HWg-Trigger MANUAL

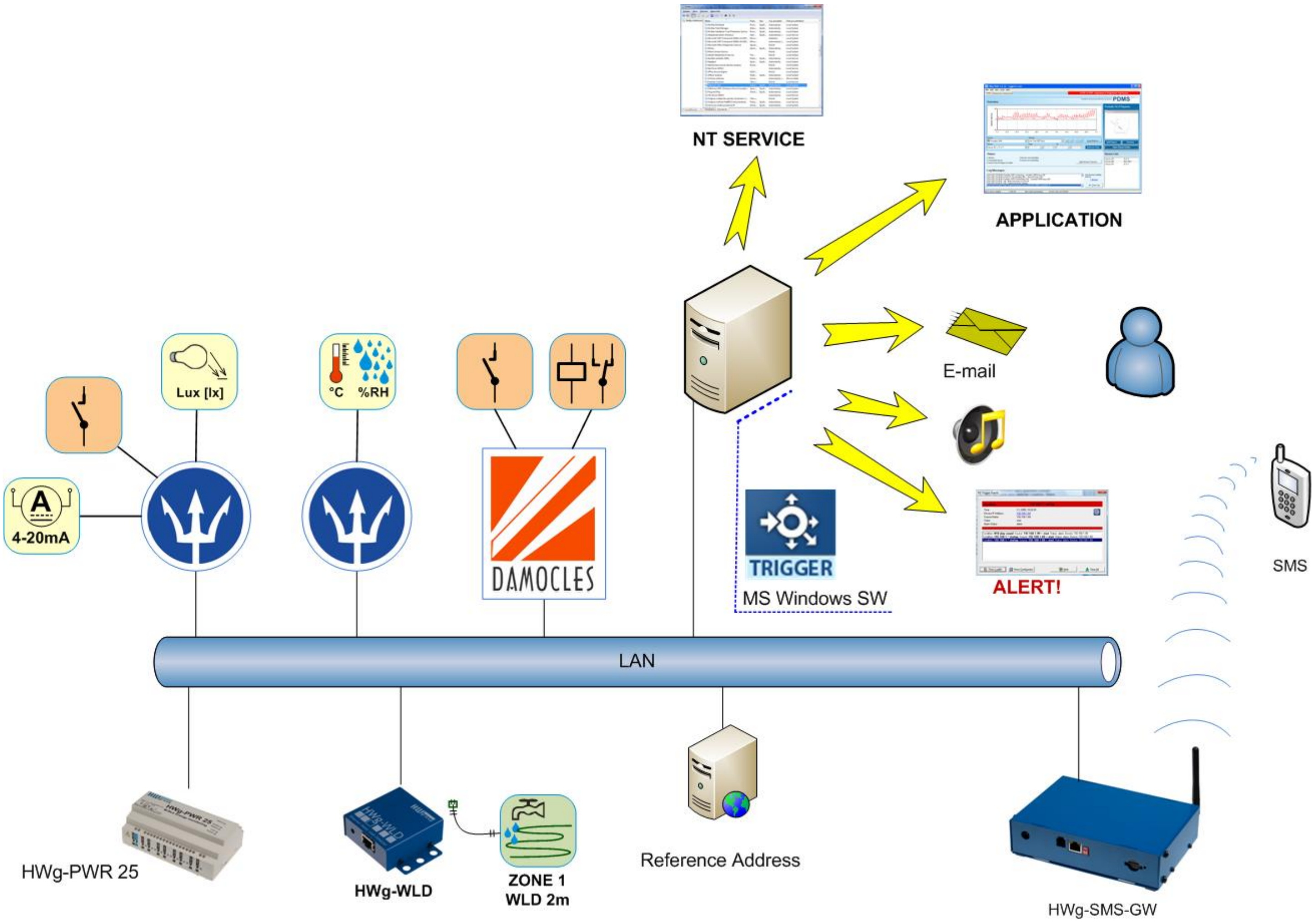
*HWg-Trigger - Windows application for (IF-THAN) events management***.**

Introduction

HWg-Trigger is a Windows application for events management. Such an event could be for example a detection of sensor disconnection, monitored values out of their safe range or a pressed button. HWg-Trigger can then perform an action in response to this event. An email or an SMS message can be then sent to several recipients, output relay in the network could be switched, HWg-Trigger can also start another application on a Windows computer or show an alarm message on the screen.

Every event is evaluated by a **Condition** and followed by an **Action** it gathers into a **Rule**. You can create up to 90 rules with this application.

HWg-Trigger is able to receive information about the events from HWg devices Poseidon, Damocles, HWg-WLD and HWg-PWR. For communication with the devices HWg-Trigger uses a combination of SNMP and XML protocols. It can in limited range replace systems for monitoring (Network Monitoring Systems) or control systems (SCADA).



Rules system

HWg-Trigger is an application processing user-created operations based on a set of rules defining the situations, in which it triggers a reaction. These rules can be combined together and each rule contains:

- **Rule Name** – An ID used only for easier rules management
- **Condition** – main definition of a trigger condition - device power-up (defined IP address), input or sensor alarm (sensor/input ID), etc. It can be also defined if the action should be triggered at the start or at the end of an alarm state, eventually in both situations.
- **Action** – defines a reaction to a matched condition (opens a window with a warning message, sends an SMS message, etc.).

It is generally required that for every action a unique rule has to be made. An exception is opening an alarm message window, which can be used as an addition to any other action.

Another category is the type of rules processed in case of a device power-up and after the start of the HWg-Trigger itself. In both cases these rules can be used for example to set the default values of remote outputs. Rules linked to a device start-up can be used as a reminder of a necessary operating conditions inspection, etc.

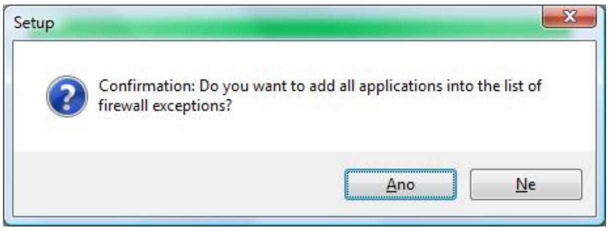
Application client / server

HWg-Trigger works as a client/server application, where the core part is an installed service (NT services).

Graphic interface works as a client – it connects to the service part. Beside configuration options it also informs the user about the actual status. In case the client part is closed, alarm message windows do not open if triggered.
Client part workability is signalised by a HWg-Trigger icon on a status bar next to the clock (systray), which changes to a crossed off icon if the connection is lost (service stopped working, etc.)

A client part is activated after the user logs in or after the first installation it can be started manually through the START menu.

Installation

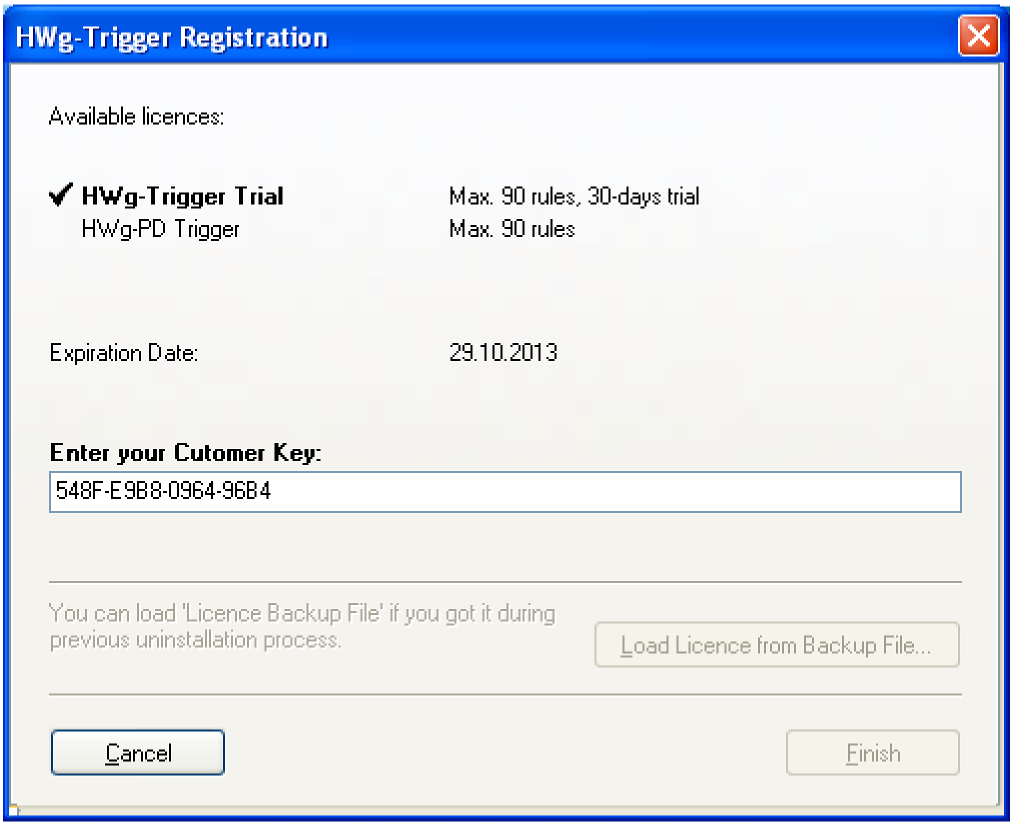


Setup

Confirmation: Do you want to add all applications into the list of firewall exceptions?

HWg-Trigger is equipped with a simple configurator, allowing quick and easy installation. As it is necessary for HWg-Trigger to operate also outside your computer, it is required to allow automatical starting of the service and open the ports needed for SNMP traps (typically 162, however this port can be changed) in your firewall's settings. In case the installer detects a standard firewall on Windows XP SP2, Windows Vista, Windows 7, Windows 8 or Windows Server 2003/2008/2012, you will be asked to allow automatical changes in the settings. After allowing the changest the installer will add this service to the list of firewall exceptions – otherwise the changes have to be done manually (Program Files\HW group\HWg-Trigger\PD_Trigger_srv.exe). It is also necessary to do the changes manually with other than original Windows firewalls (Sunbelt, ISA, Norton apod.).

! „**Trial version** " functions only for 30 days. After the trial time it is necessary to purchase a full version and enter a license number into the **Registration** form. Manual can be found in the **Help** menu.



HWg-Trigger Registration

Available licences:

✓ **HWg-Trigger Trial**	Max. 90 rules, 30-days trial
HWg-PD Trigger	Max. 90 rules

Expiration Date: 29.10.2013

Enter your Cutomer Key:

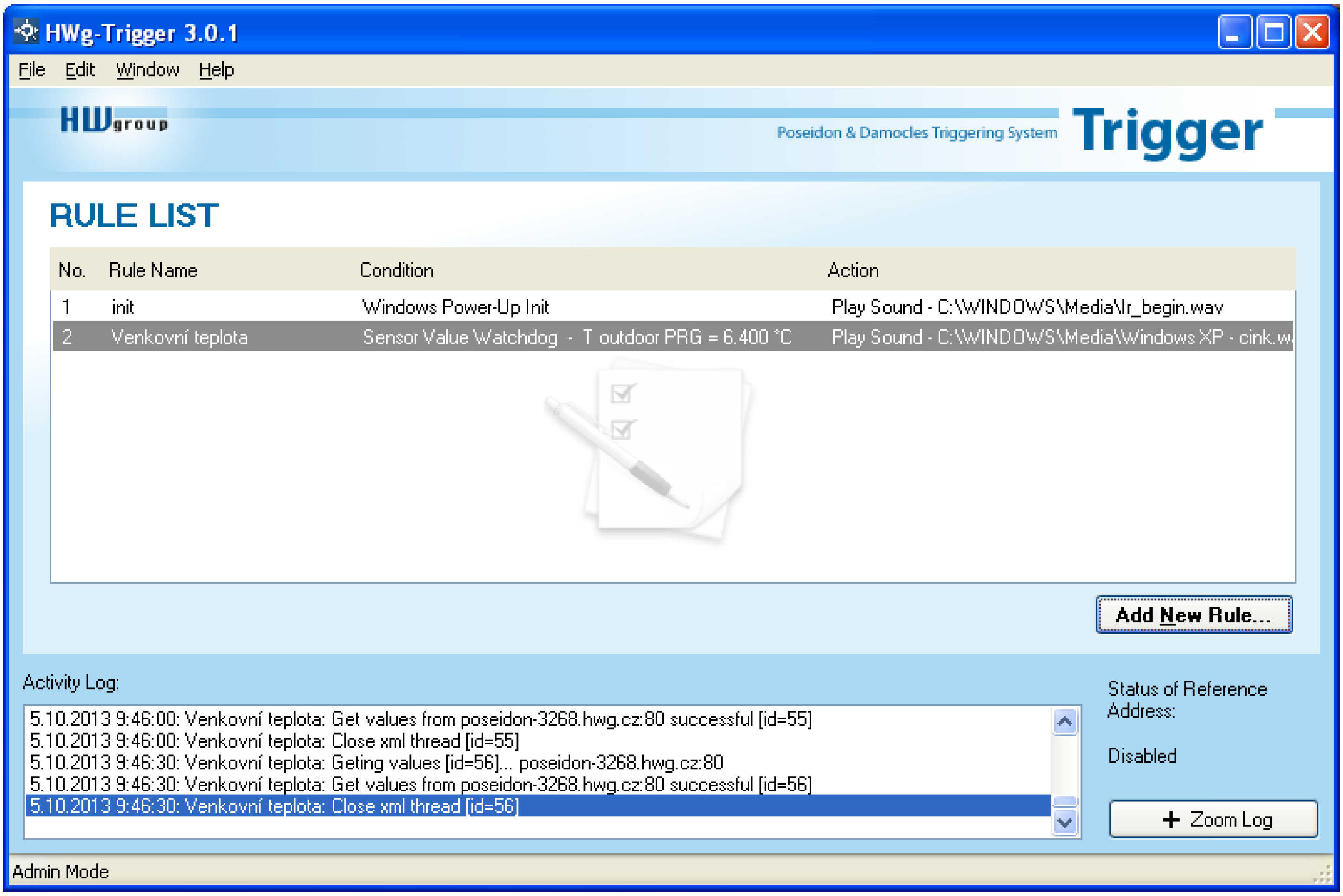
548F-E9B8-0964-96B4

You can load 'Licence Backup File' if you got it during previous uninstallation process.

! During the uninstallation HWg-Trigger application creates a backup folder containing your license. You can then use this file for reinstallation by clicking the **Load Licence from Backup File** option. The license cannot be transferred to another computer.

User interface

Main tab of HWg-Trigger shows a list of defined rules and a log of recent events. By double-clicking the rule you can open a form where you can edit its settings.



RULE LIST

No.	Rule Name	Condition	Action
1	init	Windows Power-Up Init	Play Sound - C:\WINDOWS\Media\lr_begin.wav
2	Venkovní teplota	Sensor Value Watchdog - T outdoor PRG = 6.400 °C	Play Sound - C:\WINDOWS\Media\Windows XP - cink.w

Activity Log:

```
5.10.2013 9:46:00: Venkovní teplota: Get values from poseidon-3268.hwg.cz:80 successful [id=55]
5.10.2013 9:46:00: Venkovní teplota: Close xml thread [id=55]
5.10.2013 9:46:30: Venkovní teplota: Geting values [id=56]... poseidon-3268.hwg.cz:80
5.10.2013 9:46:30: Venkovní teplota: Get values from poseidon-3268.hwg.cz:80 successful [id=56]
5.10.2013 9:46:30: Venkovní teplota: Close xml thread [id=56]
```

Status of Reference Address:

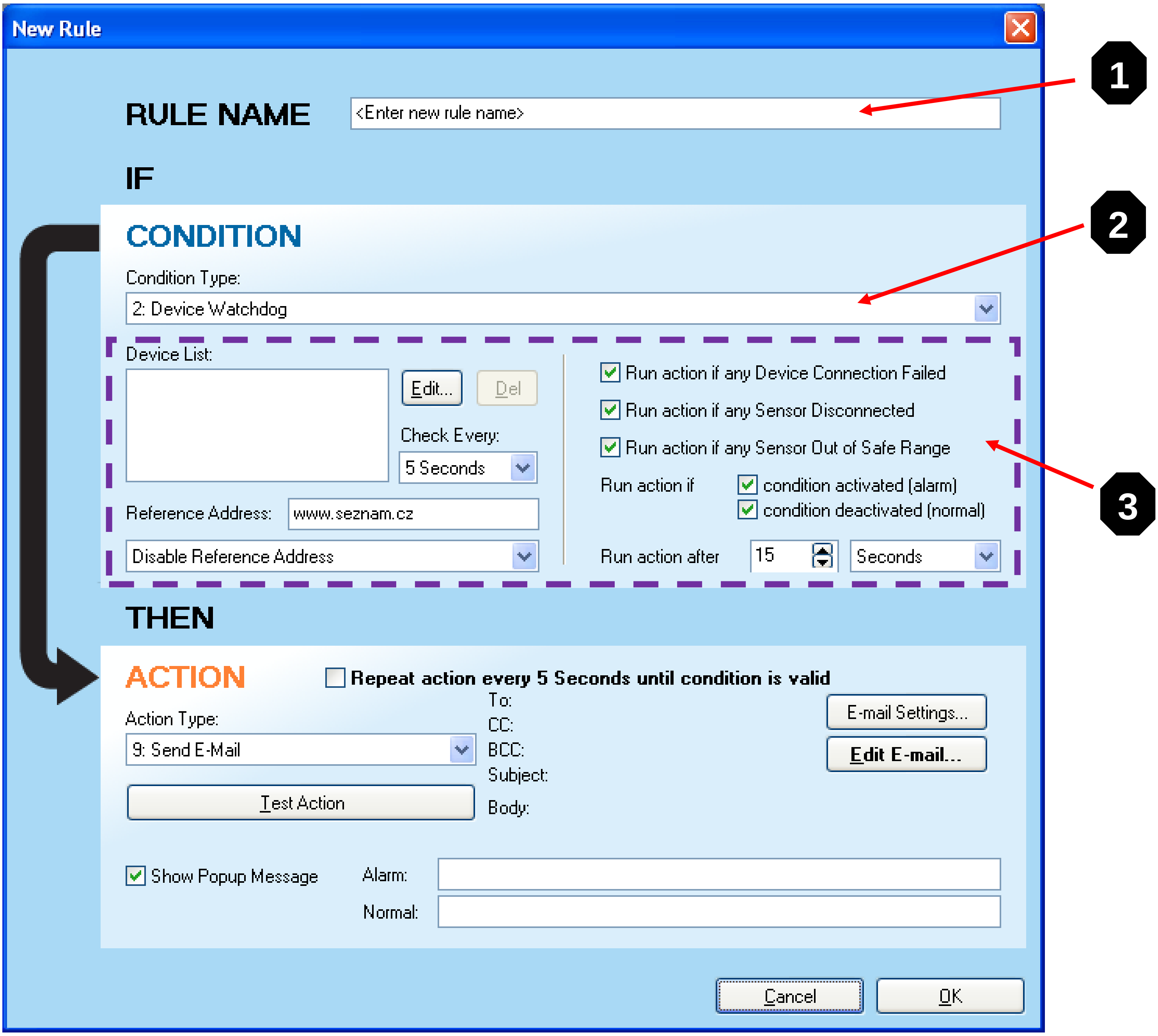
Disabled

Creating and editing the rules

New Rule/Edit Rule form is designated for creating and editing the Rules – defining the reactions to detected events.

- **Condition** defines when the Action has to be processed
- **Action** defines the action itself and its parameters.

! In both trial and full versions the number of rules you can create is limited to 90. The trial version is active only for 30 days.



New Rule

RULE NAME <Enter new rule name>

IF

CONDITION

Condition Type: 2: Device Watchdog

Device List:

Check Every: 5 Seconds

Reference Address: www.seznam.cz

Disable Reference Address

☑ Run action if any Device Connection Failed

☑ Run action if any Sensor Disconnected

☑ Run action if any Sensor Out of Safe Range

Run action if ☑ condition activated (alarm) ☑ condition deactivated (normal)

Run action after 15 Seconds

THEN

ACTION

□ Repeat action every 5 Seconds until condition is valid

Action Type: 9: Send E-Mail

To:
CC:
BCC:
Subject:
Body:

☑ Show Popup Message

Alarm:

Normal:

RULE NAME (1)

Name for better orientation in the rules list and for identification of the rule in the events list.

Condition Type (2)

Defines the type of the event this rule monitors.

CONDITION settings

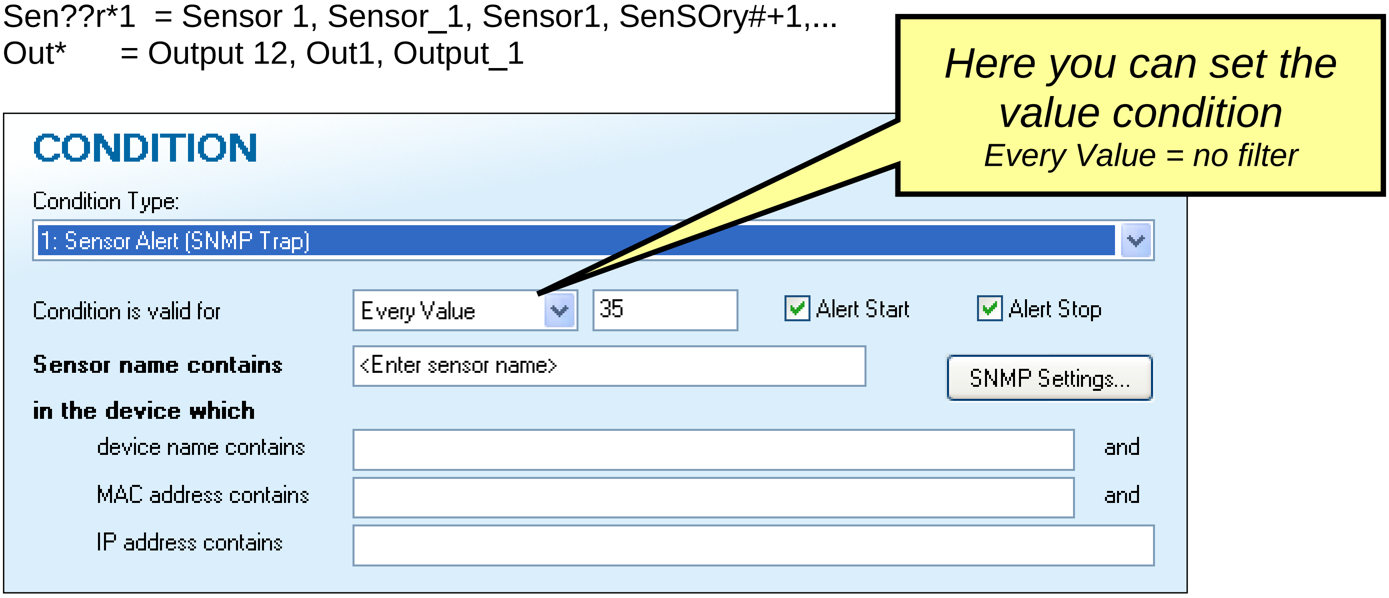
This section defines a situation, which triggers the **Action**.

1: Sensor Alert (SNMP Trap):

A condition passively awaits and reacts to a SNMP Trap received from a device.
It allows filtering of incoming SNMP traps, to set the rule to react only to the selected devices. Filter can be set to a sensor name, device name, MAC address and IP address. Traps containing the entered text will be processed by this rule. You can also use symbols „*“ and „?“ while „*“ (can be used only once in every field) replaces any number of signs and a „?“ symbol replaces one sign.

Text filter settings examples:

* 12	= Binary 12, Sensor 12, Output 12,...
Sen??r*1	= Sensor 1, Sensor_1, Sensor1, SenSOry#+1,...
Out*	= Output 12, Out1, Output_1



CONDITION

Condition Type: 1: Sensor Alert (SNMP Trap)

Condition is valid for: Every Value | 35 | ☑ Alert Start | ☑ Alert Stop

Sensor name contains: <Enter sensor name>

in the device which

device name contains: and

MAC address contains: and

IP address contains:

Here you can set the value condition
Every Value = no filter

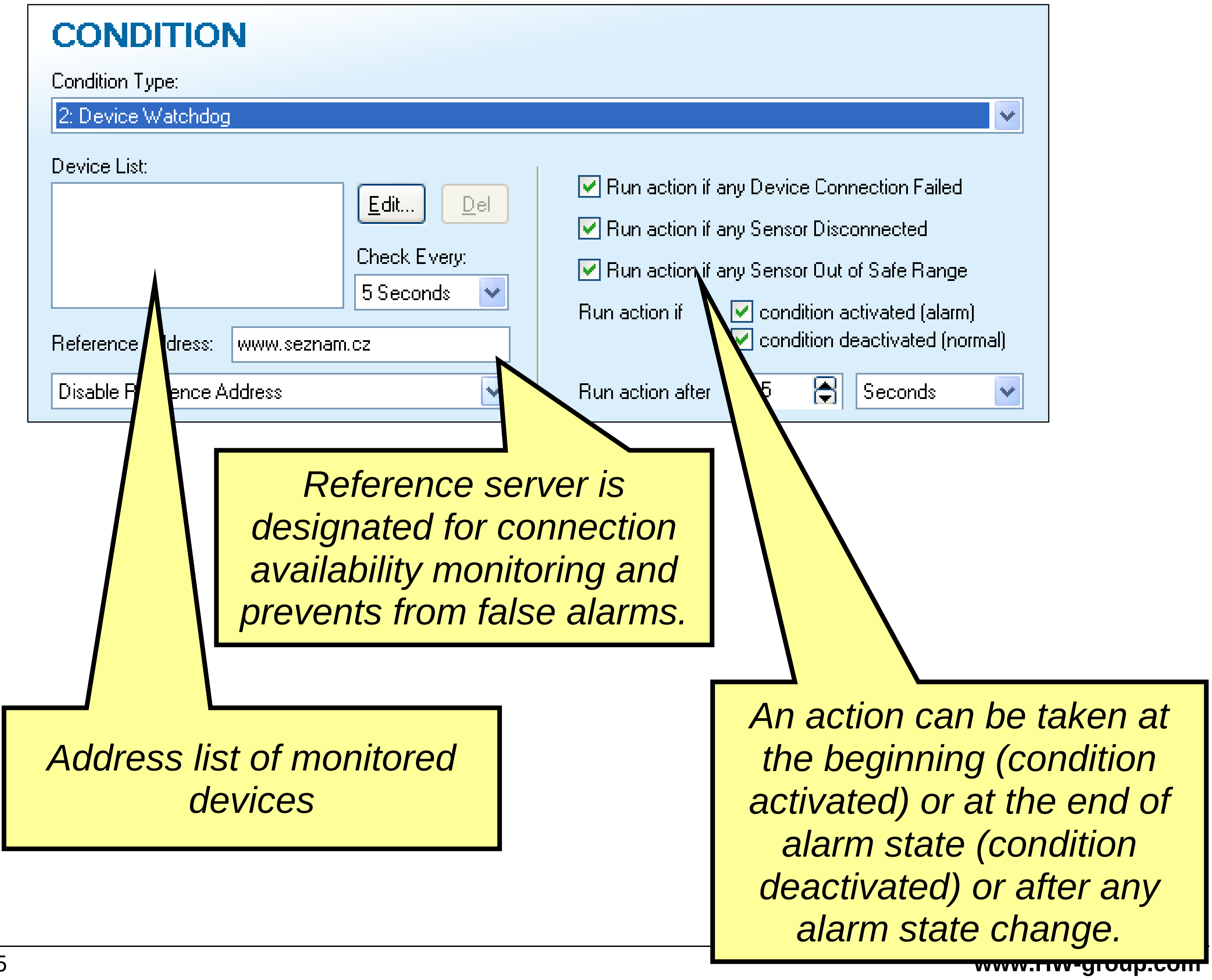
You can also determine if the rule depends on the value of the sensor (higher/lower than) and if the action is triggered at the start or at the end of the event.

2: Device Watchdog

A condition actively communicates with devices in the **Device List**.
The monitoring is done periodically (**Check Every**), where the period can be set to a range between 2 seconds and 1 hour.

Reference Address:
This rule function can be linked with a reference server availability (using Ping). A condition won't trigger unless a connection to a reference address is / is not available.
For example while using HWg-Trigger on a notebook, which is not permanently connected to the network. Device Watchdog Condition does not generate false alarms in case a computer with this application installed does not have the correct network available (A network where the reference server and the monitored devices are located).

An action can be also run after a delay (**Run Action After**), which also decreases a chance of false alarms caused by a short unavailability of a device. This sometimes happens during the time the measured values are being read. A delay time should be set to a period at least 3 times longer than the monitoring period is.
An action can be started if a connection with any of the monitored devices is lost (**Run Action if any Device Connection Failed**), if one of the sensors is disconnected (**Run Action if any Sensor Disconnected**) or if any of the sensors is out of its safe range (**Run Action if any Sensor Out of Safe Range**). It is also possible to determine that an action will be triggered at the start or at the end of an alarm state.



CONDITION

Condition Type: 2: Device Watchdog

Device List:

Check Every: 5 Seconds

Reference Address: www.seznam.cz

Disable Reference Address

☑ Run action if any Device Connection Failed

☑ Run action if any Sensor Disconnected

☑ Run action if any Sensor Out of Safe Range

Run action if ☑ condition activated (alarm)
☑ condition deactivated (normal)

Run action after 5 Seconds

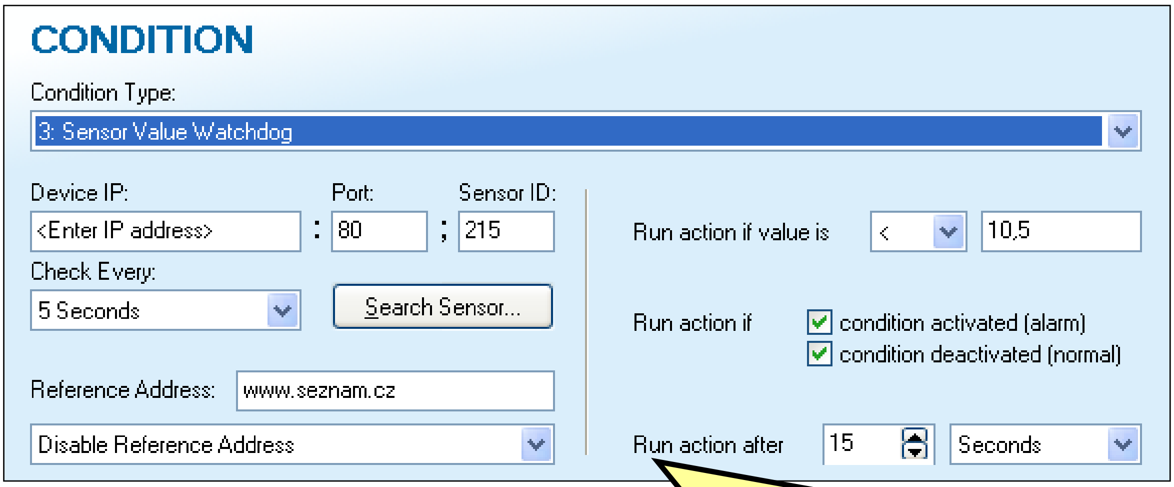
Reference server is designated for connection availability monitoring and prevents from false alarms.

Address list of monitored devices

An action can be taken at the beginning (condition activated) or at the end of alarm state (condition deactivated) or after any alarm state change.

3: Sensor Value Watchdog

The condition communicates with an IP address entered in the „**Device IP**“ field.
This function is designated for monitoring of one sensor connected to a device, by sending periodical requests on sensors’ state.



CONDITION

Condition Type: 3: Sensor Value Watchdog

Device IP: <Enter IP address> : Port: 80 ; Sensor ID: 215

Check Every: 5 Seconds

Reference Address: www.seznam.cz

Disable Reference Address

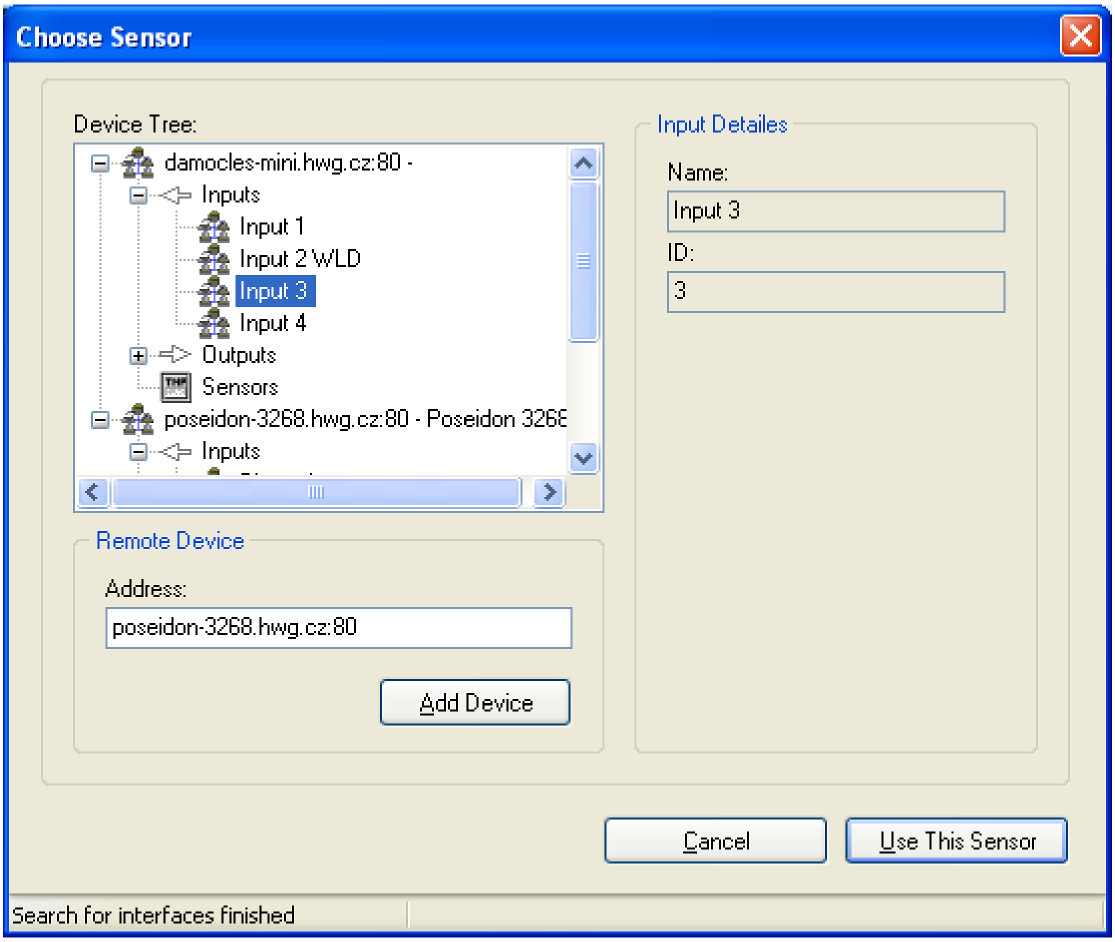
Run action if value is < 10,5

Run action if
☑ condition activated (alarm)
☑ condition deactivated (normal)

Run action after 15 Seconds

Action delay helps to filter out short failures in communication with the device.

You can also select a sensor by using the **Search Sensor** option, which opens a Device Tree list:



Choose Sensor

Device Tree:

```
⊟ damocles-mini.hwg.cz:80 -
   ⊟ Inputs
        Input 1
        Input 2 WLD
        Input 3
        Input 4
   ⊞ Outputs
     Sensors
⊟ poseidon-3268.hwg.cz:80 - Poseidon 3268
   ⊟ Inputs
```

Input Detailes

Name: Input 3

ID: 3

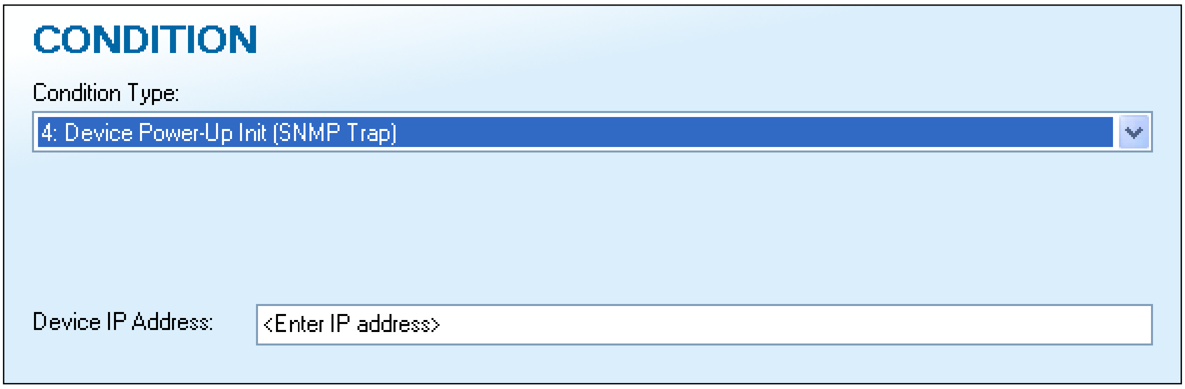
Remote Device

Address: poseidon-3268.hwg.cz:80

Search for interfaces finished

4: Device Power-Up Init (SNMP Trap)

This condition passively awaits and reacts to a SNMP Trap received from the device. It reacts to a trap sent after the power-up of the device. This type of rule is usually used to set a default state of relay outputs after the monitored device is started.

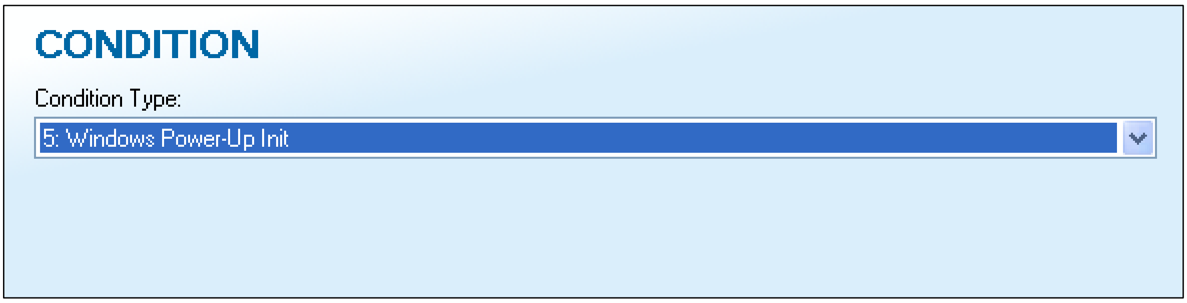

CONDITION

Condition Type: 4: Device Power-Up Init (SNMP Trap)

Device IP Address: <Enter IP address>

5: Windows Power-Up Init

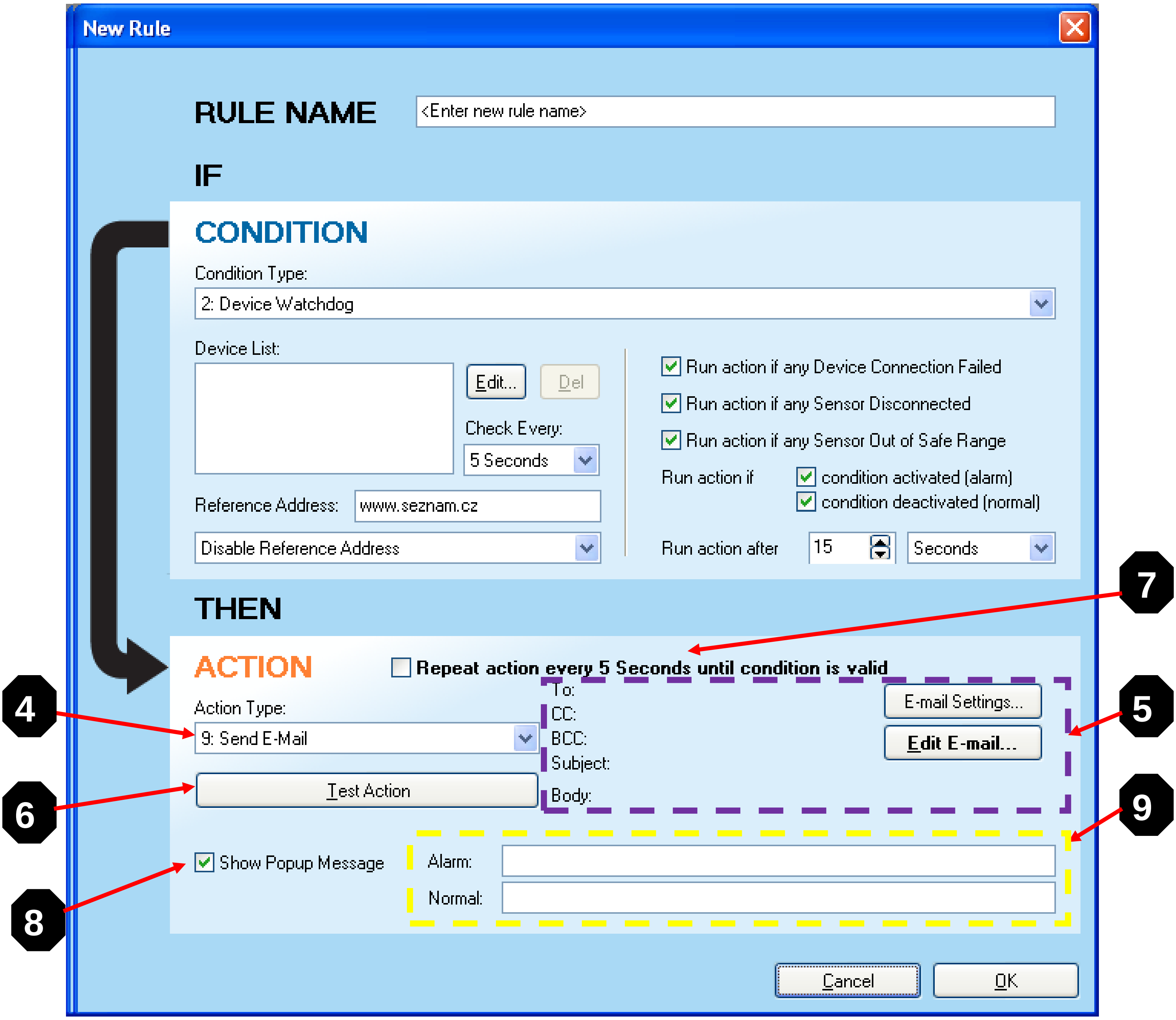
This condition triggers with the Windows power-up (On a computer where HWg-Trigger is installed). This option is usually used to set the default output states of connected remote devices.


CONDITION

Condition Type: 5: Windows Power-Up Init

Action settings

This section sets specific required actions - **Action Type (4)** and their parameters. It also offers test options.



RULE NAME <Enter new rule name>

Condition Type: 2: Device Watchdog

Device List:

Check Every: 5 Seconds

Reference Address: www.seznam.cz

Disable Reference Address

☑ Run action if any Device Connection Failed

☑ Run action if any Sensor Disconnected

☑ Run action if any Sensor Out of Safe Range

Run action if ☑ condition activated (alarm)
☑ condition deactivated (normal)

Run action after 15 Seconds

☐ Repeat action every 5 Seconds until condition is valid

Action Type: 9: Send E-Mail

To:
CC:
BCC:
Subject:
Body:

☑ Show Popup Message

Alarm:

Normal:

Action Detail (5)

Content of this section is directly related to the action type, as here you can set the details of the action, for example recipients' phone numbers, e-mail addresses or you can choose the relay outputs you want to control by this action.

Test Action (6)

This option tests the functionality of the settings.

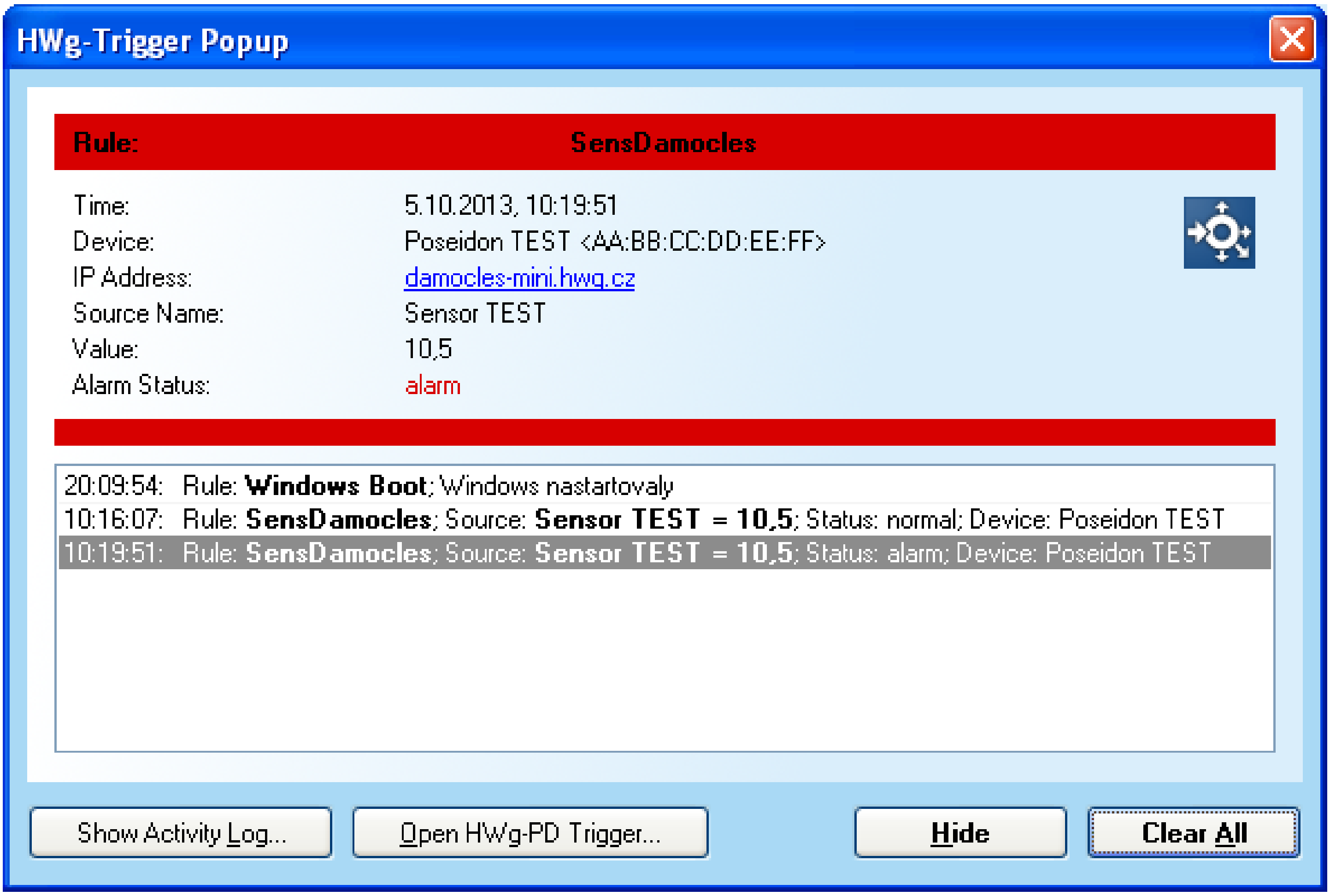
Repeat action every 5 seconds until condition is valid (7)

If activated, the action will repeat every 5 seconds until the rule's end conditions are met.

Can be used only in rules with **Device Watchdog** or **Sensor Value Watchdog** conditions.

Show Popup Message (8)

Beside action set in the **Action Type** field, HWg-Trigger will open a pop-up window with information about the detected event:



Rule: SensDamocles

Time: 5.10.2013, 10:19:51

Device: Poseidon TEST <AA:BB:CC:DD:EE:FF>

IP Address: damocles-mini.hwg.cz

Source Name: Sensor TEST

Value: 10,5

Alarm Status: alarm

```
20:09:54:  Rule: Windows Boot; Windows nastartovaly
10:16:07:  Rule: SensDamocles; Source: Sensor TEST = 10,5; Status: normal; Device: Poseidon TEST
10:19:51:  Rule: SensDamocles; Source: Sensor TEST = 10,5; Status: alarm; Device: Poseidon TEST
```

Message Detail (9)

Alarm field is used for entering the text to be shown in the pop-up window. Text entered into a field **Normal** will be used after the return to the normal state.

Action Type (4)

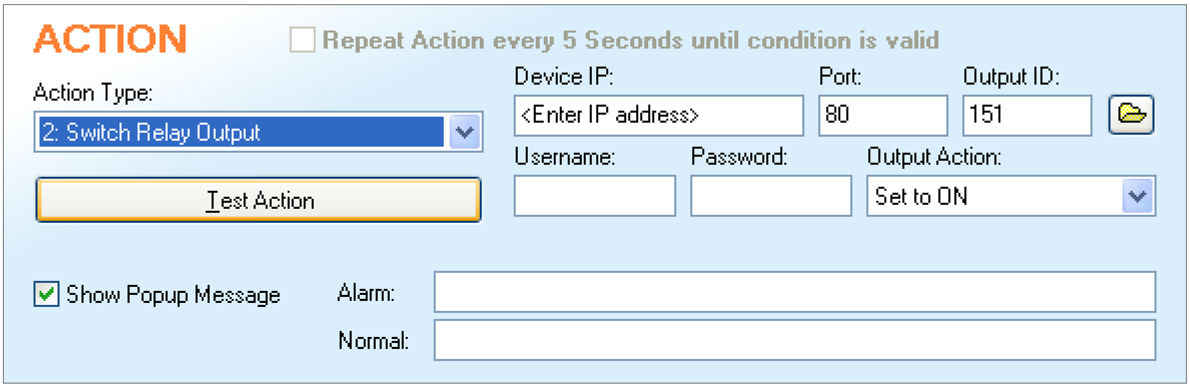
1: None

Option used to deactivate this section in order to show an alert window only. Selecting this option will automatically activate the **Show Popup Message (6)** option.

2: Switch Relay Output

This option enables you to control DO digital outputs on Poseidon and Damocles units.

Output(**Output Action**) can be switched, turned off, swithched for a specific time while the alarm is active, switch off at the end of alarm state.



ACTION

□ Repeat Action every 5 Seconds until condition is valid

Action Type: 2: Switch Relay Output

Device IP: <Enter IP address>

Port: 80

Output ID: 151

Username:

Password:

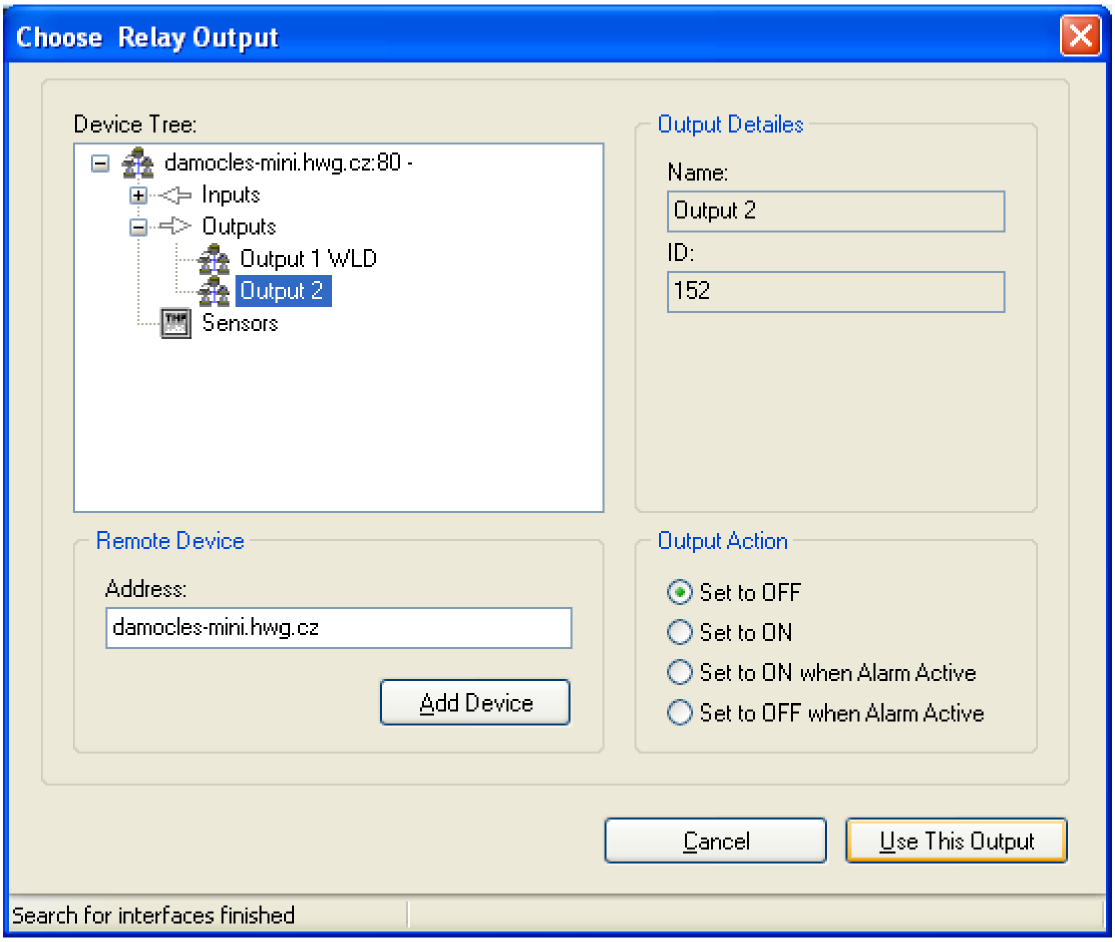
Output Action: Set to ON

☑ Show Popup Message

Alarm:

Normal:

Clicking the folder icon will open a window with a Device Tree, where you can select an output:



Choose Relay Output

Device Tree:

- damocles-mini.hwg.cz:80 -
  - Inputs
  - Outputs
    - Output 1 WLD
    - Output 2
  - Sensors

Output Detailes

Name: Output 2

ID: 152

Remote Device

Address: damocles-mini.hwg.cz

Output Action

● Set to OFF

○ Set to ON

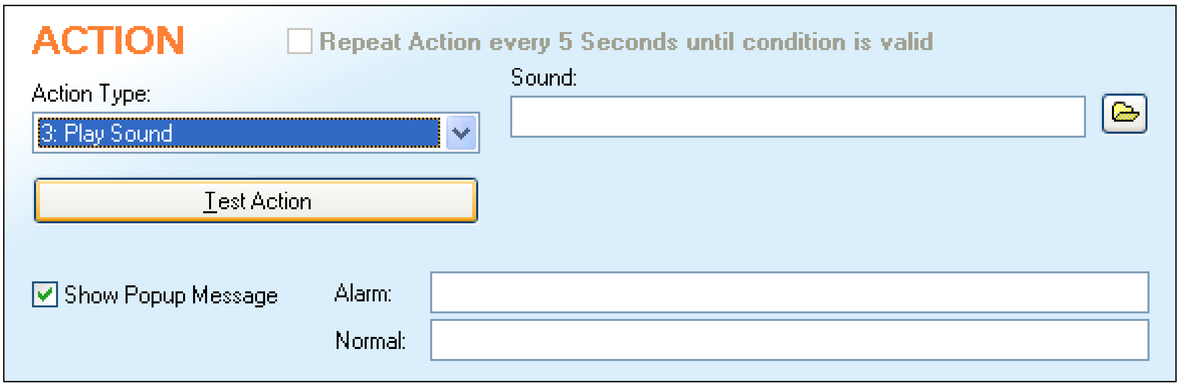
○ Set to ON when Alarm Active

○ Set to OFF when Alarm Active

Search for interfaces finished

3: Play Sound

In case of alarm with this rule a sound in a WAV format will be played. Clicking the folder icon will open a browser where you can select the WAV file (The default folder is %SystemRoot%\Media – usually C:\Windows\Media).


ACTION

□ Repeat Action every 5 Seconds until condition is valid

Action Type: 3: Play Sound

Sound:

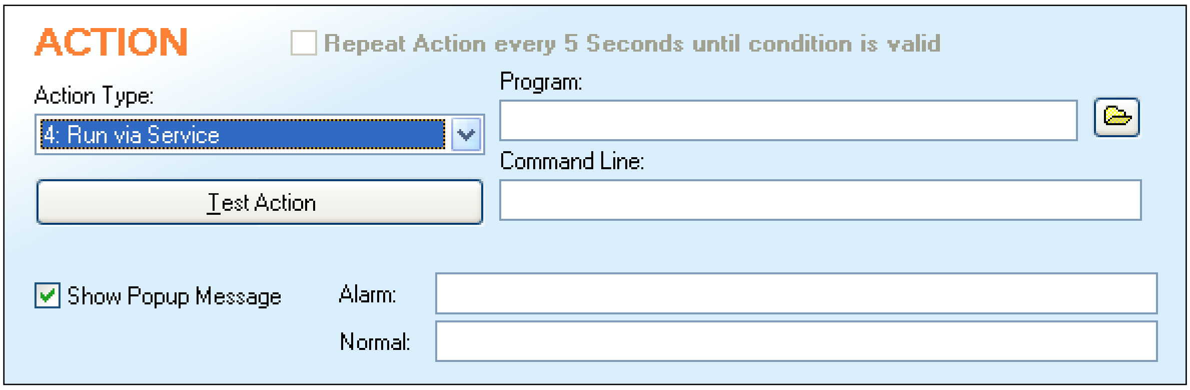
☑ Show Popup Message

Alarm:

Normal:

4: Run via Service

Opens an external application – This option is used mainly for opening applications on Windows Servers – in cases where a restart without logged user is needed or where opening the visual interface of an application is not required.
Path to an .exe file can be selected manually or installed in the system. **Command Line** allows defining the application opening parameters – more info in **Opened applications parameters**.


ACTION

□ Repeat Action every 5 Seconds until condition is valid

Action Type: 4: Run via Service

Program:

Command Line:

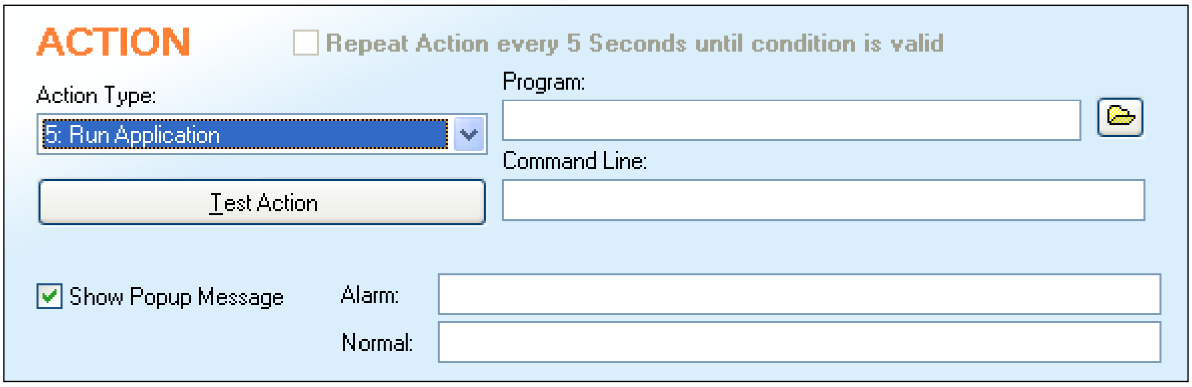
☑ Show Popup Message

Alarm:

Normal:

5: Run Application

Opens a graphic interface of an external application. Requires the user to be logged in. Path to the .exe file can be selected manually or installed in the system. **Command Line** allows defining of application opening parameters – more info in **Opened applications parameters**.


ACTION

□ Repeat Action every 5 Seconds until condition is valid

Action Type: 5: Run Application

Program:

Command Line:

☑ Show Popup Message

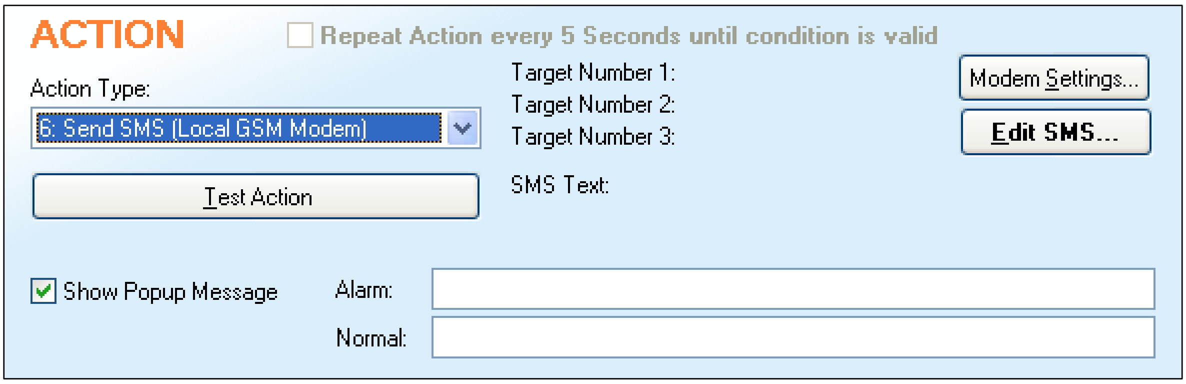
Alarm:

Normal:

! **Run Application** and **Play Sound** options can be used only if a user is logged in.

6: Send SMS (Local GSM Modem)

Sends an SMS to up to 3 phone numbers, using an external modem ModemCom/G10.


ACTION

□ Repeat Action every 5 Seconds until condition is valid

Action Type: 6: Send SMS (Local GSM Modem)

Target Number 1:
Target Number 2:
Target Number 3:

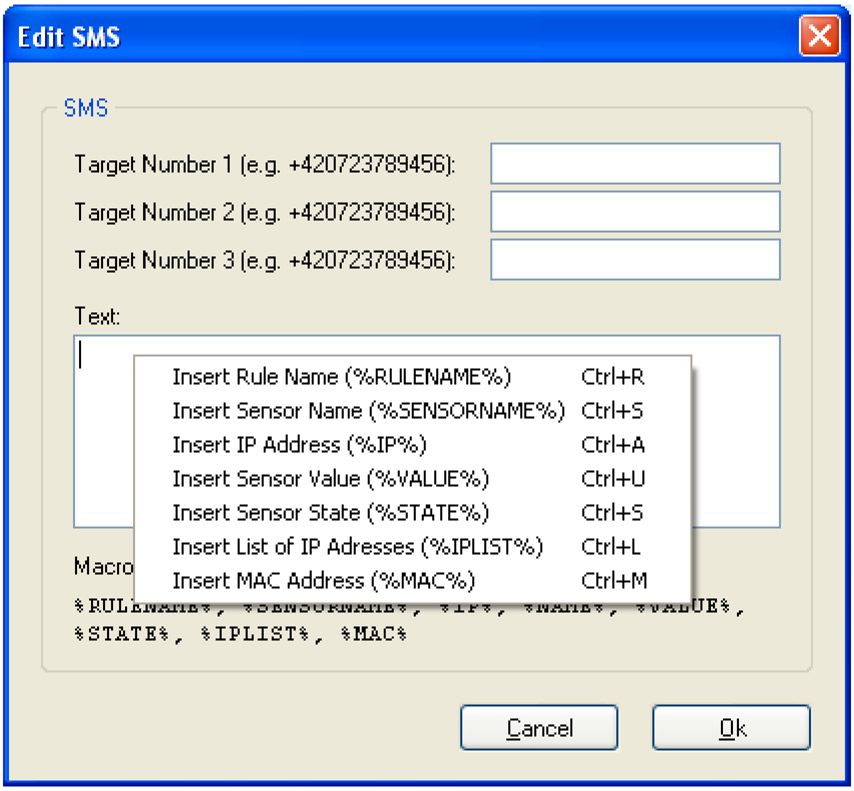
SMS Text:

☑ Show Popup Message

Alarm:

Normal:

- With macros you can include also values received with the event information into the SMS text (more info in **Macros**). Right clicking into the text field can open a list of macros. You can also use the key shortcuts for entering the macros.


Edit SMS

SMS

Target Number 1 (e.g. +420723789456):
Target Number 2 (e.g. +420723789456):
Target Number 3 (e.g. +420723789456):

Text:

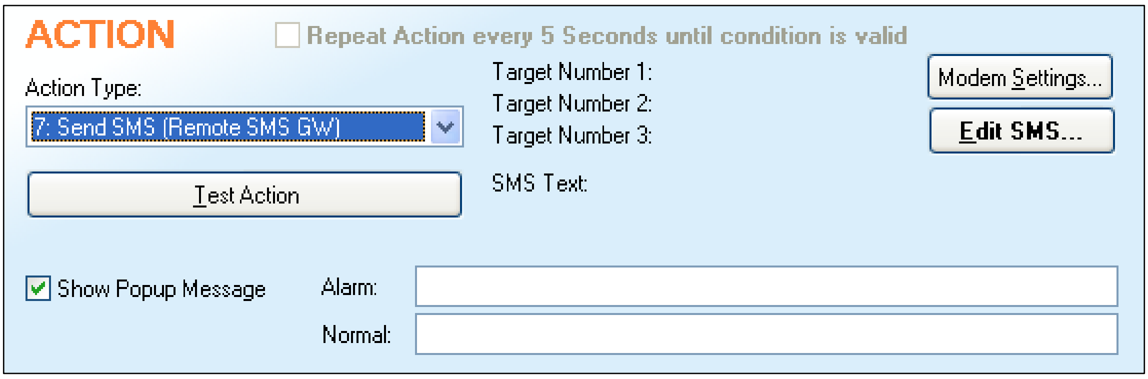
Macro

%RULENAME%, %SENSORNAME%, %IP%, %NAME%, %VALUE%,
%STATE%, %IPLIST%, %MAC%

Insert Rule Name (%RULENAME%) Ctrl+R
Insert Sensor Name (%SENSORNAME%) Ctrl+S
Insert IP Address (%IP%) Ctrl+A
Insert Sensor Value (%VALUE%) Ctrl+U
Insert Sensor State (%STATE%) Ctrl+S
Insert List of IP Adresses (%IPLIST%) Ctrl+L
Insert MAC Address (%MAC%) Ctrl+M
Cancel
Ok

7: Send SMS (Remote SMS GW)

Sends SMS to up to three phone numbers via external SMS gateway (**Poseidon**). More about gateway settings in **Remote SMS Gateway - Global Settings.** With macros you can include in the SMS text also values received with the event information (More in **Macros**).



□ Repeat Action every 5 Seconds until condition is valid

Action Type: 7: Send SMS (Remote SMS GW)

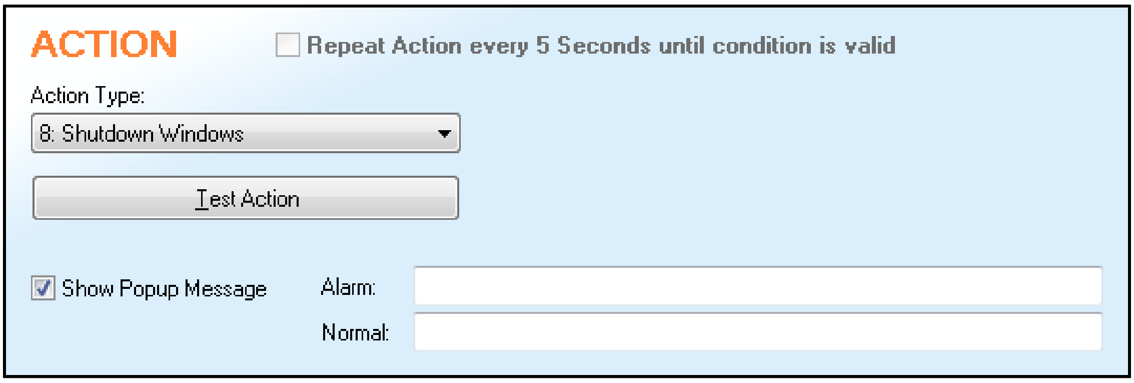
Target Number 1:
Target Number 2:
Target Number 3:
SMS Text:

☑ Show Popup Message

Alarm:
Normal:

8: Shutdown Windows

Shuts down Windows on which the HWg-Trigger installation is running, if a condition is met.



□ Repeat Action every 5 Seconds until condition is valid

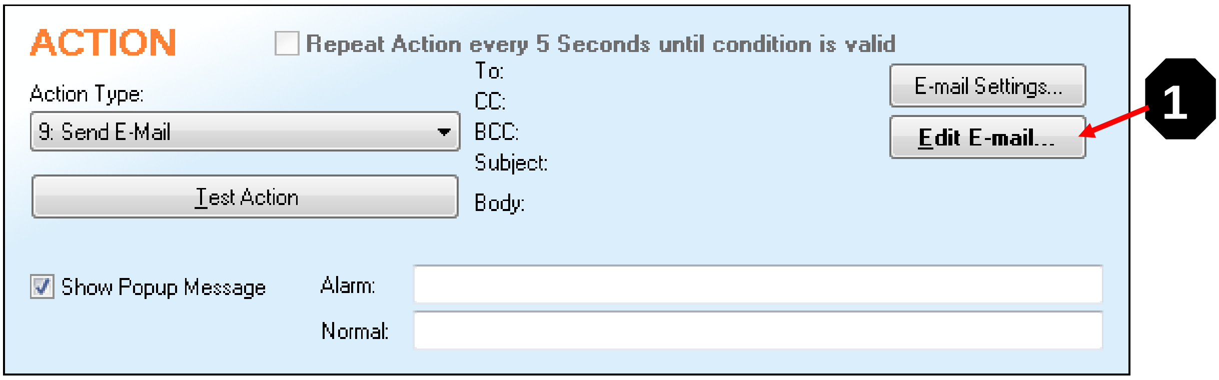
Action Type: 8: Shutdown Windows

☑ Show Popup Message

Alarm:
Normal:

9: Send E-mail

Sends a predefined e-mail via entered SMTP server – more info in **SMPT Server - Global/Settings.** As is SMS messages, you can use macros also in e-mails (more in **Macros**)



□ Repeat Action every 5 Seconds until condition is valid

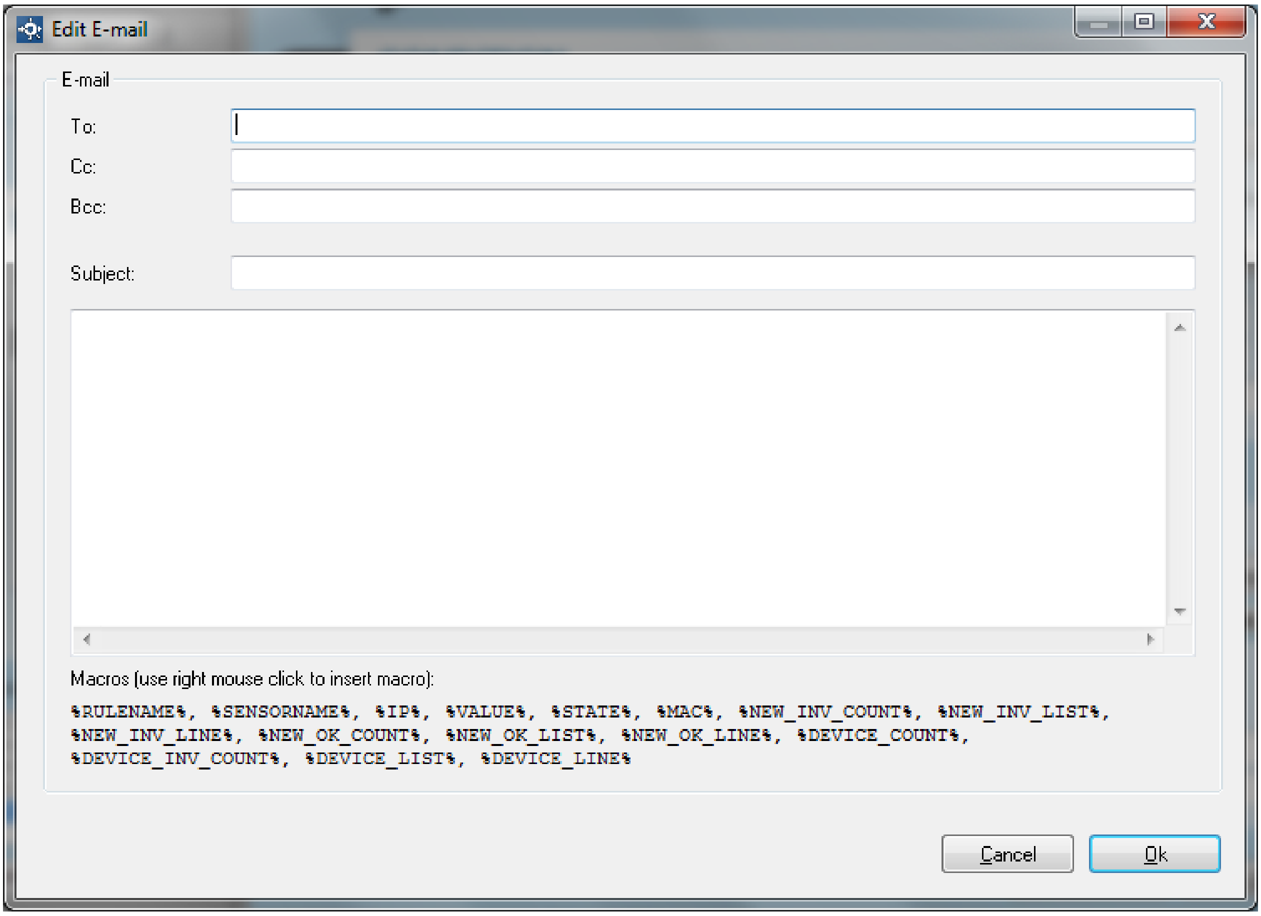
Action Type: 9: Send E-Mail

To:
CC:
BCC:
Subject:
Body:

☑ Show Popup Message

Alarm:
Normal:

Email text editor (1)



Macros (use right mouse click to insert macro):

%RULENAME%, %SENSORNAME%, %IP%, %VALUE%, %STATE%, %MAC%, %NEW_INV_COUNT%, %NEW_INV_LIST%, %NEW_INV_LINE%, %NEW_OK_COUNT%, %NEW_OK_LIST%, %NEW_OK_LINE%, %DEVICE_COUNT%, %DEVICE_INV_COUNT%, %DEVICE_LIST%, %DEVICE_LINE%

Macros

Macros are variables allowing you to enter values received with SNMP Traps into e-mails and SMS messages. Currently supported variables are:

- %RULENAME% - Rule name
- %STATE% - Alarm/Normal state – defines start or the end of each action
- %SENSORNAME% - Name of a sensor this message applies to (not for rules of Device watchdog type)
- %VALUE% - Value of a sensor this message applies to (not for rules of Device watchdog type)
- %IP% - IP address of a device this message applies to (not for rules of Device watchdog type)
- %MAC% - MAC address of a device this message applies to (not for rules of Device watchdog type)
- %NEW_INV_COUNT% - Number of devices in alarm state
- %NEW_INV_LIST% - List of devices in alarm state, printed in column
- %NEW_INV_LINE% - List of devices in alarm state, printed in line
- %NEW_OK_COUNT% - Number of devices in normal state
- %NEW_OK_LIST% - List of devices in normal state, printed in column
- %NEW_OK_LINE% - List of devices in normal state, printed in line
- %DEVICE_COUNT% - Number of items in the list of monitored devices (for rules of Device watchdog type)
- %DEVICE_INV_COUNT% - Number of devices where an action was activated (for rules of Device watchdog type)

- %DEVICE_LIST% - List of monitored devices, printed in column
- %DEVICE_LINE% - List of monitored devices, printed in line

Started applications parameters

HWg-Trigger allows opening of external applications using their directory parameters. Eventually, by using the macros, it can also enter into the parameters values received with the traps (IP address of a device or a sensor value, etc.). An application has to have its opening enabled through a command line. The parameters description vary with a particular application, but usually it could be printed out by opening the application with a /H or /? parameter.

File menu - Global Settings

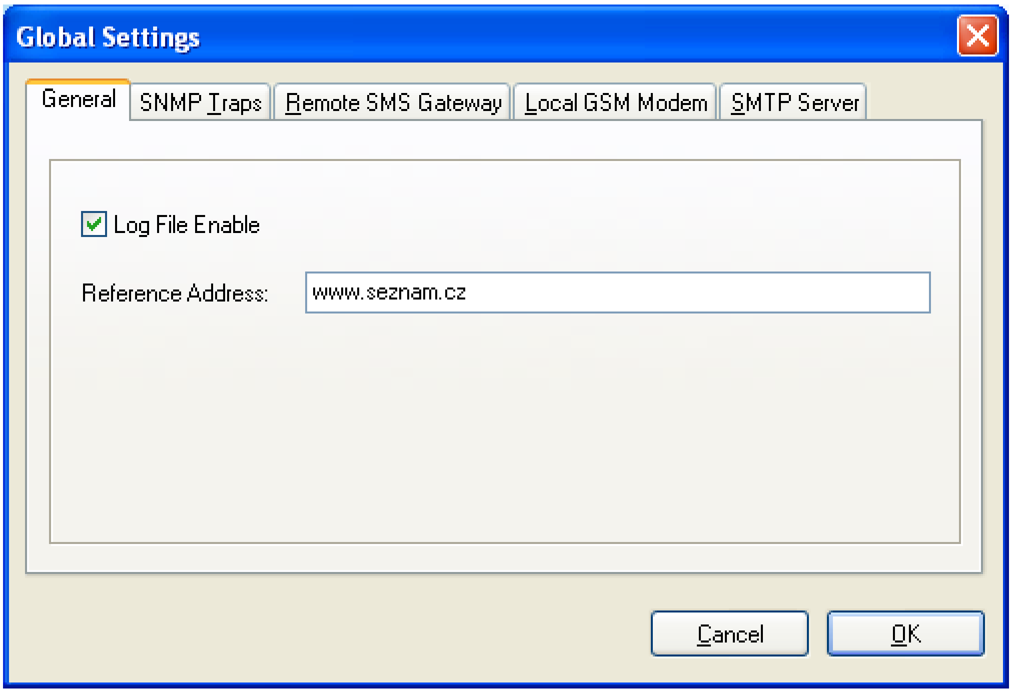
Used for setting the basic operational parameters.

! You have to be logged in in order to access this menu. A user is logged in automatically, unless you change a password using a special utility. Then it is always necessary to log in manually through a **File/Login** form.

General – Global Settings

On the **General** tab there is an option to deactivate logging of the HWg-Trigger operation info into the log file. In default the logging is enabled (**Log File Enable** – checkbox ticked), however in order to calibrate the functions and save the storage capacity, the settings can be changed (For standard usage it is not recommended to disable this option).

On this tab it is also possible to set a reference server (**Reference Address**), which is used for controlling the connectivity with the monitored devices.

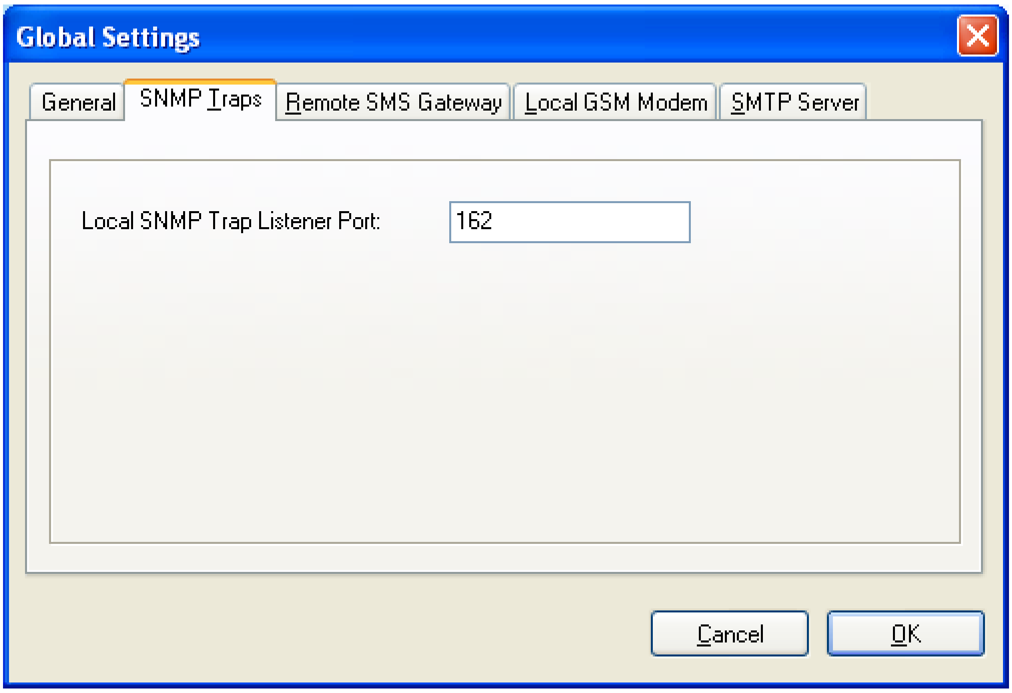


☑ Log File Enable

Reference Address: www.seznam.cz

SNMP Traps – Global Settings

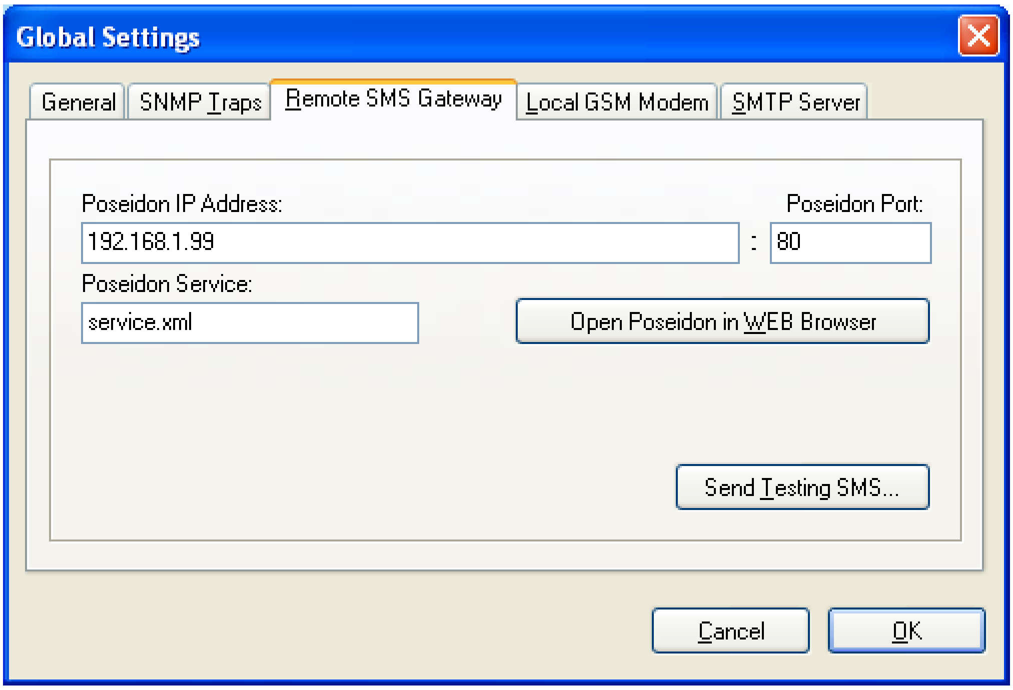
Here you can set a listening port for SNMP Traps (for **Sensor Alert, Device Power-Up Init** events). The port is set to 162 in default (port reserved for SNMP Traps), however this can be changed on systems, which use SNMP Traps.



Local SNMP Trap Listener Port: 162

Remote SMS Gateway – Global Settings

For **Send SMS (Remote GW)** action it is necessary to set a connection with a remote SMS gateway on this tab. A Poseidon device can be used as a SMS gateway and it is basically enough to enter a correct IP address of a Poseidon unit (**Poseidon IP Address**) and an html protocol gateway (**Poseidon Port** – 80 in default) and configure the SMS sending options in the Poseidon directly (**Open Poseidon in WEB Browser**).



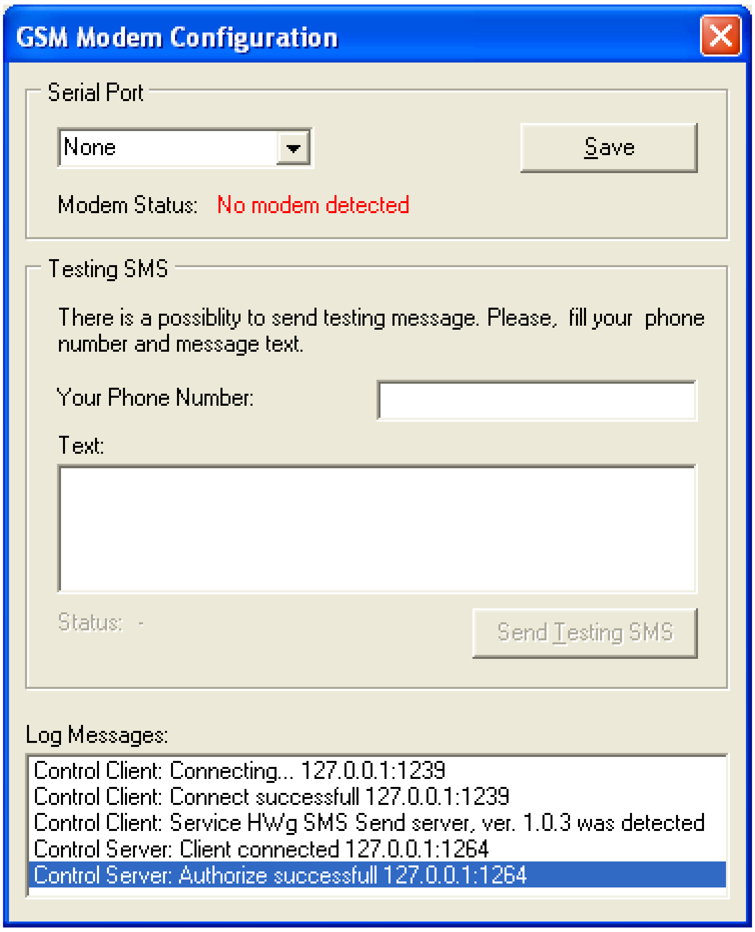
Poseidon IP Address: 192.168.1.99

Poseidon Port: 80

Poseidon Service: service.xml

Local GSM Modem – Global Settings

In order to use **Send SMS (Local GSM Modem)** action, it is necessary to enter a number of a port where a GSM modem is connected. In the **Log Messages** field you can find SMS service log messages.



GSM Modem Configuration

Serial Port: None

Modem Status: No modem detected

Testing SMS

There is a possiblity to send testing message. Please, fill your phone number and message text.

Your Phone Number:

Text:

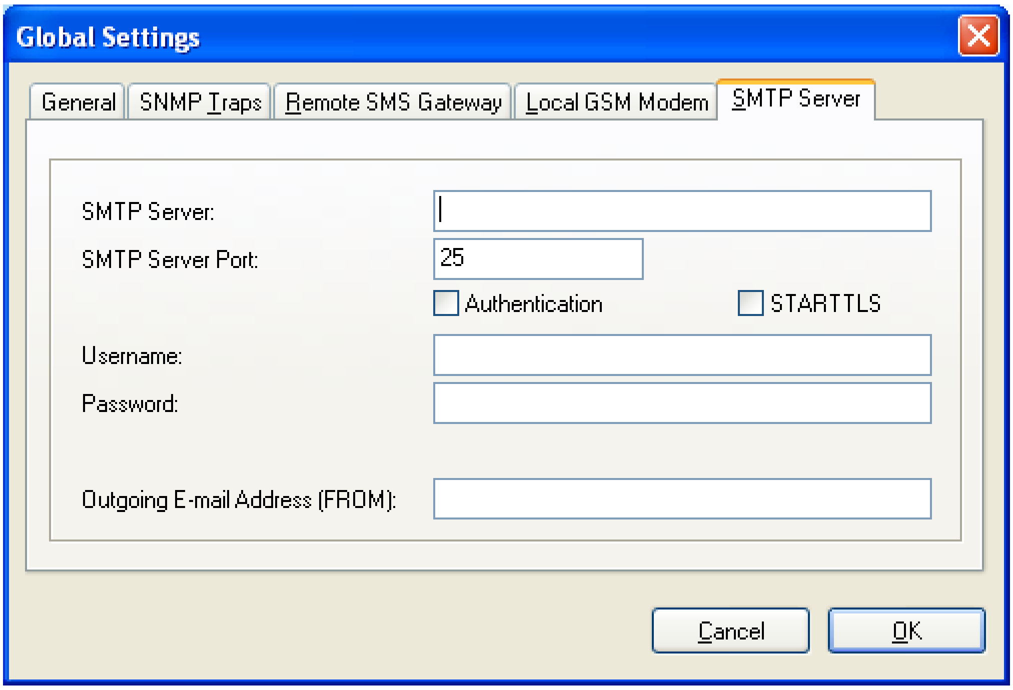
Status: -

Log Messages:

```
Control Client: Connecting... 127.0.0.1:1239
Control Client: Connect successfull 127.0.0.1:1239
Control Client: Service HWg SMS Send server, ver. 1.0.3 was detected
Control Server: Client connected 127.0.0.1:1264
Control Server: Authorize successfull 127.0.0.1:1264
```

SMTP Server – Global Settings

Parameters of a SMTP Server through which HWg-Trigger sends e-mails with operation info (action **Send E-mail)**.



SMTP Server:

SMTP Server Port: 25

□ Authentication □ STARTTLS

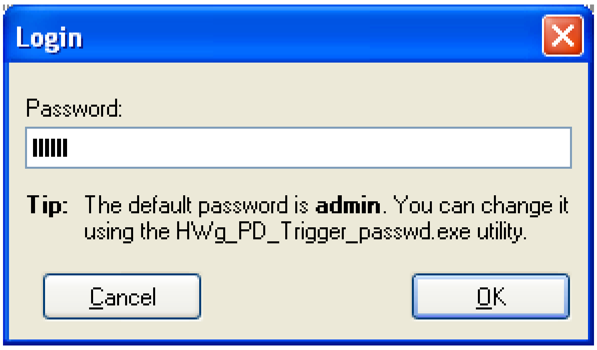
Username:

Password:

Outgoing E-mail Address (FROM):

File menu - Login

This menu is designated for authentication of user authorisation to adjust the settings of HW-Trigger – change monitored devices/sensors, adjust rules settings and to make other configuration changes. In default it is not necessary to log in, as the program is logging automatically with a password **„admin“.**



Password: ||||||

Tip: The default password is **admin**. You can change it using the HWg_PD_Trigger_passwd.exe utility.

The password can be changed using **HWg_PD_Trigger2_passwd.exe** utility, located in the HWg-Trigger folder - **C:\Program Files\HW-group\HWg-Trigger**. If the password is changed, it is required to log in prior to access most of the functions of HWg-Trigger.

Edit menu

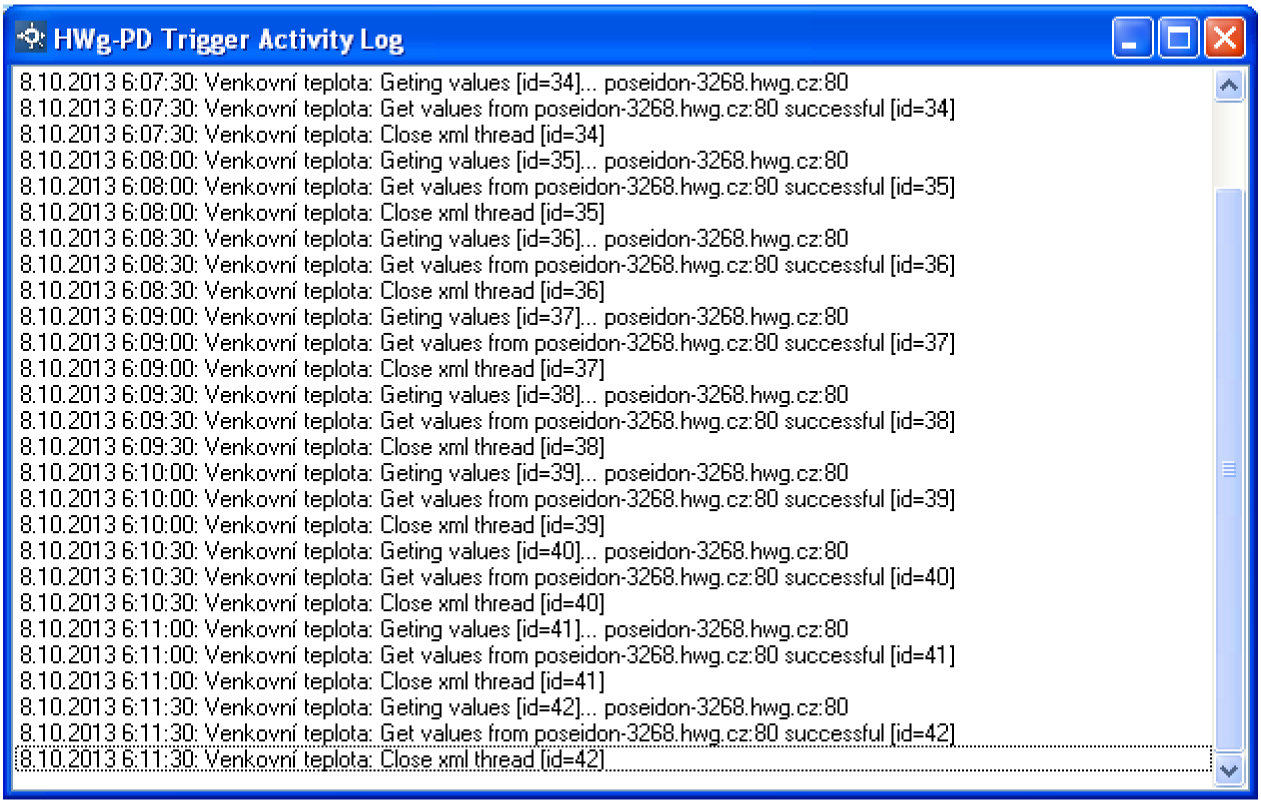
In this menu you can find three functions designated for rules management - **New Rule, Remove Rule** and **Edit Rule**.

Menu Window

A function available also for users not logged in through the login menu.

Show Activity Log

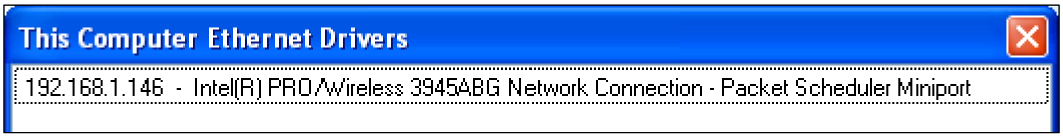
With this function you can open the application's log file, where all the events that were processed by HWg-Trigger during its functionality are recorded. This file is a very useful source of information, as the file shows details of all processed events.



```
8.10.2013 6:07:30: Venkovní teplota: Geting values [id=34]... poseidon-3268.hwg.cz:80
8.10.2013 6:07:30: Venkovní teplota: Get values from poseidon-3268.hwg.cz:80 successful [id=34]
8.10.2013 6:07:30: Venkovní teplota: Close xml thread [id=34]
8.10.2013 6:08:00: Venkovní teplota: Geting values [id=35]... poseidon-3268.hwg.cz:80
8.10.2013 6:08:00: Venkovní teplota: Get values from poseidon-3268.hwg.cz:80 successful [id=35]
8.10.2013 6:08:00: Venkovní teplota: Close xml thread [id=35]
8.10.2013 6:08:30: Venkovní teplota: Geting values [id=36]... poseidon-3268.hwg.cz:80
8.10.2013 6:08:30: Venkovní teplota: Get values from poseidon-3268.hwg.cz:80 successful [id=36]
8.10.2013 6:08:30: Venkovní teplota: Close xml thread [id=36]
8.10.2013 6:09:00: Venkovní teplota: Geting values [id=37]... poseidon-3268.hwg.cz:80
8.10.2013 6:09:00: Venkovní teplota: Get values from poseidon-3268.hwg.cz:80 successful [id=37]
8.10.2013 6:09:00: Venkovní teplota: Close xml thread [id=37]
8.10.2013 6:09:30: Venkovní teplota: Geting values [id=38]... poseidon-3268.hwg.cz:80
8.10.2013 6:09:30: Venkovní teplota: Get values from poseidon-3268.hwg.cz:80 successful [id=38]
8.10.2013 6:09:30: Venkovní teplota: Close xml thread [id=38]
8.10.2013 6:10:00: Venkovní teplota: Geting values [id=39]... poseidon-3268.hwg.cz:80
8.10.2013 6:10:00: Venkovní teplota: Get values from poseidon-3268.hwg.cz:80 successful [id=39]
8.10.2013 6:10:00: Venkovní teplota: Close xml thread [id=39]
8.10.2013 6:10:30: Venkovní teplota: Geting values [id=40]... poseidon-3268.hwg.cz:80
8.10.2013 6:10:30: Venkovní teplota: Get values from poseidon-3268.hwg.cz:80 successful [id=40]
8.10.2013 6:10:30: Venkovní teplota: Close xml thread [id=40]
8.10.2013 6:11:00: Venkovní teplota: Geting values [id=41]... poseidon-3268.hwg.cz:80
8.10.2013 6:11:00: Venkovní teplota: Get values from poseidon-3268.hwg.cz:80 successful [id=41]
8.10.2013 6:11:00: Venkovní teplota: Close xml thread [id=41]
8.10.2013 6:11:30: Venkovní teplota: Geting values [id=42]... poseidon-3268.hwg.cz:80
8.10.2013 6:11:30: Venkovní teplota: Get values from poseidon-3268.hwg.cz:80 successful [id=42]
8.10.2013 6:11:30: Venkovní teplota: Close xml thread [id=42]
```

Show IP Address of this Computer

This option prints out all the IP addresses of the network interfaces on a PC/server where the HWg-Trigger is installed. This information is important for setting the target addresses of SNMP Traps on Poseidon and Damocles devices (More in **How to set a device to work with HWg-Trigger**).



```
192.168.1.146  -  Intel(R) PRO/Wireless 3945ABG Network Connection - Packet Scheduler Miniport
```

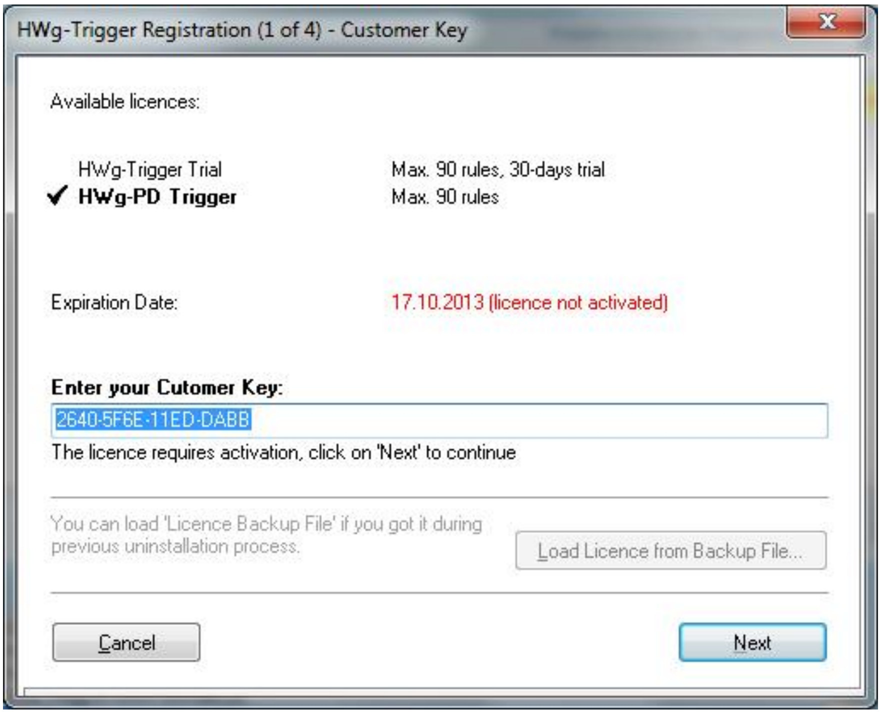
Menu Help

Registration

Registration function is used for entering the Customer Key of a purchased license to register the application.

! Trial version is working only for 30 days.

After ordering a full version of HWg-Trigger you will receive a registration number "Customer key", in a format: 1111-2222-3333-4444. Enter this number into the **Enter your Customer Key** field**.**


HWg-Trigger Registration (1 of 4) - Customer Key

Available licences:

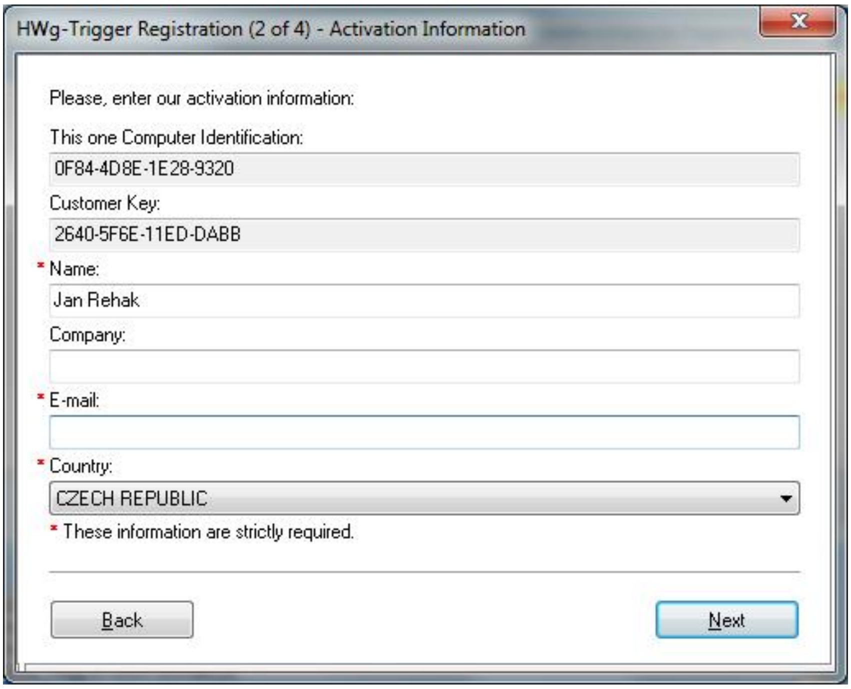
HWg-Trigger Trial	Max. 90 rules, 30-days trial
✓ **HWg-PD Trigger**	Max. 90 rules

Expiration Date: 17.10.2013 (licence not activated)

Enter your Cutomer Key:
2640-5F6E-11ED-DABB
The licence requires activation, click on 'Next' to continue

You can load 'Licence Backup File' if you got it during previous uninstallation process.

Then proceed with the registration by clicking the button **Next** and enter the other required details (fields marked with *).


HWg-Trigger Registration (2 of 4) - Activation Information

Please, enter our activation information:

This one Computer Identification:
0F84-4D8E-1E28-9320

Customer Key:
2640-5F6E-11ED-DABB

* Name:
Jan Rehak

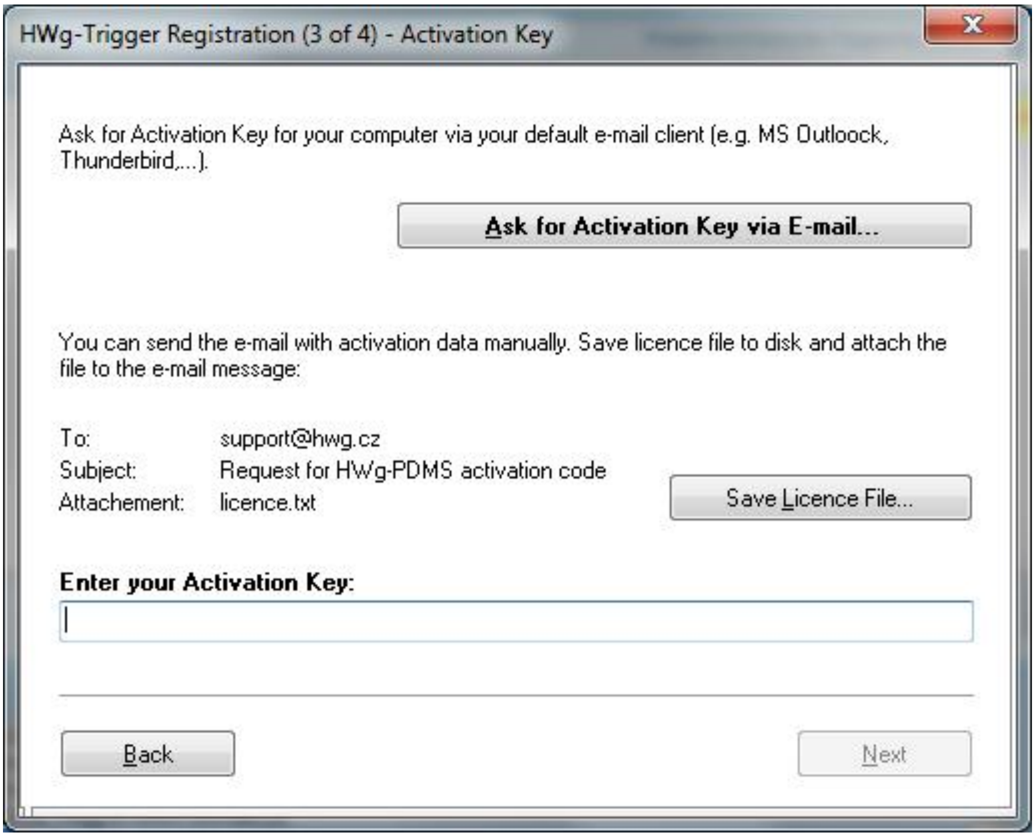
Company:

* E-mail:

* Country:
CZECH REPUBLIC

* These information are strictly required.

The software will generate a registration application "**licence.txt**".
This file then has to be saved and emailed to an email address shown next to the Save License File button.



HWg-Trigger Registration (3 of 4) - Activation Key

Ask for Activation Key for your computer via your default e-mail client (e.g. MS Outloock, Thunderbird,...).

Ask for Activation Key via E-mail...

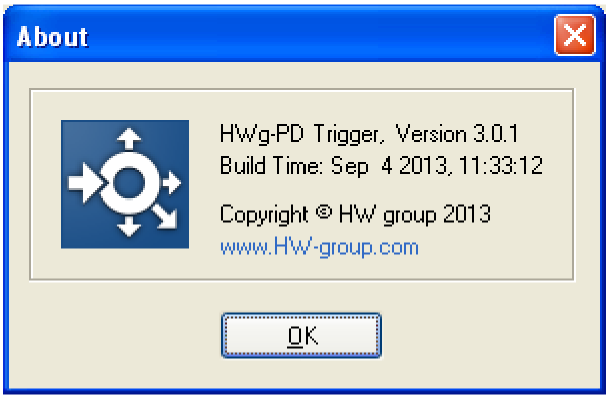
You can send the e-mail with activation data manually. Save licence file to disk and attach the file to the e-mail message:

To: support@hwg.cz
Subject: Request for HWg-PDMS activation code
Attachement: licence.txt

Save Licence File...
Enter your Activation Key:
Back
Next

Within 2-3 business days an "**Activation Key**" will be emailed back to you. The format of the code is **AAAAAAAA-BBBBBBBB-CCCCCCCC-DDDDDDDD**.

Function **"About"** will show a version number of your installation and its Build Time. This information is crucial for dealing with technical issues and therefore please include these details to your technical support inquiries.



About

HWg-PD Trigger, Version 3.0.1
Build Time: Sep 4 2013, 11:33:12

Copyright © HW group 2013
www.HW-group.com

How to set a device to work with HWg-Trigger

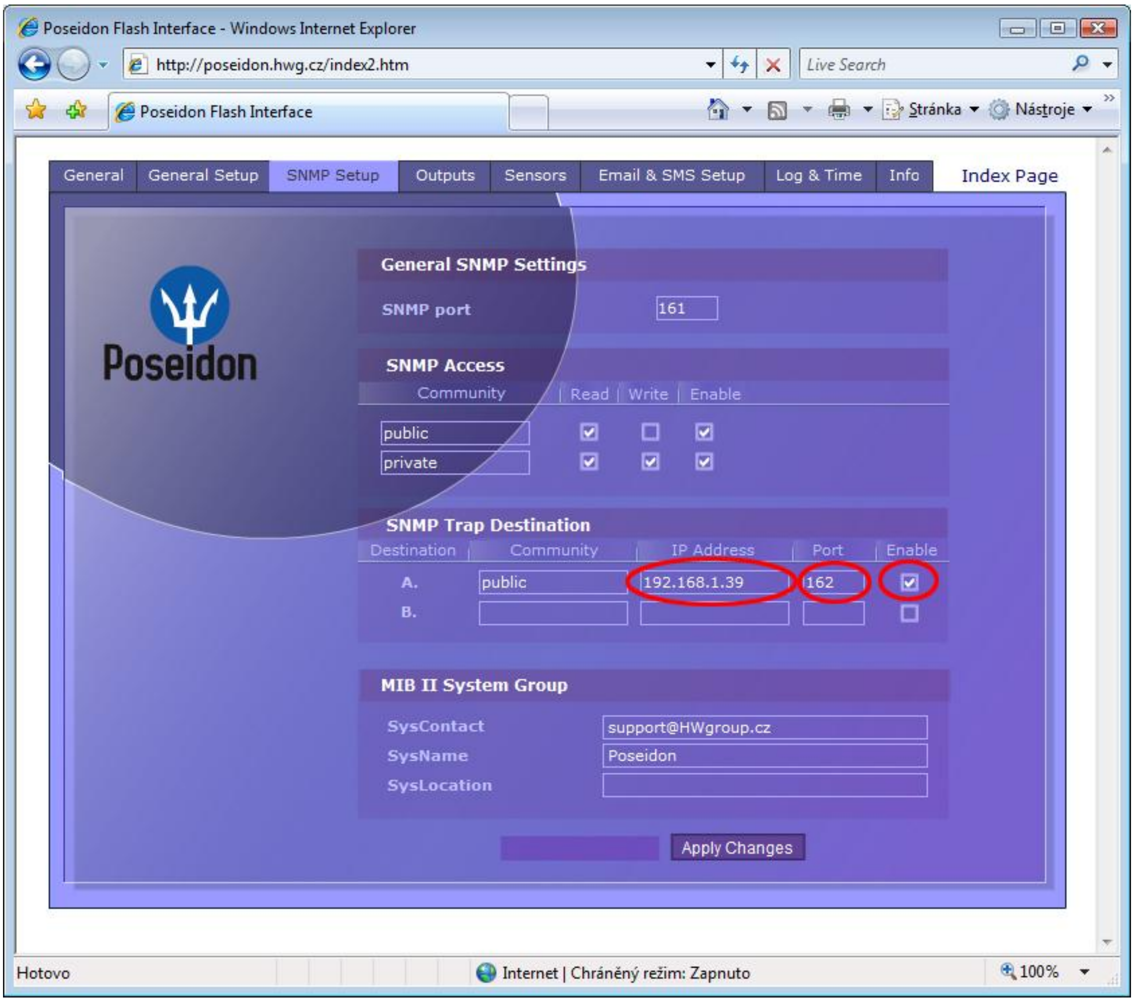
In order to set the Poseidon or Damocles units to work with HWg-Trigger, you first need to correctly set their SNMP parameters. As the configuration is thoroughly explained in the device manuals, we will point out only certain points here.

***Note:** Following rules apply only in case the Poseidon and Damocles units are at the same network as the computer with HWg-Trigger; eventually the PC has to be on a public IP address!*

Poseidon

Open the web interface of a Poseidon unit on a SNMP Setup tab. Here you can define the target destinations for SNMP Traps:

1) Into the IP Address field please enter an address found in the menu **Window /Show IP Address of this Computer** in HWg-Trigger.
2) Port has to be set to a same value as it is set in HWg-Trigger **- File/Global Settings** menu on the **SNMP Traps** tab **- Local SNMP Trap Listener Port** field (in default port 162).
3) Ticking the **Enable** checkbox activates sending of basic SNMP Traps (device power-up or reset).
4) On the **Sensors** tab enable the **Out of Safe Range SNMP Trap** option for each of the sensors you want to monitor. In case you want to monitor also the DI inputs, set the **Dry Contact Inputs state reaction** to **Send SNMP Trap**, eventually **Send SNMP Trap + SMS& Email** and define the alarm state.



General SNMP Settings

SNMP port: 161

SNMP Access

Community	Read	Write	Enable
public	☑	□	☑
private	☑	☑	☑

SNMP Trap Destination

Destination	Community	IP Address	Port	Enable
A.	public	192.168.1.39	162	☑
B.				□

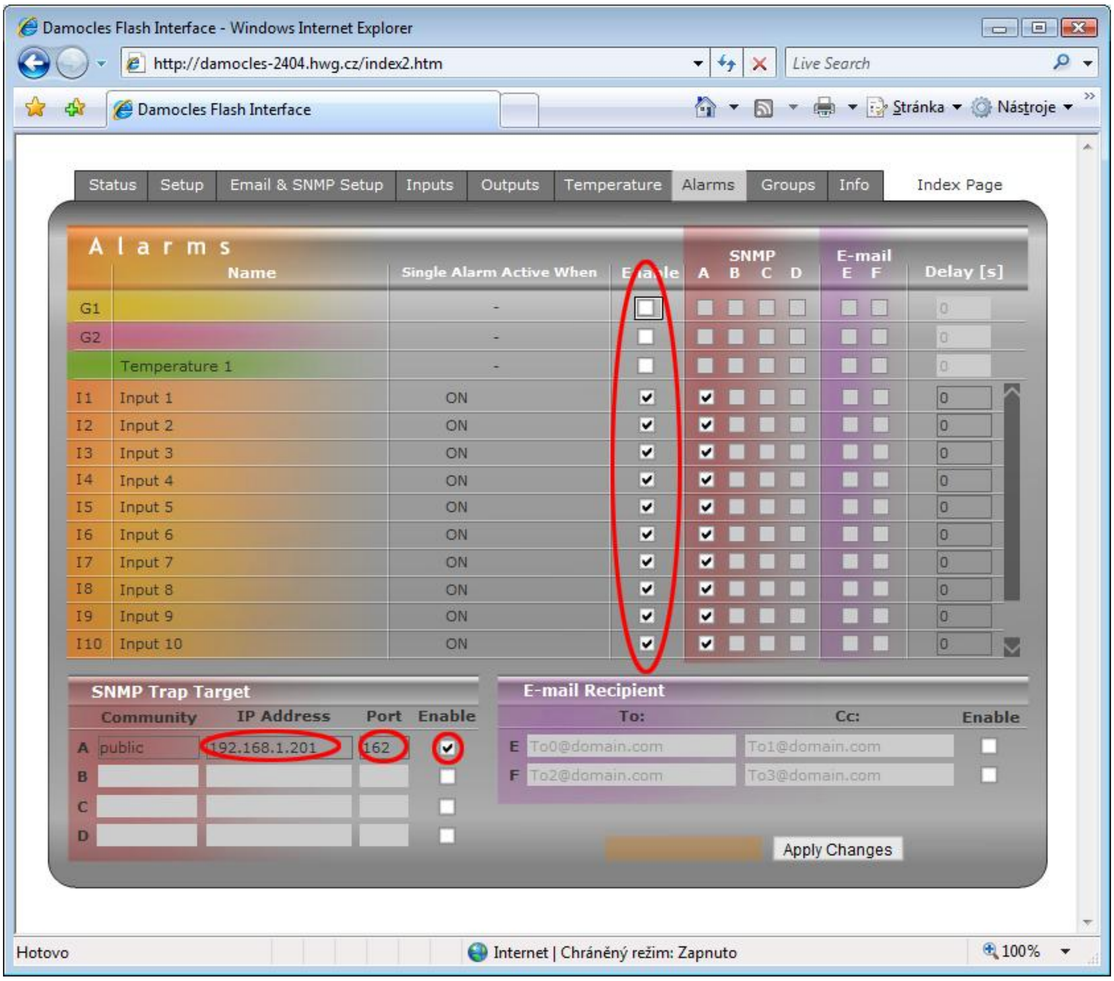
MIB II System Group

SysContact: support@HWgroup.cz
SysName: Poseidon
SysLocation:

Damocles

Damocles settings can be also changed through its FLASH interface, however with Damocles all the settings can be found on the **Alarms** tab.

If the target computer is not on a public IP address, instead of IP address a unique external address of an internet gate has to be set. It is also needed to set the packets directions, therefore please contact your network administrator for further assistance.



Alarms

	Name	Single Alarm Active When	Enable	SNMP A	B	C	D	E-mail E	F	Delay [s]
G1		-	☐	☐	☐	☐	☐	☐	☐	0
G2		-	☐	☐	☐	☐	☐	☐	☐	0
	Temperature 1	-	☐	☐	☐	☐	☐	☐	☐	0
I1	Input 1	ON	☑	☑	☐	☐	☐	☐	☐	0
I2	Input 2	ON	☑	☑	☐	☐	☐	☐	☐	0
I3	Input 3	ON	☑	☑	☐	☐	☐	☐	☐	0
I4	Input 4	ON	☑	☑	☐	☐	☐	☐	☐	0
I5	Input 5	ON	☑	☑	☐	☐	☐	☐	☐	0
I6	Input 6	ON	☑	☑	☐	☐	☐	☐	☐	0
I7	Input 7	ON	☑	☑	☐	☐	☐	☐	☐	0
I8	Input 8	ON	☑	☑	☐	☐	☐	☐	☐	0
I9	Input 9	ON	☑	☑	☐	☐	☐	☐	☐	0
I10	Input 10	ON	☑	☑	☐	☐	☐	☐	☐	0

SNMP Trap Target

	Community	IP Address	Port	Enable
A	public	192.168.1.201	162	☑
B				☐
C				☐
D				☐

E-mail Recipient

	To:	Cc:	Enable
E	To0@domain.com	To1@domain.com	☐
F	To2@domain.com	To3@domain.com	☐