



[ENG] NetPing SMS, Firmware description

Содержание

[ENG] 1. [DKSF 707.3 IU] Introduction.....	6
About What This Document Is	6
[ENG] 2. [DKSF 707.3 IU] Getting Basic Information about a Device	7
[ENG] 2.1. [DKSF 707.3 IU] How to Know Default IP Address and MAC Address of a Device?	8
[ENG] 2.2. [DKSF 707.3 IU] Connecting to a Web Interface of a Device with a Default Authorization.....	10
Web Interface	10
Authentication	10
[ENG] 2.3. [DKSF 707.3 IU] I Need to Know the Firmware and Hardware Versions, Serial Number and a Model of a Device	12
[ENG] 2.4. [DKSF 707.3 IU] Where Can I See a Hostname, a Location and Contact of a Device?..	13
[ENG] 2.5. [DKSF 707.3 IU] How to Reboot a Device?	14
[ENG] 3. [DKSF 707.3 IU] Basic Configuration	15
[ENG] 3.1. [DKSF 707.3 IU] How to Configure Hostname, Location and Contact of a Device?	16
[ENG] 3.2. [DKSF 707.3 IU] Where to Change the Settings of a Network Interface?.....	17
[ENG] 3.3. [DKSF 707.3 IU] Changing a User Name and a Password.....	19
[ENG] 3.4. [DKSF 707.3 IU] How to Restrict an Access to a Device?	20
[ENG] 3.5. [DKSF 707.3 IU] It Is Necessary to Send SNMP TRAP Notifications. How to Configure This?	21
[ENG] 3.6. [DKSF 707.3 IU] How to Set the Clock?	22
Manual configuration.....	22
Time Synchronization with External NTP Servers.....	22
[ENG] 3.7. [DKSF 707.3 IU] I Want to Configure SYSLOG. How to Do This?.....	24
[ENG] 3.8. [DKSF 707.3 IU] How to Update Firmware of a Device?	25
[ENG] 3.9. [DKSF 707.3 IU] Device Log.....	26
[ENG] 4. [DKSF 707.3 IU] Working with a Built-In GSM Modem	27
[ENG] 4.1. [DKSF 707.3 IU] I Need to Write a Number for Sending SMS Notifications. How Can I Do This?	28
[ENG] 4.2. [DKSF 707.3 IU] How to Enable an Extended Log and Troubleshoot a GSM Modem?..	29
[ENG] 4.3. [DKSF 707.3 IU] Checking a GSM Signal Strength and a Balance on a SIM Card.....	30

[ENG] 4.4. [DKSF 707.3 IU] Receiving SMS Notifications on Previously Specified Events.....	31
[ENG] 4.5. [DKSF 707.3 IU] Limiting Outgoing SMS traffic	32
[ENG] 4.6. [DKSF 707.3 IU] What SMS Commands and SMS Notifications Are Supported by a Device?.....	33
Format of an SMS Command.....	33
Format of an SMS Response	33
SMS Error Notifications.....	34
SMS notifications	35
The informational part of SMS notifications	36
[ENG] 4.7. [DKSF 707.3 IU] How to Know an IMEI of a Built-in GSM Modem?.....	37
[ENG] 5. [DKSF 707.3 IU] Working with Random SMS Notifications	38
[ENG] 5.1. [DKSF 707.3 IU] How to Send Random SMS Notifications?	39
Sending SMS Notifications through a web interface of a device	39
Sending SMS notifications via an SNMP protocol	39
An example of the sequence of steps for sending random SMS through an SNMP using the package NET-SNMP....	40
Sending SMS notifications through third-party web applications (HTTP API)	41
An example of sending random SMS using a JavaScript code	41
An example of sending random SMS using a PowerShell script.....	41
[ENG] 5.2. [DKSF 707.3 IU] Can a Device Receive Random SMS Notifications?.....	43
[ENG] 5.3. [DKSF 707.3 IU] What Notifications Are Represented in SMS Log?.....	44
[ENG] 6. [DKSF 707.3 IU] An Example of Configuring a Gateway of a NetPing SMS for sending SMS Notifications from Other NetPing Devices	45
[ENG] 7. [DKSF 707.3 IU] An Example of Configuring a Gateway of NetPing SMS to Control NetPing Devices using SMS Messages	51
[ENG] 8. [DKSF 707.3 IU] Working with WEBHOOK.....	57
[ENG] 9. [DKSF 707.3 IU] Support of an SNMP Protocol by a Device	59
[ENG] 9.1. [DKSF 707.3 IU] Can I Control a Device Using SNMP?.....	60
Configuring an SNMP Protocol.....	60
[ENG] 9.2 [DKSF 707.3 IU] What OIDs Are Supported by a Device?.....	61
[ENG] 10. [DKSF 707.3 IU] HTTP API Support.....	64
[ENG] 10.1. [DKSF 707.3 IU] GSM Modem Management	65
SMS Sending.....	65
Returned values	65

Balance Request.....	65
Returned values	65
Getting a Response to a Balance Request	65
Returned Values	66
Checking a Status of SMS Sending.....	66
Returned values	66
Example	66
Authorization.....	66



[ENG] NetPing SMS, Firmware description -

[ENG] 1. [DKSF 707.3 IU] Introduction

About What This Document Is

this document describes the functionality of the firmware **DKSF 707.3.X** for a [NetPing SMS](#) device.

A [NetPing SMS](#) device with the firmware **DKSF 707.3.X** supports the next management interfaces:

- HTTP (web interface);
- SNMP v1;
- HTTP API commands;
- SMS

A description of settings and an operation order with these management interfaces are given in this document.

A description of physical specifications, controls, indicators and an order of connecting a device are given in the document «[NetPing SMS, User Guide](#)».

The information, contained in this document, can be changed by a manufacturer without a prior notice. Although every effort was made to make the information in this document accurate and without errors, a manufacturer is not liable for their possible presence and for the consequences that may result from the errors herein. A manufacturer is not liable if supplied equipment, software and this user guide does not correspond to expectations of a user and his/her opinion about where and how to use all the above. All copyrights on supplied devices, described in this User Guide, as well as firmware and software of devices and this User Guide belong to NetPing global Ltd. Copying, replication and translation of this user guide to other languages are not allowed without a prior written permission of a rightholder. Copying, replication, changing, disassembling of provided software are not allowed without a prior written permission of a rightholder. For the part of software that is provided in source codes, there is a separate license agreement, which defines an order of its use and modification. Other trademarks used in this description belong to corresponding rightholders.

Developer and manufacturer:

NetPing east Co Ltd.

[ENG] 2. [DKSF 707.3 IU] Getting Basic Information about a Device

[ENG] 2.1. [DKSF 707.3 IU] How to Know Default IP Address and MAC Address of a Device?

A default IP address is written at the bottom of a device:



A default IP address of a device is 192.168.0.100

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

NetPing SMS
v707.3.3.E-1 / HW 1.0
netping-sms
Taiwan office

Home

HOME

| [SETUP](#) | [GSM SETUP](#) | [SMS LOG](#) | [SEND SMS](#) | [AGENTS](#) | [VARIABLES](#) | [TRAPS](#) | [WEBHOOK](#) | [FIRMWARE](#) | [LOG](#)

DEVICE IDENTIFICATION

Hostname	netping-sms
Location	Taiwan office
Contact	sp@netping.ru
Serial Number	SN: 405 048 521
MAC Address	00:a2:c9:8c:24:18
Device Model	NetPing SMS
Firmware Version	v707.3.3.E-1
Hardware Version	1.0
Uptime	12d 21h 18m 4s

NETWORK SETTINGS

IP Address	192.168.0.29
Netmask	255.255.255.0
Gateway	192.168.0.1

where:

MAC address – is a unique physical address of a device in the Ethernet network.

[ENG] 2.2. [DKSF 707.3 IU] Connecting to a Web Interface of a Device with a Default Authorization

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 an 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**

A screenshot of a dialog box titled "Authentication Required". The text inside reads: "The server http://192.168.0.24:80 requires a username and password. The server says: NetPing 2/PWR-220v3." Below the text are two input fields: "User Name:" followed by an empty text box, and "Password:" followed by an empty text box. At the bottom of the dialog are two buttons: "Log In" and "Cancel".

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] 2.3. [DKSF 707.3 IU] I Need to Know the Firmware and Hardware Versions, Serial Number and a Model of a Device

The information about firmware and hardware versions, a serial number and a model of a device can be browsed on the home page of a device web interface:

The screenshot shows the NetPing SMS web interface. At the top, there is a green header with the text "NetPing SMS" and "Home" on the left, and "v707.3.3.E-1 / HW 1.0 netping-sms Taiwan office" on the right. Below the header is a navigation menu with links: HOME, SETUP, GSM SETUP, SMS LOG, SEND SMS, AGENTS, VARIABLES, TRAPS, WEBHOOK, FIRMWARE, and LOG. The "HOME" link is highlighted with a red box. Below the navigation menu is the "DEVICE IDENTIFICATION" section, which contains a table of device information. The "Serial Number" and "Device Model" rows are highlighted with red boxes. Below the table is the "NETWORK SETTINGS" section, which contains a table of network information. At the bottom right of the network settings section is a "Reboot" button.

DEVICE IDENTIFICATION	
Hostname	netping-sms
Location	Taiwan office
Contact	sp@netping.ru
Serial Number	SN: 405 048 521
MAC Address	00:a2:c9:8c:24:18
Device Model	NetPing SMS
Firmware Version	v707.3.3.E-1
Hardware Version	1.0
Uptime	12d 21h 18m 4s

NETWORK SETTINGS	
IP Address	192.168.0.29
Netmask	255.255.255.0
Gateway	192.168.0.1

where:

Firmware Version – is a current firmware version, installed in a device. It is additionally displayed in headings on all pages of a device web interface.

A number of a firmware version looks like **DKSF PPP.VV.SS.C-M** (for example, DKSF 707.3.3.A-1), where:

- **DKSF** – is a specific prefix for all firmware of Netping Ltd;
- **PPP** – is a device model, for which a firmware is designed. A model number usually but not necessarily coincides with a project number of the hardware platform of a device;
- **VV** – is a version number. Versions are numbered starting from «1». A version number is changed to the next one if the functionality has been substantially changed or extended within the process of development;
- **SS** – is a number of a subversion. A number of a subversion is changed within every firmware update, including error fixes, updating internal modules and optimization;
- **C** – is a character, which represents a type of the firmware version. A is a stable version with a Russian interface, B is a version for testing or the first version of new firmware. E is a stable version with an English interface;
- **M** – is a numeric suffix, which represents a modification (variant) of a device model, for which the firmware is designed

Hardware Version – is a version of a printing board and/or a configuration of this device. It is additionally displayed in headings on all pages of a web interface.

Serial Number – is a unique identification number of a device. It must coincide with a number on a sticker on a device. A serial number of a device cannot be changed.

Device Model – is a model name, which is indicated both on the body of a device and in a web interface.

[ENG] 2.4. [DKSF 707.3 IU] Where Can I See a Hostname, a Location and Contact of a Device?

A hostname, a location, and a contact can be seen at the homepage of a device web interface and browsed using [SNMP](#) protocol:

The screenshot shows the NetPing SMS web interface. At the top, there is a green header with the text "NetPing SMS" and "Home" on the left, and "v707.3.3.E-1 / HW 1.0 netping-sms Taiwan office" on the right. Below the header is a navigation menu with links: HOME, SETUP, GSM SETUP, SMS LOG, SEND SMS, AGENTS, VARIABLES, TRAPS, WEBHOOK, FIRMWARE, and LOG. The "HOME" link is highlighted with a red box. Below the navigation menu is the "DEVICE IDENTIFICATION" section, which contains a table with the following data:

Hostname	netping-sms
Location	Taiwan office
Contact	sp@netping.ru
Serial Number	SN: 405 048 521
MAC Address	00:a2:c9:8c:24:18
Device Model	NetPing SMS
Firmware Version	v707.3.3.E-1
Hardware Version	1.0
Uptime	12d 21h 18m 4s

Below the "DEVICE IDENTIFICATION" section is the "NETWORK SETTINGS" section, which contains a table with the following data:

IP Address	192.168.0.29
Netmask	255.255.255.0
Gateway	192.168.0.1

At the bottom right of the "NETWORK SETTINGS" section, there is a "Reboot" button.

where:

Hostname – is a domain name of a device. It allows distinguishing several NetPing devices of the same type by their names. A hostname is displayed on the homepage and in the heading of a web interface, it is sent in Syslog notifications and is available via SNMP – OID «.1.3.6.1.2.1.1.5.0» (sysName).

Location – is a description of an installation place of a NetPing device. It is displayed on the homepage and in the heading of a web interface and is available via SNMP – OID «.1.3.6.1.2.1.1.6.0» (sysLocation).

Contact – is contact data (usually an e-mail) of an administrator. It is displayed on the homepage of a web interface and is available via SNMP – OID «.1.3.6.1.2.1.1.4.0» (sysContact).

[ENG] 2.5. [DKSF 707.3 IU] How to Reboot a Device?

A NetPing SMS device can be rebooted in two ways:

1. By clicking the button «**Reboot**» on the homepage of a device web interface.

NetPing SMS v707.3.3.E-1 / HW 1.0
netping-sms
Taiwan office

Home

[HOME](#) | [SETUP](#) | [GSM SETUP](#) | [SMS LOG](#) | [SEND SMS](#) | [AGENTS](#) | [VARIABLES](#) | [TRAPS](#) | [WEBHOOK](#) | [FIRMWARE](#) | [LOG](#)

DEVICE IDENTIFICATION

Hostname	netping-sms
Location	Taiwan office
Contact	sp@netping.ru
Serial Number	SN: 405 048 521
MAC Address	00:a2:c9:8c:24:18
Device Model	NetPing SMS
Firmware Version	v707.3.3.E-1
Hardware Version	1.0
Uptime	12d 21h 18m 4s

NETWORK SETTINGS

IP Address	192.168.0.29
Netmask	255.255.255.0
Gateway	192.168.0.1

[Reboot](#)

When clicking the button «**Reboot**» a CPU LED near an Ethernet port will blink. A device will reboot.

2. By using an **SNMP v1** protocol by setting OID values using the command «**Set**»:

OID	Name	Type	Access	Description
.1.3.6.1.4.1.25728.9 11.1.0	npSoftReboot	Integer	READ/WRITE	Software reboot of a device when writing the value «1» (the same as rebooting a device via a web interface)
.1.3.6.1.4.1.25728.9 11.3.0	npForceReboot	Integer	READ/WRITE	Immediate forced reboot of a device when writing the value «1» (processor is reset, the same as when switching a power on)

[ENG] 3. [DKSF 707.3 IU] Basic Configuration

[ENG] 3.1. [DKSF 707.3 IU] How to Configure Hostname, Location and Contact of a Device?

To configure a hostname, a location and a contact of a device, there is a need to go to the page «**SETUP**» of a device web interface:

DEVICE IDENTIFICATION	
Device Hostname (only Latin letters, digits, '-')	netping-sms
Device Location	Taiwan office
Contact	sp@netping.ru

Apply Changes

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

Device Hostname (only Latin letters, digits, '-') – is a domain name of a device. It allows distinguishing several NetPing devices of the same type by their names. A hostname is displayed on the homepage and in the heading of a web interface, it is sent in Syslog notifications and available via SNMP – OID «.1.3.6.1.2.1.1.5.0» (sysName). **On default: empty line**

Device Location – is a description of an installation place of a NetPing device. It is displayed on the homepage and in the heading of a web interface and is available via SNMP – OID «.1.3.6.1.2.1.1.6.0» (sysLocation). **On default: empty line**

Contact – is a contact data (usually, an e-mail) of an administrator. It is displayed on the homepage of a web interface and is available via SNMP – OID «.1.3.6.1.2.1.1.4.0» (sysContact). **On default: empty line**

After configuring all necessary settings click the button «**Apply changes**».

[ENG] 3.2. [DKSF 707.3 IU] Where to Change the Settings of a Network Interface?

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

NETWORK SETTINGS

IP Address	192.168.0.29
Netmask	255.255.255.0
Gateway	192.168.0.1
DNS Server	8.8.8.8
Embedded HTTP Server Port	80
SNMP Agent Port	161

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

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

Netmask – is a field for setting or changing a subnetwork mask, where devices are located. **On default: 255.255.255.0**

Gateway – is a field for setting or changing an IP address of a gateway. Value «**0.0.0.0**» means that a gateway is not specified and packages for all subnetworks will not be sent by a device. **On default: 0.0.0.0**

A device will send all outgoing packages to the gateway address. Therefore, there is a need to specify IP address of a gateway correctly if there is a need to work with a device from other subnetworks.

DNS Server – is a field for setting or changing an address of a DNS server. The value «**0.0.0.0**» means that a DNS server is not specified and a device will not send DNS requests. **On default: 0.0.0.0**

DNS server must support a recursive method of operation. Cyrillic domain names are not supported. Domain names longer than 62 characters are not supported.

DNS module works in parallel and independently from other firmware modules. DNS module stores responses from a DNS server in a DNS-cache of a device. Other firmware modules use this cache to determine an IP address, where there is a need to send a package. Right before sending a package, DNS request is not sent. If there is no corresponding record in a DNS cache at the moment of sending a package, then an outgoing package is discarded. A size of a DNS cache coincides with a number of hostnames (IP addresses) in the settings of a device.

Domain names are expanded and updated in the next cases:

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

When a record is expired, it is not deleted, like in a traditional DNS client on a PC, but it is updated. A device updates an expired record from time to time. Other firmware modules use the old information up to the moment of a successful record update.

If a DNS server does not respond, a device repeats a request three times, afterwards, it switches to the periodic repeating of a request nearly once a minute if there is no response from a server. Requests are repeated if there is no server response and when there is an error in a server response, including the error «no such name».

Embedded HTTP Server Port – is a field for setting or changing a port number, through which a built-in web interface works. When connecting to a device with a port number different from 80 through a web browser, there is a need to indicate a URL of the next appearance: `http://x.x.x.x:nn`, where `x.x.x.x` – is an IP address of a device, `nn` – is a port number indicated in the settings of a device. **On default: 80**

SNMP Agent Port – is a field for setting or changing a number of a UDP port, which is listened by an SNMP agent. **On default: 161**

After configuring all necessary settings, click the button «**Apply changes**».

[ENG] 3.3. [DKSF 707.3 IU] Changing a User Name and a Password

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

ACCESS RESTRICTIONS

Username	visor29
Password	*****
SNMP Community for Read	ping29
SNMP Community for Write	ping29
IP Filter (access granted for this subnet)	0.0.0.0
IP Filter Netmask (0.0.0.0 - disable filter)	0.0.0.0

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

Username – is a field for setting or changing a user name while accessing a device through a web interface. Latin letters, numbers and certain special characters are used. A maximum size is – 16 characters. **On default: visor**

Password – is a field for setting or changing a password when accessing a device via a web interface. Latin letters, numbers and certain special characters are used. A maximum size is – 16 characters. **On default: ping**

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

[ENG] 3.4. [DKSF 707.3 IU] How to Restrict an Access to a Device?

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

ACCESS RESTRICTIONS

Username	visor29
Password
SNMP Community for Read	ping29
SNMP Community for Write	ping29
IP Filter (access granted for this subnet)	0.0.0.0
IP Filter Netmask (0.0.0.0 - disable filter)	0.0.0.0

Apply Changes

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

IP Filter (access granted for this subnet) – is a field that determines an IP address or a subnetwork, from which it is allowed to configure and browse parameters of a device via HTTP and SNMP protocols. A netmask recorded in the field «**IP Filter Netmask**» is applied to the address, specified in the field «**IP Filter**». As a result, there is a subnetwork, from which it is allowed to control a device. To allow access for one IP address, there is a need to indicate a netmask **255.255.255.255** in the field «**IP Filter Netmask**». **On default: 0.0.0.0**

IP Filter Netmask (0.0.0.0 - disable filter) – is a field for setting or changing a filter netmask to access a device. The value «**0.0.0.0**» means that an access filter is disabled. **On default: 0.0.0.0**

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

[ENG] 3.5. [DKSF 707.3 IU] It Is Necessary to Send SNMP TRAP Notifications. How to 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, to which SNMP TRAP notifications will be sent via an SNMP protocol.

SNMP TRAP

SNMP Trap Destination #1	<input type="text"/>
SNMP Trap Destination #2	<input type="text"/>
<input type="button" value="Apply Changes"/>	

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

SNMP Trap Destination #1 – is a field for setting or changing the first address, where SNMP TRAP notifications will be sent. It is acceptable to indicate either IP address or a domain name. An empty field means that SNMP TRAP notifications will not be sent. **On default: address is not specified**

SNMP Trap Destination #2 – is a field for setting or changing the second address, where SNMP TRAP notifications will be sent. It is acceptable to indicate either IP address or a domain name. An empty field means that SNMP TRAP notifications will not be sent. **On default: address is not specified**

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

[ENG] 3.6. [DKSF 707.3 IU] How to Set the Clock?

Manual configuration

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

EMBEDDED CLOCK (RTC)

Current Date and Time	4.08.2016 16:49:33
New Date and Time (14 digits, format DDMMYYYYHHmmSS without spaces, 24h)	<input type="text"/>
<input type="button" value="Set Clock"/>	

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

Current Date and Time – is a field for browsing a current time.

New Date and Time (14 digits, format DDMMYYYYHHmmSS without spaces, 24h) – is a field for the manual setting of new time.

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

Time Synchronization with External NTP Servers

To configure a time synchronization with 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) to a device, according to which a device will set and adjust its internal clock. In total, it is possible to set up to two NTP servers. If the first NTP server is unavailable, then a device will attempt to synchronize time using the second NTP server. A correctness of the setting can be checked by generating an event and viewing the time of its recording in the log file on the page «**LOG**».

NTP SETUP

NTP Server #1	<input type="text" value="ntp.netping.ru"/>
NTP Server #2	<input type="text"/>
Timezone (-12..12)	<input type="text" value="8"/>
Daylight Saving Time (DST)	<input type="checkbox"/>
<input type="button" value="Apply Changes"/>	

In the section «**NTP Setup**» it is possible to configure:

NTP Server #1 – is a field for browsing or changing an address of the first NTP server. It is acceptable to indicate either IP address or a domain name. An empty field disables the function of time synchronization. **On default: address is not set**

NTP Server #2 – is a field for browsing or changing an address of the second NTP server. It is acceptable to indicate either IP address or a domain name. An empty field disables the function of time synchronization. **On default: address is not set**

Timezone (-12..12) – is a field for browsing or changing a local timezone. An integer positive or negative number of shifted hours from UTC is set. **On default: 3**

As NTP servers, it is possible to use NTP servers that are freely available on the Internet, for example:

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

To use NTP servers from the Internet, there is a need to have a correctly set gateway in the settings of a device on the page «**SETUP**» and there is a need to have an Internet access for a device via an NTP protocol.

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

[ENG] 3.7. [DKSF 707.3 IU] I Want to Configure SYSLOG. How to Do This?

Forwarding notifications for a Syslog server is configured on the page «**SETUP**» of a device web interface.

SYSLOG

SysLog Address	<input type="text"/>
Syslog Facility	<input type="text" value="16"/>
Syslog Severity	<input type="text" value="5"/>
<input type="button" value="Apply Changes"/>	

In the section «**Syslog**» it is possible to configure:

SysLog Address – is an IP address of a Syslog server. A log file of a device on the page «**LOG**» of a device web interface will be completely duplicated on a Syslog server.

Syslog Facility – is a type of software, for which logging is performed.

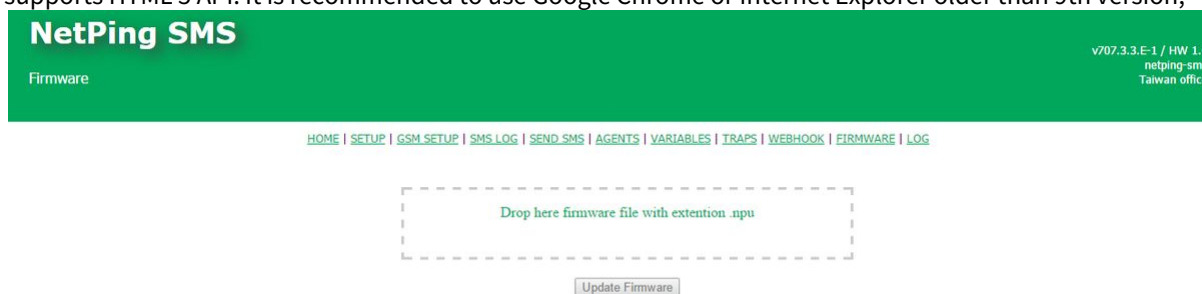
Syslog Severity – a significance level of notifications is indicated (from emergency to debugging).

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

[ENG] 3.8. [DKSF 707.3 IU] How to Update Firmware of a Device?

To update a firmware version, there is a need to:

1. Download an actual firmware (file with the extension .npu) from the official website of the company (the section «[Documentation and files](#)»);
2. Go to the page «**FIRMWARE**» of a device web interface. By using this page it is possible to update the firmware of a device without using special software. To do this, there is a need to have a browser that supports HTML 5 API. It is recommended to use Google Chrome or Internet Explorer older than 9th version;



3. Drag a file with the firmware to the indicated area of the page;
4. Wait for the software to copy to a device;
5. Click the button «**Update Firmware**»

A message about a successful completion of the operation is represented below:



Repeat an attempt if the process of updating was interrupted. A web interface (pages «**HOME**», «**SETUP**», «**FIRMWARE**») will be available even after unsuccessful firmware update.

Certain system settings may be changed after a firmware update. Do not forget to check parameters that are important for the operation.

[ENG] 3.9. [DKSF 707.3 IU] Device Log

A page «**LOG**» of a web interface represents the operation of a device. Events of a device are recorded in a system log in a chronological order. All notifications of a log are duplicated by a Syslog protocol, if in the settings of a device an IP address of a Syslog server is specified.

The first time tag in a log is 01.01.70 Mon 00:00: 00.UTC. If an IP address of an NTP server is specified in the settings of a device, a device will attempt to get a precise time. If successful, it will synchronize its internal clock with a precise time. After a time synchronization, two records will appear in the log, which represent a time jump while resetting the clock to a precise time. If the time received from a synchronization with an NTP server is different from the time of an internal clock for more than 5 minutes, the clock will not be reset. A pace of internal clock will be changed in the way to make an internal time the same as a precise time, received from an NTP server. Thanks to this process, there is no time jump in the event list of a system log.

NetPing SMS v707.3.3.E-1 / HW 1.0
netping-sms
Taiwan office

Log (Events And Messages)

[HOME](#) | [SETUP](#) | [GSM SETUP](#) | [SMS LOG](#) | [SEND SMS](#) | [AGENTS](#) | [VARIABLES](#) | [TRAPS](#) | [WEBHOOK](#) | [FIRMWARE](#) | **LOG**

```
22.07.16 Fr 18:14:55.453 modem [7]: 'TTTT'
22.07.16 Fr 18:14:55.454 SMS debug: waiting final result code
22.07.16 Fr 18:14:55.604 AT cmd [7]:'ATE0
'
22.07.16 Fr 18:14:57.608 AT cmd [7]:'ATE0
'
22.07.16 Fr 18:14:57.832 modem [7]: '
OK
'
22.07.16 Fr 18:14:57.833 AT cmd [7]:'AT
'
22.07.16 Fr 18:14:58.063 modem [8]: '
OK
'
22.07.16 Fr 18:14:58.064 AT cmd [8]:'AT+cmee=2
'
22.07.16 Fr 18:14:58.298 modem [9]: '
OK
'
22.07.16 Fr 18:14:58.299 AT cmd [9]:'AT+CMGF=0;+CSCS="UCS2";+CNMI=1,1
'
22.07.16 Fr 18:14:58.538 modem [10]: '
+CME ERROR: SIM not inserted
'
22.07.16 Fr 18:14:58.543 SMS function is stopped. Unrecoverable error!
```

© 2016 Netping East Co. Ltd

[ENG] 4. [DKSF 707.3 IU] Working with a Built-In GSM Modem

[ENG] 4.1. [DKSF 707.3 IU] I Need to Write a Number for Sending SMS Notifications. How Can I Do This?

To specify one or several phone numbers for sending SMS notifications, there is a need to go to the page «**GSM SETUP**» of a device web interface:

[HOME](#) | [SETUP](#) | **[GSM_SETUP](#)** | [SMS_LOG](#) | [SEND_SMS](#) | [AGENTS](#) | [VARIABLES](#) | [TRAPS](#) | [WEBHOOK](#) | [FIRMWARE](#) | [LOG](#)

SMS NOTIFICATION DESTINATIONS AND SMS COMMANDS SOURCES

	Notify	Commands	Memo	Mobile Number
Mobile Number for SMS, Main	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Employee 1	+79129876542
Mobile Number for SMS, Aux 1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Employee 2	+79128765432
Mobile Number for SMS, Aux 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Employee 3	+79127654321
Mobile Number for SMS, Aux 3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Employee 4	+79126543210
Unrestricted Mobile Number		<input type="checkbox"/>		

Apply Changes

In the section «**GSM SETUP**», there is a need to indicate primary and auxiliary phone numbers if necessary for sending SMS notifications.

Memo — convenient description of a phone number to identify its owner simply.

Mobile numbers — is indicated in the format: **Country_CodeOperator's_CodePhone_Number**, for example, +79127894561, where +7 is a country code, 912 is an operator's code, and 7894561 is a destination number.

In addition, in this section, it is possible to switch on sending notifications for each mobile number separately and allow receiving commands through SMS. Checkboxes «**Notify**» and «**Commands**» are used for this.

«**Notify**» — checkboxes allow sending notifications to the specified mobile number.

«**Commands**» — checkboxes allow receiving commands from the specified mobile number. If a checkbox «Unrestricted Mobile Number» is checked, SMS-commands are received from any mobile number without restrictions.

To save phone numbers click the button «**Apply changes**».

[ENG] 4.2. [DKSF 707.3 IU] How to Enable an Extended Log and Troubleshoot a GSM Modem?

An extended log for a GSM modem is enabled on the page «**GSM SETUP**» of a device web interface in the section "**GSM Modem Troubleshooting**":

GSM MODEM TROUBLESHOOTING

Log Communication with GSM Modem (Troubleshooting) <input checked="" type="checkbox"/>
Last error of GSM modem (hit F5 to refresh)

In the section «**GSM SETUP**», there is a need to check a checkbox «**Log Communication with GSM modem (Troubleshooting)**».

Log Communication with GSM modem (Troubleshooting) – is a function, which will display the information on all AT commands, which are exchanged by CPU and a GSM modem, if enabled in a system log of a device (a page «**LOG**» of a web interface). This functionality is necessary to diagnose possible problems of functioning of a GSM Modem.

Last error of GSM modem - last error of the modem. To represent an actual error, there is a need to click F5 on a keyboard.

Restart GSM — restarting a GSM-modem.

Test SMS — sending a test SMS to the numbers specified in the section «**Destination numbers for SMS-notifications, sources of SMS-commands**», with checked checkboxes «**Notify**»..

To save the setting, click the button «**Apply changes**» (true only for the extended log).

[ENG] 4.3. [DKSF 707.3 IU] Checking a GSM Signal Strength and a Balance on a SIM Card

To check a registration, a level of a GSM signal and a balance on a SIM card, there is a need to go to the page «**GSM SETUP**» of a device web interface:

GSM MODEM STATUS

Registration in GSM Network	Registered in Home Network
GSM Signal Strength	91%

USSD REQUEST

USSD Command for request of GSM Account status	<input type="text" value="*100#"/>
Reply on USSD Request	-

In the section «**GSM STATUS**» there is a need to click the button «**Request Status**». Several seconds later the information about a cell network, where a SIM card is registered will appear in the field «**Registration in GSM Network**». In the field «**GSM Signal Strength**», the information about signal strength in percents will appear.

In the section «**GSM SETUP**» there is a need to indicate a USSD code for requesting a balance of a SIM card.

USSD Command (Request of GSM Account Status etc.) – is a code of the USSD command for requesting a balance.

In the section «**USSD COMMAND**», there is a need to click the button «**Send USSD Request**». Several seconds later the information about a balance on a SIM card will appear in the field «**Response to the USSD**».

In addition, it is possible to request balance using HTTP API, more information is given in the section "[GSM Modem Management](#)".

[ENG] 4.4. [DKSF 707.3 IU] Receiving SMS Notifications on Previously Specified Events

To configure SMS notifications on previously specified events there is a need to go to the page «**GSM SETUP**» of a device web interface:

SMS NOTIFICATIONS

Ethernet link status change	<input type="checkbox"/>
Pinger status change	<input checked="" type="checkbox"/>

In the section «**SMS Notifications**», there is a need to configure the next parameters:

Pinger status change – when a connection with a polled node in the network fails and restores, an SMS notification will be sent to phone numbers, specified on the page «**GSM SETUP**» of a device web interface. In the section «**Pinger**» on the page «**GSM SETUP**» in the field «**Address to poll with ping**» it is possible to know the IP address or a DNS name to check the accessibility of a node and a polling period in the field «**Period, s (30-9999)**»:

Ethernet link interface switching on and off – in the latest firmware version, a checkbox is inactive, and there is no feature of sending notifications on switching on and switching off a link of the Ethernet interface.

PINGER

Address to poll with ping	<input type="text" value="193.168.0.1"/>
Period, s (30-9999)	<input type="text" value="30"/>

Parameters of the operation of the module «**Pinger**» on the page «**GSM SETUP**»:

1. Polling of an indicated IP address or a DNS name of a node starts once in a specified period of time (parameter «**Period, s (30-9999)**»);
2. Period of waiting for a response from a polled network node is 2 seconds;
3. A number of repeats of polling a tested node in a network is 8;
4. If there is no response from a tested node in a network for 8 repeats, «**Pinger**» informs that there is no connection with a specified node;
5. If there is a response from a tested node at the next polling period, «**Pinger**» informs that there is a connection with an indicated IP address or a DNS name.

It is possible to learn about how to specify phone numbers for sending SMS notifications from the section «[4.1. \[DKSF 707.3 IU\] I Need to Write a Number for Sending SMS Notifications. How Can I Do This?](#)».

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

[ENG] 4.5. [DKSF 707.3 IU] Limiting Outgoing SMS traffic

Firmware version DKSF 707.3.8 and up have a feature of controlling the outgoing SMS traffic. Setup of the limits is available at the page «**GSM SETUP**» in the section «**LIMITING OF OUTGOING SMS TRAFFIC**»:

LIMITING OF OUTGOING SMS TRAFFIC

Antispam, ~120 SMS messages per hour	<input checked="" type="checkbox"/>
Monthly Limit of Outgoing SMS (0..1000000)	10000
Monthly Counter of Outgoing SMS (fragments)	8

Antispam, ~120 SMS messages per hour — a checkbox that enables an hourly antispam limit. Outgoing SMS is limited using the «[Token bucket](#)» algorithm. Deviation of 1-2 SMS is allowed. **On default: Checkbox is checked.**

Monthly Limit of Outgoing SMS — is a number that limits the monthly number of outgoing SMS. It is linked to the date on a device. **On default: 10000.**

Monthly Counter of Outgoing SMS (fragments) — is a number of sent SMS during a current calendar month.

In the text, SMS fragments are considered «SMS».

To save the changes in the configurations, there is a need to click the button «**Apply changes**».

[ENG] 4.6. [DKSF 707.3 IU] What SMS Commands and SMS Notifications Are Supported by a Device?

NetPing SMS can receive various SMS commands and send SMS notifications at different events. Notifications are sent to phone numbers, indicated on the page «**GSM SETUP**» of a device web interface.

Format of an SMS Command

Requesting a value of an SNMP variable (SNMP GET request):

```
np snmp variable? password
```

Setting an SNMP variable (SNMP SET command):

```
np snmp variable=value password
```

where:

np snmp – is a prefix of a command;

variable – is a short name for an SNMP variable, specified on the page «**VARIABLES**» of a device web interface;

value – is a value for recording in an SNMP variable. Only integer numbers are supported. It is acceptable to indicate a textual value from a dictionary;

password – is a value of a parameter «**Community**», which is indicated on the page «**SETUP**» of a web interface of any NetPing device

Between a variable and a character «?» there must be no spaces and around the character «=» there must be no spaces. A text of command is case insensitive, therefore it is possible to use lowercase and uppercase Latin letters. Elements of a command are separated by spaces. It is not acceptable to use the characters «'» (apostrophe), «"» (quote), «@», «_» (underline). Including these characters can cause a firmware failure. Executing a command is confirmed by a response message (see below).

Format of an SMS Response

A response for requesting the value of an SNMP variable is as follows:

```
NP SNMP REPLY variable=value
```

A response to installing an SNMP variable is as follows:

```
NP SNMP DONE variable=value
```

where:

variable – is a short name of an SNMP variable, which is set on the page «**VARIABLES**» of a device web interface;

value – is a value of an SNMP variable and its description from a dictionary (if applicable)

Examples of response messages:

NP SNMP DONE heater=off(0)

NP SNMP REPLY t4=28

SMS Error Notifications

A password parameter in an SMS command does not correspond to the value «**Community**» on the page «**SETUP**» of a web interface of a NetPing device. A password is checked case-sensitively:

NP SNMP ERR Wrong password, access denied

A <variable> lacks in the table of SNMP variables on the page «**VARIABLES**» of a device web interface:

NP SNMP ERR Unknown variable '<variable>'

A <variable> links to the host that is missing in the table of hosts (agents) on the page «**AGENTS**» of a device web interface:

NP SNMP ERR Unknown agent '<host>' for var '<variable>'

A device was not able to get an IP address of an agent according to its domain name <fqdn>:

NP SNMP ERR DNS failed for '<fqdn>'

Receiving an IP address is not completed, maybe a DNS server does not know such host.

A procedure of defining IP addresses for a domain name is started when saving any changes in the table of hosts (agents) on the page «**AGENTS**» of a device web interface. I.e. IP addresses are determined beforehand for all hosts recorded in the table and are stored as a reserve. A repeated request is made when a life period of a record in a DNS cache is over.

There is no response from <fqdn_or_ip> after three attempts to execute an SNMP operation. A timeout for executing an SNMP operation is 2 seconds:

NP SNMP ERR No reply for '<variable>' from '<fqdn_or_ip>'

A field <snmp error> is displayed on the basis of an error code from an SNMP reply PDU:

NP SNMP ERR Reply '<snmp error>' for '<outgoing operation>'

A field <snmp error> can have the next appearance:

- Too big data – too big request, there are no resources for processing it;

- No such OID 'id' – agent has no such OID;
- Bad value – the value cannot be recorded into OID, or its type or size do not match;
- Read only – an agent refuses to record;
- Unknown error – other errors

For example:

NP SNMP ERR Reply 'Read only' for 'temp4=25'

An error appears when attempting to read a non-integer value. At the moment it is possible to read only integer values:

NP SNMP ERR Non-integer value returned for '<variable>'

where:

<variable> – is a short name of a variable, indicated in an SMS command

A <value>, indicated in an SMS command variable=value cannot be interpreted as an integer number, and it was not successful to find a match for this value in a dictionary for a variable if a text value has been set:

NP SNMP ERR Bad value '<value>' in sms

Named values (dictionary) are set in the table of variables on the page «**VARIABLES**» of a device web interface.

An example of a dictionary:

flip(-1), off(0), on(1), unknown(255)

An error when a device reads a command. Most probably a text of an outgoing command is incorrect:

NP WRONG CMD: "outgoing command"

where:

Outgoing command – is a text of an outgoing SMS command, which is completely quoted.

SMS notifications

SMS notifications look like the next:

np_name (q) information

where:

np_name – is the name of a device for identification of SMS notifications. It is set on the page «**SETUP**» of a device web interface. If the name of a device is not specified, then a name «NETPING» is used;

q – is a serial number of notifications. The number is nonvolatile – it is not zeroed when a power supply is interrupted. It is used to register missed (lost) notifications;

Information – is an informational part of SMS notifications

The informational part of SMS notifications

A notification about losing and restoring the connection of a tested network node (see the module «**Pinger**» on the page «**GSM SETUP**» of a device web interface):

PINGER STATUS: OK (IP/HOST)
PINGER STATUS: FAILED (IP/HOST)

[ENG] 4.7. [DKSF 707.3 IU] How to Know an IMEI of 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

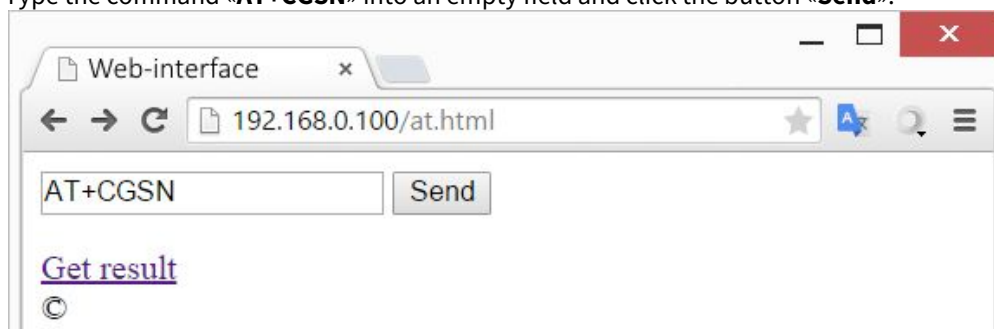
where:

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] 5. [DKSF 707.3 IU] Working with Random SMS Notifications

[ENG] 5.1. [DKSF 707.3 IU] How to Send Random SMS Notifications?

Sending SMS Notifications through a web interface of a device

Long SMS notifications are fragmented into several SMS notifications of standard length, which increases the cost of sending them.

If only Latin letters and numbers are used in SMS, one fragment can reach 160 symbols in length. A length of a fragment for notifications using Cyrillics cannot exceed 70 characters.

To send random SMS through a device web interface, there is a need to go to the page «**SEND SMS**»:

The screenshot displays the 'Send SMS' web interface. At the top, there's a green header with 'NetPing SMS' and 'Send SMS'. A navigation bar contains links: HOME, SETUP, GSM SETUP, SMS LOG, SEND SMS (highlighted), AGENTS, VARIABLES, TRAPS, WEBHOOK, FIRMWARE, LOG. Below this is a table with two columns: 'Tel. Number' and 'Name'. The table has several rows, each with a checkbox on the left and an 'X' button on the right. Below the table, there's a 'Save Phonebook' button. A text input field is provided for the message, with a 'Send SMS' button below it. The footer shows '© 2016 Netping East Co. Ltd.'

1. In columns «**Tel. Number**» and «**Name**» write one or several numbers with comments and click the button «**Save Phonebook**». To remove a number from a local memory of a web browser and click the button «**X**» on the right from the name;

Phone numbers are not saved in the memory of a device. Phone numbers are saved in a user's profile of a web browser. Because of this, every user at every computer has her own phonebook.

2. Check a checkbox with a necessary number from a phonebook of a web browser to send an SMS notification;
3. In a corresponding field write a text of SMS notification.
4. Send SMS by clicking the button «**SendSMS**»

Sending SMS notifications via an SNMP protocol

To send random SMS using an SNMP protocol, there is a need to use the OID «.1.3.6.1.4.1.25728.3800.1.9.0» («**npGsmSendSms**»), in «**npGsmSendSms**» a destination phone number is recorded as well as a text of SMS notification. To do this, see the MIB file, which can be downloaded from the page of a description of a device, the section «[Documentation and files](#)».

OID	Name	Type	Access
.1.3.6.1.4.1.25728.3800.1.9.0	npGsmSendSMS	DisplayString	READ/WRITE

A format of a random SMS notification:

```
[phone_number,phone_number,...] Message
```

where:

phone_number – is a destination number in square brackets, it is indicated in the format: **Country_codeOperator's_codePhone_number**;

Message – is a text of a message (is separated from a destination number by the space)

It is possible to send an SMS notification to up to four destination numbers, having indicated them in square brackets separated by a comma without spaces. If destination addresses are not indicated at all, an SMS will be sent to the numbers specified in the settings on the page «**GSM SETUP**» of a device web interface.

An example of the sequence of steps for sending random SMS through an SNMP using the package NET-SNMP

1. To send a random SMS, there is a need to use a special package **NET-SNMP**. To do this, there is a need to download a distributive of a package **NET-SNMP** from the section «Download» from the website: <http://net-snp.sourceforge.net/download.html>

2. After installing the package **NET-SNMP**, run the utility **snmpset.exe** in a command line. To run a command line, there is a need to use a combination of the keys «**Windows+L**». After the window «**Run**» is opened, enter a command «**cmd**» and click the button «**Enter**». Then in a command line, go to the directory of installation of the utility **snmpset.exe**:

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\eremeev>cd "C:\Program Files (x86)\net-snp\usr\bin"
C:\Program Files (x86)\net-snp\usr\bin>_
```

3. Run the utility **snmpset.exe** with the next parameters of a command line:

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

where:

COMMUNITY – is a special code word, which is installed on the page «**SETUP**» of a device web interface. On default, in devices NetPing community=SWITCH;

IP – is an IP address of a NetPing device;

OID – is an SNMP identifier of a variable «**npGsmSendSms**», which is used for sending a random SMS notification;

TYPE – is a type of a recorded value of an SNMP identifier of a variable. Symbols of types are given on the picture:

```
i: INTEGER, u: unsigned INTEGER, t: TIMETICKS, a: IPADDRESS
o: OBJID, s: STRING, x: HEX STRING, d: DECIMAL STRING, b: BITS
U: unsigned int64, I: signed int64, F: float, D: double
```


VALUE – is a recorded value, i.e. a destination number/numbers and a text of an SMS message

According to the description given above, a command to send a random SMS using the utility **snmpset.exe** is as follows:

```
C:\Program Files (x86)\net-snmplib\usr\bin>snmpset.exe -v 1 -c SWITCH 192.168.0.100
.1.3.6.1.4.1.25728.3800.1.9.0 s "[+7913000000] Hello! Test SMS!"
```

4. After a successful completion of a command, the next response must be sent:

```
SNMPv2-SMI::enterprises.25728.3800.1.9.0 = STRING: "[+7913000000] Hello! Test SMS!"
```

Sending SMS notifications through third-party web applications (HTTP API)

An example of sending random SMS using a JavaScript code

To send random SMS through third-party web applications, it is possible to use the next JavaScript code:

```
var r = new XMLHttpRequest();
r.open('POST', 'http://192.168.0.100/sendsms.cgi?utf8', true, 'visor', 'ping'); // visor:ping – user name
and a password
r.withCredentials = true;
r.send('[+7913000000] Houston, we have a problem!');
```

where:

192.168.0.100 – is an IP address of a NetPing device;

visor – is a username for connecting to a web interface of a NetPing device;

ping – is a password for connecting to a web interface of a NetPing device

It is possible to send an SMS notification to up to four destination numbers, having indicated their phone numbers in square brackets separated by a comma, without spaces. If destination phone numbers are not specified at all, an SMS will be sent to the numbers specified in the settings on the page «**GSM SETUP**» of a device web interface.

If a format of data is right, the next JavaScript code will be returned as a result:

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

A result of sending a message does not influence a returned CGI ([Common Gateway Interface](#)) response. CGI only initiates sending a message.

An example of sending random SMS using a PowerShell script

To send SMS through third-party web applications, it is possible to use the next PowerShell script:

```
$url = "http://192.168.137.100/sendsms.cgi?utf8"
$username = "visor"
$password = "ping"
$reqBody = "[+7913000000] Test message"
```

```
$req = [System.Net.WebRequest]::Create($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 – is a variable, which is set as a URL address of a NetPing device with a script for sending random SMS messages.

\$username – is a variable, which is set as a username for authorizing on a NetPing device.

\$password – is a variable, which is set as a password for authorization on a NetPing device.

\$reqBody – is a variable, which is set as a destination number in square brackets, and is indicated in a format: **Country_CodeOperator_CodePhone_Number** and a text of an SMS message (it is separated from a destination number by the space).

It is possible to send an SMS message to up to four destination numbers, having indicated their phone numbers in square brackets separated by a comma without spaces. If destination numbers are not specified at all, an SMS will be sent to numbers that are set in the settings on the page «**GSM SETUP**» of a device web interface.

[ENG] 5.2. [DKSF 707.3 IU] Can a Device Receive Random SMS Notifications?

NetPing SMS allows receiving random SMS notifications, convert and send them as SNMP TRAP notifications to IP addresses, indicated in the section «**SNMP TRAP**» on the page «**SETUP**» of a device web interface. An example of such SNMP TRAP notifications can be seen below:

Description	Source	Time	Severity
trapOID: .1.3.6.1.4.1.25728.3800.2.0.2	95.171.4.109	2016-06-10 13:03:51	
<p>Source: 95.171.4.109 Timestamp: 71 hours 20 minutes 25 seconds SNMP Version: 2</p> <p>Trap OID: .1.3.6.1.4.1.25728.3800.2.0.2</p> <p>Variable Bindings:</p> <hr/> <p>Name: .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 Value: [TimeTicks] 71 hours 20 minutes 25 seconds (25682567)</p> <hr/> <p>Name: snmpTrapOID Value: [OID] .1.3.6.1.4.1.25728.3800.2.0.2</p> <hr/> <p>Name: .1.3.6.1.4.1.25728.3800.1.10.0 Value: [OctetString] Test SMS to SNMP TRAP 03</p> <hr/> <p>Name: .1.3.6.1.4.1.25728.3800.1.11.0 Value: [OctetString] 79059</p> <hr/> <p>Description:</p>			

where:

Source – is an IP address of a [NetPing SMS](#);

Trap OID – is an identifier of an SNMP TRAP notification;

SNMP Version – is a version of an SNMP protocol;

Variable Bindings – are variables, contained in the SNMP TRAP notification: an operation time of a [NetPing SMS](#), a text of a received SMS notification and a sender's phone number. Encoding Windows-1251.

In addition, a text of random SMS notifications is displayed on the pages «**SMS LOG**» and «**LOG**» of a device web interface.

[ENG] 5.3. [DKSF 707.3 IU] What Notifications Are Represented in SMS Log?

A page «**SMS LOG**» of a web interface represents random incoming (RX) and outgoing (TX) SMS notifications (including those initiated for sending by accepted SNMP TRAP) that are recorded in chronological order.

The first time tag in a log is 01.01.70 Mon 00:00: 00.UTC. If an IP address of an NTP server is specified in the settings of a device, then a device will attempt to get a precise time. If successful, it will synchronize its internal clock with a precise time of an NTP server.

NetPing SMS

Log of SMS Messages

[HOME](#) | [SETUP](#) | [GSM SETUP](#) | SMS LOG | [SEND SMS](#) | [AGENTS](#) | [VARIABLES](#) | [TRAPS](#) | [WEBHOOK](#) | [FIRMWARE](#) | [LOG](#)

```

User-Agent: curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.15.3 zlib/1.2.3 libidn/1.18 libssh2/1.4.2
Host: 192.168.0.29
Accept: */*
Content
23.07.15 16:38 [TX +66953345975] NetPing 2PWR-220v2SMS: ping is PROBLEMb3IyOTpwaW5nMjk=
User-Agent: curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.15.3 zlib/1.2.3 libidn/1.18 libssh2/1.4.2
Host: 192.168.0.29
Accept: */*
Content
23.07.15 16:40 [TX +66953345975] NetPing 2PWR-220v2SMS: ping is OK dmlzb3IyOTpwaW5nMjk=
User-Agent: curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.15.3 zlib/1.2.3 libidn/1.18 libssh2/1.4.2
Host: 192.168.0.29
Accept: */*
Content
27.07.15 14:25 [RX +886982043687] >> 0982043687 ??????07/27 14:25????????????????
27.07.15 15:02 [TX +66953345975] NetPing 2PWR-220v2SMS: ping is PROBLEMb3IyOTpwaW5nMjk=
User-Agent: curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.15.3 zlib/1.2.3 libidn/1.18 libssh2/1.4.2
Host: 192.168.0.29
Accept: */*
Content
28.07.15 15:31 [TX +66953345975] NetPing 2PWR-220v2SMS: ping is OK dmlzb3IyOTpwaW5nMjk=
User-Agent: curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.15.3 zlib/1.2.3 libidn/1.18 libssh2/1.4.2
Host: 192.168.0.29
Accept: */*
Content
28.07.15 16:04 [TX +66953345975] NetPing 2PWR-220v2SMS: ping is PROBLEMb3IyOTpwaW5nMjk=
User-Agent: curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.15.3 zlib/1.2.3 libidn/1.18 libssh2/1.4.2
    
```

© 2016 Netping East Co. Ltd

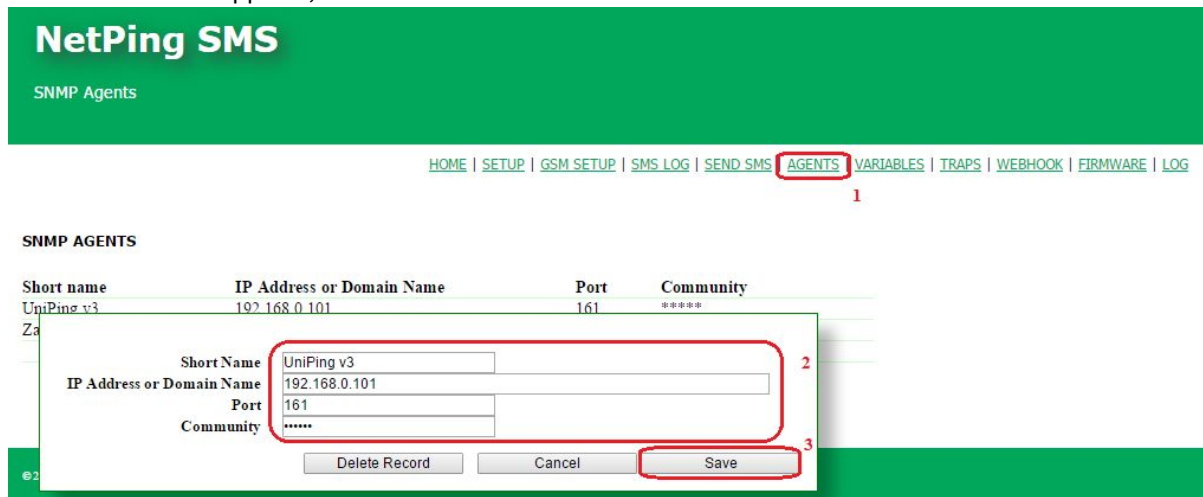
[ENG] 6. [DKSF 707.3 IU] An Example of Configuring a Gateway of a NetPing SMS for sending SMS Notifications from Other NetPing Devices

To receive SMS notifications from NetPing devices, which have a built-in GSM modem, there is a need to configure a [NetPing SMS](#) gateway as follows:

1. Go to the tab «**AGENTS**» of a device web interface. Agent is a device, which is controlled and polled via an SNMP protocol. When receiving SNMP TRAP notifications from an agent, [NetPing SMS](#) sends SMS notifications to specified phone numbers;
2. Add a new agent. To do this, there is a need to click the field «**click here to add new data**»:



In the window that appears, add:



where:

- Short Name** – is the name of an agent, which will be used in the rule for processing SNMP TRAP on the page «**TRAPS**». It can contain no more than 15 Latin letters. It is prohibited to use spaces. **On default: empty line**
- IP Address or Domain Name** – is an IP address/name of an agent, where SNMP SET commands and SNMP GET requests will be sent. In the example, an IP address of a UniPing v3 device, which is in the same local network with a [NetPing SMS](#) gateway. It can be no more than 62 characters. **On default: empty line**
- Port** – is a UDP port of an agent, where an SNMP message will be sent. **On default: 161**

Community – is used in SNMP packages. It must coincide with the Community, specified in the agent. **On default: empty line**

To remove an agent, there is a need to click it and click the button «**Delete record**» in the window that appears. To change parameters of an agent, there is a need to click the agent, edit parameters and click the button «**Save**» in the window that appears. To cancel the action, click the button «**Cancel**»;

3. On the tab «**GSM SETUP**» set phone numbers for sending SMS notifications:

[HOME](#) | [SETUP](#) | **[GSM SETUP](#)** | [SMS LOG](#) | [SEND SMS](#) | [AGENTS](#) | [VARIABLES](#) | [TRAPS](#) | [WEBHOOK](#) | [FIRMWARE](#) | [LOG](#)

1

SMS NOTIFICATION DESTINATIONS AND SMS COMMANDS SOURCES

2

	Notify	Commands	Memo	Mobile Number
Mobile Number for SMS, Main	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Employee 1	+79129876542
Mobile Number for SMS, Aux 1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Employee 2	+79128765432
Mobile Number for SMS, Aux 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Employee 3	+79127654321
Mobile Number for SMS, Aux 3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Employee 4	+79126543210
Unrestricted Mobile Number	<input type="checkbox"/>	<input type="checkbox"/>		

3

Apply Changes

4. On the page «**TRAPS**» of a web interface, there is a need to set rules for processing SNMP TRAP notifications. TRAP is an SNMP notification, which is generated by a device (an agent) when any event appears. [NetPing SMS](#) can receive traps, process them and send corresponding SMS notifications on their basis. An SNMP TRAP notification contains a message identifier (snmpTrapOID) and a set of variables. A rule includes a host source (an agent), snmpTrapOID, and a text of SMS notification. When receiving an SNMP TRAP, [NetPing SMS](#) searches a suitable rule, which has the source address and a snmpTrapOID identifier the same as the received ones. If there is a suitable rule, then an SMS notification with the text specified in the rule will be sent to all phone numbers specified on the page «**GSM SETUP**». The text can have values of variables from the body of a trap. To add a rule for processing SNMP TRAP, there is a need to click the last (empty) line of a table. A form for adding a new rule will appear on a screen. A maximum number of rules is 32:

NetPing SMS

SNMP Traps

[HOME](#) | [SETUP](#) | [GSM SETUP](#) | [SMS LOG](#) | [SEND SMS](#) | [AGENTS](#) | [VARIABLES](#) | **TRAPS** | [WEBHOOK](#) | [FIRMWARE](#) | [LOG](#)

1

SNMP TRAPS

Source Agent	snmpTrapOID	SMS Text
UniPing	.1.3.6.1.4.1.25728.8900.2.0.1	IO{npIoTrapLineN}: {npIoTrapMemo} ({npIoTrapLevelIn}) {npIoTrapLevelLegend}
Netping_IO_v2	1.3.6.1.4.1.25728.8900.2.1.0	netping p1={.1.3.6.1.4.1.25728.8900.2.2.0} switch
UniPing	.1.3.6.1.4.1.25728.8800.2.0.1	{npThermoTrapSensorN} {npThermoTrapMemo} {npThermoTrapValue} {npThermoTrapStatus}

[click here to add new data](#)

Source Agent

Trap of NetPing

Arbitrary snmpTrapOID

SMS Text

UniPing v3

npThermoTrap - thermo sensor trap

Varbinds of npThermoTrap

npThermoTrapSensorN + thermo sensor number (1..8)

npThermoTrapValue + current temperature, °C

npThermoTrapStatus + sensor status

failed(0) - error, low(1) - below safe range, norm(2) - in safe range, high(3) - above safe range

npThermoTrapLow + lower margin of safe range, °C

npThermoTrapHigh + upper margin of safe range, °C

npThermoTrapMemo + sensor memo (type DisplayString)

where:

Source Agent – is a drop-down list that contains a list of agents, configured on the page «**AGENTS**»;

Trap of NetPing – is a drop-down list that contains a list of traps that are sent by NetPing devices. It is used to make configuring easier. **On default: empty line**

Arbitrary snmpTrapOID – is a random identifier of a trap, which has to be processed. **On default: empty line**

SMS Text – is a text of an SMS notification, which will be sent if a snmpTrapOID and a source host of an SNMP TRAP package coincide with the ones indicated in a rule. A value of a variable from an SNMP TRAP package can be included in a text of an SMS message. To add a value of a variable, there is a need to add a name of a variable in a text of an SMS, by enclosing a variable name into braces {}. When receiving an SNMP TRAP package, values of variables can be inserted according to an OID text name. Before sending an SMS notification, a device will replace all names of variables in braces by values of these variables. A text of an SMS notification may contain Latin and Russian letters and numbers (default GSM alphabet).

- To encode values of the current status of parameters in a text of SMS notification, it is necessary to adjust variables. To do this, there is a need to go to the page «**VARIABLES**» of a device web interface and click the field «**click here to add new data**»:

NetPing SMS

SNMP Variables

[HOME](#) | [SETUP](#) | [GSM SETUP](#) | [SMS LOG](#) | [SEND SMS](#) | [AGENTS](#) | VARIABLES | [TRAPS](#) | [WEBHOOK](#) | [FIRMWARE](#) | [LOG](#)

SNMP VARIABLES ACCESSIBLE VIA SMS

Short Name	OID	Agent	Dictionary
PWR1 on SPWR	.1.3.6.1.4.1.25728.5500.5.1.2.1	Netping	ON(1), OFF(0)
npIoTrapLineN	.1.3.6.1.4.1.25728.8900.2.1.0	Netping_IO_v2	
npIoLevelIn.1	.1.3.6.1.4.1.25728.8900.1.1.2.1	UniPing	Close(0), Open(1)
npIoLevelIn.2	.1.3.6.1.4.1.25728.8900.1.1.2.2	UniPing	Close(0), Open(1)

click here to add new data

© 2016 Netping East Co. Ltd

In a window that appears, there is a need to enter:

Short Name	<input style="width: 60%;" type="text"/>				
OID	<input style="width: 80%;" type="text"/>				
Agent	<input style="width: 80%;" type="text" value="-"/>				
Dictionary (Enumerated Values)	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 40%; text-align: left;">Numeric Value</th> <th style="width: 60%; text-align: left;">Textual Label</th> </tr> </thead> <tbody> <tr> <td><input style="width: 95%;" type="text"/></td> <td><input style="width: 95%;" type="text"/></td> </tr> </tbody> </table>	Numeric Value	Textual Label	<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>
Numeric Value	Textual Label				
<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>				
<input type="button" value="NetPing MIB Reference"/> <input type="button" value="Delete Record"/> <input type="button" value="Cancel"/> <input type="button" value="Save"/>					

Short Name – is the name of a variable, which will be used in a text of SMS notifications. A name can have no more than 31 characters. It is prohibited to use spaces. **On default: empty line**

OID – is an identifier of a variable. It consists of no more than 62 characters. It begins with a period. For example:

.1.3.6.1.4.1.25728.8800.1.1.2.1

.1.3.6.1.4.1.25728.911.1.0

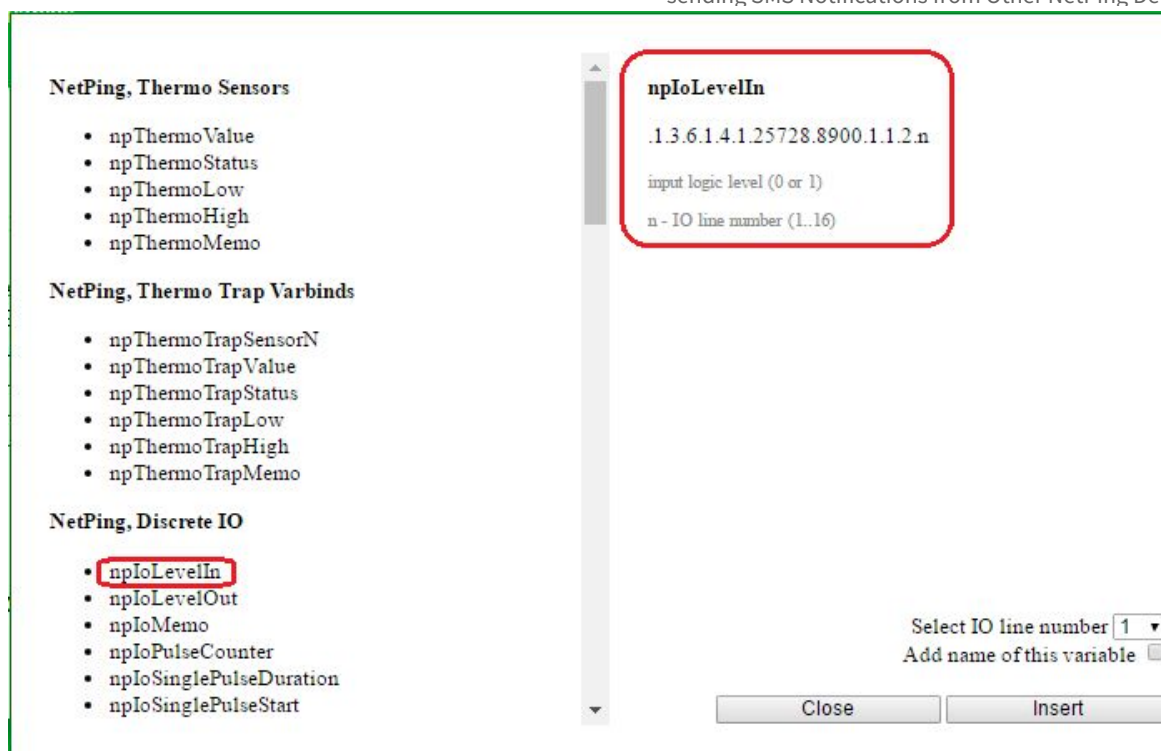
To fill in this field, there is a need to use a reference on NetPing MIB (works for NetPing devices only). **On default: empty line**

Host – is a drop-down list from short names of SNMP agents, configured on the page «**AGENTS**». **On default: an agent is not selected**

Dictionary (Enumerated Values) – is a table consisting of pairs «**Numeric Value - Textual Label**». It is not obligatory for filling. It is used to link numeric values of SNMP variables to a textual description, which is understandable for a human. A textual description can be used in SNMP commands instead of a corresponding integer value. A description is Latin letters without spaces and underlining, taking a case into account. A total length of a dictionary is 127. To store the dictionary in memory of a device, specific separating characters are used (commas, brackets, spaces), which are counted when calculating the length of a dictionary. On average, each pair «**Numeric Value - Textual Label**» needs 4 delimiter characters. There is a need to count on this when filling in a dictionary. **On default: a dictionary is empty**

To add a pair «**Numeric Value - Textual Label**» to a dictionary, fill in the last (empty) line. To delete a pair «**Numeric Value - Textual Label**», delete data in the line and click the button «**Save**»;

- A reference on NetPing MIB makes the process of adding new SNMP variables easier if a NetPing device serves as an agent. To run a reference, click the button «**NetPing MIB Reference**» in a window for adding a new SNMP variable.



The screenshot shows a configuration window with a left sidebar and a main content area. The sidebar lists three categories of variables:

- NetPing, Thermo Sensors**
 - npThermoValue
 - npThermoStatus
 - npThermoLow
 - npThermoHigh
 - npThermoMemo
- NetPing, Thermo Trap Varbinds**
 - npThermoTrapSensorN
 - npThermoTrapValue
 - npThermoTrapStatus
 - npThermoTrapLow
 - npThermoTrapHigh
 - npThermoTrapMemo
- NetPing, Discrete IO**
 - npIoLevelIn** (highlighted with a red box)
 - npIoLevelOut
 - npIoMemo
 - npIoPulseCounter
 - npIoSinglePulseDuration
 - npIoSinglePulseStart

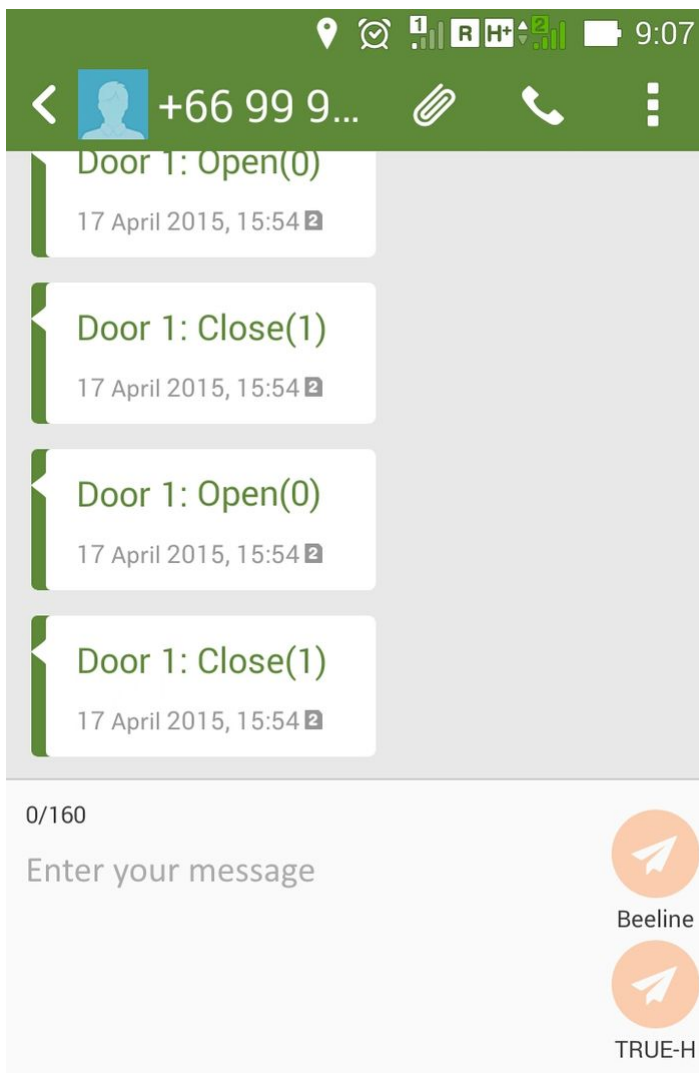
The main content area displays the details for the selected variable, **npIoLevelIn**, which is also highlighted with a red box. The details include:

- OID:** .1.3.6.1.4.1.25728.8900.1.1.2.n
- Description:** input logic level (0 or 1)
- Reference:** n - IO line number (1..16)

At the bottom right of the main content area, there is a dropdown menu labeled "Select IO line number" with the value "1" selected, and a checkbox labeled "Add name of this variable" which is currently unchecked. Below these are two buttons: "Close" and "Insert".

In a left column of a reference, there is a list of known SNMP variables. Choose a necessary SNMP variable and click on it. In the right column, an OID of this variable will be displayed, as well as a small reference. In a drop-down list «**choose index**», indicate a necessary index of an SNMP variable. Usually, an index corresponds to a number of a temperature sensor, a humidity sensor, a relay, an IO line. An index will be added to the end of OID. Check a checkbox «**add OID name**» to copy a name of an SNMP variable from a dictionary to the field «**Short name**».

As a result of the actions configured above, service staff will receive SMS notifications from a door opening sensor, which is connected to a UniPing v3 device as follows:



where:

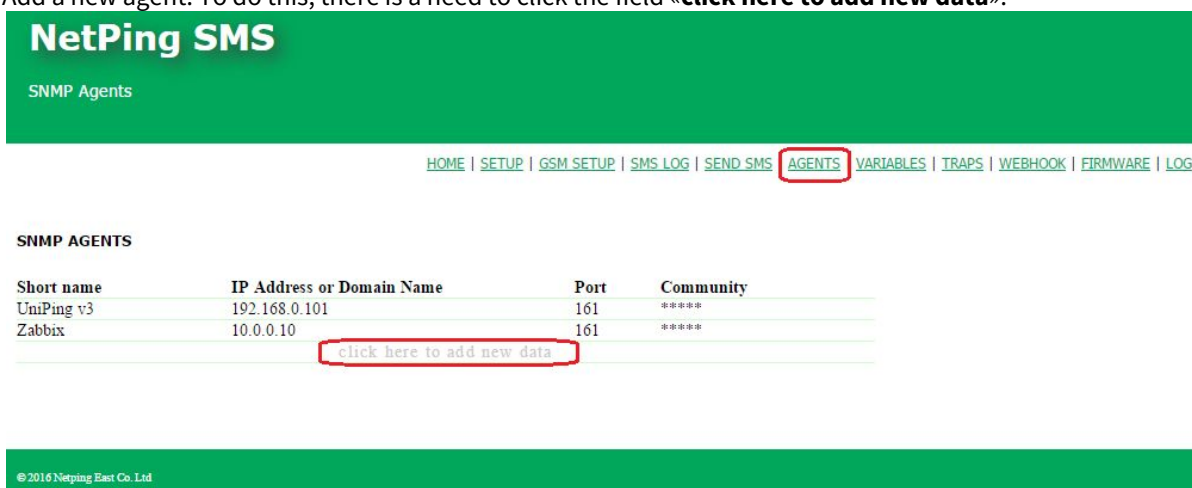
Door 1 – is a door opening sensor, which is connected to an IO line №1 of a UniPing v3 device;

Open (0)/Close (1) – is a description of the status of a sensor, which is specified on the page «**VARIABLES**» of a device web interface

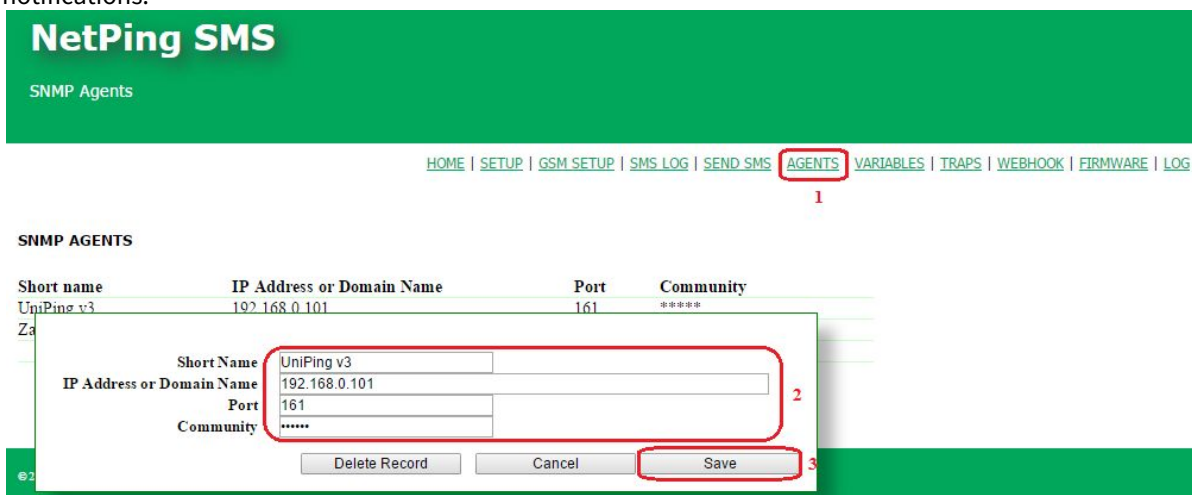
[ENG] 7. [DKSF 707.3 IU] An Example of Configuring a Gateway of NetPing SMS to Control NetPing Devices using SMS Messages

To control NetPing devices by using SMS notifications, there is a need to configure the following settings:

1. Go to the tab «**AGENTS**» of a device web interface. An agent is a device controlled or polled via an SNMP protocol. **NetPing SMS** sends either an SNMP SET command or an SNMP GET request to an agent when receiving SMS notifications of a certain format;
2. Add a new agent. To do this, there is a need to click the field «**click here to add new data**»:



In a window that appears, there is a need to add a UniPing v3 device as an agent to control it using SMS notifications:



where:

Short Name – is the name of an agent. It has no more than 15 Latin letters. Spaces are prohibited to be used. **On default: empty line**

IP Address or a Domain Name – is an IP address/a name of an agent, where SNMP SET commands and SNMP GET requests will be sent. In the example, an IP address of a UniPing v3 device is indicated, which is located in the same local network with a **NetPing SMS** gateway. It can have no more than 62 characters. **On default: empty line**

Port – is a UDP port of an agent, where an SNMP message will be sent. **On default: 161**

Community – is used in SNMP packages. It must coincide with Community, configured in an agent. **On default: empty line**

To delete an agent, there is a need to click on it, and click the button «Delete» in a window that appears. To change parameters of an agent, there is a need to click on it, edit parameters in a window that appears, and click the button «Save». To cancel the action, click the button «Cancel»;

3. On the page «**VARIABLES**» of a device web interface, there is a need to set SNMP variables. Devices are controlled with the help of SNMP variables. Parameters that can be managed by SMS notifications depend on the SNMP parameters that are added to the page «**VARIABLES**» of a **NetPing SMS** gateway.

Short Name	OID	Agent	Dictionary
PWR1 on 8PWR	.1.3.6.1.4.1.25728.5500.5.1.2.1	Netping	ON(1), OFF(0)
npIoTrapLineN	.1.3.6.1.4.1.25728.8900.2.1.0	Netping_IO_v2	
npIoLevIn.1	.1.3.6.1.4.1.25728.8900.1.1.2.1	UniPing	Close(0), Open(1)
npIoLevIn.2	.1.3.6.1.4.1.25728.8900.1.1.2.2	UniPing	Close(0), Open(1)

In the example, variables for receiving values of temperature and the status of a temperature sensor № 3 for a **UniPing v3** will be added as well as a variable for controlling an IO line № 3 in the mode «**output**».

To add a new variable, there is a need to click the button «**click here to add new data**». In a window that appears, add:

Short Name: T3

OID: .1.3.6.1.4.1.25728.8800.1.1.2.3

Agent: UniPing v3

Dictionary (Enumerated Values)	Numeric Value	Textual Label

Buttons: NetPing MIB Reference, Delete Record, Cancel, Save

Short Name – is the name of a variable, which will be used in a text of an SMS command. A name must consist of no more than 31 characters. Using spaces is prohibited. **On default: empty line**

OID – is an identifier of a variable. It consists of no more than 62 characters. It always begins with a period. For example:

.1.3.6.1.4.1.25728.8800.1.1.2.1

.1.3.6.1.4.1.25728.911.1.0

To fill in this field, it is possible to use a NetPing MIB reference (works only for NetPing devices). **On default: empty line**

Host – is a drop-down list of short names of SNMP agents, configured on the page «**AGENTS**». **On default: an agent is not selected**

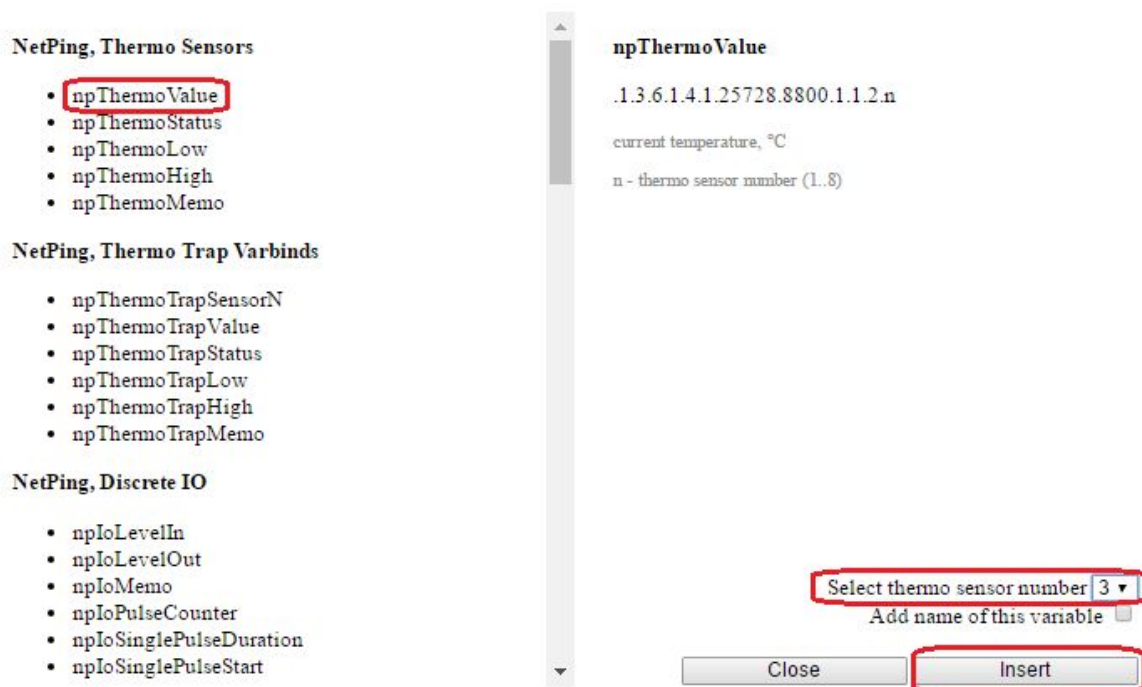
Dictionary – is a table consisting of pairs «**Numeric Value - Textual Label**». It is not obligatory to fill in. It is used for linking numeric values of SNMP variables to a textual description, understandable for a human. A textual description can be used in SNMP commands instead of a corresponding numeric integer value. The description consists of Latin letters without spaces and underlining taking a case into account. A total length of a dictionary is 127. To save the dictionary in memory of a device, special separating characters are used (commas, brackets, spaces), which are taken into account when calculating the length of a dictionary. On

average, each pair «**Numeric Value - Textual Label**» needs 4 delimiter characters. There is a need to mind this when filling a dictionary in. **On default: a dictionary is empty**

In the example, a UniPing v3 device is used, therefore, to add an SNMP OID it is possible to use a tool «**NetPing MIB Reference**». A NetPing MIB reference makes the process of adding new SNMP OID easier if a NetPing device is an agent. To run a reference, click the button «**NetPing MIB Reference**» in a window of adding a new SNMP variable.

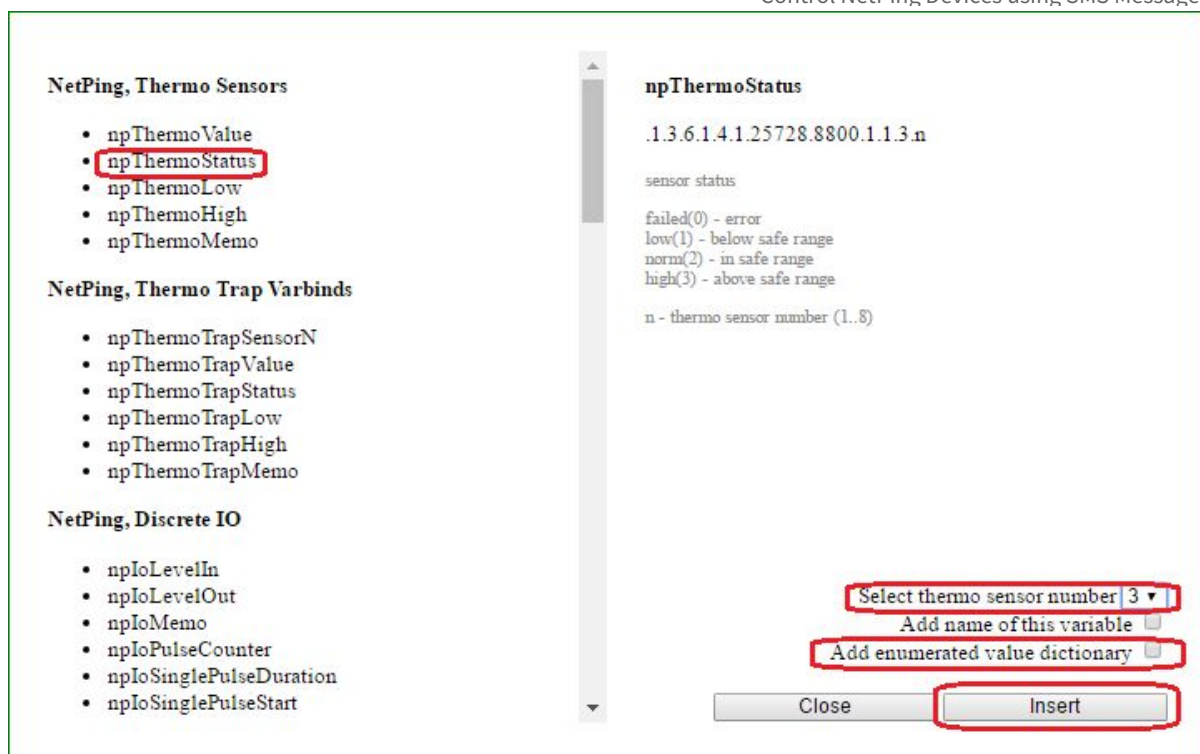
To add an SNMP variable, which allows getting a current temperature (°C) of a temperature sensor № 3, select:

- «**npThermoValue**»;
- a number of a temperature sensor



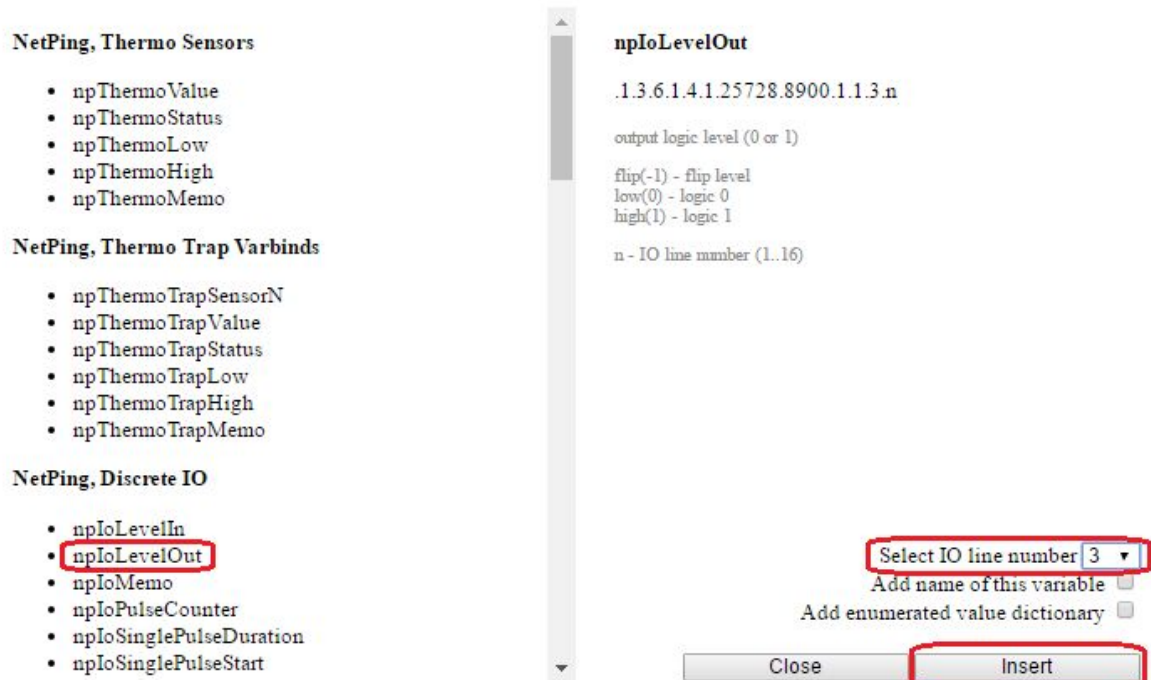
To add an SNMP variable, which allows receiving a status of a temperature sensor № 3, select:

- «**npThermoStatus**»;
- a number of a temperature sensor;
- check a checkbox «**add a dictionary of values of a variable**» for a description of numeric values of SNMP variables as a textual description, understandable for a human



To add an SNMP variable, which allows controlling an IO line № 3 in the mode «**output**» select:

- «**npIoLevelOut**»;
- a number of an IO line



4. As a result of configurations described above, on the page «**VARIABLES**» of a device web interface three configured SNMP variables will appear:

NetPing SMS

SNMP Variables

[HOME](#) | [SETUP](#) | [GSM SETUP](#) | [SMS LOG](#) | [SEND SMS](#) | [AGENTS](#) | [VARIABLES](#) | [TRAPS](#) | [WEBHOOK](#) | [FIRMWARE](#) | [LOG](#)

SNMP VARIABLES ACCESSIBLE VIA SMS

Short Name	OID	Agent	Dictionary
T3	.1.3.6.1.4.1.25728.8800.1.1.2.3	UniPingv3	
T3Status	.1.3.6.1.4.1.25728.8800.1.1.3.3	UniPingv3	failed(0), low(1), norm(2), high(3)
IoLevelOut3	.1.3.6.1.4.1.25728.8900.1.1.3.3	UniPingv3	Disable(0), Enable(1)

[click here to add new data](#)

© 2016 Netping East Co. Ltd

A variable «**T3**» for getting a current temperature of a temperature sensor № 3, which is connected to a UniPing v3 device.

A variable «**T3Status**» for receiving a status of a temperature sensor № 3, which is connected to a UniPing v3 device.

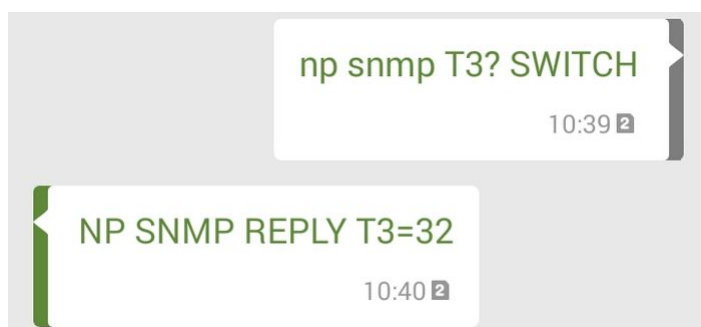
A variable «**IoLevelOut3**» for controlling an IO line № 3 in the mode «**output**» of a UniPing v3 device.

in variables «**T3Status**» and «**IoLevelOut3**» a table of pairs «**Numeric Value - Textual Label**» is configured for linking numeric values of SNMP variables to a textual description, understandable for a human.

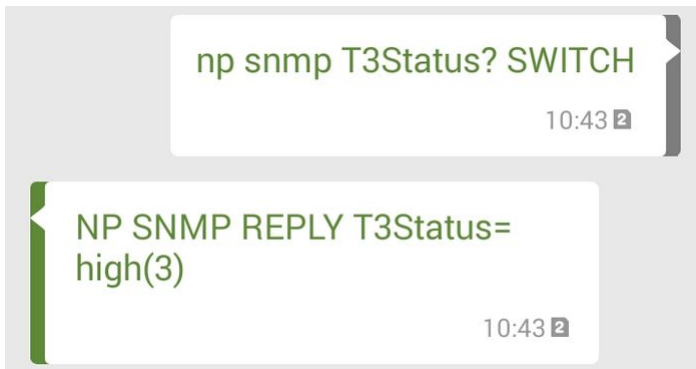
- To send SMS commands, there is a need to use the section «[\[ENG\] 4.6. \[DKSF 707.3 IU\] What SMS Commands and SMS Notifications Are Supported by a Device?](#)» of this user guide.

As a result of a described algorithm of configuring [NetPing SMS](#), a possibility to control devices that support working with an SNMP protocol by SMS notifications.

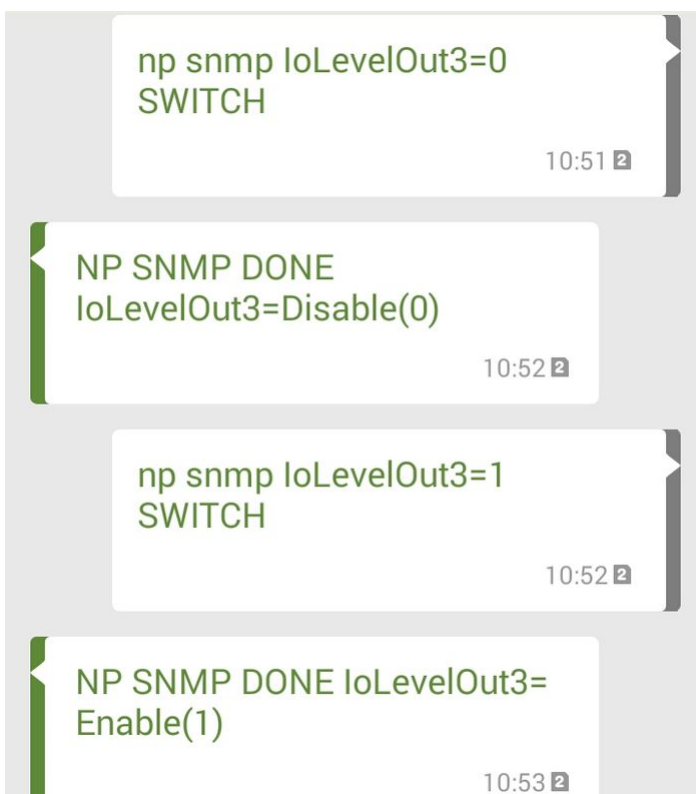
An example of sending an SMS command to get a current temperature from a temperature sensor № 3 that is completed successfully is represented below:



An example of sending an SMS command for receiving the status of a temperature sensor №3 with a successful result of completion:



An example of sending an SMS command to switch a logic level of an IO line № 3 in the mode «**output**» with a successful result of completion



[ENG] 8. [DKSF 707.3 IU] Working with WEBHOOK

WEBHOOK (web callback or HTTP push API) is a mechanism for implementing notifications about certain events, sent to the third-party services or applications in a real time mode. Unlike usual APIs, WEBHOOK is a much more effective solution for getting data in a real time mode.

NetPing SMS has this functionality with the aim of a simple integration of a device with modern third-party services and applications that support receiving WEBHOOK. For example, an integration with a service of automation [Zapier.com](https://zapier.com) allows executing a lot of actions when receiving an SMS notification by a NetPing SMS device. More detailed information on the features of [Zapier.com](https://zapier.com) can be read on the link: <https://zapier.com/zapbook/webhook/>.

To configure a mechanism of sending WEBHOOK, there is a need to go to the page «**WEBHOOK**» of a device web interface:

NetPing SMS

Web Hook

[HOME](#) | [SETUP](#) | [GSM SETUP](#) | [SMS LOG](#) | [SEND SMS](#) | [AGENTS](#) | [VARIABLES](#) | [TRAPS](#) | **WEBHOOK** | [FIRMWARE](#) | [LOG](#)

WEB HOOK SETUP

Enable

Translation Server

Called URL

Apply Changes

© 2016 Netping East Co. Ltd

where:

Enable – is a checkbox that activates WEBHOOK notifications for received SMS notifications by a NetPing SMS device. **On default: checkbox is not checked**

Translation Server – is a service that receives an SNMP TRAP notification (Trap OID: «.1.3.6.1.4.1.25728.3800.2.0.3») containing variables (a text of an SMS notification: OID «.1.3.6.1.4.1.25728.3800.1.10.0», a sender's number is: OID «.1.3.6.1.4.1.25728.3800.1.11.0», a called URL is: OID «.1.3.6.1.4.1.25728.95.31.0») from NetPing SMS, which is converted into an HTTPS request for sending to an indicated URL. **On default: empty line**

Source:	192.168.137.100	Timestamp:	2 minutes 3 seconds	SNMP Version:	2
Trap OID:	.iso.org.dod.internet.private.enterprises.lightcom.npGsm.npGsmTraps.npGsmTrapPrefix.npGsmTrapUnparsedSmsWebhook				
Variable Bindings:					
Name:	.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0				
Value:	[TimeTicks] 2 minutes 3 seconds (12386)				
Name:	snmpTrapOID				
Value:	[OID] npGsmTrapUnparsedSmsWebhook				
Name:	.iso.org.dod.internet.private.enterprises.lightcom.npGsm.npGsmInfo.npGsmUnparsedRxSms.0				
Value:	[OctetString] Test SMS for WEBHOOK				
Name:	.iso.org.dod.internet.private.enterprises.lightcom.npGsm.npGsmInfo.npGsmUnparsedRxSmsFrom.0				
Value:	[OctetString] 79059444444				
Name:	.iso.org.dod.internet.private.enterprises.lightcom.npWebhook.npWebhookUrl.0				
Value:	[OctetString] exsample.com/phone-list				
Name:	.iso.org.dod.internet.mgmt.mib-2.system.sysName.0				
Value:	[OctetString] NetPing-SMS				
Description:					

It is recommended to use an address of a translation server notifier.netping.ru

Called URL – is a URL of a third-party service or application for fulfilling certain actions on a received WEBHOOK notification. **On default: empty line**

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

[ENG] 9. [DKSF 707.3 IU] Support of an SNMP Protocol by a Device

[ENG] 9.1. [DKSF 707.3 IU] Can I Control a Device Using SNMP?

A NetPing SMS device supports polling parameters and control via an SNMP v1 protocol.

More detailed information about an SNMP protocol can be read on the links:

- https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol
- <http://net-snmp.sourceforge.net/>

OIDs that are supported by a device are specified in the MIB file **DKSF_707.3.X_MB.mib**. The MIB file can be downloaded from the page with a description of a device, the section «[Documentation and files](#)».

A device supports:

- reading OID using requests GET, GET-Next via an SNMP v1 protocol;
- setting OID values using a SET command via an SNMP v1 protocol;
- sending SNMP TRAP notifications to events

Configuring an SNMP Protocol

To access a device via an SNMP v1 protocol, there is a need to configure the next parameters using a device web interface:

- **SNMP Community for Read** – is a password, which needs to be indicated in any request for reading parameters via an SNMP protocol. It is specified on the page «**SETUP**»;
- **SNMP Community for Write** – is a password which needs to be indicated in any request for recording parameters via an SNMP protocol. It is specified on the page «**SETUP**»

ACCESS RESTRICTIONS

Username	visor29
Password	*****
SNMP Community for Read	ping29
SNMP Community for Write	ping29
IP Filter (access granted for this subnet)	0.0.0.0
IP Filter Netmask (0.0.0.0 - disable filter)	0.0.0.0

[ENG] 9.2 [DKSF 707.3 IU] What OIDs Are Supported by a Device?

A description of OIDs, which are supported by a device, is represented in the table:

OID	Name	Type	Access	Description
RFC 1213				
.1.3.6.1.2.1.1.1.0	sysDescr.0	Display String	READ	A textual description of a device. For example, NetPing SMS, FW v707.3.3.A-1.
.1.3.6.1.2.1.1.2.0	sysObjectID.0	OID	READ	A number of a branch with parameters of a device is always «1.3.6.1.4.1.25728».
.1.3.6.1.2.1.1.3.0	sysUpTime.0	TimeTicks	READ	A time from the moment of the last switching a device on.
.1.3.6.1.2.1.1.4.0	sysContact.0	Display String	READ/WRITE	Administrators data, usually an e-mail.
.1.3.6.1.2.1.1.5.0	sysName.0	Display String	READ/WRITE	A domain name of a device.
.1.3.6.1.2.1.1.6.0	sysLocation.0	Display String	READ/WRITE	A location of a device.
.1.3.6.1.2.1.1.7.0	sysServices.0	Integer	READ	Binary representation of this OID is a set of supported services. Always «72», a device plays a role of a final host.
.1.3.6.1.2.1.2.2.1.1.1	ifIndex.1	Integer	READ	Interface index. Always «1».
.1.3.6.1.2.1.2.2.1.3.1	ifType.1	Integer	READ	A type of a network interface of a device. Always «ethernetCsmacd (6)».
.1.3.6.1.2.1.2.2.1.4.1	ifMtu.1	Integer	READ	A maximum data size, which is possible to be sent via a network. Always «1514».
.1.3.6.1.2.1.2.2.1.5.1	ifSpeed.1	Gauge	READ	An approximate data transfer speed in bit/s. Always «100 000 000».

OID	Name	Type	Access	Description
.1.3.6.1.2.1.2.2.1.6.1	ifPhysAddress.1	PhysAddress	READ	MAC address of a device.
NetPing MIB				
.1.3.6.1.4.1.25728.90.1.0	npTrapEmailTo.0	Display String	READ	A variable included in traps. E-mail, where messages are sent using a NetPing notification forwarding service.
.1.3.6.1.4.1.25728.95.31.0	npWebhookUrl	Display String	READ	A variable included in traps. A URL specified by a user for a NetPing Webhook forwarding service.
.1.3.6.1.4.1.25728.911.1.0	npSoftReboot.0	Integer	READ/WRITE	Software reboot of a device when writing a value «1».
.1.3.6.1.4.1.25728.911.2.0	npResetStack.0	Integer	READ/WRITE	Software reboot of a network interface when writing a value «1».
.1.3.6.1.4.1.25728.911.3.0	npForceReboot.0	Integer	READ/WRITE	Immediate forced reboot of a device when writing a value «1» (a processor is reset the same as when switching a power off).
.1.3.6.1.4.1.25728.3800.1.1.0	npGsmFailed.0	Integer	READ	A status of a built-in GSM modem: 0 – OK 1 – Failed (no connection) 2 – FatalError (unrecoverable error, a modem is blocked)
.1.3.6.1.4.1.25728.3800.1.2.0	npGsmRegistration.0	Integer	READ	A status of a GSM network connection: 0 – Impossible 1 – HomeNetwork 2 – Searching 3 – Denied 4 – Unknown 5 – Roaming 255 – InfoUpdate

OID	Name	Type	Access	Description
.1.3.6.1.4.1.257 28.3800.1.3.0	npGsmStrength .0	Integer	READ	GSM signal strength: 0...31 = 0% ... 100% 99 – unknown 255 – updating info
.1.3.6.1.4.1.257 28.3800.1.9.0	npGsmSendSMS	Display String	READ/ WRITE	Sending a random SMS notification. Format: [phone_number,phone_number,...] Message where: phone_number – is a destination number in square brackets, indicated in the format: Country_codeOperator's_codePhone_number Message – is a text of a message (is separated from a destination number by a space) It is possible to send SMS to several (up to four) numbers, having indicated them in square brackets separated by a comma, without spaces. If there are no square brackets with a destination number in the beginning of a message, then a message is sent to destination numbers specified on the page «GSM SETUP» of a device web interface.
.1.3.6.1.4.1.257 28.3800.1.10.0	npGsmUnparse dRxSms	Display String	READ	A variable, which has a recorded incoming SMS, which is not a command for a device.
.1.3.6.1.4.1.257 28.3800.1.11.0	npGsmUnparse dRxSmsFrom	Display String	READ	A variable, into which a source number of an SMS is recorded, which is not a command for a device.

[ENG] 10. [DKSF 707.3 IU] HTTP API Support

[ENG] 10.1. [DKSF 707.3 IU] GSM Modem Management

An interface of URL-encoded commands in a device can be used for the integration with web applications without using an SNMP protocol.

SMS Sending

```
http://192.168.0.100/sendsms.cgi?utf8
```

URL is invoked by the POST method. POST data are the text of an SMS in UTF-8 encoding. More detailed information about sending random SMS messages can be read in the section «[\[ENG\] 5.1. \[DKSF 707.3 IU\] How to Send Random SMS Notifications?](#)».

Returned values

Successful execution of a command:

```
sendsms_result('ok',3217763174,2);
```

The first argument is the result of placing into the queue, it must be 'ok'.

The second argument is id for checking status. It starts with a random number and is increased at 1 at each sending of an SMS message to every number. When a 32-bit id is overfilled, it is reset.

The third argument is the number of destinations, specified in the sending queue.

Balance Request

```
http://192.168.0.100/ussdstart.cgi?requestcode
```

where:

request code — is a[code]x. For example, a100x means *100#. In the code of the USSD request, «*» is changed for «a», «#» is changed for «x» (Latin characters).

Returned values

Successful completion of the command:

```
ussdsend_result('ok');
```

Getting a Response to a Balance Request

```
http://192.168.0.100/ussdread.cgi
```

Induce 20 seconds after requesting a SIM card balance.

Returned Values

```
ssdsend_result("response_from_gsm_operator");
```

Checking a Status of SMS Sending

```
http://192.168.0.100/sms_status.cgi?id=3217763174&n=2
```

where:

id – is taken from a response to sendsms.cgi.

n – indicates a number of consequent ids, for which status is checked. Therefore, it is possible to check separate destination numbers or entire group sending at once.

Returned values

```
sms_status_result('success',3);
```

The first argument is:

- error – faulty arguments in a request or an internal error;
- unknown – information on at least one of checked ids is already unavailable, or id «from future» is used;
- waiting – at least one id is still waiting in the queue;
- fail – is an error of sending (of at least one id from a group);
- success – is a successful sending for all requested id group

The second argument is a bit mask, it has the meaning only for the responses 'success' and 'fail'. A left (older) bit corresponds to the first from the checked ids, a right (younger) bit corresponds to the last one from the id group. A mask width corresponds to the argument n in the invoke. Bit = 1 if for this id SMS sending is executed successfully.

Example

When sending SMS notifications to two destination numbers the next response is returned (for example):

```
| sendsms_result('ok',3217763178,2);
```

To check sending SMS notification to the second destination, invoke:

```
| http://192.168.0.100/sms_status.cgi?id=3217763179&n=1
```

As a result, a response is returned:

```
| sms_status_result('success',1);
```

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