[ENG] NetPing IO R401, Firmware Description

Содержание

[ENG] 1. [DKSF 561.1.6] Introduction 5
What This Document Is About? 5
Copyright and Disclaimer 5
[ENG] 2. [DKSF 561.1.6] Basic device information 6
[ENG] 2.1. [DKSF 561.1.6] Default username, password and network settings 7
[ENG] 2.2. [DKSF 561.1.6] Basic device information 8
[ENG] 2.3. [DKSF 561.1.6] Restart the device firmware. 10
[ENG] 2.4. [DKSF 561.1.6] The Log of a Device 12
General Events 12
Events from IO Lines 12
Events from the «Watchdog» Module 13
SYSLOG Support 13
[ENG] 3. [DKSF 561.1.6] Basic configuration 14
[ENG] 3.1. [DKSF 561.1.6] Name, location and contact details of the device 15
[ENG] 3.2. [DKSF 561.1.6] Network Settings 16
[ENG] 3.3. [DKSF 561.1.6] Access Restrictions 18
[ENG] 3.4. [DKSF 561.1.6] SNMP TRAP Sending 19
[ENG] 3.5. [DKSF 561.1.6] Syslog 20
[ENG] 3.6. [DKSF 561.1.6] Date amd Time Settings 21
[ENG] 3.7. [DKSF 561.1.6] Backup and Restore a Device Configuration 23
Backup configuration 23
Restore configuration 23
[ENG] 4. [DKSF 561.1.6] Setting E-MAIL notifications 24
Errors in sending e-mail notifications 25
Some errors that may occur when sending email notifications: 25
[ENG] 5. [DKSF 561.1.6] Work with channels of discrete input-output 26
[ENG] 6. [DKSF 561.1.6] SNMP support 29
[ENG] 6.1. [DKSF 561.1.6] Description 30
SNMP TRAP messages from IO lines 31
Front (Level Change 0 → 1) — when the logic level on the IO-line changes from low to high. 31

Decay (Level Change 1 → 0) — when the logic level on the IO-line changes from high to low. 31
[ENG] 6.2. [DKSF 561.1.6] Supported OIDs 32
[ENG] 6.3. [DKSF 561.1.6] SNMP TRAP 36
SNMP TRAP when changing the level on the IO-line 36
SNMP TRAP on WATCDOG state change 36
[ENG] 7. [DKSF 561.1.6] HTTP API Support 38
[ENG] 8. [DKSF 561.1.6] Internal logic and automation. 40
[ENG] 8.1. [DKSF 561.1.6] «Logic» 41
Control elements 41
Input → Conditions 42
Output → Actions 44
Pinger 45
SNMP SETTER 46
[ENG] 8.2. [DKSF 561.1.6] «Watchdog» 47
[ENG] 9. [DKSF 561.1.6] How to Update the Firmware of the Device? 49
Notes 50

[ENG] 1. [DKSF 561.1.6] Introduction

What This Document Is About?

This document describes the functionality of the DKSF 561.1.6 firmware for the NetPing IO R401.

The device NetPing IO R401 with the firmware of the DKSF 561.1.6 version support the next management interfaces:

- HTTP (web-interface);
- SNMP v1;
- URL encoded HTTP commands;

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.

A user guide can be explored at the link: [ENG] NetPing Input+Relay R404, User guide.

Copyright and Disclaimer

Developer and manufacturer:

NetPing east Co Ltd.

www.netpingdevice.com

sales@netpingdevice.com

[ENG] 2. [DKSF 561.1.6] Basic device information

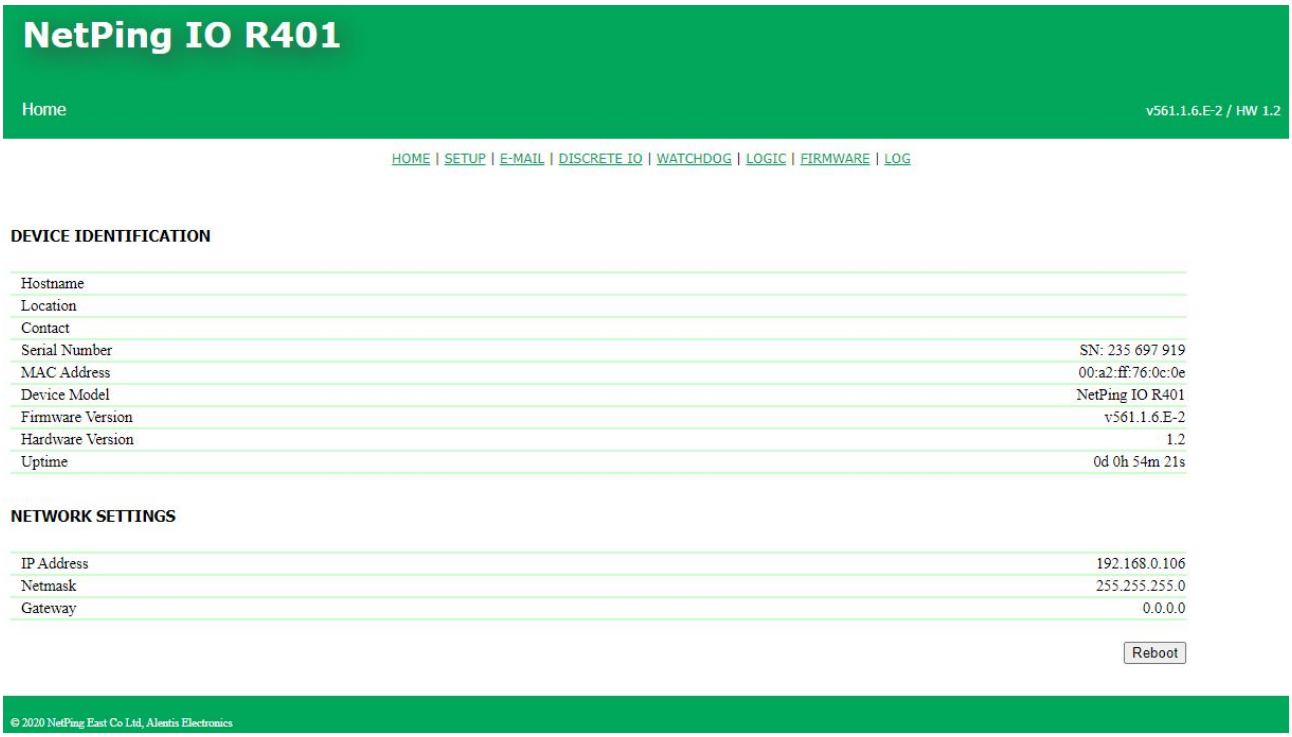
To connect to the Web interface of the device, it is recommended to use the Chrome browser.

[ENG] 2.1. [DKSF 561.1.6] Default username, password and network settings

- Web interface login: visor
- Password: ping
- IP-address: 192.168.0.100 / 24
- Web port: 80
- SNMP port: 161
- Read/Write community: SWITCH

[ENG] 2.2. [DKSF 561.1.6] Basic device information

Basic information about the device is available in the "DEVICE IDENTIFICATION" block on the "MAIN" page of the Web interface.



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.

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.

MAC address — device MAC address.

Device model — the device model; for firmwares suitable for several models, several models can be specified at once.

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 561.1.6.E-2), 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;
- **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.

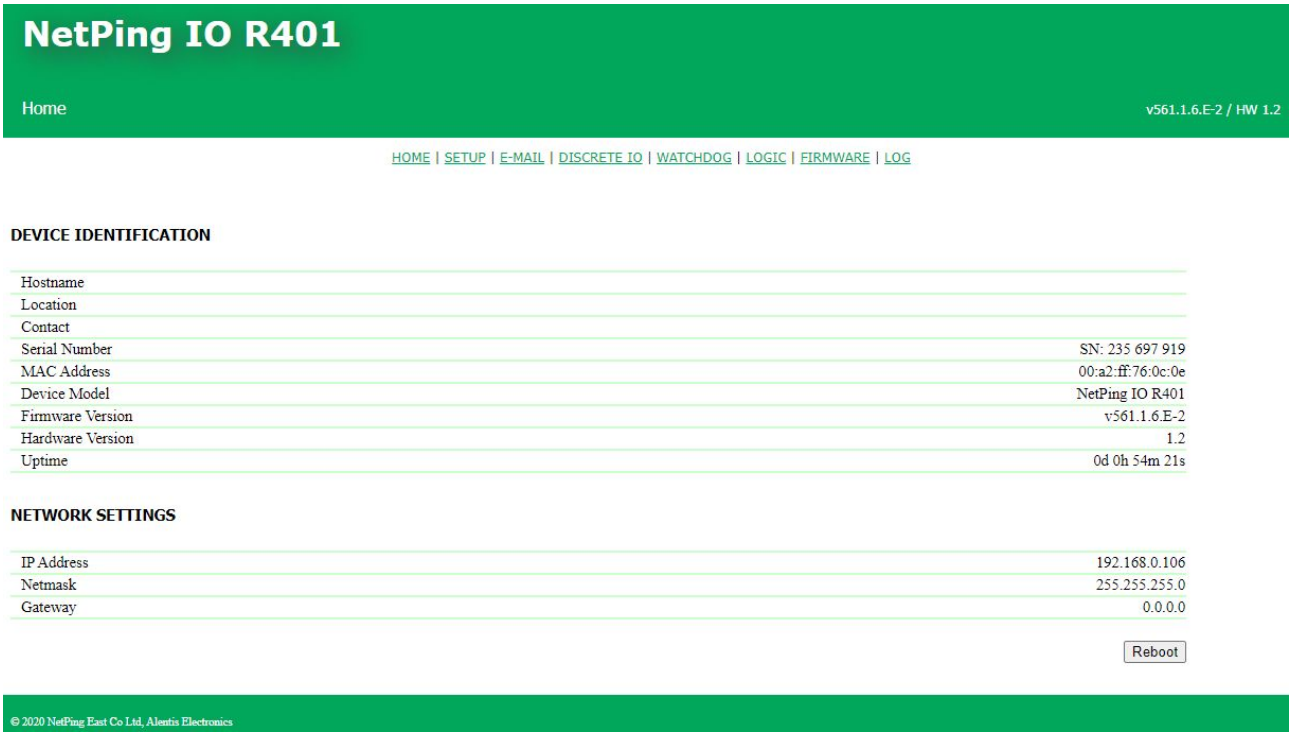
Uptime — is the uptime of a device since the last switching on or rebooting.

[ENG] 2.3. [DKSF 561.1.6] Restart the device firmware.

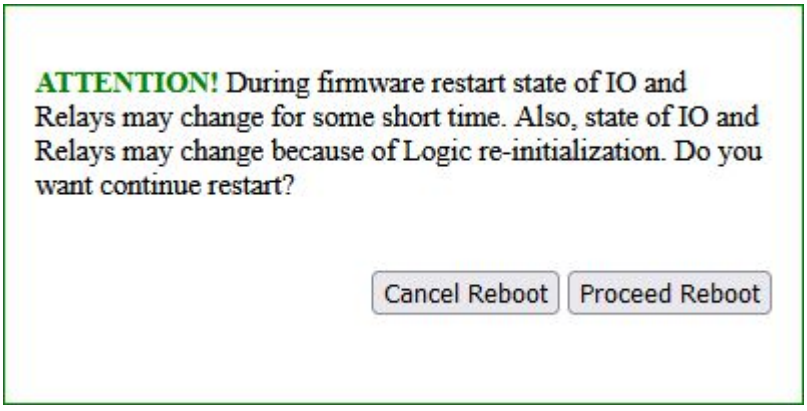
You can restart the firmware in three ways:

1. Web-interface:

On the main page of the device, at the bottom of the interface there is a button "Reboot":



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.

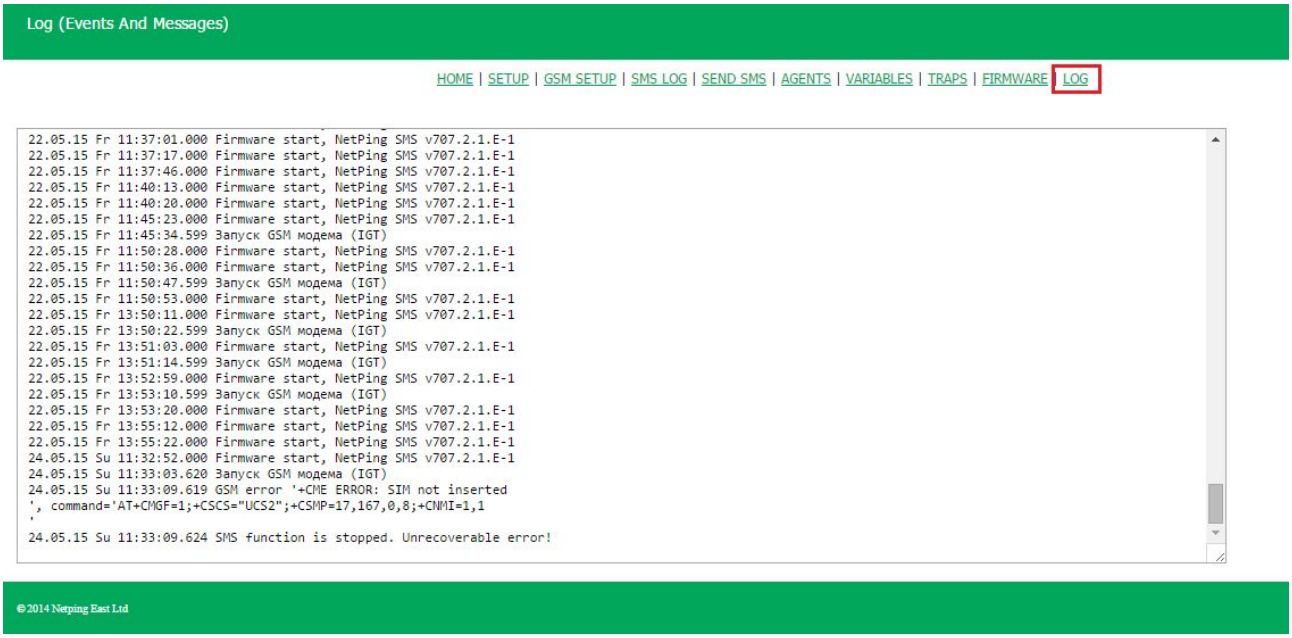
2. Using an **SNMP v1** protocol by setting OID values by the command **Set**:

OID	Name	Type	Access	Dscription
.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).

[ENG] 2.4. [DKSF 561.1.6] 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 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.

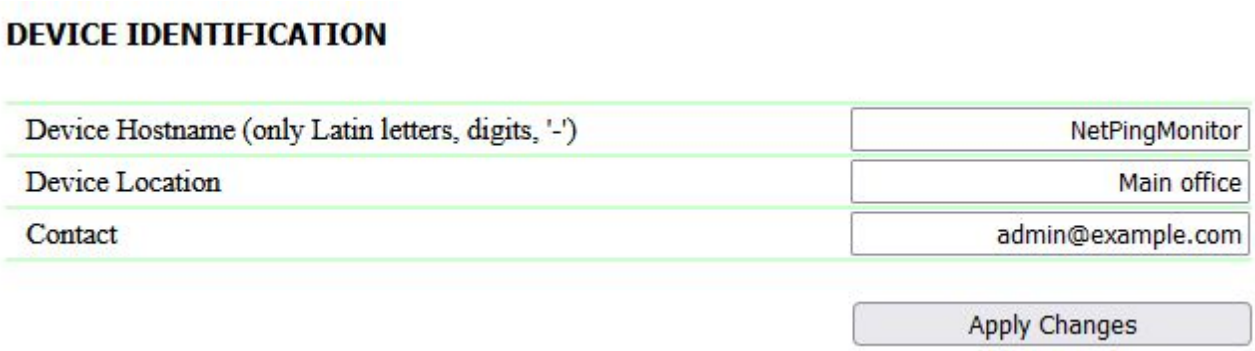
SYSLOG Support

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. [DKSF 561.1.6] Basic configuration

[ENG] 3.1. [DKSF 561.1.6] Name, location and contact details of the device



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	Dscription
.1.3.6.1.2.1.1.5.0	sysName	DISPLAYSTRING (SIZE (0..255))	READ/WRITE	Device Hostname
.1.3.6.1.2.1.1.6.0	sysLocation	DISPLAYSTRING (SIZE (0..255))	READ/WRITE	Device Location
.1.3.6.1.2.1.1.4.0	sysContact	DISPLAYSTRING (SIZE (0..255))	READ/WRITE	Contact

[ENG] 3.2. [DKSF 561.1.6] Network Settings

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.

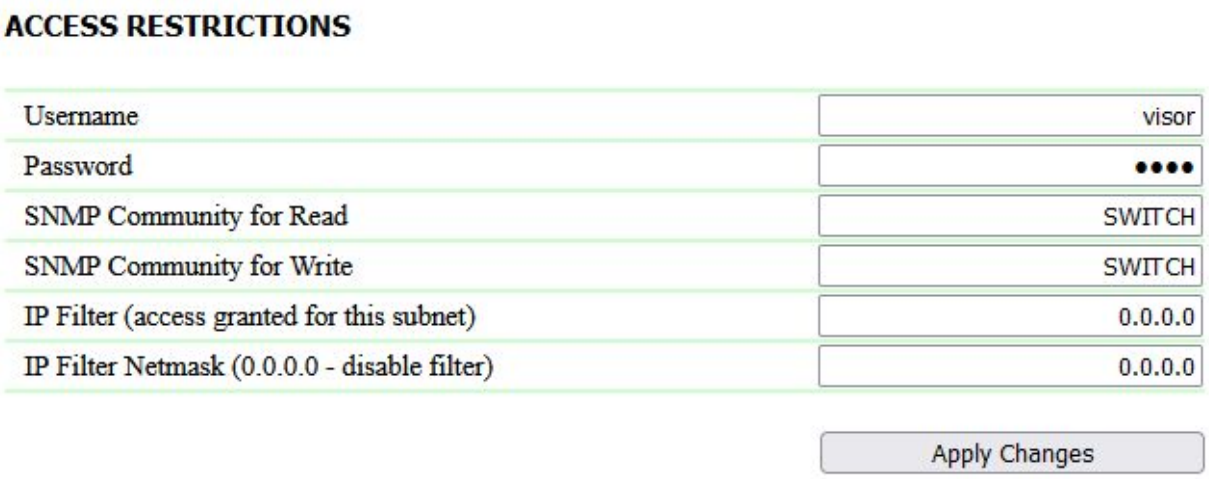
Embedded HTTP server port — the field for setting the port number on which the web server will listen for incoming connections. On default: 80.

SNMP Agent Port — a field for setting the UDP port number that the SNMP agent listens to. On default: 161.

> 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».

[ENG] 3.3. [DKSF 561.1.6] Access Restrictions



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.

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

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 255.255.255.255 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.

[ENG] 3.4. [DKSF 561.1.6] SNMP TRAP Sending

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. On default: the address is not specified.

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

[ENG] 3.5. [DKSF 561.1.6] Syslog

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).

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

[ENG] 3.6. [DKSF 561.1.6] Date amd Time Settings

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**».

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.

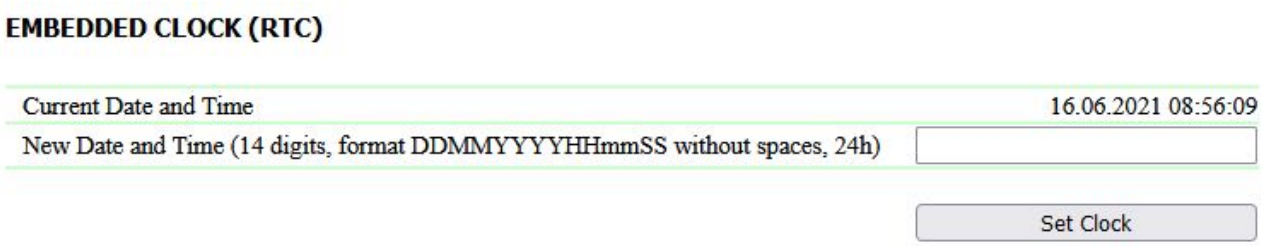
Timezone — a configuration of a local timezone. On default: UTC+03.00.

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

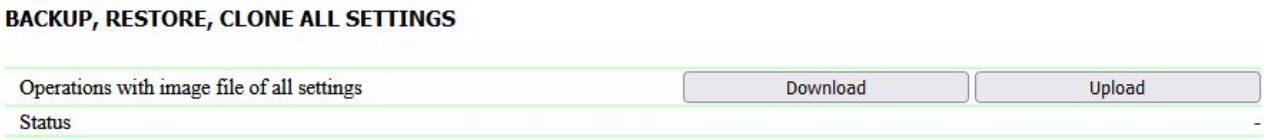
To use the NTP servers from the Internet, a device is going to have a gateway correctly configured, and a device should have the Internet connection via an NTP protocol.



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.

[ENG] 3.7. [DKSF 561.1.6] Backup and Restore a Device Configuration



Backup configuration

To save a backup copy of the configured device configuration to a binary file, go to the **«SETUP»** page of the device web interface. In the **«Backup, restore, clone all settings»** section, click the **«Download»** button:

After that, a settings file with the .bin extension will appear on the local disk of the PC, for example, USS-001-125-ServerRoom-1_setup.bin (the device name configured on the «SETUP» page of the web interface is substituted before the underscore in the file name).

Restore configuration

To save a backup copy of the configured device configuration to a binary file, go to the **«SETUP»** page of the device web interface. In the **«Backup, restore, clone all settings»** section, click the **«Upload»** button:

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

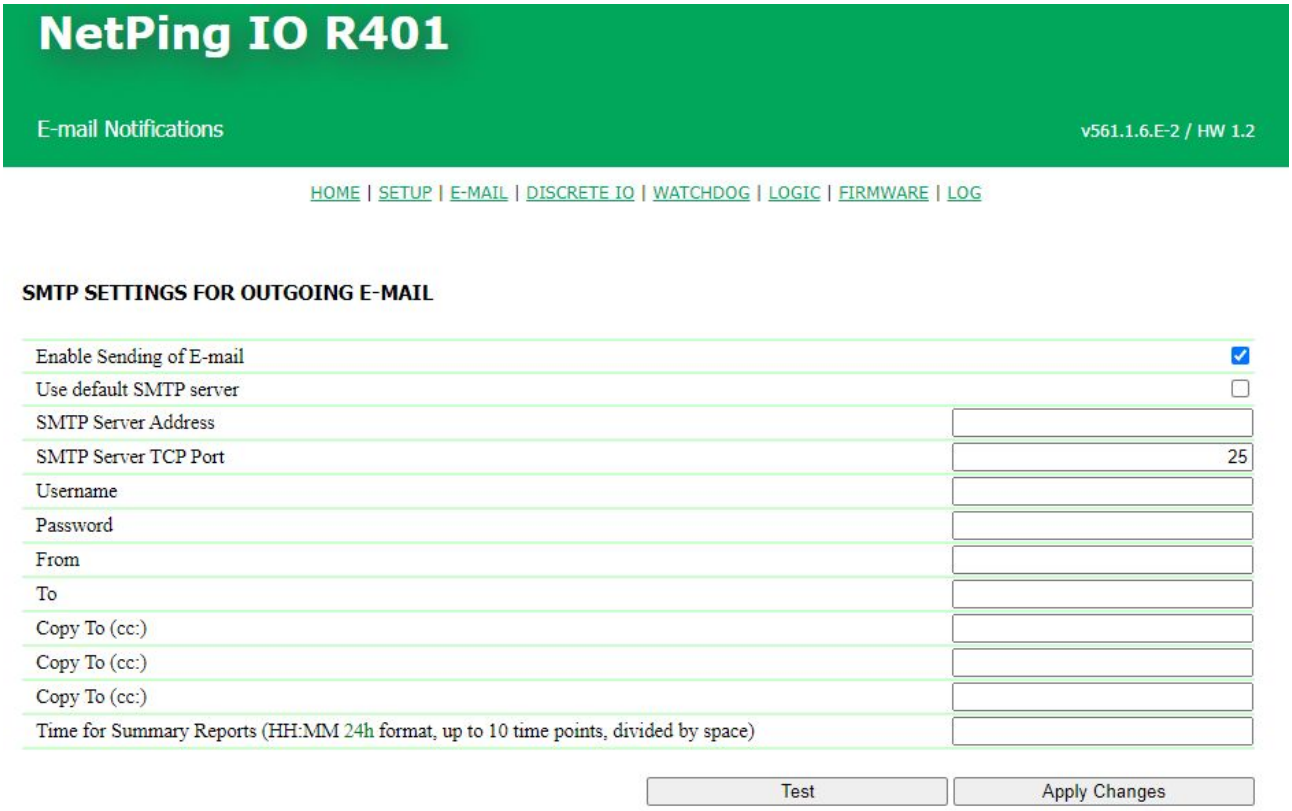
This can be used for the quick setting reproduction among identical devices. Specified parameters are not cloned and should be configured manually and individually for every device.

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 561.1.6] Setting E-MAIL notifications

E-MAIL notifications are sent when events occur, specified in the settings of device objects, for example, when the state of an input line changes, a sensor changes, or a "watchman" is triggered. You can configure the sending of e-mail notifications on the "E-MAIL" page of the device's web interface.



- **Enable sending email notifications** — enable or disable email notifications. Default: checked.
- **Use default SMTP server** — use the settings of the NetPing SMTP server, which is intended for free use on NetPing devices. Default: checked.
- **SMTP server address** - the address of the outgoing mail server. Default: empty string.
- **SMTP server port** - mail server port. Default: 25.
- **Username** - The username of the SMTP server. Default: empty string.
- **Password** — password of the SMTP server user. Default: empty string.
- **From (from:)** — the sender's address. If a device name is specified, it will be added to the From: field of the mail message automatically at the time of sending. Default: an empty string or, if using the default server, %sn%_%devicename%@smtp.netping.ru, where %sn% is the serial number of the device, %devicename% is the device name.
- **To (to:)** — email notification recipient address. Default: empty string.

- **Cc (ss:)** — addresses of secondary recipients of email notifications to which a copy is sent. Default: empty string.
- **Time of reports (format HH:MM, up to 12 parcels, separated by a space)** — time of day when daily reports on the status of sensors will be sent by email. Up to 12 parcels per day. Default: empty string.

After setting the parameters, click the "**Apply Changes**" button.

The device can only work with mail servers that support the SMTP protocol and the AUTH PLAIN and AUTH LOGIN authentication methods, as well as the method without authentication. However, the device cannot support SSL, TLS, or other encryption.

The subject of each email notification includes a serial number, which is needed to prevent email clients (in particular, gmail.com) from automatically combining messages with the same subject into a chain, which breaks the apparent order of messages in the incoming mail array and makes it difficult to perceive the sequence of notifications. Periodic e-mail reports contain a subject line like this: "Sensor Status Report #7d732006".

Errors in sending e-mail notifications

If errors occur while connecting to the SMTP server, they are written to the Device Log and sent to SysLog.

Some errors that may occur when sending email notifications:

sendmail: 535 Incorrect authentication data was received in response to AUTH PLAIN — invalid username/ password.

sendmail: message discarded, server IP unknown - The server's IP address is unknown. It may be that there is no connection to DNS and the resolution of the name to an IP address cannot be performed.

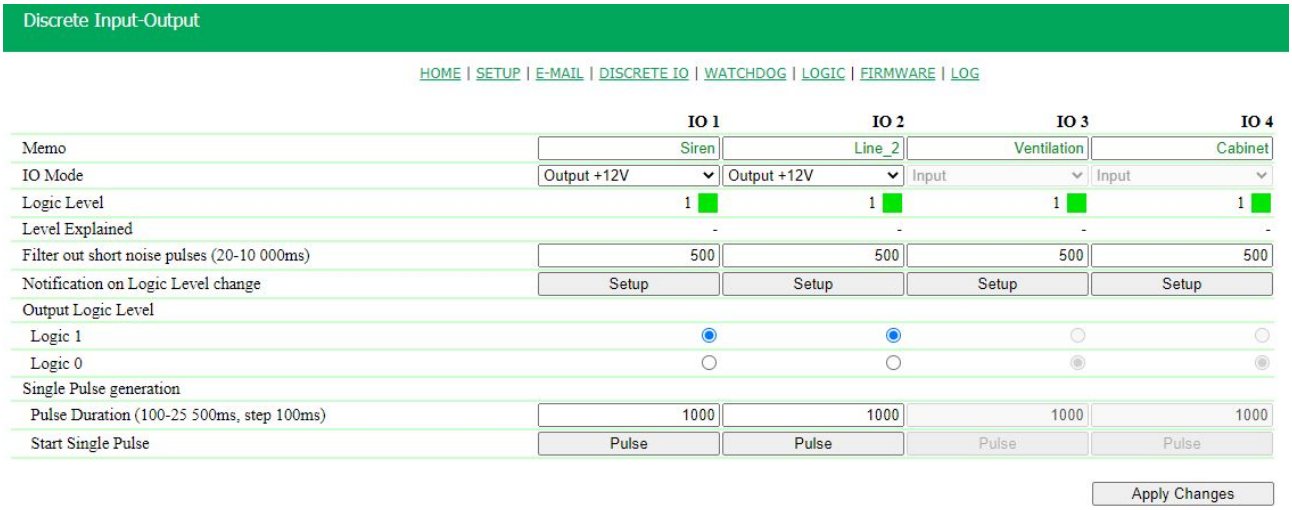
No room for new mail message - The outgoing queue is full. For example, the mail server is unavailable, the message is queued.

[ENG] 5. [DKSF 561.1.6] Work with channels of discrete input-output.

For channels of discrete input-output, the following functionality is available on the device:

- Web interface;
- HTTP API;
- SNMP, SNMP TRAP;
- All notification channels, available in the firmware;
- Logic;
- Customizable notifications.

In order to work with the channels via web interface you need to open the **«DISCRETE IO»** page of the device web interface:



Memo — short description of the sensor. Memo is used in SYSLOG and log messages, and also included in SNMP TRAP, SMS reports and notifications (only for model with GSM modem), E-mail reports and notifications. The maximum size is 16 characters. **Default: empty.**

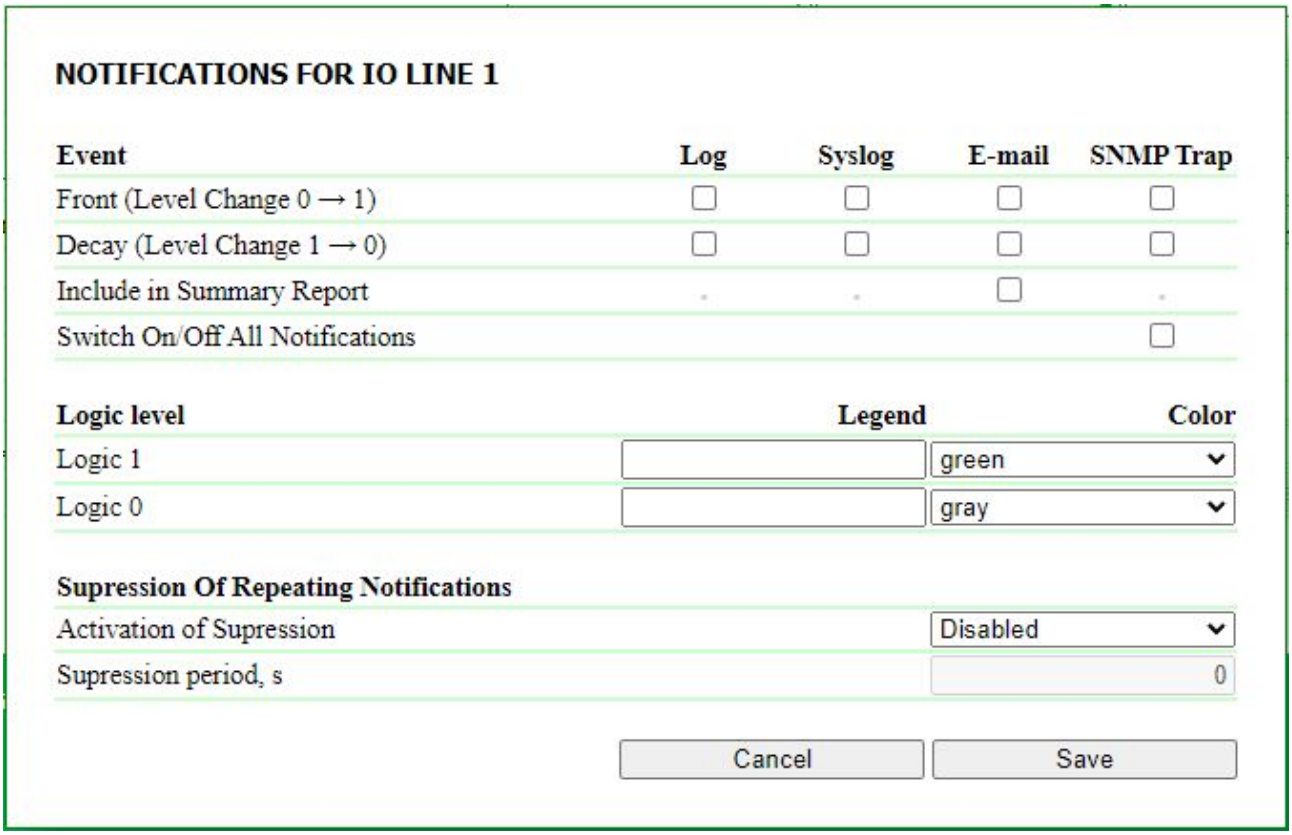
IO Mode — setting the line operation mode: **«input»** (for connecting dry contact sensors to the IO-line), **«output +12V»** (for controlling external devices). **Default: input.**

Logic Level — the current logic level on the IO-line. Refreshes automatically when the logical level of the line changes without having to refresh the entire page.

Level Explained — logical level text legend. **Default: empty.**

Filter out short noise pulses — field for setting the time during which the IO-line, configured as an «input», must remain in a stable state in order to register it. This parameter allows you to filter out short interference signals or bounce of mechanical contacts. **Default: 500 ms.**

Notification on Logic Level change — **«Setup»** button, a settings menu appears for sending notifications. Here you can also specify the decoding of the digital values of the current level of the IO-line, color indication and other settings:



- **Front (Level Change 0 → 1)** — IO-line status change from «0» to «1» .
- **Decay (Level Change 1 → 0)** — IO-line status change from «1» to «0».
- **Include in Summary Report** — add a line to a periodic report by SMS or E-mail. The time for sending reports is configured on the «SMS», «EMAIL» pages.
- **Switch On/Off All Notifications** — enabling and disabling all possible notification methods at once for all events.
- **Logic Level, Legend** — textual decoding of the logical level of the IO-line. It will be displayed in the **«Level Explained»**, as well as be present in SYSLOG and log messages, in SNMP TRAP, SMS and e-mail notifications.
- **Logic Level, Color** — selection of the color of the virtual logic level indicator, It will be displayed in the **«Level Explained»** (the color of the physical LEDs on the front panel is not customizable), possible options are white, gray, orange, red, green. **Default: for «Log. 1» — green, for «Log. 0» — gray.**
- **Supression Of Repeating Notifications** — a function that saves you from spam when the logical level on the line is frequently changed. This option allows you to suppress repeated uninformative notifications, taking into account the specifics of the connected sensor.
- **Activation of Supression** —configures a transition that triggers a re-notification suppression period. It is set to a value corresponding to an alarm (for example, a power failure). Asymmetric activation is required so that exiting the alarm state does not trigger spam suppression. Until the suppression period expires, all notifications for any state transitions are discarded. Possible values — **«Disabled»**, **«0 → 1»** , **«1 → 0»** and **«Any Change»** (0 → 1 & 1 → 0).
- **Supression Period, s** — the time during which recurring notifications will be suppressed. Possible values are 0–65500 seconds.

Output Logic Level — setting a logic level on a line that acts as an **«output»**. The state of logic **«1»** means the presence of voltage on the output line (open collector circuit). The state of logic **«0»** means no voltage on the output line. **Default: Logic «0»**.

Start Single Pulse — when you press the **«pulse»** button, the IO-line, working as **«output»**, will be inverted for the set time. The duration of the impulse is set in the field **«Pulse Duration»** (100-25500ms, step 100ms). If the line is configured as **«input»**, the pulse button is inactive.

[ENG] 6. [DKSF 561.1.6] SNMP support

[ENG] 6.1. [DKSF 561.1.6] Description

The device supports SNMP v1 protocol. SNMP TRAP partially in v2.

You can read more about the SNMP protocol at the links:

- http://ru.wikipedia.org/wiki/SNMP
- http://www.SNMP.ru/doku.php

The OIDs supported by the devices can be found in the MIB files on the device description pages in the «**Documentation and Files**» section.

Devices support:

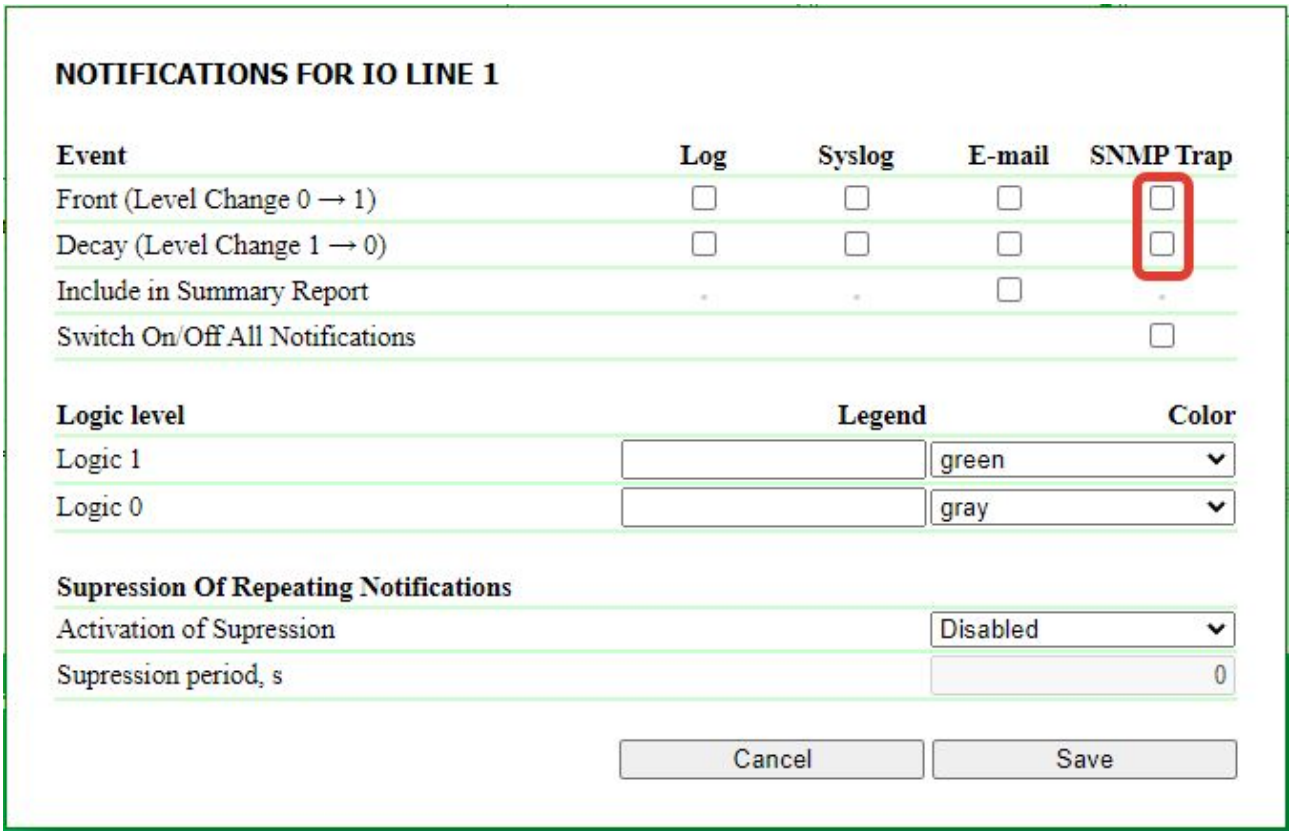
- reading OID using **Get**, **Get-Next** requests via SNMP v1 protocol;
- setting OID values using the **Set** command via the SNMP v1 protocol;
- sending **TRAP** messages on events.

In order to configure the sending of SNMP TRAP messages, you need to:

1. On the «**SETUP**» page, in the SNMP TRAP section, configure the address and UDP port of the primary and secondary (if necessary) trap receivers.

2. On the pages of the IO-lines, in the notification settings dialogs for each sensor, enable the checkboxes of the events that send Traps.

SNMP TRAP messages from IO lines



Front (Level Change 0 → 1) — when the logic level on the IO-line changes from low to high.

Decay (Level Change 1 → 0) — when the logic level on the IO-line changes from high to low.

[ENG] 6.2. [DKSF 561.1.6] Supported OIDs

The description of the OIDs supported by the device is shown in the table:

For your convenience we recommend you 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	Dscription
RFC1213				
.1.3.6.1.2.1.1.1.0	sysDescr	OctetString	READ	A textual description of the device.
.1.3.6.1.2.1.1.2.0	sysObjectID	OID	READ	Branch number with device parameters always «.1.3.6.1.4.1.25728»
.1.3.6.1.2.1.1.3.0	sysUpTime	TimeTicks	READ	Runtime since last power on or reboot (uptime).
.1.3.6.1.2.1.1.4.0	sysContact	OctetString	READ/WRITE	Contact details, usually the administrator's email.
.1.3.6.1.2.1.1.5.0	sysName	OctetString	READ/WRITE	Device name.
.1.3.6.1.2.1.1.6.0	sysLocation	OctetString	READ/WRITE	Location of the device.
.1.3.6.1.2.1.1.7.0	sysServices	Integer	READ	The binary representation of this OID is the set of supported services. Always "72", the device acts as an end 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 associated with a physical or logical interface. For most software, ifIndex is the name of the interface

OID	Name	Type	Access	Dscription
.1.3.6.1.2.1.2.2.1.2	ifDescr	OctetString	READ	A string containing information about the interface. The line contains the manufacturer's name, device model and hardware interface version
.1.3.6.1.2.1.2.2.1.3.1	ifType	Integer	READ	Device network interface type
.1.3.6.1.2.1.2.2.1.4.1	ifMtu	Integer	READ	Packet size by 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	Device MAC-Address
NetPing MIB				
.1.3.6.1.4.1.25728.911.1.0	npSoftReboot	Integer	READ/WRITE	Software restart of the device when writing the value "1"
.1.3.6.1.4.1.25728.911.2.0	npResetStack	Integer	READ/WRITE	Software reboot of the network interface when writing the value "1"
.1.3.6.1.4.1.25728.911.3.0	npForceReboot	Integer	READ/WRITE	Immediate forced reboot of the device when writing the value "1" (reset the MCU as at power on)
Discrete IO lines				
.1.3.6.1.4.1.25728.8900.1.1.1.n	npIoLineN.n	Integer	READ	IO line index.
.1.3.6.1.4.1.25728.8900.1.1.2.n	npIoLevelIn.n	Integer	READ	The current state of the line.

OID	Name	Type	Access	Dscription
.1.3.6.1.4.1.25728.8900.1.1.3.n	npIoLevelOut.n	Integer	READ/WRITE	IO-line control in the «output» mode. 0 — low level (GND) 1 — high level (12V). Also, this OID 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». Not applicable for input lines 3...4
.1.3.6.1.4.1.25728.8900.1.1.6.n	npIoMemo.n	DisplayString	READ	IO line memo.
.1.3.6.1.4.1.25728.8900.1.1.9.n	npIoPulseCounter.n	Counter32	READ/WRITE	Counter of impulses on the IO-line. It is counted on the positive edge of the pulse after filtering short pulses. For forced zeroing, write down «0». Also clears when the 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 (permissible values are from 100 ms to 25 500 ms, with a step of 100 ms). Not applicable for input lines 3...4
.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 npIoSinglePulseDuration.n variable. Not applicable for input lines 3...4
WATCHDOG				
.1.3.6.1.4.1.25728.5800.3.1.1.n	npPwrChannelN	Integer	READ	Ordinal number of the watchdog, where n is the number of the watchman, a number from 1 to 2
.1.3.6.1.4.1.25728.5800.3.1.4.n	npPwrResetsCounter	Integer	READ/WRITE	The total number of watchdog activations. Write "0" for zero
.1.3.6.1.4.1.25728.5800.3.1.5.n	npPwrRepeatingResetsCounter	Integer	READ	Number of watchdog triggers in a row

OID	Name	Type	Access	Dscription
.1.3.6.1.4.1.25728.5800.3.1.6.n	npPwrMemo	OctetString	READ	Managed Entity Reminder

[ENG] 6.3. [DKSF 561.1.6] SNMP TRAP

A formal description of SNMP TRAP messages can be found in the MIB files supplied with the device firmware. They can be downloaded on the pages of the site with the description of devices in the "Documentation and files" section. The SNMP TRAP message is sent in SNMP v1 / v2c format, while the description in the MIB files is in SNMP v2c format.

The one-to-one correspondence of SNMP TRAP message authentication for v1 and v2c is described in RFC3584 «Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework.» Programs for processing SNMP notifications, as a rule, convert between the two formats without difficulty.

SNMP TRAP when changing the level on the IO-line

Identification 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**

Variables in the set of npIoTrap (varbind list)

.1.3.6.1.4.1.25728.8900.2.1.0	Integer	The number of an IO line, the change of which triggered sending of a TRAP message
.1.3.6.1.4.1.25728.8900.2.2.0	Integer	The logic level value on the IO-line («0» or «1»)
.1.3.6.1.4.1.25728.8900.2.6.0	Display String	Memo (win1251)
.1.3.6.1.4.1.25728.8900.2.7.0	Display String	Logical level Explained. Human-readable description of the numeric value of the logic level of the IO-line

SNMP TRAP on WATCDOG state change

npPwrWdogTrap identification

General view of SNMP TRAP	**.1.3.6.1.4.1.25728.5800.6**

SNMP v1 generic-trap	**enterpriseSpecific(6)**
SNMP v1 specific-trap	**1**
SNMP v2 snmpTrapOID	**.1.3.6.1.4.1.25728.5800.2.0.1**

snmpTrapOID npPwrWdogTrap

Decryption of the event type and channel number can be enabled by the corresponding checkboxes in the notification settings dialog.

.1.3.6.1.4.1.25728.5800.6.100.n	Start of timer reset, where n is the number of WATCHDOG 1...4
.1.3.6.1.4.1.25728.5800.6.101.n	Watchdog reset paused due to missing event , where n is the number of the WATCHDOG 1...4
.1.3.6.1.4.1.25728.5800.6.102.n	Normal watchdog operation resumed, address ping resumed, where n is the number of WATCHDOG 1...4

npPwrWdogTrapData identification

General view of SNMP TRAP	**.1.3.6.1.4.1.25728.5800.2**

[ENG] 7. [DKSF 561.1.6] HTTP API Support

HTTP API			
Description	Request	Response	Notes
Input-Output Lines			
Line status query	/io.cgi?ioN • N — line number	io_result('error') io_result('ok', -1, 1, 339) • First argument: always 'ok' (on request error - 'error'). • Second argument: always "-1", for future API extensions. • Third argument: the current momentary state of the IO-line, including the reset state. • The fourth argument: the pulse counter on this IO-line, is counted on the edge.	
Requesting the status of all lines	/io.cgi?io	io_result('error') io_result('ok', 246); • First argument: always 'ok' (on request error - 'error'). • Second argument: bitmap of line status.	Bitmap (represented in decimal format): • bit 0 = line 1 • bit 1 = line 2 • ... • bit 3 = line 4 For example: • 0000 — 0 (all lines - log.0) • 1110 — 14 (4 - log.0, rest - log.1)
Line control in «Output» mode	/io.cgi?ioN=S • N — line number • S — operating mode (1 - on (log.1), 0 - off (log.0))	io_result('error') io_result('ok')	Not applicable for input lines 3...4
Switching the line to the inverse state in the «Output» mode	/io.cgi?ioN=f • N — line number	io_result('error') io_result('ok')	Not applicable for input lines 3...4

HTTP API			
Reset, switching the line to the inverse state for a while in the «Output» mode	/io.cgi?ioN=f,time • N — line number • time — reset time.	io_result('error') io_result('ok')	Not applicable for input lines 3...4
Changing the line mode	/io.cgi?ioN&mode=S • N — line number • S — mode (1 — «Output», 0 — «Input»)	io_result('error') io_result('ok')	Not applicable for input lines 3...4

[ENG] 8. [DKSF 561.1.6] Internal logic and automation.

The device allows you to implement simple automation scenarios thanks to built-in logic and automation modules.

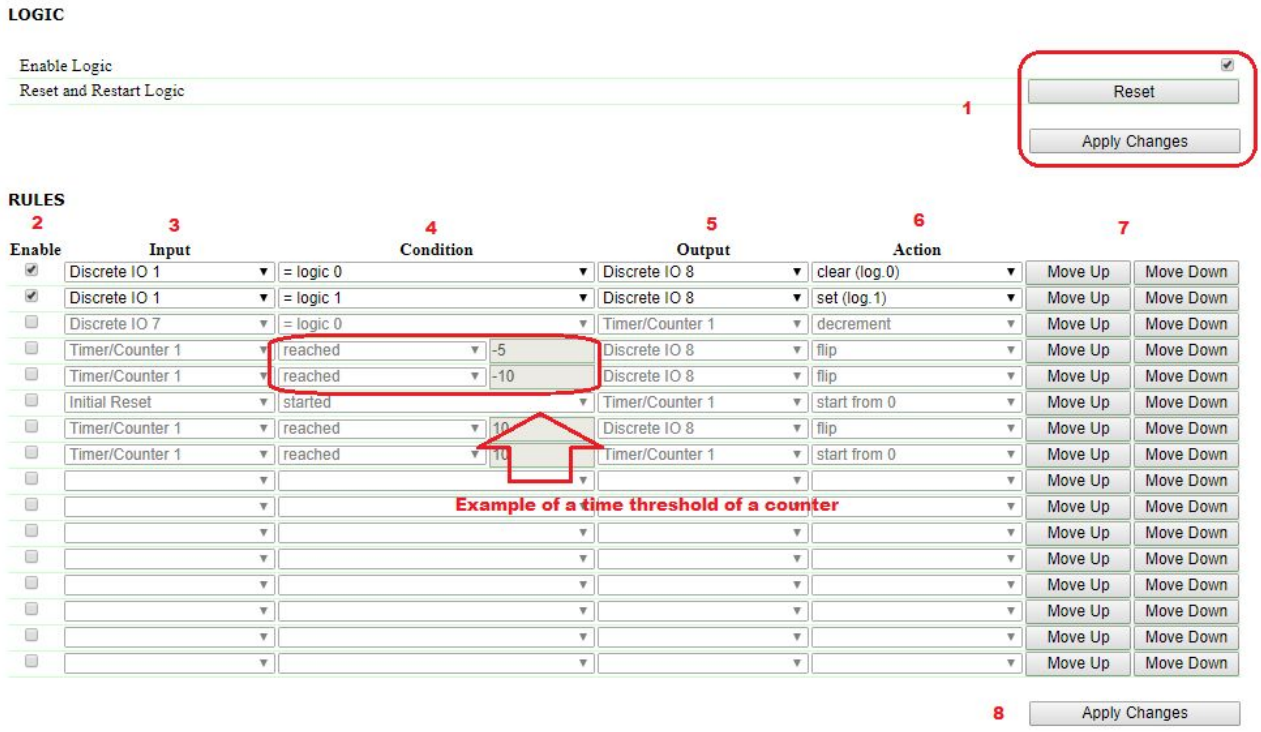
[ENG] 8.1. [DKSF 561.1.6] «Logic»

- Control elements
- Input → Conditions
- Output → Actions
- Pinger
- SNMP SETTER

> It is strictly forbidden to use a NetPing device to control electrical circuits if a control violation can cause significant damage.

The logic module is designed for simple automation and can perform tasks such as maintaining a microclimate, controlling automatic on/off of backup equipment, delay and sequence of switching on equipment, simple logic of repetitions of certain actions, counting the number of triggering of sensors, etc. The logic works on the basis of rules programmed by the user through the web interface. The «LOGIC» page of the device web interface describes the module operation algorithm and its configuration options.

The logic module is based on a list of programmed rules.



Control elements

1. Control buttons for the «LOGIC» module:

- «**Enable Logic**» — check-box that enables and disables the work of logic. After changing the state of the check-box, it is necessary to save the current settings by clicking the «Apply Changes» button.
- «**Reset**» — initiates a logic reset ("Initial Reset" signal).
- «**Apply Changes**» saves the current settings.

2. Rule enable checkbox — logic rule activation checkbox. Inactive rules are grayed out.

3. Input — source of information for the rule to work. Possible values are shown in the table below.

4. Condition — the condition under which the rule is applied and a command is issued that changes the exit state. The available set of conditions varies depending on which input type is selected and reflects the meaning of the input state. Possible values depending on the type of input are presented below.

5. Output — the entity that will be acted upon when the rule is triggered. Possible values are shown in the table below.

6. Action — the action to be performed on the output entity. Possible values are shown in the table below.

7. Check-box for activation of the «Move Up»/«Move Down» buttons of the logic level. Inactive rules are grayed out. The buttons are used to change the position of the rule in the list, does not affect the functionality.

> Conflicting rules should be avoided if they could lead to an attempt to control the same output at the same time.

8. Apply changes. The «Apply Changes» button saves the programmed logic rules in the device memory.

Input → Conditions

Conditional (4, see the figure) event at which the rule is applied and a command is issued that changes the output state. The available set of conditions changes depending on which input type (3, see the figure) is selected, and reflects the meaning of the input state. Possible values depending on the type of input are presented below.

Input	Descripion	Conditions	Descripion
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.	Started	The rule is triggered 5 seconds after the reset.
		Ended	The rule is triggered 10 seconds after the reset.
Discrete IO 1..4	Current logic level of the IO-line	= logic 0	The logic level of the selected IO-line has switched to 0 or 1.
		= logic 1	
Pinger 1..2	Checking a remote host via ping (ICMP Echo requests)	got no response	Missing or receiving a response from the host being checked by the pinger.
		got response	

Input	Description	Conditions	Description
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.
Schedule	Specifies the day and time when the rule will be triggered	hh:mm ddd	The rule will be triggered at the specified time and days of the week. Time entry format hh:mm ddd, where: hh - hours in the range 0 ... 23; mm - minutes in the range 0 ... 59; ddd - numbers of days of the week in ascending order (if the day of the week is not specified, the schedule is triggered every day). Examples: "22:10 46" - the rule is triggered at 22:10 every Thursday and Saturday. "22:10 14567" - the rule is triggered every Monday and every day from Thursday to Sunday.

Output → Actions

Actions (6, see the figure) that can be performed with one or another of the outputs (5, see the figure) of the device.

Output	Description	Actions	Description
Timer/ Counter 1..4	The control of a built-in timer/ counter. it is not recommended to mix the functions of timer and counter.	start from 0 (the timer function)	Start the timer from 0. The countdown is carried out in seconds with a resolution of 0 ... 1sec.
		reset	Stop and reset the timer. Reset counter.
		increment (the counter function)	Add 1 (increment) to the current counter value.

Output	Descripion	Actions	Descripion
		decrement (the counter function)	Decrease 1 (decrement) from the current counter value. The counter value does not decrease below zero.
Discrete IO 1..2	The control of IO line	clear (log.0)	Set the line to log.0 state.
		set (log.1)	Set the line to log.1 state.
		flip	Flip log. state of the line
		pulse	To send an impulse to the line. Duration is set in the settings of the IO line.
SNMP Setter 1..4	The sending of SNMP SET commands to the other devices	switch off	Record the value corresponding to «off» to the specified OID in Setter's settings.
		switch on	Record the value corresponding to «on» to the specified OID in Setter's settings.

Pinger

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 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. **Default: empty.**

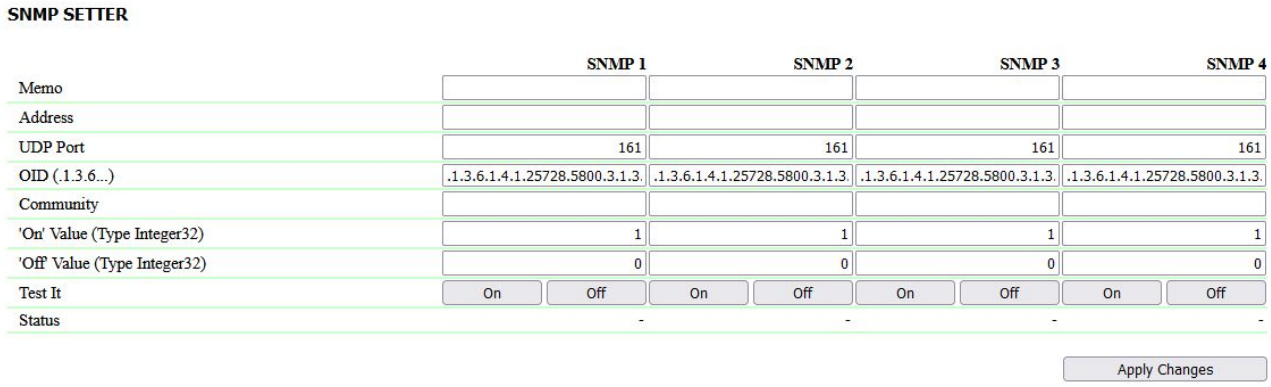
Polling Period, 5-900s — the value is selected according to the speed of detecting the fault. A regular check is carried out with the indicated period. Please note that overly frequent power switching can reduce equipment service life. **Default: 15.**

Ping Timeout, 100-10000ms — 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 «no response», and retries stop until the next verification period. **Default: 1000.**

Status — possible values: «**no response**», «**response**», «**-**». 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 «no response» 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 «no response» status.

SNMP SETTER



SNMP 1..4 — SNMP SETTER Channel.

Memo — textual description of the remote object, for ease of perception (up to 30 sympols). **Default: empty.**

Address — an IP address or domain name (up to 62 characters) where the SNMP SET request will be sent to. **Default: empty.**

UDP Port — a port, where the SNMP SER requests are sent to. **Default: 161.**

OID (.1.3.6...) — OID 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 OID's is contained in the MIB file from the device or in the documentation to the device. **Default: .1.3.6.1.4.1.25728.5800.3.1.3.1.**

Community — SNMP Community write of remote device. **Default: empty.**

'On' Value (Type Integer32) — the value that will be recorded in the OID on the remote device when the «switch on» action is called in the logic rule. The value type is a 32-bit signed integer. **Default: 1.**

'On' Value (Type Integer32) — the value that will be recorded in the OID on the remote device when the «switch off» action is called in the logic rule. The value type is a 32-bit signed integer. **Default: 0.**

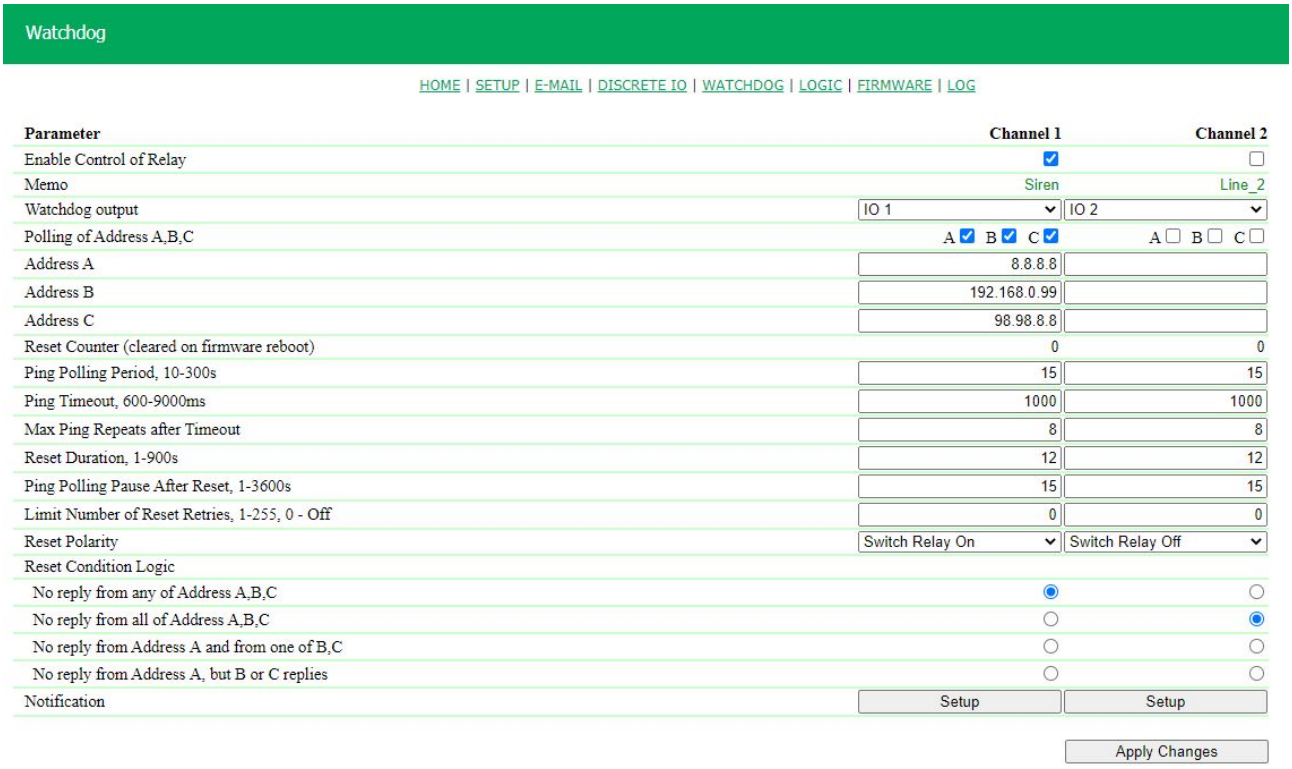
Test It — when you press the «**On**» and «**Off**» buttons the device sends the corresponding requests with the values immediately. They are used to check the operaion of SNMP SETTER.

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.

[ENG] 8.2. [DKSF 561.1.6] «Watchdog»

«Watchdog» — This is a special module that constantly, at a specified frequency, ping the specified addresses (ICMP Echo) using ping. If there is no response, a short-term impulse (change of state) of the relay or the I/O line (in the «output» mode) resets the power supply of the connected device or performs other actions.

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



Enable Control of Relay — check-box that allows the «Watchdog» module to control the output. **Default: off.**

Memo — text description description, filled in the "Memo" field on the page of the managed object. **Default: empty.**

Watchdog output — an IO-line to be controlled by the watchdog.

Polling of Address A, B, C — is a set of checkboxes that allow to specify addresses that are included to polling individually. **Default: all off.**

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

Address A (**B, C**) — fields for configuring addresses for polling. Both the IP address and the domain name can be specified. Up to three addresses can be configured. An empty field disables polling. **Default: all empty.**

Reset Counter (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 if firmware rebooted.

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. **Default: 15 s.**

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**». **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 «no response». 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. **Default: 8.**

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

Ping Polling Pause After Reset, 1-3600s — is a field for setting the time for which the polling is stopped after the reset is completed. **Default: 15 s.**

Limit Number of Consequtive 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. **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 Address A,B,C — if at least one of addresses did not respond.

No reply from all of Address A,B,C — if all requested addresses did not respond.

No reply from Address A and from one of B,C — 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 — 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.

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] 9. [DKSF 561.1.6] How to Update the Firmware of the Device?

In order to update the firware of the device do the following steps:

1. Download an up-to-date firmware from the official website of the company (the «**Downloads**» section): http://www.netpingdevice.com.
2. Go to the «**Firmware**» page of the device web interface. You can easily update the firmware of the 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 the device
5. Click the «**Update Firmware**» button

Wait for the message on the successful operation completion:

Some system settings may be changed after the firmware update. Do not forget to check the parameters important for the operation.

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

Notes

1. If there was an error with the firmware version when you were dragging the file to the specified area of the page, or the file does not contain the .npu extension, the following informational message appears:

2. Before downgrading the built-in version of the firmware of the device there is always an informational message:

We highly recommend you to get in touch with the technical supprt via support@netpingdevice.com before you start the process of downgrading the firmware version.