WatchDog

Options/Actions

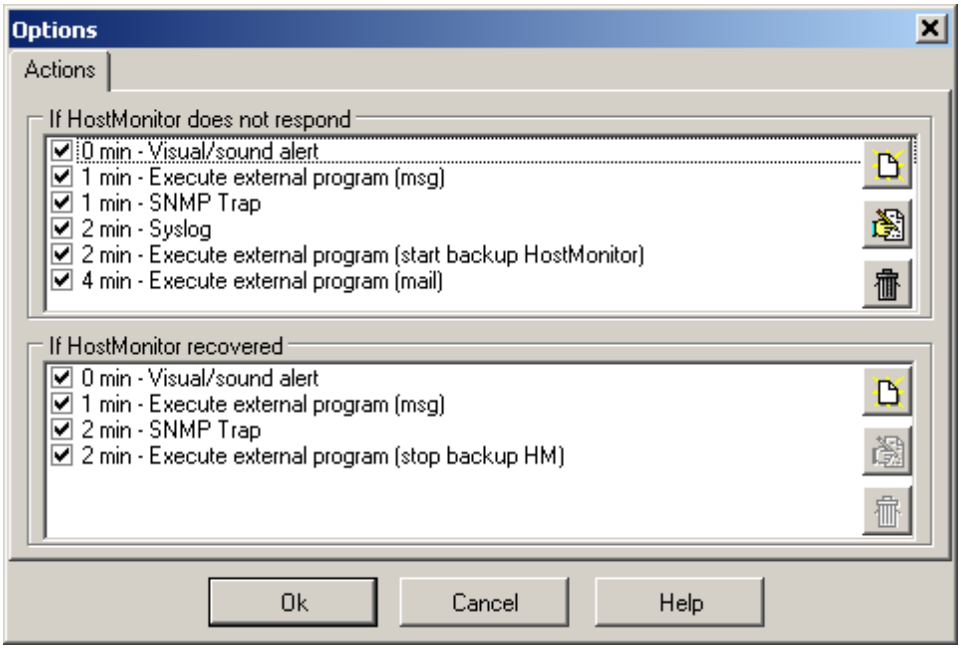
If you want to receive alerts while you away from HostMonitor and WatchDog, you need to setup “actions”.

You may setup 2 lists of actions
- one set will be executed when HostMonitor does not respond for some time
- another set will be executed when connection established and it is stable for specified period of time

To work with actions you can use the Options dialog. To bring up this dialog use menu Options

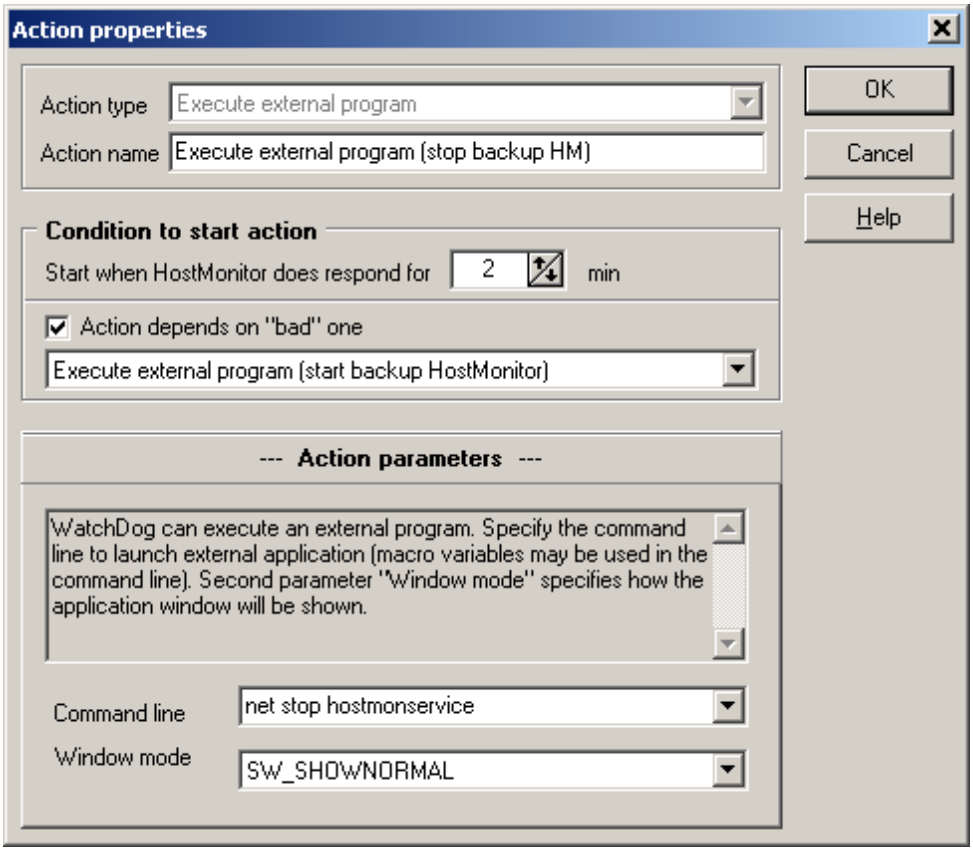
To modify each set of actions use buttons located on right side of the list:

- **Add** Add new action into set
- **Edit** Bring up Action Properties dialog for editing parameters of the selected action
- **Delete** Remove selected action



Here is a list of available actions to kick off in response to a problem:
- Visual/Sound alert
- Execute external program
- Syslog
- SNMP Trap

Action properties are defined in the Action Properties dialog. Some properties are common across all action types. However, each type of action has a set of parameters that are specific to the action type. Let's have a look at the common properties first (these parameters located in the upper half of the Action Properties dialog):



Action name
The name of the action; WatchDog auto populates this field with a suggested name based on the type of action; you can change that name to whatever name you want.

Condition to start action
Start when HostMonitor does not respond for N min
This parameter tells when “bad” action should be executed – when connection to HostMonitor is dropped and reconnect attempts fail for N minutes
Start when HostMonitor does respond for N min
This parameter tells when “good” action should be executed – when connection to HostMonitor is established and it is stable for N minutes (0 means action should be executed when connection just established)

Action depends on "bad" one
This optional parameter is available for "Good" actions only. You can set "Good" action dependable on a "Bad" action. Why do you need it? For example you defined "Bad" action to send an e-mail notification to the network administrator when connection lost for 3 minutes, also you defined «Good» action to send a notification when connection restored and it is stable for 2 minutes. What happens if connection was lost for 1 minute then everything works fine for an hour? WatchDog will not send a notification about failure (because connection restored after 1 minute) but the program will send notification about restoring "Good" status. To avoid unnecessary "Good" action execution you can mark "Action depends on bad one" option and select "Bad" action. In this case WatchDog will start "Good" action only if corresponding "Bad" action was executed.

Action-specific settings:

Visual/Sound alert

This action is designed to play a sound file (WAV, MID, etc). In addition to the common action parameters, the «Visual/Sound alert» action has the following options:

Sound file
Specify full path to the sound file or click small button on the right side and select file from the Open File dialog.

Show WakeUP window and play sound every N sec
With this option enabled WatchDog will display a popup window with information about the event and will play a sound repeatedly until you click "Stop sound" button.
Note: If you start WatchDog on Windows Vista, 2008 or Windows 7 using service mode, WatchDog ignores this option and plays sound file just one time (because you cannot stop sound using GUI).

Execute external program

Name of this action tells for it self, it launches specified external application. In addition to the common action parameters this action has 2 more parameters:

Command line
Specify command line to launch external application. Macro variables may be used in the command line.
E.g. on Windows system you may

- send message to another system in the LAN using command like net send * "%HMSystemAddr% %EventText%";
- start backup HostMonitor as application: c:\program files\HostMon8\hostmon.exe;
- start backup HostMonitor as service: net start HostMonService;
- start sendmail program to send e-mail message
- and so on.

There is no HostMonitor for Linux so you cannot start backup HostMonitor there, however this action may help in some cases.

Window mode
This option enabled on Windows systems only, it specifies how the application window will be shown. Choose one of the possible options:

SW_SHOWNORMAL	displays an application window in its original size and position.
SW_HIDE	starts application without displaying its window.
SW_MAXIMIZE	displays an application window as a maximized window.
SW_MINIMIZE	displays an application window as a minimized window.
SW_SHOWMINNOACTIVE	displays an application window as a minimized window. The active window remains active.
SW_SHOWNOACTIVATE	displays an application window in its original size and position. The active window remains active.

Syslog

This action sends data using the Syslog protocol. Syslog is the standard event logging subsystem for Unix, also you can install some Syslog service for Windows. Syslog daemon receives standard UDP Syslog messages sent from routers, switches, UNIX hosts, HostMonitor, other network devices and can display the details on screen, log to files, terminal devices, etc. Syslog also allows you to forward log entries to another machine for processing, in this way syslog functions as a distributed error manager
In addition to the common action parameters, the «Syslog» action has the following parameters:

Server
This is the name or IP address of the Syslog server.

Port
The default Syslog port is 514, but you can specify a non-standard port.

Message
Provide text message to send. Macro variablesare supported in the message to be substituted with their actual values at the action execution time.

Severity
Log messages are prioritized by a combination of facility and urgency level. Levels (severity) can be considered various levels of a problem (e.g. warning, error, emergency) whereas facilities are considered to be service areas (e.g. printing, email, network, etc). The levels available are the following:

- Emergency A panic condition. System is unusable.
- Alert A condition that should be corrected immediately, such as a corrupted system database.
- Critical Critical conditions, e.g., hard device errors.
- Error Errors.
- Warning Warning messages.
- Notice Conditions that are not error conditions, but should possibly be handled specially.
- Info Informational messages.
- Debug Messages that contain information normally of use only when debugging a program.

Facility
Facility is a number that considered as a service area. The various facilities are listed below:

0	kernel messages
1	user-level messages (messages generated by random user processes)
2	mail system
3	system daemons
4	security/authorization messages
5	messages generated internally by syslogd
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem

9	clock daemon
10	security/authorization messages
11	FTP daemon
12	NTP subsystem
13	log audit
14	log alert
15	clock daemon
16-23	reserved for local use

SNMP Trap

This action sends a message to the management station using the SNMP protocol. The SNMP (Simple Network Management Protocol) is the Internet standard protocol for exchanging management information between management console applications and managed entities (hosts, routers, bridges, hubs, etc).
In addition to the common action parameters, the «SNMP Trap» action has the following parameters:

Destination address
Here you should provide the host name (e. g. mail.maincorp.com) or IP address (e. g. 204.71.200.68) of the host that will receive SNMP Trap messages. This machine should be running a SNMP console in order to receive the trap message. You can use macro variables in this field.

Also you may specify non-standard UDP port. Port number can be provided after a colon following the destination address (e.g. 195.168.10.10**:1162**).

Agent address
Provide IP address of the agent that generated the SNMP Trap. If you keep default value “localhost”, WatchDog will use IP address of the system where it is running.

Community
Specify the SNMP community name used for this trap. The default community for most systems is "public". The community string must match the community string used by the SNMP console.

Enterprise
This field identifies the type of the object causing the trap.

Trap type
Choose one of the generic trap types:
- Cold Start
- Warm Start
- Link Down
- Link Up
- Authentication Failure
- EGP Neighbor Loss
- Enterprise Specific

Specific

If Trap type is Enterprise Specific, provide an ID of the trap.

MIB OID
SNMP Trap message can include OID relevant to the message and its value. Define object identifier in this field (object identifier is the name that uniquely identifies the object, e.g. OID "1.3.6.1.2.1.2.1" represents the number of network interfaces on which system can send/receive IP datagrams).

MIB Value
Define an object's value. You can use macro variables in this field as well.

MIB Type
Choose type of the data. It can be one of the following:
- NULL
- INTEGER
- OCTET STRING
- OBJECT IDENTIFIER
- IP ADDRESS
- UNSIGNED32
- COUNTER
- GAUGE32
- TIMETICKS
- OPAQUE
- COUNTER64

Macros

While defining some of the alert action's parameters you can use special macro variables:

%HMVersionText%	Version of HostMonitor, like HostMonitor v. 10.70
%HMVersionBin%	Binary version, like 0812
%HMSystemName%	Name of the system where HostMonitor is running
%HMSystemAddr%	Host name or IP address of the system where HostMonitor is running (address that was specified as connection parameter)
%HMStartedTime%	Date and time when HostMonitor was started
%HMStatusString%	String that represents status of target HostMonitor, like the following - monitoring started, alerts enabled, modifications stored - monitoring stopped, alerts disabled, modifications not stored If connection to HostMonitor was dropped, this variable returns 'request failed' string
%WDSystemAddr%	IP address of the system where WatchDog is running
%WDSystemName%	Host name of the system where WatchDog is running
%ConnectedAt%	Date and time when connection to HostMonitor was established, can be used for "good" actions

%ConnectedTime%	Time when connection to HostMonitor was established, can be used for “good” actions
%DisconnectedAt%	Date and time when connection was lost, can be used for “bad” actions
%DisconnectedTime%	Time when connection was lost, can be used for “bad” actions
%EventText%	Returns 'Connection established' string for “good” actions and ‘Connection lost’ for “bad” actions

The following table illustrates where you can use macro variables:

Action	Macros applicable	Action parameters where macros are applicable
Visual/sound alert	No	
Execute external program	Yes	Command line
Syslog	Yes	Message
SNMP Trap	Yes	Destination address MIB value