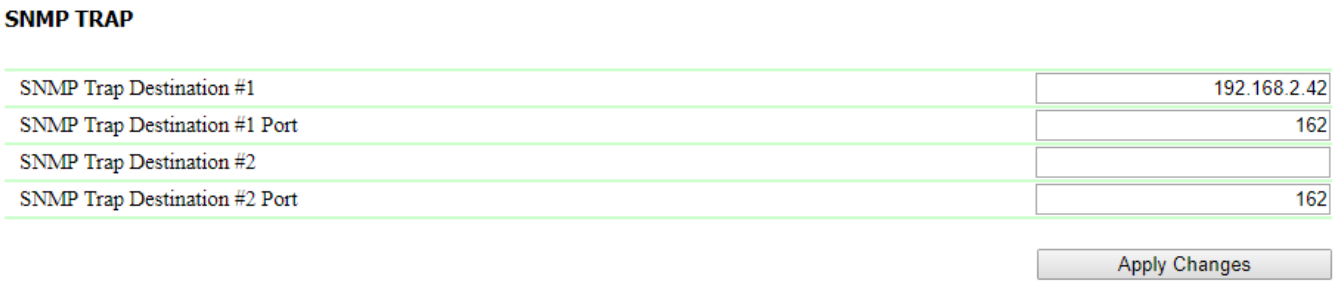
> A device will still respond to an ICMP request (ping) from any address even when access filters are specified.

After setting up all necessary parameters, click the button «Apply changes».

[ENG] 3.6. [DKSF 70/71.7 IU] There Is a Need to Send SNMP Trap-Notifications. How Can I Configure This?

IP-addresses for sending SNMP TRAP notifications are configured on the page «SETUP» of a device web interface. This group of settings allows setting up to two addresses where SNMP TRAP notifications will be sent to using an SNMP protocol.

> Events that are going to trigger these notifications are going to be specified on the other pages of a device web interface.



In the section «SNMP TRAP», it is possible to configure the next:

SNMP Trap Destination #1 — is a field for setting up or changing the first address where SNMP TRAP notifications are going to be sent to. It is acceptable to indicate either an IP address or a domain name. An empty field means that SNMP TRAP-notifications are not going to be sent. On default: the address is not specified.

SNMP Trap Destination #2 — is a field for setting up or changing the second address where SNMP TRAP notifications are going to be sent to. It is acceptable to indicate either an IP address or a domain name. An empty field means that SNMP TRAP-notifications are not going to be sent. O n default: the address is not specified.

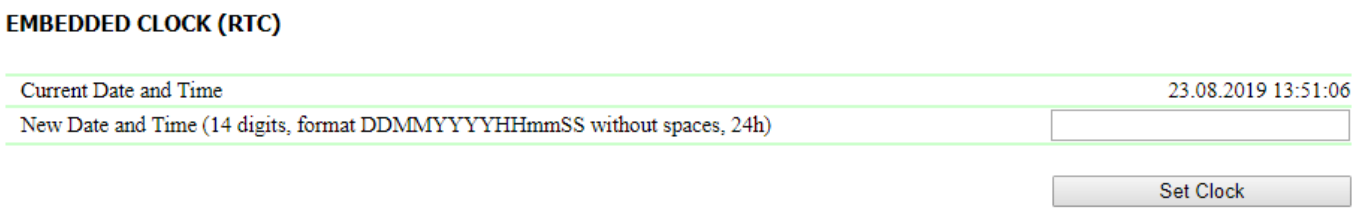
Port — is a field for setting up a port (for each address), where SNMP TRAP notifications are going to be sent to. On default: 162.

After setting all necessary parameters, click the button «Apply changes».

[ENG] 3.7. [DKSF 70/71.7 IU] How to Set the Clock?

SETTING THE CLOCK MANUALLY

To set the clock manually, there is a need to go to the page «SETUP» of a device web interface:



In the section «Embedded Clock (RTC)», it is possible to see and configure:

- Current Date and Time — is a field for viewing current time;
- New Date and Time (14 digits, format DDMMYYYYHHMMSS with no spaces) – is a field for setting the new time manually.

After setting the clock, click the button «Set Clock».

TIME SYNCHRONIZATION WITH EXTERNAL NTP SERVERS

To configure synchronization with the external NTP servers, there is a need to go to the page «SETUP» of a device web interface.

This group of settings allows setting addresses of NTP-servers (servers of precise time), according to which a device will set and adjust its internal clock. Overall, it is possible to set up to 2 NTP-servers. If the first NTP-serer is unavailable, then a device will attempt to synchronize its time with the second one. It is possible to check the correctness of the adjustment by generating a time synchronization event and viewing this event in the log at the page «LOG».

In the section «NTP Setup», there is a need to configure:

NTP Server #1 — configuring the first NTP- server. It is acceptable to indicate or an IP-address either a domain name. On default: ntp.netping.ru.

NTP Server #2 — configuring the second NTP- server. It is acceptable to indicate or an IP-address either a domain name. On default: the address is not specified.

> If an IP-address of an NTP-server is specified in the settings of the device, a device will attempt to get precise time and will synchronize its internal clock with the precise time if successful. After the time synchronization, there will be two records in the log that represent the time leap when the clock is reset to the precise time. If the time received at synchronization with an NTP-server is different from the time of the internal clock for less than 5 minutes, the clock is not reset. Instead, the pace of internal clock is changed in the way to make the internal time equal to the precise time received from the NTP-server. Thanks to this, there is no time leap in the list of events in the log, which simplifies the analysis of the log.

Timezone — a configuration of a local timezone. On default: UTC+03.00.

Daylight Saving Time (DST) — is a manual configuration of the daylight saving time. When a checkbox is checked, the internal clock of the device shifts an hour ahead. On default: a checkbox is not checked.

You can use freely available NTP servers on the Internet as NTP servers. For example, one from http://www.pool.ntp.org/, specifically:

- 0.europe.pool.ntp.org;
- 1.europe.pool.ntp.org;
- 2.europe.pool.ntp.org;
- 3.europe.pool.ntp.org

To use the NTP servers from the Internet, a device is going to have a gateway correctly configured, and a device should have the Internet connection via an NTP protocol.

To set a new date and time do the following: set the timezone and save the configurations, then fill in the fields of the new date and time according to the format specified at the webpage, and click the button «Apply changes».

[ENG] 3.8. [DKSF 70/71.7 IU] I Want to Configure SYSLOG. How Can I Do This?

Transfer of notifications to the SYSLOG server is configured at the page «Setup» of a device web interface.

> Events, according to which these notifications will be sent, are set at other pages of a device web interface.

In the section «SYSLOG» it is possible to configure the following:

SysLog Address – is an IP address of the SYSLOG server. A log file of a device will be duplicated completely on the SYSLOG server.

Syslog Facility – is a type of programs, for which logging is maintained.

Syslog Severity – indicates the urgency of notifications (from emergency to debugging).

After setting up all necessary parameters, click the button «Apply changes».

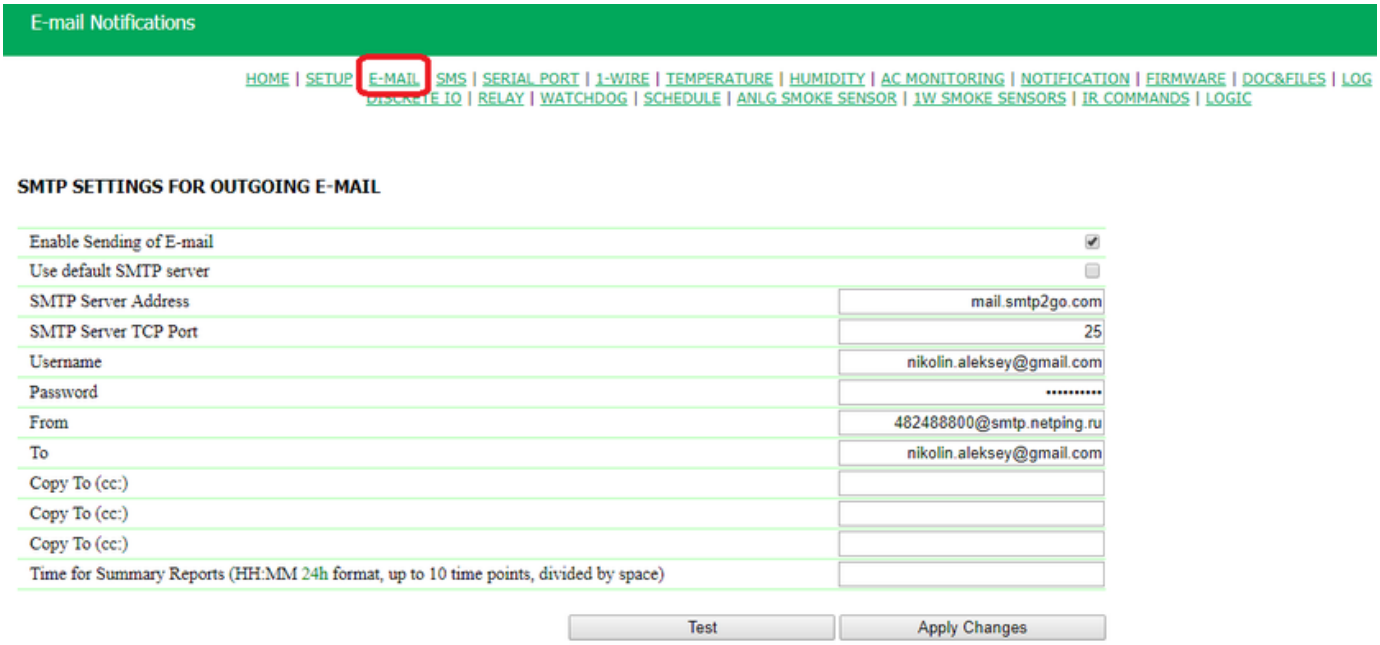
[ENG] 3.9. [DKSF 70/71.7 IU] How to Receive Notifications and Reports via Email?

To configure a module of sending email notifications and periodic email reports about statuses of sensors, there is a need to go to the page «EMA IL» of a device web interface. The equipment sends notifications using an SMTP protocol.

> The events that trigger sending email notifications are specified at the other pages of a device web interface.

> A subject of each email notification includes a serial number that is necessary to avoid automatic joining of notifications with the same subject into the same thread that is often done by email clients (such as gmail.com). Such joining disrupts the visual order of notifications in the array of incoming emails and makes it difficult to understand the consequence of notifications. When a serial number is added, the subject of the email is unique.
> The subject looks as follows: Sensor Status Report #7d732006.

> If the name of a device is specified, it is added to the field "From:" of the email together with the email address that is specified in the field of settings «From:)».
>
> How to specify a name for a device is described at the page «[ENG] 3.1. [DKSF 70/71.7 IU] How to Set up a Hostname, Location, and Contacts of a Device?».



where:

Enable Sending of Email — switching on or off email notifications. По умолчанию: a checkbox is checked.

Use Default SMTP Server — using default parameters of an SMTP server in NetPing that is designed for the free use at NetPing devices. On default: a checkbox is not checked.

SMTP Server Address — is an address of the email server of the outgoing mail. On default: empty line.

SMTP Server TCP Port — is a port of the email server. On default: 25.

Username — the username of a user of an SMTP server. On default: empty line.

Password — the user's password for the SMTP server. On default: empty line.

From — a sender's address. On default: empty line.

To — a destination address for email notifications. On default: empty line.

Copy to — addresses of the secondary recipients of the email notifications where a copy is sent. On default: empty line.

Time for Summary Reports (HH:MM 24 hour format, up to 1o time points divided by space) — is the time of the day when daily reports about the

statuses of sensors are going to be emailed. Up to 12 attempts per day. On default: empty line..

After setting the parameters, click the button «Apply changes».

Several errors that can be made when sending email-notifications are as follows:

sendmail: in a response to AUTH PLAIN, there are 535 Incorrect authentication data prompts — login and/or password are incorrect.

sendmail: email is withdrawn, IP server is unknown — the IP address of a server is unknown. Probably, there is no connection, and DNS cannot convert a hostname into an IP address.

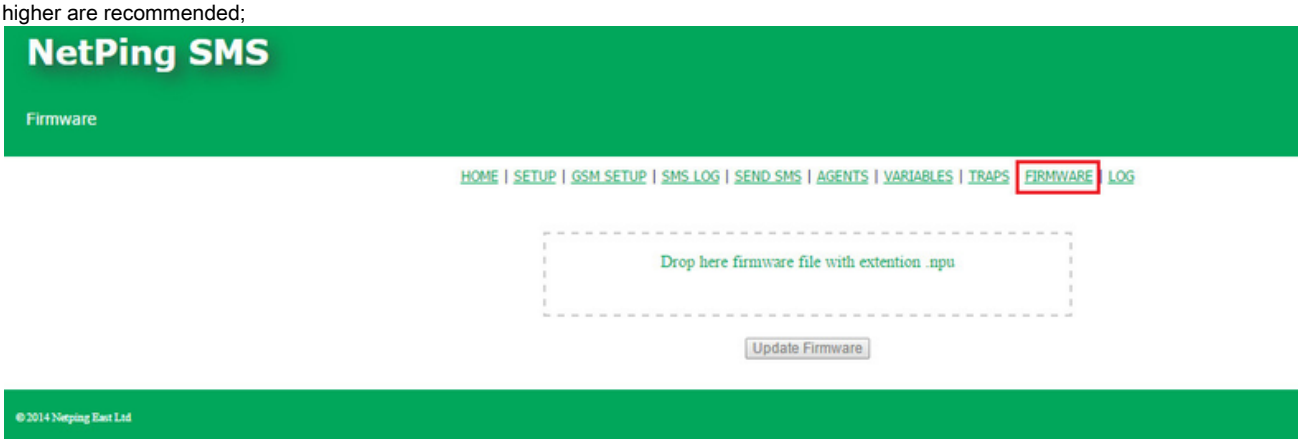
No room for new mail message — the queue of outgoing messages is full. For example, an email server is unavailable and a notification was placed in the queue.

> A device works only with the email servers that support an SMTP-protocol and authentication methods AUTH PLAIN and AUTH LOGIN, as well as a no-authentication method! At the same time, the device does not support SSL, TLS or any other encoding!

[ENG] 3.10. [DKSF 70/71.7 IU] How to Update the Firmware of the Device?

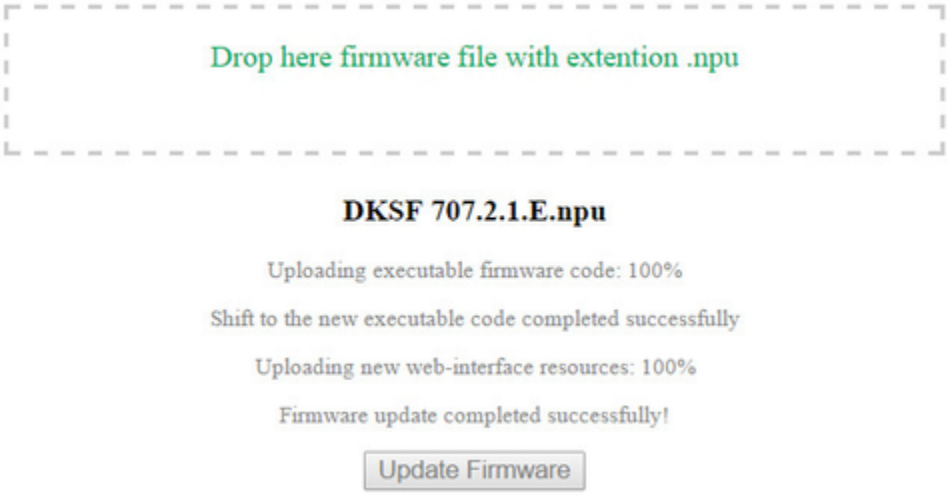
There is a need to do the following to update an embedded firmware version:

1. Download an up-to-date firmware from the official website of the company (section «Downloads»): http://www.netpingdevice.com.
2. Go to the page «Firmware» of a device web interface. You can easily update the firmware of a device from this page without using any specific software. To do that, you will need a browser supporting HTML 5 API. Google Chrome or Internet Explorer of the 9th version and higher are recommended;



3. Drag a firmware file to the indicated page area;
4. Wait until a firmware file is copied to a device
5. Click the button «Update Firmware»

Wait for the message on a successful operation completion:



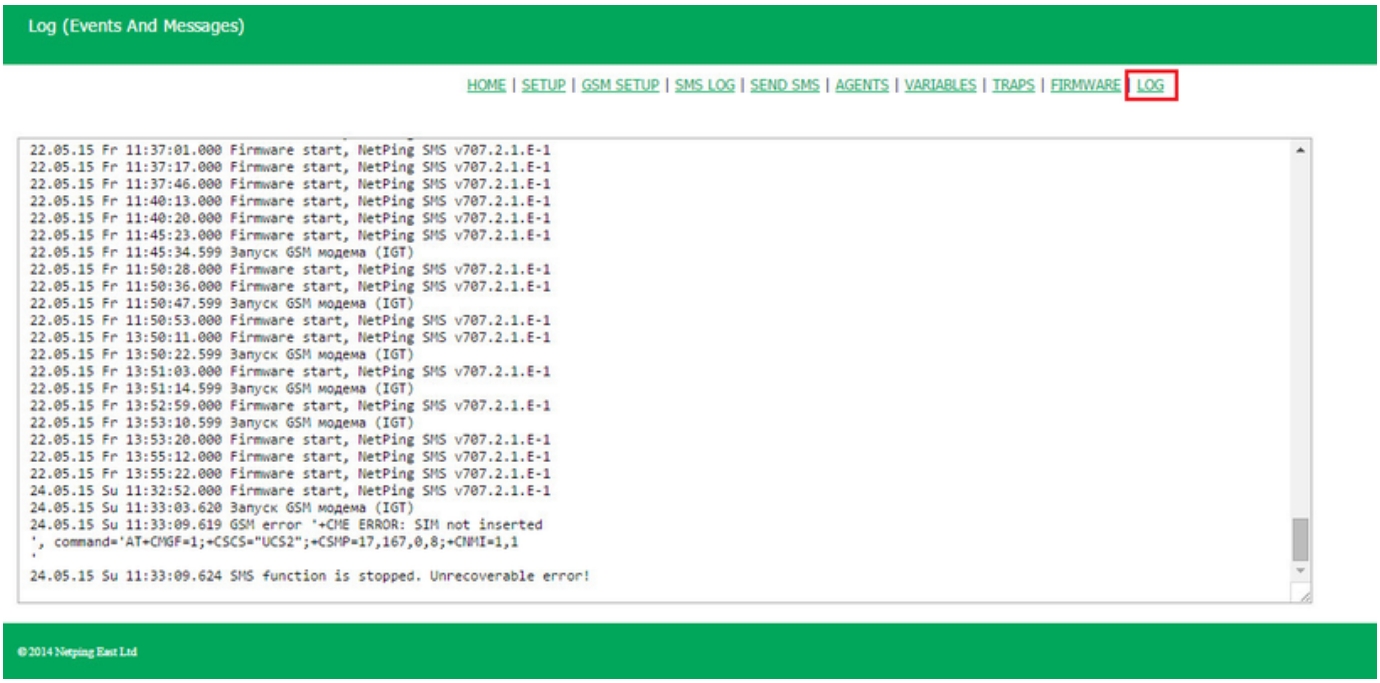
Retry if an updating process was interrupted. A web interface (pages «Home», «Setup», «Firmware») will be available even if the firmware was not successfully updated.

> Certain system settings may be changed after updating. Do not forget to check the most important operation parameters.

[ENG] 3.11. [DKSF 70/71.7 IU] The Log of a Device

The page «Log» of a device web interface represents a device operation. All events are saved in the log in a chronologic order. All notifications of the log are duplicated via SYSLOG protocol if an IP address of SYSLOG server is specified in the settings of a device.

The first time tag in the log is 01.01.70 Mon 00:00: 00.UTC. If an IP address of an NTP server is specified in the settings, a device will try to receive a precise time. If successful, a device will synchronize its internal clock with a precise time. After a time is synchronized in the log, two entries appear that represent a time jump when setting the clock correctly. If the time received when synchronising with an NTP server is different from the time of an internal clock for less than 5 min, its clock is not reset. The pace of internal clock is changed in the way for an internal time to coincide with a precise time received from an NTP server after a while. Therefore, there is no time jumps in the events list in a log, which makes analysing it easier.



GENERAL EVENTS

Operation Start (Reboot) – is written into the log when a device is turned on.

Clock Reset – is written into the log if a received time from an NTP server is different from an internal time for more than 5 min. The entry is displayed in two rows: the first row has a time tag before resetting an internal clock, and the second one is made just after a reset is made.

EVENTS FROM TEMPERATURE SENSORS

Thermo chan.N "XXXX":normal YYC – is recorded into the log if a mode of sending SNMP TRAP notifications from temperature sensors is configured, and a temperature on a temperature sensor is within the limits set by a user. YY – is a current temperature on a temperature sensor.

Thermo chan.N "XXXX": above normal YYC – is recorded into the log if a mode of sending SNMP TRAP notifications from temperature sensors is configured and a temperature on a temperature sensor is above the upper threshold, set by a user. N – is a number of a temperature sensor. XXXX – is a description of a temperature sensor, specified by a user at the page of a web interface. YY – is a current temperature on a temperature sensor.

Thermo chan.N "XXXX": below normal YYC – is recorded into the log if a mode of sending SNMP TRAP notifications from temperature sensors is configured and a temperature on a temperature sensor is below the lower threshold, specified by a user. N – is a number of a temperature sensor. XXXX – is a description of a temperature sensor, specified by a user at the page of a web interface. YY – is a current temperature on a temperature sensor.

Thermo chan.N "XXXX": failure – is recorded into the log if a mode of sending SNMP TRAP notifications from temperature sensors is configured and a temperature sensor does not respond (is not connected). N – is a number of a temperature sensor. XXXX – is a description of a temperature sensor, specified by a user at the page of a web interface. When a sensor operation is restored, a notification about a status of a temperature range is sent (see above).

EVENTS FROM IO LINES

Input/output: line N "XXXX": 0->1 – is recorded into the log if a mode of sending SNMP TRAP notifications from IO lines is configured, and an IO line has switched from the status «0» to the status «1». N – is a number of an IO line. XXXX – is a description of an IO line, specified by a user at the page of a web interface.

Input/output: line N "XXXX": 1->0 – is recorded into the log if a mode of sending SNMP TRAP notifications from IO lines is configured and an IO line has switched from the status «1» to the status «0». N – is a number of an IO line. XXXX – is a description of an IO line, specified by a user at the page of a web interface.

EVENTS FROM THE «WATCHDOG» MODULE

Watchdog: resetting chan.N "XXXX". A (IPA) YYYY, B (IPB) YYYY, C (IPC) YYYY – is recorded into the log when the Watchdog is triggered. N – is a number of a power management channel. XXXX – is a description of a power management channel, specified by a user at the page of a web interface. IPA, IPB, IPC – are IP addresses, specified in the settings of the «Watchdog».YYYY – is a status of corresponding requested IP address. It may be: responds, silent, ignores.

Watchdog: chan.N "XXXX". - a limit of repeated resets is reached (Y). Resets are paused. – is recorded into the log if a limit of consequent resets of a connected device is reached in the operating mode «Watchdog». N – is a number of a power management channel. XXXX - is a description of a power management channel, specified by a user at the page of a web interface.Y – is an amount of consequent resets of a connected device that has been performed.

Watchdog: chan.N "XXXX" reset. - a response is received. Resetting pause is over.

SYSLOG SUPPORT

All notifications in the log are duplicated by sending notifications via SYSLOG protocol if addresses of SYSLOG server are specified in the settings of a device at the page «Setup» of a web interface.

SYSLOG server is convenient to use for centralized collecting of notifications about events that take place at numerous devices and computers, operating in the network, particularly about the events at Netping devices.

[ENG] 3.12. [DKSF 70/71.7 IU] How to Disable All Notifications Quickly?

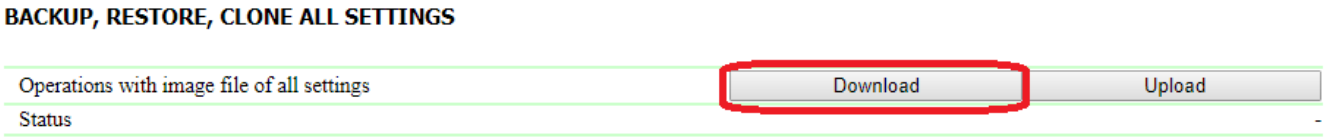
It is possible to disable all notification types at the page «Setup» of a device web interface. To do this, there is a need to check a checkbox «Disable all notifications» and click the button «Apply changes»:

> The setting «Disable all notifications» does not disable notifications sent to the log file and SYSLOG.

[ENG] 3.13. [DKSF 70/71.7 IU] Backing up and Restoring a Device Configuration

Backing up a configuration

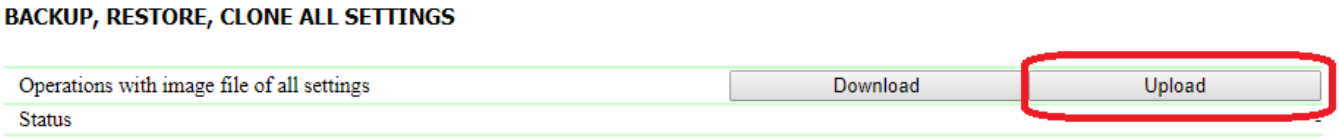
To save a backup copy of a setup configuration of a device into a binary file, there is a need to go to the page «SETUP» of a device web interface. In the section «Backup, Restore, Clone All Settings», click the button «Download»:



After this, a local disk of the PC is going to have a file with the settings and with the extension of .bin, for example, USS-001-125-ServerRoom-1_setup.bin (before the underscore in the file name, there is a name of a device that is specified on the page «SETUP » of a web interface).

Restoring a Configuration

To download a backup copy of the setup configuration from a binary file to the device, there is a need to go to the page «SETUP» of a device web interface. In the section «Backup, Restore, Clone All Settings», click the button «Upload»:



Afterward, there is a need to select a necessary file of the .bin format to upload the configuration. Successful uploading is followed by the representation of the status «Uploading of settings completed successfully» with the following reboot of the device:

When restoring the settings, the indicated parameters are saved the same:

- A name of a device;
- IP address;
- Subnet mask;
- Gateway;
- HTTP server port

This can be used for the quick setting reproduction among identical devices. Specified parameters are not cloned and should be configured manually and individually for every device.

A binary configuration file can contain sensitive information (passwords, IP addresses) in the unencrypted.
If this is a dangerous situation, then the file should be stored using external safety means, for example, to put them to the archive protected with a password.

Before uploading the configuration to the EEPROM, the identity of the versions of "donor" and "acceptor" of settings is automatically tested. If the version of the «donor» is not suitable, then there is no uploading, and the error notification is displayed: «The image of settings is incompatible!».

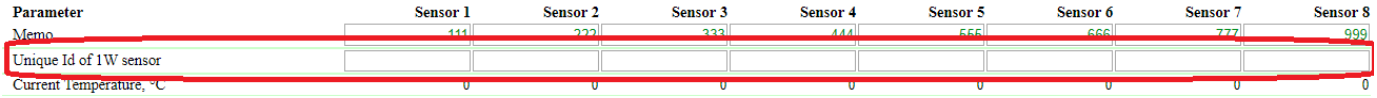
[ENG] 4. [DKSF 70/71.7 IU] Working with Temperature Sensors

[ENG] 4.1. [DKSF 70/71.7 IU] Which Temperature Sensors Are Supported by a Device?

A device supports connecting temperature sensors of the 1-Wire type.

> A device does not support temperature sensors of the T811, TS and WT types.

To connect a 1-Wire temperature sensor, there is a need to link its unique ID number to the sensor X in the field «Unique ID of 1W sensor» at the page «TEMPERATURE».



Parameter	Sensor 1	Sensor 2	Sensor 3	Sensor 4	Sensor 5	Sensor 6	Sensor 7	Sensor 8
Memo	111	222	333	444	555	666	777	999
Unique Id of 1W sensor								
Current Temperature, °C	0	0	0	0	0	0	0	0

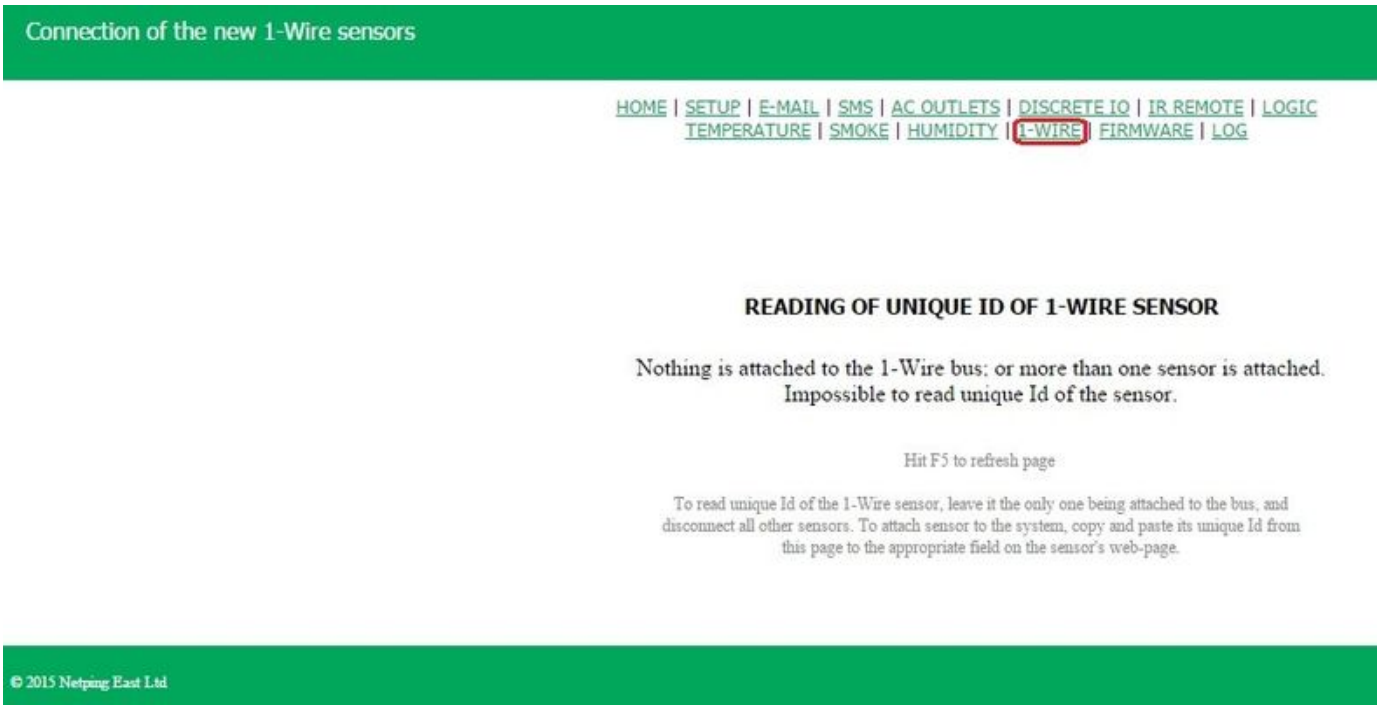
A unique ID of a 1-Wire sensor can be learned from the section «4.2. [DKSF 70/71.7 IU] How to Detect a Unique Id Number of a 1-Wire Temperature Sensor?».

Temperature values and statuses of temperature sensors are updated automatically with no need to reload a web page manually.

It is possible to connect up to eight temperature sensors of a 1-Wire type to a device in total.

[ENG] 4.2. [DKSF 70/71.7 IU] How to Detect a Unique Id Number of a 1-Wire Temperature Sensor?

To read a unique Id of a 1-Wire sensor, there is a need to go to the page «1-WIRE» of a device web interface:



To determine a unique Id using a web interface, there is a need to do as follows:

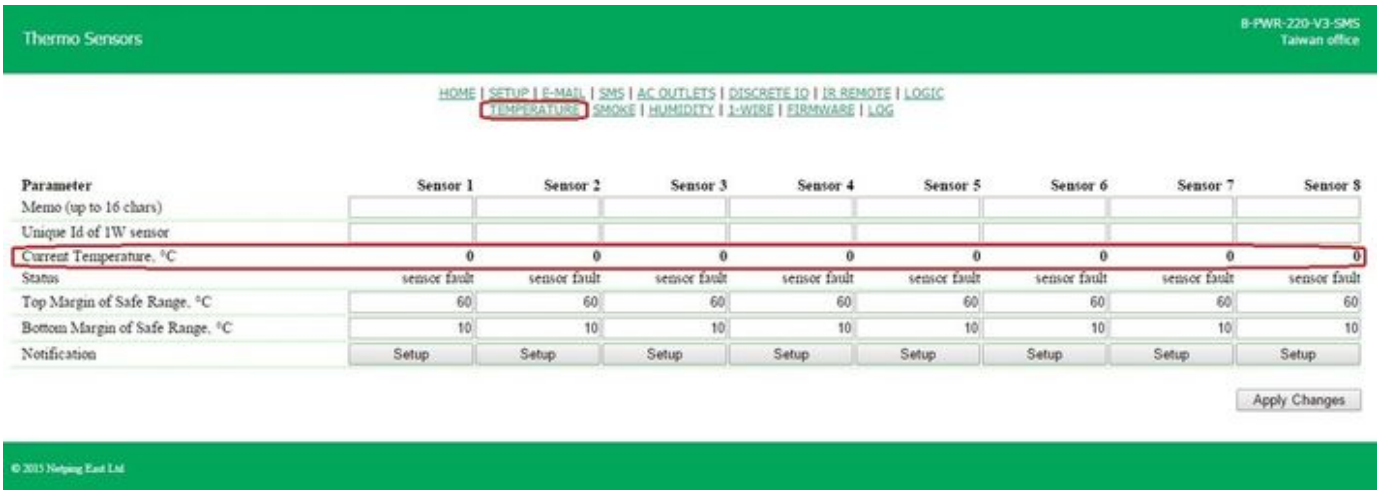
1. Unplug all 1-Wire sensors from a device;
2. Plug a sensor, which unique number you want to know to a device;
3. Go to the address http://<ip_address_of_a_device>/ow_new.cgi or go to the page «1-WIRE» of a web interface. A unique Id of a sensor will be displayed in the browser window.

A unique number of a 1-Wire sensor looks like the following: 2818 0ea2 0600 0039 (16 hexadecimal digits 0..9,a..f).

To plug a 1-Wire sensor, copy its unique number from this page to a corresponding field at the page of a web interface.

[ENG] 4.3. [DKSF 70/71.7 IU] Where to See the Current Temperature?

To see a current temperature of temperature sensors, there is a need to go to the page «TEMPERATURE» of a device web interface:



Temperature values and sensor statuses are updated automatically not less than four times a minute with no need to reload a page manually.

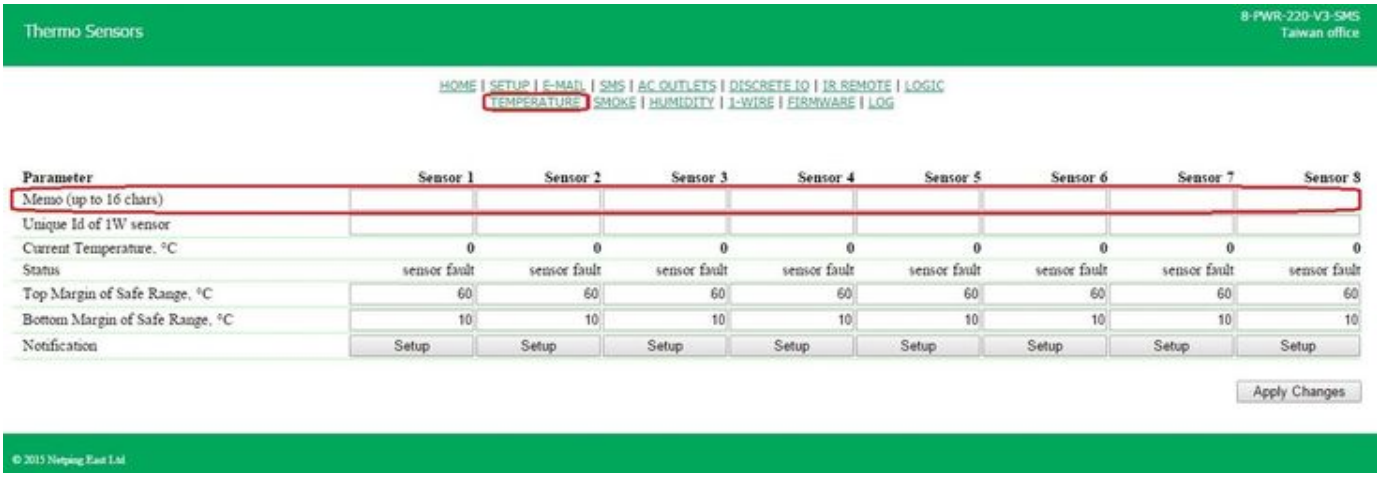
Current Temperature, °C – displays a current temperature of a sensor in degrees of Celcius. A temperature value is automatically updated from time to time without reloading a web page.

Status – displays a current status of a temperature sensor. Possible values are:

- Failure – a temperature sensor is not connected or does not respond;
- Normal – a temperature sensor responds, and a temperature value is within the limit of a specified range for this temperature sensor;
- Above normal – a temperature sensor responds, and a temperature value is above a specified range for this temperature sensor;
- Below normal – a temperature sensor responds, and a temperature value is below a specified range for this temperature sensor.

[ENG] 4.4. [DKSF 70/71.7 IU] Is It Possible to Set a Description for Temperature Sensors?

To set a description for temperature sensors, there is a need to go to the page «TEMPERATURE» of a device web interface:



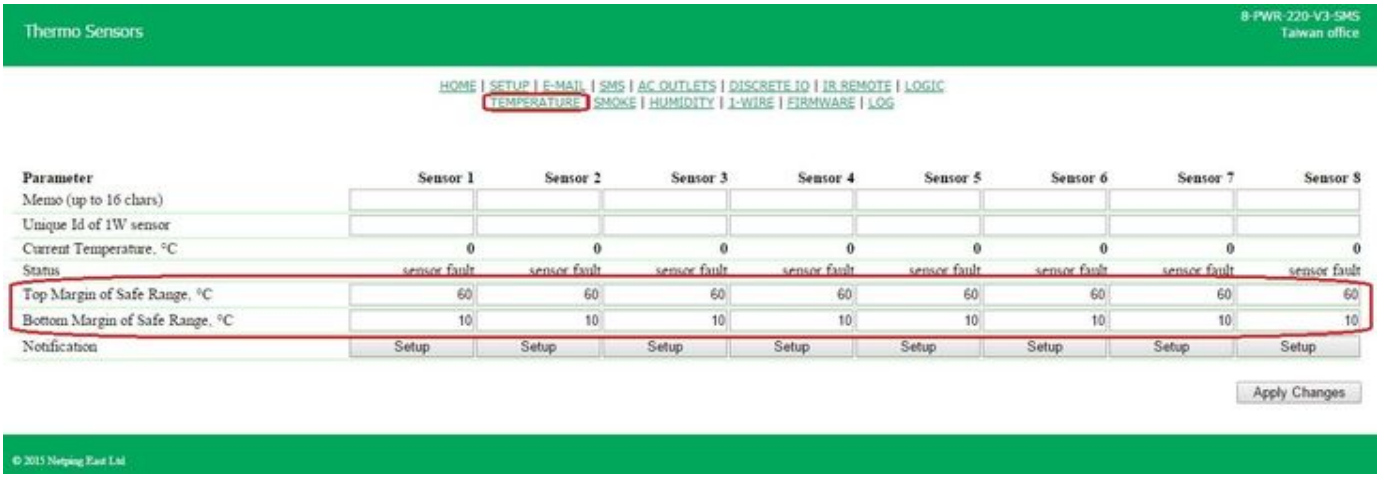
A description for temperature sensors is set in the field «Memo».

Memo – is a field for setting a brief description of a temperature sensor. A memo is used in SYSLOG and log notifications, and is also included into SNMP TRAP, SMS, e-mail notifications, email reports about a status of sensors. Its maximum size is 16 characters. On default: empty line

After changing the settings, there is a need to save the parameters by clicking the button «Apply changes».

[ENG] 4.5. [DKSF 70/71.7 IU] Setting Up the Top and the Bottom Margins of the Norm for the Temperature Sensor

To configure a top and bottom margin of a safe range for a temperature sensor, there is a need to go to the page «TEMPERATURE» of a device web interface:



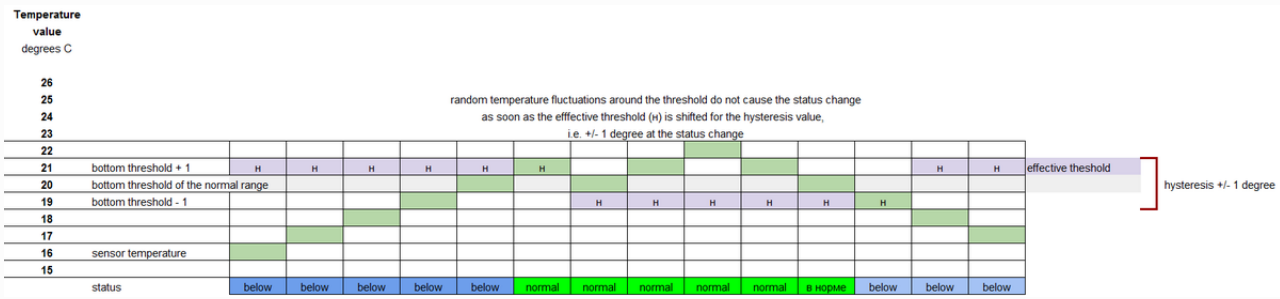
where:

Top Margin of Safe Range, °C – is a field for setting a top margin of a temperature range for each temperature sensor. A temperature range is used to specify conditions for generating SNMP TRAP and Syslog notifications as well as e-mail and SMS notifications (in a device with an embedded GSM modem). On default: 60

Bottom Margin of Safe Range, °C – is a field for setting a bottom margin of a temperature range for each temperature sensor. A temperature range is used to specify conditions for generating SNMP TRAP and Syslog notifications as well as e-mail and SMS notifications (in devices with an embedded GSM modem). On default: 10

To prevent frequent triggering of a top and bottom margins, a switching hysteresis of 1°C is used.

A hysteresis sets a «corridor» around a specified temperature, within the limits of which top and bottom margins of a safe range do not respond to temperature oscillations. This feature allows to avoid frequent random notifications from a temperature sensor caused by natural spontaneous oscillations of a temperature measured by a sensor. If a current status of a temperature sensor is «above normal», then a threshold for switching a status is a specified temperature minus a hysteresis value. And vice versa, if the current status is «below normal», then a threshold for switching is a specified temperature plus a hysteresis value. As soon as a temperature increases or decreases reaching a threshold value (taking a hysteresis into account), thus leaving margins of a «corridor», a temperature status is changed. Operation logic of hysteresis is explained in the picture below.



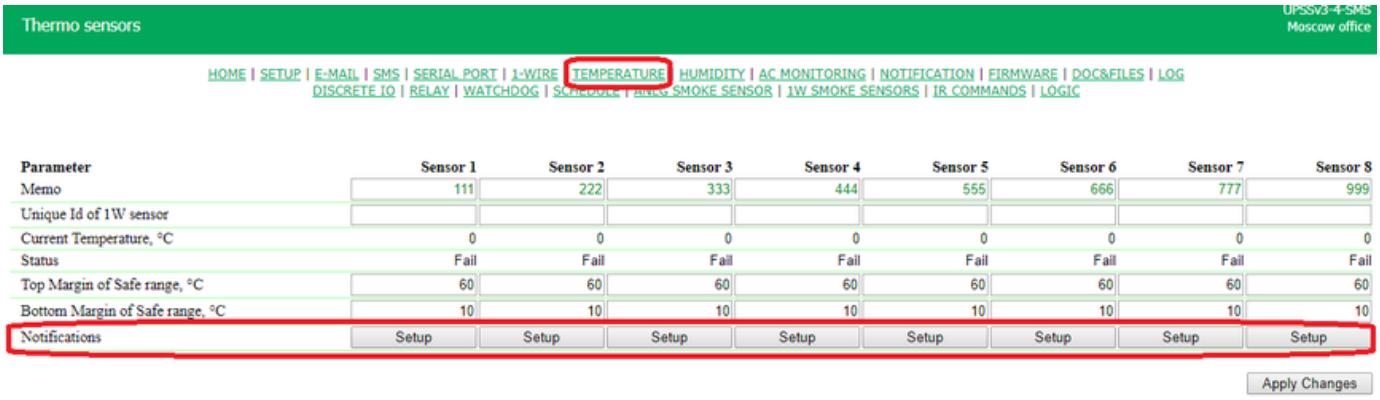
Status – displays a current status of a temperature sensor. Its possible values are:

- Failure – a temperature sensor is not connected or does not respond;
- Normal – a temperature sensor responds and a temperature value is within the margins of a specified range for this temperature sensor;
- Above normal - a temperature sensor responds, and a temperature value is above a specified range for this temperature sensor;
- Below normal - a temperature sensor responds, and a temperature value is below a specified range for this temperature sensor

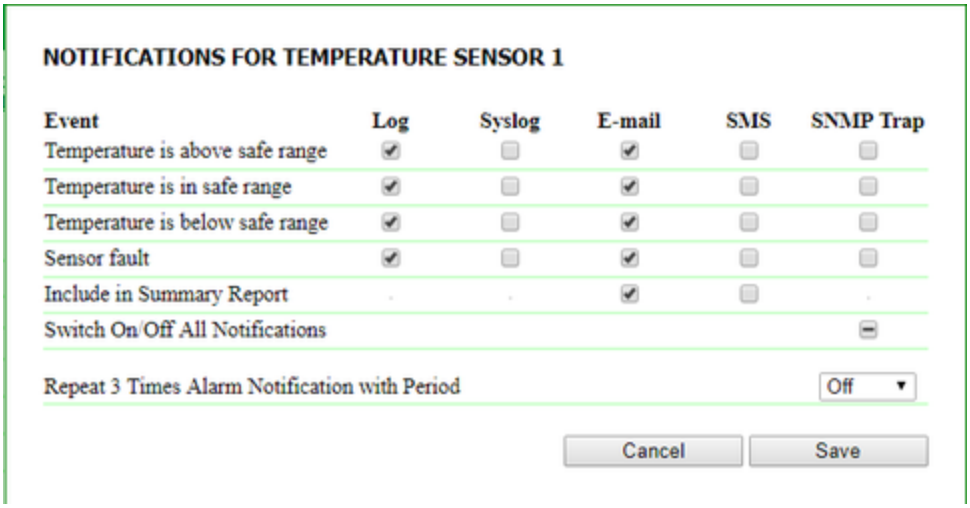
After changing the settings, there is a need to save the parameters by clicking the button «Apply changes».

[ENG] 4.6. [DKSF 70/71.7 IU] I Want to Configure Sending the Notifications When a Status of a Temperature Sensor Is Changed. How to Do This?

Sending notifications when a status of a temperature sensor is changed is configured at the page «TEMPERATURE» of a device web interface:



When clicking the button «Setup», the menu of settings appears for configuring notifications of the next types: Log, Syslog, Email, SMS (in devices with a built-in GSM modem) and SNMP Trap:



where:

- Temperature is above safe range — is check boxes enabling sending notifications when the top margin of the safe temperature range is exceeded. On default: a checkbox is not checked.
- Temperature is in safe range — is checkboxes enabling sending notifications if the current temperature is back to the safe range. On default: a checkbox is not checked.
- Temperature is below safe range — is checkboxes enabling sending notifications if the current temperature falls below the bottom margin of the safe range. On default: a checkbox is not checked.
- Sensor fault — is checkboxes enabling sending notifications in case if a sensor fails. On default: a checkbox is not checked.
- Include in Summary Report — is checkboxes enabling sending periodic reports about the status of a sensor via email and/or SMS. The time of sending reports is indicated at the pages «SMS» and «EMAIL». On default: a checkbox is not checked.
- Switch On/Off All Notifications — is a checkbox that switches on and off all possible notification types for all events at once. On default: a checkbox is not checked.
- Repeat 3 Times Alarm Notification with Period — is an option for the third-time repeats of the alarm notification with the specified interval (5, 30 minutes, 2, 6, 12, 24 hours). If readings are back to the safe range, repeats are stopped. A repeated notification contains the time of the initial event (for example, 23:21:15.719 Thermo: chan.1 +26C, above the safe range (10..20C) since 01.06 23:16).

After setting up all necessary settings, click the button «Save».

[ENG] 5. [DKSF 70/71.7 IU] Working with Humidity Sensors

[ENG] 5.1. [DKSF 70/71.7 IU] Which Humidity Sensors Are Supported by a Device?

A device supports humidity sensors of a 1-Wire type.

> A device does not support humidity sensors of an WS type.

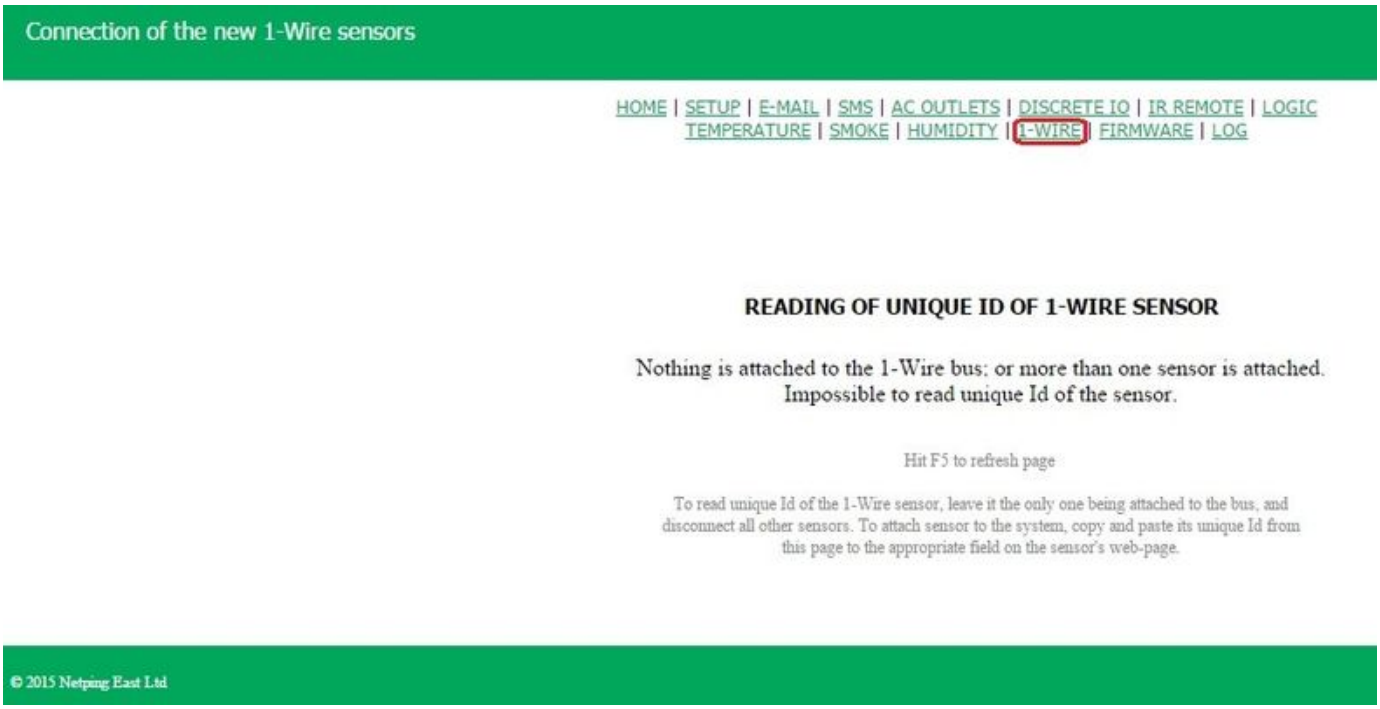
A unique Id of a 1-Wire sensor can be learned from the section «5.2. [DKSF 70/71.7 IU] How to Determine a Unique Id of a 1-Wire Humidity Sensor?».

Values of relative humidity, temperature, and status of humidity sensors are updated automatically with no need to reload a web page manually.

It is possible to connect up to four humidity sensors to a device.

[ENG] 5.2. [DKSF 70/71.7 IU] How to Determine a Unique Id of a 1-Wire Humidity Sensor?

To read a unique Id of a 1-Wire sensor, there is a need to go to the page «1-WIRE» of a device web interface:



To determine a unique Id using a web interface, there is a need to do as follows:

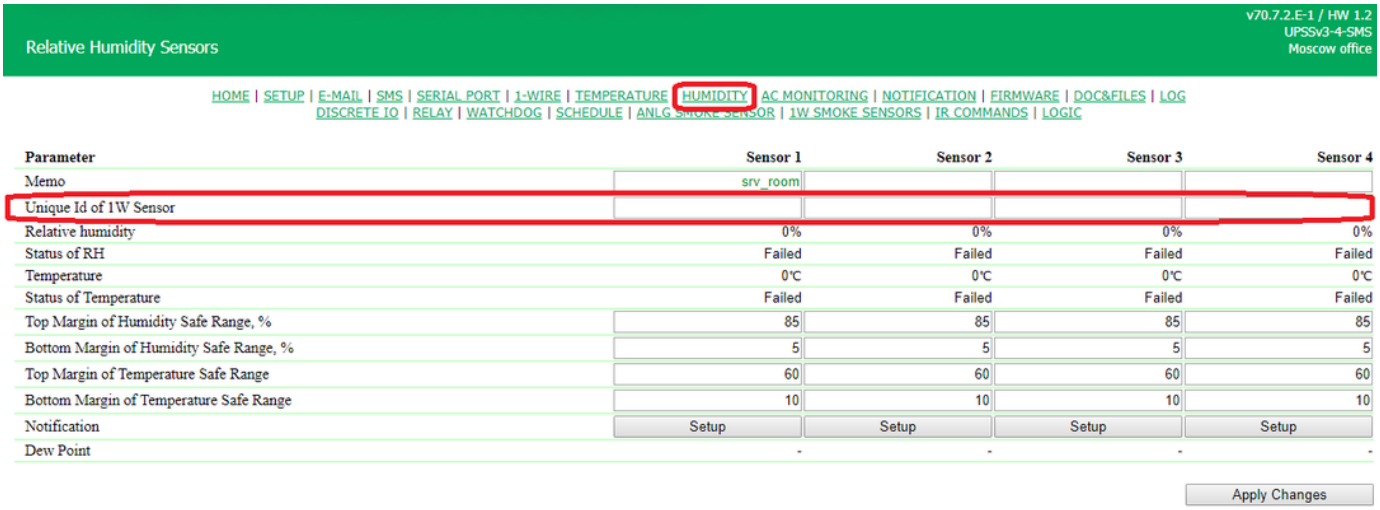
1. Unplug all 1-Wire sensors from a device;
2. Plug a sensor, which unique number you want to know to a device;
3. Go to the address http://<ip_address_of_a_device>/ow_new.cgi or go to the page «1-WIRE» of a web interface. A unique Id of a sensor will be displayed in the browser window.

A unique number of a 1-Wire sensor looks like the following: 2818 0ea2 0600 0039 (16 hexadecimal digits 0..9,a..f).

To plug a 1-Wire sensor, copy its unique number from this page to a corresponding field at the page of a web interface.

[ENG] 5.3. [DKSF 70/71.7 IU] Initial Configuration of Humidity Sensors

At the page «HUMIDITY» of a device web interface, readings of humidity sensors connected to a device are displayed. Up to four humidity sensors of the 1-Wire model line can be connected to a device.



To connect a sensor, indicate its unique Id number in the field «Unique Id of 1W sensor».

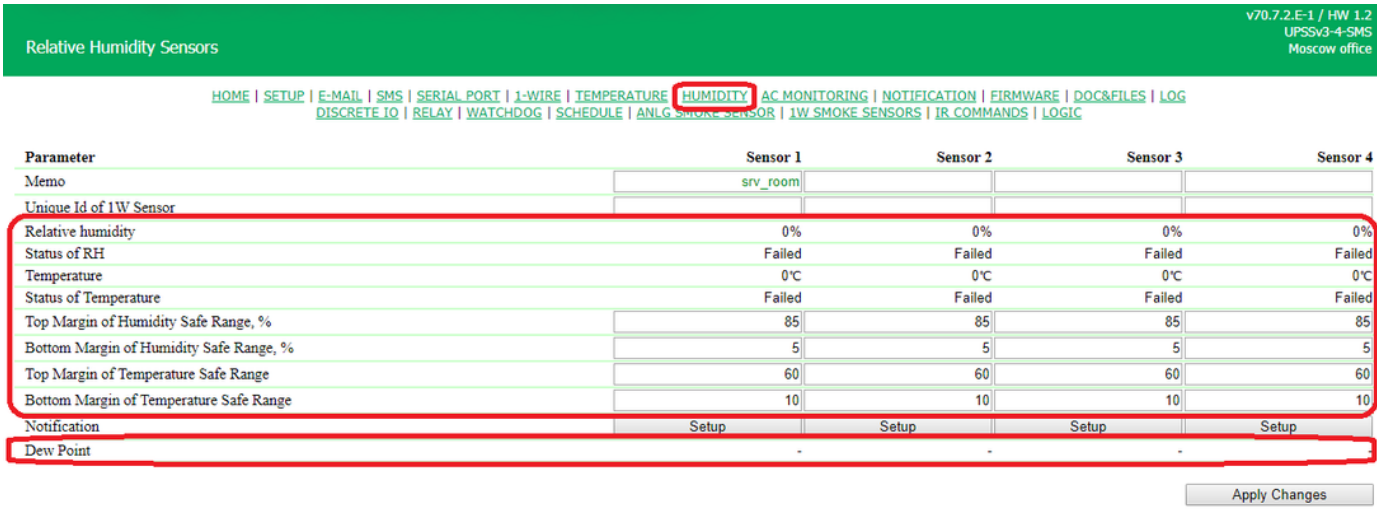
A unique Id of 1W sensor looks like: 2818 0ea2 0600 0039 (consists of four groups of hexadecimal digits 0...9 a...f.). On default: empty line.

A unique Id number of a 1-Wire sensor can be learned in two ways:

1. A unique Id of a 1-Wire humidity sensor can be applied to the sticker on the sensor itself;
2. A unique Id of a 1-Wire humidity sensor can be read from the sensor, and the procedure is described at «5.2. [DKSF 70/71.7 IU] How to Determine a Unique Id of a 1-Wire Humidity Sensor?».

[ENG] 5.4. [DKSF 70/71.7 IU] Viewing Readings and Configuring Parameters of Humidity Sensors in a Web Interface

To view the readings and configure parameters of humidity sensors, there is a need to go to the page «HUMIDITY» of a device web interface:



where:

Relative humidity — are readings of a sensor that determines the relative humidity, in %.

Status of RH — this parameter defines the status of a humidity sensor in the current moment of time. Possible variants: «failed», «below safe range», «normal», «above safe range».

Temperature— are readings of a temperature sensor that is built in a humidity sensor, in °C.

Status of Temperature — this parameter defines the status of a temperature sensor that is built in a humidity sensor, in the current moment of time. Possible variants: «failed», «below safe range», «normal», «above safe range».

Top Margin of Humidity Safe Range, % — is a humidity value, when exceeding which, the sensor is switched to the status «above safe range». Hysteresis ± 1 percentage point. On default: 85.

Bottom Margin of Humidity Safe Range, % — is a humidity value, when falling below which, the sensor is switched to the status «below safe range». Hysteresis ± 1 percentage point. On default: 5.

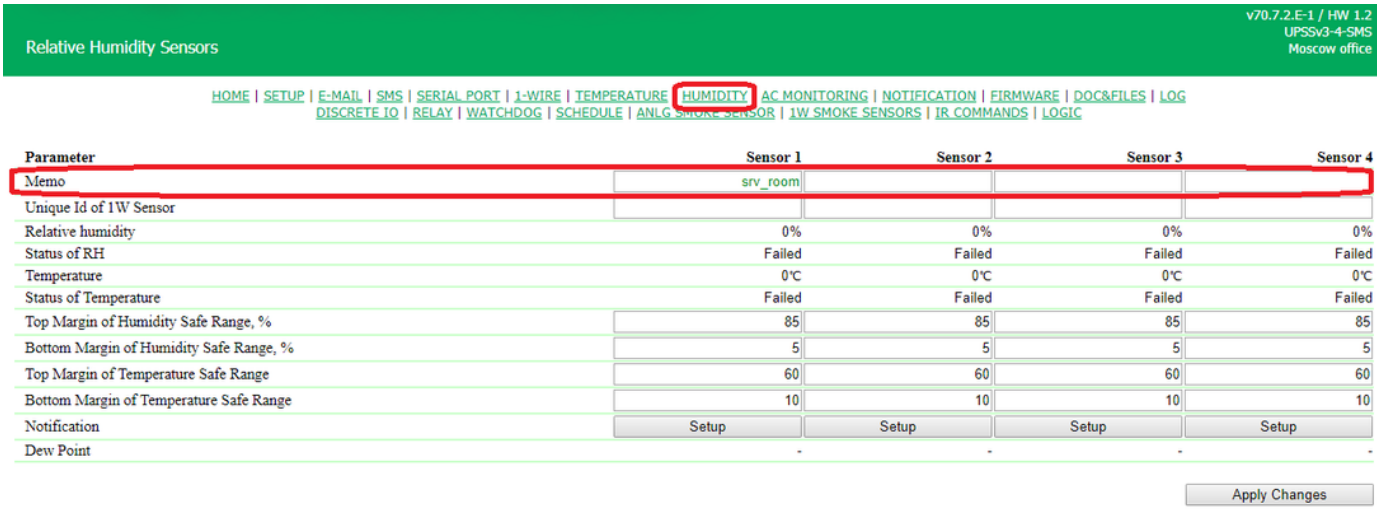
Top Margin of Temperature Safe Range, °C — is a temperature value, when exceeding which, the sensor is switched to the status «above safe range». Hysteresis ± 1 percentage point. On default: 60.

Bottom Margin of Temperature Safe Range, °C — is a temperature value, when falling below which, the sensor is switched to the status «below safe range». Hysteresis ± 1 percentage point. On default: 10.

Dew Point — is a temperature of a dew point, it is calculated using the readings of the relative humidity and temperature, in °C. More details about a dew point — https://en.wikipedia.org/wiki/Dew_point

[ENG] 5.5. [DKSF 70/71.7 IU] Is It Possible to Set Up a Description for Humidity Sensors?

To set up a description for humidity sensors, there is a need to go to the page «HUMIDITY» of a device web interface:



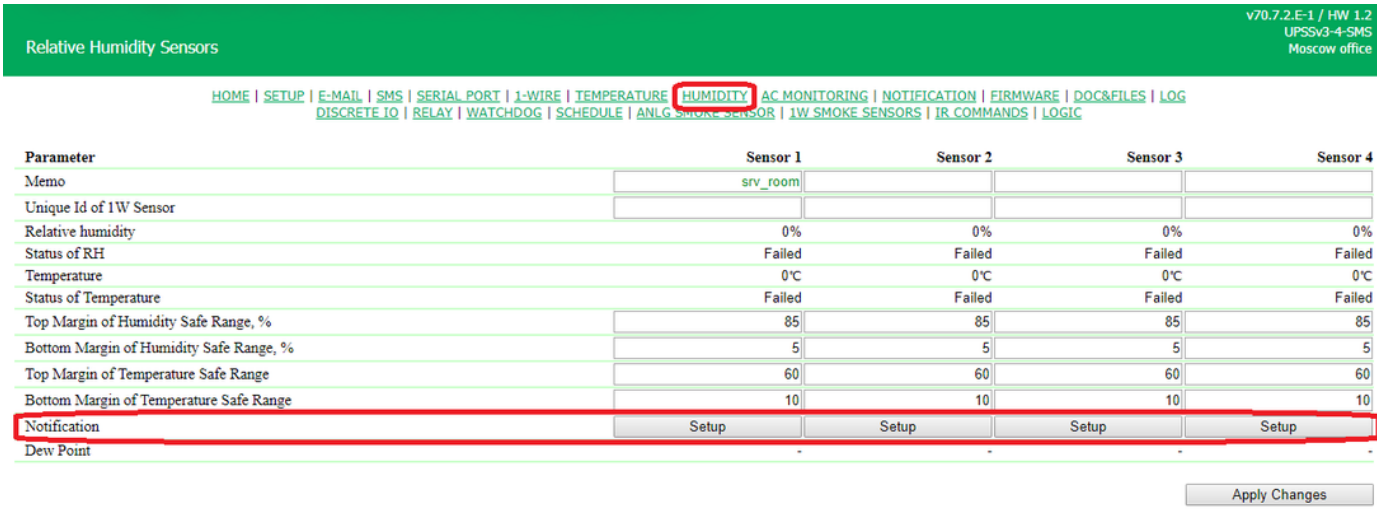
A description of humidity sensors is set in the field «Memo».

Memo — is a field for setting a brief description of a humidity sensor. A memo is used in SYSLOG and log notifications and is included in the SNMP TRAP, and SMS notifications (for a device with a built-in GSM modem), email-notifications, email-reports about the status of sensors. Maximum size is 30 characters. On default: empty line.

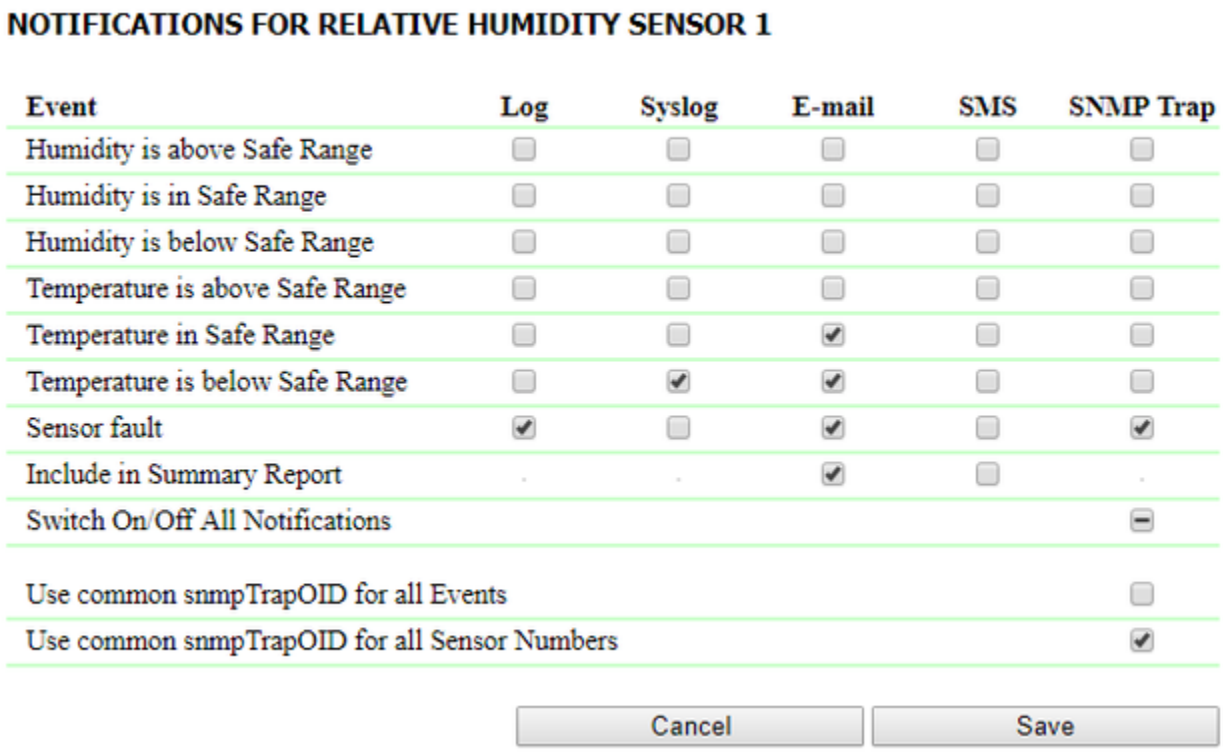
After changing the settings, there is a need to save the parameters by clicking the button «Apply changes».

[ENG] 5.6. [DKSF 70/71.7 IU] I Want to Configure Sending Notifications When a Status of a Humidity Sensor Is Changed. How Can I Do That?

Sending notifications when the status of a humidity sensor is changed, is configured at the page «HUMIDITY» of a device web interface:



When clicking the button «Setup», a menu of settings for sending notifications of the next types appears: Log, Syslog, Email, SMS (in a device, with a built-in GSM modem) and SNMP Trap:



where:

Humidity is above Safe Range — is a checkbox, when checked a device will send notifications if relative humidity exceeds above the top margin of a safe humidity range. On default: checkbox is not checked.

Humidity is in Safe Range — is a checkbox, when checked a device will send notifications if the relative humidity is back to the safe humidity range. On default: checkbox is not checked.

Humidity is below Safe Range — is a checkbox, when checked, a device will send notifications if relative humidity fell below the safe humidity range. On default: checkbox is not checked.

Temperature is above Safe Range — is a checkbox, when checked, a device will send notifications if the temperature exceeds the top margin of the safe temperature range. On default: checkbox is not checked.

Temperature is in Safe Range — is a checkbox, when checked, a device will send notifications, if the temperature is back to the safe temperature range. On default: checkbox is not checked.

Temperature is below Safe Range — is a checkbox when checked, a device will send notifications if the temperature fell below the safe temperature range. On default: checkbox is not checked.

Sensor fault — is a checkbox, when checked, a device will send notifications if a connection with a sensor is lost/restored. On default: checkbox is not checked.

Include in Summary Report — is a checkbox, when checked, reports about a status of a humidity sensor will be emailed and/or sent in SMS (in a device with a built-in GSM-modem). The time for sending reports is configured at the pages «SMS» and «E-MAIL». On default: checkbox is not checked.

Switch On/Off All Notifications — is a checkbox that switches on and off all possible notification types for all events at once. On default: checkbox is not checked.

Checkboxes «Use common snmpTrapOID for All Events» and «Use common snmpTrapOID for all Sensor Numbers» can be used to direct all events from all humidity sensors as one snmpTrapOID notification or divide events and numbers of humidity sensors among different snmpTrapOID notifications, up to sending completely individual ones. This allows receiving individual SNMP Trap-notifications for processing them in monitoring systems, for example, humidity sensor 3 getting damp or a humidity sensor 2 is at the safe range. If a humidity sensor fails, two SNMP Trap notifications are sent: one about humidity, and another one about temperature.

Usually, snmpTrapOID is used that looks like the next .1.3.6.1.4.1.25728.8400.D.127.99 (where D — is an accessory code, 6 — is a humidity Trap, 7 — is a temperature Trap). At the same time, there is a need to analyze variables included in a Trap notification when defining a notification source (a specific sensor) and an event (readings above/below a safe range, sensor failure). If a device or software accepting SNMP Trap, cannot check variables, it is possible to enable event code and/or sensor number right in a snmpTrapOID and thus receive unique SNMP Trap-notifications for all events at all sensors.

It is possible to enable encoding of event types, by unchecking the checkbox «Use common snmpTrapOID for All Events», and in this case, a Trap notification will look like the next:

> .1.3.6.1.4.1.25728.8400.D.S.99, where S — is a status code of a sensors (i.e. events), possible variables are: 100 (failed), 101 (below sage range), 102 (in the safe range), 103 (above the safe range);

It is possible to enable encoding of event types, by unchecking the checkbox «Use common snmpTrapOID for all Sensor Numbers», in this case, a Trap notification will look like the following:

> .1.3.6.1.4.1.25728.8400.D.127.N, where N — is a sensor number, from 1 to 4.

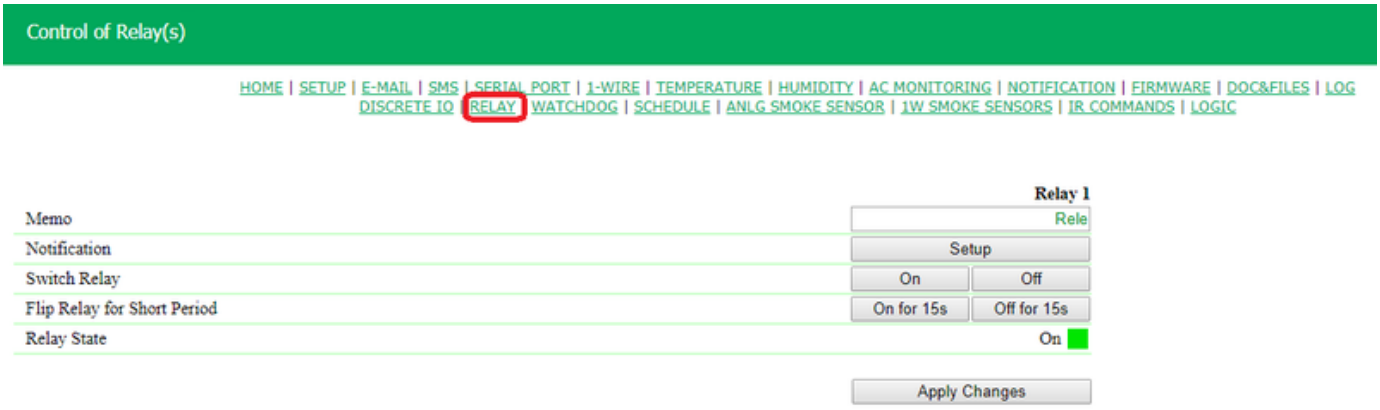
Variables (varbind list) included in Trap, are described in the section 15.4. [DKSF 70/71.7 IU] Support SNMP TRAP

After setting up all necessary parameters, click the button «Apply changes».

[ENG] 6. [DKSF 70/71.7 IU] Working with a Built-In Relay

[ENG] 6.1. [DKSF 70/71.7 IU] Manual Relay Management Using a Web Interface

A built-in relay is manually controlled from the page «RELAY» of a device web interface:



This page allows controlling an outgoing channel of a built-in relay. A channel can be switched on/off for the short term (15s), switched to the mode «Off», «On».

Memo — is a field for viewing or changing a short description of the relay. Memo is used in log and SYSLOG notifications and is duplicated to the page of the «Watchdog» module. It is also included in SMS notifications (for a device with a built-in GSM modem), email notifications and email reports about the status of sensors. Its maximum size is — 30 characters. On default: empty line.

On for 15 sec — clicking the button switches the relay on for 15 seconds.

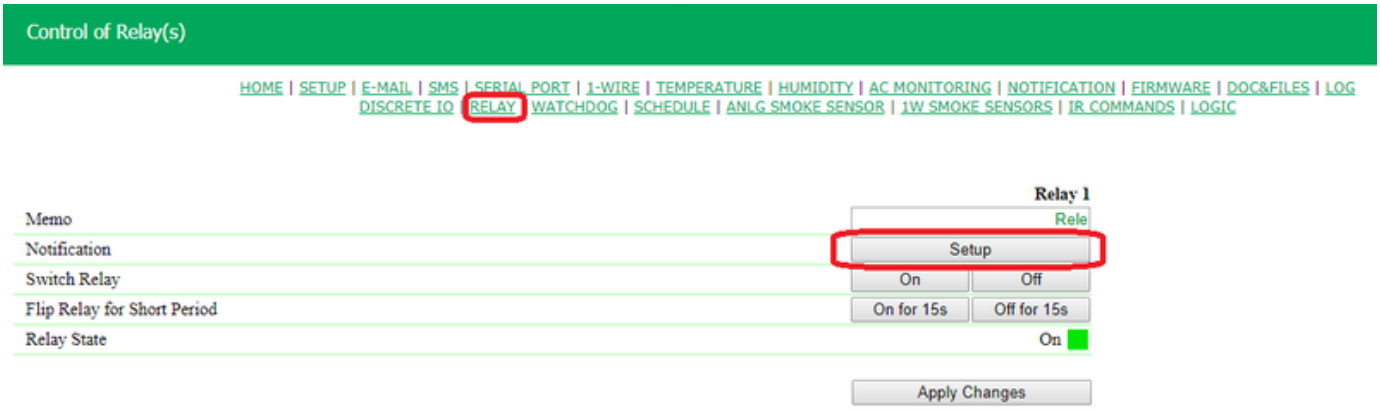
Off for 15 sec — clicking the button switches the relay off for 15 seconds.

Relay State — is the current status of a relay. Possible variants are: «Off», «On». Relay status is automatically updated when the status of a relay is changed with no need to update the entire page.

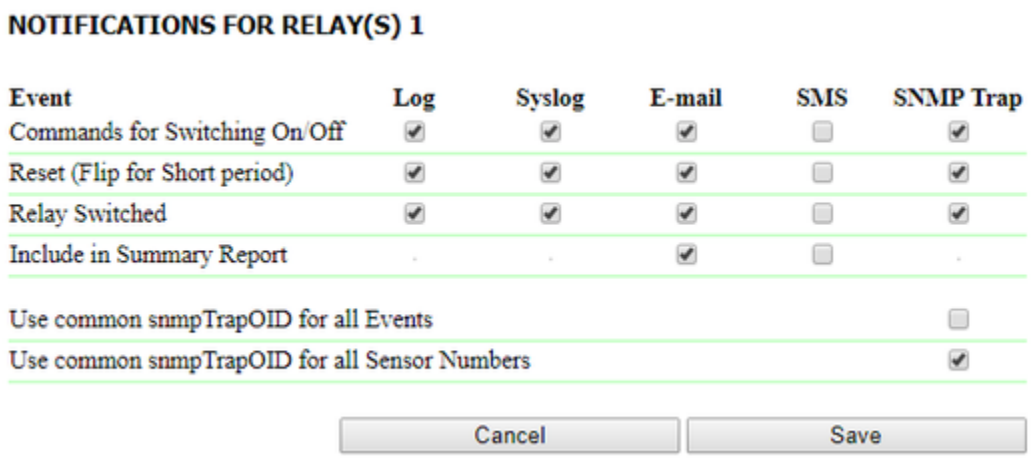
After setting up all necessary parameters, click the button «Apply changes».

[ENG] 6.2. [DKSF 70/71.7 IU] I Want to Configure Sending Notifications about Events when a Relay Is Switched. How Can I Do This?

To configure sending notifications about events when a built-in relay is triggered, there is a need to go to the page «RELAY» of a device web interface:



When clicking the button «Setup», a configuration menu appears for sending notifications of the next types: Log, Syslog, email, SMS (in a device with a built-in GSM modem) and SNMP Trap:



where:

Commands for Switching On/Off — is a checkbox, when checked, notifications will be sent about a device receiving a command about switching a relay on and off.

Reset (Flip for Short Period) — is a checkbox, when checked, notifications will be sent about a short term relay switching.

Relay Switched — is a checkbox, when checked notifications will be sent about switching a relay status.

Include in Summary Report — is a checkbox, when checked, reports about a status of a built in relay will be emailed and/or sent in SMS. The time of sending reports is configured on the pages «SMS» and «E-MAIL».

Checkboxes «Use common snmpTrapOID for all Events» and «Use common snmpTrapOID for all Sensor Numbers» can be used to direct all events from all relays in a single snmpTrapOID-notification or divide the events and relay numbers among different snmpTrapOID-notifications up to completely individual notifications.

Usually, an snmpTrapOID is used that looks like .1.3.6.1.4.1.25728.5500.6.127.99, at the same time, to determine a source of notifications (certain relay) and an event (a command is received, reset is required, a relay is currently switched), there is a need to analyse variables included in a Trap notification. If a device or software that accepts SNMP Trap, cannot test variables, there is a possibility to include an event code and/or a relay number to the snmpTrapOID directly and ths get unique SNMP Trap notifications for every event in every relay.

Encoding a type of events can be enabled by unchecking a checkbox «Use common snmpTrapOID for all Events», in this case a Trap notification will look like as follows:

.1.3.6.1.4.1.25728.5500.6.S.99, where S — is an event code, 100 (a relay is switched off), 101 (a relay is switched on), 102 (a relay received a command on/off), 103 (reset, short term switching of a relay).

> The events 100, 101 are used to confirm that the command has been executed. For example, a command for switching off an already switched relay does not form an event 100 (switched off).

Encoding a number of a channel can be switched on by unchecking a checkbox «Use common snmpTrapOID for all Sensor Numbers».In this case, a Trap notification will look like as follows:

> .1.3.6.1.4.1.25728.5500.6.127.N, where N — is a relay number (always 1).

Variables (varbind list), described in the section [ENG] 15.4. [DKSF 70/71.7 IU] SNMP TRAP Support, are included in a Trap. In addition, there a source of a on/off/switch command in a varbind list .

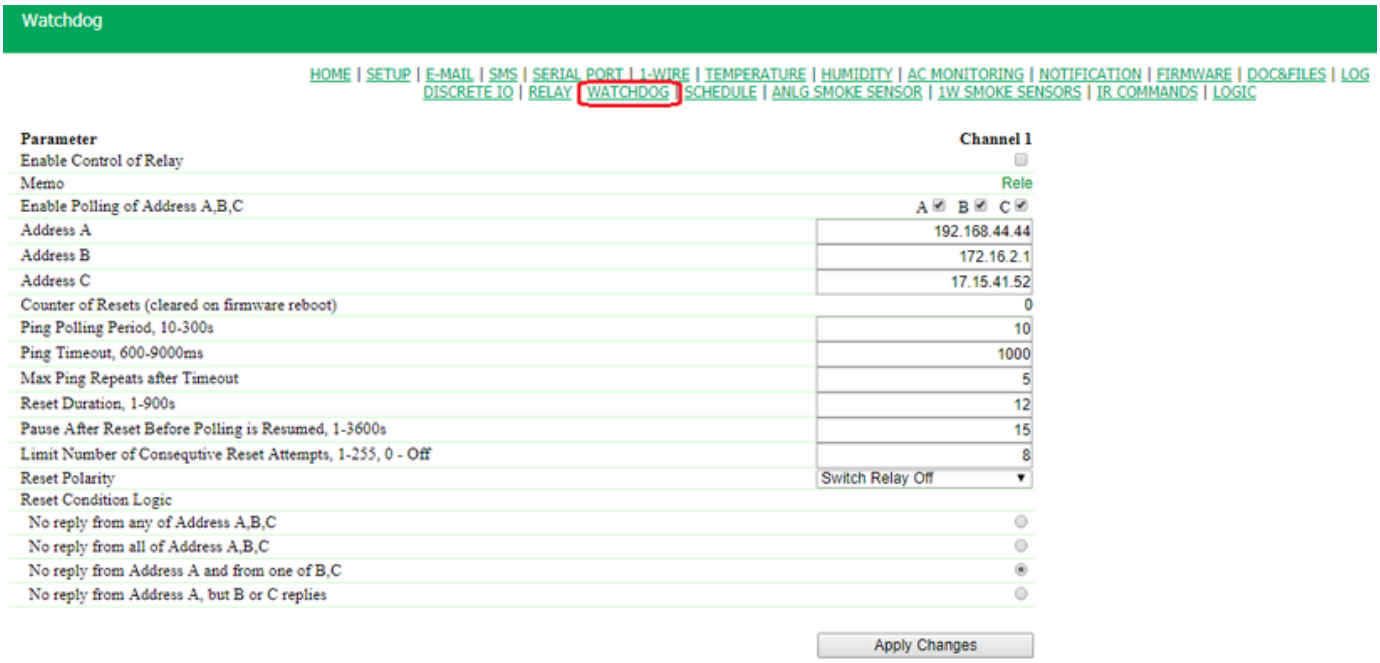
After setting all necessary parameters, click the button «Apply changes».

[ENG] 6.3. [DKSF 70/71.7 IU] What Is «Watchdog» and How Can It Be Configured?

«Watchdog» — is a specific operation mode of a relay channel. In this mode, specified addresses are pinged by ping (ICMP Echo) with a set frequency. If there is no response, the power is switched off for short term thus rebooting a device that is connected to the terminals of the relay.

> If indicated IP addresses are outside the IP subnetwork of a device, there is a need to specify a gateway address at the page «SETUP» of a device web interface to access the external network.

To configure the module «Watchdog», there is a need to go to the page «WATCHDOG» of a device web interface:



where:

Enable Control of Relay — is a checkbox that allows the module «Watchdog» to control a relay, otherwise a relay is not controlled by the watchdog. On default: a checkbox is not checked.

Memo (what's connected) — is a description of a relay that is entered in the field «Memo» at the page «RELAY» of a device web interface.

Enable Polling of Address A, B, C — is a set of checkboxes that allow to specify addresses that are included to polling individually. On default: checkboxes are not checked.

> If no checkboxes are installed or IP-addresses for checked checkboxes are not specified, polling will not be executed and the «Watchdo g» mode will be de-facto disabled.

Address A (B, C) — is a field to view or change polling addresses. It is acceptable to indicate either IP-address or a domain name. It is possible to configure up to three addresses. An empty field disables polling. On default: address is not specified.

Counter of Resets (cleared on firmware reboot) — is an informational field that shows how many times a channel was rebooted as a result of the actions of the module «Watchdog». A counter does not take into account a number the number of reboots in the «manual mode». A counter is cleared when a NetPing device is de-energized.

Ping Polling Period, 10-300s — is a field for setting a time period of how frequently ping is repeated. The period is strict, which means that it is set from the start of the previous poll to the beginning of the next poll, and does not depend on the time of receiving responses. On default: 15 sec.

Ping Timeout, 600-9000ms — is a field for setting a timeout before ping repeats. The value should not exceed the usual time of the response to the ping for the network with some reserve to ensure avoiding false positives of the module «Watchdog». On default: 1000 ms.

Max Ping Repeats after TimeOut — is a field for setting a maximum number of attempts to get a response to «ping». If a number of attempts is over, an IP address is considered «silent». It is desirable that the ping polling period exceeds the ping timeout multiplied by the maximum number of attempts. If this condition is not fulfilled, then a new polling cycle will be postponed until the specified number of attempts is over. On default: 8.

Reset Duration, 1-900s — is a field for setting the time for which a relay changes its status to the opposite one. On default: 12 s.

Pause After Reset Before Polling Is Resumed, 1-3600s — is a field for setting the time for which the polling is stopped after the reset is completed. On default: 15 s.

Limit Number of Consecutive Reset Attempts, 1-255, 0 - Off) — is a field for setting the number of consequent unsuccessful resets, after which functioning of the «load» is not restored and there is still no response to ping. This can happen at the stable failure of the «load» that is impossible to restore by switching the power on and off. When the limit of repeats is reached, resets are stopped, but a periodic ping request continues. Resets are unlocked when there is a response on ping. Resets are stopped and a regular operation order is restored after a response to ping and everything is recorded in the log. Parameter value 0 disables the limit. On default: 0.

Reset Polarity — is a field that allows indicating what action is going to be done to reboot the connected load: «Switch Relay Off» or «Switch Relay On» at outcoming terminals. On default: Switch Relay Off.

Reset Condition Logic — determines a condition at which a device connected to terminals is going to be rebooted.

No Reply from Any of Addresses (A, B, C) — a connected device will be rebooted if at least one of addresses did not respond.

No Reply from All of Addresses (A, B, C) — a connected device will be rebooted only if all requested addresses did not respond.

No Reply from Address A and from one of B or C — a connected device will be rebooted if address A and any of addresses B or C, or both B and C did not respond.

No Reply from Address A, but B or C Replies — a connected device will be rebooted only if address A did not respond but address B and/or address C did respond. That said, if all addresses do not respond, a connected device will not be rebooted.

After setting all necessary parameters, click the button «Apply changes», so that a device executes a command.

If one of the parameters is set incorrectly, it will be highlighted in red:

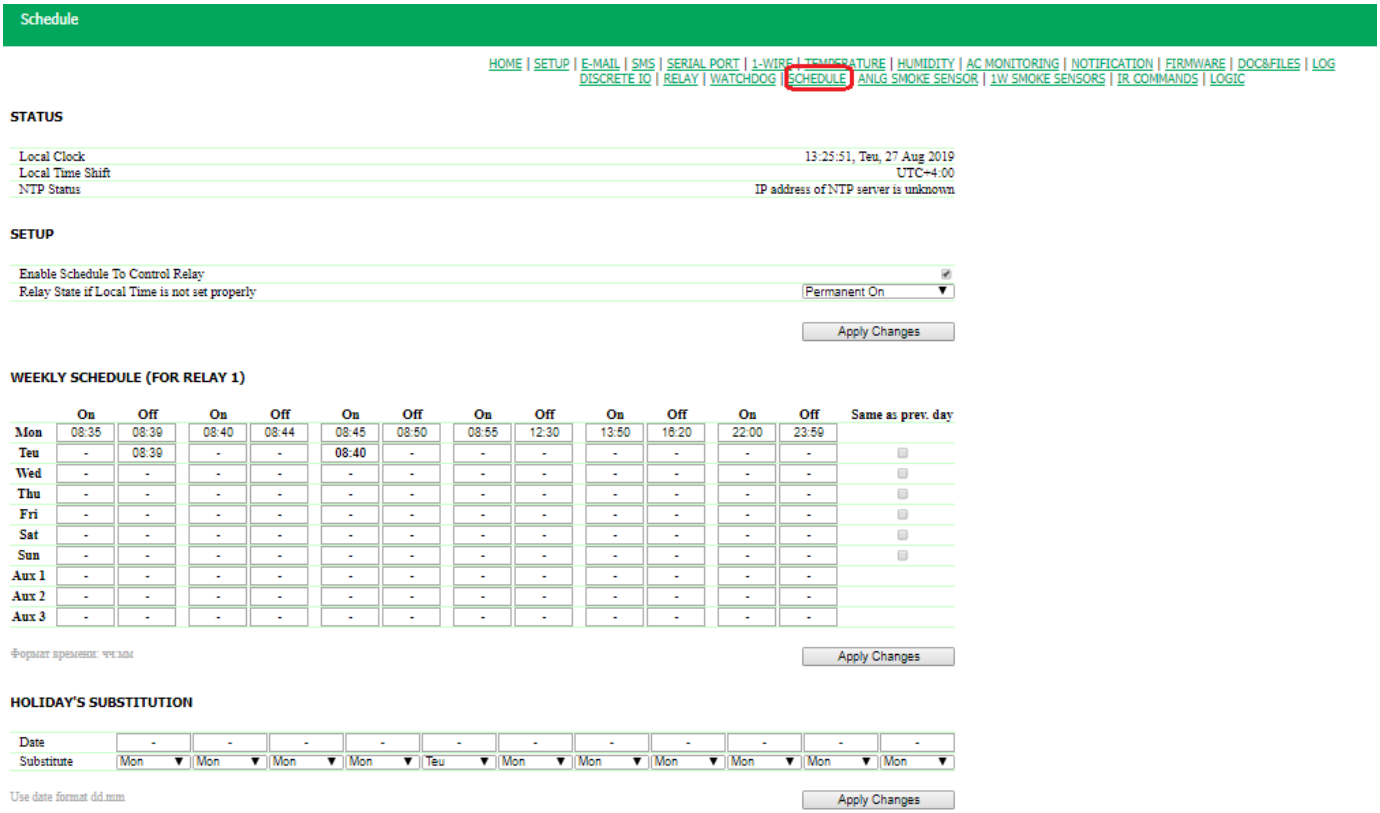
Counter of Resets (cleared on firmware reboot)	0
Ping Polling Period, 10-300s	1
Ping Timeout, 600-9000ms	1000

There is a need to correct a parameter value and click the button «Apply changes» one more time.

To understand the configuration process of the «Watchdog» module better, it is possible to read the article «Automatic Reloading of a Hanging Router that Is Connected to NetPing 2/PWR-220 V3/ETH Power Distribution Unit» in the NetPing company blog.

[ENG] 6.4. [DKSF 70/71.7 IU] What Is a «Schedule» and How to Configure It?

A «Schedule» module allows configuring a schedule according to which a relay is going to switch on and off.



STATUS

Local Clock — shows current time, day of the week and date.

Local Time Shift — time zone. It is configured on the page «SETUP» of a device web interface.

NTP Status — shows a status of time synchronization via an NTP protocol. NTP server addresses are configured on the page «SETUP» of a device web interface.

SETUP

Enable Schedule to Control Relay — is a checkbox that enables the module «Schedule» to control the relay, otherwise the relay is not controlled by the schedule.

Relay State if Local Time is not set properly — the setting defines the reaction of the relay if a lock of the device has been incorrectly set up. The correctness is determined by the date relative to 01.01.2000. If there is no access to NTP, the clock usually shows the date of January 1970. The date after 01.01.2000 is considered correct. The next modes are available: «Permanent On», «Permanent Off», «Ignore Failure».

Permanent On — when the clock is reset, the relay will always be on regardless of the configured schedule.

Permanent Off — when the clock is reset, the relay will always be off regardless of the configured schedule.

Ignore Failure — when the clock is reset, a relay will continue to work on the basis of the time of the system clock regardless of their incorrectness.

After setting all necessary parameters, there is a need to click the button «Apply changes».

WEEKLY SCHEDULE

In the section «Weekly Schedule (For Relay 1)», the schedule is specified to control the relay. For each day of the week, it is possible to set up to 6 switchings on and up to 6 switchings off for the relay in the specified time of the day. They can be filled in anyway, including unpaired and skipped elements. There is a possibility to switch on the relay on Monday and switch it off on Friday, or vice versa, to switch it off for the weekend. There is the only condition: the time of switching on and switching off the relay in the line that corresponds to the days should increase from left to the right.

The column «Same as prev.day» allows changing the schedule of the previous days for the current day, for example, to form the same schedule

for all workdays Monday through Friday.

The time of the last switching on and off is highlighted on the page in bold, which allows to quickly determine which action worked and which action is going to be executed the next.

After setting all necessary parameters, there is a need to click the button «Apply changes».

HOLIDAY'S SUBSTITUTION

The lines «Aux 1», «Aux 2», «Aux 3» allow setting specific schedules for holidays.

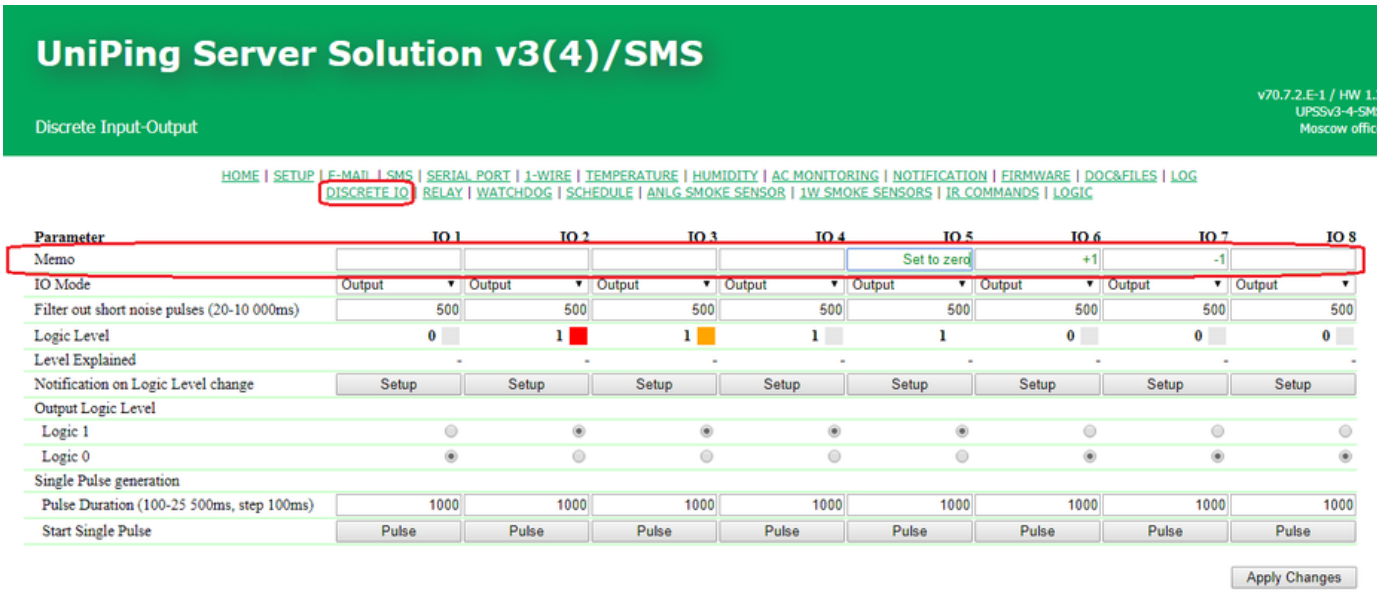
In the section «Holiday's Substitution» up to 11 substitutions are available.
In the field «Date», a date of a holiday is specified in the format «dd.mm».
A drop-down menu «Substitute» is used to choose a random schedule that is going to be applied for that day, with no link to the actual day of the week for that holiday.

After setting all necessary parameters, there is a need to click the button «Apply changes».

[ENG] 7. [DKSF 70/71.7 IU] Working with the Channels of the Discrete Input-Output

[ENG] 7.1. [DKSF 70/71.7 IU] How to Avoid the Necessity to Remember Numbers of Input-Output Lines in Notifications?

To set a description for the input-output line, there is a need to go to the page «INPUT-OUTPUT» of a device web interface:

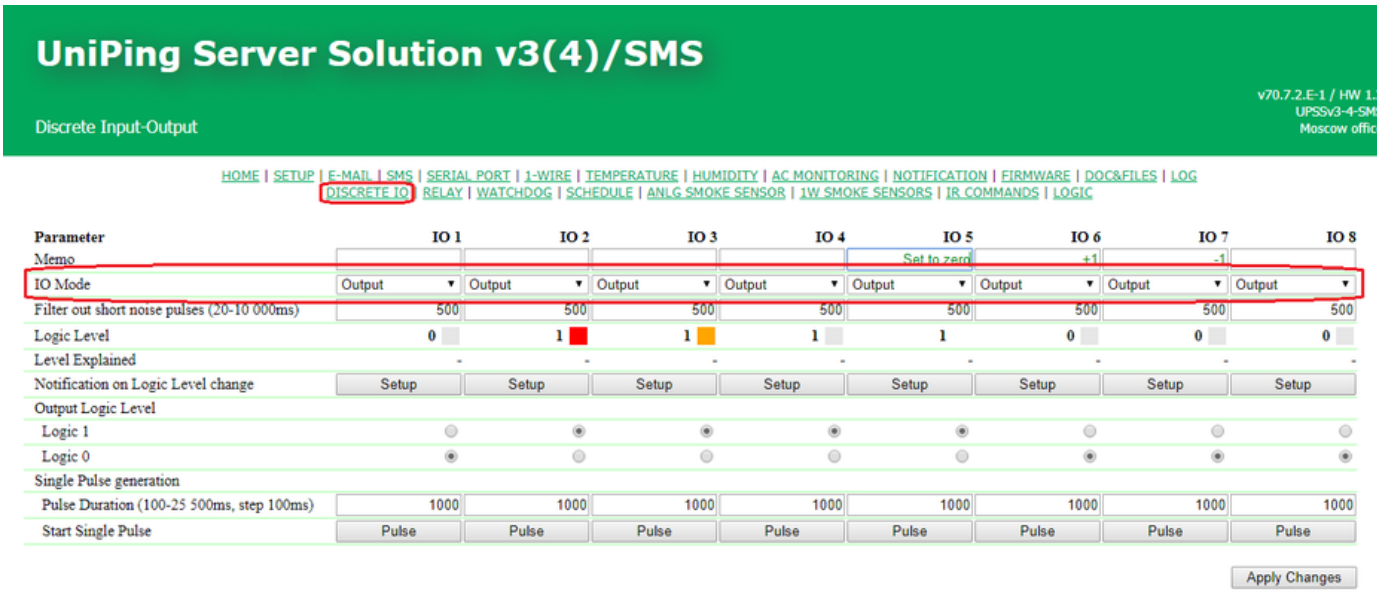


Memo — is a field for setting a brief description of an IO line. A memo is used in the notifications of the SYSLOG and log notifications and is included into SNMP TRAP, SMS-notifications (for a device with a built-in GSM-модемом), email-notifications, email-reports about the status of sensors. The maximum size is — 30 characters. On default: an empty line.

In addition, notifications include a text description of a logic level of the line. The detailed information on how to configure encoding is given in «[ENG] 7.5. [DKSF 70/71.7 IU] I Want to Configure Sending Notifications when a Logic Level of an IO Line Is Changed. How to Do This?

[ENG] 7.2. [DKSF 70/71.7 IU] Configuring an Operation Mode for an Input-Output Line

To configure an operation mode of an IO-line, there is a need to go to the page «Discrete Input-Output» of a device web interface:



where:

IO Mode — allows setting an IO line in the modes «input», «output». On default: input.

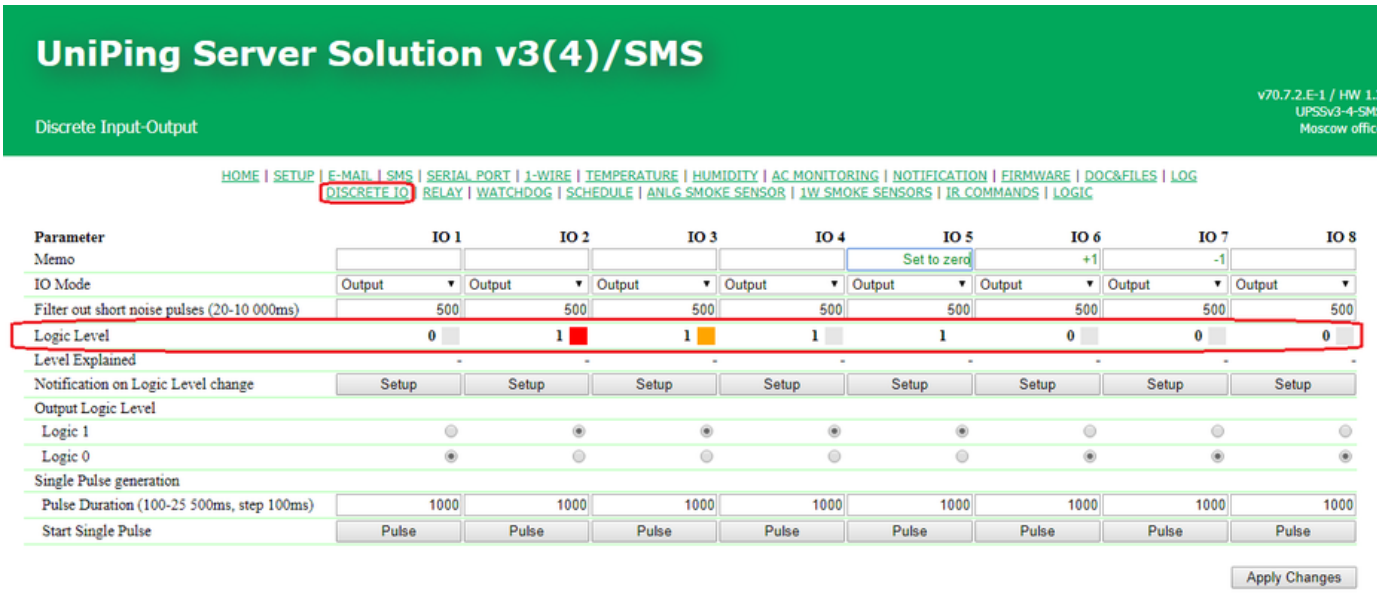
The operation mode of an IO line «input» is used to connect "dry contact" sensors to an IO line, for example, a door sensor.

The operation mode «output» of an IO line is used to control external devices for example NetPing AC/DIN socket.

At the page «DISCRETE IO», current settings of the discrete input-output channels are displayed. In the «input» and «output» modes, it is possible to configure automatic sending of SNMP TRAP, SYSLOG, email, SMS notifications (in devices with a built-in GSM modem), notifications in a log and sending a periodic report about a status. In the «output» mode, it is possible to set a logic level on a line through the web, SNMP, and HTTP API interfaces.

[ENG] 7.3. [DKSF 70/71.7 IU] How to Determine a Current Logic Level of an Input-Output Line?

To determine a current logic level of an IO line, there is a need to go to the page «DISCRETE IO» of a device web interface:



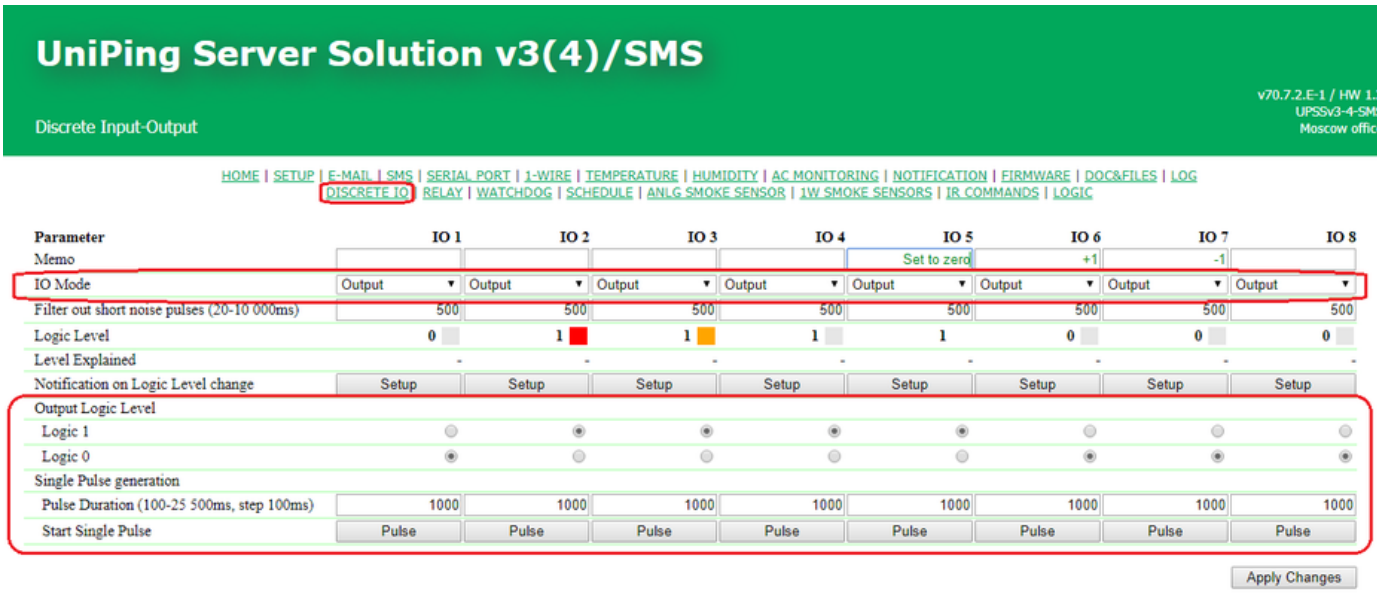
where:

Logic Level — is a field that represents a current logic level of an IO line. It is updated automatically when a logic line is changed with no need to update the entire page.

> Status of an IO-line is updated in a real-time mode, right after the actual change of the level of the line, using a mechanism HTML5 Server Sent Events, not through periodic updating of the page every few seconds.
>
> This mechanism often fails if several pages of a web interface of the same device are opened in different tabs, in different browsers or at different computers. NetPing devices have the same SSE-channel.
>
> A real-time status update does not work in IE and Edge browsers because they do not support SSE. For these browsers, there is a need to manually update the page to retrieve the actual information.

[ENG] 7.4. [DKSF 70/71.7 IU] How to Control an Input-Output Line in an «Output» Mode?

To control an IO-line, there is a need to go to the page «DISCRETE IO» of a device web interface:



1. Set the operation of an IO-line to the «output» mode;
2. Check the checkbox «Output Logic Level» to «Logic 0» or «Logic 1»;
3. Save the parameters by clicking the button «Apply changes».

IO Mode — is a field that represents a current logic level at the IO-line. It is updated automatically when a logic level of a line is changed with no need to update the entire page.

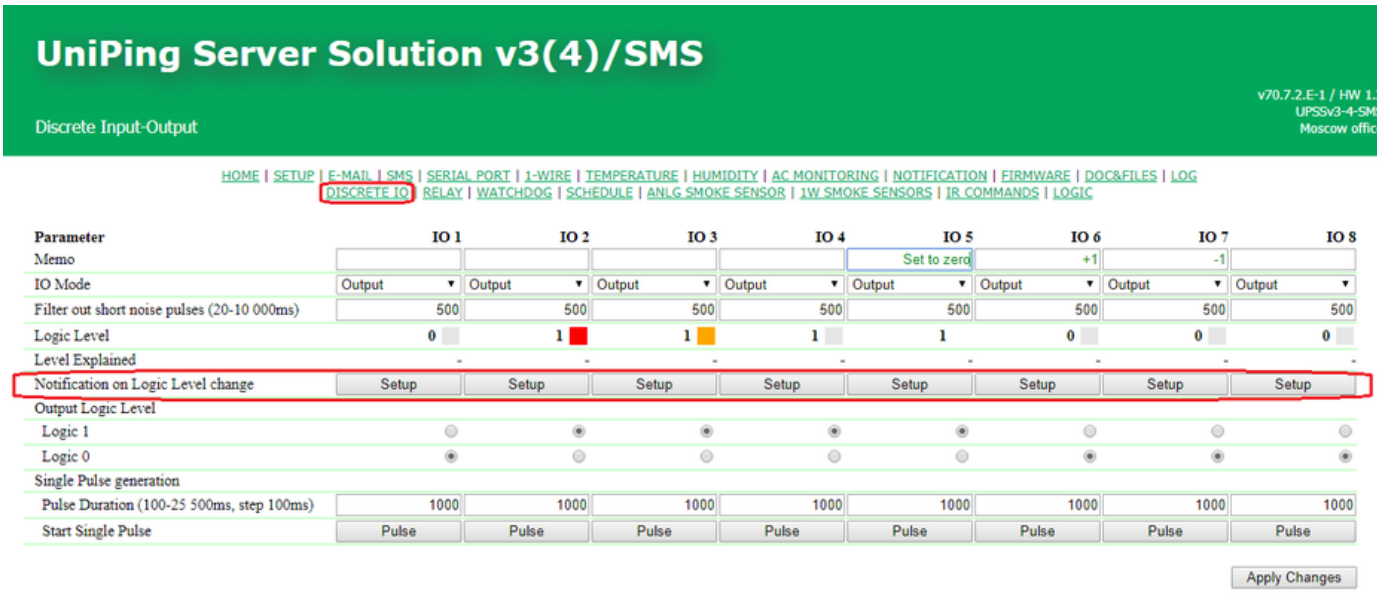
Output Logic Level — is a parameter of a logic level on the line that operates as «output». A logic «1» means having voltage at the input line (open collector circuit). A status of a logic «0» means having no voltage at the output line. On default: logic «0».

Single Pulse Generation — when clicking the button «Pulse», an IO-line that works as an «output», will be inverted for a specified period of time. Pulse duration is set in the field «Pulse Duration (100-25500ms, step 100ms)». If a line is configured as «input», a button for issuing a pulse is inactive.

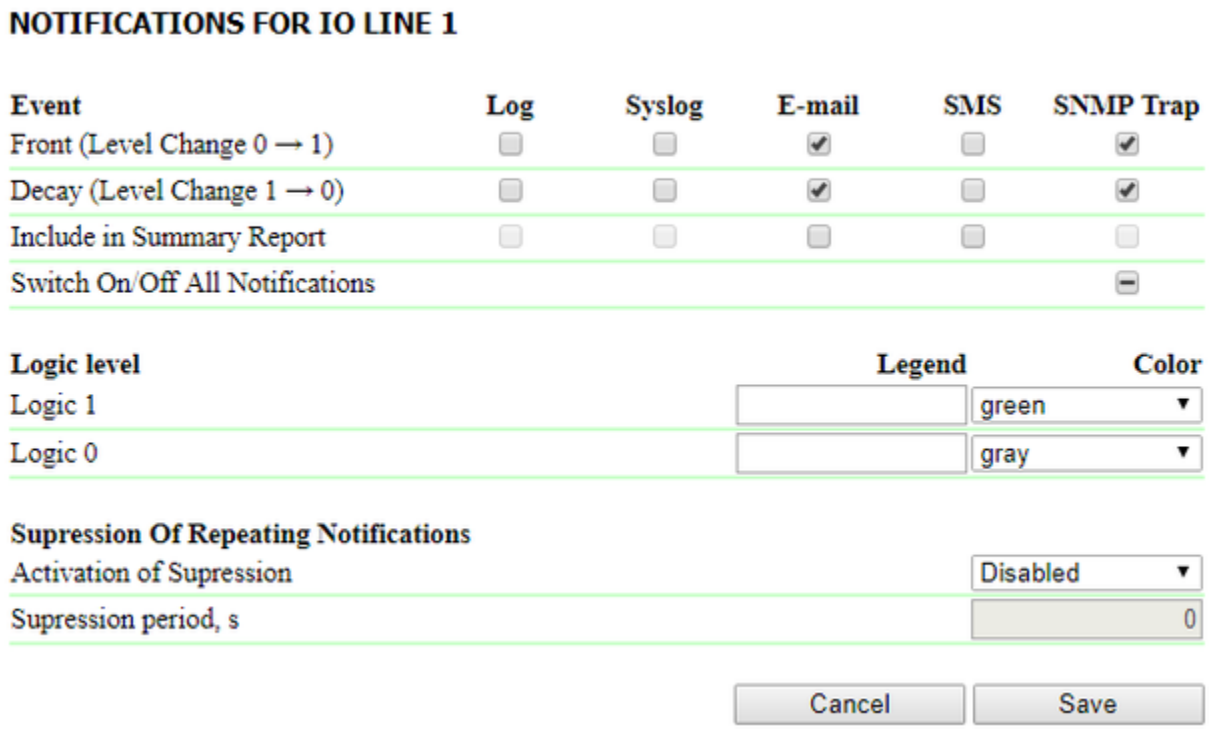
> In addition, an IO-line can be managed using SMS-commands (in devices with a built-in GSM-modem), HTTP API commands, SNMP protocol or a built-in logic of a device.

[ENG] 7.5. [DKSF 70/71.7 IU] I Want to Configure Sending Notifications when a Logic Level of an IO Line Is Changed. How to Do This?

Notifications when logic of an IO line is hanged are configured at the page «DISCRETE INPUT-OUTPUT» of a device web interface:



When clicking the button «Configure», there appears a menu of settings for configuring notifications of the next types: Log, Syslog, Email, SMS (in devices with a built-in GSM-modem), SNMP Trap. At the same menu, it is possible to indicate the description of digital values of the current level of an IO-line, color indication, and other settings:



where:

Front (Level Change 0->1) — enabling sending notifications when the status of an IO-line is changed from «0» to «1». On default: checkbox is not checked.

Decay (Level Change 1->0) — enabling sending notifications when the status of an IO-line is changed from «1» to «0». On default: checkbox is not checked.

Include in Summary Report — enabling sending daily periodic reports about a status of an IO-line via email and/or SMS. Time for sending reports is configured on the pages «SMS», «EMAIL». In default: the check box is not set.

Switch On/Off All Notifications —switching on and off all possible notification methods for all events at once.In default: the check box is not set.

Logic Level 1/0 — textual decoding of the logical level of the IO line. It will be displayed in the field «Level explained» on the page «DISCRETE IO », as well as be present in SYSLOG and log messages, in SNMP TRAP, SMS and email notifications.

Colour — the selection of colour of the virtual logical level indicator that is displayed on the page«DISCRETE IO» (the color of the physical LEDs on the front panel cannot be adjusted), the possible options are “white”, “gray”, “orange”, “red”, “green”. In Default: for “Log. 1 "- green, for" Log. 0 ”is gray.

Supression Of Repeated Notifications — a function that can be useful to save from spam when changing the log level on the line very often.

This option allows you to suppress repeated uninformative notifications, considering the specifics of the connected sensor. For example, a motion sensor, if there is a working person in its coverage area, gives out a spontaneous series of alarms. This option eliminates the need for multiple repeated notifications of virtually one presence detection event.

Activation of Supression - sets the transition, which starts the period of suppression of repeated notifications. It is set to the value corresponding to the alarm (for example, about the loss of voltage). Asymmetric activation is necessary so that the output from the alarm state does not trigger spam suppression. Until the suppression period ends, all notifications for any state transitions are discarded. The possible values are “Disabled”, (0 → 1), (1 → 0) and “Any change” (0 → 1 & 1 → 0).

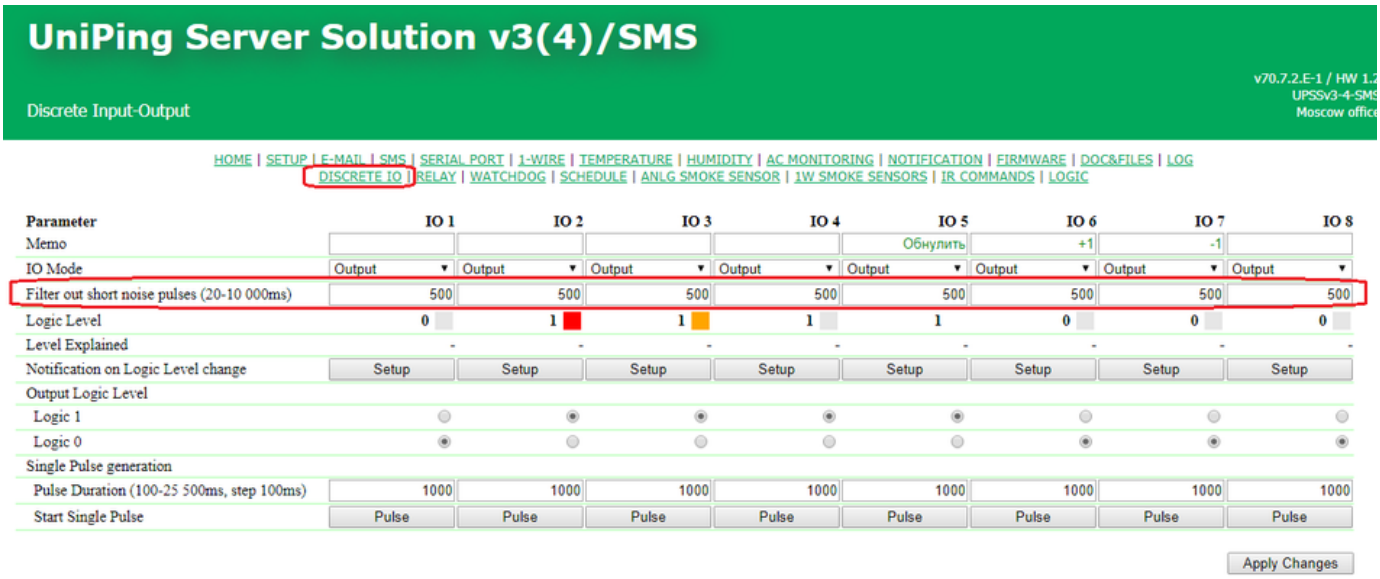
Supression Period — the time needed for the supression of repeated notifications. Possible values are 0–65,500 seconds.

After setting all necessary parameters press the "Apply Changes" button.

[ENG] 7.6. [DKSF 70/71.7 IU] What do I need a Filter out short noise pulses in DISCRETE IO Line Settings for?

A Filter out short noise pulses is a field for setting the time during which the IO line configured as an “input” must remain in a stable condition for its registration. Through this process, this parameter allows you to filter out short interference signals or bounce of mechanical contacts. In default: 500 m/s.

The Filter out short noise pulses is configured on the “DISCRETE IO” page of the device web interface:



[ENG] 8. [DKSF 70/71.7 IU] Work with an analog smoke sensor (current sensor)

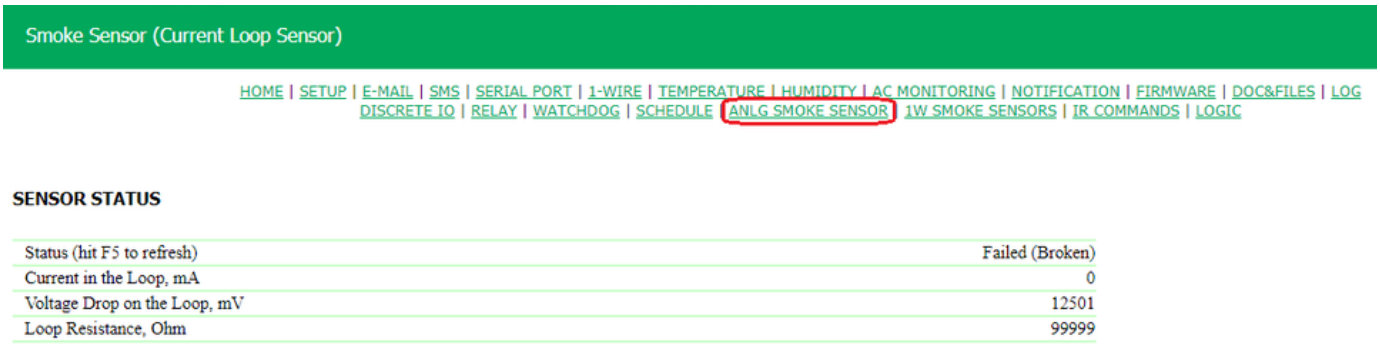
[ENG] 8.1. [DKSF 70/71.7 IU] The View of a Sensor Status

The Page "ANLG SMOKE SENSOR" of the device's web interface shows the status and allows you to configure parameters of smoke detector (current loop). Smoke sensors and other sensors can be connected to the input of the current sensor. These sensors should have a standard interface in the form of a 5-20 mA current loop. The current loop is powered from the device side with a voltage of 12 V, and the sensor gives a signal by changing its resistance, which causes a change in the current in the loop.

The device has one interface for connecting sensors. Several sensors can be connected sequentially or parallel to each other.

The triggered sensor can be detected by means of current, voltage or resistance, their values will create SNMP TRAP-messages about the alarm.

To view the current status of smoke sensor you should go open the page "ANLG SMOKE SENSOR" of the device`s web interface.



In the section "SENSOR STATUS" you can see:

Status (hit F5 to refresh) -a condition of a current sensor at the moment of time. In order to view the immediate status it is necessary to update the page by pressing the button F5.

Possible sensor conditions:

- Cut off current (deenergized);
- Disconnection (break-off);
- Short circuit (Loop short);
- Normal;
- Alarm.

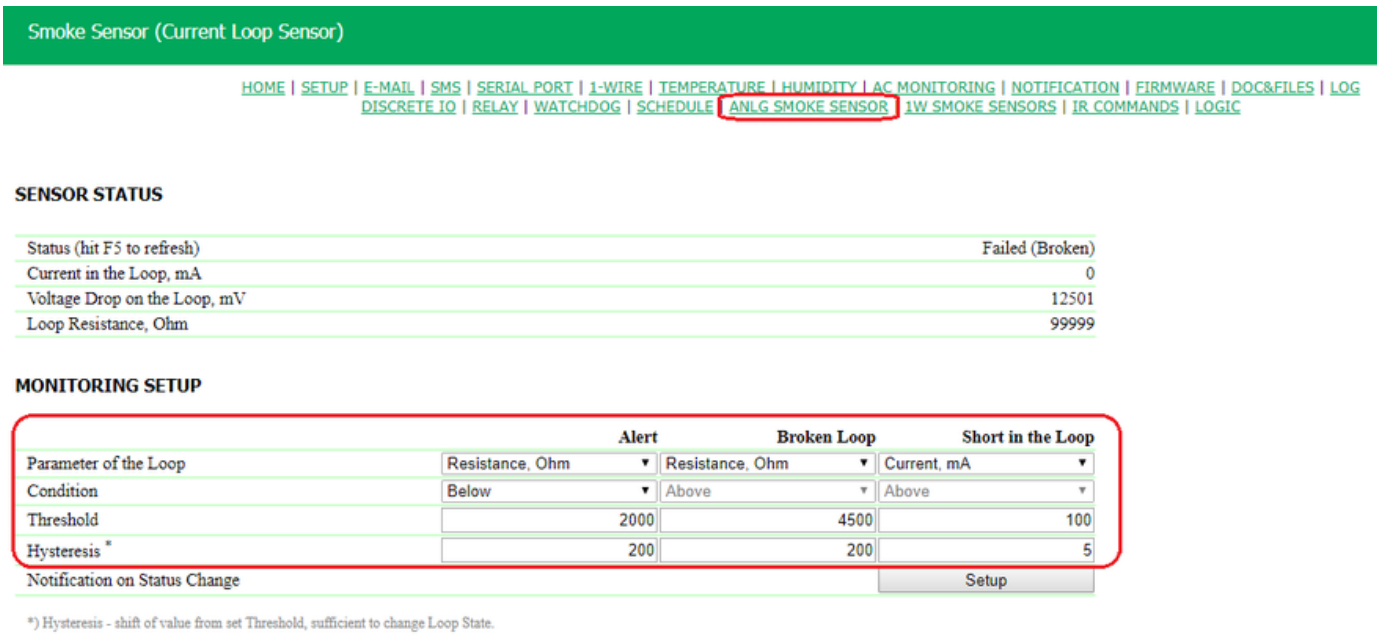
Current in the Loop — a current value of loop current, mA.

Voltage Droop on the Loop — a current value of voltage droop on the loop, mV.

Loop Resistance — a current calue of loop resistance, Ohm.

[ENG] 8.2. [DKSF 70/71.7 IU] MONITORING SETUP: Alert, Broken Loop, Short in the Loop

In order to set the threshold of such events as alert, lbroken loop, short in the loop of smoke sensor it is necessary to go to the page "ANLG SMOKE SENSOR" of device`s web interface.



In the section "MONITORING SETUP" it is possible to set up parameters which will determine the status of current sensor.

The current sensor can take three types of status apart from normal and off-the-line:

- Alert;
- Broken Loop;
- Short in the Loop.

You can set an edge condition for every status, and the sensor will get the appropriate status according to the conditions.

Parameter of the Loop - sets up a parameter with the value which determines the decisions taking to change the sensor status. Some possible parameters: "Resistance, Ohm", "Current, mA", "Voltage, mV". In Default: Resistance.

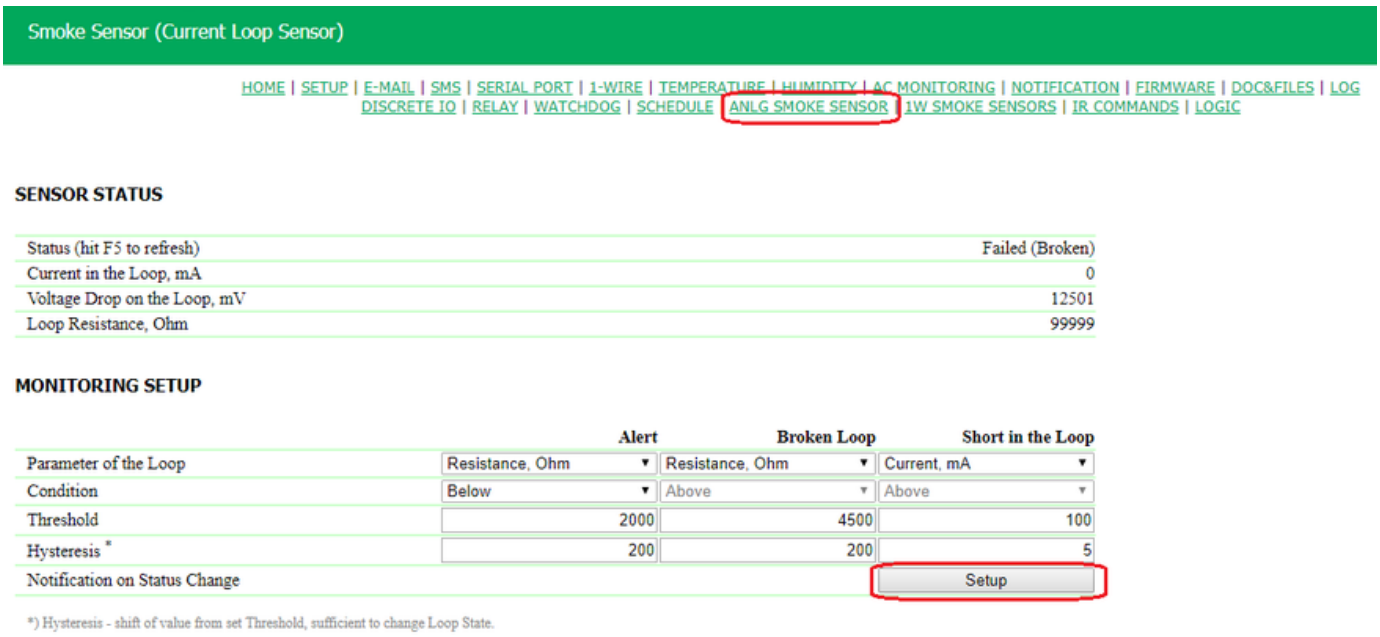
Condition - a sensor condition change will be fulfilled is a current Parameter in the Loop gets more/less than a Threshold value. In Default: depen ding on the condition

Threshold - a Threshold value upon transition through which a Status Change will be fulfilled. In Default: depending on the condition

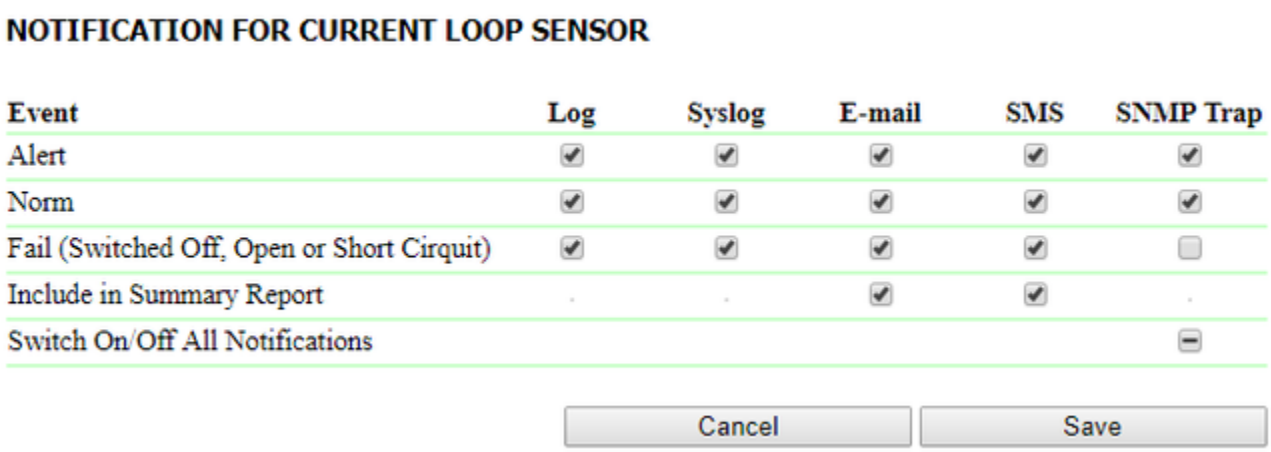
Hysteresis - a "deadspace" of a parameter close by the Threshold. It is necessary for eliminating the condition switching from small random fluctuations of a measured Parameter of the Loop close by the preset thresholds as a result of electric interference, measurement errors and so on. In Default: 200 (Alert), 200 (Broken Loop), 50 (Short in the Loop).

[ENG] 8.3. [DKSF 70/71.7 IU] I want to configure Notification on Status Change for the Smoke Sensor. How can I do it?

The configuring of Notifications on Status Change when Smoke Sensor (Current Loop Sensor) status changes in carried out on the page "ANLG SMOKE SENSOR" of device`s web interface:



Whe you press the button "Setup" you can see the menu of NOTIFICATION FOR CURRENT LOOP SENSOR for these notification: Log, Syslog, SMS (in devices with the built-in GSM-modem) and SNMP TRAP:



where:

Alert - is sending notifications when there is a transitions to the status "Alert". In Default: check-box is not set up.

Norm — is sending notifications when there is a transition to the status "Norm". In Default: check-box is not set up.

Fail (Switched Off, Open or Short Circuit) - is sending notifications when there is a transition to the status "Switched Off", "Broken Loop" or "Short Circuit on the Loop". In Default: check-box is not set up.

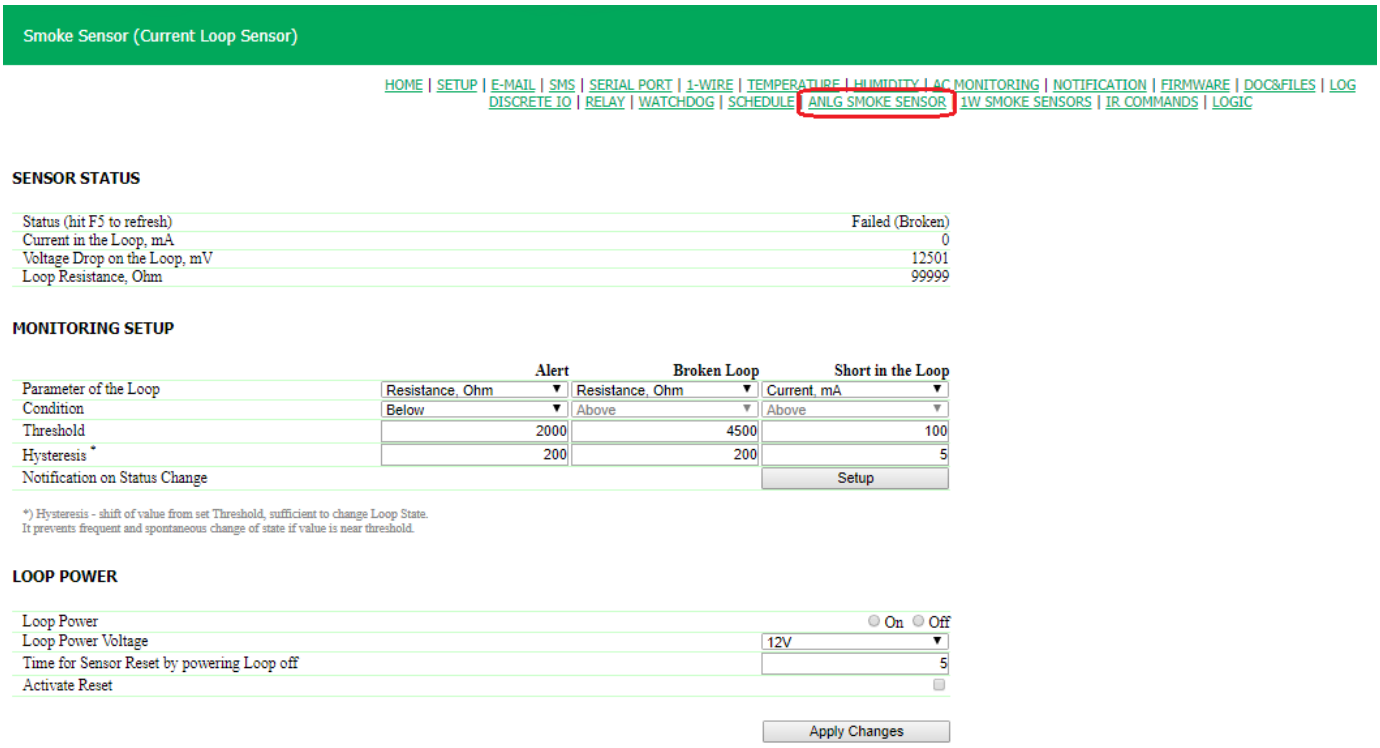
Include in Summary Report - is sendind Summary Reports about Sensor Status via email and/or SMS. The time for sending Summary Reports is indicated on the pages "SMS" and "EMAIL".

Switch On/Off All Notifications - is switch on or off all possible ways of evens notifications immediately. In Default: check-box is not set up.

After configuring all necessary adjustments press the button "Save".

[ENG] 8.4. [DKSF 70/71.7 IU] The Configuration of Loop Power

The configuration of Loop Power is carried out on the page "ANLG SMOKE SENSOR" of device`s web interface.



where:

LOOP POWER - switching on/off sensor Power Voltage. In Default:

Loop Power Voltage - a choice of sensor power voltage, available only 12 B. In Default: 12V.

> Warning
> Attention! You need to choose the Loops Power Voltafe very precisely and carefully in order not to damage tha sensor. The majority of sensors work from 12 V, and overvoltage can damage them.

Time for Sensor Reset by powering Loop off, sec - the time during which the Loop Power will be removed in order to reset it. In Default: 5

Activate Reset - the check-box, after the setting up ot it the Activate Reset of circuit sensor will be carried out by switching off power on an indicated period of time. To compete Activate Reset press the button"Apply Change". In Default: check box is not set up.

After setting up all necessary configurations press the "Apply Changes".

[ENG] 9. [DKSF 70/71.7 IU] Work with 1-Wire Smore Sensors

[ENG] 10. [DKSF 70/71.7 IU] Work with the NetPing Power Quality Monitoring Sensor 1-Wire

[ENG] 11. [DKSF 70/71.7 IU] Work With SMS-Messages and Built-In GSM-Modem

[ENG] 11.1. [DKSF 70/71.7 IU] How to Find Out a USSD Balance on a SIM-Card?

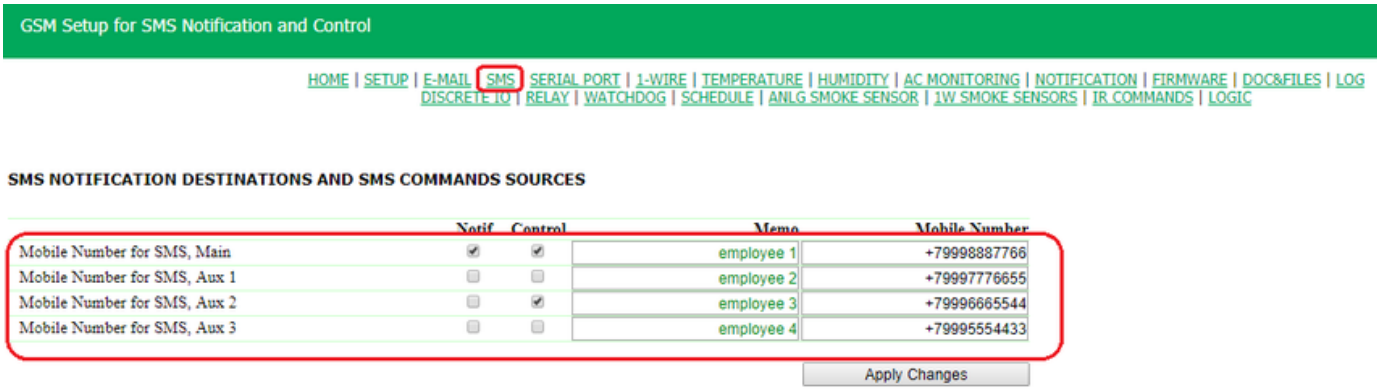
> The information is related to the devices UniPing server solution v4/SMS with the built-in modem.

In order to find out the Account Status on your SIM-card inserted in a slot of a built-in GSM-modem of the device, you need to open the page "SMS" of the device`s web interface.

[ENG] 11.2. [DKSF 70/71.7 IU] I Need to Configure the Numbers to Send SMS-Notifications. How Can I do This?

> The information in this section is applicable to the devices UniPing server solution v4/SMS a built-in GSM-modem.

In order to set one or several phone numbers to sent SMS Notifications, you need to open the page "SMS" of the device`s web interface:



In the section "SMS NOTIFICATION DESTINATIONS AND SMS COMMANDS SOURCES" you need to indicate the Main and Aux (Auxiliary) phone numbers to send SMS Notifications.

Memo - is a convenient indications of a phone number in letters for simple identification of its owner.

MobileNumber is indicated in the format of CountrycodeOperatorcodeCustomernumber, for example, +79127894561, where +7 is a country

code, 912 - is an operator code, 7894561 is a customer number.

Moreover, in this section you can switch on Notifications for every mobile number and give permission to control the device with the help of SMS-commands, the check-boxes "Notif" and "Control" are responsible for these functions.

"Notif" - check-boxes allow to send Notification to the indicated mobile number. In order to receive SMS Notifications you need to permit their sending to at least one mobile number.

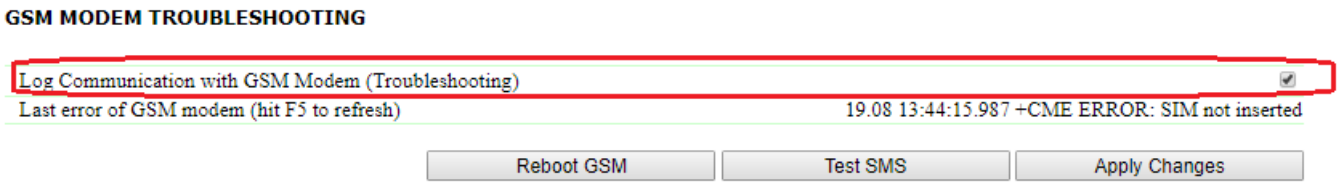
"Control" - check boxes allow to receive relay control commands, IO and etc, from the indicated mobile number. If no one check-box "Control" is marked, SMS commands are receved from any mobile number without restrictions.

To save the mobile numbers press the button "Apply Changes"

[ENG] 11.3. [DKSF 70/71.7 IU] How Can I Enable an Extended Log for a GSM-Modem?

> The information in this section is applicable to the devices UniPing server solution v4/SMS with a built-in GSM-modem.

An extended log for GSM-moded is enabled on the page "SMS" of the device`s web interface



In the section "GSM MODEM TROUBLESHOOTING" you have to set up a check-box "Log Communication with GSM Modem (Troubleshooting)"

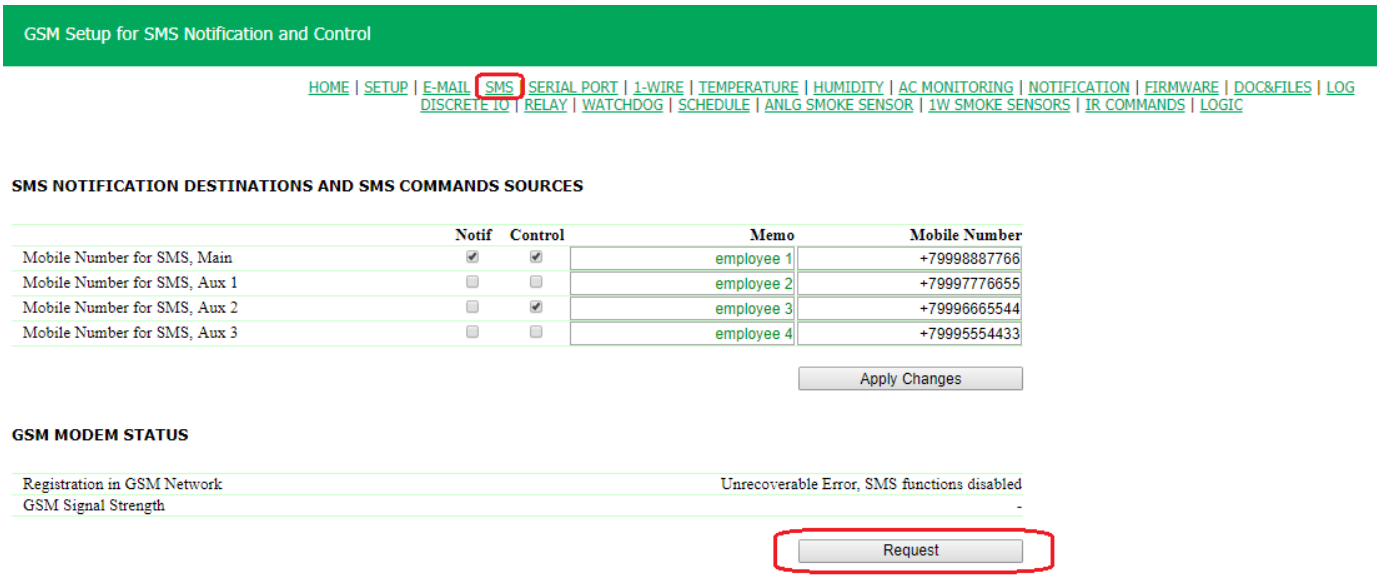
Log Communication with GSM Modem (Troubleshooting) - is a function with the enabling of which you can see the information about all AT-commands on the page "LOG", which CPU swaps with a GSM-modem.

To save the configuration press the button "Apply Changes"

[ENG] 11.4. [DKSF 70/71.7 IU] The GSM-Signal Strength Checking

> The information in this section is applicable to the devices UniPing server solution v4/SMS with a built-in GSM-modem

In order to check the registration and the GSM-signal strength in a SIM card, inserted in the device, you need to open the page "SMS" of the device`sweb interface:



In the section "GSM MODEM STATUS" you have to press the button "Request". In several second in the section "Registration in GSM Network" you can see the information about the type of a mobile network your SIM-card has been registered. In the section "GSM Signal Strength" you can observe the information and the condition of a signal in percents.

[ENG] 11.5. [DKSF 70/71.7 IU] The Receiving of SMS-Notifications by Watchdog Events

> The information in this section is applicable to the devices UniPing server solution v4/SMS with a built-in GSM-modem.

For the configuration of SMS NOTIFICATIONS by watchdog events you need to open the page "SMS" of the device`s web interface:

In the section "SMS NOTIFICATIONS" it is possible to configure:

Ethernet link status change - when the status of the relay changes, if the relay is controlled by the "Watchdog" module, so the sending of the SMS Notifications to the mobile numbers, which were written in the section"SMS NOTIFICATION DESTINATIONS" will be implemented.

Pinger status change (Loss/reactivation of connection with the specified IP (pinger)) - while detecting the loss and reactivation of connection of the checked network node there will be the sending of SMS Notifications to the mobile numbers specified in the section "SMS NOTIFICATION DESTINATIONS" in the page "SMS" of the device`s web interface. In the section "PINGER" in the page "SMS" you can configure the address for checking network node availability by IP address or DNS-name in the entry field "Address to poll the ping" and the period for checking in the entry field "Period, s (30-9999)".

The operating parameters of the "Pinger" module on the page "SMS":

1. The poll of the configured IP address or DNS name starts once in a specified period (the parameter "Period, s (30-9999)";
2. The wait period for the responce from an IP address or DNS-name is 2 seconds;
3. The number of retries of checking the IP address or DNS-name is 8
4. If there is no response from the checked network node for 8 repetitions, “Pinger” reports that there is no connection with the specified IP address or DNS-name;
5. If there is a responce from the checked network node at the next polling period, "Pinger" reports that there is a connection with the specified IP address or DNS-name.

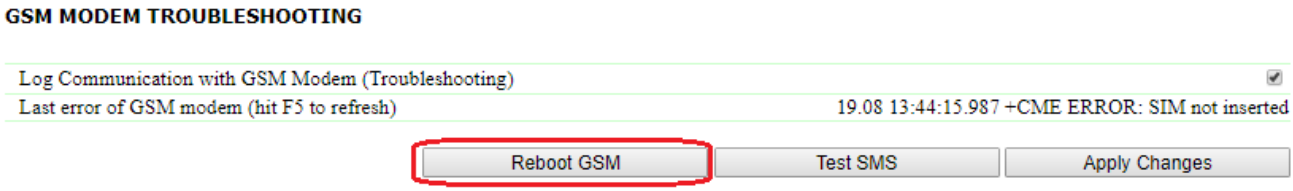
In order to find out how to register phone numbers for sending SMS notifications you can study the section "[ENG] 11.2. [DKSF 70/71.7 IU] I Need to Configure the Numbers to Send SMS-Notifications. How Can I do This?"

After configuration all the necessary parameters press the button "Apply Changes"

[ENG] 11.6. [DKSF 70/71.7 IU] GSM Modem Troubleshooting

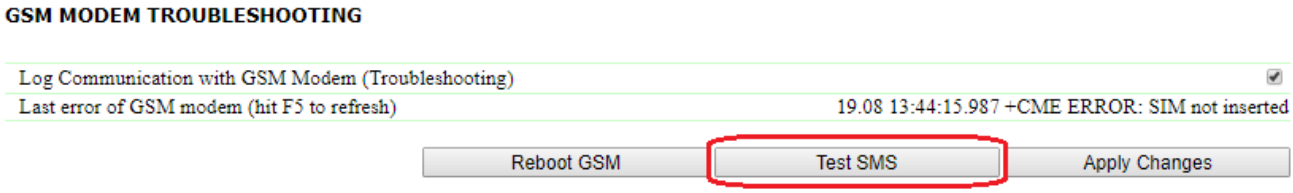
> The information in the section is applicable to the devices UniPing server solution v4/SMS with a built-in GSM modem.

If SMS notifications are not sent for any resons and the device is not controlled by SMS commands, you can restart the GSM modem on the page "SMS" of the device's web interface. In the "GSM MODEM TROUBLESHOOTING" section, click the "Reboot GSM" button, after that the modem will reboot:



In the entry field "Last error of GSM modem (hit F5 to refresh)" the data and time of the last modem error is indicated as well as the error itself. To display the current error press the F5 key.

After rebooting and initializing the GSM modem, you can send a test SMS message by pressing the "Test SMS" button:



As a result, the mobile numbers registered in the section "SMS NOTIFICATION DESTINATIONS AND SMS COMMANDS SOURCES" on the page "SMS" of the device`s web interface should get the SMS message with the text "NetPing SMS Test"

[ENG] 11.7. [DKSF 70/71.7 IU] What kinds of SMS Notifications can this Device Send?

> The information in this section is applicable to the devices UniPing server solution v4/SMS with a built-in GSM modem.

SYNTAX OF SMS NOTIFICATIONS

SMS Notifications look like:

```
np_name (q) information
```

where:

np_name — is the name of the device for the identification of SMS messages. The name is set on the page "SETUP" of the device`s web interface. If the name of the device is not set, the "NETPING" name is used instead of it.

q - is the sequence number of messages. The number is nonvolatile. It does not reset when the power is switched off. It is needed for the registration of the missed (lost) messages.

Information - is the informative part of SMS messages.

INFORMATIVE PART OF SMS MESSAGES

A messages of the status change of IO line.

```
IOn=0|1 label transcript
```

where:

n — a number of IO line, 1...8.

label — IO line label, it is set in the "Memo" entry field on the "DISCRETE IO" page of the device's web interface. If the label is not specified (empty), then it is not included in the SMS.

transcript — is a decoding of the logical level of IO line, it is set in the pop-up dialogue of the notification configurations from IO line on the "DISC RETE" page of the device`s web interface. If the decoding is not set (empty), so it is not included in SMS.

Messages from Temperature Sensor

TEMP.SENSOR n "label" IS FAILED — temperature sensor failure (the sensor stopped responding to the poll)

TEMP.SENSOR n "label" IN SAFE RANGE (t1TO t2), NOW tC — the onset of a normal temperature condition within a specified range.

TEMP.SENSOR n "label" OUT OF RANGE (t1 TO t2), NOW tC — the temperature goes beyond the specified range.

where:

n — number of a temperature sensor, 1...8.

t — current temperature, °C.

t1, t2 — the thresholds of normal temperature range, °C.

label — a label of a temperature sensor which is set in the entry field “Memo” on the page “TEMPERATURE” of the device`s web-interface. The label in the message text is enclosed in quotation marks. If the label is not specified (empty), then it is not included in the SMS.

Messages from Humidity Sensor

RHn "label" FAILED — humidity sensor failure (the sensor stopped responding to the poll)

RHn "label" is OK, h% h_status, tC t_status — the recovery of the sensor operation (the sensor began to respond to the poll.

RHn "label" h% (below safe range h1..h2%) — relative humidity values below a specified range

RHn "label" h% (in the safe range h1..h2%) — relative humidity values in the norms of a specified range.

RHn "label" h% (above the safe range h1..h2%) — relative humidity values above a specified range

RHn "label" tC (below the safe range t1..t2C) — temperature values below a specified range (a temperature sensor is built into the relative humidity sensor).

RHn "label" tC (normal t1..t2C) — temperature values to the norms of a specified range (a temperature sensor is built into the relative humidity sensor).

RHn "label" tC (above normal t1..t2C) — temperature values above a specified range (a temperature sensor is built into the relative humidity sensor).

where:

n — number of Humidity Sensor, 1...4.

h — relative humidity, %.

h1, h2 —the thresholds of normal relative humidity range, %.

t — current temperature, °C.

t1, t2 — the thresholds of normal temperature range , °C.

h_status — humidity status, possible values: «below normal», «normal», «above normal».

t_status — temperature status, possible values: «below normal», «normal», «above normal».

label — humidity sensor label is set in the “Memo”entry field on the “HUMIDITY SENSORS” page of the device’s web interface. The label in the message text is enclosed in quotation marks. If the label is not specified (empty), then it is not included in the SMS.

Messages from an analog smoke sensor (current in the loop)

ANALOG SMOKE SENSOR: OK — the sensor has returned to a normal status

ANALOG SMOKE SENSOR: NOT POWERED — transition to the cut off status (cut off current).

ANALOG SMOKE SENSOR: ALARM! — transition to the "Alarm" status

ANALOG SMOKE SENSOR: FAILED (OPEN LOOP) — transition to the break off (open loop) status

ANALOG SMOKE SENSOR: FAILED (SHORT CIRCUIT) — transition to the «Short Circuit» status

Messages from a buil-in relay/Watchdog

RELAY n "label" ORDERED TO SWITCH OFF|ON — the relay got an order to switch off/on

RELAY n "label" SWITCHED OFF|ON — the relay is switched off/on

WDOG n "label" RESET — the message about the operation of the "Watchdog" module (a short-term on /off of the relay is carried out to restore the operation of the device connected to it).

where:

n — the relay number.

label — a relay label is set in the “Memo” entry field on the “RELAY” page of the device’s web interface. The label in the message text is enclosed in quotation marks. If the label is not specified (empty), then it is not included in the SMS.

A message about the recovery/failure of the cheched node in network (the "Pinger" module on the "SMS" page):

PINGER STATUS: OK|FAILED (IP/HOSTNAME)

where:

IP/HOSTNAME — IP address/DNS name of the checked node in network.

PERIODIC SMS REPORTS ON THE STATUS OF SENSORS, IO LINES AND RELAYS.

The device has the ability to send a daily report in the form of SMS messages on the status of sensors, IO lines and relays. You can read more about setting the time for sending this report in the section [ENG] 11.9. [DKSF 70/71.7 IU] Setting the Time for Sending a Summary Report About the Status of Sensors, IO Lines and Relays in the Form of SMS Messages

CUSTOM NOTIFICATIONS

The device's firmware has the ability to send custom notifications of various events. You can read more about custom notifications in the section [ENG] 14. [DKSF 70/71.7 IU] Device Support for Custom Notifications . The syntax for such notifications is not explicitly defined and is user-configurable.

[ENG] 11.8. [DKSF 70/71.7 IU] How Can I Control the Device using SMS Commands?

> The information in this section is applicable to the devices UniPing server solution v4/SMS with a built-in GSM modem.

The device has an ability to be controlled remotely using SMS commands.

> The firmware of the device has the ability to set white lists - numbers that are allowed to control the device. Read more about white lists in the section [ENG] 11.2. [DKSF 70/71.7 IU] I Need to Configure the Numbers to Send SMS-Notifications. How Can I do This?

THE SYNTAX OF SMS COMMANDS

The common format of an SMS command text:

```
NETPING fff community_w kkkkk
```

where:

fff — a code of a command, for example, P1+ (see below).

community_w — a password which corresponds to SNMP community for recording. It is set on the "SETUP" page of the device web-interface. It is possible to use Latin letters, numbers and some special symbols.

kkkkk — A request identifier (arbitrary number from 3 to 9 digits). It is repeated in the response to set the correspondence between the request and the response. An optional command element. If the identifier is not in the command, you can not see it in the response.

> Warning
>
> The text of the command is case insensitive, it is possible to use lowercase and uppercase letters. Command elements are separated by spaces. The characters (symbols) ‘(apostrophe),“ (quotation mark), @ are not allowed. Switching on these characters may cause a firmware failure. A command completion is confirmed by a response message (see below).

THE CODES OF COMMANDS

The command code is indicated together, without any spaces.

The codes of commands	The description
Pn+	Switch on the relay n, where n is the relay number
Pn-	Switch off the relay n, where n is the relay number
PnR	Reset the relay n, where n is the relay number. The direction (mode) of the reset corresponds to that one configured in the «Watchdog» module.
Pn?	Request relay status n, where n is the relay number
P?	Request relay status in a short form. As the device is equipped with one relay, the responce is identical to the command "Pn?"
Lm+	Set the line m to log. 1, where m is the number of the IO line. The line should be in the "exit" mode.
Lm-	Set the line m to log.0, where m is the number of the IO line. The line should be in the "exit" mode.
LmP	Give an impulse to the line m, where m is the number of the IO line. The line should be in the "exit" mode.
Lm?	Request the status of the line m, where m is the number of the IO line
L?	Request the status of all IO lines in a short form.
N?	Request the pinger status on the "SMS" page
Ka	Send the IR command through the IRC-TR v2 , where a is a number of a command
Tb?	Request the values of a Temperature Sensor b, where b - is a number of a Temperature Sensor

Hx?	Request the values of a Humidity Sensor x, where x - is a number of a Humidity Sensor.
T?	Request the values of all the Temperature Sensors. Only connected sensors values are displayed. The sign of connectivity is a specified 1W address.
H?	Request the values of all Humidity Sensors. Only connected sensors values are displayed. The sign of connectivity is a specified 1W address.
RB20	Reboot the device. The reboot will occur in 20 seconds after receiving a command.

THE EXAMPLES OF SMS COMMAMDS

Switch on command of the relay of 1 device:

```
NETPING P1+ SWITCH
```

Switch off command of the relay of 1 device:

```
NETPING P1- SWITCH
```

REPLY MESSAGES TO SMS COMMANDS

Confirmation of the command execution, such as switching a relay or changing a state of a discrete output line:

```
NP DONE fff kkkkk
```

where:

fff — is the code of the original command, which execution is confirmed by this message. For example, P1.

kkkkk — a request identifier (arbitrary number from 3 to 9 digits). It is repeated in the response to establish the correspondence between the request and the response. An optional command element. If the identifier is not in the command, you can not see it in the response.

An error occurred while the device is taking it. Most likely it is the wrong text of the original command:

```
NP WRONG CMD: "original command kkkkk"
```

where:

original command — the text of the original command fully quoted

kkkkk — a request identifier (arbitrary number from 3 to 9 digits). It is repeated in the response to establish the correspondence between the request and the response. An optional command element. If the identifier is not in the command, you can not see it in the response.

Wring password (Community) in an original command:

```
NP WRONG PASSWD IN kkkkk
NP WRONG PASSWD
```

where:

kkkkk — a request identifier (arbitrary number from 3 to 9 digits). It is repeated in the response to establish the correspondence between the request and the response. An optional command element. If the identifier is not in the command, you can not see it in the response (the second command).

RESPONSE MESSAGES TO STATUS / STATE REQUEST SMS COMMANDS

Response to the request (NETPING Pn? community_w kkkkk) about the relay status:

```
NP REPLY Pn+ kkkkk
```

where:

n — the number of the relay

b —the state of the relay, possible states are encoded with the symbols «+» (swtiched on), «-» (switched off)

kkkkk — a request identifier (arbitrary number from 3 to 9 digits). It is repeated in the response to establish the correspondence between the request and the response. An optional command element. If the identifier is not in the command, you can not see it in the response.

Response to the request (NETPING Lm? community_w kkkkk) about the IO line:

```
NP REPLY Lm=l(mode) kkkkk
```

where:

m — the number of the IO line

l — the logical level of the IO line, possible values: 0 (logical zero), 1 (logical unit).

mode — IO line operating mode, possible values: IN (input), OUT (output).

kkkkk —a request identifier (arbitrary number from 3 to 9 digits). It is repeated in the response to establish the correspondence between the request and the response. An optional command element. If the identifier is not in the command, you can not see it in the response.

Response to the request (NETPING L? community_w kkkkk) about all IO lines:

```
NP REPLY Lm=l(mode) Lm=l(mode) Lm=l(mode) Lm=l(mode) Lm=l(mode) Lm=l(mode) Lm=l(mode) kkkkk
```

where:

m – the number of the IO line

l — the logical level of the IO line, possible values: 0 (logical zero), 1 (logical unit).

mode — IO line operating mode, possible values: IN (input), OUT (output).

kkkkk — a request identifier (arbitrary number from 3 to 9 digits). It is repeated in the response to establish the correspondence between the request and the response. An optional command element. If the identifier is not in the command, you can not see it in the response.

Response to the request (NETPING N? community_w kkkkk) about the state of the pinger built-in the SMS module:

```
NP REPLY N=0|1 kkkkk
```

where:

N=0 — the specified IP address / DNS name is silent.

N=1 — the specified IP address / DNS name is responding.

kkkkk —a request identifier (arbitrary number from 3 to 9 digits). It is repeated in the response to establish the correspondence between the request and the response. An optional command element. If the identifier is not in the command, you can not see it in the response.

Response to the request (NETPING Tb? community_w kkkkk) about the values of the Temperature Sensor. Sensor number b failed or not connected:

```
NP REPLY Tb=? SENSOR FAILED kkkkk
```

where:

b — the number or the Temperature Sensor;

kkkkk —a request identifier (arbitrary number from 3 to 9 digits). It is repeated in the response to establish the correspondence between the request and the response. An optional command element. If the identifier is not in the command, you can not see it in the response.

Response to the request (NETPING Tb? community_w kkkkk) about the values of the Temperature Sensor:

```
NP REPLY Tb=tC BELOW|IN|ABOVE SAFE RANGE (t1..t2C) kkkkk
```

where:

b — the number of the Temperature Sensor.

t — the current temperature value, °C.

t1, t2 — the thresholds of the normal temperature range, °C.

kkkkk —a request identifier (arbitrary number from 3 to 9 digits). It is repeated in the response to establish the correspondence between the request and the response. An optional command element. If the identifier is not in the command, you can not see it in the response.

Response to the request (NETPING Hx? community_w kkkkk) about the values of the Humidity Sensor. Sensor number b failed or not connected:

```
NP REPLY Hx=? SENSOR FAILED kkkkk
```

where:

x — the number of the Humidity Sensor;

kkkkk —a request identifier (arbitrary number from 3 to 9 digits). It is repeated in the response to establish the correspondence between the request and the response. An optional command element. If the identifier is not in the command, you can not see it in the response.

Response to the requst (NETPING Hx? community_w kkkkk) about the values of the Humidity Sensor:

```
NP REPLY Hx=h% BELOW|IN|ABOVE SAFE RANGE (h1..h2%) T= tC BELOW|IN|ABOVE SAFE RANGE (t1..t2C) kkkkk
```

where:

x — the number of the Humidity Sensor

h — the current value of the relative humidity, in %.

h1, h2 — the thresholds of the normal relative humidity range, %.

t — the current value of temperature, in °C

t1, t2 — в the thresholds of the normal temperature range, in °C.

kkkkk —

a request identifier (arbitrary number from 3 to 9 digits). It is repeated in the response to establish the correspondence between the request and the response. An optional command element. If the identifier is not in the command, you can not see it in the response.

[ENG] 11.9. [DKSF 70/71.7 IU] Setting the Time for Sending a Summary Report About the Status of Sensors, IO Lines and Relays in the Form of SMS Messages

> The information in this section is applicable to the devices UniPing server solution v4/SMS with a built-in GSM modem.

In order ot set the time for sending the summary report in the form of SMS messages you need to open the "SMS" page of the device`s web interface.

where:

Time to send Summary Report (24h format hh:mm, up to 5 time points, separated by space) — it is the time when the reports will be sent in the for of SMS about the sensors status, IO line and the relay. In Default: empty line.

After setting the time it is necessary to save all the parameters changes by pressing the button "Apply Changes".

[ENG] 11.10. [DKSF 70/71.7 IU] How to Find Out IMEI of the Built-in GSM Modem?

> The information in this section is applicable to the devices UniPing server solution v4/SMS with a built-in GSM modem.

To get an IMEI (International Mobile Station Equipment Identity) of a built-in GSM modem, there is a need to go to a service page of a web-interface of a device via the address:

```
http://192.168.0.100/at.html
```

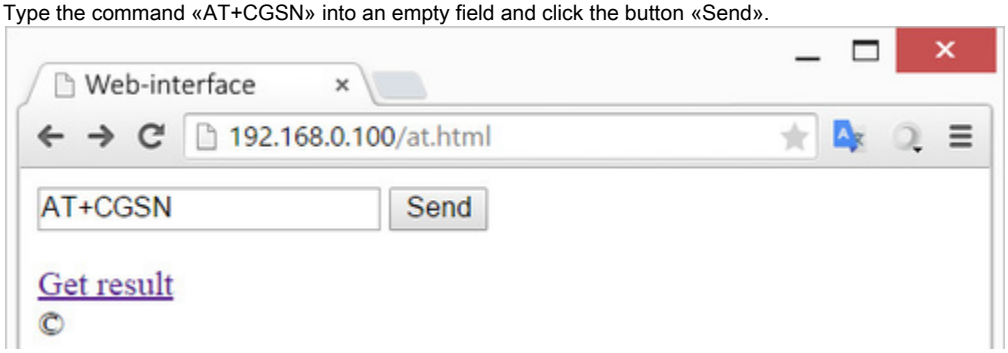
where:

192.168.0.100 – is a default IP address of a NetPing device;

/at.html – is a service page for sending AT-commands

To send an AT-command for receiving an IMEI, there is a need to:

1. Type the command «AT+CGSN» into an empty field and click the button «Send».



2. Click the link «Get result» to view an IMEI of a built-in GSM modem.

[ENG] 11.11. [DKSF 70/71.7 IU] How to Send Arbitrary SMS?

> The information in this section is applicable to the devices UniPing server solution v4/SMS with a built-in GSM modem.

The firmware of the UniPing server solution v4/SMS device in DKSF in the version 70.7.X includes the ability to send arbitrary SMS messages using the SNMP protocol and the third-party web applications (HTTP API).

SENDING SMS MESSAGES USING SNMP

> To send arbitrary SMS in Cyrillic using the SNMP protocol, you need to use the encoding UTF-8 (Converting files to UTF-8) or Windows-1251 in the text of the SMS message.

. To send SMS using the SNMP protocol, you need to use the variable “npGsmSendSmsUtf8” or “npGsmSendSmsWin1251”, in which the recipient's telephone number and SMS message text are recorded. To do this, look at the MIB file, which can be downloaded on the device description page in the "DOC&FILES" section.

OID	Name	Type	Access	Description
.1.3.6.1.4.1.25728.3800.1.9.0	npGsmSendSmsUtf8	DisplayString	READ/WRITE	Sending an arbitrary SMS message in UTF-8 encoding.
.1.3.6.1.4.1.25728.3800.1.10.0	npGsmSendSmsWin1251	DisplayString	READ/WRITE	.Sending an arbitrary SMS message in Windows-1251 encoding.

The Format of an arbitrary SMS message:

```
[phone_number1,phone_number2,phone_number3,phone_number4] Message
```

where:

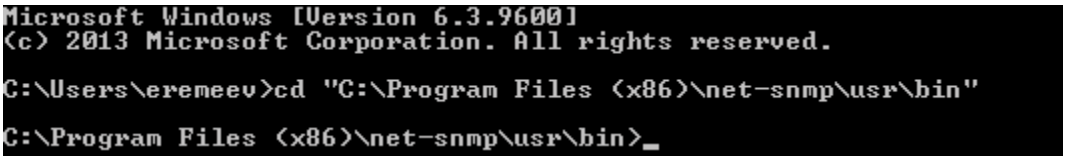
phone_number —recipient number in square brackets (you can send SMS to several recipients, indicating them in square brackets, separated by commas, without spaces. If you do not select recipients, SMS will go to the numbers specified in the settings on the "SMS" page of the device’s web interface);

Message — message text (written with a space from the recipient number)

An Example command sequence for sending arbitrary SMS via SNMP using the NET-SNMP packet

1. To send an arbitrary SMS, you can use the special NET-SNMP package.

2. After installing the NET-SNMP package, run the snmpset.exe utility on the command line. To start the command line, use the keyboard shortcut "snmpset.exe". After opening the "Run" window, enter the "cmd" command and press the "Enter" key. Next, at the command line, go to the installation directory of the snmpset.exe:



3. Run the snmpset.exe utility with the following command line parameters:

```
snmpset.exe -v 1 -c COMMUNITY IP OID TYPE VALUE
```

where:

COMMUNITY — a special code word that is set on the "SETUP" page of the device’s web interface. On the NetPing devices, by default community = SWITCH;

IP — an IP address of the NetPing device through with the arbitrary SMS message will be sent;

OID — an SNMP identifier of the variable “npGsmSendSmsUtf8” or “npGsmSendSmsWin1251”, which is used to send an arbitrary SMS message;

TYPE — a type of a registered value of the SNMP identifier of the variable. The type designation is shown in the picture:

VALUE - a registered value, i.e. the text of the SMS message.

According to the description written above, a command to send an arbitrary SMS using the utility snmpset.exe:

```
C:\Program Files (x86)\net-snmp\usr\bin>snmpset.exe -v 1 -c SWITCH 192.168.0.100 .1.3.6.1.4.1.25728.3800.1.9.0 s "[+79130000000] Hello! Test SMS!"
```

4. After the successful execution of the command, the following answer should be received:

```
SNMPv2-SMI::enterprises.25728.3800.1.9.0 = STRING: "[+79130000000] Hello! Test SMS!"
```

(HTTP API)SENDING SMS MESSAGES THROUGH THIRD-PARTY WEB APPLICATIONS (HTTP API)

> The maximum length of the arbitrary SMS messages should not exceed 250 characters.

An example of sending arbitrary SMS using JavaScript code

To send SMS via third-party web applications, you can use the following JavaScript code:

```
var r = new XMLHttpRequest();
r.open('POST', 'http://192.168.0.100/sendsms.cgi?utf8', true, 'visor', 'ping'); // visor:ping – the user name and password
r.withCredentials = true;
r.send('[+79130000001,+79130000002,+79130000003,+79130000004] Huston, we have a problem!');
```

where:

192.168.0.100 — an IP address of the device in Default.

visor — a default username for connecting to the device's web interface.

ping — a default password for connecting to the device`s web interface.

You can send SMS to several recipients, indicating them in square brackets separated by commas, without spaces. If you do not select recipients, SMS will be sent to the numbers specified in the settings on the "SMS" page of the device's web interface.

If the data format is correct, the JavaScript code is returned as the result:

```
sendsms_result('ok');
```

The result of sending a message does not affect the response returned by the CGI (Common Gateway Interface). CGI only initiates the sending process of a message.

An example of sending arbitrary SMS using a PowerShell script

To send SMS via third-party web applications, you can use the following PowerShell script:

```
$url = "http://192.168.0.100/sendsms.cgi?utf8"
$username = "visor"
$password = "ping"

$reqBody = "[+79130000001,+79130000002,+79130000003,+79130000004] Huston, we have a problem!"

$req = [System.Net.WebRequest]::Create($url)
$req.Method = "POST";

$req.Credentials = new-object System.Net.NetworkCredential($username, $password)

$Body = [System.Text.Encoding]::UTF8.GetBytes($reqBody);
```

```
$stream = $req.GetRequestStream();
$stream.Write($Body, 0, $Body.Length);

$stream.Flush();
$stream.Close();

$resp = $req.GetResponse().GetResponseStream()
$resp.Close()
```

where:

$url - a variable value that sets the IP address of the NetPing device and a script for sending arbitrary SMS messages;

$username — $ username - a variable value that sets the username for authorization in the NetPing device;

$password — a variable value where the password for authorization on the NetPing device is set;

$reqBody — a variable value where the recipient number is set in square brackets and the text of the SMS message (which is written separated by a space from the recipient number. You can send SMS to several recipients by adding them in square brackets, separated by commas, without spaces).

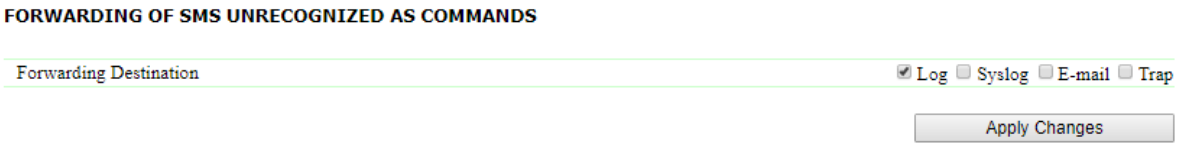
[ENG] 11.12. [DKSF 70/71.7 IU] How can I Configure the Forwarding of Incoming Unrecognized SMS As a Command?

The device firmware provides the possibility to configure SMS forwarding, which were unrecognized as commands:

- to the log;
- to Syslog (Syslog must be configured in the device)
- by email;
- by SNMP TRAP message;
- to an arbitrary phone number (using custom notifications. For more information about custom notifications, see [ENG] 14. [DKSF 70/71.7 IU] Device Support for Custom Notifications .

For example, this function makes it possible to implement the processing of incoming SMS for any third-party service on the basis of the device or to notify the user of incoming SMS (if the SIM card is used not only for the monitoring device aims, but, for example, for personal purposes - SMS from a bank or from customers).

The forwarding is configured on the "SMS" page. Having selected the necessary delivery methods by check boxes, save the changes with the button "Apply Changes"

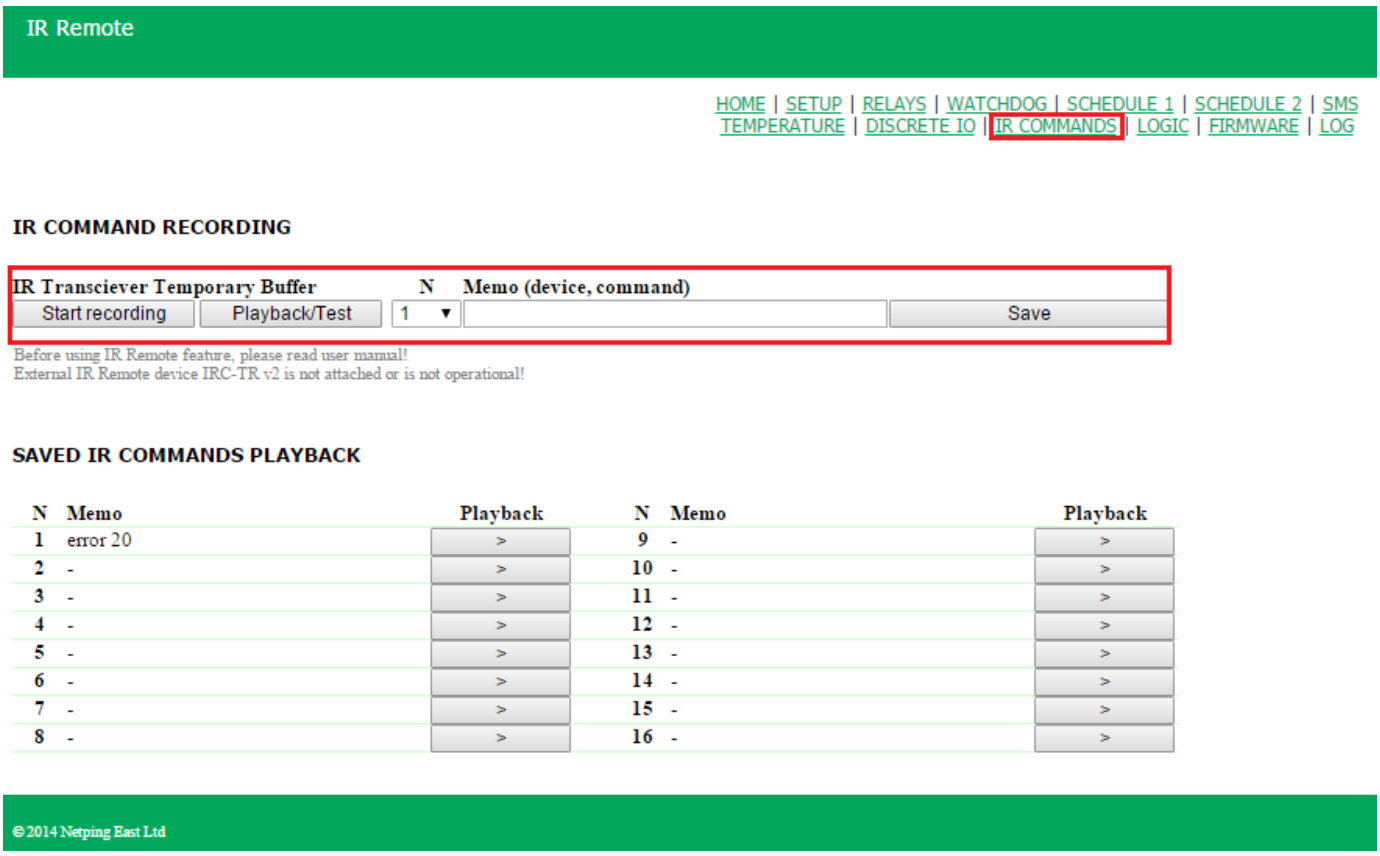


[ENG] 12. [DKSF 70/71.7 IU] Work with IR Command Module

[ENG] 12.1. [DKSF 70/71.7 IU] How Can I Record IR Commands Corectly?

An IR Control module works with an IR transceiver IRC-TR v2. The transceiver can record and reproduce IR signals from remote controls of home appliances.

To record IR commands, there is a need to go to the page «IR COMMANDS» of a device web interface:



New IR commands are recorded in the section «IR COMMAND RECORDING»:

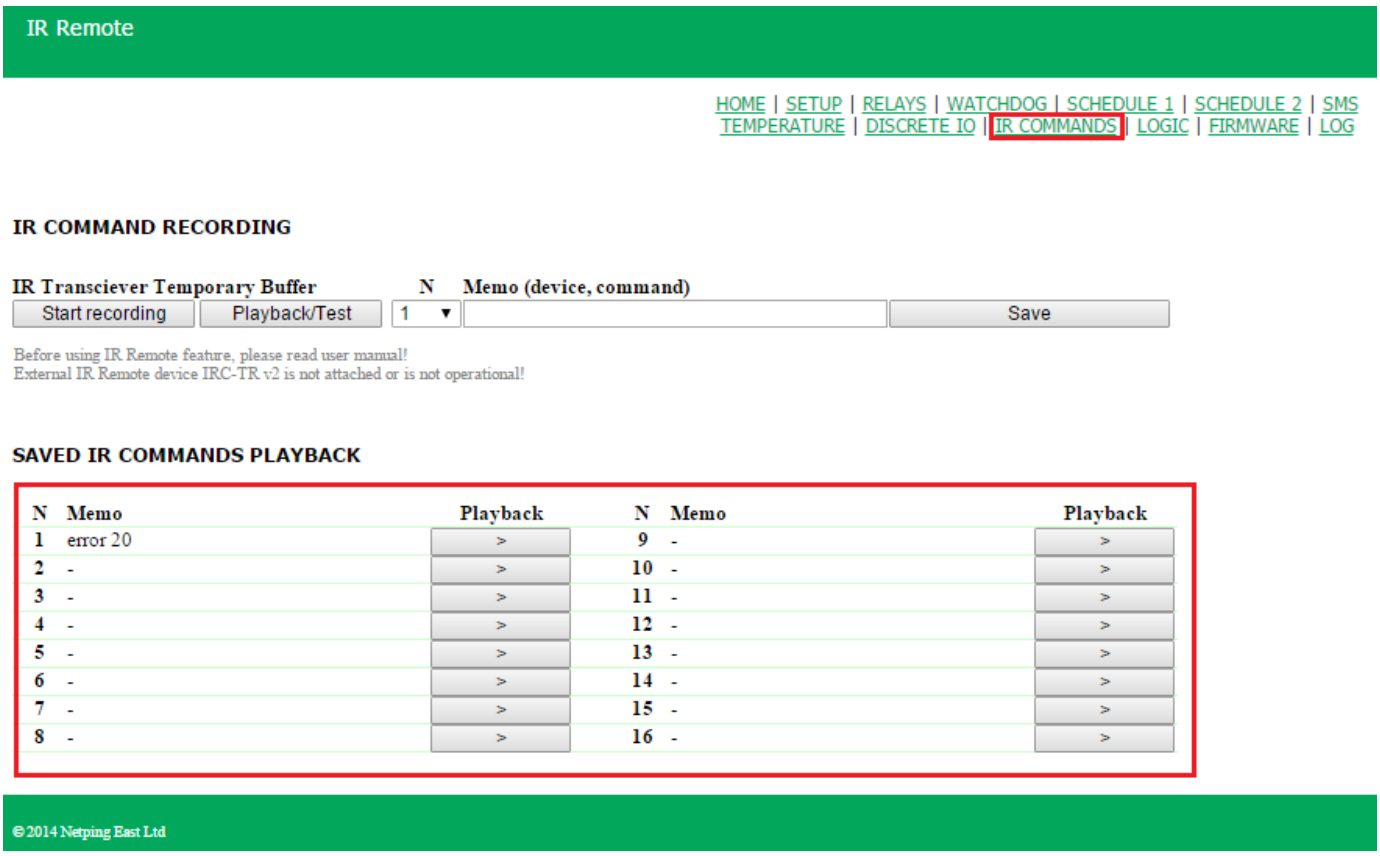
1. Prepare an IR remote, from which it is necessary to capture a command.
2. Make sure that a red LED on the IR transceiver glows steadily
3. Choose a command number «N» and enter its description into the field «Memo (device, command)».
4. Click the button «Start recording». Send a command from an IR remote 30 seconds after clicking the button «Start recording». Otherwise, a transceiver will go to a standby mode. A remote and a transceiver must be disposed coaxially at the distance of 10-30 cm for an «eye» of a transceiver to see a transmitting IR LED of a remote. A command will be recorded.
5. Check a recorded command by clicking the button «Play/Test».
6. Click the button «Save» to save a command in a nonvolatile memory if a command is successfully reproduced.

It is desirable to check again the operation of an IR command by clicking a corresponding button «>» in the section of saved commands.

[ENG] 12.2. [DKSF 70/71.7 IU] Playback of IR Commands Via the Web Interface

An IR control module works with an IR transceiver IRC-TR v2. A transceiver can record and reproduce IR signals from remotes of home appliances.

To reproduce IR commands, go to the page «IR COMMANDS» of a web interface of a device:



In the section «Saved IR Commands» recorded IR commands are reproduced.

To reproduce a saved IR command click the button «>» in the section «Saved IR Commads» next to the name of a necessary command. A red LED on a transceiver must be switched off for 0.5 s., initiating reproducing a command.

> Do not reproduce «empty» command cells, where there is no proper record of an IR command. This can cause a transceiver to freeze.

You can also playback IT commands with the help of the SNMP and HTTP API protocoles of the commands.

[ENG] 12.3. [DKSF 70/71.7 IU] Can I Play Back the IR Commands via SNMP?

IR commands can be played back via SNMP. The necessary information is contained in the MIB file which corresponds to the applicable firmware version of the device. You can download the required MIB file on the device description pages in the "Downloads" section:

- UniPing server solution v4/SMS;
- UniPing server solution v3.

> The record commands is only possible with the help of the device`s web interface.

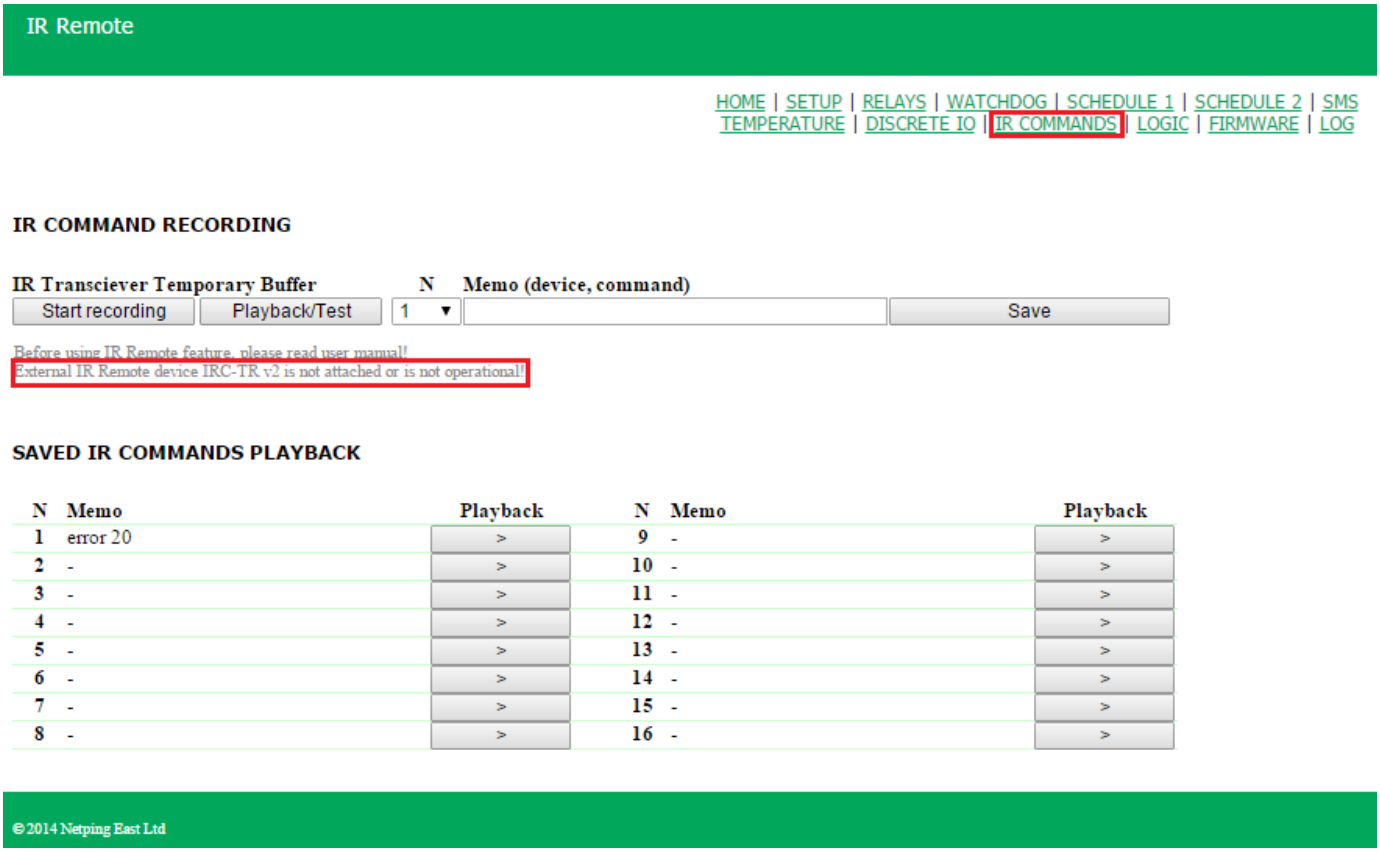
The playback of IR commands via SNMP protocole:

1. Before you make an IR command, make sure that the transceiver is in a standby condition, reading the status via OID .1.3.6.1.4.1.25728 .7900.1.3.0. The status value «commandCompleted (0)» or «commandAccepted (2)» means tha IR transceiver is ready to play the IR command.
2. To make an IR command, write down the command number (the cell number of the saved command) in the OID .1.3.6.1.4.1.25728.7900. 1.1.0.
3. If the transceiver is in the “protocolError (1)” state, the reset is performed by recording the value “1” to OID .1.3.6.1.4.1.25728.7900.1.2.0 (valid for IR module expansion IRC-TR v1).
4. After the reset of the command, you have to wait for the readiness of "commandCompleted (0)", reading the status. If repeated playback of the IR command does not violate the logic of the equipment operating, then it is better to repeat the process of the command 2–4 times, each time checking the readiness before executing the command.

All the states of and IR extension module you can see in MIB files DKSF_70.7.x_ MB.mib, DKSF_71.7.x_ MB.mib (OID «npIrStatus») or on the page [ENG] 15.3. [DKSF 70/71.7 IU] Which OID are Supported By the Device? of this description of the firmware.

[ENG] 12.4. [DKSF 70/71.7 IU] How Can I Determine the Version of a Built-In Firmware of IR module?

To determine a firmware version of an IR module, go to the web page «IR Commands» of a device web interface:



In the section «Saved IR Commands» there is an inscription «A version of a connected IR control module is IRC-TR v2: HW X.X / BL X.X / FW X.X»

where:

HW – is a hardware version of an IR module.

BL – is a Bootloader version of an IR module.

FW – is a firmware version of an IR module.

> A version of the hardware, loader and firmware can be seen if a module is correctly connected to a device and works properly. Otherwise, in the section «Saved IR Commands» there will be an inscription «External IR Remote device IRC-TR v2 is not attached or is not operating!»

[ENG] 12.5. [DKSF 70/71.7 IU] Recommendations

If a transceiver is stuck in a protocol as a result of a failure, noise, an operator's error or managing software failure, and reacts improperly to incoming commands, a reset can be performed by a short-term (5 s.) switching off a transceiver from a NetPing device.

Try to avoid recording commands in electroluminescent or LED lighting. The flickering light with a frequency of operation of the electronic ballast can decrease a quality of a recorded IR signal.

Watch avoiding any objects, particularly operator's hands, between an emitter of an IR remote and an «eye» of a transceiver while recording commands.

If a recorded command works unreliably, change a location of a transceiver in relation to a controlled device. In addition, change conditions of recording a command.

[ENG] 13. [DKSF 70/71.7 IU] Work with the "LOGIC" module

[ENG] 13.1. [DKSF 70/71.7 IU] What is "LOGIC"?

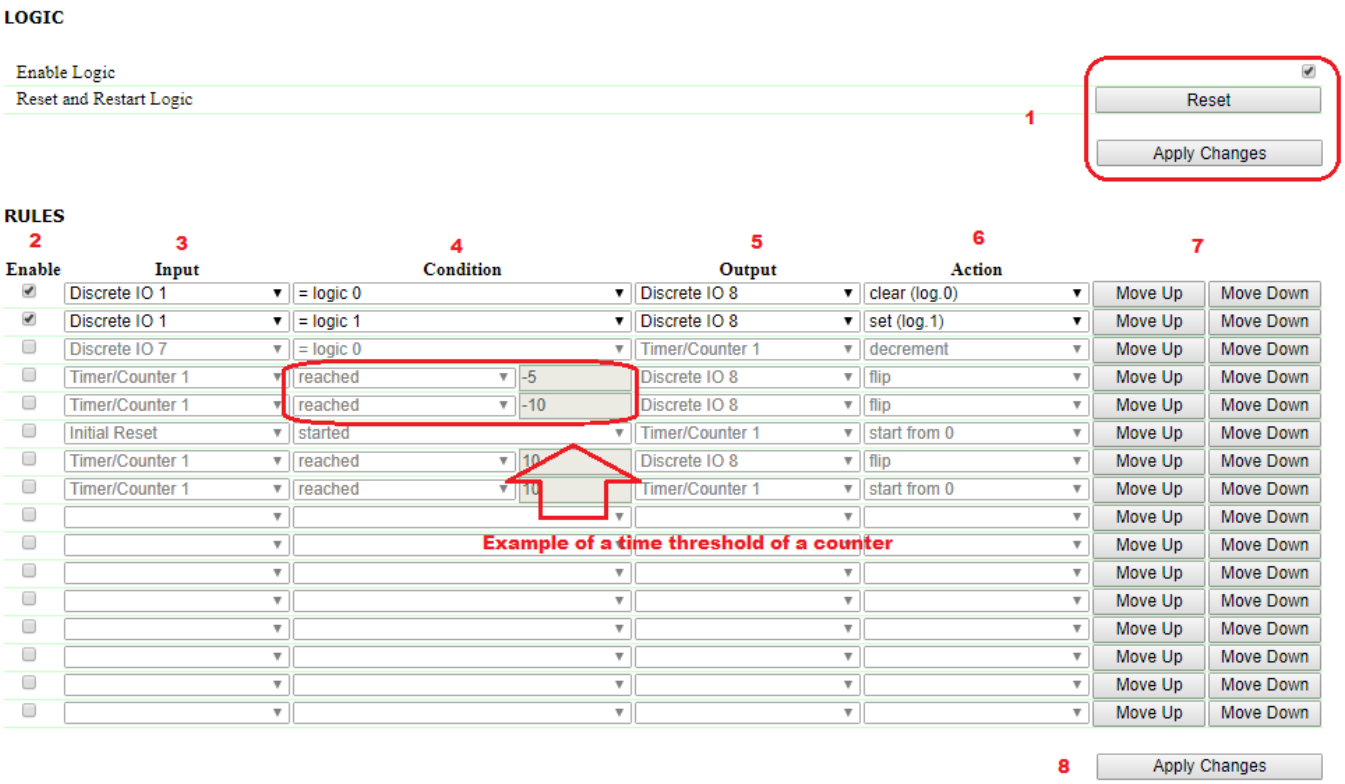
A logic module of a firmware is designed for a simple automation and can perform such tasks as maintaining a microclimate, controlling automatic turning on - turning off a backup equipment, etc. The logic operates on the basis of rules programmed by a user through a web interface. The page «LOGIC» of a device web interface describes an operating algorithm of a module and its configuration capabilities.

> It is prohibited to use a NetPing device to manage electrical circuits when a violation of the control may cause a significant damage.

[ENG] 13.2. [DKSF 70/71.7 IU] How Can I Use the "LOGIC" module?

> IMPORTANT. In the updated module "LOGIC" (beginning from the DKSF 70/71.7.2 firmware version), all the rules are identical to the rules of the "If" type in previous versions of the logic (the logic of the module has become non-blocking or the so-called anarchic). They work at the moment when the condition of the rule becomes true and have no priorities. All sources of controlling the output of rules are simultaneously active and equal (for example, for relays or IO lines).

The operation of the logic module is based on a list of programmed rules.



where:

1. The buttons of controling the "LOGIC" module:

- «Enable Logic» — a check-box that enables and disables the operation of logic. After changing the state of the check box, you need to save the current settings with the button "Apply Changes"
- «Reset» — initiates the reset of logic (the signal «Reset and Restart Logic»).
- «Apply changes» saves the current settings.

2. Check box RULES Enable — check box of activation the rule logic. Inactive rules are displayed in gray colour.

3. Input - the source of information for work of a rule. Possible values are presented in the table below.

4. Condition — the condition when the rule is applied and a command is issued that changes the state of the output. The available set of conditions varies depending on the type of a selected input, and reflects the meaning of the input state. Below you can see possible values depending on the type or input.

Input of the rule	Decoding	Possible conditions (events)	Condition decoding
Reset and Restart Logic	A signal that is active at the start (restart) of the firmware or after you press the “Reset” button (1) on the logic page, before all other logical rules For more details look here -[ENG] 13.5. [DKSF 70/71.7 IU] Initial Reset and Initial Output Status	Has begun	The rule is triggered in 5 seconds after the reset.
		Has finished	The rule is triggered in 10 seconds after the reset.

IO-line 1..8	Current logic level of IO line	= log. 0	The logic level of the selected IO line has switched to 0 or 1.
		= log. 1	
Termo 1..8	Readings of temperature sensor 1-Wire	below [N]	The temperature sensor readings dropped below or rose above the threshold N, where N is the set temperature threshold. It is allowed to set the threshold with a floating point, up to decimal, for example, 5.3.
		above [N]	
		failed	The sensor failed
Humidity Sensor 1..4	Reading of a relative humidity sensor with a built-in temperature sensor	t below [N]	The temperature readings of the humidity sensor dropped below or rose above threshold N, where N is the set temperature threshold. It is allowed to set the threshold with a floating point, up to decimal, for example, 5.3.
		t above [N]	
		relative humidity above [N]	Relative humidity rose above N, where N is the specified humidity threshold.
		relative humidity below [N]	Relative humidity dropped below N, where N is the specified humidity threshold.
		failed	The sensor failed
Pinger 1..2	Verifying the remote host using ping (ICMP requests)	fell silent	The response from the host verified by the pinger has disappeared or appeared. About setting up the pinger itself — [ENG] 13.4. [DKSF 70/71.7 IU] What is SNMP SETTER?
		responding	
Relay 1	The status of a built-in relay	= on	A built-in relay 1 turned on or off.
		= off	
ANLG Smoke Sensor	Analog Smoke Sensor (Current in the Loop)	normal	The sensor status - normal
		alert	Smoke detector alert (configured on the sensor page).
		failed loop	Failed current in the loop (broken look or short in the loop).
		off	The sensor is off. The current loop is deactivated.
	These smoke sensor (current in the loop) conditions are used to configure operation with current loop type sensors similar to a smoke sensor ИП212-141 The Criteria of the norm, alarm, failure are set in the settings on the page " ANLG SMOKE SENSOR ".	current (mA) has become above [N]	The current flowing through the current loop has become above/below than the set value mA, where N is the current in mA. It can be applied if the current is specified for the current sensor in its various conditions.
		current (mA) has become below [N]	
		resistance. (Ohm) has become above [N]	The resistance of the current in loop has become higher / lower than N, where N is the resistance value in Ohm. For current sensors, the resistance of the sensor in various conditions is more often specified. In most cases, such sensors do not have a current stabilizer, but simply a key, relay or transistor that changes the resistance of the sensor. This condition can be used if you install resistance of various ratings on the output relay of sensors connected in parallel to a common loop - you will get the “addressing” of the sensors when the triggered sensor can be identified by the loop resistance.
		resistance (Ohm) has become below [N]	
Timer / Counter 1..4	Program Timer / Counter	reached [N]	The internal timer / counter has become> = the set threshold [N]. The timer / counter value is any number (> 0) controlled by the “add 1” and “decrease 1” commands (counter functions), or the period of time from the “start from 0” command in seconds with a resolution of 0.1 second (timer functions) . it is not recommended to mix the functions of timer and counter.
Smoke 1..4	1-Wire smoke sensor	in normal state	The sensor is operating normally
		alarm	The sensor detected smoke.
		off	The current in loop connected to the sensor is deactivated.
		failed	The sensor is failed

5. Output — The element of the device that is controlled by the rule

6. Action — possible actions of the output of the rule

Possible outputs of the rules and actions for them are presented in the table:

Output of the rule	Decoding	Possible actions	Actions decoding
ANLG SMOKE SENSOR	Power control of an analog smoke sensor (current in the loop)	off	Turn off the power to the sensor
		on	Turn on the power to the sensor
		reset	Reset the sensor (off-on power for the time which is specified in the settings).
Smoke 1..4	The control of 1-Wire-smoke sensor	on power	Power on the current loop
		off power	Power off the current loop
		switch power	Switch power of the current loop
		reset	Reset the sensor (on/off power)
Relay 1	The control of the built-in relay	off	Turn off the relay
		on	Turn on the relay
		switch	Switch the relay to the opposite state
Signal 1..4	Activation of a signal to send a custom notification —[ENG] 14. [DKSF 70/71.7 IU] Device Support for Custom Notifications	activate	Send a signal. For a custom notification on the "NOTIFICATIONS" page, start sending it using a logic rule.
Timer/Counter 1..4	The control of a built-in timer/counter it is not recommended to mix the functions of timer and counter.	set from 0 (the timer function)	Start the timer from 0. The countdown is carried out in seconds with a resolution of 0 ... 1sec.
		reset to 0	Stop and reset the timer. Reset counter.
		add 1 (the counter function)	Add 1 (increment) to the current counter value.
		decrease 1 (th counter function)	Decrease 1 (decrement) from the current counter value. The counter value does not decrease below zero.
IO line 1..8	The control of IO line	off (log.0)	Set the line to log.0 state.
		on (log.1)	Set the line to log.1 state.
		switch	Switch log. state of the line
		impulse	To send an impulse to the line. Duration is set in the settings of the IO line.
IR 1..4	Send an IR command with a specified number	send a command	Play the command with the specified number recorded in the memory of the IRC-TR v2 mod ule.
SNMP Setter 1..2	The sending of SNMP SET commands to the other devices	off	Record the value corresponding to “off” to the specified OID in Setter’s settings.
		on	Record the value corresponding to “on” to the specified OID in Setter’s settings.

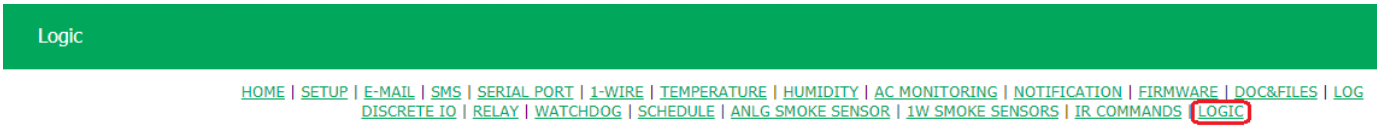
7. The buttons “above” / “below”. The buttons are used to change the position of a rule in the list. Starting with DKSF software version 70/71.7.2, the order of the rules does not affect the priority of the rules.

> You should avoid conflicting rules if they can lead to an attempt to control the same output simultaneously.

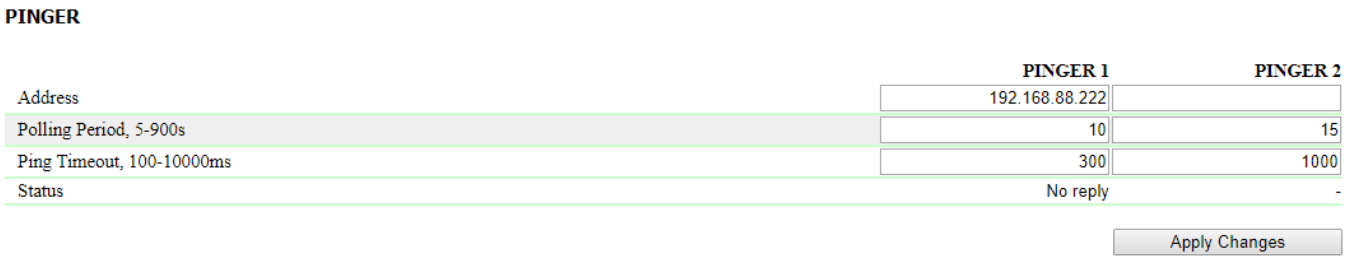
8. Apply the changes. The "Apply Changes" button saves the programmed logic rules in the device memory.

[ENG] 13.3. [DKSF 70/71.7 IU] How Can I Configure the Pinger in the "LOGIC" Module?

In order to configure the pinger you have to open the "LOGIC" page of the device`s web interface:



In the “PINGER” section, you can configure the network accessibility of the specified IP address/DNS name. The result of the check (pinger status) can be selected as the “input” of the logic rule. You can find out how to configure a rule in the "LOGIC" module by studying the section [ENG] 13.2. [DKSF 70/71.7 IU] How Can I Use the "LOGIC" module?. You can configure no more than two pingers - “PINGER 1”, “PINGER 2”. A typical application of pinger is automatic power-up of backup equipment in case of connection line failure.



where:

ADDRESS — IP address / DNS name of the device which is checked for availability. An empty line disables the poll.In Default: empty line.

Polling Period, s (5-900) — the value is selected according to the speed of detecting the fault. A regular check is carried out with the indicated period. Please note that overly frequent power switching can reduce equipment service life. In Default: 15.

Ping Timeout, ms (100-10000) —ping response timeout. The timeout is selected for reasons of typical device response speed, taking into account network delays. If there is no response to ping after a timeout, the ping is repeated. If after four periods of sending there is no answer, the status of the pinger changes to “silent”, and retries stop until the next verification period. In Default: 1000.

Status — possible values: «No reply», «Silent», «-». If the poll is not completed, the status can be unidentified. In this case rules that depend on the pinger are triggered when the pinger status changes to the specified one.

If you use domain names, you should take into accont that due to the unavailability of the DNS server or the lack of an IP address in the settings, the "LOGIC" DNS module will not be able to determine the availability of the polled address. "Pinger" changes into the "silent" status.

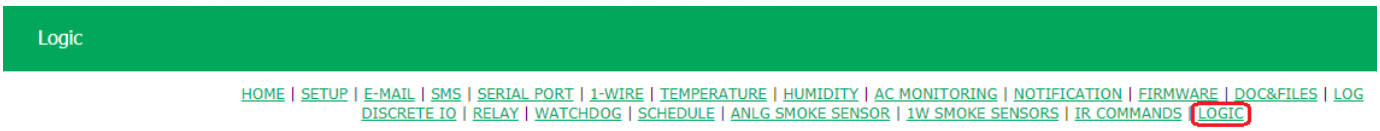
If the polled address is not set or the DNS server (if the address is set by a domain name) is not available, the pinger is in the "silent" status.

After configuration of the pinger values you should press the "Apply Changes" button.

[ENG] 13.4. [DKSF 70/71.7 IU] What is SNMP SETTER?

SNMP Setter is used as the output of the “LOGIC” module rule and you need it to set the SNMP OID variable value on the remote device using SNMP v1 protocol. In particular, you can control IO lines, relays, and other parameters of a remote NetPing device over a network.

SNMP SETTER is configured on the "LOGIC" page of the web interface:



In the section «SNMP SETTER» you can configure the SETTER`s parameters:

Number of Channel («SNMP 1», «SNMP 2») — in this version of the software two SNMP SETTER “channels” are implemented.

Memo — customtext up to 30 characters. In Default: empty line.

Address — an IP address or domain name (up to 62 characters) where the SNMP SET request will be sent to. In Default: empty line.

UDP Port — a port, where the SNMP SER requests are sent to. In Default: 161.

OID (.1.3.6...) — an identifier of the variable value that will be set on a remote device. It is necessary to specify the full OID in numerical notation, starting with .1.3 ... The list of variable values is contained in the MIB file from the device or in the documentation to the device. To see the MIB file conveniently of in the form of a tree and checking the functions of variable values, you can use the free software iReasoning MIB Browser or any similar software. In Default: .1.3.6.1.4.1.25728.5800.3.1.3.1.

Community — SNMP Community with the right to sign (Write), configured on a remote device. In Default: empty line.

"On" Value (Type Integer32) — the value that will be recorded in the OID on the remote device when the “On” action is called in the logic rule. The value type is a 32-bit signed integer. In Default: 1.

"Off" Value (Type Integer32) — the value that will be recorded in the OID on the remote device when the “Off” action is called in the logic rule. The value type is a 32-bit signed integer. In Default: 0.

Test It — when you press the «On» and «Off» buttons the device sends the corresponding requests with the values immediately. They are used to check the operaion of SNMP SETTER.

Status — in a few seconds after sending a request to set a variable value, the result is displayed in the "Status" entry field. “OK” means that confirmation is received and the variable value is set successfully. “Timeout” means that no approvement has been received. This can happen as a result of the unavailability of the controlled device, its failure, the wrong address, port or community. A dash “-” means that the SNMP SETTER has not sent a command yet. "Waiting for a response" means that SNMP SETTER sent a command to a remote device and is waiting for a response. Other options mean that an answer was received with an error code, its text decryption is displayed in the status line.

After changing the settings press th "Apply Changes" button.

[ENG] 13.5. [DKSF 70/71.7 IU] Initial Reset and Initial Output Status

At the start of the logic, it is possible to set the outputs and the equipment they control in a known and predetermined initial state. To do this, use the rules with the entry "Initial Reset".

The rule "Initial reset" with the condition "Enables" is triggered 5 seconds after the reset. The rule with the term “Ended” is triggered in 10 seconds after the reset. After that, the usual application of the rules starts with sources other than “Initial reset” in an infinite loop. So, it is possible to generate a 5-second external reset pulse at one or more outputs or to ensure the correct sequence of power supply to external devices.

[ENG]13.6. [DKSF 70/71.7 IU] IR Commands

The rule of the "LOGIC" module can be controlled by means the IR commands via the external IRC-TR v2 module. First of all, you have to write the necessary commands from the remote control (s) to the cells 1 ... 4 of the IRC-TR v2 module. The action “Send a command” for the “IR 1..4”o utput reproduces the IR command recorded under the corresponding number.

> As a rule, if you press one button on air conditioner remotes, they do not send the code of the pressed button, but a complete package of settings, such as temperature, fan speed, damper operation mode, etc.

[ENG] 13.7. [DKSF 70/71.7 IU] The Examples of the "LOGIC" Module Configuration

The automation examples based on the "LOGIC" module are published on the blog in our official website:

1. CONTROLLING TOO FREQUENT DOOR OPENING IN A SERVER ROOM ON THE BASIS OF A NEW MODULE "LOGIC" OF A NETPING DEVICE
2. SEQUENTIAL SERVERS STARTUP WITH PAUSES ON THE BASIS OF THE NEW MODULE "LOGIC" OF A NETPING POWER DISTRIBUTION UNIT
3. INTERMITTENT OPERATION OF THE VENTILATION SYSTEM ON THE BASIS OF A NEW MODULE "LOGIC" OF A NETPING POWER DISTRIBUTION UNIT
4. THERMOSTAT WITH THE EMERGENCY MODE (PERIODIC SWITCHING A HEATER ON) WHEN A TEMPERATURE SENSOR FAILS WITH SMS-NOTIFICATION

[ENG] 14. [DKSF 70/71.7 IU] Device Support for Custom Notifications

In the device's web-interface, it is possible to create custom notifications (SMS EMail) with an arbitrary text, which can include additional information about the event that caused the notification. The customizable notifications work in parallel with standard SMS and email notifications with the fixed text. Except the sending SMS and email, configured notifications allow you to generate an HTTP GET request designed to integrate NetPing with cloud services. For example, with the automation service Zapier.com or ifttt.com, which allows you to perform a lot of actions receiving relevant notifications. You can learn more about the possibilities provided by Zapier.com at https://zapier.com/zapbook/webhook/, and ifttt.com at https://ifttt.com/discover.

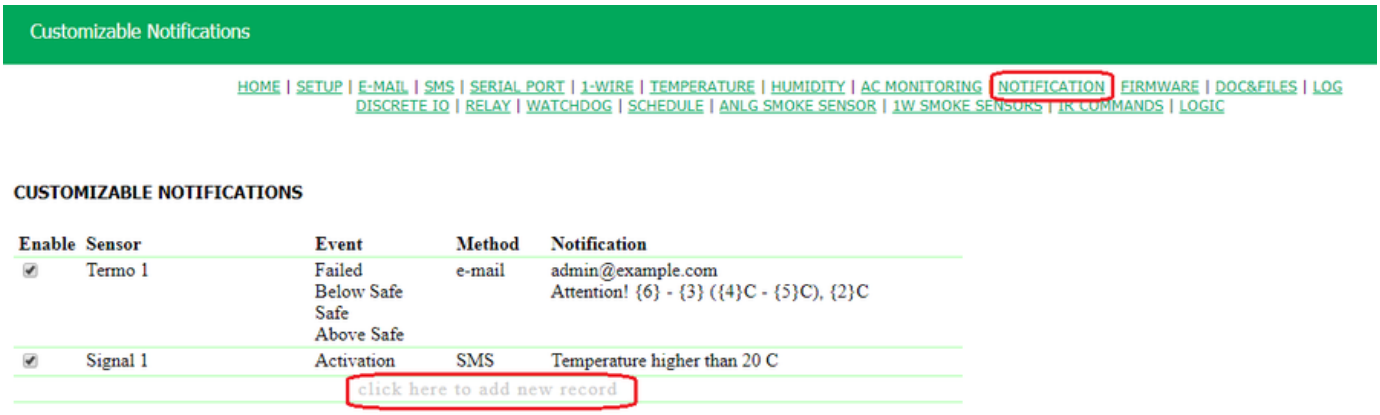
NetPing does not have a client`s HTTP / HTTPS, and to complete the request, it accesses the proprietary cloud service webhook.netping.ru. It is transparent, does not remember and does not accumulate information passed through it. Available for any NetPing device and does not require any prior authorization and configuration.

Remember that requests to the called service come from the Internet, so you need to specify the external address of the service, and not the address of the local network.

NetPing does not have a client`s HTTP/HTTPS, and to complete the request, it accesses the proprietary cloud service webhook.netping .ru. It is transparent, does not remember and does not accumulate information passed through it. Available for any NetPing device and does not require any prior authorization and configuration.

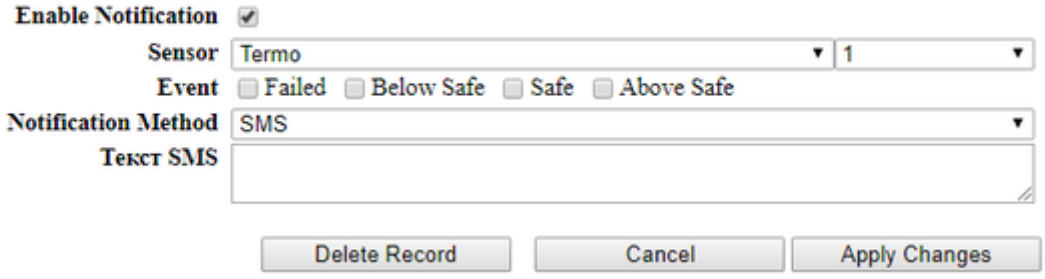
Remember that requests to the called service come from the Internet, so you need to specify the external address of the service, and not the address of the local network.

To create a custom notification, go to the "NOTIFICATIONS" page of the device's web interface and click on the line "click here to add new record " (maximum 16 custom notifications):

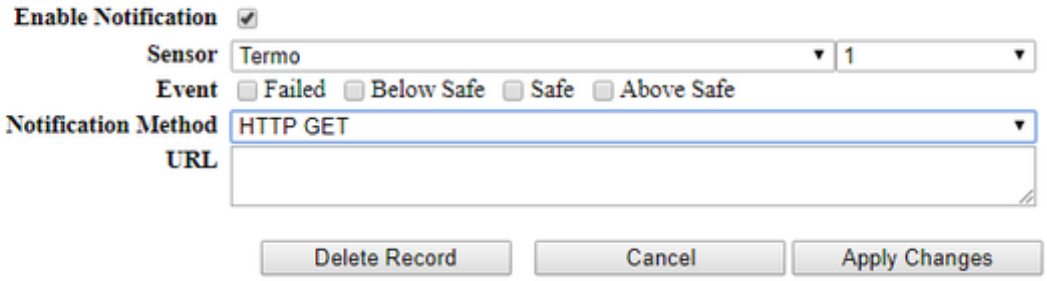


A notification settings window will appear with the following parameters (the screenshot below shows an already customized notification from the temperature sensor on channel 5).

SMS-notification:



HTTP GET-notification:



Email-notification:

The description of sensors and events:

> When you use the channel number “any channel”, it is recommended to use the substitution with the channel number so that the notification contains information about the sensor which caused this notification.

The Sensor	The Event	The Description
Termo 1..8/any channel	failed sensor	Sensor failed of not connected
	below normal	Temperature has dropped below normal
	normal	Temperature has returned to normal
	above normal	The temperature has risen above normal
Humidity (rel. humid) 1..4 / any channel	failed sensor	Sensor failed of not connected
	below normal	Relative humidity has dropped below normal
	normal	Relative humidity has returned to normal
	above normal	Relative humidity has risen above normal
Humidity (temperature) 1..4 / any channel	failed sensor	Sensor failed or not connected
	below normal	The temperature of humidity sensor has dropped below normal
	normal	The temperature of humidity sensor has returned to normal
	above normal	The temperature of humidity sensor has risen above normal
Smoke (analog current in the loop)	normal	Readings are normal
	Alarm!	The sensor detected the smoke
	broken look	broken current in the loop
	Short in the Loop	short in the loop

	failed (broken)	The sensor (current in the loop) failed (deacivated)
Smoke (1W) 1..4 / any channel	normal	Readings are normal
	Alarm!	The sensor detected the smoke
	off	The sensor (current in the loop) is switched off
	failed	The sensor failure
IO line 1..8 / any channel	Log.0	Logic line level switched to 0
	Log.1	Logical line level switched to 1
Relay	off	The relay is off
	on	The relay is on
Watchdog	reset	The "Watchdog" module carried out the reset of the relay
	suspense	The operation of the module is suspensed
	restore	The operaion of the module is restored
Signal 1..4 / any channel	activation	The signal has been activated by logic. So, the rule of logic worked, the output of it is the “Signal 1..4”. More details about the rules of logic and, in particular, the signal can be found in the section [ENG] 13.2. [DKSF 70/71.7 IU] How Can I Use the "LOGIC" module?
Monitoring 220V		
GSM	SMS not a command	Incoming SMS is not a command
	SMS from unknown numbers	An incoming SMS from an unknown number (subject to the setting of white lists of numbers). Read more about setting up white lists in the section: [ENG] 11.2. [DKSF 70/71.7 IU] I Need to Configure the Numbers to Send SMS-Notifications. How Can I do This?

The Description of notification methods:

The method of notification	The description
SMS	Arbitrary SMS notifications. At the beginning of the text of a custom SMS notification, you can specify up to four recipients by specifying their phone numbers in square brackets, separated by commas. Numbers are indicated in the format "Countrycode OperatorcodeCustomernumber". There must be a space between the closing square bracket and the message text. For example, "[+ 79130000001, + 79130000002, + 79130000003, + 79130000004] Houston, we have a problem!. If you do not specify the recipients, i.e. there are no square brackets at the beginning of the text, the SMS will be sent to the numbers specified in the settings on the “SMS” page of the device’s web interface and marked with a “Notif” checkmark.
HTTP GET	The called URL of a third-party service or cloud application. In order to send these notifications, the following scheme is used:Net Ping--SNMP TRAP --> webhook.netping.ru–HTTP(URL) --> destination server. Therefore, the destination server must be accessed via a white address and access to it must be from the outside.
email	The sending of the email notification is carried out to the addresses specified on the "EMAIL" page. In a custom notification it is possible to set the subject of the message in the "Subj" entry field (substitutions are possible) and the text of the email message itself. The recipient cannot be set, messages are sent to the recipients specified on the "EMAIL" page.

You can put the information from the NetPing MIB branch related to the sensor, IO line, or the relay that caused the event in the custom notification text. Format: {N}, where N is the SNMP OID component located in front of the sensor index.

For example, the text of the SMS notification “{6} - {3} ({4}°C - {5}°C), {2}°C" for the temperature sensor includes the following information from the NetPing MIB branch of the tree:

The Substitution	The Complete OID of variable value from NetPing MIB	The name of the variable value from NetPing MIB	The description
{6}	.1.3.6.1.4.1.25728.8800.1.1.6.n	npThermoMemo	The memo of the Temperature Sensor, where n — a number of sensor 1..8.
{3}	.1.3.6.1.4.1.25728.8800.1.1.3.n	npThermoStatus	The Status of the Sensor, where n — a number of sensor.

{4}	.1.3.6.1.4.1.25728.8800.1.1.4.n	npThermoLow	The lower border of the range of normal temperature values, where n is the number of sensor.
{5}	.1.3.6.1.4.1.25728.8800.1.1.5.n	npThermoHigh	The upper border of the range of normal temperature values, where n is the number of sensor.
{2}	.1.3.6.1.4.1.25728.8800.1.1.2.n	npThermoValue	Current temperature at the temperature sensor, where n is the number of sensor.

Additionally.

In the SMS text in the custom event notifications from GSM (SMS is not a command and SMS from an unknown number), the following substitution can be used:

- {11} - sender's mobile number;
- {12} - SMS text encoded 1251;
- {13} - SMS text encoded UTF8.

[ENG] 15. [DKSF 70/71.7 IU] SNMP Protocole Device Support

[ENG] 15.1. [DKSF 70/71.7 IU] Can I Control The Device be Means of SNMP?

The devices UniPing server solution v4/SMS and UniPing server solution v3 support the control via SNMP v1 protocol.

You can read about the SNMP protocole more using these links:

- https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol
- http://www.snmp.com/

OID supported by devices can be found in the MIB files DKSF_70.7.X_ MB.mib, dksf_71.7 .X_ MB.mib on the device description pages in the Downloads" section:

- UniPing server solution v4/SMS
- UniPing server solution v3

The devices support:

- reading OID using Get, Get-Next requests via SNMP v1;
- setting OID values using the Set command via SNMP v1 protocol;
- sending TRAP messages on events.

[ENG] 15.2. [DKSF 70/71.7 IU] Configuration of Sending SNMP TRAP Messages

1. On the “SETUP” page in the SNMP TRAP section, configure the address and UDP port of the main and additional (if necessary) trap receiver.
2. On the sensor pages in the individual notification dialog settings for every sensor, enable the check boxes of events sending Traps.

SNMP TRAP

SNMP Trap Destination #1	192.168.2.42
SNMP Trap Destination #1 Port	162
SNMP Trap Destination #2	
SNMP Trap Destination #2 Port	162

Apply Changes

SNMP TRAP MESSAGES FROM IO-LINE

- Front (Level Change 0->1) — the sending of SNMP TRAP messages when the logic level on the IO line changes from low to high.
- Decay (Level Change 1->0) — the sending of SNMP TRAP messages when the logic level on the IO line changes from high to low.

NOTIFICATIONS FOR IO LINE 2

Event	Log	Syslog	E-mail	SMS	SNMP Trap
Front (Level Change 0 → 1)	☑	☑	☐	☑	☑
Decay (Level Change 1 → 0)	☑	☑	☐	☐	☑
Include in Summary Report	☑	☑	☑	☑	☑
Switch On/Off All Notifications					▬

Logic level	Legend	Color
Logic 1		red
Logic 0		gray

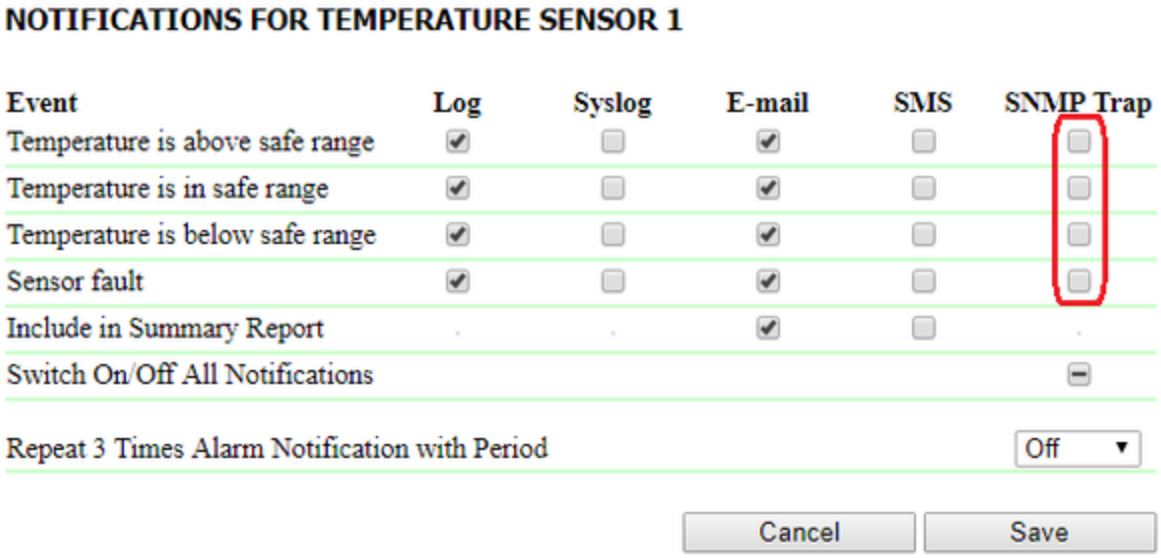
Supression Of Repeating Notifications

Activation of Supression	Disabled
Supression period, s	0

Cancel Save

SNMP TRAP-MESSAGES FROM TEMPERATURE SENSORS

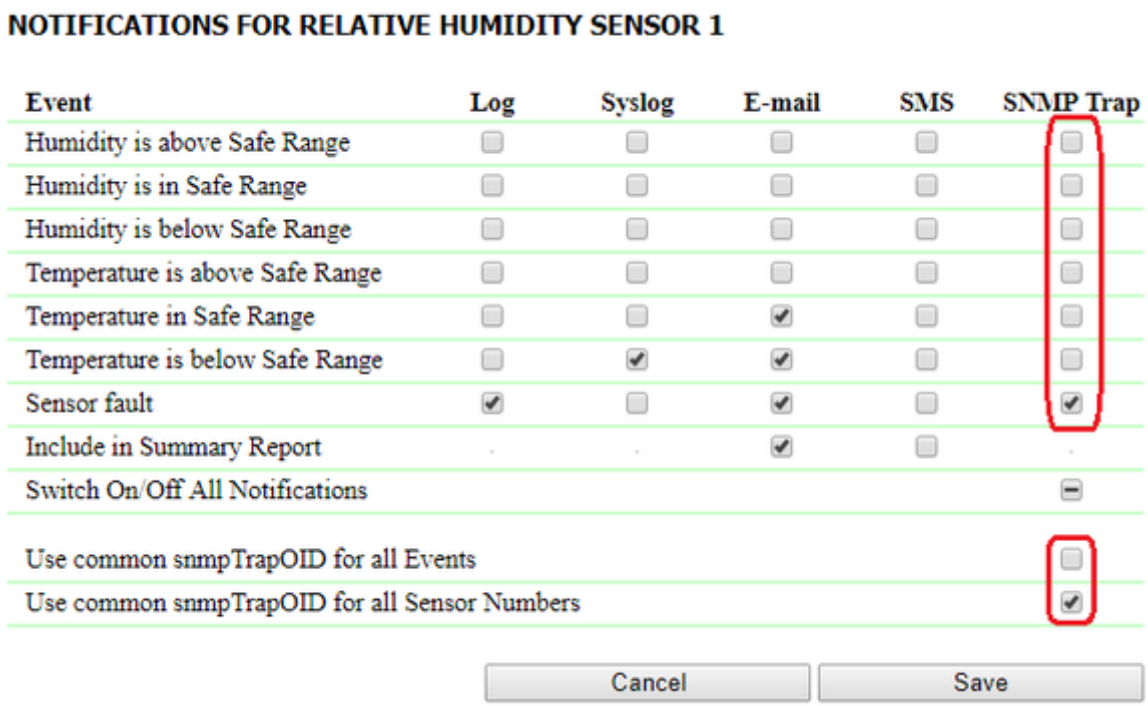
- Temperature is above safe range — the sending of SNMP TRAP messages when the upper limit of the norm specified for the sensor is exceeded.
- Temeprature is in the safe range — the sending of SNMP TRAP messages if the temperature in the sensor returned to the specified range.
- Temperature is below safe range — the sending of SNMP TRAP messages when the temperature drops below the range specified for the sensor.
- Sensor fault — the sending of SNMP TRAP messages when there is a faulty sensor.



SNMP TRAP-MESSAGES FROM HUMIDITY SENSORS

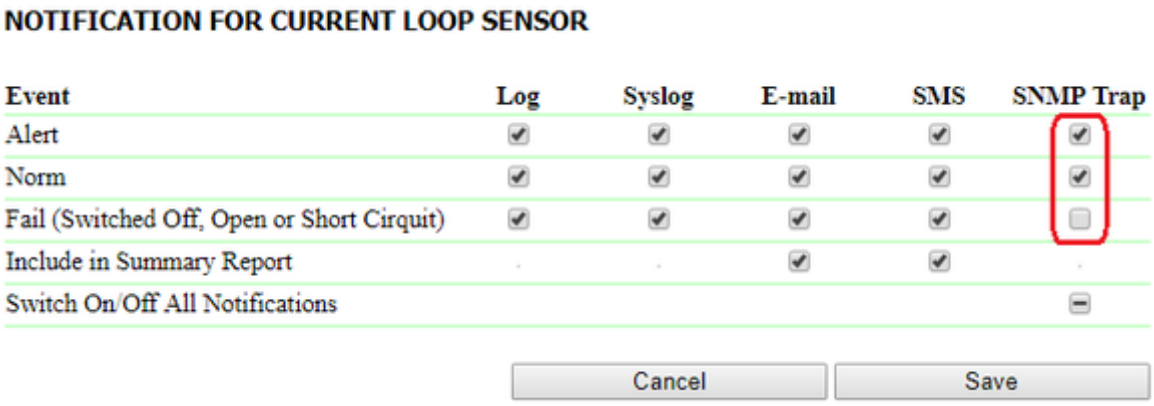
- Humidity is above Save Range — the sending of SNMP TRAP messages when the relative humidity exceeds the upper limit of the normal range specified for the sensor.
- Humidity is in Safe Range — the sending of SNMP TRAP messages if the relative humidity on the humidity sensor has returned to the specified normal humidity range.
- Humidity is below Safe Range — the sending of SNMP TRAP messages when the relative humidity drops below the lower limit of the normal humidity range specified for the sensor.
- Temperature is above Safe Ramge — the sending of SNMP TRAP messages when the humidity sensor temperature exceeds the upper limit of the normal temperature range specified for this sensor.
- Temperature is in Safe Range — the sending of SNMP TRAP messages if the temperature of the humidity sensor on the sensor has returned to the specified normal temperature range.
- Temperature is below Safe Range — the sending of SNMP TRAP messages when the temperature of the humidity sensor drops below the lower limit of the normal temperature range specified for the sensor.
- Sensor fault — the sending of SNMP TRAP messages when the sensor fails. If the humidity sensor fails, two SNMP Trap messages arrive: one is for humidity and the other is for temperature.
- Use common snmpTrapOID for all Events and Use common snmpTrapOID for all Sensor Numbers — the sending of SNMP TRAP messages for all events from all humidity sensors with a single snmpTrapOID message or messages that allow you to split events and numbers of humidity sensors into different snmpTrapOID messages, up to completely individual ones. This allows you to receive

individual SNMP Trap messages for processing them in control systems, for example, “dampening of the humidity sensor 3” or “humidity sensor 2 is normal”.



SNMP TRAP- MESSAGES FROM CURRENT LOOP SENSOR

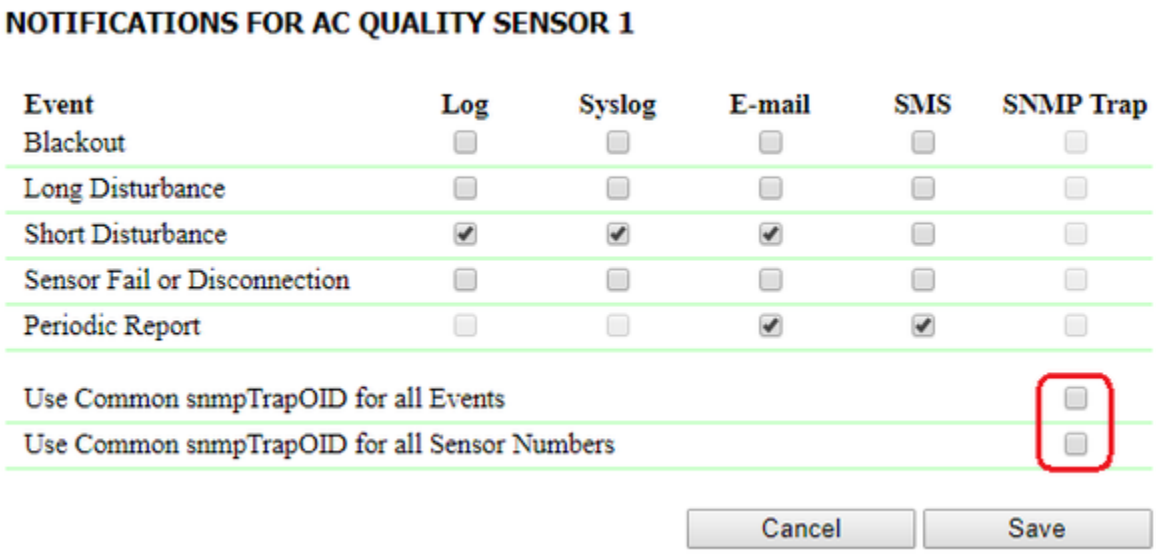
- Alert — the sending of SNMP TRAP messages when the current loop readings reached alert conditions.
- Norm — the sending of SNMP TRAP messages if the current loop parameters have returned to the specified normal range.
- Fail (Switched Off, Open or Short Cirquit)— the sending of SNMP TRAP messages in case of a disconnection, failure, break of a loop or short circuit of a current loop.



SNMP TRAP MESSAGES FROM AC QUALITY SENSORS

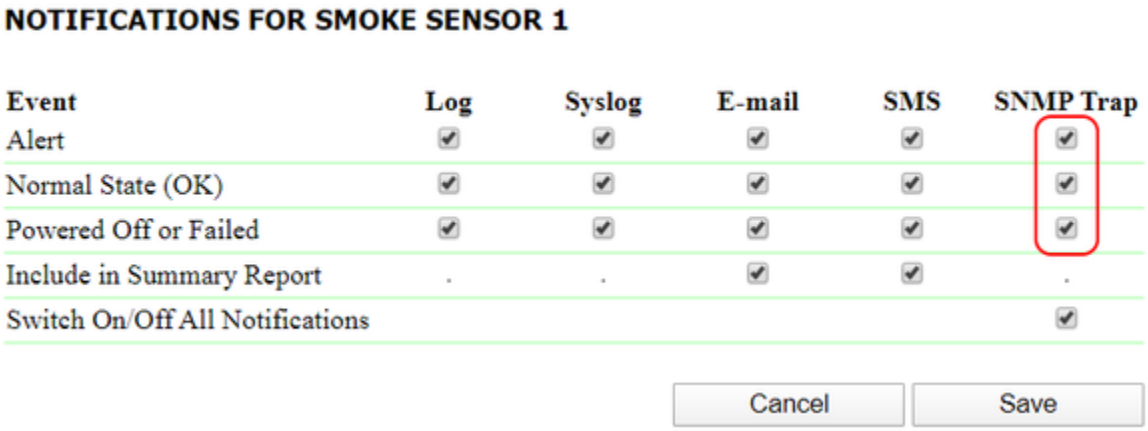
- Use common snmpTrapOID for all the events and Use common snmpTrapOID for all the channels — the sending of SNMP TRAP messages for all the events from all 220V voltage sensors with a single message or messages that allow you to split events and numbers

of 220V voltage sensors into different messages, up to completely individual ones. This allows you to receive individual SNMP Trap messages for processing them in monitoring systems.



SNMP TRAP MESSAGES FROM 1-WIRE SMOKE SENSORS

- Alert — the sending of SNMP TRAP messages if the smoke detector has detected smoke.
- Norm — the sending of SNMP TRAP messages if the smoke detector has returned to normal state
- Fail (Swtched Off, Open ot Short Cirquit) — the sending of SNMP TRAP messages in case of connection loss or when the current loop is disconnected.



[ENG] 15.3. [DKSF 70/71.7 IU] Which OID are Supported By the Device?

You can see the description of OID supported by the device.

For convenient perception of the information it is recommended to use any convenient MIB browser, where you can download the MIB file for the current firmware and get the data from the table below in the form of a tree.

OID	Name	Type	Access	Description
RFC1213				
.1.3.6.1.2.1.1.1.0	sysDescr	OctetString	READ	Text description of the device
.1.3.6.1.2.1.1.2.0	sysObjectID	OID	READ	Number of the branch with the device`s parameters always «.1.3.6.1.4.1.25728»
.1.3.6.1.2.1.1.3.0	sysUpTime	TimeTicks	READ	Operating time since last switching on or reboot
.1.3.6.1.2.1.1.4.0	sysContact	OctetString	READ/WRITE	Contact information, as a rule, an email of the administrator
.1.3.6.1.2.1.1.5.0	sysName	OctetString	READ/WRITE	Domain name of the device
.1.3.6.1.2.1.1.6.0	sysLocation	OctetString		Location of the device
.1.3.6.1.2.1.1.7.0	sysServices	Integer	READ	The binary representation of this OID is a set of supported services. Always “72”, the device acts as the final host
.1.3.6.1.2.1.2.1.0	ifNumber	Integer	READ	Number of device network interfaces
.1.3.6.1.2.1.2.2.1.1.1	ifIndex	Integer	READ	An interface index is a unique identification number connected with a physical or logic interface. For most ifIndex software, this is the name of the interface.
.1.3.6.1.2.1.2.2.1.2	ifDescr	OctetString	READ	A line including the interface information. The line includes the manufacturer’s name, device model and hardware interface version
.1.3.6.1.2.1.2.2.1.3.1	ifType	Integer	READ	A type of the device network interface
.1.3.6.1.2.1.2.2.1.4.1	ifMtu	Integer	READ	Packet size over the network interface. Always «1514»
.1.3.6.1.2.1.2.2.1.5.1	ifSpeed	Integer	READ	The speed of the network interface. Always«100000000»
.1.3.6.1.2.1.2.2.1.6.1	ifPhysAddress	OctetString	READ	MAC-address of the device
NetPing MIB				
.1.3.6.1.4.1.25728.90.1.0	npTrapEmailTo	OctetString	READ	A variable value in the set of traps. Email where messages are forwarded to using the NetPing message forwarding service
.1.3.6.1.4.1.25728.911.1.0	npSoftReboot	Integer	READ/WRITE	Soft reset of the device when recording the value "1"
.1.3.6.1.4.1.25728.911.2.0	npResetStack	Integer	READ/WRITE	Soft reset of the network interface when recording the value "1"
.1.3.6.1.4.1.25728.911.3.0	npForceReboot	Integer	READ/WRITE	Immediate forced reboot of the device when recording the value “1” (processor reset when turning on the power)
.1.3.6.1.4.1.25728.3800.1.1.0	npGsmFailed	Integer	READ	The status of a built-in GSM modem (for the device UniPing server solution v4/SMS with a built-in GSM modem): 0 — OK 1 — Failed (no connection) 2 — FatalError (unrecoverable error, the modem is locked)
.1.3.6.1.4.1.25728.3800.1.2.0	npGsmRegistration	Integer	READ	GSM network connection status (for device UniPing server solution v4/SMS with a built-in GSM modem): 0 — Impossible 1 — HomeNetwork 2 — Searching 3 — Denied 4 — Unknown 5 — Roaming 255 — InfoUpdate
.1.3.6.1.4.1.25728.3800.1.3.0	npGsmStrength	Integer	READ	GSM signal strength (for the deviced UniPing server solution v4/SMS with a built-in GSM modem): 0…31 = 0% … 100% 99 — unknown 255 — updating info

.1.3.6.1.4.1.25728.3800.1.9.0	npGsmSendSMSUtf8	DisplayString	READ/WRITE	The sending an arbitrary SMS message in UTF-8 encoding (for the device UniPing server solution v4/SMS with a built-in GSM modem). Format: [phone_number,phone_number,...] Message where: phone_number — the recipient number in square brackets, indicated in the format: CountryCodeOperatorCodeCustomerNumber, e.g., +79998887766. Message — message text (written with a space from the recipient number). Only Latin letters are allowed in the SMS text. You can send SMS to several (up to four) numbers, indicating them in square brackets, separated by commas, without spaces. If there are no square brackets with the addressee number at the beginning of the message, the message is sent to the addressees indicated on the “SMS” page of the device’s web interface.
.1.3.6.1.4.1.25728.3800.1.10.0	npGsmSendSMSWin1251	DisplayString	READ/WRITE	Sending an arbitrary SMS message encoded Windows-1251 (for devices UniPing server solution v4/SMS with a built-in GSM modem). Format: [phone_number,phone_number,...] Message where: phone_number — recipient number in square brackets, indicated in the format: CountryCodeOperatorCodeCustomerNumber, e.g., +79998887766 Message — message text (written with a space from the recipient number). You can send SMS to several (up to four) numbers, indicating them in square brackets, separated by commas, without spaces. If there are no square brackets with the recipient number at the beginning of the message, the message is sent to the recipients indicated on the “SMS” page of the device’s web interface.
A built-in Relay				
.1.3.6.1.4.1.25728.5500.5.1.1.1	npRelayN.1	Integer	READ	The number of a relay
.1.3.6.1.4.1.25728.5500.5.1.2.1	npRelayMode.1	Integer	READ/WRITE	Relay Mode These modes are available: 0 — Off 1 — On -1 — Switching between off and on
.1.3.6.1.4.1.25728.5500.5.1.3.1	npRelayStartReset.1	Integer	READ/WRITE	OID for forced short-time relay shutdown. Write the number “1” to disable the channel for 15 seconds
.1.3.6.1.4.1.25728.5500.5.1.6.1	npRelayMemo.1	DisplayString	READ	The Memo of the relay
.1.3.6.1.4.1.25728.5500.5.1.14	npRelayFlip.1	Integer	READ/WRITE	OID to switch between off and on. Write “-1” to switch.
.1.3.6.1.4.1.25728.5500.5.1.15.1	npRelayState.1	Integer	READ	The current status of the relay: 0 — The relay is off 1 — The relay is on
IRC-TR v2				
.1.3.6.1.4.1.25728.7900.1.1.0	npIrPlayCmd	Integer	READ/WRITE	In order to send the IR command, write the number of the IR command
.1.3.6.1.4.1.25728.7900.1.2.0	npIrReset	Integer	READ/WRITE	To reset the IR transceiver write "1". After the reset indicate the IR command and check the IP status

.1.3.6.1.4.1.25728.7900.1.3.0	npIrStatus	Integer	READ	The status of the IR transceiver The next statuses are available: commandCompleted (0) — the command is completed; the command which does not demand any process of its operation; protocolError (1) — the wrong code of the command or the command is not accepted commandAccepted (2) — the command is accepted, the execution has been lanched. After the completion of the command the status does not change because there will not be possible to have faults any more. Before sending the next command, you need to wait about 0.5 seconds; errorUnknown (16) — unknown error; errorBadNumber (17) — the wrong parameter of the command; errorEmptyRecord (18) —an attempt to play an empty record; errorFlashChip (19) —the fault or shut down the flash chip errorTimeout (20) — no response from IRC-TR v2 extension module; errorExtBusBusy (21) — the external i2c bus is busy, it is impossible to connect with the IRC-TR v2 IR extension module (for example, with a bus short circuit)
1-Wire Smoke Sensor				
.1.3.6.1.4.1.25728.8200.1.1.1.n	npSmokeSensorN.n	Integer	READ	The index of the 1-Wire smoke sensor, where n — a number of a sensor
.1.3.6.1.4.1.25728.8200.1.1.2.n	npSmokeStatus.n	Integer	READ	The status of the 1-Wire smoke sensor, where n —a number of a sensor: 0 — Normal 1 — Alert 4 — StopOut 5 — Failure
.1.3.6.1.4.1.25728.8200.1.1.3.n	npSmokePower.n	Integer	READ/WRITE	Power control of the 1-Wire smoke sensor, where n — number of the sensor: 0 — Off 1 — On
.1.3.6.1.4.1.25728.8200.1.1.4.n	npSmokeReset.n	Integer	READ/WRITE	OID for forced short-term reset of the 1-Wire smoke sensor, where n — number of the sensor. Write the number “1” to reset the channel for 10 seconds
.1.3.6.1.4.1.25728.8200.1.1.6.n	npSmokeMemo.n	DisplayString	READ	The memo of the 1-Wire smoke sensor, where n - number of the sensor
Analog Smoke Sensor (Current loop)				
.1.3.6.1.4.1.25728.8300.1.1.1.1	npCurLoopN.1	Integer	READ	The index of the smoke sensor (Current Loop).
.1.3.6.1.4.1.25728.8300.1.1.2.1	npCurLoopStatus.1	Integer	READ	The status of the loop: 0 — Normal 1 — Alert 2 — Brocken Loop 3 — Short in the current loop 4 — Power is off
.1.3.6.1.4.1.25728.8300.1.1.3.1	npCurLoopI.1	Integer	READ	mA Current in the smoke sensor circuit, mA
.1.3.6.1.4.1.25728.8300.1.1.4.1	npCurLoopV.1	Integer	READ	Voltage drop in the smoke sensor circuit, mV
.1.3.6.1.4.1.25728.8300.1.1.5.1	npCurLoopR.1	Integer	READ	Resistance in the smoke sensor circuit, Ohm
.1.3.6.1.4.1.25728.8300.1.1.7.1	npCurLoopPower.1	Integer	READ/WRITE	Smoke sensor supply voltage control: 0 — Off 1 — On 2 — Reset of the current sensor power
1-W Relative Humidity sensor				

.1.3.6.1.4.1.25728.8400.1.1.1.n	npRelHumN.n	Integer	READ	The index of the humidity sensor, where n — number of a sensor
.1.3.6.1.4.1.25728.8400.1.1.2.n	npRelHumValue.n	Integer	READ	The value of a relative humidity, %, where n — number of a sensor
.1.3.6.1.4.1.25728.8400.1.1.3.n	npRelHumStatus.n	Integer	READ	The status of a relative humidity, where n - number of a sensor: 0 — failed or not connected sensor 1 — below normal 2 — normal 3 — above normal
.1.3.6.1.4.1.25728.8400.1.1.4.n	npRelHumTempValue.n	Integer	READ	Temperature value, °C, where n — number of the sensor
.1.3.6.1.4.1.25728.8400.1.1.5.n	npRelHumTempStatus.n	Integer	READ	Temperature status, °C, where n — number of the sensor
.1.3.6.1.4.1.25728.8400.1.1.6.n	npRelHumMemo.n	DisplayString	READ	The memo of the humidity sensor. where n - number of the sensor
.1.3.6.1.4.1.25728.8400.1.1.7.n	npRelHumSafeRangeHigh.n	Integer	READ	The upper limit of the range of normal values of relative humidity,%, where n is number of the sensor
.1.3.6.1.4.1.25728.8400.1.1.8.n	npRelHumSafeRangeLow.n	Integer	READ	The lower limit of the range of normal values of relative humidity,%, where n - number of the sensor
.1.3.6.1.4.1.25728.8400.1.1.9.n	npRelHumTempSafeRangeHigh.n	Integer	READ	The upper limit of the range of normal temperature values, ° C, where n - number of the sensor
.1.3.6.1.4.1.25728.8400.1.1.10.n	npRelHumTempSafeRangeLow.n	Integer	READ	The lower limit of the range of normal temperature values, ° C, where n is the sensor number
1-W Temperature sensor				
.1.3.6.1.4.1.25728.8800.1.1.1.n	npThermoSensorN.n	Integer	READ	The temperature sensor identifier, number from 1 to 8 inclusive
.1.3.6.1.4.1.25728.8800.1.1.2.n	npThermoValue.n	Integer	READ	The current temperature in the temperature sensor°C, where n —number of the sensor
.1.3.6.1.4.1.25728.8800.1.1.3.n	npThermoStatus.n	Integer	READ	The status of the temperature sensor, where n — number of the sensor: 0 — failed or not connected sensor 1 — below normal 2 — normal 3 — above normal
.1.3.6.1.4.1.25728.8800.1.1.4.n	npThermoLow.n	Integer	READ	The lower limit of normal temperature range, °C, where n — number of the sensor.
.1.3.6.1.4.1.25728.8800.1.1.5.n	npThermoHigh.n	Integer	READ	The upper limit of normal temperature range, °C, where n - number of the sensor.
.1.3.6.1.4.1.25728.8800.1.1.6.n	npThermoMemo.n	DisplayString	READ	The memo of the temperature sensor, where n — number of the sensor.
.1.3.6.1.4.1.25728.8800.1.1.7.n	npThermoValuePrecise	FixedPoint1000 (Integer)	READ	The current temperature in the temperature sensor with an accuracy of three decimal figures, ° C, where n - number of the sensor.
IO Lines				
.1.3.6.1.4.1.25728.8900.1.1.1.n	npIoLineN.n	Integer	READ	The IO line number, where n - the line number, a number from 1 to 8 inclusive
.1.3.6.1.4.1.25728.8900.1.1.2.n	npIoLevelIn.n	Integer	READ	The current status of the IO line, where n - the line number, a number from 1 to 8 inclusive
.1.3.6.1.4.1.25728.8900.1.1.3.n	npIoLevelOut.n	Integer	READ/WRITE	IO-line control in the "output" mode, where n is the line number, a number from 1 to 8 inclusive: 0 - logic zero 1 - logic unit This OID also allows you to switch the state of the IO line from state “0” to state “1” and vice versa. To change the state of the IO line write "-1"
.1.3.6.1.4.1.25728.8900.1.1.6.n	npIoMemo.n	DisplayString	READ	The memo the short description for the IO line), where n - the line number, a number from 1 to 8 inclusive
.1.3.6.1.4.1.25728.8900.1.1.9.n	npIoPulseCounter.n	Counter32	READ/WRITE	The counter of the pulses on the IO line, where n - the line number, a number from 1 to 8 inclusive It is counted from the positive edge of the pulse after filtering short pulses. To force zero, write “0”. Also, resets when power is turned off

.1.3.6.1.4.1.25728.8900.1.1.12.n	npIoSinglePulseDuration.n	Integer	READ/WRITE	The duration of one pulse at the output of the IO line (valid values from 100 ms to 25 500 ms, in increments of 100 ms), where n - the line number, a number from 1 to 8 inclusive
.1.3.6.1.4.1.25728.8900.1.1.13.n	npIoSinglePulseStart.n	Integer	READ/WRITE	To send a single pulse to the output of the IO line, write “1”. The pulse duration is taken from the variable value npIoSinglePulseDuration.n, where n - the line number, a number from 1 to 8 inclusive

[ENG] 15.4. [DKSF 70/71.7 IU] SNMP TRAP Support

A formal description of SNMP TRAP messages can be found in the DKSF_70.7.x_ MB.mib,DKSF_71.7.x_ MB.mib files attached to the firmware of UniPing server solution v4/SMS and UniPing server solution v3. They can be downloaded on the pages from the website with a description of the devices in the "DOCS&FILES" section. An SNMP TRAP message is sent in SNMP v1 / v2c format, while the description in MIB files is in SNMP v2c format.

The unique mutual correspondence of the identification of SNMP TRAP messages for v1 and v2c is described in RFC3584 «Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework».

The programs for processing SNMP notifications, as a rule, carry out the convertation between two formats easily.

To send SNMP TRAP messages you must:

- to specify the address and the port for sending SNMP TRAP on the page "SETUP" of the device`s web interface.
- to allow the sending of SNMP TRAP messages by enabling the corresponding check boxes in thhe standard dialogues of the notifications of the corresponding sensors. You san see more details about it in the section [ENG] 15.2. [DKSF 70/71.7 IU] Configuration of Sending SNMP TRAP Messages

SNMP TRAP WHILE CHANGING THE LEVEL ON THE IO LINE IN THE MODE

Identification of npIoTrap

SNMP v1 enterprise	.1.3.6.1.4.1.25728.8900.2
SNMP v1 generic-trap	enterpriseSpecific(6)
SNMP v1 specific-trap	1
SNMP v2 snmpTrapOID	.1.3.6.1.4.1.25728.8900.2.0.1

Variable values in the set of npIoTrap (varbind list)

OID	The type of the data	The description
.1.3.6.1.4.1.25728.8900.2.1.0	Integer	The IO-Line number (starting with "1") the change of which has made the sending of a TRAP message
.1.3.6.1.4.1.25728.8900.2.2.0	Integer	Logic level values on the IO line («0» ot «1»)
.1.3.6.1.4.1.25728.8900.2.6.0	Display String	The memo (the text description of the line, encoding win1251)
.1.3.6.1.4.1.25728.8900.2.7.0	Display String	The decoding of the logic level. The description of a numerical value of the logic level of the IO line which is understandable for perception

SNMP TRAP WHILE CHANGING THE STATUS OF THE TEMPERATURE SENSOR

Identification of npThermoTrap

SNMP v1 enterprise	.1.3.6.1.4.1.25728.8800.2
SNMP v1 generic-trap	enterpriseSpecific(6)
SNMP v1 specific-trap	1
SNMP v2 snmpTrapOID	.1.3.6.1.4.1.25728.8800.2.0.1

Variable values in the set of npThermoTrap (varbind list)

OID	The type of the data	The description
.1.3.6.1.4.1.25728.8800.2.1.0	Integer	The sensor number (1...8), the change of which has made the sending of a TRAP message
.1.3.6.1.4.1.25728.8800.2.2.0	Integer	The current value of the temperature, °C

.1.3.6.1.4.1.25728.8800.2.3.0	Integer	The status of the temperature sensor: 0 — failed or not connected sensor 1 — below normal 2 — normal 3 — above normal
.1.3.6.1.4.1.25728.8800.2.4.0	Integer	The lower limit of normal, °C
.1.3.6.1.4.1.25728.8800.2.5.0	Integer	The upper limit of normal, °C
.1.3.6.1.4.1.25728.8800.2.6.0	Display String	The memo (text description of the installation location of the temperature sensor, encoding win1251)

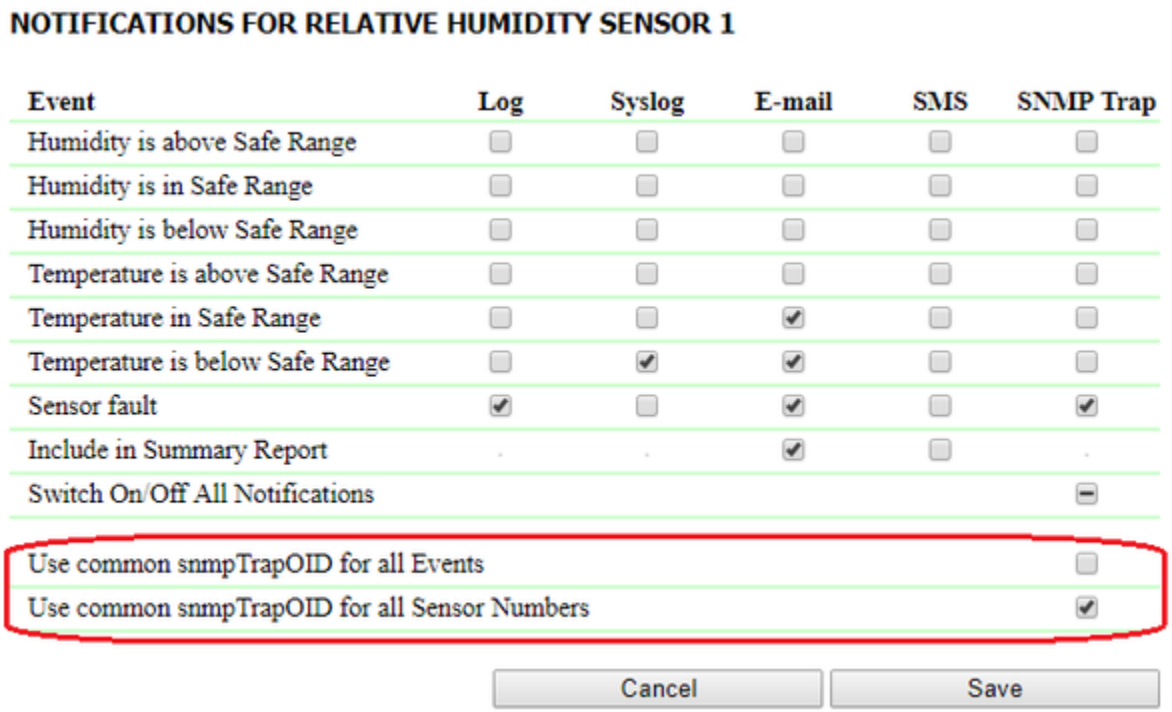
SNMP TRAP WHILE CHANGING THE STATUS OF THE HUMIDITY SENSOR

Identification of npRelHumTrap

General view of SNMP TRAP from the humidity sensor about the humidity readings	.1.3.6.1.4.1.25728.8400.6.127.99

snmpTrapOID npRelHumTrap (SNMP TRAP messages while changing the status of humidity)

You can enable the decryption of the type of events and channel number by the corresponding check boxes in the notification settings dialog.



OID	The description
.1.3.6.1.4.1.25728.8400.6.100.n	The fault of the humidity sensor, where n - number of the sensor 1...8
.1.3.6.1.4.1.25728.8400.6.101.n	The readings of the relative humidity below Safe Range, where n - number of the sensor
.1.3.6.1.4.1.25728.8400.6.102.n	The readings of the relative humidity is in Safe Range, where n - number of the sensor
.1.3.6.1.4.1.25728.8400.6.103.n	The readings of the relative humidity is above Safe Range, where n - number of the sensor
.1.3.6.1.4.1.25728.8400.6.127.n	Common snmpTrapOID for all the events, where n - number of the sensor
.1.3.6.1.4.1.25728.8400.6.m.99	Common snmpTrapOID for all the channels, where m — a code of the event (100, 101, 102, 103)

.1.3.6.1.4.1.25728.8400.6.127.99	Common snmpTrapOID for all the events and channels

Identification of npRelHumTrapTemp

General view SNMP TRAP from the humidity sensor about the temeprature readings	.1.3.6.1.4.1.25728.8400.7.127.99

snmpTrapOID npRelHumTrapTemp (SNMP TRAP messages while changing the status of temperature)

You can enable the decryption of the type of events and channel number by the corresponding check boxes in the notification settings dialog.

OID	The description
.1.3.6.1.4.1.25728.8400.7.100.n	The fault of the temperature sensor, where n - number of the sensor 1...8
.1.3.6.1.4.1.25728.8400.7.101.n	The readings of the temperature sensor below Safe Range, where n - number of the sensor
.1.3.6.1.4.1.25728.8400.7.102.n	The readings of the temperature of the humidity sensor is in Safe Range, where n - number of the sensor
.1.3.6.1.4.1.25728.8400.7.103.n	The reading of the temperature of the humidity sensor is above Safe Range, where n - number of the sensor
.1.3.6.1.4.1.25728.8400.7.127.n	Common snmpTrapOID for all the events, where n — number of the sensor
.1.3.6.1.4.1.25728.8400.7.m.99	Common snmpTrapOID for all the channels, where m — the code of the event (100, 101, 102, 103)
.1.3.6.1.4.1.25728.8400.7.127.99	Common snmpTrapOID for all the events and channels

Variable values in the set of npRelHumTrapData (varbind list)

OID	The type of the data	The description
.1.3.6.1.4.1.25728.8400.3.1.0	Integer	The number of the sensor (1...4), the change of which has made the sending of a TRAP message
.1.3.6.1.4.1.25728.8400.3.2.0	Integer	The current value of the relative humidity, %, or temperature °C
.1.3.6.1.4.1.25728.8400.3.4.0	Integer	The status of the relative humidity and temperature
.1.3.6.1.4.1.25728.8400.3.6.0	Display String	The memo (text description of the installation location of the humidity sensor, encoding win1251)
.1.3.6.1.4.1.25728.8400.3.7.0	Integer	The upper limit of the range of relative humidity and temperature values
.1.3.6.1.4.1.25728.8400.3.8.0	Integer	The lower limit of the range of relative humidity and temperature values

SNMP TRAP WHILE CHANGING THE STATUS OF ANALOG SMOKE SENSOR

IDENTIFICATION OF NPCURLOOPTRAP

SNMP v1 enterprise	.1.3.6.1.4.1.25728.8300.2
SNMP v1 generic-trap	enterpriseSpecific(6)
SNMP v1 specific-trap	1
SNMP v2 snmpTrapOID	.1.3.6.1.4.1.25728.8300.2.0.1

Variable values in the set of npCurLoopTrap (varbind list)

OID	The type of the data	The description

.1.3.6.1.4.1.25728.8300.2.1.0	Integer	The number of the current loop, the change of which has made the sending of a TRAP message (in the current device the value is always "1")
.1.3.6.1.4.1.25728.8300.2.2.0	Integer	The status of the loop: 0 — Normal 1 — Alert 2 — Brocken Loop 3 — Short in the current loop 4 — Power is off
.1.3.6.1.4.1.25728.8300.2.3.0	Integer	Current in the Loop, mA
.1.3.6.1.4.1.25728.8300.2.4.0	Integer	Voltage Drop on the Loop, mV
.1.3.6.1.4.1.25728.8300.2.5.0	Integer	Loop Resistance, Ohm
.1.3.6.1.4.1.25728.8300.2.7.0	Integer	Loop Power: 0 — Off 1 — On

SNMP TRAP WHILE CHANGING THE STATUS OF 1-WIRE SMOKE SENSOR

Identification of npSmokeTraps

SNMP v1 enterprise	.1.3.6.1.4.1.25728.8200.2
SNMP v1 generic-trap	enterpriseSpecific(6)
SNMP v1 specific-trap	1
SNMP v2 snmpTrapOID	.1.3.6.1.4.1.25728.8200.2.0.1

Variable values in the set of npSmokeTraps (varbind list)

OID	The type of the data	The description
.1.3.6.1.4.1.25728.8200.2.1.0	Integer	The number of the 1-wire smoke sensor (1..4), the change of which has made the sending of a TRAP message
.1.3.6.1.4.1.25728.8200.2.2.0	Integer	The status of the 1-Wire smoke sensor 0 — Normal 1 — Alert 4 — StopOut 5 — Failure
.1.3.6.1.4.1.25728.8300.2.6.0	Display String	The memo (text description of the installation location of the 1-wire smoke sensor sensor, encoding win1251)

SNMP TRAP ABOUT THE STATUS OF THE GSM MODEM

> The information is for the devices UniPing server solution v4/SMS with a built-in GSM modem.

Identification of npGsmTraps

SNMP v1 enterprise	.1.3.6.1.4.1.25728.3800.2
SNMP v1 generic-trap	enterpriseSpecific(6)

SNMP v1 specific-trap	1
SNMP v2 SNMPTrapOID	.1.3.6.1.4.1.25728.3800.2.0.1

Variable values of the set of npGsmTraps (varbind list)

OID	The type of the data	The description
.1.3.6.1.4.1.25728.3800.1.1.0	Integer	The status of a built-in GSM modem 0 — OK 1 — Failed (no connection) 2 — FatalError (unrecoverable error, the modem is locked)
.1.3.6.1.4.1.25728.3800.1.2.0	Integer	GSM network connection status: 0 — Impossible 1 — HomeNetwork 2 — Searching 3 — Denied 4 — Unknown 5 — Roaming 255 — InfoUpdate
.1.3.6.1.4.1.25728.3800.1.3.0	Integer	GSM signal strength: 0…31 = 0% … 100% 99 — Unknown 255 — Updating info

Identification of npGsmTrapUnparsedSms

SNMP v1 enterprise	.1.3.6.1.4.1.25728.3800.2
SNMP v1 generic-trap	enterpriseSpecific(6)
SNMP v1 specific-trap	1
SNMP v2 SNMPTrapOID	.1.3.6.1.4.1.25728.3800.2.0.2

Variable values in the set of npGsmTrapUnparsedSms (varbind list)

OID	The type of the data	The description
.1.3.6.1.4.1.25728.3800.1.11.0	DisplayString	The phone number of incoming unidentified SMS
.1.3.6.1.4.1.25728.3800.1.12.0	DisplayString	The text of incoming unidentified SMS, encoded Windows-1251
.1.3.6.1.4.1.25728.3800.1.13.0	DisplayString	The text of incoming unidentified SMS, encoded UTF-8

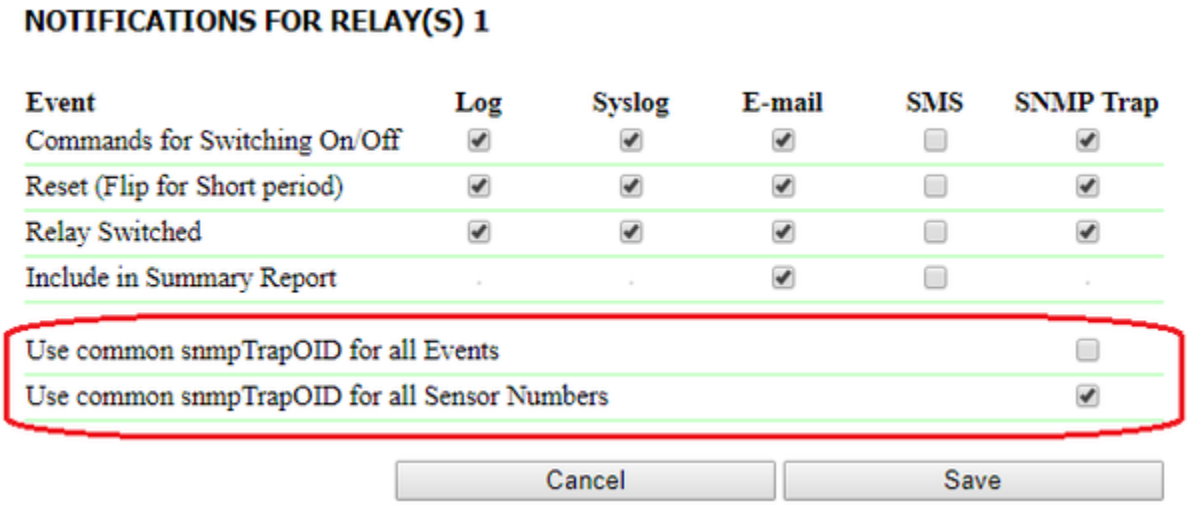
SNMP TRAP WHILE CHANGING THE STATUS OF A BUILT-IN RELAY

Identification of npRelayTrap

General view of SNMP TRAP from a built-in relay	.1.3.6.1.4.1.25728.5500.6

snmpTrapOID npRelayTrap (SNMP TRAP messages while changing the relay status)

You can enable the decryption of the type of events and channel number by the corresponding check boxes in the notification settings dialog.



OID	The description
.1.3.6.1.4.1.25728.5500.6.100.n	Relay is Switched Off, where n - number of the relay (always 1)
.1.3.6.1.4.1.25728.5500.6.101.n	Relay is Switched On, where n - number of the relay (always 1)
.1.3.6.1.4.1.25728.5500.6.102.n	Relay has received a command for the status changing (for Switching On/Off), where n - number of the relay (always 1)
.1.3.6.1.4.1.25728.5500.6.103.n	Th reset has been started, where n - number of the relay (always 1)
.1.3.6.1.4.1.25728.5500.6.127.n	Common snmpTrapOID for all the events, where n - number of the relay (always 1)
.1.3.6.1.4.1.25728.5500.6.m.99	Common snmpTrapOIDfor all the channels, where n - the code of the event (100, 101, 102, 103)
.1.3.6.1.4.1.25728.5500.6.127.99	Common snmpTrapOID for all the events and channels

Variable values in the set of npRelayTrap (varbind list)

OID	The type of the data	The description
.1.3.6.1.4.1.25728.5500.3.1.0	Integer	The number of the relay, where n - number of the relay (always 1)
.1.3.6.1.4.1.25728.5500.3.2.0	Integer	Relay Status, off (1) или off (0), not considering the Switch command of the relay
.1.3.6.1.4.1.25728.5500.3.6.0	DisplayString	Memo
.1.3.6.1.4.1.25728.5500.3.15.0	Integer	The current status of the relay at the time of sending the Trap message, on (1) or off (0)
.1.3.6.1.4.1.25728.5500.3.18.0	Integer	The relay switch command source: : -1 — unknown 1 — web interface 2 — SNMP 3 — SMS 4 — HTTP API 5 — Watchdog 6 — Schedule 7 — Logic
.1.3.6.1.4.1.25728.5500.3.19.0	DisplayString	The time of the events

[ENG] 16. [DKSF 70/71.7 IU] The Support via the device NetPing HTTP API

NetPing HTTP API is implemented in the internal Web server of the device. You can take readings of sensors, control IO lines, control relays, etc. by sending HTTP requests to the NetPing device.

[ENG] 16.1. [DKSF 70/71.7 IU] The IO Lines Control

The interface of the URL-encoded commands in the device can be used to integrate with web-applications without using the SNMP protocole. The IO lines control is available via the interface of the URL-encoded com

THE REQUEST ABOUT A CERTAIN IO LINE

```
http://192.168.0.100/io.cgi?ioN
```

where:

N — the line number, indicated after ?io.

RETURN VALUES

Error (wrong request format or wrong number of the IO line):

```
io_result('error')
```

Successful completion of the command

```
io_result('ok', -1, 1, 339)
```

The first argument: always 'ok' (upon request error - 'error').

The second argument: always «-1», for expanding the API in the future.

The third argument: the current instantaneous status of the IO line, including the reset status.

The forth argument: the counter of pulses on this IO line.

The name JSON-P callback-a is fixed, io_result(), and can not be changed in the request.

THE REQUEST OF THE STATUS OF ALL IO LINES

If the number of the line is not indicated, there will be a status bit map of all the lines.

```
http://192.168.0.100/io.cgi?io
```

RETURN VALUES

```
io_result('ok', 246);
```

where:

The first argument: always 'ok' (upon request error - 'error').

The second request: the status bit map of the lines.

bit 0 = line 1

bit 1 = line 2

...

bit 7 = line 8

Example:

The IO status of the IO lines								bit map
IO 1	IO 2	IO 3	IO 4	IO 5	IO 6	IO 7	IO 8	
0	0	0	0	0	0	0	0	0

1	0	0	0	0	0	0	0	1
0	1	0	0	0	0	0	0	2
0	0	1	0	0	0	0	0	4
0	0	0	1	0	0	0	0	8
0	0	0	0	1	0	0	0	16
0	0	0	0	0	1	0	0	32
0	0	0	0	0	0	1	0	64
0	0	0	0	0	0	0	1	128
1	1	1	1	1	1	1	1	255
1	1	1	0	0	1	1	1	231
1	0	1	1	1	1	1	0	125
0	1	0	0	1	0	0	0	18
1	1	0	1	1	0	0	0	27

LINE SWITCHING (IN EXIT MODE)

Switching to the state “0” or “1”:

```
http://192.168.0.100/io.cgi?ioN=0
http://192.168.0.100/io.cgi?ioN=1
```

where:

N — the line number, indicated after ?io.

Switching to an alternative (inverse) state.

```
http://192.168.0.100/io.cgi?ioN=f
```

where:

N — the line number, indicated after ?io.

Short-term switching to the inverse state, i.e., the creation of a pulse.

```
http://192.168.0.100/io.cgi?ioN=f,5
```

where:

N – the line number, indicated after ?io.

Duration in seconds is set after the decimal point.

THE CHOICE OF IO LINE OPERATION MODE

Setting the line operation mode: “0” - input, “1” - output:

```
http://192.168.0.100/io.cgi?ioN&mode=0
http://192.168.0.100/io.cgi?ioN&mode=1
```

where:

N — the ine number, indicated after ?io.

RETURN VALUES

Error (wrong request format or wrong number of the IO line):

```
io_result('error')
```

The command is completed:

```
io_result('ok')
```

AUTHORIZATION

To add a login and password to the structure of a URL-encoded command, it is possible to use the next scheme:

- http://<username>:<password>@<host>:<port>/<URL-path>?<parameters>

where:

<username>:<password> – are credentials for authorization in a device web interface;

<host> – is an IP address of a device;

<port> – is a port of an HTTP server;

<URL-path>?<parameters> – is a URL-encoded command

[ENG] 16.2. [DKSF 70/71.7 IU] The Control of The Relay

The interface of URL-encoded command in the device can be used for the integration with web applications without the SNMP protocole. The relay control is available via the interface of URL-encoded commands.

REQUEST OF THE RELAY STATE

```
http://192.168.0.100/relay.cgi?rN
```

where:

N —the relay number is indicated after ?r.

RETURN VALUES

```
Error (wrong format of the request or wrong relay number):
relay_result('error');
```

Successful completion of the command:

```
relay_result('ok', 0, 1);
```

where:

The first argument: always 'ok' (upon request error - 'error')

The second argument: the source of the relay control:

0 — OFF;

1 — ON.

The third argument: the instantaneous current state of the relay (“0” or “1”), considering the account the functioning of the “Watchdog” module, activation of a reset, impulse output, etc.

THE RELAY SWITCHING

Manual relay on and off:

```
http://192.168.0.100/relay.cgi?rn=s
```

After ?r the relay number is indicated, after = the number of mode is indicated.

where:

n — the relay number;

s — the relay operation mode:

0 — Off;

1 — On.

Switching (inverting) the relay, on <-> off:

```
http://192.168.0.100/relay.cgi?rn=f
```

Short-term switching of the relay to the inverse state (issuing a reset pulse):

```
http://192.168.0.100/relay.cgi?rn=f,10
```

Duration in seconds is indicated after the decimal point.

RETURN VALUES

An error is returned if the request format is incorrect as a result of setting an incorrect / invalid value for the relay number or relay mode.

```
relay_result('ok')
relay_result('error')
```

AUTHORIZATION

To add a login and password to the structure of a URL-encoded command, it is possible to use the next scheme:

- http://<username>:<password>@<host>:<port>/<URL-path>?<parameters>

where:

<username>:<password> – are credentials for authorization in a device web interface;

<host> – is an IP address of a device;

<port> – is a port of an HTTP server;

<URL-path>?<parameters> – is a URL-encoded command

[ENG] 16.3. [DKSF 70/71.7 IU] Control of Temperature Sensors

The interface of URL-encoded commands in the device can be used to integrate with web applications without using the SNMP protocol. Via the interface of URL-encoded commands, control of temperature sensors is available.

REQUEST OF THE STATE

```
http://192.168.0.100/thermo.cgi?tN
```

where:

N — number of the temperature sensor, indicated after ?t.

RETURN VALUES

Error in the request (wrong format or wrong number of sensor):

```
thermo_result('error')
```

Successful completion of the command

```
thermo_result('ok', 36, 2);
```

where:

The first argument: always 'ok' (upon request error - 'error').

The second argument: current temperature.

The third argument: the sensor status

0 - Sensor not connected or malfunctioning

1 - Temperature is below normal

2 - Temperature is normal

3 - Temperature above normal

AUTHORIZATION

To add a login and password to the structure of a URL-encoded command, it is possible to use the next scheme:

- http://<username>:<password>@<host>:<port>/<URL-path>?<parameters>

where:

<username>:<password> – are credentials for authorization in a device web interface;

<host> – is an IP address of a device;

<port> – is a port of an HTTP server;

<URL-path>?<parameters> – is a URL-encoded command

[ENG] 16.4. [DKSF 70/71.7 IU] The Control of Smoke Sensor (Current in the Loop)

The interface of URL-encoded commands in the device can be used to integrate with web applications without using the SNMP protocol. Smoke detector control is available through the URL-encoded command interface.

REQUEST OF THE STATE

```
http://192.168.0.100/curdet.cgi
```

RETURN VALUES

```
curdet_result('ok', 0, '')
```

where:

The first argument: always 'ok' (no error possible).

The second argument: numeric status value.

The third argument: textual status value:

0 — Normal;

1 — Alert;

2 — Broken Loop;

3 — Short in the Loop;

4 — Power Off.

SENSOR RESET

A short-term power supply is removed from the current loop:

```
http://192.168.0.100/curdet.cgi?reset
```

RETURN VALUES

```
relay_result('ok')
relay_result('error')
```

An error can return if the request format or text is incorrect.

AUTHORIZATION

To add a login and password to the structure of a URL-encoded command, it is possible to use the next scheme:

- http://<username>:<password>@<host>:<port>/<URL-path>?<parameters>

where:

<username>:<password> – are credentials for authorization in a device web interface;

<host> – is an IP address of a device;

<port> – is a port of an HTTP server;

<URL-path>?<parameters> – is a URL-encoded command

[ENG] 16.5. [DKSF 70/71.7 IU] The Control of the 1-wire Smoke Sensors

The interface of URL-encoded commands in the device can be used to integrate with web applications without using the SNMP protocol. Through the interface of URL-encoded commands, control of 1-wire smoke detectors is available.

REQUEST ABOUT THE RELAY STATE

```
http://192.168.0.100/smoke.cgi?sN
```

where:

N — the number of the smoke sensor.

RETURN VALUES

Error in the request (wrong format, wrong number of sensor)

```
relay_result('error');
```

Successful completion of the command

```
smoke_result('ok', 1, 'Норма');
smoke_result('ok', 1, 'OK');
```

where:

The first argument is 'ok',

The second - status in numbers, the third - status in text:

0 - Norm;

1 - Alert;

4 - The loop power is off;

5 - Sensor failure, or the sensor is absent on the 1-wire bus.

CONTROL OF THE LOOP POWER

Turning on, off, short-term shutdown of the voltage supplied to the current loop to power an external fire detector. Voltage relief is used to reset the triggered detector to its initial state:

```
/smoke.cgi?sN&on
/smoke.cgi?sN&off
/smoke.cgi?sN&reset
```

where:

N — the number of the state.

RETURN NUMBER

Error (wrong format of the request or wrong relay number

```
relay_result('error');
```

Successful completion of the command:

```
relay_result('ok');
```

AUTHORIZATION

To add a login and password to the structure of a URL-encoded command, it is possible to use the next scheme:

- http://<username>:<password>@<host>:<port>/<URL-path>?<parameters>

where:

<username>:<password> – are credentials for authorization in a device web interface;

<host> – is an IP address of a device;

<port> – is a port of an HTTP server;

<URL-path>?<parameters> – is a URL-encoded command

[ENG] 16.6. [DKSF 70/71.7 IU] The Control of the Transceiver of the IR Commands

An interface of URL-encoded commands in a device can be used to integrate with web applications without using an SNMP protocol. It is possible to control an IR command transceiver through the interface of URL-encoded commands.

SENDING AN IR COMMAND

```
http://192.168.0.100/ir.cgi?play=N
```

where:

N – is a number of a command.

RETURNED VALUES

```
ir_result('ok')
ir_result('error')
```

An error is returned only if a request format is incorrect or a command number is wrong. Errors of the module IRC-TRv2 are not checked when a response is formulated.

AUTHORIZATION

To add a login and password to the structure of a URL-encoded command, it is possible to use the next scheme:

- http://<username>:<password>@<host>:<port>/<URL-path>?<parameters>

where:

<username>:<password> – are credentials for authorization in a device web interface;

<host> – is an IP address of a device;

<port> – is a port of an HTTP server;

<URL-path>?<parameters> – is a URL-encoded command

[ENG] 16.7. [DKSF 70/71.7 IU] Control of the Humidity Sensors

The interface of URL-encoded commands in the device can be used to integrate with web applications without using the SNMP protocol. Through the interface of URL-encoded commands, humidity sensor control is available.

REQUEST OF THE RELATIVE HUMIDITY STATE

```
http://192.168.0.100/relhum.cgi?hN
```

where:

N — number of the humidity sensor.

RETURN VALUES

Successful completion of the command:

```
relhum_result('ok', 55, 2)
```

where:

The first argument: always 'ok'.

The second argument: relative humidity,%.

The third argument: sensor status:

0 - the sensor is not connected or fails;

1 - humidity below normal;

2 - humidity is normal;

3 - humidity is above normal.

REQUEST OF THE TEMPERATURE STATE

```
http://192.168.0.100/relhum.cgi?tN
```

where:

N — number of humidity sensor

RETURN VALUES

Successful completion of the command

```
relhum_result('ok', 25, 2)
```

where:

The first argument: always 'ok'.

The second argument: temperature, ° C.

The third argument: sensor status:

0 - the sensor is not connected or failed;

1 - temperature is below normal;

2 - temperature is normal;

3 - temperature is above normal.

AUTHORIZATION

To add a login and password to the structure of a URL-encoded command, it is possible to use the next scheme:

- http://<username>:<password>@<host>:<port>/<URL-path>?<parameters>

where:

<username>:<password> – are credentials for authorization in a device web interface;

<host> – is an IP address of a device;

<port> – is a port of an HTTP server;

<URL-path>?<parameters> – is a URL-encoded command

[ENG] 16.8. [DKSF 70/71.7 IU] Control of The GSM Modem

The interface of URL-encoded commands in the device can be used to integrate with web applications without using the SNMP protocol. Via the interface of URL-encoded commands, control of the built-in GSM modem is available.

SENDING SMS

```
http://192.168.0.100/sendsms.cgi?utf8
```

The URL is called by the POST method. POST data is an SMS text encoded in UTF-8. You can read more about sending arbitrary SMS messages in the section [ENG] 11.11. [DKSF 70/71.7 IU] How to Send Arbitrary SMS?

In order to send SMS in encoding Windows 1251, you can use:

```
http://192.168.0.100/sendsms.cgi
```

RETURN VALUES

Successful completion of the command:

```
smssend_result('ok');
```

Error in the request text

```
smssend_result('error');
```

GSM modem is busy

```
smssend_result('busy');
```

SIM CARD BALANCE REQUEST

```
http://192.168.0.100/ussdstart.cgi?coderequest
```

where:

code request — a[code]x.For example, a100x, which means * 100 #. In the USSD code of the request, “*” is replaced by “a”, “#” is replaced by “x” (Latin characters).

RETURN VALUES

Successful completion of the command

```
ussdsend_result('ok');
```

RECEIVING A RESPONSE TO A SIM CARD BALANCE REQUEST

```
http://192.168.0.100/ussdread.cgi
```

Call in 20 minutes after requesting SIM card balance.

RETURN VALUES

Successful completion of the command:

```
ussdsend_result("request_gsm_operator");
```

[ENG] 17. [DKSF 70/71.7 IU] Documentation and Files

In the “DOC&FILES” page of the device’s web interface, you can open the section with the documentation for the device and download the necessary files to configure some control systems.

Documentation - the links to Russian and English language documentation.

Files for configuring monitoring systems - MIB, OIDLIB (for the PRTG Network Monitror monitoring system) files and templates for the Zabbix monitoring system. They are stored in the device’s memory as part of the firmware. To download them you do not need the Internet.