Welcome to Advanced Host Monitor version 15

Advanced HostMonitor

Copyright © 2000-2026 Advanced Network Software
Modified: July, 2026

Contents

Introduction **10**

TestLists **14**

Test list properties 16

Main Window 17

Folder Tree 18

View List 25

Test Detail Area 30

Info Pane 36

Quick Log pane 36

Folder Bar 37

Status Bar 37

SuperMatrix window 38

Recent Events 44

Top Hosts 45

Test Info dialog 47

Test history 48

Auditing Tool 52

Backup options 57

Tests & Test methods **58**

Tests: General Information 58

Links 59

Tests: Agent List 61

Tests: Common Properties 65

Master/Dependent test settings 70

Optional status processing 75

Test Methods 85

Ping 88

Trace 90

URL 92

HTTP 97

SOAP/XML 102

OPC 107

Certificate expiration 110

Domain expiration 111

WebDAV Free Space 112

Apache 113

NGINX 115

Tomcat 120

IIS 123

SMTP 126

POP3 127

IMAP....129
E-Mail....131
Mail Relay....136
TCP....139
UDP....141
NTP/SNTP....143
DNS....144
DHCP....145
LDAP....146
RADIUS....148
DICOM....150
SIP....151
RAS....153
UNC....154
Drive Free Space (Windows WMI / WinRM)....155
Drive Free Space (Win/UNIX: SNMP)....156
HDD SMART....157
Folder/File Size....161
Count Files....162
Folder/File Availability – FTP / FTPS / SFTP....163
File Integrity....166
Compare Files....166
Text Log....168
Process (Windows RPC / WinRM)....175
Process (Win/UNIX: SNMP)....176
Service....177
NT Events Log....179
CPU Usage....186
Memory....189
Performance Counter....191
WMI....194
Dominant Process....198
Registry....200
Firewall Status....202
DHCP Pool....203
Antivirus status....204
Windows updates (time since last update)....205
VM Host status....206
VM Host CPU usage....207
VM Host free memory....209
VM Host Datastore space....210
VM guests status....212
VM guests CPU usage....213
VM guests free memory....215
VM guests free disk space....216
RMCP Ping....218
IPMI Health....220
IPMI Temperature, Fans, Voltage, Current (Analog tests)....221
IPMI Discrete....223
HP iLO Health....228

HP iLO Temperature....229
HP iLO Fans....229
HP iLO Power....230
HP iLO Disks....231
Redfish Health....232
Redfish Temperature, Fans, Voltage, Current and Power tests....234
Redfish Sensor....236
Cisco Health....239
Cisco Temperature....240
Cisco Fans....241
Cisco Power....242
Cisco CPU Usage....243
Cisco Memory....244
Juniper Health....245
Juniper Temperature....246
Juniper Fans....247
Juniper CPU Usage....248
Juniper Memory....249
Big-IP Health....250
Big-IP Temperature....251
Big-IP Statistics....252
Big-IP Disk Free Space....253
Big-IP CPU Usage....254
Big-IP Memory....256
Netscaler Temperature....257
Netscaler Statistics....258
Netscaler CPU Usage....259
Netscaler Memory....260
NetApp Health....261
NetApp CPU Usage....262
NetApp Temperature....263
NetApp RAID....264
NetApp Free Space....266
QNAP Health....267
QNAP Temperature....268
QNAP Fans....269
QNAP Free Space....270
QNAP CPU Usage....271
QNAP Memory....272
Synology Health....273
Synology Temperature....274
Synology Disk Load....275
Synology Free Space....276
Synology CPU Usage....277
Synology Memory....278
SonicWall CPU Usage....279
SonicWall Memory....280
UPS Health....281
UPS Load....282
UPS Charge level....283

UPS Input voltage....284
UPS Output voltage....285
UPS Temperature....286
UPS Remaining time....287
Printer Status....288
Printer supply levels....289
Database test....290
ODBC Query....291
SNMP Get....295
SNMP Credentials....298
SNMP Trap....300
SNMP Table....308
Active Script....312
Shell Script....315
External....327
SSH....328
IT Temperature Monitor....330
Traffic Monitor....332
Network Interfaces Status (NIS)....335
HM Monitor....339
Macros....342
Templates....345
Template folders / Default templates....356
Patterns dialog....360
Acknowledgement....362
Accounts....365
Master password....365
Connection Manager and Password Generator....366
SSH Key Manager....373
SNMP Credentials....375
Profiles....377
Schedules....378
Color palettes....380
Mail templates....382
Report manager....384
"Simple" HTML, WML, DBF, TXT reports....387
Dashboard reports....387
Compact HTML reports....390
Custom HTML reports....392
SLA Reports....393
Macros....395
Actions & Action profiles....398
Action Profiles....400
Action Properties....406

Action methods....412
Show popup message....412
Play sound....412
Hangouts chat....412
Microsoft Teams....413
Telegram message....414
Slack message....415
Viber message....416
Jabber message....416
ICQ message (obsolete)....417
Record HM Log....418
Generate reports....418
Send e-mail....420
Send message to pager (TAP)....421
Send message to pager (SNPP)....422
Send message to beeper....422
Send SMS (GSM)....423
Send SMS (SMPP/IP)....424
Stop service....426
Start service....426
Restart service....427
Reboot remote system....428
Reboot local machine....429
Execute external program....430
Start program remotely....430
Kill process....431
Log Event....432
SQL Query....433
HTTP request....434
Send data to TCP/UDP port....435
Syslog....436
SNMP Set....438
SNMP Trap....439
Dial-up to the network....441
Disconnect dial-up connection....442
Repeat test....442
Change test interval....442
Execute HMS script....443
Macros....454
Logs & Reports....486
Logs....486
Common Log....486
Private Log....486
Custom logs....487
System Log....487
User operations log....487
Log processing....487
Log Viewer....488

Log Analyzer....488
Reports....489
Macros....489
Remote Control Interface & Operators....491
RCI (Remote Control Interface)....491
RCI Status window....491
User....493
Custom menu profiles....493
Operators....494
Login As....496
User Preferences dialog....498
Interface....499
IP-Monitor....499
Columns....500
Options dialog....502
Preferences....502
Behavior....504
Startup....506
Service....508
Access method....509
Proxy....509
Log settings: Primary log / Backup log....510
Compact Logs....514
System Log....515
User operations log....515
External syslog....517
Log processing....519
HTML Colors....522
Log Viewers....522
Reports....522
Message window settings....523
Mailer....524
Pagers....526
ICQ....527
Jabber....527
SMS: GSM....528
SMS: SMPP....532
Ping/Trace....533
RCI....534
Active RMA Server....536

Scheduler....537
Miscellaneous....538
Command line parameters....545
Network discovery, map and replicator....546
Network discovery....546
Network map....548
Replicator....551
System info....556
Tools....559
Local Info....559
Trace....559
Telnet....560
IP Monitor....561
Expression editor....562
Auxiliary applications....563
Log Analyzer....564
Log Analyzer: ODBC logs Manager....565
Log Analyzer: Quick chart....568
Log Analyzer: Full screen chart....569
Log Analyzer: Filter....571
Log Analyzer: Report Manager....573
Log Analyzer: Options....578
Log Analyzer: Scripts....581
Log Analyzer: optional command line parameters....585
Log Visualizer....586
RMA for Windows....593
RMA for Linux, FreeBSD, NetBSD, OpenBSD and Solaris....604
RMA Manager....611
Telnet Service....624
Web Service....639
Web Interface....645
Web Service: Authentication modes....657
Web Service: SSL....659
RCC....665
WatchDog....670
MIB Browser....682
Target system....689
SNMP Credentials....689
WMI Explorer....691
Process Meter....697
Disk Meter....702
Target system....704

SNMP Credentials....705
Connecting to remote host using command line parameters....707
IPMI Browser....709
Redfish Meter....714
Installation / Technical information / Other....719
How To Install / Upgrade / Uninstall Advanced Host Monitor....719
UAC and Virtualization....721
How to install HostMonitor as Win32 service....722
System Requirements:....724
Technical Info:....726
Troubleshooting:....728
Appendix #1: Useful SQL queries for popular SQL servers....729
Appendix #2: User operations log: list of implemented operations....760

Introduction

HostMonitor is a network monitor program. You can create a list of jobs and tests in advance on a "set and forget" basis. Among the many checks it can do, it can monitor any TCP service, ping a host, retrieve an URL, check the available disk space, check integrity of your files and web site, test your SQL servers, check SMTP/POP/IMAP/DNS/LDAP servers, test Windows NT services, monitor CPU Usage, and much more.
HostMonitor checks network servers at regular intervals and takes pre-defined actions if a device does not respond. It can provide a visual and sound warning, send an E-mail message to a mailbox, pager or mobile phone, execute external programs, restart NT services, reboot local or remote computers, dial-up to the network, etc. All these actions allow you to respond to a problem before your users start to complain.

HostMonitor can generate test result log files and reports. HostMonitor provides different log file detail levels and log file formats and can be configured to suit your needs. The highly flexible Report Manager allows you to create and customize reports to your liking in a variety of ways.
Also the package includes a Log Analyzer which can illustrate separate information for each tested host. The Log Analyzer can collect statistical information and show graphs of all request times for specific time periods for all or individual servers. Using the statistical information, an administrator can analyze request times for specific servers over a period of time.

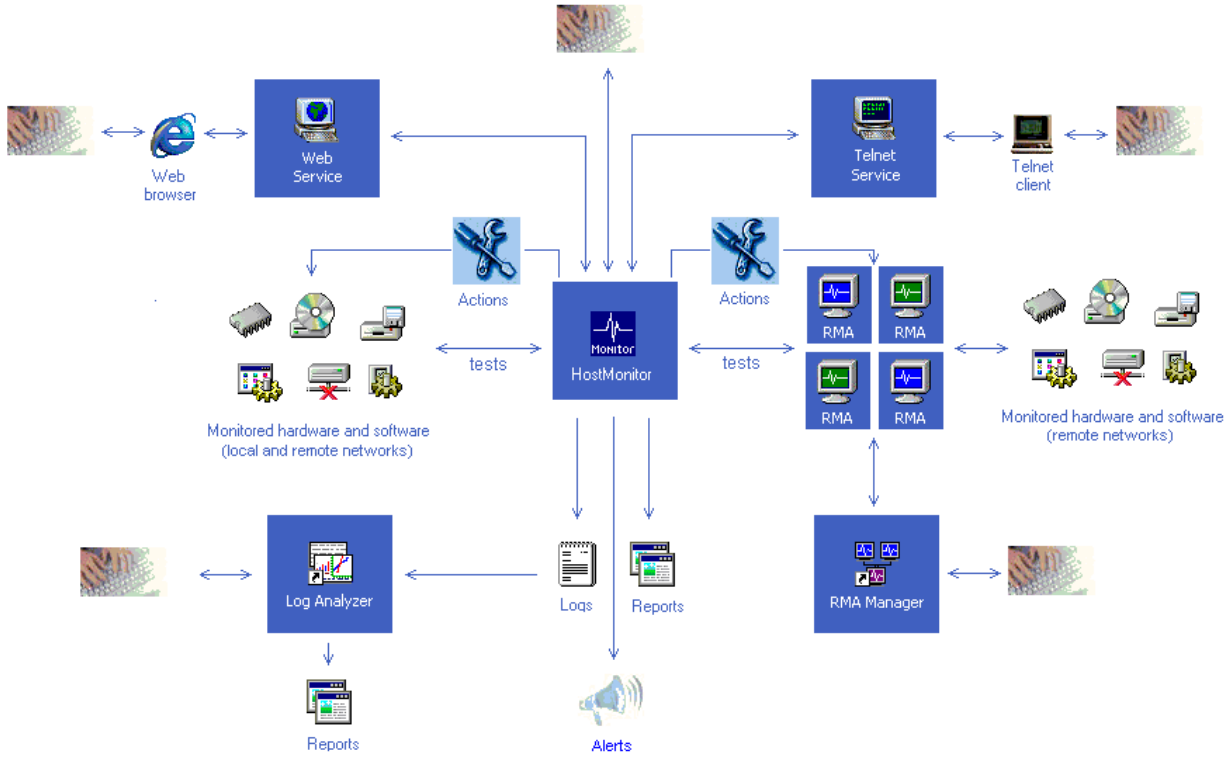
HostMonitor provides system administrators with the benefits of a powerful network monitor at an affordable price. HostMonitor is a network administrator's vigilant assistant. Administrative overhead is reduced as the administrator doesn't need to check servers manually. Network administrator downtime is reduced and user satisfaction improved by the prompt response to server failures.
It is surprisingly easy to install, administer and use. HostMonitor is a system tray program and can be launched at startup or started as a Win32 Interactive Service. It is a "must-have" utility for anyone supporting a range of IT equipment.

Satellite applications:

Advanced Host Monitor package has the following auxiliary components in addition to the HostMonitor (the core of a whole package) itself and the Log Analyzer:

RMA
RMA is a small application that accepts control requests from HostMonitor. RMA can be installed on remote systems and runs there as an application or as a Win32 service. Being controlled by a HostMonitor RMA performs tests and sends the results back to the HostMonitor.
RMA for Windows...
RMA for FreeBSD, Linux, NetBSD, OpenBSD, Solaris

RMA Manager
RMA Manager utility is designed to control and manage the array of Remote Monitoring Agents. It allows you to change settings for hundreds of agents installed on remote systems at the same time and from one location. Both RMA Manager and HostMonitor are using the same list of Remote Monitor Agents. Working with this list you may select group(s) of agents and then perform the following actions for the whole group: get information about an agent: version, platform, list of tests supported by the agent, list of allowed tests, etc; change agent's configuration: change TCP port, timeout, password; enable/disable tests, change different management parameters, etc; reload agent (restart application); force agent to reread settings from its ini file; terminate agent; and even upgrade agent's code remotely.
Details...



T

Telnet Service
This application works like Telnet server and allows you to control HostMonitor remotely using any telnet client. Telnet Service allows you to check brief or detailed status of any test and folder. Also you can disable and enable tests, reset statistics, enforce test execution and even change some parameters of the tests. HM Telnet Service allows you to start or stop monitoring process, enable or disable alerts, change global macro variables, etc.
Details...

Web Service
This application works as an HTTP server and provides web interface for HostMonitor. It means you can install Web Service on a local or remote system and check (and control) HostMonitor in real time using a web browser on any computer that is connected to the Internet.

Web Service allows you to check brief or detailed status of any test and folder. Also you may disable or enable tests, reset statistics and enforce test execution. You will be able to start and stop monitoring, enable and disable alerting, etc.
Details...

RCC
RCC allows you to work with HostMonitor which is running on a remote system just like you work with HostMonitor when it is started on your local system. RCC has exactly the same interface as the one of the HostMonitor. Via RCC you will be able to modify alert profiles, reports, change any option, edit mail templates, create new or modify existing test items, etc.
Details…

WatchDog
Lets say you have installed HostMonitor on reliable server and setup thousand test items to monitor entire network (or several networks). HostMonitor will inform you in case of any problem. Unless... unless something happens to system where HostMonitor is running. WatchDog can be installed on another system and monitor HostMonitor. WatchDog can be used as interactive application that displays statistics information and charts in real-time. On the other hand, you may start WatchDog as Win32 service, setup some actions and leave it unattended.
Details…

MIB Browser
MIB Browser allows you to view the hierarchy of SNMP MIB variables in the form of a tree and provides you with additional information about each node. With MIB Browser you can easily load (compile) standard and proprietary MIB files, view and manipulate data that are available in an SNMP agent.….
Details…

WMI Explorer
Explorer allows you to explore the full set of WMI management classes, objects and their properties; browse through objects and settings on remote machines; execute any WQL query and view the result set.
Details…

Process Meter
Process Meter displays chart with information about all processes running on local or remote system. It may show the following information for each process:

- CPU usage
- Handles
- Threads
- Memory usage
- VM size
- Address space usage

Each process represented by a bar; red colored bar indicates process that uses resources over specified limit.
Details…

Disk Meter
Disk Meter displays chart with information about all disk drives mounted on local or remote system. Each disk represented by a bar; red colored bar indicates disk with free space below specified limit. DiskMeter can connect to remote system using WMI or SNMP protocol and retrieve data from various systems:

- Windows
- FreeBSD
- Linux
- AIX
- ESXi
- Solaris
- NetApp NAS

Details..

IPMI Browser
IPMI (Intelligent Platform Management Interface) is a set of computer interface specifications for out-of-band management of computer systems. IPMI subsystem works independently of the host CPU, firmware and operating system. IPMI provides a way to manage a computer that may be powered off or otherwise unresponsive by using a network connection to the hardware rather than to an operating system.
IPMI Browser retrieves data from remote servers using IPMI protocol, shows charts with temperature sensors, voltage, current and fans speed. Also you may check all available counters (e.g. disk status, memory errors) with details: value, lower and upper thresholds, critical and non-repairable thresholds; export data into text file and more.
Details...

IP-Tools
Also you can use IP-Tools. IP-Tools is a popular and powerful network tool that provides 20 TCP/IP utilities (for computer diagnostics that help to detect problems on LAN or WAN, detect trojans on your computer or for retrieving various information). This is an indispensable set of tools for anyone who uses Internet and/or Intranet.
IP-Tools is a separate package, however an Enterprise license for Advanced HostMonitor includes a bonus license for IP-Tools.
Details...

TestLists

All monitored tasks are stored in TestList files (with the HML extension - HostMonitorList). Any number of HML files can be created, but only one may be loaded into the program at any given time.
To open an HML file, either

- use the File -> Load TestList menu command;
- pick one of the recently used HML files listed under File -> Recent list
- specify a file to load in the HostMonitor command line using the parameter "/List=TestListFileName";
- or define a default TestList in the Options dialog on the "Startup" page.

By default, the last used file is loaded at program startup. You can also load an HML file implicitly as part of an HMS script (see the LoadTestList command for more details). To run a script use the File -> Execute script menu command.

All commands for operations with TestLists are located in the "File" menu:

New TestList	Closes the current list (if opened) and creates a new empty list
Load TestList	Displays the Open dialog box for loading an existing TestList
Recent List	Follow the arrow to choose from the list of recently used TestList files
Append from HML file	Appends items from an existing HML file to the current list
Import from IP-Tools	Imports data from an IP-Tools HostList file and appends the items to the current list
Import from Text file	Imports data from a special format text file
Export to Text file	Exports the settings of all (or selected) tests into text file
Execute script	Executes an HMScript
Save	Saves the current file
Save as	Saves the current file under a new name
Properties	Displays "Test list properties" window
Print	Prints a report
Exit	Exits HostMonitor

All information relating to the tests defined in the current TestList is displayed in the program's main window.

Notes:

If local user closes HostMonitor application and chooses to save changes in test list on application prompt and HostMonitor cannot save file, then HostMonitor does not quit and allows you to fix the problem or use "Save As" option to save test list using different file.

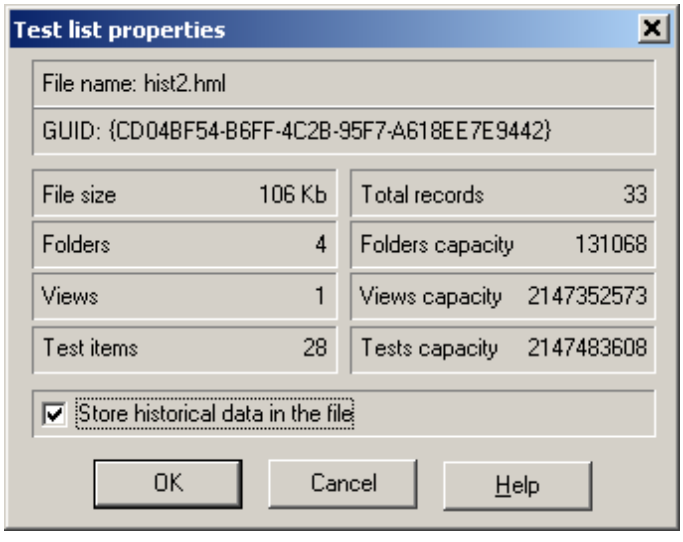
If remote user reloads HostMonitor (or HostMonitor is being stopped because system is being restarted) and test list was not modified and HostMonitor cannot save updated statistics, HostMonitor quits anyway.

However if remote user reloads HostMonitor and test list was modified and HostMonitor cannot save these modifications into file then HostMonitor does not quit until local operator will fix the problem or will use “Save As” option to save test list using different file.

When you restart or shutdown system, HostMonitor saves all test list modifications automatically.

Also, please take a look at “Auto save” options located on Preferences page in HostMonitor Options dialog

Test list properties



"Test list properties" window provides information about loaded HML file and allows you to enable or disable "Store historical data in the file" option. Use menu File -> Properties to access this information. HostMonitor/RCC shows the following information:

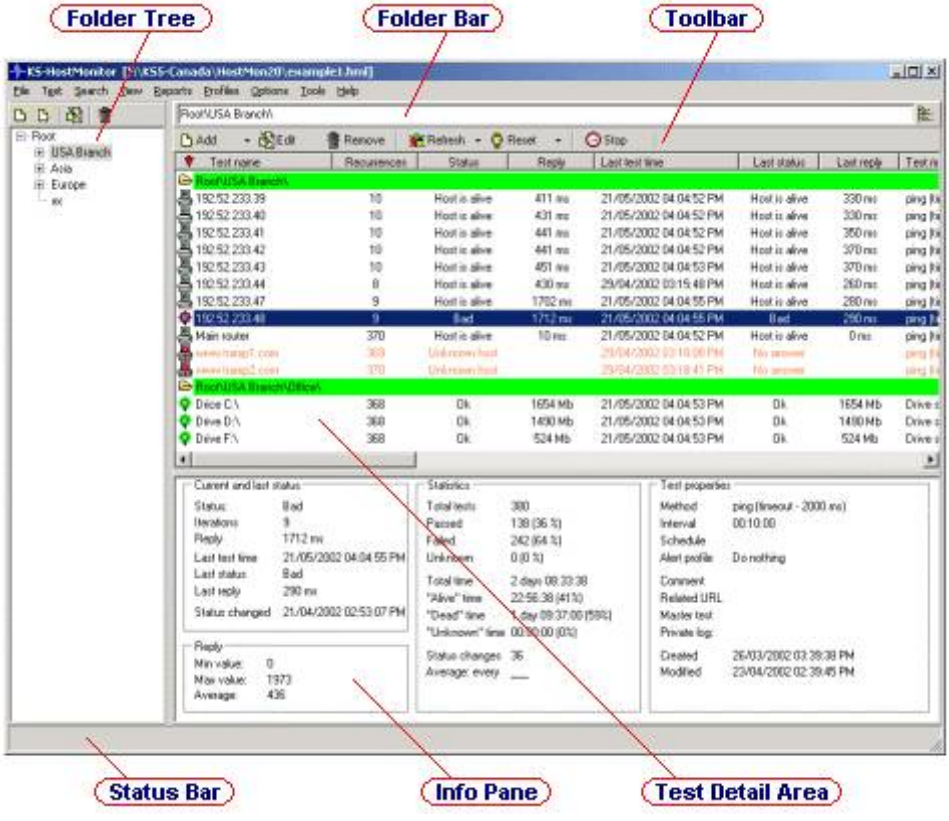
- file name, file size, GUID of the test list
- number of folder, views and test items
- folders, views and test items capacity – these numbers show how many new folders, views or test items can be created within test list

"Store historical data in the file" option tells HostMonitor to collect additional statistical information for each test item. If option is enabled HostMonitor will calculate statistics for last 48 hours, last 60 days, last 24 months, and so on. With this option enabled you will be able to get historical charts for each test item without using Log Analyzer or Log Visualizer, setup HostMonitor to generate SLA reports, etc. Also HostMonitor will be able to generate "prediction" reports. It will try to predict test results for next 7 days. Web Service will be able to provide additional information about each test items as well.
On the other hand HostMonitor will use more system memory when this option is enabled and HML file will be about twice bigger. If you have many thousand of test items and you are using ODBC logging to store test results in your database for future analyzing by your own or 3rd party tools, then you may consider disabling of this option. Also you may disable it when SLA reports are not important for you.
"Store historical data in the file" option is enabled by default when you create new test list. Also HostMonitor enables this option for your "old" test list created by older versions of the software in case test list contains less than 5000 test items. However you can enable or disable this option at any time. Note: if you disable option, HostMonitor removes collected information so you will not be able to restore it; when you enable option, HostMonitor starts collecting information however it will take some time.

Note 1: operator may change HML file properties if he has access to root folder and has right to remove tests and folders.
Note 2: if you change system date forward and back this will affect stored statistical information. If you need to play with system date for some reason, we recommend to stop/pause monitoring until you restore correct system date.

Main Window

The main HostMonitor window is divided into five logical areas, each of which can be made visible or hidden in menu View (except the Test Detail Area, which is always visible):



- FolderTree & Views List;
- Test Detail Area;
- Info Pane & Quick Log Pane;
- Folder bar;
- Status bar

This window is customizable to your personal preferences. You can change font style and font color, select color palette, change size or make some parts invisible, select style for test list, etc (Click here to see more screen shots).
For more information see User Preferences and optionsdialog.

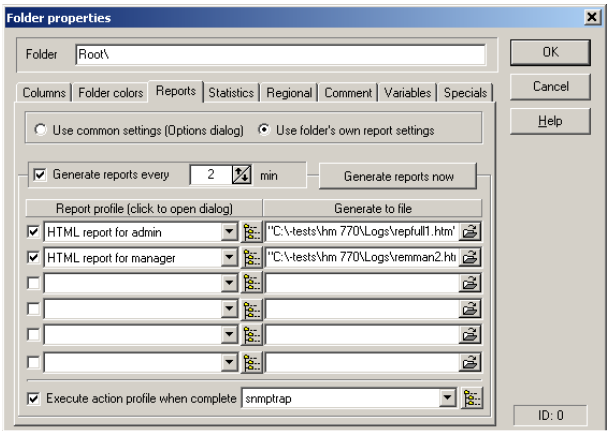
See also: SuperMatrix, Recent Events, Top Hosts, Test Info, Test History, Auditing Tool

Folder Tree

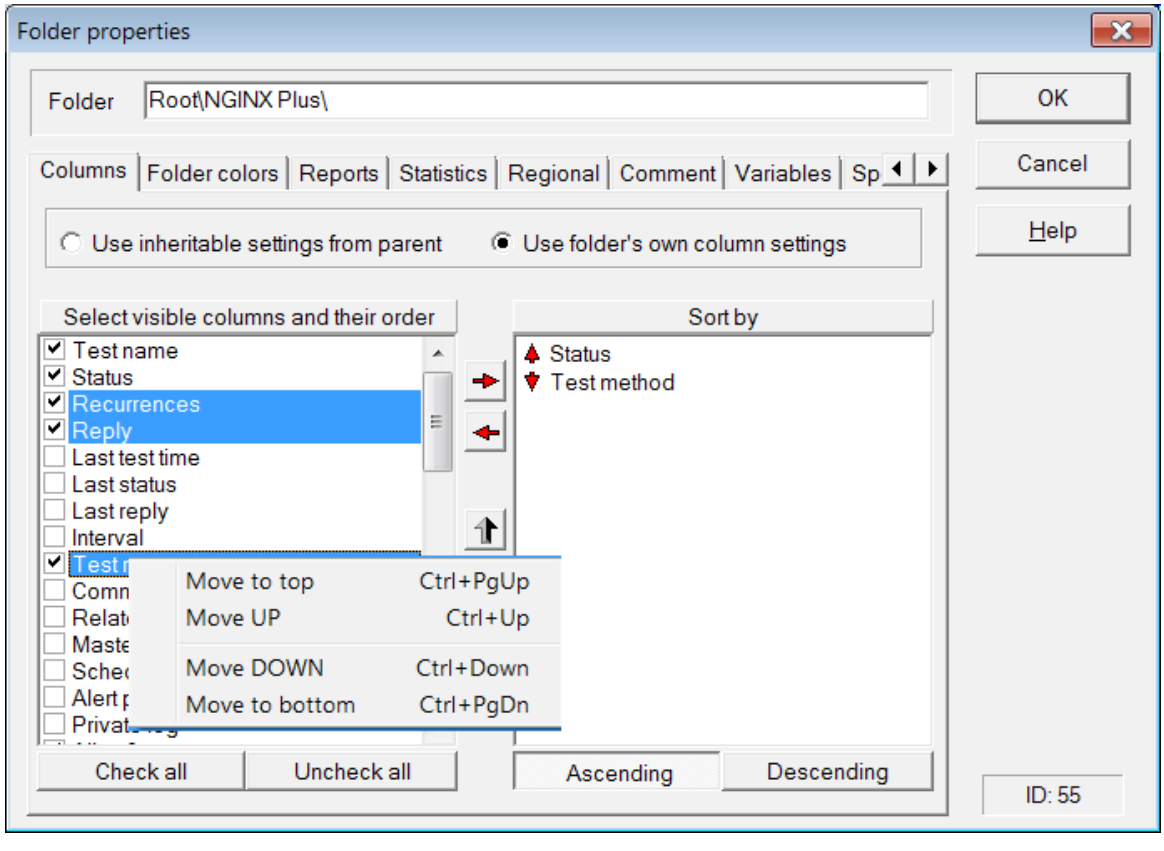
Folders help you organize your tests in logical groups presented as a tree-like structure. The folder tree is displayed in the left-hand panel of the main HostMonitor window. Each folder may contain tests and/or nested subfolders, and has a number of properties which you may change or edit in Folder Properties dialog.

These settings are located on the following pages:

- Columns
- Folder colors
- Reports
- Statistics
- Regional
- Comment
- Variables
- Special



- **Columns**
  on this page you may define the list of visible fields (in other words the list of test attributes to display) and the list of attributes to sort test items by.
  Also you may add up to 8 custom fields for the Folder. You can use most of test related variables to define field value and any static text to describe the field (you cannot use "historical" variables like %Stat24Hours_MinReply%, %Stat30Days_AliveRatio%). You may use one or several variables in each field and static text but you cannot use expressions like %TestID% + %FailureID% (here + will be considered as static text, not mathematical operator, in other words HostMonitor will display value of these two variables, not sum of the values). For example you may create FolderA for file related test items and tell HostMonitor to display filename, file size and modification time for each test item; another FolderB may contain URL test items and display HTTP response code as additional field.
  Note: you may add custom fields for Views and for GUI settings specified on "operator" level as well.



- **Folder colors**
  on this page you may select a Color palette specific to the folder (by default all folders use the same palette, specified in the Options dialog);

- **Reports**
  up to 6 individual reports can be associated with a folder;
  You may use "**Generate reports every N min**" option to tell HostMonitor how often reports should be generated. "Generate reports now" button allows you to create reports immediately (e.g. for testing purposes).
  If you need to create reports every time a test changes its status, you may add the "Generate reports" action to the Action Profile. The other way to implement the same behavior would be to add a "Run HMS Script" action, and include a CreateReport command in the script to execute.
  Note: To exclude some tests from reports use test property "Exclude from reports".

  Execute action profile when complete
  With this option enabled HostMonitor will create report files and then launch the specified alert profile (for example you may use this option to send reports by e-mail). Note: only "scheduled" actions will be executed, i.e. a condition to start action should be set to "on the schedule" (in Action Properties dialog).

- **Statistics**
  settings located on this page allow you to setup a schedule to reset statistical information for the tests. Please note: if you are using "quarterly" schedule and "Last day" option, HostMonitor will reset statistics on the last day of the LAST month of each quarter (March, June, September and December). This is different from the other type of "quarterly" schedule - when you are using some specified day to perform action (e.g. the 1st day), then statistics will be cleared on a specified day of the FIRST month of each quarter (January, April, July and October).

- **Regional**
  here you may specify GMT offset different from your local time zone and mark one or both options:
  - Apply remote site time settings to GUI and reports
  - Apply remote site time settings to schedules assigned to the tests and actions

  "Apply remote site time settings to GUI and reports"
  This option tells HostMonitor and RCC to display test properties (such as time when the test was last performed, creation time, modification time, time when test status was acknowledged, etc) using time of the specified region (time zone).
  Note #1: By default descendant sub-folders inherit regional options from parent folder however you may set different time zone for each subfolder. Nevertheless HostMonitor/RCC applies the same time zone for all visible items using settings of the selected (parent / current) folder for entire list (view / report). "All visible items" may have the following meanings:
  - all test items displayed when some Folder is selected
  - all test items displayed by some View
  - all test items included into report file

In other words: all test items included into view/report are displayed with the same time zone settings; HostMonitor uses time zone of the selected (parent/current) folder for entire view/report.
For example you create "USA" folder with "New-York" and "Seattle" subfolders (USA ->NewYork; USA->Seattle) and set GMT -5 for USA and New-York, GMT -8 for Seattle. Then if you generate report for USA including subfolders (New-York and Seattle!), all test items within this report will use GMT -5 time zone. If you generate report for "Seattle" subfolder, test items within this report will use GMT -8 time offset.
This allows you to create similar sets of reports (the same list of folder and tests) using local time for one set and using remote time for another set of reports. You may create one empty folder and include 2nd folder with tests into this empty one using different regional settings for parent and descendant folders.

Note #2: "Apply remote site time settings to GUI and reports" option does not affect DBF reports; it works for Text, HTML, and WML reports.

"Apply remote site time settings to schedules assigned to the tests and actions"
This option tells HostMonitor to apply time restrictions (schedules) to tests and alerts execution using time of specific time zone. This allows you to apply the same schedule for test items used to monitor hosts around the world.
By default descendant sub-folders inherit regional options from parent folder however you may set different time zone for each subfolder.

Note: There are special macro variables that allow you to use remote site time as parameters of the actions.

- **Comment**
  inheritable comment for the folder. It can be used for informational purposes; also comments can be used as parameters for actions. E.g. you may use the 1st comment line as a destination e-mail address for alerts that send notification messages to the staff in charge. Another comment line may be used as a name of the server that should be rebooted by «restart remote system» action. In this way you may use a single action profile for sending alerts to different recipients that are responsible for tests within the folder. You can access the whole comment or a particular comment line using macro variables %FolderComment%, %FCommentLineXX% (where XX is a number of the line). For more information, refer to macro variables section of this manual

- **Variables**
  Here you may specify folder-related user-defined variables. Just like comment lines, list of variables can be inherited from parent folder or you may specify unique list of variables for particular folder.
  These variables can be used as parameters of actions assigned to test items, so you may define descriptive variable like fvar_BackupMailServerIP = 10.10.1.15 and use %fvar_BackupMailServerIP% variable instead of non descriptive %FCommentLine2%. What is more important, these variables can be used as parameters of test items (see Templates)!

Note: To add a new variable to the end of the list go to the last existing line and press Down Arrow key. Press INSERT button to insert a new line. Press CTRL+DEL to remove variable. Press F2 to edit variable. Also dialog provides popup menu that allows you to sort items alphabetically by name or by value.
Plus you may copy entire list of variables into clipboard using popup menu item "Copy list" and you may insert list of variable from clipboard using menu item "Paste list". This allows you to copy variables from one folder to another or create such list using any text editor (just type variable_name=variable_value pairs in each line).

HostMonitor version 8 provides option that allows variables inheriting from parent folder plus using local variables that may override inherited variables with the same name. In other words: for each subfolder you may choose one of the following modes:
- use folder variables only
- use inherited variables only (inherit all variables from parents)
- use inherited variables; folder variables may override inherited variables
When you choose 3rd mode, Folder Properties dialog will display 2 lists: one read-only list shows all inherited variables, another list allows you specify local variables

- **Specials**
  the following options are not inheritable; it means subfolders do not inherit such behavior unless you specify the option directly for subfolders as well.

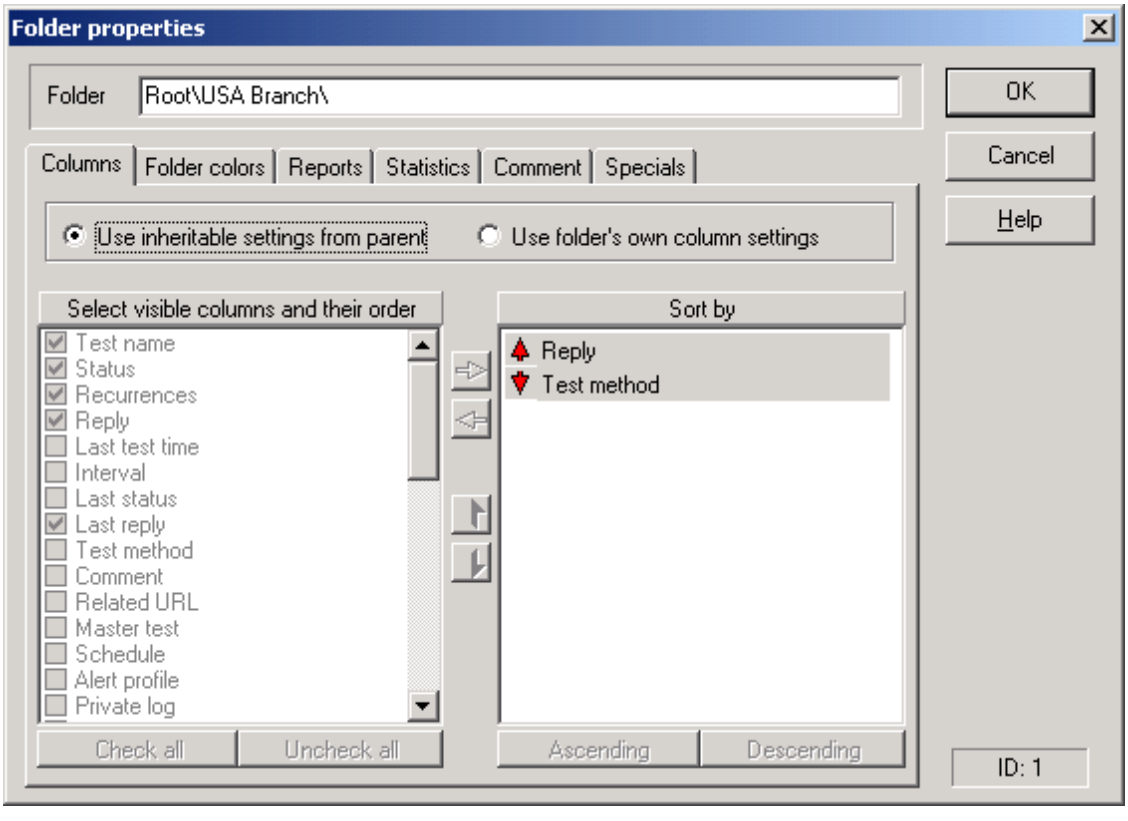
  - **Non-simultaneously test execution**
    With this option enabled tests that located in the folder will not be executed at the same time. Test items located in different folders may be executed simultaneously even in case option is set for all of these folders. Option is useful when you need to call some non-reentrant application/script.

  - **Test statuses should not affect tray icon color**
    As you know HostMonitor changes color of the tray icon when a test fails. This option allows you to make exception for the set of test items.

  Use folder specific agent
  This option allows you to select Remote Monitoring Agent (RMA) on per-folder basis.
  If you set "Test by: folder-specific agent" option for test item, HostMonitor will use agent specified for the folder where test item is located. If you move or copy test item from one folder to another, HostMonitor will use agent selected for new parent folder.
  Also, there is SetFolderAgent command supported by HM Script. You may use script to copy folders and subfolders, change some variables (e.g. target host name or IP address), change agent and copy test items that will inherit new settings automatically.

A new folder automatically inherits properties defined for the parent folder (the top folder inherits the common settings defined in the Options dialog). Once a folder is created, you can change its properties as needed, rename or delete the folder, create tests and nested subfolders, and so on.
For example you can set up a folder representing your company, define a set of report profiles (for the administrator, IT manager, technical support personnel, etc.), then create several subfolders, one for each of the company offices, and you are done! HostMonitor will be automatically generating uniform reports for all company offices (each report will contain test results specific to the office).
In another example, folders can be created based on a test method (Ping, CPU Usage, etc.). For each folder, define a different set of visible columns, depending on the type of a test. Thus, for a ping test folder a logical choice would include the "Reply" field, whereas for a CPU Usage folder the "Average reply" field might make sense.

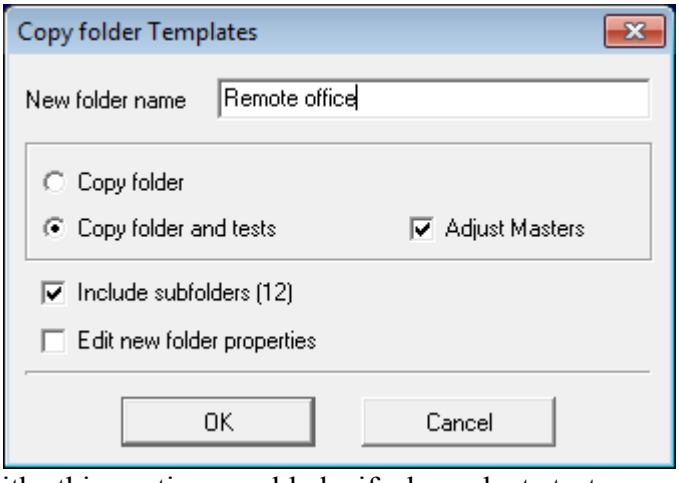
Folder properties are edited in the Folder Properties dialog available through the Properties command in the pop-up menu that appears when you right-click on a folder.



As you can see in the picture above, the editable properties on the Columns page are grayed out. This is done because the "Use inheritable settings from parent" option is selected, which means the folder being edited does not define properties (visible columns in this case) of its own, but rather uses ones specified somewhere up the folder hierarchy. This way, changes made to an upper-level catalog are automatically propagated onto its descendent subfolders.
Similarly, the other folder properties, such as Color Scheme and Reports, can be either inherited from the parent or set individually for any particular folder.

HostMonitor supports Drag&Drop operations, allowing you to easily move folders around, change their display order, and move tests from one catalog to another.

Copy
Popup menu item “Copy” allows you to copy folders with (or without) sub-folder, copy folder with tests, copy folders and sub-folder with tests. You may edit folder properties (e.g. change folder-level variables) before HostMonitor will copy test items.



Adjust Masters: with this option enabled, if dependant tests copied with master(s) then HostMonitor adjust master-dependant relations for newly created tests. E.g. if you copy 6 tests (5 Cisco tests that depends on 1 Ping test) then new Cisco tests will depend on new Ping test (if you are using folder-related variables for target IP address, then new tests will start to monitor new device without any manual adjustments).

Home folder
Since the version 6 HostMonitor provides a "home folder" option that can be specified for each operator. If you do so, the operator(s) will see test items within their own specified folder (and its sub-folders) only. In this way, you may easily separate work/permissions among departments of a company.

View List

In addition to Folder tree (first introduced in HostMonitor 3.0), HostMonitor 6.70 provides another feature - Views list.

What is the difference between folders and views?

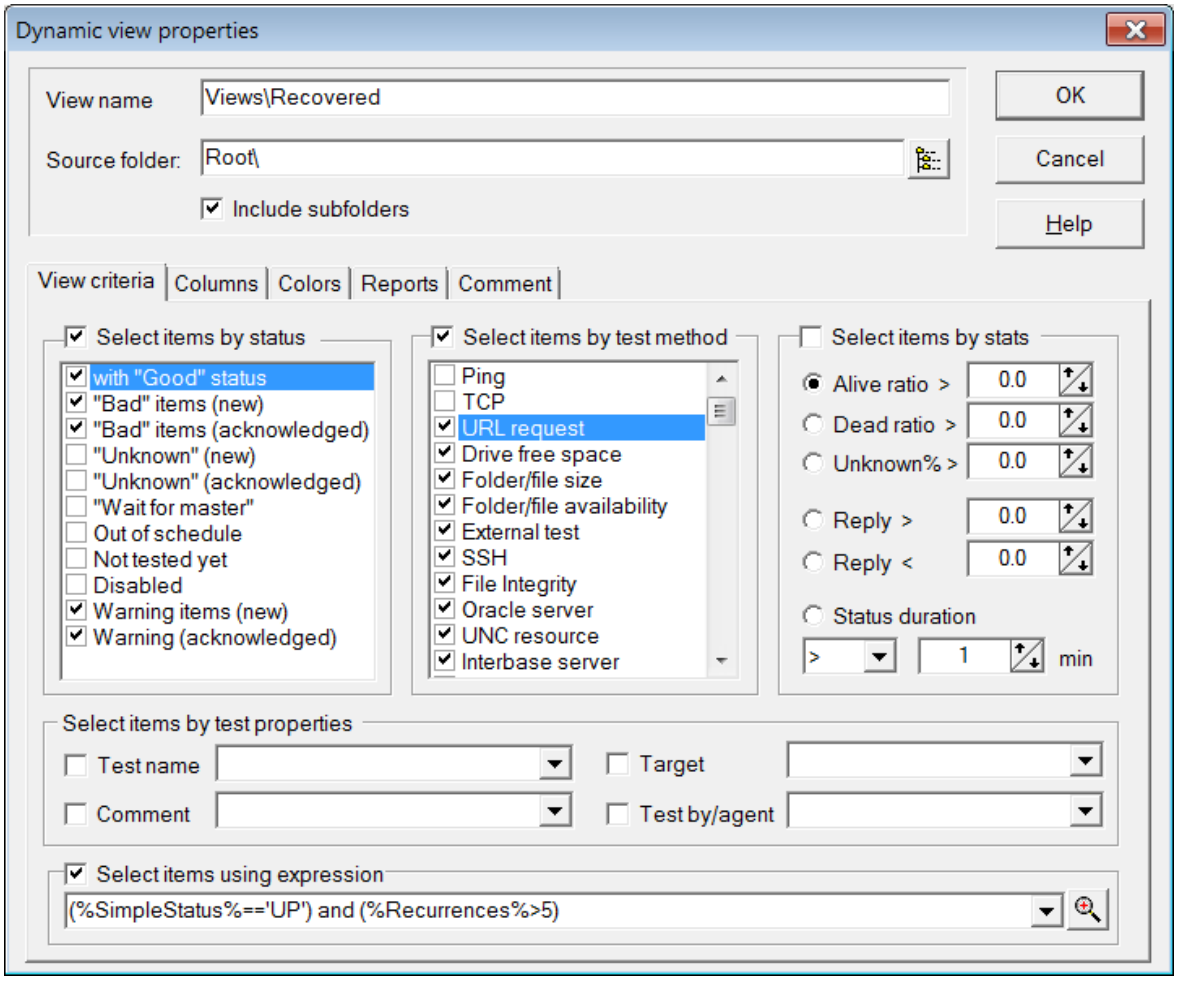
- Folders contain static set of test items. “Static” means HostMonitor does not change set of test items, however operator may add or remove items from the folder, move or copy test items from one folder to another, etc.
- Views do not “contain” test items, you cannot add or remove test items from the view. Instead of this you may specify rules that tell HostMonitor which test items should be displayed by the view. E.g. you may use one view to display disabled test items, use another view to display all ping test items with reply time over 500 ms and setup the 3rd view to show test items that changed status during last 10 minutes.

What is common for folders and views?

- For each folder and view you may specify its own set of reports, color palette, list of visible fields and sorting mode; or you may keep “Use inheritable settings from parent” option to use the same palette or sorting mode for set of views.
- Folders and views allow you to select single test item or a set of test items and modify the test(s) parameters, e.g. you may change test properties, enable or disable items, acknowledge test status, etc.

Top view
This is special view that cannot be removed. Top view neither provides “view criteria” nor “reports” settings; it does not display any test items. However using the top view you may easily change color palette, sorting mode or list of visible fields for all views with appropriate “Use inheritable settings from parent” option enabled.
If you choose personal color palete for the top view, HostMonitor will change color palette for all windows (including Trace and Telnet tools) when you switch from “folders tree” to “views list” and vice versa

Each view has a number of properties which you may change using View Properties dialog.



Source folder

The View gets test items from some specific folder; this folder is called source folder or parent folder. You may choose absolutely any folder as a source folder. If you remove a source folder, HostMonitor will remove all views related to the folder.

Include subfolders

If you enable "Include subfolders" option, view will select test items from the folder and its descendant subfolders. If you choose root folder as source folder and mark "Include subfolders" option, view will work with entire test list.

Note: Views display test items in a single list using single sorting operation for all items, while folders show test items grouped by subfolders and sort items within each group.

Other properties of the view are grouped on several pages in the dialog window:

- View criteria
- Columns
- Colors
- Reports
- Comment

View criteria page

Options located on this page define which test items should be displayed by the view. You may enable one or several filters:

- Select items by status
- Select items by test method
- Select items by stats
- Select items by test properties

Note: If you enable several filters, view will display test items that satisfy all of these filters (logical AND).

Select items by status

This option allows you to filter test items by status, e.g. view may display tests with a "Warning" or "Unknown" status only. Click mouse button on the check box next to a status name to mark/unmark the item. Use "Mark all" popup menu item to select all available statuses, use "Clear all" popup menu item to deselect all items.

Select items by test method

This option allows you to filter test items by test method, e.g. view may display Ping, TCP and UDP tests. Click the mouse button on the check box next to a test method name to mark/unmark the item. Use "Mark all" popup menu item to select all available test methods, use "Clear all" popup menu item to deselect all items.

Select items by stats

You may use this group of the settings to filter test items using statistical information. Use one of the following options:

- Alive ratio > N%
- Dead ratio > N%
- Unknown ratio > N%
- Reply > N
- Reply < N
- Status duration > N min
- Status duration < N min

Select items by test properties

Test name

This filter allows you to select test items by name. If you mark the option and specify a string to compare, the view will display test item when its name contains specified text (case insensitive).
This filter allows you to specify several search strings separated by a comma, e.g. “mail server test,dns test“ or "10.10.1.5,192.168.1". Note: do not use space between elements, just a comma.

Target

This filter allows you to select test items by target object (target host/file/port/service/folder/process/etc monitored by the test items). Here you may specify hostname used for Ping, TCP, UDP, SMTP and other internet related tests, IP address or part of the address, filename used for the file related test methods, etc.
E.g.

- If you type “www.mywebserver.com”, the view will display test items that check host www.mywebserver.com (it can be Ping, TCP, URL, HTTP or some other tests).

- If you type “applog.txt”, the view will display all test items that check file applog.txt (e.g. Folder/File Size, Text Log, File Integrity or Folder/File Availability test methods).
- You may use “Target” filter to display all test items that monitor some specific process on various servers (use name of the process as target, e.g. ntvdm.exe) or you may use this filter to show all test items that monitor various processes on some specific server (use name of the server as target, e.g. bdk100.domain2.com)
- Also you may use full IP address or part of the IP address, e.g. “192.168.12.10” tells HostMonitor to display all test items that check specific host 192.168.12.10, while “192.168.12” tells HostMonitor to display tests items that check any host in range 192.168.12 1-192.168.12.255 or *.192.168.12

Test by (agent)
Here you may provide name of the agent (RMA) that performs the tests or type “HostMonitor” to show test items performed directly by HostMonitor.
This filter allows you to specify several search strings separated by a comma, e.g. agent-1,remoteagent2 or 10.10.1.5,192.168.1. Note: do not use space between elements, just a comma.

Comment
This filter allows you to select test items by test comment. If you mark the option and provide some text, the view will display test item when any line of the test comment contains specified text (case insensitive).

Select items using expression
This option allows you to use expressions like the following to select test items you need

```
('%SimpleStatus%'=='UP') and (%Recurrences%>5)
('%SimpleStatus%'=='UP') and ('mail' in '%AlertProfile%')
('%Status%'=='Out of schedule') and ('%LastStatus%'=='Bad')
```

These expressions should follow the same rules that are used for “advanced actions”
Note: Web Service does not support some variables. If View should be available thru web interface as well, you may use the following variables:

%ACKCOMMENT%
%ACKNOWLEDGEDAT%
%ACKNOWLEDGEDBY%
%ACKNOWLEDGEDDATE%
%ACKNOWLEDGEDTIME%
%ACKRECURRENCES%
%ACKRESPONSETIME%
%AGENT%
%ALERTPROFILE%
%ALIVERATIO%
%ALIVETIME%
%AVERAGEREPLY%
%COMMENTID%
%COMMENTLINE%
%CREATEDTIME%
%CURRENTSTATUSDURATION%
%CURRENTSTATUSDURATION_SEC%
%CURRENTSTATUSID%
%CURRENTSTATUSITERATION%
%DATE%
%DATETIME%
%DEADRATIO%
%DEADTIME%
%DEPENDANTTESTSNAME%
%DEPENDANTTESTSPATH%
%FAILEDCNT%
%FAILUREITERATION%
%FOLDER%
%FOLDERID%
%FULLPATH%
%HOSTADDR%
%HOSTADDRB%
%HOSTID%
%HOSTNAME%
%INTERVAL%
%INTERVAL_MIN%
%INTERVAL_SEC%
%IP%
%IP4%
%ITERATIONS%
%LASTFAILUREID%
%LASTREPLY%
%LASTREPLY_CSTYLE%
%LASTSIMPLESTATUS%
%LASTSTATUS%
%LASTTESTTIME%
%MASTERTEST%
%MASTERTESTS%
%MAXREPLY%
%METHODID%
%MINREPLY%
%MODIFIEDTIME%
%PASSEDCNT%
%PAUSECOMMENT%
%PREVIOUSSTATUS%
%PREVIOUSSTATUSDURATION%
%PREVIOUSSTATUSDURATION_SEC%
%PREVIOUSSTATUSTIME%
%PRIVATELOG%
%RECURRENCES%
%RELATEDURL%
%REPLY%
%REPLY_CSTYLE%
%REPLY_INTEGER%
%REPLY_NUMBER%
%SCHEDULENAME%
%SIMPLESTATUS%
%STATUS%
%STATUSCHANGEDTIME%
%STATUSCHANGESCNT%
%STATUSID%
%TASKCOMMENT%
%TESTID%
%TESTMETHOD%
%TESTNAME%
%TESTPROBETIME%
%TIME%
%TOTALTESTS%
%TOTALTIME%
%UNKNOWNCNT%
%UNKNOWNRATIO%
%UNKNOWNTIME%

Columns page
On this page you may define the list of visible fields (in other words the list of test attributes to display) and the list of attributes to sort tests by. If you keep "Use inheritable settings from parent" option, view will inherit settings from the top view that, in turn, may inherit global settings specified in the Options dialog.
Also you may add up to 8 custom fields for the View. You can use most of test related variables to define field value and any static text to describe the field (you cannot use "historical" variables like %Stat24Hours_MinReply%, %Stat30Days_AliveRatio%). You may use one or several variables in each field and static text but you cannot use expressions like %TestID% + %FailureID% (here + will be considered as static text, not mathematical operator, in other words HostMonitor will display value of these two variables, not sum of the values). For example you may create View-Files for file related test items and tell HostMonitor to display filename, file size and modification time for each test item; another View-WEB may display URL test items and provide HTTP response code as additional field.
Note: you may add custom fields for Folders and for GUI settings specified on "operator" level as well.

Colors page
On this page you may select a color palette specific to the view. If you keep "Use inheritable settings from parent" option, view will inherit color scheme from the top view that, in turn, may inherit global settings specified in the Options dialog.

Reports page
Up to 6 individual reports can be associated with each view. If you keep "Use inheritable settings from parent" option, HostMonitor will not create separate reports for the view unless you specify this view as parameter of "Generate reports" action. "Use inheritable settings from parent" option also tells HostMonitor to include the view(s) into reports created for parent (source) folder when

- You are using "Generate reports" action with "Folder + subfolders/views with inherited settings" option to create folder-level reports
- You are using "Generate reports every N min" folder-level option

Global "reports" options located in the Options dialog do not generate reports for the views.
Note: view has its own filter (view criteria), while report profile has another filter. Reports generated for the view will show tests items that fit both (logical AND) filters.

Comment page
Text comment for informational purposes

Test Detail Area

Appearing on the right side, the Test Detail Area displays, in table form, tests contained in the current (selected) folder and (if the Show tests in subfolders option is enabled) its descendent subfolders. As it was mentioned in the Folder Tree section, display parameters for the Test Detail Area, like visible columns, color scheme, etc can be changed for the whole program or for the selected folders.

As you could expect, **all** tests defined in the working TestList are performed according to their schedules, regardless of whether they are currently displayed or not.
To perform the operations with a test or a group of tests you can use Toolbar, popup menu or a Test menu in the main window of the program. Tests and their parameters are defined in the Test Properties dialog.

Toolbar

The Test DetailArea toolbar is located right above the test grid, and contains six buttons accompanied by a pull-down menu:

Add button	brings up the Test Properties dialog to let you create a new test;
Add pull-down menu	lists all available test methods; choosing an item brings up the Test Properties dialog with the appropriate test method pre-selected in it.
Edit button	allows you to edit the properties of the selected test item(s) in the Test Properties dialog.
Remove button	removes the selected test item(s).
Refresh button	refreshes status information for tests in the selected folder, by performing each of the tests immediately.
Refresh pull-down menu:	• Refresh selected host(s); • Refresh current folder only; • Refresh current folder and subfolders; • Refresh all tests.
Reset button	resets the statistics for the tests in the selected folder. For more information about test counters and statistics in HostMonitor, click here.
Reset pull-down menu	• Reset selected host(s); • Reset current folder only; • Reset current folder and subfolders; • Reset all tests.

Stop/Start button	Stop button suspends all activities until monitoring is resumed by clicking the Start button

Popup menu

Test Detail Area has its own popup menu to perform varied test operations. Click right mouse button to bring up this menu and select the item you need:

Edit
Opens the Test Properties dialog for editing parameters of the selected test or a group of tests (also to edit selected tests you can use the Enter button).
Add
Brings up the Test Properties dialog to let you create a new test
Copy
Lets you create a copy of selected tests in a folder of your choice. Copy function will create new test item(s) with the same* properties as the existing one, then you will be able to modify each item independently; HostMonitor will perform separate check for each item.
When you copy test item(s), you may choose one of the following options:
- Just copy
  this option tells application to create exact* copy of selected test items.
- Edit copied items before using
  this option allows you to modify test properties for each copy of the test(s). HostMonitor will not execute new test(s) until you close Test Properties dialog using "Ok" button. Also you may click "Cancel" button, in such case HostMonitor will offer a choice: skip (do not copy) this test item or skip this and the following items from being copied.
- Disable copied items
  tells application to create copy of selected test items and disable copies from being tested (you may edit and then enable test items at convenient time)

* Note: When HostMonitor copies test item(s), it copies test properties, assigns unique TestID to new instance of the item and sets statistical counters to 0.
See also Check and copy

Link
If you want to see exactly the same test item(s) in several different folders, use Link operation. Then if you select original test or any of its links and modify test settings, your changes will automatically take effect for all links of the test.
Link info
Using this menu item you may access “Links list” dialog window, it shows the information about all folders which contain links to selected test item. You may remove some links or you may remove test itself (including all links to the test).
Remove
Removes selected test/link items from the list (after confirmation). The same result can be achieved by pressing the Del button.

Refresh selected test(s)
Refreshes status information for the selected tests, by performing each of the tests immediately, without waiting until time of the test interval is elapsed (if the test is disabled, HostMonitor will ask to enable the test). The same result can be achieved by pressing the Space button.
Refresh this folder
Refreshes the status information for tests in the selected folder, by performing each of the tests immediately.
Refresh all tests
Refreshes the status information for all tests (except disabled), by performing each of the tests immediately.

Pause
Allows you to pause monitoring for selected test item(s) for a specific amount of time, e.g. next 20 min or till June 21 at 17:30 - the time when HostMonitor will resume monitoring automatically.
Resume
At any time you may resume paused test item(s) manually.
Note: You may pause entire monitoring (all test items) using main menu “Monitoring -> Pause”.

Set planned pause
Allows you to schedule test items to be paused at sometime in the future. For example you may select set of test items and tell HostMonitor to pause execution of these items next Sunday between 01:00AM and 03:00AM. Option available thru main menu “Test” -> “Set planned pause”.
Tests scheduled for pause
Opens dialog window that shows all items scheduled to be paused (not items that are paused right now). Using this dialog windows you may check “pause schedule” for each item, sort the list using different sort orders, also you may reschedule time for selected items or repeal pause for the items. Option available thru main menu “Test” -> “Tests scheduled for pause”.

Disable test
Tests can be temporarily disabled without the need to delete and re-create them (HostMonitor does not perform checks for disabled tests). This command disables one or several selected test items.
Enable test
Enables selected test item(s). When operator enables a test item, HostMonitor always logs a record AFTER following test probe (even if the status of the test does not change). This clearly shows the exact time when the test was enabled.
Disable this folder
Disables all test items within selected folder.
Enable this folder
Enables all test items within selected folder.
Note: Option "Request for comment when test gets disabled" tells HostMonitor to request comment every time operator disables test item(s). However operator may continue operation without entering any information (keep comment field empty). This option located on Behavior page in the Options dialog.

Test Info
Use this command to bring up Test Info dialog
History charts

Displays "Test history" dialog for selected test item(s)

Log Analyzer

Starts Log Analyzer application and displays statistics and charts for selected test.
Note: RCC can start Log Analyzer when Log Analyzer is installed on the same system and log file is accessible (or ODBC log is in use)

View private log

Displays private log for the selected test, if it has one.

Trace

Opens the built-in Trace utility and starts trace to the selected host. This menu item available for the following tests: Ping, TCP, URL, SMTP, POP3, IMAP, DNS, DHCP and LDAP.

Telnet

Opens the built-in Telnet utility and setup selected host as a target address. This menu item available for the following tests: Ping, TCP, URL, SMTP, POP3, IMAP, DNS, DHCP and LDAP.

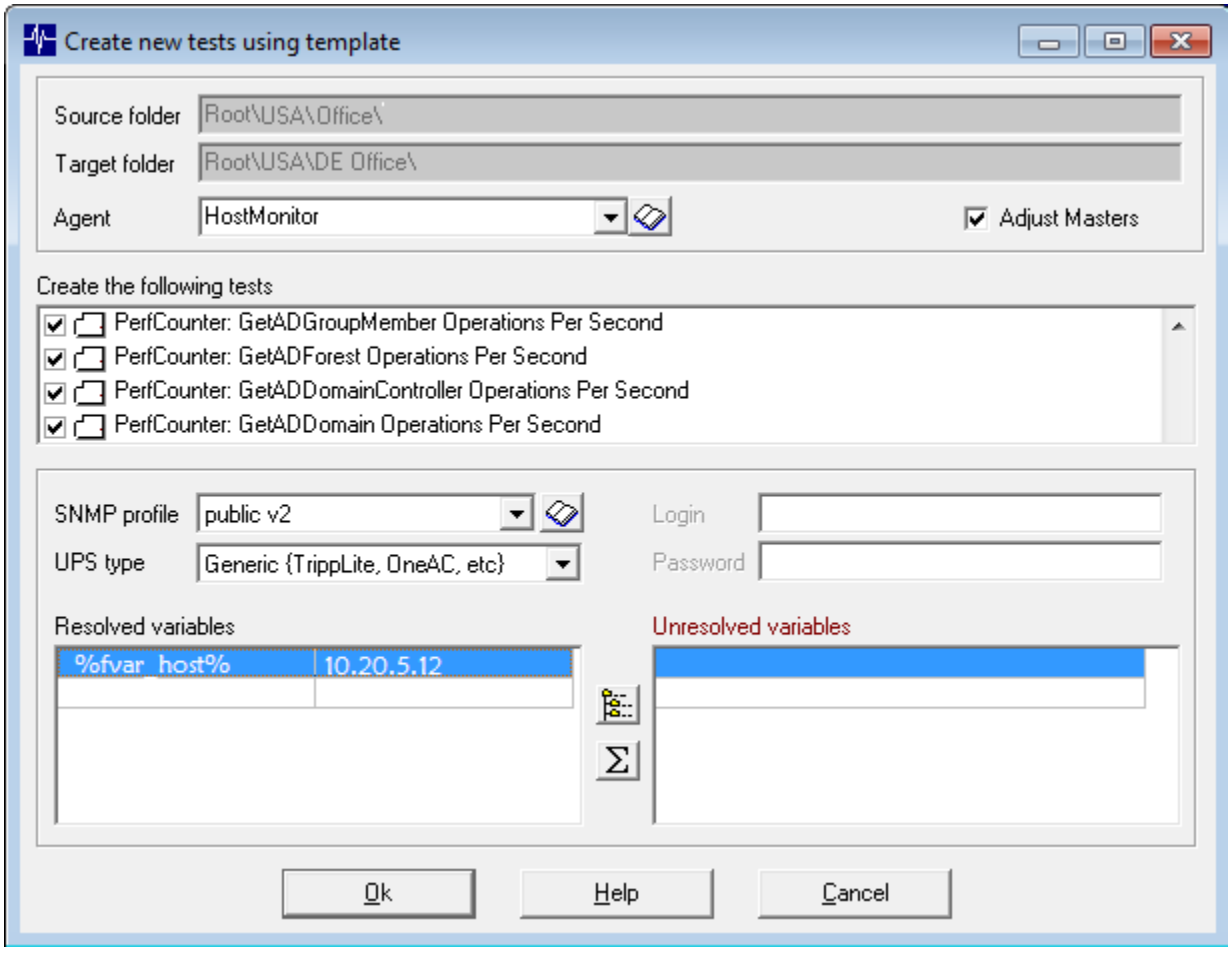
System Info uses various protocols to collect data and shows information and tests related to the host

For some test methods additional menu items available:
IPMI Browser retrieves data from servers using IPMI protocol
WMI Explorer allows you to explore the full set of WMI management classes and objects
Disk Meter displays chart with information about all disk drives mounted on target system
Process Meter displays chart with information about all processes running on target system

Note: main menu Tools offers similar items. You may start Trace, Telnet, Log Analyzer, Disk Meter, Process Meter, WMI Explorer, MIB Browser, IPMI Browser, System info to explore resources on specific host. If you are using RCC GUI installed on remote systems, you may copy DiskMeter.exe, IpmiBrowser.exe, MibBrowser.exe, ProcessMeter.exe, WmiExplorer.exe modules to RCC system as well.
Menu **Tools->Recent** keeps history of recent actions. E.g. you may check disk space on HostA using SuperMatrix window, check processes on HostB using Network Map, call IPMI Browser from main window - all these commands will be stored in Tools->Recent menu.

Also you may create your own menu items with associated commands. For more information, refer to Custom menu profiles section of this manual.

Check and copy
You may select set of tests, click on “Check and copy” popup menu item and select target folder.



Then you may change some parameters, e.g. change monitoring agent, set SNMP profile for SNMP related tests, change type of UPS device (for UPS related tests), set login and password for tests that require account information (see also: Connection Manager). If you are copying “template” tests and some of them depend on master(s), then HostMonitor checks if master template test items selected as well. Also HostMonitor checks if all variables will be resolved after replication - if there are some missed variables, you may define variables using Folder Properties and User Defined Variables dialogs.

Adjust Masters option - with this option enabled, if dependant tests copied with master(s) then HostMonitor adjusts master-dependant relations for newly created tests. E.g. if you copy 6 tests (5 UPS tests that depends on 1 Ping test) then new UPS tests will depend on new Ping test (if you are using folder-related variables for target IP address, then new tests will start to monitor new device without any manual adjustments).
If you copy just dependant tests without related master test, then HostMonitor will either
- unlink newly created (replicated) dependant tests from this “missed” master (if master is “template” test)
- keep dependency on original master test (if master tests are “normal” test items)

If you want to copy test items without any checks and modifications, use “Copy” function.

Note: Network Map Replicator offers more options, like
- Skip if similar test for target host already exists
- Adjust test settings automatically
- If Master tests not copied, try to find new masters using existing tests as examples

Menu Search

There are pretty standard search functions available thru this menu:

Find	- searches for test item(s) using simple text search within currently visible properties of the tests
Search again	- repeats the last search starting from current position (test item)
Find Bad test	- searches for test items with “bad” status (bad, no answer, bad content)

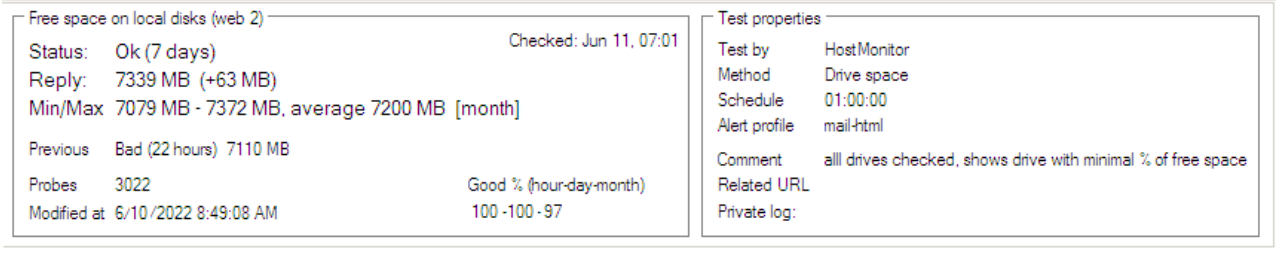
However there is one “advanced” option - “use expression” option available when you search for test item(s) within test list. With this option enabled you may specify search expressions using test related macro variables, constants, logical operators, etc. E.g.:

```
('%Reply%'>90) and ('%Status%'=='Bad')
('web' in '%TestName%') and ('10.10.' in '%agent%')
```

These expressions should conform to the same rules that are used for "advanced actions" but “historical” macro variables (variables like %StatTODAY_MinReply%, %StatThisWeek_DeadRatio%) cannot be used here.

Info Pane

With the Info Pane made visible, information on the currently selected test is displayed in the resizable area at the bottom, right below the Test Detail Area, allowing you to grasp test details at a glance. The Info Pane comes in particularly handy when you choose to display tests in the Test Detail Area as small or large icons (see User preferences dialog -> Interface page for more information on display options).



Use menu “View” -> ”Info Pane” to make this pane visible or to hide it.
You may click on Min/Max item in order to change time inteval used for data calculation: this hour / today / yesterday / this month / since reset. Double click will open Test History window

Also HostMonitor calculates time used by main thread for logging and actions (does not include time used by auxiliary threads, its not so important). You may see information like the following using Info Pane

Performed tests: 1877564 | 12.05/sec
Performed actions: 1008651 | 0.01/sec | ATC: 0.26 msec/action
Log records: 290543 | 2.10/sec | ATC: 0.01 msec/record
Logging pool usage: 0.5%

Where ATC means Average Time Consumption
This option can be useful for investigation of some 3rd party software related problems (e.g. if ODBC driver specified for ODBC logging consumes too much time).
Note: to see such performance information you should select folder item or several test items in Test Detail Area. If you select single test item, you will see different information about this specific test only

Quick Log pane

Quick Log pane allows you to check the history of latest events for each test or folder. When you select menu “View”->”Quick Log”, HostMonitor opens a pane located at the bottom of the main window and displays last 10 events for selected test or 50 events for selected folder (folder's list includes last events for every test within the folder).
Quick Log may work in 3 different modes:
- Show test results
- Show actions
- Show test results and actions

You may select Quick Log mode using popup menu that appears when you click right mouse

button on Quick Log pane.

“Show test results” mode
The term "event" means a log record that was added with every test status change. If logging mode for the test is set to "Reply" or "Full", HostMonitor will add a new record when test status changes or the value of "Reply" field changes.
There is popup menu item "Find the test". It allows for a test that generated the selected log record to be found quickly and is useful when the Quick Log shows records for entire folder.

In “Show actions” mode, HostMonitor shows the following information:
- Event time: the time when action was executed (or failed)
- Test: name of the test item that had triggered action execution
- Status: status of the test
- Action result: result of the action execution
- Action method: type of the action

If “use color palette” option is enabled, HostMonitor uses different colors for executed and failed actions. If you select a specific test in Test Details Pane, HostMonitor will display latest actions triggered by this test only. If no test is selected, folder item is selected or several test items are selected, HostMonitor will display actions triggered by all test items within current folder, sorting actions by the time of execution.
Note: you may tell HostMonitor to ignore some actions, i.e. do not store information about action results in Quick Log. The option “Quick Log: store action results” is located in Action Properties dialog. You may disable the option for unimportant actions, like “Play sound” action.

Folder Bar

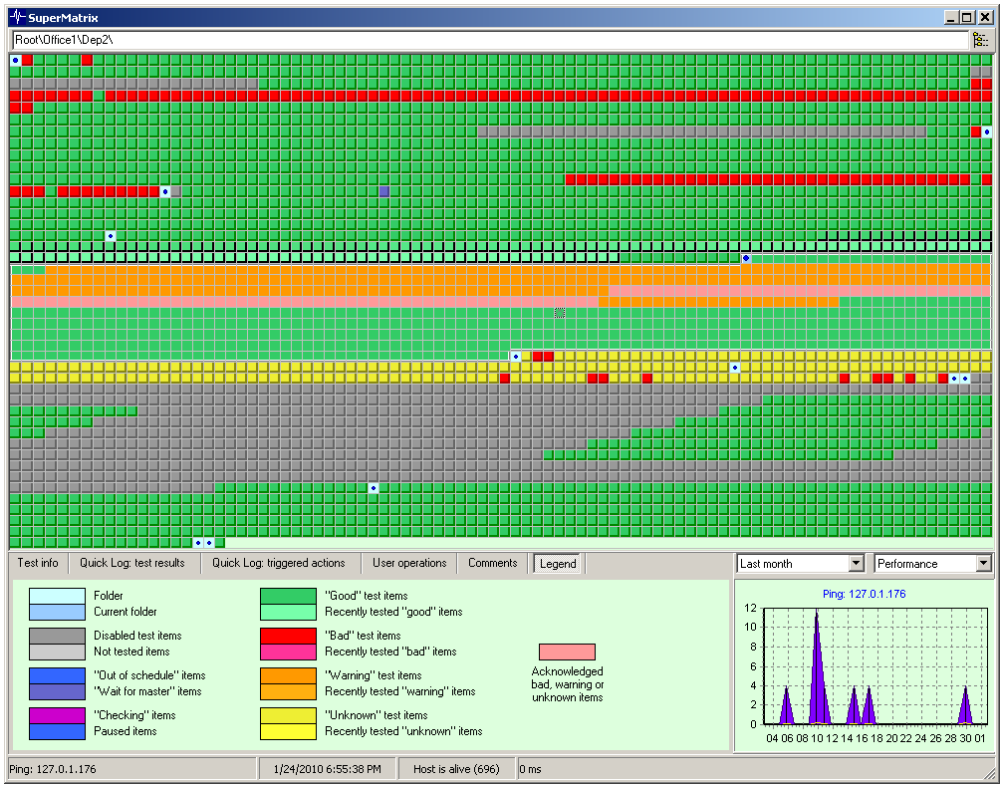
The Folder Bar provides a convenient way of accessing the tree when you need it, so that you can hide the Folder Tree panel and free up some screen space for the Test Detail Area. The name of the currently selected folder appears in the text box inside the Folder Bar. To select a different folder, pick a folder in the folder tree dialog that pops up when you click the button to the right of the text box.

Status Bar

Depending on the mouse pointer position, the Status Bar provides you with some helpful information on where you are and what is going on.

SuperMatrix window

When you have many thousands of test items this option can be very useful as it can display thousands of test items on one screen. For example if you have display with resolution 1600x1200, you may see about 19,000 test items on the screen. Use menu “View” -> “Super matrix” to open this window.



HostMonitor updates items in real time, using different colors for different test statuses, also recently tested items displayed in more vivid colors.

Popup menu items allow you to perform various operations on selected test item or folders.

- Acknowledge status
- Edit
- Find
- Search again
- Go to
- Refresh selected test(s)
- Refresh folder
- Refresh all items
- Pause
- Resume
- Disable selected test(s)
- Enable selected test(s)
- Disable folder

- Enable folder
- Test info
- History charts
- Log Analyzer
- View private log
- Related URL
- Trace
- Telnet
- Explore WMI
- Process Meter
- Disk Meter
- IPMI Browser
- Set profiles
- Hide panels
- Current color palette
- Quick switch to Trends | Reply | Icons

Also you may create your own menu items with associated commands. For more information, refer to Custom menu profiles section of this manual.

"Hot keys" provide quick access to some functions such as

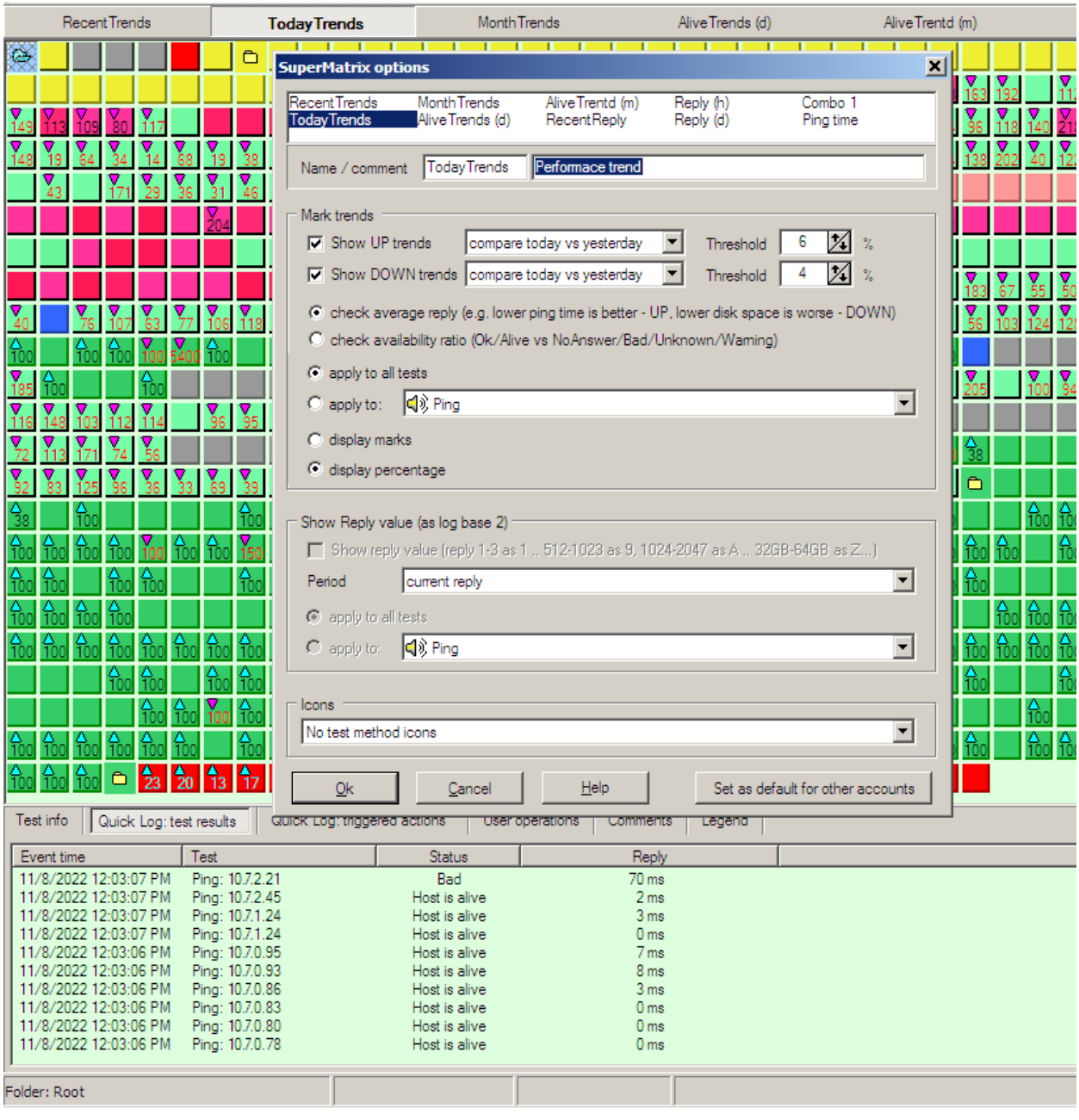
- Enter - edit test settings for selected item
- Space - refresh selected item(s)
- Ctrl+I – show Test Info dialog
- Ctrl+F – find test item by name
- F3 - search again
- Ctrl+G – tells HostMonitor/RCC to activate main window and find selected test in Test Details area
- Double mouse click: show 4 history charts for selected test item

Additional panels provide detailed information for selected test item:

- Test info – test properties and statistics
- Quick Log for test results
- Quick Log for actions triggered by the test item
- User operations performed on the test item (pause, disable, acknowledgment)
- Chart – chart shows performance and/or status related history for various periods of time (e.g. last month or last 48 hours, this week or last year)

You can turn this panel off at any time and see even more items on your screen.

Visualization options



SuperMatrix window may provide additional information for each test item
1) up and/or down trends based on average reply value of the tests items. HostMonitor may check and compare several time intervals:
- compare this and last hour
- compare today and yesterday
- compare this and last month

2) up and/or down trends based on availability ratio of the tests items (good/bad status ratio). HostMonitor may check and compare several time intervals:
- compare this and last hour

- compare today and yesterday
- compare this and last month

3) display reply value as log base 2
- current reply
- hourly average
- daily average
- monthly average

4) display test method icon for each test item; display icons just for bad/unknown/warning test items; display icons for specific test method

You may mark two or all three options, in this case “trends” option will be prioritized and lowest priority will be set to “icons” option. So reply marks will be displayed when trend does not reach specified limit and icons will be displayed when test reply value is empty (or reply option is set for another test method).

Note 1
In some cases higher reply value marked as UP(good) trend and lower values marked as DOWN(bad) trend. E.g.
- Memory test, VM host free memory, VM guest free memory (more free memory is better)
- Drive free space, VM host datastore space, VM guest free disk space
- UPS charge level
- UPS remaining time

Other tests show DOWN trend for higher reply numbers. E.g.
- TCP, UDP, URL, HTTP (reply field shows response time - higher response time is worse)
- CPU Usage, VM host CPU usage, VM guest CPU usage (higher CPU load is bad, down trend)
- Dominant Process (in all modes: CPU Usage, Handles, Threads, Memory usage)

For some tests UP/DOWN marks choosed depending on settings and options. E.g.
- Ping test - higher percentage of received packets displayed as UP trend; while higher response time, higher jitter or higher lost percentage displayed as DOWN trend
- Apache test - higher number of Idle workers displayed as UP trend; higher number for other parameters displayed as DOWN trend
- IIS test - higher number displayed as UP trend for the following options:
  ```
  File Cache Hits %
  Metadata Cache Hits %
  Kernel URI Cache Hits %
  URI Cache Hits %
  Output Cache Hits %
  ```
- Big-IP statistics - higher number displayed as UP trend for the following options:
  ```
  HTTP compression ratio
  HTTP Cache hits ratio
  HTTP Cache hits ratio (for cacheable data)
  ```
- Netscaler statistics - higher number displayed as UP trend for the following options:
  ```
  SSL cache hit ratio
  HTTP compression ratio
  Cache hit ratio
  ```
- WMI, Performance Counter, SNMP Get, SNMP Table - trend mode depends on comparision mode set for the test (less than or more than)

Some tests do not show trends when "apply to all tests" mode used. E.g. if you want to see trend marks for the following tests, you need to choose specific test method for "mark trends" option:
- File/Folder Availability
- File Integrity
- Compare Files
- Text Log
- Domain expiration

Note 2
Reply value displayed as log base 2 (inverse representation of the power of 2). E.g. [3] is displayed for reply values in 8-15 range. [M] is displayed for replies between 4MB and 8MB. 0 is 0.

		KB		MB	
0	0	**A**	1-2 KB	K	1-2 MB
1	1-3	B	2-4 KB	L	2-4 MB
2	4-7	C	4-8 KB	M	4-8 MB
3	8-15	D	8-16 KB	N	8-16 MB
4	16-31	E	16-32 KB	O	16-32 MB
5	32-64	F	32-64 KB	P	32-64 MB
6	64-127	G	64-128 KB	Q	64-128 MB
7	128-255	H	128-256 KB	R	128-256 MB
8	256-511	I	256-512 KB	S	256-512 MB
9	512-1023	J	512-1024 KB	T	512-1024 MB

	GB		TB		PB
U	1-2 GB	**e**	1-2 TB	**o**	1-2 PB
V	2-4 GB	f	2-4 TB	p	2-4 PB
W	4-8 GB	g	4-8 TB	q	4-8 PB
X	8-16 GB	h	8-16 TB	r	8-16 PB
Y	16-32 GB	i	16-32 TB	s	16-32 PB
Z	32-64 GB	j	32-64 TB	t	32-64 PB
a	64-128 GB	k	64-128 TB	u	64-128 PB
b	128-256 GB	l	128-256 TB	v	128-256 PB
c	256-512 GB	m	256-512 TB	w	256-512 PB
d	512-1024 GB	n	512-1024 TB	x	512-1024 PB

y	1-2 EB (exabyte 2^60)	z	2-4 EB

Profiles

You may setup 10 profiles and switch between profiles with one click.
For example you may
- use one profile in order to display up and down trends for Ping tests based on average reply values gathered today and yesterday with 10% up-threshold and 5% down-threshold
- use another profile in order to display up and down trends for all tests based on availability ratio of this and last month with 5% up-threshold and 2% down-threshold
- 3rd profile: display current reply for CPU Usage tests and show icons for other test methods

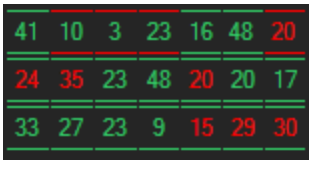
Each operator may set its own profiles. Also admin may setup default profiles for all operators that did not set personal profiles yet (“admin” in this case operator with “edit GUI options for all accounts” permission)

Quick switch

Also you may temporarily override profile settings and display just trends or reply value or icons for ALL test methods. You may use popup menu items or hot keys: Ctrl+E (show icons); Ctrl+R (show reply values); Ctrl+T (show trends). HostMonitor will use limits and time period specified for current profile but will apply selected option for all items (even if profile set to show trends just for memory test, for example); also it will display icons regardless of test status and size of the cells.
You may press the same hot key (or use the same menu item) in order to deactivate “quick switch” mode and activate profile settings again. Or just switch to another profile when needed.

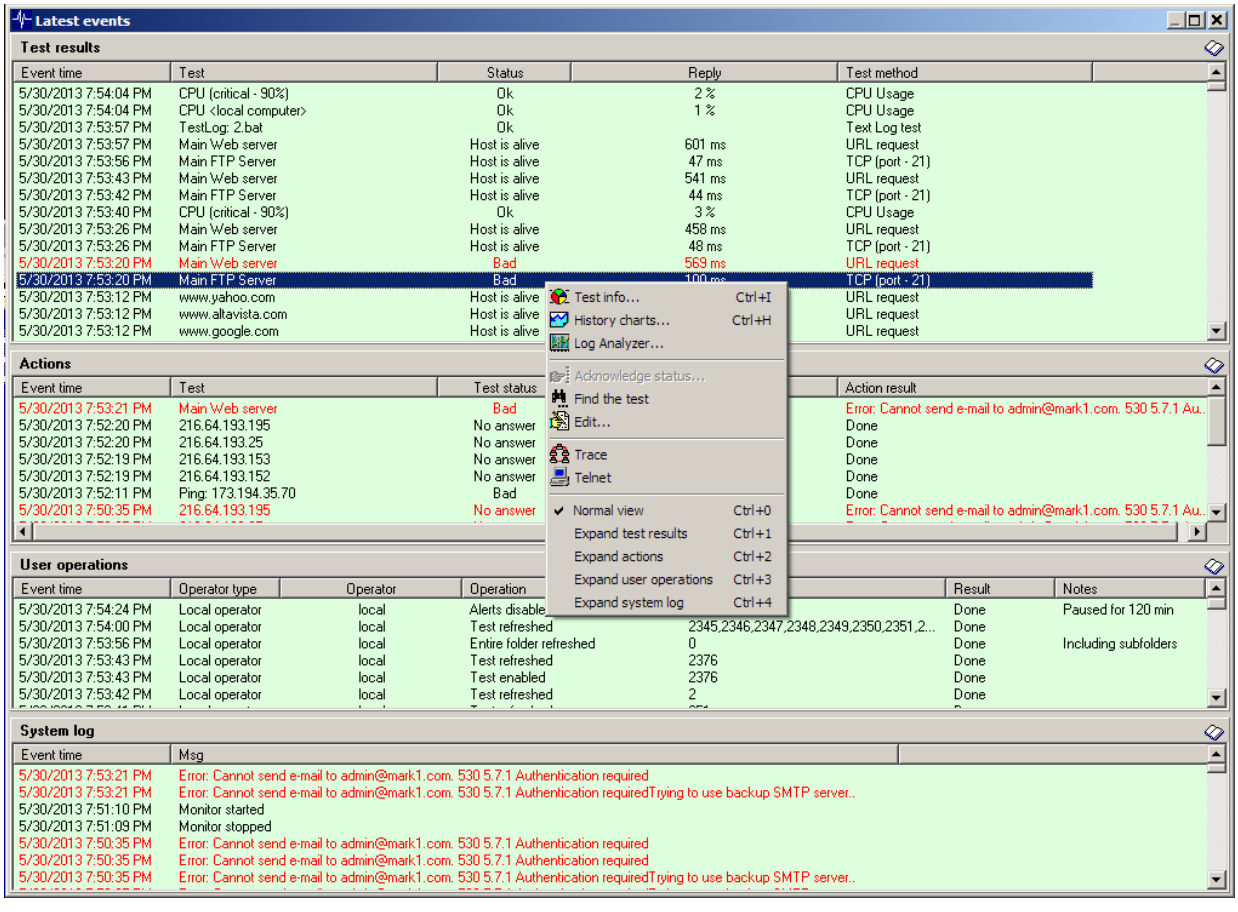
Current color palette

This option turns off bright green-yellow-red cells colors and tells SuperMatrix window to use current palette. Also “icons” mode works differently in this case, images will be selected based on test method AND test status.



Recent Events

Recent Events windows shows all events in one place: test results, actions, user operations and HostMonitor system messages. Popup menu allows you to retrieve additional information for selected test item (Test Info, History charts), start Log Analyzer, trace route to target host, acknowledge test status, etc
In order to access this module use menu “View” -> “Recent events”.



Top Hosts

Top Hosts window may show user defined set of "top" test items. In order to access this module use menu “View” -> “Top hosts”.

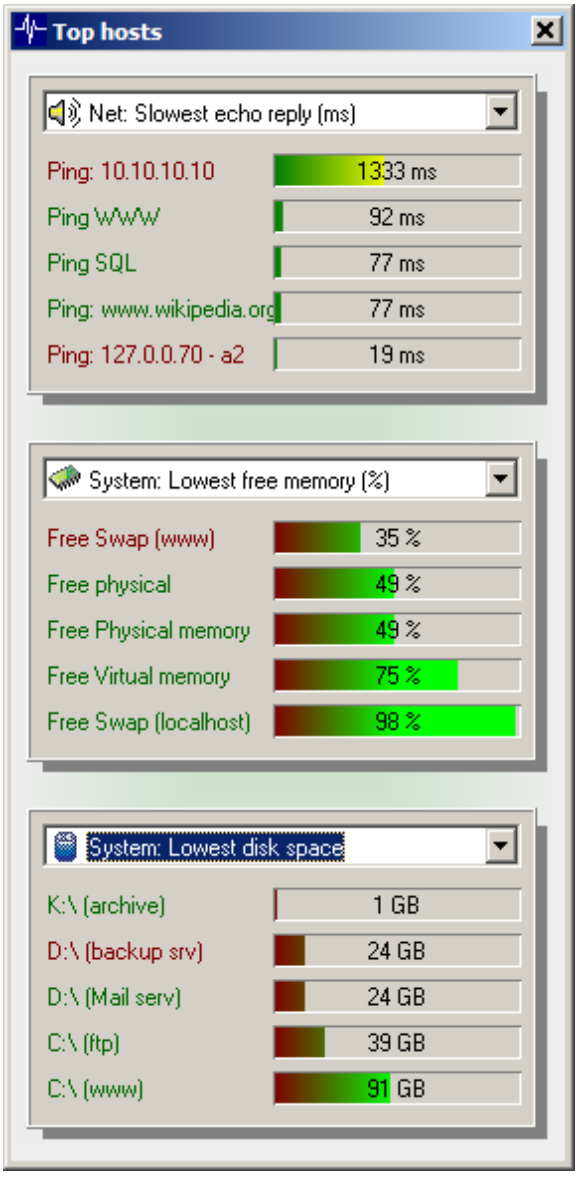
Window may show 5 top hosts in each category:

Network:

- Highest ratio of lost packets	Ping tests
- Slowest echo reply (ms)	Ping tests
- Highest traffic	Traffic Monitor

Web:

- Highest traffic	Appache, Tomcat, IIS
- Highest error ratio	NGINX, Tomcat and IIS
- Lowest cache hit ratio	NGINX and IIS cache related tests
- Slowest web site (ms)	URL, HTTP



Memory tests:

- Lowest free memory, virtual
- Lowest free memory, physical
- Lowest free memory, swap/page
- Lowest free memory, virtual (%)
- Lowest free memory, physical (%)
- Lowest free memory, swap/page (%)
- Lowest free memory (%)

  note: this mode tells HostMonitor to check all memory related test items (virtual, physical and swap memory tests)

Dominant Process tests:

- Process: Highest CPU usage (%)
- Process: Highest handles usage
- Process: Highest threads number
- Process: Highest memory usage
- Process: Highest VM usage

System resources:

- Highest CPU usage (%)	CPU Usage
- Lowest disk space (%)	Disk Free Space and UNC tests
- Lowest disk space	Disk Free Space and UNC tests
- Hottest system/CPU	QNAP, Synology, NetApp, Cisco, Juniper and HP iLO Temperature tests

HDD info:

- Oldest disks (days)	HDD SMART tests
- Hottest disks (C)	QNAP Temperature, Synonoly Temperature and HDD Smart tests
- Worst disks	HDD SMART tests (# of relocated, pending, uncorrectable sectors)
- Highest disk load (%)	Synology Disk Load and Performance Counter('% Disk Time') tests

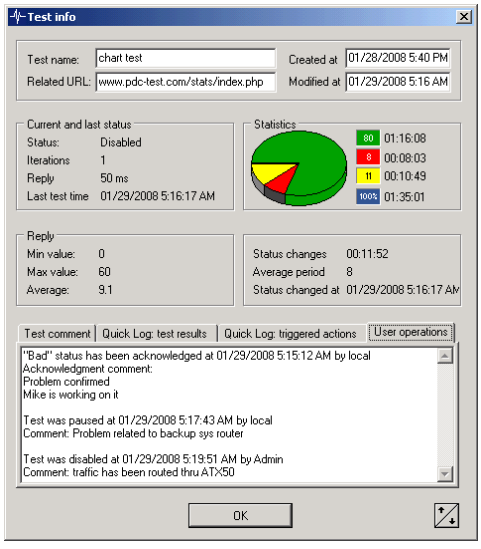
Note: Average mode is not applicable for HDD SMART modes.

UPS

- Highest load	UPS Load tests
- Highest temperature	UPS Temperature tests
- Lowest charge level	UPS Charge tests

Popup menu allows you to skip Disabled, Paused and/or Acknowledged test items, you may check Test Info, History charts for specific item or set of items, etc.
Menu items "Show test name" and "Show host name" tell HostMonitor to display test name or target host name (or IP address).
Note1: HostMonitor may adjust long test names trying to fit text in the window, for example it can remove "free disk space" text from the test name when test displayed in "System: Lowest disk space" group).
Note2: Average mode is not applicable for HDD SMART modes.

Test Info dialog



Test Info dialog shows information about latest acknowledgement, pause and disabling operations on specified test item. Also this window shows unique ID of the test item, test statistics, number of links to the test item, test comment, Quick Log and the actions triggered by the test item.
Note: button beside test name field may switch display mode from “name” to “full path+name”

Also, when you select SNMP Table test item, Test Info dialog shows table with data retrieved from SNMP agent. For each retrieved counter, it shows OID, current value, previous value and difference. HostMonitor/RCC allows you to sort items by each parameter; also you may copy data to clipboard as CSV (comma separated values) or TSV (tab separated values) list.

When “Related URL” field specified for the test item points to some web site, you may click on this field displayed by Test Info dialog. HostMonitor will open default browser and show web site. Also it may open default mailer program when URL points to some e-mail address (e.g. mailto:admin@mycompany.com)

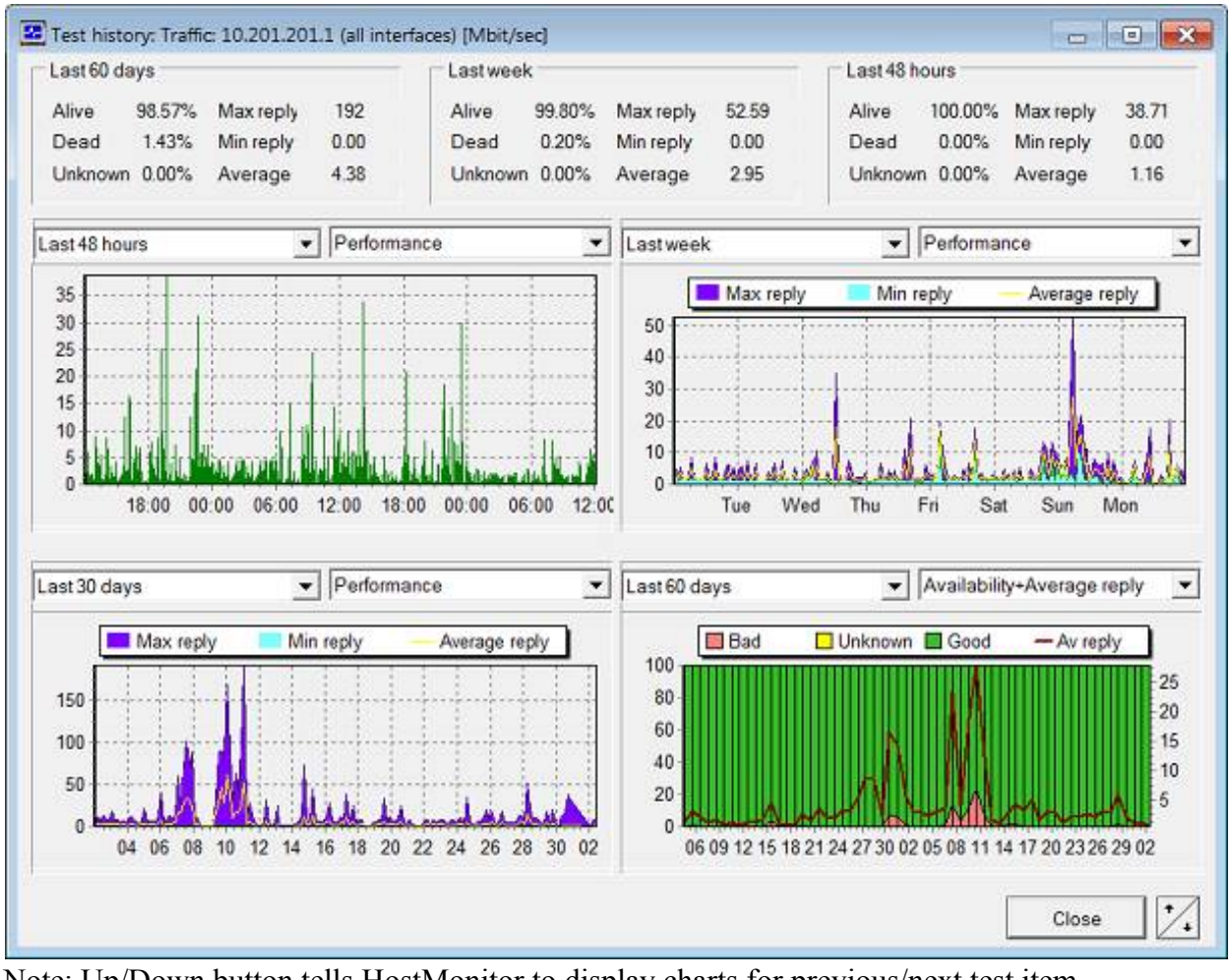
If Log Visualizer is installed, Test Info dialog allows you to call Log Visualizer using necessary command line switches to start utility in maintenance-free mode. So you just need to click a button to see the chart for the test item.

You may bring up dialog using main menu Tests -> Test info; also you may use popup menu or simply press Ctrl+I

Test history

When "Store historical data in the file" option (located in "Test list properties" dialog) is enabled, HostMonitor collects additional statistical information for each test item. Such information can be displayed by "Test history" window, SLA reports, Web Service interface, etc.

"Test history" window shows 4 "historical" charts for single test item. You may select test item and use "History charts" popup menu item or press Ctrl+H to open this window. For each chart you may choose different display modes and different time intervals.
RCC (Remote Control Console) may show time offset in History window title (when time on HostMonitor system is different from RCC time)



Note: Up/Down button tells HostMonitor to display charts for previous/next test item.

Chart mode

- Availability:	shows information about alive/dead/unknown ratio based on test results
Availability +Average reply:	shows information about alive/dead/unknown ratio plus line that displays average reply of the test probes (note: left axis provides information about alive/dead ratio; right axis provides information about average reply)

- Performance: shows information about minimum, maximum and average reply values of the test (see brief and detaled mode)

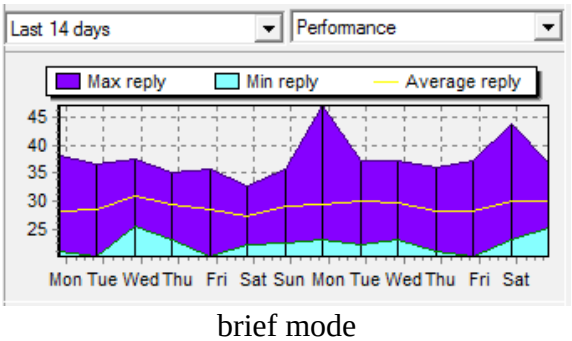
Time period

- Prediction: next 7 days
- Today
- Yesterday
- Last 24 hours
- Last 48 hours
- This week
- Last week
- Last 7 days
- Last 14 days
- This month
- Last month
- Last 30 days
- Last 60 days
- This year
- Last year
- Last 12 months
- Last 24 months

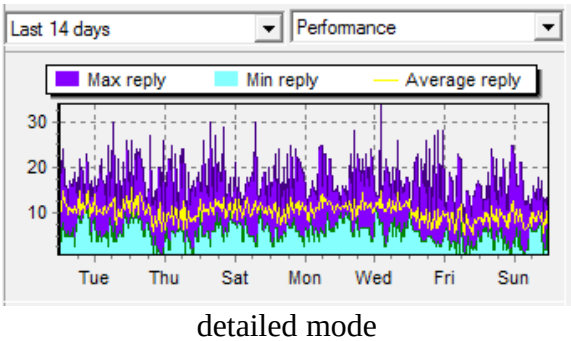
"Prediction: next 7 days" mode tells HostMonitor to calculate and show statistical counters for future 7 days. HostMonitor analyzes previous 30 days of test results trying to predict future test results. HostMonitor shows counters (text labels) for next 7 days while charts show data for last 7 days and next 7 days (using different color for past and the future). Of course software cannot tell you what really happens in the future, its just assumption based on historical data.

Detailed mode available for Performance charts
History-related windows may display charts using 2 modes:

- brief (works without log files, supported since version 8)
- detailed (requires compact logs, supported since version 13)



brief mode



detailed mode

HostMonitor automatically chooses detailed or brief mode for charts. If you just installed HostMonitor version 13, there are no data yet so Brief mode will be used. After 5-10 minutes HostMonitor may switch to Detailed mode for some time intervals (Today; Last 24 hours). In couple days HostMonitor may enable Detailed mode for [Yesterday], [Last 48 Hours], [Last 7 days], [Last 14 days] time intervals. And finally Detailed mode will be enabled for [This month], [Last 30 days], [Last moth], [Last 60 days] intervals.
Note #1: [This year], [Last year], [Last 12 months], [Last 24 months] - only brief mode supported for such time intervals.
Note #2: If you disable compact logs, only brief mode will be used.

Charts can be updated by timer so you may keep Test History window open and you will see

updates. Refresh rate depends on selected time interval: 5min for daily charts; 1 hour interval for weekly charts; 2 hours interval for monthly charts.

Zoom/Unzoom operations adjust time labels. Various formats can be set depending on selected time interval:

- day of the month
- day of the week (day of the month)
- day of the week
- day of the week hh:mm
- hh:mm
- hh:mm:ss

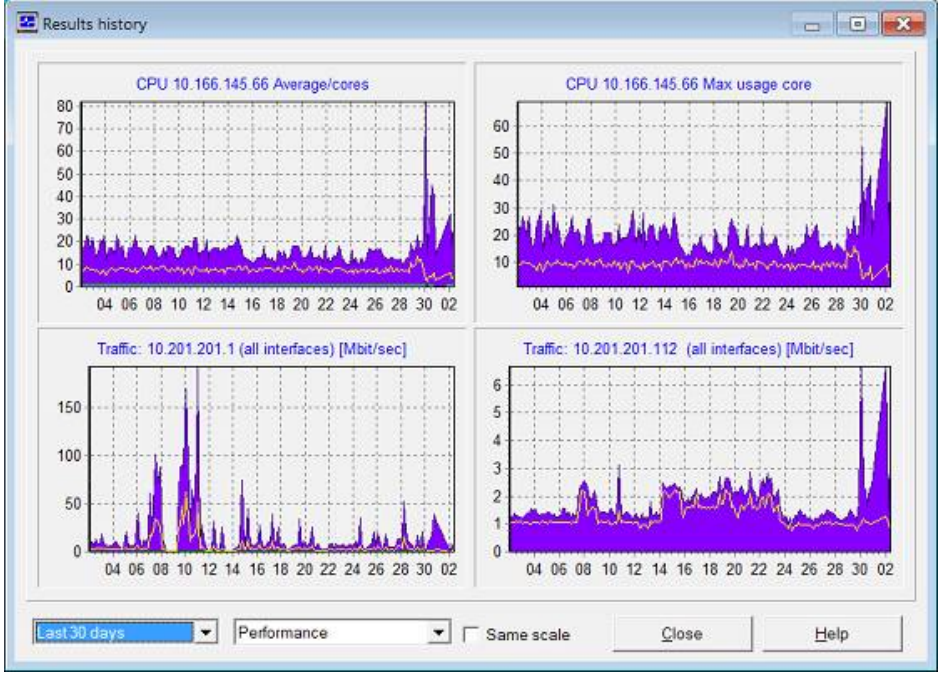
How to zoom? Draw a rectangle around the chart area you want to see in detail - click left mouse button and drag cursor from top-left to bottom-down. Dragging in the opposite direction resets axis scales (unzoom).
Note: you may zoom in chart when single test item selected.

You may copy raw data from chart into clipboard using popup menu items

- Copy to CSV
- Copy to CSV all tests (available when several tests displayed)

Also popup menu offers options to hide maximum, average and minimum results, e.g. you may display just minimum values for Memory tests and display maximum plus average values for CPU Usage tests.

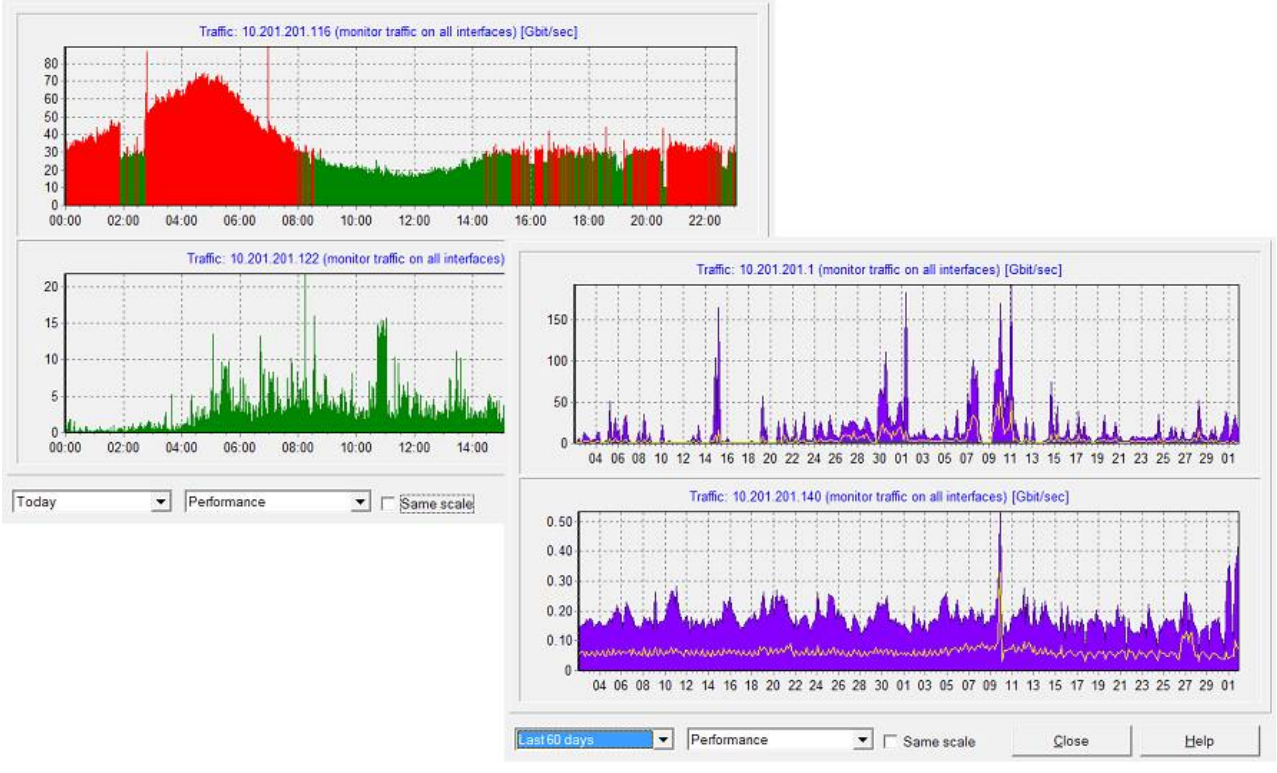
Also you may select up to 16 test items or choose a folder item (in Test Details area) and open "History" window that will show up to 16 charts at once. If you select more than 16 test items or selected folder contains more than 16 test items, HostMonitor will show charts for 1st 16 test items.



HostMonitor (RCC) will display single chart for each test, you may choose display mode and time periods as well, however these settings will be applied to all 16 charts at once.

If you double click mouse button on any chart, HostMonitor will open 4 charts history window for specified test item so you will be able to see charts for various time periods for selected test.

If you open Test History window for 2 or 3 selected test items, charts will be located one below another. Horizontal mode allows to see more details on the charts



"Same scale for groups" option sets the same scale for groups of selected tests. For example:

- if you select CPU Usage and Drive Free Space test and open Test History window, then HostMonitor will use one scale for CPU tests and another scale for drive free space tests
- if you open Test History window for Drive Free Space tests some of which use GB units while others display percent of free space, then HostMonitor will use one scale for tests with "%" units, other scale for tests with "GB" units
- if you open such window for CPU Usage, Ping, Trace and Traffic Monitor test items, then HostMonitor will use one scale for Traffic Monitor tests, another scale for CPU+Ping+Trace test items

Auditing Tool

Any operator that has access to “Root“ folder (in other words has access to all test items) and owns rights to configure tests, folders and action profiles may launch Auditing Tool (available thru menu View). Auditing Tool checks test and action settings, operational system, license, options and inform you about possible problems.
Note: when you setup some test or action, HostMonitor verifies settings at this time however some problems may appear later. E.g. you may setup “Execute external program” action using correct path to executable module but later someone can move or remove the file.

Among various possible problems Auditing Tool checks for the following problems:

- missed external files that were specified for “Active Script” and “External” tests, “Play sound”, “Execute external program” and “Execute HM script” actions;
- missed templates for “Send message to pager (TAP)”, “Send message to pager (SNPP)”, “Send SMS (GSM)”, “Send SMS (SNPP)”, “Send e-mail”, “Send message to ICQ” and “Send message to Jabber” actions;
-
- not defined user-defined variables specified as parameters of any action (e.g. destination e-mail address or service name);
- not defined user-defined variables specified in condition to start “advanced mode” actions;
- not defined user-defined variables specified in “Normal”, “Warning” and “Tune up Reply” expressions (see optional status processing);
- not defined folder-level variables specified as parameters of any test item;

- possible loops between master and dependant test items including test items dependant on expression. Auditing Tool checks mixed links between tests as well (e.g. TestA depends on list of other tests including TestB, TestB depends on expression that includes TestC and TestC depends on expression that includes TestA);

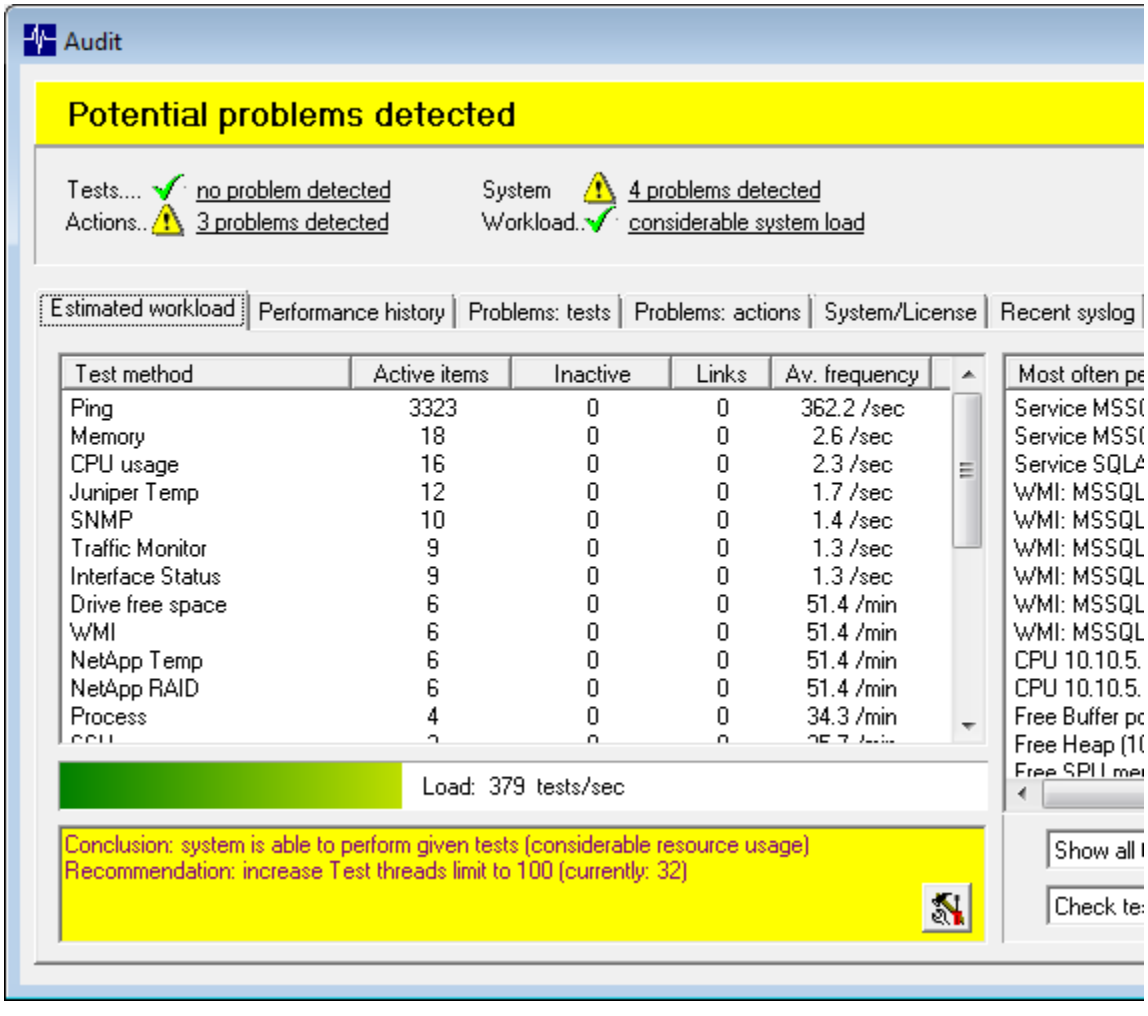
- some possible problems related to OS and your license (e.g. you should not use Windows XP Service Pack 1 or Windows 2000 Service Pack 1)

- also, if you enable "Show unused actions" option, HostMonitor will check test items, report settings, scheduler and so on and displays list of alert profiles that are not in use.
  Note: Auditing report does not include action profiles without actions such as "Do nothing" profile

- ATC time (Average Time Consumption) consumed by primary and/or backup ODBC logging. Auditing Tool warns you when logging process is too slow for your configuration (e.g. you have a lot of tests performed with short interval and you are using Full logging mode). Then you may try to increase performance (e.g. replace ODBC driver or move your SQL server to faster machine) or change logging/testing options.

When error in test list detected you may double click mouse button on the item (or use popup menu item) to open Test Properties dialog, correct the problem then use "Revalidate" button to recheck your settings. The same popup menu allows you to open Folder Properties dialog and edit settings of the folder where selected test item is located. "Do not check disabled" items option allows you to skip disabled test items from auditing.
If there are some errors detected in action profiles you may double click mouse button on the item or use popup menu item to open Action Profiles dialog, correct the problem and use "Revalidate" button to recheck your settings.

Auditing Tool includes “Estimated workload” tab that provides information about estimated load of HostMonitor. Also auditing tool shows most frequently used test items for each test method. It allows you to view items performed directly by HostMonitor, Remote Monitoring Agents or all items without separation.



The tool scans all tests within the loaded list and calculates estimated frequency of checks for each test type. This allows you to check which test method will be used most frequently and thus will use most of the systems resources.
Of course software speed and CPU load depends on many factors, e.g. 400 fast Ping tests every second can be considered as medium load; while 100 URL or Dominant Process tests per second can be considered as high load - various tests use different amounts of system resources and exact resource usage depends on lots of factors, some of which are beyond calculations.
That’s why after significant changes in test list we recommend to let HostMonitor run for some time (at least 10 minutes) and then use Auditing Tool to check for possible problems and recommendations based on your actual settings (e.g. it may recommend increasing thread limit or limit related to Active RMA agents).

Conclusion could be different if there are too many tests that must be performed with high frequencies. For example:

Conclusion: system is not able to perform all the tests!
Recommendation: increase "tests/sec for Active RMA" limit to 512 and reconsider (increase by 15%) intervals for tests performed by Active RMA tests.
Note: Reports processing consumes too much time: 20% (18 ms/report, 11 rep/sec)

Please note:

- SNMP Trap tests are not calculated because HostMonitor doesn't know how often traps will be sent by 3rd party software.
- Also if you use dynamic monitoring list (e.g. you have setup HostMonitor to import tests from some dynamic database or you are using script to disable/enable tests under some conditions), calculated estimate load could be far from real.

Performance history

On “Performance history” page you may check HostMonitor performance charts for:

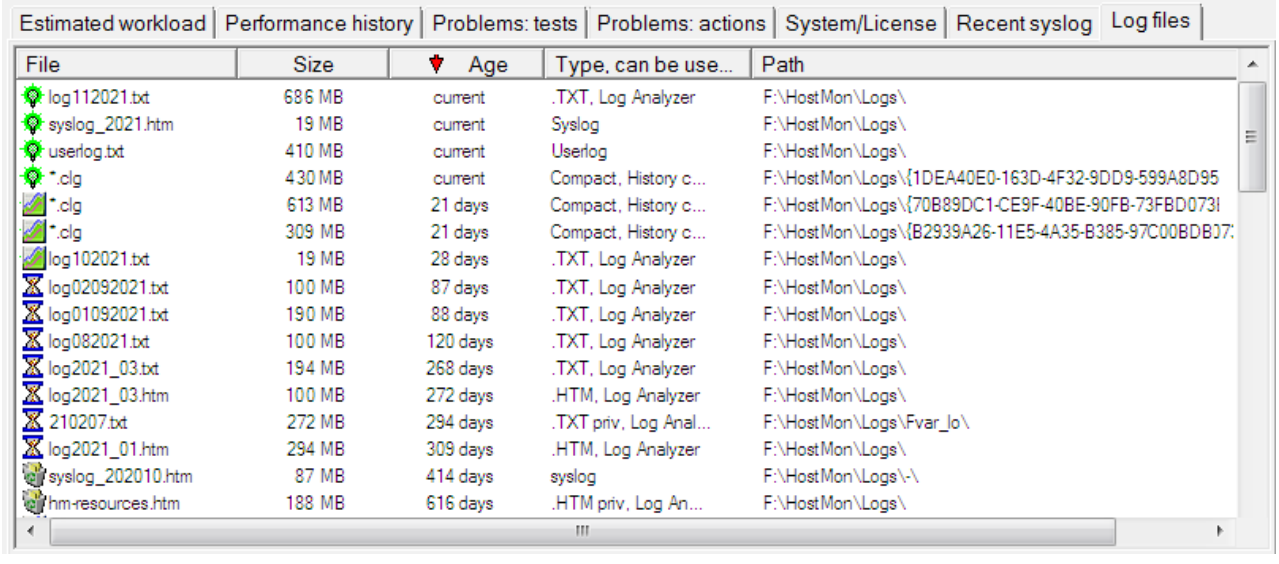
- number of “good” test results
- number of “unknown” test results
- number of “bad” test results
- number of executed “good” action
- number of executed “bad” action
- ATC time (Average Time Consumption) consumed by started actions
- number of log records with test results
- number of system log records
- ATC time (Average Time Consumption) consumed by logging

These charts can be created for last 24 or 48 hours; for last 14 or 30 days.

Recent sys log

Also Auditing Tool provides “Recent sys log” page. Here you can see up to 128 recent records from system log. This is especially useful when you are connecting to HostMonitor from remote system using RCC and you do not have access to system log file itself.

Log Files page



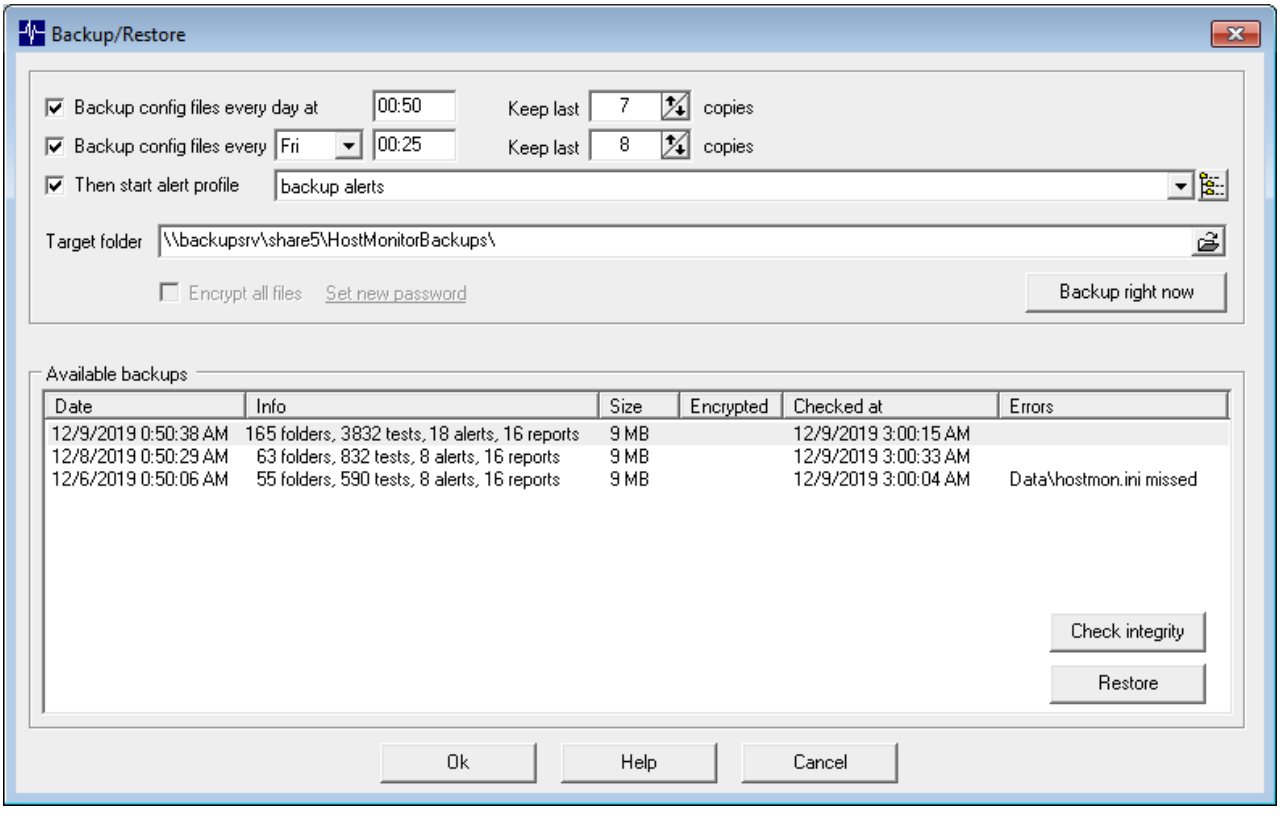
Some customers have just 2-3 log files - one log file with test results (common log), single system log file and user operations log.
Other customers may have thousand log files:

- common log file(s) with test results, changed monthly, weekly or daily
- private log files for 30,000 test items (each of 30,000 logs can be changed on regular basis as well if you are using file name like %TestID%-%yyyymmdd%.log)
- system log files (can be changed on regular basis as well)
- user operation logs
- compact log files

There are log processing options but some customers do not setup HostMonitor to remove old log files automatically and keep 500,000 forgotten log files.
Auditing Tool finds and displays all log files in a single table. It shows file name, size, age, type of the log and location. In some cases it shows summary - single record with size of all *.txt or *.clg files in the folder.
You may sort items by any field (e.g. name, size, age) and use popup menu items in order to remove unnecessary files.

Backup options

HostMonitor may create backup copies of all data files once a day and/or once a week; keep last N daily and/or weekly copies; remove old archives, start actions when backup procedure failed, etc.
You may adjust backup options or restore settings from archive using menu File->Backup options (you should use user account with "backup/restore operations" permission; by default only admin account has such permission, you may adjust account settings and permissions using menu User->Operators
Note: only "scheduled" actions will be executed, i.e. a condition to start action should be set to "on the schedule" (in Action Properties dialog).



Also HostMonitor may backup your VB and Java scripts, HostMonitor script files (.HMS, .VBS, .JS, .PS1, .CMD, .BAT files). If you are using some external scripts for tests or actions, we recommend storing them in Scripts subfolder within HostMonitor data folder (e.g. C:\ProgramData\HostMonitor\Scripts\).
Note: compression and encryption for archives will be implemented soon.

Tests & Test methods

Tests: General Information

HostMonitor is network-monitoring software that allows you to keep a close eye on what is going on the network. Monitoring is done by performing periodic checks of the network resources that are to be watched. These checks, in the HostMonitor terminology, are called tests. It is the administrator's responsibility to identify exactly what needs to be checked, and create a set of tests that will be doing the job.

In order to be able to create a monitoring environment that suits your needs, it does what you meant it to do and reacts to events adequately and predictably, you must have a good enough understanding of it:

- Each test has a set of properties that can be divided into statical and dynamical properties. HostMonitor doesn't change statical properties; the user has to set them in the Test Properties dialog (e.g. Test Name, Comment, Related URL, list of Master tests, Test Interval, Schedule, Alert Profile, etc). When performing tests HostMonitor changes dynamical properties, such as: Status, Reply, Last Test Time, Recurrences, and all kinds of statistical information. User can't directly change dynamical properties, only can reset statistics for specified tests using a 'Reset' button in a Toolbar or menu item Test->Reset. Testing of specified tests can also be manually performed at any time (not waiting for the time interval) using a 'Refresh' button in a Toolbar or menu item Test->Refresh (or just select a set of tests and press 'Space' button). User can set a list of the test properties to display by using Columns page in the User Preferences dialog.

- HostMonitor performs tests in intervals that are set individually for every test, or on scheduled time (day of the week, or month, see Schedule). Depending on the test result, HostMonitor assigns one of the available statuses to it ('Host is alive', 'No answer', 'Unknown', 'Unknown host', 'Ok', 'Bad', 'Bad contents'; there are also special statuses available: 'Not tested', 'Checking..', 'Disabled', 'Wait for Master', 'Out of schedule', ‘Paused’).

- After finishing a test HostMonitor performs next steps:
  - Checks “Optional status processing” options (“Reverse alert”, “Use Warning status”, “Use Normal status”) and sets user defined status when necessary
  - Updates statistics (dynamical properties), such as Total time, Alive time, Dead time, Total tests, Passed tests, Failed tests, Average reply, etc;
  - If necessary, HostMonitor adds information into a log file. You can find information about different log file types in Log&Reports section of this documentation;
  - If necessary, the program starts actions defined in the action profile.

Note: To operate with a test or a group of tests user can use Toolbar, popup menu or main menu Test. List of available actions: Add test, Edit test(s), Create link, Remove test/link, Copy test(s), Enable/Disable test(s), Pause/Resume test(s), Refresh test(s) status, Reset statistics, Show statistics, View private log, Trace, Telnet. For more information about user interface, please, refer to TestList&Windows section of this documentation.

Links

Links allow you to put the same test item(s) into several different folders. Unlike “copy” operation that creates independent copy of the test item, “link” operation does not create another test item - it creates link (image) of the test item. What is the difference?

- **Copy:** If you need to create a test item similar to existing one and then change some parameters of new item (e.g. you want to have similar test items to check set of services on different servers), use Copy operation. Copy will create new test item(s) with the same properties, then you will be able to modify each item independently; HostMonitor will perform separate checks (test probes) for each item.
- **Link:** If you want to see exactly the same test item(s) in several different folders, use Link operation. If you select original test or any of its links and modify test settings, your changes will automatically take effect for all links of the test.

Working with links

“Link” function is available through the main menu Test and from the context popup menu (to access the popup menu select the test(s) and click right mouse button). Also if you select test item that already has some links, you will see “Links info” menu item. Using this menu item you may access “Links list” dialog window, it shows the information about all folders which contain links to selected test item. You may remove some links or you may remove test itself (including all links to the test).

If test changes its status, HostMonitor will reflect status change in all folders which contain links to the item. The same is true for any test modifications. If you select any of the links and then disable, enable, pause or resume the item, acknowledge test status or change some parameters of the test, you will see the same effect in all folders with linked test item.

However if you select some test/link items and click “Remove” button, HostMonitor will remove only selected items. So, if you select 2 of 3 links to the same test item and click Remove button, HostMonitor will remove 2 selected links but keep the 3rd one. If you want to remove all links to the test, you should select all links or use “Links list” dialog.
Also you may use menu item "Test | Remove items with links". It allows you to remove selected set of test items including links to these selected items, even when some of links are not selected. E.g. if you select just 1 link of each test, this function will remove selected items and all items linked to them.

Parent folder

If you take a look at the test list, original test item and all of its links look exactly the same (unless you are using different color palettes for different folders). The reports will show tests and links, RCC and Web Service will display links as well. So, there is no difference which item is original and which item just a link? Almost. There is only one function that makes the difference – actions. If you are using folder related macro variables (e.g. %FCommentLine1% or %FullPath%) as

parameter of some action, HostMonitor will use parameters of the parent folder - original folder where test was created.

If you create a link to the test in another folder, the parent folder is still the same. If you then move a link to a different folder, the parent is still the same. However if you move original item to a different folder, HostMonitor will change the parent folder of the test. Also if you remove the original item while keeping the link, HostMonitor will reassign the parent folder to the folder where link is located. If your test items have many links and you are not sure which one is original, use "Links list" dialog window, it will show the parent folder and the list of the links.

Links and "Home folder" option

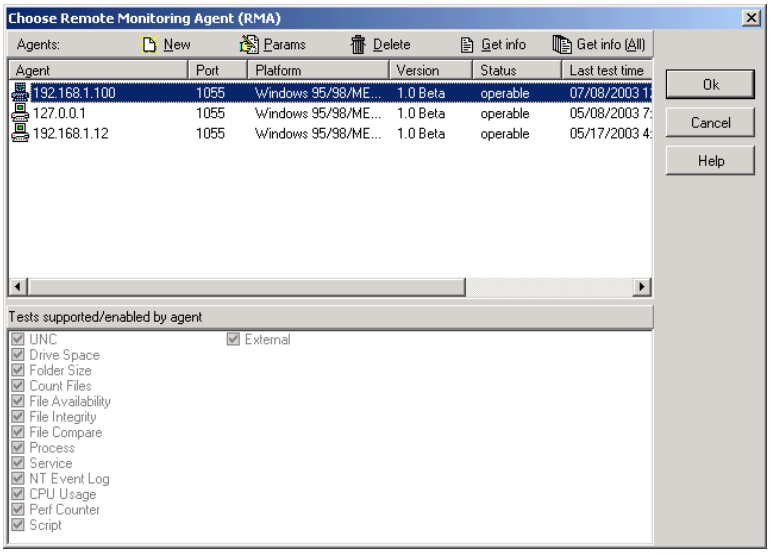
The "Home folder" option allows you to limit access to the folders on per-account basis. What happens when operator does not have access to the entire test list but has access to some low-level folder and this folder contains some links while other links to the same test located above allowed home folder? Operator will be able to work with this test item and modifications will have effect in all linked folders (of course operator should have necessary rights to perform operation, e.g. "configure test/folder" permission).
Operator may remove only links located within its home folder; it cannot remove links/tests located outside of the scope (even using "Links list" dialog window).

Other notes:

1) Linked items show slightly different status icons, so you know when your modifications will have effect in several folders (e.g. "Host is alive" item shows icon for single test item; - for linked item)
2) Test Properties dialog shows yellow warning icon when you are editing linked test item. You may click on the icon to bring up "Links list" dialog.
3) Estimated Load window shows information about links as well (just for informational purpose - links create minimum increase in system load).
4) If you want to remove entire folder, HostMonitor will ask for confirmation when the folder contains subfolders or test items. If the folder contains links only, it will be removed without confirmation.
5) When you export tests using "export current folder" or "export current folder and subfolders" option, HostMonitor exports tests located in the folder then it exports links (items whose parent folder located outside of the scope but one of the test links located within scope). This allows you to find and modify or remove information about links easily.
6) Import function may create links as well (use "LinkedTo=<full_folder_name>" parameter)

Tests: Agent List

HostMonitor can perform tests by itself or it can use Remote Monitoring Agent for this purpose. RMA is a small application that accepts requests from HostMonitor, performs test and provides information about test result back to HostMonitor.
When you setup the properties of a test in Test Properties dialog you may select an agent from drop down list or click on a button (to the right of the field) to manage agent list.



How to do:

- How to add new agent to the list
- How to edit network connection parameters for an agent
- How to obtain information about agent(s)

How to add new agent to the list

To add a record for a (new) agent click on "New" button or press Insert key in the list of agents. When the dialog "Agent Connection Parameters" appears choose type of the agent (passive RMA or active RMA) and set the following parameters for the agent:

Passive RMA

Passive RMA is small application that accepts requests from HostMonitor, performs test (or action) and provides information about test result back to HostMonitor.

- Agent address:
  provide the host name or an IP address of the system where RMA is installed
- Item name:
  name of the agent (this name will be displayed in agent's list, and will be used by HostMonitor for agent identification). By default an address of an agent will be used as name for it but you may specify any other name that you like
- Port:
  TCP port that will be used for communication between HostMonitor and the agent. Here you

should specify the same port that you have already specified when that agent was installed and configured on a remote system (by default agent uses port #1055)

- Timeout:
  communication timeout in seconds. A maximum amount of time that HostMonitor will wait for an answer from the agent. Please note: this timeout should be big enough to allow an agent to perform a test before sending an answer to HostMonitor. When, for example, you are launching an external test and an external program needs 15 seconds to perform this test then the timeout should be set to 15 seconds plus an amount of time that is necessary for data exchange between HostMonitor and an agent.
- Password:
  here you should provide the same password that you have specified when an agent was installed and configured on a remote system.

After you have finished entering the above information click "Test/Get info" button to check the settings of an agent or click "Ok" button to check the settings and close dialog. HostMonitor will try to establish connection with an agent and get information about an agent: platform, version, comment, etc.
If connection with an agent was established, HostMonitor updates all agent information and sets status of the agent to "operable". If HostMonitor was not able to get proper information from an agent, it sets its` status to "no answer" (if no answer was received from an agent) or "bad answer" (if some error code was received from an agent, e.g. wrong password).

Active RMA

Active RMA – Remote Monitoring Agent that is not waiting for TCP connection from HostMonitor like Passive RMA. Active RMA itself establishes connection with HostMonitor and RMA Manager. This allows you to install RMA inside private network protected by firewall without necessity to open any TCP port (Passive RMA requires 1 open TCP port). Also Active RMA allows you to monitor system that does not have fixed IP address, e.g. system that is connecting to the network using temporary dial-up connection.

There are just 2 obligatory parameters

- Name
  unique name of the agent. You should not assign the same name for several agents. If you do so, HostMonitor will accept connection from the 1st started agent and reject connection from the other agents with the same name
- Password
  minimum six character length password. An empty password using is not permitted.

The password is required for every communication session between RMA and HostMonitor or RMA and RMA Manager. All traffic between RMA and HostMonitor or RMA and RMA Manager is encrypted and the password itself is never transmitted through the network without encryption.
Note: you should use exactly the same name and password that were used when you setup Active RMA on remote system using rma_cfg utility.

Note: Options located on "Active RMA Server" page in the Options dialog allow you to specify TCP port that will be utilized by HostMonitor to listen for incoming connections from Active RMA agents.

Backup agent

Since the version 6.00 HostMonitor allows you to setup primary and backup agents. Using this feature, HostMonitor is able to balance load between agents and use the backup agent when primary one does not respond. Yes, RMA is pretty stable software however system may not respond due to some hardware or network error.

When you have installed second agent you may choose one of the following "Load balancing" options:

- **Backup only**
  In this case, HostMonitor will request the main agent to perform the tests and will switch to backup agent only in case when the primary agent is not responding.
- **50/50**
  With this option selected, HostMonitor will balance requests for service between the agents. Even if you specify a single primary agent for all your tests, some tests will be performed by primary agent and the others by backup RMA. If either primary or the backup agent does not respond, tests will be performed by another (paired) RMA.
- **Redundant check**
  This option available for Passive RMA only. When “Redundant check” mode is selected for 2nd (backup) agent, HostMonitor uses specified agent as “backup” agent as well (this means HostMonitor sends request to backup RMA when cannot establish connection with primary agent). Also HostMonitor sends request to 2nd RMA every time primary RMA returns “bad” test result (e.g. “No answer”, “Unknown host”, “Bad”). This means test can be performed from 2 different locations and “Bad” status will be used when both checks performed by both agents fail. Yes, you can use “master-dependant” test relations for such checks and for other much more complicated schemes. However this option allows you to simplify setup, you need just 1 test item instead of 2 items.
  The following table illustrates how HostMonitor performs test using 2 agents in “Redundant check” mode:

1st RMA result	2nd RMA result	Test status
“Good” status	Not used	“Good” status
“Unknown” status	“Good” status	“Good” status
“Unknown” status	“Unknown” status	“Unknown” status
“Unknown” status	“Bad” status	“Bad” status
“Bad” status	“Bad” status	“Bad” status
“Bad” status	“Unknown” status	“Bad” status
“Bad” status	“Good” status	“Good” status

Note 1: "Primary agent" - the agent that is specified for the test execution. As you may specify different agents for different test items, the same agent can be a "primary" and "backup", depending on the situation. For example, you may use AgentA to perform set of WMI tests and use AgentB to perform SNMP tests. In case of an emergency AgentB may execute WMI tests as well (AgentB is backup agent for AgentA). AgentA may perform SNMP tests in the case of AgentB failing (AgentA is backup agent for AgentB).

Note 2: Options on Misc page in the Options dialog allow you to choose behaviour of the tests when primary agent does not respond. "If backup agent is specified and connection to primary RMA failed" parameter allows you to choose one of the two options:

- Set "Unknown" status, log the error, then repeat test using backup agent
- Request backup agent without reporting error

How to edit connection parameters for the agent

To change connection parameters for an agent, select it from the list and click “Params” button (or just double-click it). "Agent Connection Parameters" dialog will pop up, there you may setup connection parameters (agent address, port, timeout, password, etc) like it was already described in previous abstract ("How to add new agent to the list").

How to obtain information about agent(s)

When you create a new agent record in the list, HostMonitor tries to connect to a specified agent and gets information from it. But you can refresh/reload this information at any time. To retrieve information about single agent, select an agent and click “Get Info” button. To retrieve information about all agents from the list, just click “Get Info (All)” button.
HostMonitor will then try to connect to each agent and gets the following information:

- Agent: an internal name of an agent;
- Platform: OS platform that this agent is designed for;
- Version: the version number of the agent;
- Developer: the company that created RMA software;
- Comment: the content of a comment field that you or system administrator had provided when a remote agent was installed and configured.

If a connection with agent was established, HostMonitor updates all information and sets the status of an agent to "operable". If HostMonitor was not able to get information from an agent, it sets the status to "no answer" (if no answer from an agent was received) or "bad answer" (if some error code was received from an agent, e.g. wrong password).

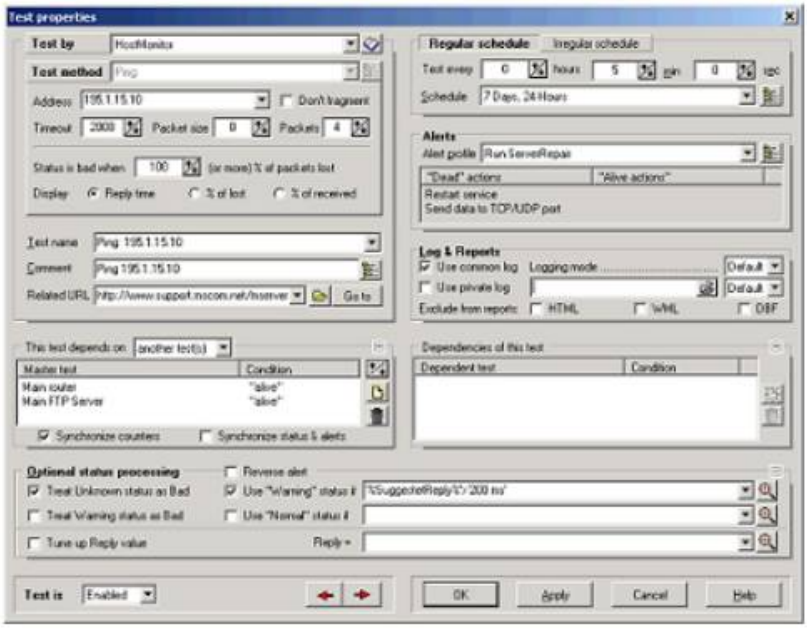
Mark unused
This popup menu item tells HostMonitor to grey out all RMA agents currently not used. HostMonitor checks all folder settings, test settings (within loaded test list), action setting and Network Discovery settings.

RMA Manager

To manage an array of Remote Monitoring Agents you may use RMA Manager utility. It allows you to change settings for hundreds of agents that are installed on remote systems at one time and from one location. Also RMA Manager allows you to reload or terminate agents, force agents to reread settings from their ini files and even upgrade agent's code remotely.
Both RMA Manager and HostMonitor are using the same list of Remote Monitor Agents.

Tests: Common Properties

Test Properties dialog



When you view/edit existing test item you may use hot keys:
Alt+Left and Alt+Right – discard changes and move to previous/next test item;
Shift+ALT+Left - save changes and move to previous test item;
Shift+ALT+Right - save changes and move to next test item

Popup menu items:

- Copy host to clipboard (Ctrl+H)
- Resolve host to IP and copy (Ctrl+I)
- Copy host and IP
- Find record for this host in Connection Manager (Ctrl+Q)

Application checks for appropriate record based on agent, host, and test method. Records for specific host and agent are prioritized; then application checks for records with agent set to "any", for records with IP range; etc. If only default (*) record found or no matched records found, HostMonitor offers to create a new record
if you use the 'Find record for this host in Connection Manager' option and there is no matched record, HostMonitor/RCC will ask which type of record you want to add: an RPC mode entry or a WinRM mode entry.

Most properties are common across all test methods. However, each method has a set of parameters that are specific to the test type. Let's have a look at the common properties first:

Test By

Test can be performed by HostMonitor itself (by default) or by Remote Monitoring Agent. You may select an agent from drop down list or click on a button (to the right of the field) to manage agent list.

Also HostMonitor version 9+ allows you to choose “folder-specific agent” item. In such case HostMonitor will use agent specified for the folder where test item is located. If you move or copy test item from one folder to another, HostMonitor will use agent that was specified for this new parent folder.
Note: you may specify folder-level agent using options located on Specials page in Folder Properties dialog.

Test Name

The name of the test; HostMonitor auto populates this field with a suggested name based on the type and other test parameters; you can change that name to whatever name you want.

Comment

Here you may provide any comments that make sense to you. You can specify one-line comment directly in the Test Properties dialog or press button to bring-up popup dialog for entering multi-line comments. Also Test Properties dialog provides option that allows you to edit comment lines as plain text so you may easily enter large text or copy/paste multiline comment to/from clipboard. Click button to use this option.
Note: in the status bar, in reports, and in the Test Detail Area HostMonitor will display only the 1st comment line. However using macro variables (%TaskComment%, %CommentLine1%, %CommentLine2%, etc) you can access the whole comment or any of its lines.
Note: there is “hidden” option that allows you to change titles for comment lines displayed by “Comment” dialog. You may add line like
AlternativeCommentTitles=address;phone;admin_name;admin_e-mail
into [Misc] section of hostmon.ini file and restart HostMonitor. Then Comments dialog will display “address” instead of %CommentLine1%, “phone” instead of %CommentLine2%, “admin name” instead of %CommentLine3% and so on.

Related URL

For each test, a related URL can be specified. By adding this property to the list of visible columns or to a report, you will make the related URLs appear in the test list view or report sheet. In HTML reports, URLs appear as hyperlinks. In the list view, tests with a related URL will have a popup menu item that launches the associated program (typically, your default Internet browser).
You can customize the Related URL field of a test item with an additional optional hint string. For example **[title=GOOGLE]**https://www.google.com?paramA=1 – this string tells the HostMonitor GUI to display a short title GOOGLE in various menu items, in the reports, etc. When you click on such an item, the URL specified after the title will be used.
- %RelatedURL% variable provides the URL without a hint (https://www.google.com?paramA=1)
- %RelatedURLHint% variable provides only a hint (GOOGLE)

Enabled/Disabled

This option enables or disables test execution.

Schedule

The following parameters specify when HostMonitor should perform the test. There are 3 different ways to setup schedule for the test:

- Regular schedule

- Irregular schedule
- Irregular schedule by expression

A regular schedule assumes the test will be launched at fixed time intervals, for instance, every 10 minutes. In addition, Schedule profile can be associated with a test to give you more control on your monitoring activities. For example, if you want to test your proxy server only from Monday to Friday, select the "Monday-Friday, 24 hours" schedule profile. You may select an existing schedule from a drop-down list or create any number of your own schedules. If you do not select a schedule profile, HostMonitor will check the host every day of the week, 24 hours a day.

With an irregular schedule, you may select one of the following options:
- Start test once a day
- Start test once a week
- Start test once a month

This allows you to perform the test on a given day of a week or a month, at a given time (e.g. every Monday at 9:00 am; or on the 15th of every month at 3:00pm).
Note:"Start test once a month" mode allows you to specify "Last day" option. In such case the test will be performed on the last day of each month.

Irregular schedule by expression
This mode allows you to provide expressions like "May,Sep-Dec Mon#1,Fri#L 06:00,22:00" which tells HostMonitor to perform test on 1st Monday and last Friday in May, September, October, November and December at 06:00 and 22:00.
You may specify 1 or 2 expressions for each test. Test will be performed when any of these expressions allows, for example test can be performed at 08:00 in May and June, at 10:00 in October and November.
Each expression consists of 3 parts: <month> <day> <time>

month — Here you may specify * (which equivalent to Jan-Dec), comma separated list of months or range of months. Valid months names are: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov and Dec

day — Here you may specify * (which means every day of the month), comma separated list of numbers (range of dates) or comma separated list of weekdays (Mon, Tue, Wed, Thu, Fri, Sat and Sun)
E.g.

10,15,25	means 10th, 15th and 25th day of the month
10-15	means from 10th till 15th day of the month
Mon, Fri	means Monday and Friday
Tue-Fri,Sun	means Tuesday, Wednesday, Thursday, Friday and Sunday

Also for weekday lists you may provide optional parameter separated by # sign which specifies number of the week (1,2,3,4,5 or L. 'L' means last week of the month). Note: if you specify #5 and there is not 5 of the given day-of-week in the month, then test will not be performed that month.
E.g.

Mon#1,Fri#L	means 1st Monday of the month and last Friday of the month
Mon,Wed,Sat-Sun#2	means every Monday, every Wednesday, 2nd Saturday and 2nd Sunday of the month

time — Here you may specify comma separated "time of the day" list in hh:mm or *:mm format (* means perform test every hour).
Note: HostMonitor will not perform "irregular" tests more often than once in 5

minutes.

Examples:

* * 10:30	Every day at 10:30
* * *:30	Every day at 00:30, 01:30, 02:30 ... 23:30
* * *:00,*:30	Every hour at 00 and 30 min
* 10-15 00:00	Every midnight from 10th to 15th day of each month
* Wed,Fri 10:30,*:00	Every Wednesday and Friday, every hour at 00 min and 10:30

Jun 5,10,15 20:00
Start test at 20:00 on June 5th, 10th and 15th

Oct,Nov Mon-Fri#2 15:00
Every 2nd Monday-Friday of the month (October and November only) at 15:00

May,Sep-Dec Mon#1,Fri#L 22:00
Start test in May, September, October, November and December every 1st Monday and last Friday of the month at 22:00

Jan,May,Sep Mon,Fri,Sun#1 15:30,17:20
Start test every Monday, every Friday and 1st Sunday of January, May and September at 15:30 and 17:20

Alert profile

Alerts are a highly flexible mechanism that allows you to implement different behaviors for different types of events and conditions. Choose one of the existing Alert Profiles or create a new one, designed specifically to suit your needs.
You can design an alert profile, using different alert methods, such as a visual and sound warning; send an E-mail message to a mailbox, pager or mobile phone; execute an external program, restart service, reboot local or remote computer, dial-up to the network, send data to TCP/UDP port, execute SQL Query, and much more. For more information, please, refer to Action&Action profile section of this documentation.
If you don't select an alert profile, HostMonitor will only write down a record to the log file (if the logging is enabled), and no other action will be taken even if the status of the host changes.

In most cases single alert profile is enough for test item because each alert profile may contain several actions with different starting conditions, different time restriction options; also you may use “advanced mode” actions.
However in some cases you may reduce number of alert profiles by using 2 alert profiles per test item. If you enable "Allow 2nd alert profile for test items" option (located on Preferences page in HostMonitor Options dialog), you will be able to assign 1 or 2 alert profiles for each test item.

Logging options

Use common log

If the "Use common log" option is selected, HostMonitors records test data into a single log file (or database) shared by all tests. Common log settings located on the Log Settings page in the Options dialog.
Choose one of the following options to specify when information should be recorded:

- Default - the default logging mode specified in the Options dialog will be used (note: you may use different settings for Primary and Backup logs);
- Brief - record information whenever status of the test changes;
- Full - record all test results, regardless of whether their status had changed or not;
- Reply - record information into log every time the status or reply value of the test changes.

For more information about different logging options, please, refer to Log&Reports section of this documentation.

Use private log

Additionally, for each test you can define its own, dedicated log file by checking the "Use private log" option. The type of a private log is determined based on the file extension: HTML for .htm*, DBF for .dbf, plain text for any other extension.
Private logs can be configured to work in one of the following modes:

- Default - the Primary log settings defined in the Options dialog are used.
- Brief - record information whenever status of the test changes;
- Full - record all test results, regardless of whether their status had changed or not;
- Reply - record information into log every time the status or reply value of the test changes.

If a private log is specified, the popup menu for that test will contain the item, "View private log". For more information about different logging options, please, refer to Log&Reports section of this documentation.

Exclude from reports

These check boxes allow the user to exclude the test information from reports. For more information about the report customization, please, refer to Report Manager section of this documentation.

Master/Dependent test settings

This test depends on another test(s)

For each test, you can define a list of other tests it depends on, or Master tests. For each Master test you can choose the condition to perform the dependent test based on the status of the Master test:

- "Alive";
- "Alive" or "Unknown";
- "Dead";
- "Dead" or "Unknown".

As an example, consider a network configuration where the accessibility of the company's several web servers depends on the state of a single router. When the router is down, there is probably little sense in trying to do the dozens of tests designed to collect information on the web servers.
That was, of course, a very simplified example. With this feature, you can implement quite sophisticated dependencies involving a number of master tests, which, in turn, depend on the results of other tests. For more information on dependencies, please, see the following options: "Syncronize counters", "Syncronize status & alerts", "Consider status of the master test obsolete after N seconds" (Options dialog).
Note: Using Remote Control Console to edit test properties, it is possible to see 'ID <number>' instead of the name of the master test. This means that the master test is located in the folder you do not have access to. If you need information about this master test, it can be provided by an operator with a higher level of rights.

This test depends on expression

Instead of making test to be dependent on a list of Master tests you can define a condition to perform the test using logical expression.
This mode is more complicated than a standard list of Master tests but it is very flexible. Just several simple examples:

- with expression ('%::Ping Router::SimpleStatus%'=="UP") and ('%::Ping Router::Reply %'<'800 ms') HostMonitor performs a test when the test named "Ping Router" has a good status and the reply time for the router is below 800 ms;
- use expression like ('%::TestA::SimpleStatus%'=='UP') or ('%TestB:: SimpleStatus %'=='UP') to perform a test when either TestA or TestB has "good" status.

Note: There is special button in Test Properties dialog that allows you to bring up "Expression editor" window for convenient expression editing.

OtherwiseStatus
Sometimes HostMonitor may fail to parse logical expressions. For example when a variable has no value due to the failure to perform some other tests. In this case HostMonitor will not perform the dependant test. Instead it will set a special status for the current dependent test. The same happens when a logical expression returns "false" value (this means that a condition was not met). You may define this status in the "OtherwiseStatus" property of the test. You can provide the status name

('Host is alive', 'No answer', 'Unknown', 'Unknown host', 'Ok', 'Bad', or 'Bad contents') or specify a macro variable that describes the status of another test (e.g. %::Ping Router::Status%).
For more information on dependencies, see the following options: "Synchronize counters", "Synchronize status & alerts", "Consider status of the master test obsolete after N seconds" (Options dialog).

Note: HostMonitor stores master-dependant test expressions using unique ID of each test item. When you setup new expression HostMonitor checks for master tests existence, also it allows you to select specific test item in case several test items have the same name. As result you may rename test items without necessity to modify master-dependant expressions.
Note: If you import test items from import text file manually and there is no "DpExprID" parameter specified or there are incorrect test IDs specified in this parameter while "DpExpression" parameter contains non-unique test names, HostMonitor will display dialog that allows you to select specific master test items. If import procedure works without human interaction (e.g. procedure was initiated by "Execute HM Script" action), the same problem (invalid or not specified IDs and non-unique test name) will be resolved by HostMonitor in different way – HostMonitor will use 1st matched test.

Synchronize counters

This option only applies to tests that have one or more master tests. When the option is turned off, and some test is not being launched because its launching condition has not been met, HostMonitors simply marks such a test with the "Wait for Master" status and does not change any counters. If, however, the option is turned on, HostMonitor will update statistics information accordingly to the Master test status. Thus, if a router the other tests depend on has been tested to a "No answer" status, HostMonitor will increment respective counters (like "Dead time", "Failed tests", etc) for router and for all dependent tests with the "Synchronize counters" option on.

Synchronize status & alerts

This option is applicable only if "Synchronize counters" is also selected. When the option is turned on, besides synchronizing counters, the dependent test receives the status of the master test, which in turn will start action dispatching based on the status propagated from the master test.

Example: On your corporate network you have 10 web servers and 1 router that is critical to the entire network. A router Ping test is set up to page the administrator if the router does not respond. So when the router goes down, and the "Synchronize status&alerts" option is turned off, HostMonitor sends a message to the administrator's pager and suspends all dependent tests. If "Synchronize status&alerts" is on, in addition to the router problem notification, actions defined on the dependent tests will be launched as well.

Master does not expire

If this option set for some master test, it overrides global option "Consider status of the master test obsolete after N seconds" located in Options dialog. The option can be useful when master test execution requires significant system resources (e.g. count files on hard drive) and you know conditions checked by such test cannot be changes frequently

Dependencies of this test

This is a read-only list for information purpose. It displays tests that depend on the current test.

Logical expressions:

When you are using "Test depends on expression" option or custom "Normal"/"Warning" statuses, you should provide logical expression.
In the expression you can use:

- numbers and strings (in quotes). Strings that contain a number plus one of the following unit specificators [ms, Kb, Mb, Gb, %] are compared as numbers, so that '900 Kb' is less than '9 Mb' ('900 Kb' is equivalent to 921600)

- macro variables related to the current test or to any other test;
- global macro variables;

- logical operators [and, or, xor, not, <, >, >=, <=, ==, <>];

- arithmetic operators [div, mod, *, +, -]
  div (integer division)
  mod (remainder)
  * (multiplication)
  + (addition)
  - (subtraction)
  Note: The value of (x div y) is the value of x divided by y and then rounded in the direction of zero to the nearest integer; 'mod' operator returns the remainder obtained by dividing its operands (in other words, (x mod y) == x - (x div y) * y);

  Also HostMonitor supports numbers in binary format, such number should contain only 0 and 1 and should be finished with 'B' character, e.g. '1110B' or '00101111B'. You may use the same arithmetic operations that you are using for decimal numbers, plus you may use AND, OR and XOR operators to perform bitwise operations, e.g. ('%Reply%' and '010B')=='010B'.
  When at least one operand of AND/OR/XOR operators specified in binary format, HostMonitor will use binary format for result as well. E.g. (6 and '11111111B') will return '110B'. If you want to convert number in binary format to decimal format, you may use addition (+), subtraction (-) or multiplication operations. E.g. '110B'+0 will return '6'.

- string operators

in	Expression 'Substr' in 'Str' searches for a sub string "Substr" in a string "Str". Operator returns True when "Str" contains "Substr"; otherwise operator returns False
getword	Expression like ("string" getword N) returns Nth word from text string counting from beginning; Example: ('40 10 50' getword 3) == '50' ('50' - third word)
endword	Expression like ("string" endword N) returns Nth word from text string counting from end of the string Example: ('40 10 50' endword 3) == '40' ('40' - 3rd word

	counting from the end of the string)
csvfield	Retrieves field from CSV (comma-separated values) string. ('string' csvfield N) returns field #N. Examples: ('40,10 10,50' csvfield 2) == '10 10' ('"error 5","10,1,2",10,50' csvfield 2) == '10,1,2'
tsvfield	Retrieves field from TSV (tab-separated values) string. Works similar to csvfield command: 'string' tsvfield N returns field #N.
getval	Finds specified XML tag, returns value. Example "<tagAA>value11</tagAA><tagBB>value22</tagBB>" gettagval "tagBB" == "value22"
getnumberwithdot	Usage <string> getnumberwithdot <num> This operator ignores all words within <string> except integer numbers and numbers with the period, returns number #num and then replaces the period character with system decimal separator (so it may replace the period with comma when system decimal separator is the comma). Example ('wordA wordB 21.10,15.00' getnumberwithdot 2)=='15.00' ('wordA wordB 21 15.00' getnumberwithdot 2)=='15.00' ('15.00' will be replaced with '15,00' when system decimal separator is comma)
getnumberwithcomma	Usage <string> getnumberwithcomma <num> This operator ignores all words within <string> except integer numbers and numbers with comma, returns number #num and then replaces comma with system decimal separator (so it may replace comma with the period when system decimal separator is the period). Example ('wordA wordB 21.10,15.00' getnumberwithcomma 2)=='10,15' ('wordA wordB 21 15.00' getnumberwithcomma 2)=='15' ('10,15' will be replaced with '15.10' when system decimal separator is the period)
getnumber	Usage <string> getnumber <num> This operator ignores all words and symbols within <string> except integer numbers, returns number #num ('wordA wordB 21.10,15.00' getnumber 2)=='10' ('wordA wordB 21 15.00' getnumber 2)=='15'
the following operators useful when you need to parse multi-line text where lines separated by CR, LF or CRLF characters	
getlinewith	checks for specified text, returns 1st matched line with this text
getlinestarts	returns 1st line that starts with specified text

getlineends	returns 1st line that ends with specified text

- parentheses
  In complex expressions, common rules of precedence determine the order in which operations are performed:

Operators	Precedence
not	first (highest)
div, mod, *	second
+, -, in	third
<, >, >=, <=, ==, <>	fourth
and, or, xor	fifth (lowest)

  An operator with higher precedence is evaluated before an operator with lower precedence, while operators of equal precedence associate to the left. You can use parentheses to override precedence rules. An expression within parentheses is evaluated first and then its result is treated as a single operand.

Note: There are special buttons in Test Properties dialog that allow you to bring up "Expression editor" window for "Warning", "Normal", and "Tune up Reply" expressions editing.

Optional status processing

When HostMonitor performs checks it may assign one of the following statuses as a result of the test probe:

- Ok, Host is alive – “good” statuses;
- Bad, No answer, Bad contents – “bad” statuses

Also HostMonitor may use “Unknown” and ”Unknown host” statuses when it is impossible to perform the check.

You may specify for each test item additional rules that tell HostMonitor how to process the result. HostMonitor may parse specified logical expressions and set “Warning” or “Normal” status when appropriate expression is True.
Note: HostMonitor checks logical expressions after test check is done and “reverse alert” option is processed.

Statuses by groups

“Good” statuses	“Bad” statuses	“Unknown” statuses	“Inactive” statuses*	User-defined statuses
Host is alive	No answer	Unknown**	Disabled	Warning**
Ok	Bad	Unknown host**	Wait for master	Normal
	Bad contents		Out of schedule	
			Paused	

* “Inactive” statuses indicate that test was not performed for some reason
** ”Warning” and “Unknown” statuses might be processed as “bad” statuses depending on “Treat Unknown status as Bad” and “Treat Warning status as Bad” option
*** When HostMonitor performs the test, it shows temporary status “Checking”

Reverse alert

When this option is selected, HostMonitor regards test results that are normally considered benign, as abnormal ones, and vice versa.
This can be useful in some situations. For example, CPU Usage test returns an "Ok" status if the processor load ratio is below a predefined value. With the "Reverse alert" option turned on, the test will work the other way around, so the administrator will be alerted when the processor load is below a predefined value.

Here is how the conversion works for different status values:

Original status	**Reverse status**
Host is alive	Bad
No answer	Ok
Ok	Bad
Bad	Ok
BadContents	Ok

Other status values are not affected.

Treat Unknown status as Bad

With this option enabled, if test results cannot be obtained, actions are launched by HostMonitor the same way as if the test returned a "Bad" status. Details available below

The option is not applicable to some of the test types. Please refer to the table below for the meaning of "Unknown" status for different test types:

Test	Option is applicable *	"Unknown" status condition
Ping	Yes	Host name cannot be resolved into IP address
Trace	Yes	Host name cannot be resolved into IP address
URL request	No	
HTTP	Yes	Host name cannot be resolved into IP address
TCP	Yes	Host name cannot be resolved into IP address
UDP	Yes	Host name cannot be resolved into IP address
NTP	Yes	Host name cannot be resolved into IP address
SMTP	Yes	Host name cannot be resolved into IP address
POP3	Yes	Host name cannot be resolved into IP address
IMAP	Yes	Host name cannot be resolved into IP address
Mail Relay	Yes	Host name cannot be resolved into IP address
DNS	Yes	Host name cannot be resolved into IP address
DHCP	Yes	Host name cannot be resolved into IP address
LDAP	Yes	Host name cannot be resolved into IP address
RADIUS	Yes	Host name cannot be resolved into IP address
DICOM	Yes	Host name cannot be resolved into IP address
RAS	Yes	Connection was not established because of a problem on local system, e.g. modem is used by another application
UNC	Yes	Resource is unavailable (option is applicable for free space check only)
Disk free space	Yes	Disk drive information is unavailable (e.g. removable disk ejected or target system inaccessible)
Folder/File size	Yes	File/folder doesn't exist
Count Files	Yes	Folder doesn’t exist
File/Folder Availability	Yes	Target server rejects connection, e.g. wrong username or password rejected by FTP server
Compare files	Yes	Target file(s) does not exist
File Integrity	Yes	File doesn't exist or read error
Text Log	Yes	File doesn't exist or read error
Database	No	
ODBC Query	Yes	SQL query fails, or the data field specified is not found in the result set
Process	Yes	Information (list of processes) cannot be retrieved
Service	Yes	Connection to CS Manager cannot be established
SNMP Get	Yes	Information cannot be retrieved
SNMP Trap	Yes	Ambiguous configuration. Trap fits both ("good" and "bad")

		filters
NT Events Log	Yes	Information cannot be retrieved
CPU Usage	Yes	Information cannot be retrieved
Memory	Yes	Information cannot be retrieved
Performance Counter	Yes	Information cannot be retrieved
WMI	Yes	Information cannot be retrieved
Dominant Process	Yes	Information cannot be retrieved
External test	Yes	HostMonitor cannot execute external program (program doesn't exist) or program doesn't return ERRORLEVEL within a specified time
Active Script	Yes	Script returns "Unknown" status, or an error occurred during the script execution
Shell Script	Yes	Script returns "Unknown" status, or an error occurred during the script execution
Temperature Monitor	Yes	Information cannot be retrieved
Traffic Monitor	Yes	Information cannot be retrieved
HM Monitor	Yes	Host name cannot be resolved into IP address

* This option is applicable for any test performed by Remote Monitoring Agent because the test may return "Unknown" status in case of RMA failure.

Use Normal status

You may mark this option and provide logical expression to specify when HostMonitor should use “Normal” status for the test item.
“Normal” status is processed similar to other “good” statuses – “Ok” and “Host is alive”. When HostMonitor sets “Normal“ status, it increases “Alive” statistics counters and executes specified “good” actions. When test status changes from “Ok” to “Normal” or vice versa, HostMonitor does not reset “Recurrences” counter. The only difference between Normal and Ok (or “Host is alive”) status is that you may use different colors for Normal and Ok statuses and sort test items by status so “Normal” items will be located below (or above) of “Ok” and “Host is alive” items. You may setup specific colors for Normal items to be used by HostMonitor/RCC GUI, HTML reports, HTML log files, charts and Web interface.

IMPORTANT: HostMonitor checks logical expressions after test check is done and “reverse alert” option is processed.
I.e.

- HostMonitor performs the test;
- processes "Reverse alert" option;
- sets “suggested” macro variables (%SuggestedStatus%, %SuggestedSimpleStatus%, %SuggestedReply%, %SuggestedRecurrences% and %FailureIteration%) without touching regular counters (%Status%, %Reply%, %Recurrences%, etc);
- then HostMonitor checks "Warning" and "Normal" expressions, processes “Tune up Reply” option and finally modifies current test status and statistisc counters (Status, Reply, Alive%, Passed tests, Failed tests, etc).

Use Warning status / Treat Warning Status as Bad

You may mark "Use Warning status" option and provide logical expression to specify when HostMonitor should use "Warning" status for the test item.
Note: HostMonitor checks logical expressions after test check is done and "reverse alert" option is processed.
Behaviour of this status is more complicated, it depends on additional option - "Treat Warning status as Bad". "Warning" status is processed by HostMonitor similar to "Unknown" status, therefore "Treat Warning status as Bad" option works similar to "Treat Unknown status as Bad" option that is used for Unknown test status.

- "Treat Unknown status as Bad" and "Treat Warning status as Bad" **do NOT** have an influence on the following features:
  - Statistics: unknown test status always increments "unknown" statistics counters; warning status always increments "bad" counters (Dead time, Failed tests, Dead ratio, etc)
  - Test color: "unknown" and "warning" test items always use their own specific colors, independently on "Treat Warning status as Bad" or "Treat Unknown status as Bad" option
  - Folder color: HostMonitor draws folder using color specified for Warning items when folder does not contain any unacknowledged (new) "bad" test but contains some unacknowledged (new) Warning item(s). In other words: "bad" items have top priority, while "warning" items have higher priority than "unknown" items.
  - Logging: HostMonitor always records event when test status changes (Bad -> Bad Contents -> Warning -> No answer -> Host is alive...) unless logging is disabled
  - Reports: you may use separate filter items and different colors for each status (bad, unknown, warning)
  - Dashboard reports: HostMonitor uses color specified for Warning items when folder does not contain any unacknowledged (new) "bad" test but contains some unacknowledged (new) Warning item(s). In other words: "bad" items have top priority, while "warning" items have higher priority than "unknown" items.
  - Macro variables: statistical variables (%HM_WarningItems%, %HM_AckWarningtems%, %HM_UnknownItems%, etc) provide information about bad/unknown/warning test items regardless of "Treat Unknown/Warning status as Bad" options
  - HMScript: _AllWarning and _AllUnknown parameters may be used instead of name of the test (e.g. if you need to disable all test items in Warning status)
  - Master-dependent test relations: HostMonitor treat Warning status just like other "Bad" statuses (Bad, Bad Content, No answer)

- "Treat Unknown status as Bad" and "Treat Warning status as Bad" options **do HAVE** an influence on the following features:
  - Tray icon: when the option is disabled, "unknown"/"warning" test item will trigger yellow icon (unless there are "red" test items already in the list); enabled "Treat * status as Bad" option tells HostMonitor to use red icon color when test status changes to "unknown"/"warning"
  - %SimpleStatus% macro variable returns "WARNING" string for Warning test items when "Treat Warning as Bad" option is disabled; otherwise it returns "DOWN" string. The variable returns "UNKNOWN" and "DOWN" for Unknown tests accordingly.
  - Actions: most important - these options define HostMonitor's behavior when test status changes.

If options are disabled, HostMonitor will reset recurrences counter for each status change (bad <-> unknown <-> warning). Also, if options are disabled, HostMonitor will not start standard actions for "Unknown" and/or "Warning" statuses (however you may use advanced actions). As a result this leads to reset of Acknowledged flag, so if you acknowledge Warning status and then status of the test changes to Bad, HostMonitor clears ACK flag and starts specified "bad" actions. Therefore you may need to acknowledge test status again.
If options are enabled, HostMonitor treats "bad", "unknown" and "warning" as the same status and will not reset "recurrences" counter, will not clear ACK flag either but will start standard actions for "Unknown" and/or "Warning" statuses.

Why you may need Warning/Normal statuses?

- Example #1: You are monitoring CPU Usage on set of servers. You setup alert threshold (condition that tells HostMonitor when it should use "bad" status and start "bad" alerts) to 80% however you want to separate servers with CPU usage over 50% (and below 80%). So, you may mark "Use Normal status" option and provide expression like `('%SuggestedSimpleStatus%'=='UP') and ('%SuggestedReply%'>'50 %')`. This allows you to show CPU Usage test items with CPU load between 50% and 80% using different color/sorting mode.

- Example #2: You are monitoring free disk space on set of servers. You setup alert threshold (when HostMonitor should use "bad" status and start "bad" alerts) to 1 GB however you want to be warned when free space is below 3 GB. So, you may mark "Use Warning status" option and provide expression like `('%SuggestedSimpleStatus%'=='UP') and ('%SuggestedReply%'<'3 Gb')`. If you do not mark "Treat Warning status as Bad", HostMonitor will change test status from "Ok" to "Warning" and reset "recurrences" counter when free disk space falls below 3 GB (also HostMonitor may start "advanced" mode actions, e.g. send e-mail to IT staff). You may acknowledge Warning status for such test items.
  Later if disk free space falls below 1 GB, HostMonitor will change test status from Warning to Bad, reset Recurrences counter again, clear Acknowledged flag and start specified "bad" alerts (e.g. send e-mail or page admin). So you will be able to acknowledge "Bad" status now.
  This also allows you to generate different reports for "bad" and "warning" servers, and HostMonitor will use different colors for folders that contain "bad" or "warning" items.

- Example #3: You need to monitor a device that works unreliably – often changes its status from "good" to "bad" and vice versa and you want to be alerted when the device definitely is "dead", not just lost network connection for a minute. Then you may enable "Treat Warning status as Bad", mark "Use Warning status" option and use expression like `('%SuggestedSimpleStatus%'=='DOWN') and (%SuggestedRecurrences%<4)`. In such case HostMonitor will use Warning status for initial 3 failed probes and change status to Bad after 4th failed check.
  Similarly you may enable "Use Normal status" option and use expression like `('%SuggestedSimpleStatus%'=='UP') and (%SuggestedRecurrences%<4)`
  Note 1: You need to enable "Treat Warning status as Bad" option to avoid reset of "recurrences" counter.
  Note 2: Most likely you will use "Start when 4 consecutive Bad results occur" option for the actions assigned to such test item.

- Example #4: you may configure HostMonitor to use Normal status for 1st and 2nd failed probes, use Warning status for 3rd and 4th failed probes and set Bad status starting from 5th failed check:
  - enable “Use Warning" status” option and provide `(%FailureIteration% > 2) and (%FailureIteration% < 5)` expression
  - enable “Use Normal status” option and use expression like `(%FailureIteration% > 0) and (%FailureIteration% < 3)`

You could setup “advanced” alerts (actions) to use similar alerting scheme since version 4.0. HostMonitor 6.50 allows you to setup visual distinction between such test items: different colors, different reports, etc.

Tune up Reply

"Tune up Reply value" option was implemented in HostMonitor version 7.06. This test property allows you to specify expression that tells HostMonitor how to recalculate (modify) Reply value of the test item after each probe. HostMonitor checks “Tune up Reply” expression after test probe is done and "reverse alert" option is processed.
I.e.

- HostMonitor performs the test;
- processes "Reverse alert" option;
- sets "suggested" macro variables (%SuggestedStatus%, %SuggestedSimpleStatus%, **%SuggestedReply%**, %SuggestedRecurrences% and %FailureIteration%) without touching regular counters (%Status%, %Reply%, %Recurrences%, etc);
- then HostMonitor evaluates "Warning", "Normal" and “Tune up Reply” expressions and finally modifies current test status, reply field and statistics counters (Status, Reply, Alive%, Passed tests, Failed tests, etc).

“Tune up Reply” expression may contain regular text, macro variables and arithmetical expressions. Each arithmetical expression should be concluded into square brackets, e.g. “tune up Reply” expression [%SuggestedReply% div 1024 div 1024] Mb tells HostMonitor to divide result of the test by 1048576 (1024*1024) and add Mb suffix to the result. It can be useful when you need to convert bytes to Megabytes, e.g. some WMI requests return high values in bytes. BTW: [%SuggestedReply% div 1024 div 1024] is equivalent to [%SuggestedReply% div 1048576]

You may use several arithmetical expressions in “Tune up Reply” field. E.g. [%SuggestedReply% div 3600] hours [(%SuggestedReply% mod 3600) div 60] min [%SuggestedReply% mod 60] seconds

In these arithmetical expressions you can use:

- numbers and strings (in quotes). Strings that contain a number plus one of the following unit specificators [ms, Kb, Mb, Gb, %] are compared as numbers, so that '900 Kb' is equivalent to 921600

- macro variables related to the current test or to any other test;

- global macro variables;

- the following arithmetical operators:
  div (integer division)
  mod (remainder)
  * (multiplication)
  + (addition)
  - (subtraction)
  and (bitwise and)
  or (bitwise or)
  xor (bitwise xor)
  Note: the value of (x div y) is the value of x divided by y and then rounded towards zero to the nearest integer; 'mod' operator returns the remainder obtained by dividing its operands (in other words, (x mod y) == x - (x div y) * y);
  Also HostMonitor supports numbers in binary format, such number should contain only 0 and 1 and should be finished with 'B' character, e.g. '1110B' or '00101111B'. You may use the same arithmetic operations that you are using for decimal numbers, plus you may use AND, OR and XOR operators to perform bitwise operations, e.g. ('%SuggestedReply%' and '010B')=='010B'.
  When at least one operand of AND/OR/XOR operators specified in binary format, HostMonitor will use binary format for result as well. E.g. (6 and '11111111B') will return '110B'. If you want to convert number in binary format to decimal format, you may use addition (+), subtraction (-) or multiplication operations. E.g. '110B'+0 will return '6'.
  Note: HostMonitor always use decimal format for statistics, charts, etc.

- string operators

getword	Expression like ('string' getword N) returns Nth word from text string counting from beginning; Example: ('40 10 50' getword 3) returns '50'
endword	Expression like ("string" endword N) returns Nth word from text string counting from end of the string Example: ('40 10 50' endword 3) returns '40'
csvfield	Retrieves field from CSV (comma-separated values) string. ('string' csvfield N) returns field #N. Examples: ('40,10 10,50' csvfield 2) returns '10 10' ('"error 5","10,1,2",10,50' csvfield 2) returns '10,1,2'
tsvfield	Retrieves field from TSV (tab-separated values) string. Works similar to csvfield command: ('string' tsvfield N) returns field #N.
gettagval	Finds specified XML tag, returns tag value. Example "<tagAA>value11</tagAA><tagBB>value22</tagBB>" gettagval "tagBB" == "value22"
getnumberwithdot	Usage <string> getnumberwithdot <num>

	This operator ignores all words and characters within <string> except integer numbers and numbers with the period, returns number #num and then replaces the period character with system decimal separator (so it may replace the period with comma when system decimal separator is the comma). Example ('wordA wordB 21.10,15.00' getnumberwithdot 2)=='15.00' ('wordA wordB 21 15.00' getnumberwithdot 2)=='15.00' ('15.00' will be replaced with '15,00' when system decimal separator is comma)
getnumberwithcomma	Usage <string> getnumberwithcomma <num> This operator ignores all words and characters within <string> except integer numbers and numbers with comma, returns number #num and then replaces comma with system decimal separator (so it may replace comma with the period when system decimal separator is the period). Example ('wordA wordB 21.10,15.00' getnumberwithcomma 2)=='10,15' ('wordA wordB 21 15.00' getnumberwithcomma 2)=='15' ('10,15' will be replaced with '15.10' when system decimal separator is the period)
getnumber	Usage <string> getnumber <num> This operator ignores all words and symbols within <string> except integer numbers, returns number #num ('wordA wordB 21.10,15.00' getnumber 2)=='10' ('wordA wordB 21 15.00' getnumber 2)=='15'
the following operators useful when you need to parse multi-line text where lines separated by CR, LF or CRLF characters	
getlinewith	checks for specified text, returns 1st matched line with this text
getlinestarts	returns 1st line that starts with specified text
getlineends	returns 1st line that ends with specified text

- string functions

substr('str',start,length)	The substr method extracts the characters from a string (str), beginning at "start" and through the specified number of characters (length), and returns the new sub string. First character is at index 1. To extract characters from the end of the string, use a negative start number.
replace('str','oldsubstr','newsubstr')	Method replaces a specified part (oldsubstr) of a string (str) with another string (newsubstr) and returns new (modified) string.

indexof('str','substr')	Method returns the position of the first occurrence of a substring (substr) in a string (str). Note: First character is at index 1. If Substr is not found, indexof returns zero.
lastindexof('str','substr')	Method returns the position of the last found occurrence of a substring (substr) in a string (str). The string is searched backward, but the index returned is the character position from left to right (starting at 1). If Substr is not found, lastindexof returns zero.

- parentheses.
  In complex expressions, common rules of precedence determine the order in which operations are performed:

Operators	Precedence
div, mod, *	first (highest)
+, -	second
and, or, xor	third

An operator with higher precedence is evaluated before an operator with lower precedence, while operators of equal precedence associate to the left. You can use parentheses to override precedence rules. An expression within parentheses is evaluated first and then its result is treated as a single operand.

If/else statements

HostMonitor version 8.64+ allows you to use "if…else" statements for "Tune up Reply" expression.
When you use "if" statement, expression for "Tune up Reply" option may look like the following samples

If (condition) reply_expresion
This is the simplest form of the statement. Condition is logical expression. If condition is True, HostMonitor sets Reply field using reply_expresion. Otherwise Reply field will be empty.
Example:

```
If ('%SuggestedReply%'>100) ['%SuggestedReply%'-100]
```

If (condition) reply_expresion; else reply_expression2
If condition is True, HostMonitor sets Reply field using reply_expression. Otherwise Reply field will be modified according to reply_expression2.
Example:

```
If (('%SuggestedReply%'>40) and ('%SuggestedReply%'<60)) 50; else ['%SuggestedReply%']
```

If (condition) reply_expresion; If (condition2) reply_expresion2; else reply_expression3
If condition is True, HostMonitor sets Reply field using reply_expression. Otherwise HostMonitor checks condition2; if condition2 is True, HostMonitor sets Reply field using reply_expression2; otherwise Reply field will be modified according to reply_expression3.
Example:

```
if ('%SuggestedReply%'<12) Low voltage; if ('%SuggestedReply%'>15) High voltage; else
[%SuggestedReply%]
```

Formal definition:

```
if (condition1) replyexpr1 [; if (condition2) replyexpr2 [; if …] | [; else replyexpr3]] | [; else replyexpr4]
```

Some basic rules:

- if/if, if/else statements should be separated by semicolon (;)
- if logical expression (condition) is True, HostMonitor sets Reply field value and does not continue evaluation of the following expressions (if any)
- if condition is False and next statement is "else" statement, HostMonitor sets Reply field using expression specified in “else” statement and does not continue evaluation
- if condition is False and next statement is "if" statement, HostMonitor continues evaluation by checking next condition
- if logical expression (condition) is invalid (e.g. there are some missed brackets), HostMonitor considers condition as False

Test Methods

Listed below are the various test methods supported by HostMonitor, along with the description of their method-specific parameters

LAN

Ping
Trace
TCP
UDP
NTP
DNS
DHCP
LDAP
RADIUS
DICOM
SIP
RAS

Web

URL
HTTP
SOAP/XML
OPC
Certificate expiration
Domain expration
WebDAV Free Space
Apache
NGINX
Tomcat

SNMP

SNMP Get
SNMP Trap
SNMP Table
Traffic Monitor
Interfaces status

Database

Database Server
ODBC Query

Windows

Drive Free Space
HDD SMART
CPU Usage
Memory
Service
Process
Dominant Process
WMI
Performance Counter
NT Events Log
Registry
Firewall status
DHCP Pool
Antivirus status
Windows updates

VMWare / Hyper-V

VM host status
VM host CPU usage
VM host free memory
VM host free datastore space

VM guest status
VM guest CPU usage
VM guest free memory
VM guest free disk space

Mail

SMTP
POP3
IMAP
E-Mail
Mail Relay

Other

Temperature Monitor
HM Monitor

UNIX
Drive Free Space
CPU Usage
Memory
Process
Shell Script
SSH

IPMI
RMCP Ping
IPMI Health
IPMI Temperature
IPMI Fans
IPMI Voltage
IPMI Current
IPMI Discrete

Cisco
Cisco Health
Cisco Temp
Cisco Fans
Cisco Power
Cisco CPU Usage
Cisco Memory

Juniper
Juniper Health
Juniper Temp
Juniper Fans
Juniper CPU Usage
Juniper Memory

QNAP
QNAP Health
QNAP Temp
QNAP Fans
QNAP Free Space
QNAP CPU Usage
QNAP Memory

Synology
Synology Health
Synology Temp
Synology Disk Load
Synology Free Space
Synology CPU Usage
Synology Memory

Files
UNC
Folder/File Size
Count Files
Folder/File Availability
File Integrity
Compare Files
Text Log

HP
HP iLO Health
HP iLO Temp
HP iLO Fans
HP iLO Power
HP iLO Disks

F5 Big-IP
Big-IP Health
Big-IP Temperature
Big-IP Statistics
Big-IP Free Space
Big-IP CPU Usage
Big-IP Memory

Citrix Netscaler
Netscaler Temperature
Netscaler Statistics
Netscaler CPU Usage
Netscaler Memory

NetApp
NetApp Health
NetApp CPU Usage
NetApp Temperature
NetApp RAID status
NetApp Free Space

UPS
UPS Health
UPS Load
UPS Charge level
UPS Input voltage
UPS Output voltage
UPS Temperature
UPS Remaining time

Redfish
Redfish Health
Redfish Temperature
Redfish Fans
Redfish Voltage
Redfish Current
Redfish Power
Redfish Sensor

Printers
Printer Status
Printer Levels

Custom
Active Script
Shell Script
External
SSH

Ping

The ping command verifies connections to remote computers, routers and other network components by sending ICMP (Internet Control Message Protocol) echo packets to the remote component and listening for echo reply packets. It's best to use the Ping method to check a remote connection in general. To check specific services and conditions, HostMonitor provides a number of special test types.
In addition to the common test parameters, the Ping test has the following options:

Address
Here you should provide the domain name (e. g. www.yahoo.com) or IP address (e. g. 204.71.200.68) of the host that you wish to monitor. Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) and specify hostname with suffixes ::ipv4 or ::ipv6 (e.g. www.google.com::ipv4 or www.6bone.net::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.
Note: on Windows NT 4.0, Windows 2000 and Windows XP SP1 IPv6 protocol is not supported. You may use menu Tools -> Local Info to check is your system IPv6 ready.
Also, a range of IPv4 addresses (e.g. 10.10.1.100 – 10.10.1.254) rather than a single address can be specified. In this case, HostMonitor will create a separate test for each of the addresses within that range.

Timeout
Specify a timeout interval in milliseconds.

Packet size
Specify the size of ECHO packets. This parameter is optional. If its value is 0 (default value), HostMonitor will use global Packet Size parameter specified on Ping/Trace page in the Options dialog.

Packets
Specify the number of ECHO packets.

Don't fragment
This option tells HostMonitor to set "Do Not Fragment" bit on the ping packet.

Time to Live
Time to Live parameter is common for all Ping tests; specify this parameters on Ping/Trace page in the Options dialog.

Alert if loss ratio N% or more
A packet loss threshold can be specified for a Ping test, based on which the test status is determined.

Alert if Jitter over N ms
Jitter - amount of variation in response time, calculated by using the following formula Jitter = SquareRoot(SumOf((ReplyTime[i] - AverageReply)^2) / (ReceivedPacketCount-1))
(when this option enabled, HostMonitor will send at least 3 ICMP packets)

Display mode
Tells HostMonitor what kind of data should be displayed in the Reply field:

- Reply time - the "Reply" field will represent average reply time
- % of lost - display percentage of lost packets,
- % of received - display percentage of received packets.
- Jitter - amount of variation in response time

Note: Test Info window may show Loss ratio and Jitter in addition to selected "reply" value

HostMonitor may set 6 statuses for Ping tests:

"Ok"	this status used when Jitter" option is enabled and Jitter time within specified limit (when "Alert if lost ratio" option enabled, it should be within specified limit as well)
"Host is alive"	this status used when "Jitter" option was not enabled and loss ratio within specified limit
"Bad"	this status means either Jitter or Loss ratio is out of the limits
"No answer"	HostMonitor sets "no answer" status when does not receive any response from target system
"Unknown host"	host name could not be resolved to IP address
"Unknown"	test performed by Remote Monitoring Agent and there is some RMA related error (e.g. HostMonitor cannot connect to the agent)

Trace

Traces the route to a remote host over the network. This test allows you to check the route that all packets take to go from your machine to a specific host on the Internet (Intranel, LAN). It also can check the time each hop (or each machine packets go through) takes to answer.
In addition to the common test parameters, the Trace test has the following options:

Address
Here you should provide the domain name (e. g. www.yahoo.com) or IP address (e. g. 204.71.200.68) of the host route that you want to test. Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) and specify hostname with suffixes ::ipv4 or ::ipv6 (e.g. www.google.com::ipv4 or www.6bone.net::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.
Note: on Windows NT 4.0, Windows 2000 and Windows XP SP1 IPv6 protocol is not supported. You may use menu Tools -> Local Info to check is your system IPv6 ready.

Timeout
Specify a timeout interval in milliseconds.

Packet size
Specify the size of ECHO packets in bytes.

Retries
Specify how many times HostMonitor will try to resend ECHO packets when it does not receive the respond.

Alert when
Choose one of the conditions to determine whether route is “good” or “bad”:

- route was changed	HostMonitor will mark test as “Bad” every time route changed
- number of hops different from NN	Test will change status to “Bad” if number of hops is different from specified
- number of hops greater than NN	Test will change status to “Bad” if number of hops is greater than specified
- number of hops less than NN	Test will change status to “Bad” if number of hops is less than specified
- maximum reply time more than NN milliseconds	Mark test as “Bad” when reply time from any of the hosts is longer than specified
- traffic thru the host	HostMonitor will mark test as “Bad” every time traffic will go thru specified intermediate host
- traffic bypass host	HostMonitor will mark test as “Bad” every time traffic will not go thru specified intermediate host

Display
This option determines the kind of information HostMonitor will display in Reply field. Choose one of the following options:

- Total time
- Average reply time
- Maximum reply time
- Number of hops
- Number of non-responding devices
- Route, brief mode (list of IP addresses only)
- Route, full mode (hop, IP address, time)

See also: variables specific to Trace test

URL

HostMonitor can perform a URL (Universal Resource Locator) check based on the HTTP (web), HTTPS (secure web), FTP or Gopher protocols. To perform URL check HostMonitor can connect to a remote server directly or through a proxy server, this proxy server can be defined on the PROXY page in the Options dialog.
In addition to the common test parameters, the URL test has the following options:

Basic parameters:

URL
Enter the URL you want to monitor. HostMonitor is not limited to the retrieval of HTML files for the HTTP and HTTPS checking, it can also retrieve other types of pages, even CGI scripts.
Examples of URLs include:
- http://www.yahoo.com/index.html
- https://www.super.secure.server.gov:444/unpublished/mainpage.html
- ftp://ftp.bhs.com/incoming/list.txt

Translate date macro variables
This option allows you to use date & time variables in the "URL" and "Post data" field. It is useful when you have to monitor web pages that are created on regular basis. E.g. such URL may look like "http://www.sql.company.com/logs/**%mm%-%dd%-%yyyy%**.html".

Password protected page
Use this option when the URL specified requires a name and password for access.
User name
If the URL specified requires a name and password for access, enter the user name in this box.
Password
If the URL specified requires a name and password for access, enter the password in this box.

Special parameters:

Optional headers
You may specify optional HTTP headers which will be added to the request. For example you can define cookies using string like "Cookie: name1=value1; name2=value2; name3=value3". When you send data to the server using POST method, HostMonitor automatically inserts "Content-Type: application/x-www-form-urlencoded" header.

HTTP POST request
POST requests send data (defined in "Post data" field) to the web server to be processed in some way, like by a CGI script. In this case URL is not a resource to retrieve; it's usually a program to handle the data you are sending. The HTTP response is normally the program output, not a static file. The most common use of POST is to submit HTML form data to CGI scripts. In this case, the "Content-Type:" header should be set to "application/x-www-form-urlencoded". So, when you

choose “HTTP POST request” option, HostMonitor adds this header into "Optional headers" field by default.-

Use client certificate
An HTTPS server may require client authentication, in which case a local client certificate should be sent to the server for authentication. Client certificates contain information that identifies the user, as well as information about the organization that issued the certificate.
”Use client certificate” option allows you to choose certificate that will be sent to the server. If test is performed directly by HostMonitor, application will show list of certificates installed on local system. If URL test is performed by Remote Monitoring Agent (RMA), HostMonitor will request specified RMA to retrieve list of certificates installed on system where agent is running.

Advanced options:

FTP: Passive mode
In this mode HostMonitor uses passive FTP semantics (option available for FTP checks only) which might be required in order to work properly with some firewalls.

HTTP/HTTPS: Code 302 (redirect) is Ok
This parameter determines the HostMonitor's behavior, when HTTP/HTTPS server issues a redirect. If option disabled and HTTP server returns code 301 (Moved Permanently) or 302 (Moved Temporarily), HostMonitor marks test as "Bad". With this option enabled HostMonitor sets "Host is alive" status.

HTTPS: Ignore unknown certificate authority problems
This option allows checking web servers that use HTTPS protocol and security certificates that were issued by not trusted company. With this option enabled, HostMonitor will accept security certificates issued by any company. When this option is disabled and the certificate belongs to non-trusted company then HostMonitor will set the test status to "no answer".

HTTPS: Accept certificates with invalid host name
This option tells HostMonitor to accept SSL/PCT-based certificate even if certificate was issued to a different host

HTTPS: Accept certificates with invalid dates
This option tells HostMonitor to accept expired SSL/PCT-based certificates
By default these options are greyed out, this means HostMonitor should use global options specified on Misc page in the Options dialog. If you mark or unmark test options, these settings will override global options (for this specific test item only).

Check contents

HostMonitor can search for a string (or several strings) in the returned page and start alert actions when string exists (or doesn't exist) on the page. Define string(s) and condition to alert using following options:

Mode
This option determines condition to check. Choose one of the available modes:

- should contain HostMonitor will set "Bad contents" status when page does not contain specified string
(may check multiline text, CR and LF replaced with space character, CRLF replaced with 2 space chars)

- should not contain HostMonitor will set "Bad contents" status when page contains specified string
(may check multiline text, CR and LF replaced with space character, CRLF replaced with 2 space chars)

- use expression HostMonitor will consider the string as boolean (logical) expression, evaluate expression using data received from the server, and set "Bad contents" status when retrieved page does not satisfy the required conditions.
For example: if you define expression like "'No errors' and not ('Error' or 'Warning')", then HostMonitor will mark test as "Host is alive" when retrieved page contains string 'No error' and does not contain either 'Error' or 'Warning'

Expression
Enter a string of text to check the returned page. Remember that HTML tags are part of a document, so include the HTML tags if they are part of the text you are searching for (for example, "<B>Hello</B> World").
If you chose "use expression" mode, you may use expressions like "("Total" and "End Of Page") and not ('Error' or 'Warning')". In this case, a test will have a "Host is alive" status when monitor can receive specified page and this page contains both strings "Total" and "End Of Page", and doesn't contain either strings "Error" or "Warning". In the expression you may use strings (must be put in quotes (') or in double quotes ("")); round brackets; logical operators "and", "or", "not".

Translate date macro variables
This option allows you to use date & time variables in the search string. It is useful when you have to monitor web pages that shall be updated regularly. E.g. if you provide "%mm%-%dd%-%yyyy%" in the search string, HostMonitor will check the retrieved document for the presence of a current date and will set "Bad content" status for the documents without current date stamp. This could be useful for testing various scripts and applications that generate web pages.

Case sensitive
With this option enabled search is case sensitive

Whole words only
Searches are for words only. With this option disabled, the search string might be found within longer words.

The URL test doesn't automatically retrieve any objects linked from the page. You can, however, instruct HostMonitor to retrieve the nested frames and images.

Download nested frames
Select this box if you want to retrieve all frames referenced in a frameset and count their retrieval time in the total time to download this page. If "Download images" is also checked, HostMonitor will attempt to retrieve all images in all frames. In case the program successfully retrieve page specified in the URL field but cannot receive one of the nested frames, HostMonitor will mark test as "Bad contents".
Note: if src parameter of the frame/iframe tag set to "about:blank" and there is "data-lazy-src" option, then HostMonitor checks URL specified in "data-lazy-src" parameter (there is no such parameter in HTML specifications but its often used by JS code).

Download images
Enable this option if you want the status and response time statistics to include the retrieval time for all of the embedded images in the page. Embedded images include those referenced by <IMG> HTML tags. Images that appear more than once in a page are only retrieved once. In case the program successfully retrieves the page specified in the URL field but cannot receive one of images, HostMonitor will mark test as "Bad contents".

Check digest

Compute and check digest for entire page
With this option enabled HostMonitor will compute CRC, MD5 or SHA digest of the downloaded data and do a comparison each subsequent time test is performed. If the hash changes, the test will have "Bad contents" status.
If "Download nested frames" and/or "Download images" options are enabled, HostMonitor will compute digest for the nested frames and/or images as well.

Compute and check digest within the following tags
This option allows you to specify some important parts of the document and check digest only for these parts. E.g. check digest for HTML code between <table and </table> sections
If "Download nested frames" and/or "Download images" options are enabled, HostMonitor will compute digest for the nested frames and/or images as well.

Digest mode
CRC32
MD5
SHA256
SHA512
Use MD5, SHA256 or SHA512 when you need to check for unauthorized file modifications (SHA256 or SHA512 is preferred).
CRC32 can be used for legitimate modifications monitoring.

Recalculate checksum when page content changes detected

With this option enabled, the new CRC or digest will be recorded as the default in case the error "page content changed" occurs, so the test will return to "Good" status until the digest changes again.

Note: some server-based scripts can check agent's name and return different information for different HTTP agents (e.g. generate different HTML pages for Internet Explorer or Netscape). To get correct test results you may need to change "Agent name" parameter. Use Miscellaneous page in the Options dialog for this purpose.

See also: variables specific to URL, HTTP, SOAP and SIP tests

HTTP

The HTTP test provides you with the ability to monitor HTTP based servers, verify the content of dynamically generated pages, check for the changed content. Also it can help you verify that CGI scripts and back-end databases are functioning properly.
In contrast to URL test, that can perform HTTP request as well, HTTP test does not use wininet.dll (part of Internet Explorer). In this way we can avoid any problems related to IE's bugs (of course we can make mistakes as well but we are always able to correct our own mistakes :-).
Also using HTTP test you can define more parameters specific to HTTP protocol and setup more varied checks.
In addition to the common test parameters, the HTTP test has the following options:

HTTP request parameters:

URL
Enter the URL you want to monitor (for example, http://www.ourbiggestserver.com)

Proxy
Optionally, a proxy server can be used to access the URL. Select a proxy server from the drop down list or choose "<none>" to perform direct request to HTTP server.
You can open Proxies List dialog to modify the list of proxy servers. For each item from the proxy list you can specify:
- Domain name or IP address of the HTTP proxy server
- TCP port
- User name
- Password

Request
Choose type of HTTP request:

- HEADER request for HTTP header. Server will return status information about the document (HTTP header) but will not transfer data. It allows you to check web server functionality with minimum network traffic but you cannot check the content of the web page.

- GET request the page specified by URL parameter. Server will return status information (HTTP header) and data. You can use "Check content" and "Check CRC" options to monitor contents of the page.

- POST send data (defined in "Post data" field) to the web server to be processed in some way, like by a CGI script. In this case URL is not a resource to retrieve; it's usually a program to handle the data you are sending. The HTTP response is normally the program output, not a static file. The most common use of POST is to submit HTML form data to CGI scripts. In this case, the "Content-Type:" header is usually set to "application/x-www-form-urlencoded". So, when you choose POST request, HostMonitor adds this header into "Optional headers" field by default. However you can change that header to another one or remove it.

Follow redirect
This parameter determines the HostMonitor's behavior, when the server issues a redirect. When the option enabled HostMonitor follows redirect and retrieve URL specified by server. If option disabled and HTTP server returns code 301 (Moved Permanently) or 302 (Moved Temporarily), HostMonitor marks test as "Bad".

Post data
If the URL is for a POST request, enter the post variables as name1=value1&name2=value2. This option is used to verify that a form is working correctly by performing the same request that occurs when a user submits a form. See also the "Check content" option for a way to verify that the correct form response was received.

Authorization
Use this option when the URL specified requires a name and password for access
User name
If the URL specified requires a name and password for access, enter the user name in this box.
Password
If the URL specified requires a name and password for access, enter the password in this box.
HostMonitor supports basic and NTLM authentication methods.

Agent
Some server-based scripts can check agent's name and return different information for different HTTP agents (e.g. generate different HTML pages for Internet Explorer or Netscape). You can change this parameter to get correct results.

Timeout
Specify the number of seconds that the test should wait for a page to complete downloading before timing-out. Once this time period is over, the monitor will mark test as "No answer". If you have checked the "Download nested frames" or "Download images" option, HostMonitor will use the same timeout for all frames/images referenced on the page.
If the Timeout property is set to 0 (default value), HostMonitor will use default Windows timeout specified for TCP protocol.

Allow per-session cookies
With this option enabled HostMonitor remembers cookies received from the server, and sends them back in case of redirection to another URL.
This option can be useful when you need to check some access-restricted resources. Often web-based authorization systems use cookies to identify user. How it usually works:

- user opens login page, enters login and password, and clicks "Login" button;
- browser sends POST or GET request to a server with data entered by user;
- server checks login/password and (in case data are correct) assings session ID for the user;
- server sends cookie that contains ID to user's browser, and redirects user to another page;
- browser must store cookie and send it back to server every time it (browser) requests access-restricted pages

So, now HostMonitor can work like your browser and login to your mailbox to check whether you have the new messages. See also the "Check content" option for a way to verify that the correct response was received.

Optional headers
Specify optional HTTP headers those will be added to request. For example you can define cookies using string like "Cookie: name1=value1; name2=value2; name3=value3". When you send data to the server using POST method, HostMonitor automatically insert "Content-Type: application/x-www-form-urlencoded" header.

Optional test parameters:

The HTTP test doesn't automatically retrieve any objects linked from the page. You can, however, instruct HostMonitor to retrieve the nested frames and images.

Download nested frames
Select this box if you want to retrieve all frames referenced in a frameset and count their retrieval time in the total time to download this page. If "Download images" is also checked, HostMonitor will attempt to retrieve all images in all frames. In case the program successfully retrieve page specified in the URL field but cannot receive one of the nested frames, HostMonitor will mark test as "Bad contents".

Download images
Enable this option if you want the status and response time statistics to include the retrieval time for all of the embedded images on the page. Embedded images include those referenced by <IMG> HTML tags. Images that appear more than once on a page are only retrieved once. In case the program successfully retrieves the page specified in the URL field but cannot receive one of the images, HostMonitor will mark test as "Bad contents".

Check CRC
With this option enabled HostMonitor will save CRC (Cyclical Redundancy Check) of the downloaded data and do a checksum comparison each subsequent time test is performed. If the checksum changes, the test will have "Bad contents" status.
By default HostMonitor calculates (and checks) CRC for page specified in the URL. But if "Download nested frames" and/or "Download images" options are enabled, HostMonitor will calculate CRC for the nested frames and/or images as well.

Recalculate CRC when page content changes detected
With this option enabled, the new checksum will be recorded as the default in case the error "page content changed" occurs, so the test will return to "Good" status until the checksum changes again.

Check header
HostMonitor can search for a string (or several strings) in the HTML header (received from a server) and start alert actions when the string exists (or doesn't exist) in the header. Define string(s) and condition to alert using following options:
Mode
This option determines condition to check. Choose one of the available modes:

- should contain	HostMonitor will set “Bad contents” status when HTTP header does not contain specified string
- should not contain	HostMonitor will set “Bad contents” status when HTTP header contains specified string
- use expression	HostMonitor will consider the string as boolean (logical) expression, evaluate expression using data received from the server, and set “Bad contents” status when retrieved HTTP header does not satisfy the required conditions. Example if you define expression like “’HTTP/1.1’ and not (‘301’ or ‘302’)”, then HostMonitor will mark test as “Host is alive” when retrieved data contains string ‘HTTP/1.1’ and contains neither ‘301’ nor ‘302’.

Expression

Enter a string to check the returned HTTP header. If you chose “use expression” mode, you may use expressions like "(‘HTTP/1.1’ or ‘HTTP/1.0’) and not ('301' or '302')". In this case, a test will have a “Host is alive” status when monitor gets reply from the server and retrieved HTTP header contains either strings "HTTP/1.1" or "HTTP/1.0", and doesn't contain either strings "301" or "302". In the expression you may use strings (must be put in quotes (‘) or in double quotes (“)); round brackets; logical operators **and**, **or**, **not**.

Case sensitive

With this option enabled search is case sensitive

Whole words only

Searches are for words only. With this option disabled, the search string might be found within longer words.

Check contents

HostMonitor can search for a string (or several strings) in the returned page and start alert actions when string exists (or doesn’t exist) on the page. Define string(s) and condition to alert using following options:

Mode

This option determines condition to check. Choose one of the available modes:

- should contain	HostMonitor will set “Bad contents” status when page does not contain specified string (may check multiline text, CR and LF replaced with space character, CRLF replaced with 2 space chars)
- should not contain	HostMonitor will set “Bad contents” status when page contains specified string (may check multiline text, CR and LF replaced with space character, CRLF replaced with 2 space chars)
- use expression	HostMonitor will consider the string as boolean (logical) expression, evaluate expression using data received from the server, and set “Bad contents” status when retrieved page does not satisfy the required conditions.

	For example if you define expression like "'No errors' and not ('Error' or 'Warning')", then HostMonitor will mark test as "Host is alive" when retrieved page contains string 'No error' and does not contain either 'Error' or 'Warning'

Expression
Enter a string of text to check the returned page. Remember that HTML tags are part of a document, so include the HTML tags if they are part of the text you are searching for (for example, "<B>Hello</B> World").
If you chose "use expression" mode, you may use expressions like "("Total" and "End Of Page") and not ('Error' or 'Warning')". In this case, a test will have a "Host is alive" status when monitor can receive specified page and this page contains both strings "Total" and "End Of Page", and doesn't contain either strings "Error" or "Warning". In the expression you may use strings (must be put in quotes (') or in double quotes ("")); round brackets; logical operators **and**, **or**, **not**.
Translate date macro variables
This option allows you to use date & time variables in the search string. It is useful when you have to monitor web pages that shall be updated regularly. E.g. if you provide "%mm%-%dd%-%yyyy%" in the search string, HostMonitor will check the retrieved document for the presence of a current date and will set "Bad content" status for the documents without current date stamp. This could be useful for testing various scripts and applications that generate web pages.
Case sensitive
With this option enabled search is case sensitive
Whole words only
Searches are for words only. With this option disabled, the search string might be found within longer words.

Set "Bad" status when total download time is longer than NN msec
With this option enabled HostMonitor will check total download time and mark status as "Bad" when download time is longer than specified.

BTW: When HostMonitor cannot retrieve page at all, it marks test as "No answer" and Reply value will be empty. In case all checks passed, HostMonitor mark status as "Host is alive" and display total download time in the "Reply" field. Also "Reply" field will display total download time when any reply received from HTTP server, even if its message about error such as "Page not found" error.

See also: variables specific to URL, HTTP, SOAP and SIP tests

SOAP/XML

SOAP is a protocol specification for exchanging structured information in the implementation of Web Services. It relies on Extensible Markup Language (XML) for its message format, and usually relies on Hypertext Transfer Protocol (HTTP) or Simple Mail Transfer Protocol (SMTP) for message negotiation and transmission.
As an example, a SOAP message could be sent to a web service such as a market price database, with the parameters needed for a search. Then the site would return an XML-formatted document with the resulting data, e.g., prices, location, options.

This test method allows performing SOAP requests version 1.1 and 1.2 over HTTP and HTTPS protocols. HostMonitor supports GET and POST requests, client and server side certificates; optional HTTP headers can be specified as well.
If you need to check XML data delivered by SMTP protocol and retrieved over POP3 or IMAP protocol, you may use E-Mail test method.

In addition to the common test parameters, the SOAP/XML test has the following options:

URL
Enter the URL where you want to send SOAP request

Translate date macro variables
This option allows you to use date & time variables in the "URL" field. E.g. such URL may look like "http://www.hostname.com/engine/service.asmx?**%mm%-%dd%-%yyyy%**"

Request
Choose type of HTTP request:

- **GET** use this method when target web server supports GET requests for specified URL; additional parameters can be specified as part of the URL
- **POST** use this method when target web server supports POST requests for specified URL. In such case additional parameters of the request (SOAP envelope) should be specified in "Parameters" field

Parameters
Normally when you perform POST request, you should specify SOAP Envelope using this field. It may contain parameters of the request in SOAP Body.
Sample:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<SOAP-ENV:Envelope
 xmlns:SOAP-ENV="http://www.w3.org/2003/05/soap-envelope"
 xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
 xmlns:tm="http://microsoft.com/wsdl/mime/textMatching/"
 xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
 xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/"
 xmlns:tns="http://www.mathertel.de/CalcFactors/"
 xmlns:s="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xmlns:xsd="http://www.w3.org/2001/XMLSchema" >
<SOAP-ENV:Body>
<tns:AddDouble xmlns:tns="http://www.mathertel.de/CalcFactors/">
 <tns:number1>55.22</tns:number1>
```

```
  <tns:number2>65.71</tns:number2>
 </tns:AddDouble>
 </SOAP-ENV:Body>
 </SOAP-ENV:Envelope>
```

There are several buttons located beside “Parameters” field, they help you to create empty SOAP envelope, validate envelope, etc

- Create new SOAP envelope
- Add parameter
- Check SOAP envelope

SOAP version

Here you may select SOAP version 1.1 or version 1.2.
If you select SOAP version 1.1, please do not forget to specify SOAPAction in “Optional headers” field.

Optional headers

Specify optional HTTP headers those will be added to the request. For example you can define cookies using string like “Cookie: name1=value1; name2=value2; name3=value3”.
Also, you should use this field to specify SOAPAction when SOAP version 1.1 is selected.
Note: when you send data to the server using POST method, HostMonitor automatically inserts “Content-Type: application/soap+xml” or “Content-Type: text/xml” header.

Password protected page

Use this option when the server requires a name and password for access.

User name

When authentication is required, enter the user name in this box.

Password

When authentication is required, enter the password in this box.

Advanced options:

HTTP/HTTPS: Code 302 (redirect) is Ok

This parameter determines the HostMonitor's behavior, when HTTP/HTTPS server issues a redirect. If option disabled and HTTP server returns code 301 (Moved Permanently) or 302 (Moved Temporarily), HostMonitor marks test as "Bad". With this option enabled HostMonitor can follow redirected URL.

HTTPS: Ignore unknown certificate authority problems

This option allows checking web servers that use HTTPS protocol and security certificates that were issued by not trusted company. With this option enabled, HostMonitor will accept security certificates issued by any company. When this option is disabled and the certificate belongs to non-trusted company then HostMonitor will set the test status to "No answer".

HTTPS: Accept certificates with invalid host name

This option tells HostMonitor to accept SSL/PCT-based certificate even if certificate was issued to a different host

HTTPS: Accept certificates with invalid dates
This option tells HostMonitor to accept expired SSL/PCT-based certificates
By default these options are greyed out, this means HostMonitor uses global options specified on Misc page in the Options dialog. If you mark or unmark test options, these settings will override global options (for this specific test item only).

Use client certificate
An HTTPS server may require client authentication, in which case a local client certificate should be sent to the server for authentication. Client certificates contain information that identifies the user, as well as information about the organization that issued the certificate.
"Use client certificate" option allows you to choose certificate that will be sent to the server. If test is performed directly by HostMonitor, application will show list of certificates installed on local system. If test is performed by Remote Monitoring Agent (RMA), HostMonitor will request specified RMA to retrieve list of certificates installed on system where agent is running.

Timeout
You may specify the number of seconds that the test should wait for a page to complete downloading before timing-out. Once this time period is over, the monitor will mark test as "No answer".
If the Timeout property is set to 0 (default value), HostMonitor will use default Windows timeout specified for TCP protocol.

Check mode

After you setup request parameters, you should tell HostMonitor how it should check data retrieved from the server
- Check CRC. This is simple CRC check.
- Check content as text. In this mode HostMonitor can search for a string within retrieved data and start alerts when string exists (or doesn't exist) on the page.
- Check XML value. Using this mode you may specify XPath that allows you to select some structures within retrieved data and specify additional conditions to check result set.

Check XML value
Using this mode you may specify XPath that allows you to select some structures within retrieved data and specify additional conditions to check result set. You may check row count, check data in 1st row, check any row or every row, check average value or sum of all values. E.g. you may setup HostMonitor to select all <temperature> fields and set Bad test status when value of any of such fields is over 50.

XPath
XPath (XML Path Language) is a query language for selecting nodes from an XML document. by a variety of criteria. Before checking "alert" conditions HostMonitor may process specified XPath, this allows you to setup very flexible queries.
Examples

/farm/server/drive[last()]	Selects the last "drive" element that is the child of the "server" element that in turn is child of the "farm" element
/farm/server/cpu[temperature>80]	Selects all "cpu" elements (child of the "server" element

	that in turn is child of the “farm” element) that have a temperature element with a value greater than 80
//drive[@type=’fixed’]	Selects all “drive” elements that have an attribute named “type” with a value of “fixed”

Alert when

This option specifies when exactly retrieved value(s) should be considered as “bad” and appropriate alert actions should be started. There are 3 parameters should be provided: aggregation mode, compare mode and compare value.

1) Aggregation mode. Specifies how HostMonitor should compare result data when query returns several rows. Choose one of the following option:

Row count	Tells HostMonitor to calculate row count and compare number of the rows to the specified number
1st row	Tells HostMonitor to check only 1st retrieved counter. If the counter matches specified compare condition, HostMonitor will set “Bad” test status.
Any row	Tells HostMonitor to check each retrieved counter. If ANY counter matches specified compare condition, HostMonitor will set “Bad” test status.
Every row	Tells HostMonitor to check all retrieved counters. If EVERY counter matches specified compare condition, HostMonitor will set “Bad” test status.
Average	Tells HostMonitor to calculate average value of the counters and compare calculated average value to the specified number.
Sum/Total	Tells HostMonitor to calculate sum of the counters and then compare total value to the specified number.

Notes:

- If there is single counter in result set then “1st row”, “Any”, “Every”, “Average” and “Total” modes are equivalent (except “Average” and “Total” do not compare value to a string).
- You may use Average and Total mode only with numeric data

2) Compare mode

HostMonitor compares calculated value with a specified number or string. The following compare modes are supported:

- less than the specified number
- greater than the specified number
- equal to the specified value (number or string)
- different from the specified value (number or string)
- contains the specified string
- doesn't contain the specified string

Display:

- detected value
- response time

This option tells HostMonitor what value should be displayed in Reply field of the test item

Check content as text

HostMonitor can search for a string (or several strings) within retrieved data and set “bad” test status when string exists (or doesn’t exist) on the page. Define string(s) and condition to alert using following options:

Mode

This option determines condition to check. Choose one of the available modes:

should contain	HostMonitor will set “Bad contents” status when retrieved page does not contain specified string
should not contain	HostMonitor will set “Bad contents” status when retrieved page contains specified string
use expression	HostMonitor will consider the string as boolean (logical) expression, evaluate expression using data received from the server, and set “Bad contents” status when retrieved page does not satisfy the required conditions. For example if you define expression like ("<Price>" and "<Index>") and not (“Error” or “Warning”), then HostMonitor will set “Host is alive” status when monitor can receive specified page and this page contains both strings "<Price>" and "<Index>", and doesn't contain either strings "Error" or "Warning". In the expression you may use strings (must be put in quotes (‘) or in double quotes (“)); round brackets; logical operators **and**, **or**, **not**.

Options:

Case sensitive	With this option enabled search is case sensitive
Whole words only	Searches are for words only. With this option disabled, the search string might be found within longer words.
Translate macros	This option allows you to use date & time variables in the search string. It is useful when you have to monitor data that shall be updated regularly. E.g. if you provide “%mm%-%dd%-%yyyyy%” in the search string, HostMonitor will check the retrieved document for the presence of a current date and will set “Bad content” status for the documents without current date stamp.

Check CRC

With this option selected HostMonitor will save CRC (Cyclical Redundancy Check) of the received data and do a checksum comparison each subsequent time test is performed. If the checksum changes, the test will have "Bad contents" status.

Recalculate CRC when page content changes detected

With this option enabled, the new checksum will be recorded as the default every time “Bad content” error occurs, so the test will return to “Good” status until the checksum changes again.

Get CRC button allows you to retrieve and save CRC before performing test.

See also: variables specific to URL, HTTP, SOAP and SIP tests

OPC

The OPC UA standard is a series of specifications developed by industry vendors, end-users and software developers. These specifications define the interface between Clients and Servers, including access to real-time data, monitoring of alarms and events, access to historical data and other application.
This test method allows performing OPC requests over HTTP and HTTPS protocols. HostMonitor supports client and server side certificates; optional HTTP headers can be specified as well.
Note: HostMonitor does not support OPC requests based on Microsoft DCOM that exposes vulnerabilities at Enterprise layers.

In addition to the common test parameters, the OPC test has the following options:

URL
Enter the URL where you want to send OPC request

Timeout
You may specify the number of seconds that the test should wait for a page to complete downloading before timing-out. Once this time period is over, the monitor will mark test as “No answer”.

Optional headers
Specify optional HTTP headers those will be added to the request. For example you can define cookies using string like “Cookie: name1=value1; name2=value2; name3=value3”.

Advanced options:

HTTP/HTTPS: Code 302 (redirect) is Ok
This parameter determines the HostMonitor's behavior, when HTTP/HTTPS server issues a redirect. If option disabled and HTTP server returns code 301 (Moved Permanently) or 302 (Moved Temporarily), HostMonitor marks test as "Bad". With this option enabled HostMonitor can follow redirected URL.

HTTPS: Ignore unknown certificate authority problems
This option allows checking web servers that use HTTPS protocol and security certificates that were issued by not trusted company. With this option enabled, HostMonitor will accept security certificates issued by any company. When this option is disabled and the certificate belongs to non-trusted company then HostMonitor will set the test status to "No answer".

HTTPS: Accept certificates with invalid host name
This option tells HostMonitor to accept SSL/PCT-based certificate even if certificate was issued to a different host

HTTPS: Accept certificates with invalid dates
This option tells HostMonitor to accept expired SSL/PCT-based certificates

By default these elements are greyed out, this means HostMonitor uses global options specified on Misc page in the Options dialog. If you mark or unmark test options, these settings will override global options (for this specific test item only).

Password protected page
Use this option when the server requires a name and password for access.
Login/password
When authentication is required, provide the user name and the password

Use client certificate
An HTTPS server may require client authentication, in which case a local client certificate should be sent to the server for authentication. Client certificates contain information that identifies the user, as well as information about the organization that issued the certificate.
"Use client certificate" option allows you to choose certificate that will be sent to the server. If test is performed directly by HostMonitor, application will show list of certificates installed on local system. If test is performed by Remote Monitoring Agent (RMA), HostMonitor will request specified RMA to retrieve list of certificates installed on system where agent is running.

Check result

After you setup request parameters, you should tell HostMonitor what exactly data should be checked and specify conditions to check result set.

Item
Specify item name that should be verified by HostMonitor, e.g. Factory5/Unit1/TemperatureValue

Alert when
The following options specify when exactly retrieved value(s) should be considered as "bad" and appropriate alert actions should be started: aggregation mode, compare mode and compare value.

Aggregation mode. Specifies how HostMonitor should compare result data when query returns several rows. Choose one of the following option:

Row count	Tells HostMonitor to calculate row count and compare number of the rows to the specified number
1st row	Tells HostMonitor to check only 1st retrieved counter. If the counter matches specified compare condition, HostMonitor will set "Bad" test status.
Any row	Tells HostMonitor to check each retrieved counter. If ANY counter matches specified compare condition, HostMonitor will set "Bad" test status.
Every row	Tells HostMonitor to check all retrieved counters. If EVERY counter matches specified compare condition, HostMonitor will set "Bad" test status.
Average	Tells HostMonitor to calculate average value of the counters and compare calculated average value to the specified number.
Sum/Total	Tells HostMonitor to calculate sum of the counters and then compare total

	value to the specified number.

Notes:

- If there is single counter in result set then "1st row", "Any", "Every", "Average" and "Total" modes are equivalent (except "Average" and "Total" do not compare value to a string).
- You may use Average and Total mode only with numeric data

Compare mode

HostMonitor compares calculated value with a specified number or string. The following compare modes are supported:

- less than the specified number
- greater than the specified number
- equal to the specified value (number or string)
- different from the specified value (number or string)
- contains the specified string
- doesn't contain the specified string

Certificate expiration

This test allows you to check SSL certificate expiration date and start alerts when certificate expires within specified number of days.
Basically this test designed for HTTPS servers however it may work with any server that supports implicit mode. In other words test will work with some SMTP, POP3, IMAP servers but not with all of them.
In addition to common test parameters, for this test you should specify the following options:

Host
Provide hostname or IP address of the server you want to check (e.g. www.gmail.com). Also you can specify the target as IP/hostname in order to test servers behind the load balancer.

Port
Specify port used by the server for incoming connections (HTTPS servers usually use TCP port 443)

Timeout
This is the amount of time in seconds the program will wait for a response from the server before the request fails.

Use StartTLS
This option allows to check SMTP servers that work in Explicit mode

Alert when certificate expires in less than N days
Alert when certificate expires in more than N days
You may mark one of both of these options. HostMonitor will check certificate expiration date and set “Bad” test status when expiration date is out of specified range.

There are some variables specific to Certificate Expiration test, you may use these variables as parameters of actions assigned to such test items.

Domain expiration

This test allows you to check domain expiration date and start alerts when domain registration expires within specified number of days.
In addition to common test parameters, for this test you should specify the following options:

WhoIs server
Provide hostname or IP address of WhoIs server that maintains records for domain you want to check (e.g. whois.internic.net)

Please note: unfortunately there is no strict format for information provided by WhoIs servers; different servers provide data using different formats; some servers do not provide necessary information at all. We tested HostMonitor with over 100 different WhoIs servers however it may not work with your "favorite" WhoIs server (in such case HostMonitor will set Unknown test status and display error message in Reply field of the test, e.g. "Cannot find expiration date").
If you experience such problem, please send request to support@ks-soft.net and we will try to adapt HostMonitor for your needs.

Port
Specify port used by WhoIs server for incoming connections (normally WhoIs server use port 43)

Timeout
This is the amount of time in seconds the program will wait for a response from the server before the request fails.

Alert when domain … expires within N days
Here you should provide domain name and threshould for alert. HostMonitor will set Bad test status when registration for specified domain expires within N days

There are some variables specific to Domain Expiration test, you may use these variables as parameters of actions assigned to such test items.

WebDAV Free Space

Web Distributed Authoring and Versioning (WebDAV) protocol provides a framework for users to create, change and move documents on a server (WebDAV modules available for Apache HTTP Server, Microsoft's IIS and other web servers).
WebDAV servers are frequently deployed with quota (size) limitations. This test method checks amount (or percentage) of free space and may trigger alerts when free space falls below specified limit.
In addition to common test parameters, WebDAV Free Space test has the following options:

URL
Provide HTTP or HTTPS URL to target resouce.

Optional header
Here you may specify optional HTTP headers which will be added to the request.

Login/password
If target server requires authentication, specify login name and password in these fields.

Alert if free space less than <N> MB / GB / TB / %
Specify threshold value. HostMonitor will set Bad test status and trigger actions assigned to the test when amount of free space falls below this limit.

Apache

Apache HTTP Server is a free and open source web server for UNIX and Windows platforms. Apache is the most widely used web server, it can be customized to meet the needs of many different environments by using extensions and modules.
In addition to the common test parameters, Apache test has the following options:

Status URL
Provide HTTP or HTTPS URL to machine-readable version of the status page supported by Apache `mod_status` module. E.g.
`http://apache5.domain.com/server-status?auto`
`mod_status` module can be disabled by default, you should enable the module and set ExtendedStatus On using Apache config file (httpd.conf). Also you may specify which hosts or users can access the page. Apache documentation

Username / password
If status page requires authentication, provide the username and the password

Alert when <parameter> above X or below Y
Choose parameter to check and set upper and lower limits. HostMonitor will set Bad test status and trigger specified actions when parameter value will be out of the range.

Connections/sec (average since last test)	Average connections/sec (CPS) ratio Spikes in CPS can indicate increased customer activity or a DDoS attack. Drops in CPS, on the other hand, can be signs of network connectivity issues or saturation of an essential system resource. A good way to configure Apache test limits is by first determining what the baseline traffic of your application is and then setting alerts around it, so HostMonitor will set Bad test status and trigger specified actions when the stats are significantly higher (indicating a sudden traffic spike) or if the values drop significantly (indicating an issue that blocks traffic somewhere).
Bytes/sec (average since last test)	Average traffic This metric measures the amount of data being transferred in and out of the server. It can be used as an indicator of server performance, relative to constraints such as network infrastructure.
Busy workers	The number of worker threads/processes serving requests Apache has several process models. The most common one is worker processes running idle waiting for service requests. As more requests come in, more workers are launched to handle them, up to a preconfigured limit. Once past that limit all requests are queued and clients experience service delays.
Idle workers	The number of idle worker threads/processes If you consistently see a large number of idle workers, you may want to

	lower your MinSpareServers (for the prefork MPM) or MinSpareThreads (for the worker and event MPMs) setting so that you are not sustaining a higher number of processes or threads than necessary to process your rate of traffic. Maintaining more processes or threads than you actually need will unnecessarily exhaust system resources. If, on the other hand, you have very few idle workers at all times, you may see slower request processing times because your server continually needs to spawn new processes or threads to handle new requests, rather than making use of the idle threads or processes already on hand. If you see the total number of workers (busy + idle) approaching your MaxRequestWorkers limit, any additional requests that come in will end up in the TCP ListenBacklog (which has a maximum size of ListenBacklog), until the next worker thread becomes available. Increasing MaxRequestWorkers can help reduce the number of queued requests, but do not to set it unnecessarily high, as each additional worker thread or process requires additional system resources.

Also you may setup additional tests: URL or HTTP test, Domain Expiration, Certificate Expiration, Network traffic, CPU Usage, Memory, Drive Free Space.

Memory

Memory is very important resource to monitor when using Apache. If Apache runs out of memory, system will start swapping to disk, which greatly degrades performance. To guard against memory leakage (which is particularly important if you use mod_php), you may set `MaxConnectionsPerChild` to a high value (e.g. 1000) rather than leaving it unbounded (set to 0, means that processes will never be forced to restart). If you choose to set this directive, please make sure not to set it too low, because restarting processes carries some overhead.

CPU Usage

The more connections Apache needs to serve, the more threads or processes are created (depending on the MPM in use), each of which requires additional CPU. If you see continually high CPU usage on your Apache server, this can indicate that you don't have enough resources to serve the current rate of requests. If you are running a database and/or application server on the same host as Apache, you may consider moving them onto separate machines. This gives you more flexibility to scale each service.

Drive Free Space

Even if the web server is not physically storing files on the host machine, space is required for logging, temporary files, and other supporting files.

NGINX

NGINX is high performance HTTP and reverse proxy server. HostMonitor can monitor various parameters: requests/sec (RPS) or connections/sec (CPS) ratio, check for non-handled (dropped) connections, check HTTP error responses ratio and more. HostMonitor may check open source NGINX and commercial NGINX Plus servers.
In addition to the common test parameters, NGINX test has the following options:

Status URL
Provide URL to page containing the current activity data. E.g.
https://nginx.domain1.com/status
https://test.nginx.server1.com/status/format/json
https://demo.nginx.com/api/3/http/caches

HostMonitor may check NGINX servers using several modules:

1) ngx_http_stub_status_module – standard NGINX module, provides access to basic status information. It can be enabled with the `--with-http_stub_status_module` configuration parameter. If you setup NGINX test using Status URL pointing to basic status web page, HostMonitor will be able to check the following parameters:
- Connections/sec
- Requests/sec
- Non handled ratio
- Non handled count
- Current connections
- Busy(active) connections
- Waiting(idle) connections

2) **nginx-module-vts** (VTS) open source module (https://github.com/vozlt/nginx-module-vts)
If you are using this module, Status URL should point to JSON document containing the current activity data, e.g.
```
https://test.nginx.server1.com/status/format/json
https://test.nginx.server1.com/status/control?
cmd=status&group=server&zone=::main
```
HostMonitor can to check the following parameters:
- Connections/sec
- Requests/sec
- Non handled ratio
- Non handled count
- Current connections
- Busy(active) connections
- Waiting(idle) connections
- 1xx error responses ratio
- 3xx error responses ratio
- 4xx error responses ratio
- 5xx error responses ratio

- Total error responses ratio

3) NGINX Plus (up to R14 version)
If you are using commercial NGINX Plus, point Status URL to JSON document containing the current activity data (e.g. `https://nginx.domain1.com/status`)
This way HostMonitor will be able to check all above parameters; also it will be able to check Cache hit ratio, SSL fails ratio, Health check results.

4) NGINX Plus R14+
If you are using commercial NGINX Plus version R14 or higher, then Rest API requires different URLs depending on parameters you need to check. HostMonitor knows how to make Rest API calls and it may modify URL accordingly to test settings however you need to specify correct basic URL pointing to the correct location (the same location you specified in NGINX config file),
e.g. if you setup NGINX using location /api directive then use URL like
http://demo.nginx.com/**api**/3
Then depending on "alert when" option, HostMonitor may use requests like
http://demo.nginx.com/**api**/3/ssl
http://demo.nginx.com/**api**/3/connections
http://demo.nginx.com/**api**/3/http/caches
http://demo.nginx.com/**api**/3/http/server_zones
etc
Note: In order to collect data from virtual servers, upstream server groups, or cache zones, you need to configure your NGINX server: enable shared memory zones for the objects you want to collect data for. A shared memory zone stores configuration and run-time state information referenced by NGINX worker processes.
https://docs.nginx.com/nginx/admin-guide/monitoring/live-activity-monitoring/#using-the-rest-api

Username / password
If status page requires authentication, provide the username and the password

Zone/server
When you set the test to check error responses ratio, you may specify server or upstream zone. if you keep this field empty, HostMonitor will check average error responses ratio among all available zones.

Alert when <parameter> above X or below Y
Choose parameter to check and set upper and lower limits. HostMonitor will set Bad test status and trigger specified actions when parameter value will be out of the range.

The following parameters can be checked when you are using any status module: stub_status, VTS or NGINX Plus	
Connections/sec (average since last test)	Average connections/sec ratio since last test probe. Spikes in CPS can indicate increased customer activity or a DDoS attack. Drops in CPS, on the other hand, can be signs of network connectivity issues or saturation of an essential system resource.

	Note: we think its better to check Requests/sec parameter (RPS)
Requests/sec (average since last test)	Average requests/sec ratio since last test probe Spikes in RPS can indicate increased customer activity or a DDoS attack. A spike can also be connected to errors from upstream servers. Drops in RPS, on the other hand, can be signs of network connectivity issues or saturation of an essential system resource like CPU or RAM.
Non handled ratio (since last test)	Non-handled/Total connections ratio (%) Ideally value of this counter should be zero, meaning you don't have dropped connections. If this number rises, look out for resource saturation.
Non handled count (since last test)	Number of non handled connections Ideally value of this counter should be zero, meaning you don't have dropped connections. If this number rises, look out for resource saturation.
Current connections	The current number of client connections *Current = active (stub_status or VTS module)* *Current = active+idle (when NGINX Plus used)* There is configurable hard limit on the total number of connections that nginx can handle, the limit is equal to the number of worker_connections*worker_processes in your nginx configuration) Once the limit is reached, connections will be dropped and users will see errors. Note: this limit includes all connections, from clients to nginx and from nginx to to upstream servers.
Busy(active) connections	The current number of active client connections If stub_status or VTS modules used, this parameter shows number of connections in reading and writing state. *Busy = reading+writing (stub_status or VTS module)* *Busy = active (NGINX Plus)*
Waiting(idle) connections	The current number of idle client connections waiting for a request.
The following parameters can be checked when you are using VTS module or NGINX Plus (stub_status module does not provide necessary information)	

1xx error responses ratio (average since last test)	1xx_codes / total_HTTP_responses ratio (%) Use this mode to trigger alerts if the fraction of 1xx responses rises above a threshold.
3xx error responses ratio (average since last test)	3xx_codes / total_HTTP_responses ratio (%) Use this mode to trigger alerts if the fraction of 3xx responses rises above a threshold (3xx class of status code indicates the client must take additional action to complete the request).
4xx error responses ratio (average since last test)	4xx_codes / total_HTTP_responses ratio (%) Use this mode to trigger alerts if the fraction of 4xx responses rises above a threshold. In theory, a 4xx response is the user's fault, not the fault of the server (e.g. unauthorized access or wrong URL request). However, if many users are suddenly requesting missing pages, there's a good chance it's due to some changes on server side.
5xx error responses ratio (average since last test)	5xx_codes / total_HTTP_responses ratio (%) Use this mode to trigger alerts if the fraction of 5xx responses rises above a threshold (5xx class of status code indicated the server failed to fulfill a request). The appropriate threshold is very depending on the nature of your web site, so you'll have to look at historical data to set an appropriate threshold. If this rate is climbing, that's probably worth investigating. And if it's a sharp increase, that's going to need urgent attention.
Total error responses ratio (average since last test)	All_responses(except_2xx) / total_HTTP_responses ratio (%)
The following parameters can be checked when you are using NGINX Plus	
Cache hit ratio (average since last test)	# of responses read from the cache / # of all responses ratio (%) HostMonitor checks the following counters: hit - The total number of valid responses read from the cache. stale - The total number of expired responses read from the cache updating - The total number of expired responses read from the cache while responses were being updated revalidated - The total number of expired and revalidated responses read from the cache miss - The total number of responses not found in the cache. expired - The total number of expired responses not taken from the cache. bypass - The total number of responses not looked up in the cache
SSL fails ratio	failed SSL handshakes / total SSL handshakes ratio (%)

(average since last test)	
SSL handshakes / sec (average since last test)	NGINX is commonly used to terminate encrypted SSL and TLS connections on behalf of upstream web and application servers. SSL termination at the edge of an application reduces the load on internal servers, simplifies certificate management and reduces certificate costs. However, because it is extremely CPU intensive, it can create a scalability bottleneck that may limit growth. A single Intel core can typically perform up to 350 full 2048 bit SSL handshake operations per second, using modern cryptographic ciphers. NGINX's SSL performance scales with the number of cores available on the host server, so an 8 core virtual machine could accept traffic from over 1,000 new users per second and still have resources to spare.
Health checks	NGINX and NGINX Plus can continually test your upstream servers, avoid the servers that have failed, and gracefully add the recovered servers into the load-balanced group. For passive health checks NGINX monitor transactions as they happen and try to resume failed connections. If the transaction still cannot be resumed, NGINX and NGINX Plus mark the server as unavailable and temporarily stop sending requests to it until it is marked active again. NGINX Plus can periodically check the health of upstream servers by sending special health-check requests to each server and verifying the correct response. HostMonitor receives results of NGINX health checks; if problems detected, HostMonitor sets Bad test status and show problem description in Reply field of the test, e.g. "Backup server 10.10.1.1:8080 UNHEALTHY (fails 65/120688)"

Also you may setup additional tests: URL or HTTP test, Domain Expiration, Certificate Expiration, Network traffic, CPU Usage, Memory, Drive Free Space.

Tomcat

The Apache Tomcat software is an open source implementation of the Java Servlet, JavaServer Pages, Java Expression Language and Java WebSocket technologies. Its one of the most commonly used servers for Java applications.
In addition to the common test parameters, Tomcat test has the following options:

Status URL
Provide URL to XML version of Tomcat Manager App status page, e.g.
`http://tomcat5.mainslot.com/manager/status/?XML=true`
Note: access to the Tomcat Manager application is disabled by default. How to configure Manager Application access:
https://tomcat.apache.org/tomcat-8.0-doc/manager-howto.html#Configuring_Manager_Application_Access

Username / password
Normally status page requires authentication, provide the username and the password

Pool name
When you set the test to check Used memory or Free memory ratio (see **Alert when** parameter), you may specify memory pool name, e.g. PS Eden Space, PS Survivor Space, Compressed Class Space, Metaspace, etc
If you do not provide pool name (keep this field empty), HostMonitor will check total heap memory usage.

Connector
Connector is component that supports the HTTP protocol. It enables Catalina to function as a stand-alone web server, in addition to its ability to execute servlets and JSP pages. A particular instance of this component listens for connections on a specific TCP port on the server.
If you specify connector name, HostMonitor will check parameters of this connector (e.g. number of busy threads or errors/sec rate). If you keep this field empty, HostMonitor will check ALL connectors and find the one with highest usage (highest load, traffic or errors ratio).
Also you may specify connector name using wildcard * at the end. E.g. if you type http-bio* HostMonitor will check connectors that fit the pattern and find the one with highest usage (e.g. highest errors/sec ratio)

Alert when <parameter> above X or below Y
Choose parameter to check and set upper and lower limits. HostMonitor will set Bad test status and trigger specified actions when parameter value will be out of the range.

Free memory ratio (%)	Free memory / maximum ratio Running low on heap memory can be caused by a wide variety of factors. This will severely affect application performance and may lead to OutOfMemoryError error - one of the most common problems that users experience with Tomcat so it's a good idea to do everything you can to prevent errors before they occur. HostMonitor may check total heap memory or specific memory pool (see Pool name parameter). If Maximum limit is not set for some memory pool, HostMonitor will not be able to calculate free memory ratio; use

	“Used memory (MB)” test mode in this case.
Used memory (MB)	Memory used by JVM heap or specific memory pool Running low on heap memory will severely affect application performance. HostMonitor will check specific memory pool when you provide pool name using “Pool name” field, e.g. PS Eden Space, PS Survivor Space, Compressed Class Space, Metaspace; also it can check JVM heap memory (when you keep “Pool name” field empty).
Busy threads	Number of busy threads This metric is critical for tracking the resource consumption. Each incoming request requires a thread for the duration of that request. If more simultaneous requests are received than can be handled by the currently available request processing threads, additional threads will be created up to the configured maximum (the value of the `maxThreads` attribute). If still more simultaneous requests are received, they are stacked up inside the server socket created by the Connector, up to the configured maximum (the value of the `acceptCount` attribute). Any further simultaneous requests will receive "connection refused" errors, until resources are available to process them. By default, Tomcat uses a `maxThreads` number of 200.
Busy threads ratio (%)	busyThreads / maxThreads ratio You may use this metric instead of “Busy threads”
Requests/sec	Average requests/sec (RPS) ratio since last test probe Spikes in RPS can indicate increased customer activity or a DDoS attack. Drops in RPS, on the other hand, can be signs of network connectivity issues. A good way to configure test limits is by first determining what the baseline traffic of your application is and then setting alerts around it, so HostMonitor will set Bad test status and trigger specified actions when the stats are significantly higher (indicating a sudden traffic spike) or if the values drop significantly (indicating an issue that blocks traffic somewhere).
Bytes/sec	Average traffic (received+sent) This metric measures the amount of data being transferred in and out of the server. It can be used as an indicator of server performance, relative to constraints such as network infrastructure.
Processing time	Average processing time per request (since last test probe) If your system takes too long to respond to requests, users are likely to

	quit so it’s important to monitor this response time and investigate the potential causes
Errors/sec	Number of errors per second (since last test probe) Note: any response code 4xx and 5xx will increment the error count
Errors/requests ratio	Errors / total requests ratio The appropriate threshold is very depending on the nature of your web site, so you'll have to look at historical data to set an appropriate threshold. If this rate is climbing, that’s probably worth investigating. And if it’s a sharp increase, that’s going to need urgent attention.

Also you may setup additional tests: URL or HTTP test, Domain Expiration, Certificate Expiration, Network traffic, CPU Usage, Memory, Drive Free Space.

IIS

Internet Information Services (IIS) is an extensible web server running on Windows OS including Windows 10 and Windows Server 2022 (starting from Windows NT 3.51). It may support web site extensions like SharePoint Web Application.
In addition to the common test parameters, the IIS test has the following options:

Target host
Provide the host name (e.g. mainserver.domain.com) or IP address (e.g. 10.10.1.55) of the IIS server that you wish to monitor. Use Connection Manager to store account information necessary to perform connections to remote systems.

Site
If you are running several web sites on IIS server, you may tell HostMonitor which site should by checked by this test. You may select site name from drop down list or you may set “Total” when you need to check statistics for entire IIS server.

Alert when <parameter> above X or below Y
Choose parameter to check and set upper and lower limits. HostMonitor will set Bad test status and trigger specified actions when parameter value will be out of the range.

Current connections (ALL instances/sites)	The number of active connections established with the web service (ALL sites, Site test property is not used for this counter)
Current requests	Current number of active requests currently being processed. Includes anonymous, non-anonymous, CGI, temporarily blocked requests
Current CGI requests	Current number of CGI requests that are simultaneously being processed by the web service.
Current ISAPI requests	Current number of ISAPI extension requests that are simultaneously being processed by the web service.
Current Anonymous requests	The active anonymous requests currently being processed. A typical scenario looks like: - user requests a page - connection is established and "Current Connections" increase - the request is being processed and "Current Anonymous requests" increase - the request has been processed and "Current Anonymous requests" decrease - the connection is idle for some time - the connection is closed, and "Current Connections" decrease
Current NonAnonymous requests	The active non-anonymous requests currently being processed
Current BlockedAsyncIO requests	Current requests temporarily blocked due to bandwidth throttling settings.

Bytes transferred/sec	Average traffic (received+sent) since last test probe This metric measures the amount of data being transferred in and out of the server. It can be used as an indicator of server performance, relative to constraints such as network infrastructure.
Bytes received/sec	The rate at which bytes are received by the web service.
Bytes sent/sec	The rate at which bytes are sent by the web service.
Files transferred/sec	The number of files send and received per second (average rate since previous test probe)
Files received/sec	The number of files received per second
Files sent/sec	The number of files sent per second
Requests/sec	Average requests/sec ratio since last test probe Spikes in RPS can indicate increased customer activity or a DDoS attack. Drops in RPS, on the other hand, can be signs of network connectivity issues.
CGI requests/sec	The rate of CGI requests (since previous test probe)
ISAPI requests/sec	The rate of ISAPI extention requests
Anonymous requests/sec	The number of requests from users over an anonymous connection per second (since previous test probe)
NonAnonymous requests/sec	The number of requests from users over a non-anonymous connection per second (since previous test probe)
GET requests/sec	The rate of HTTP GET requests (since previous test probe)
HEAD requests/sec	The rate of HTTP HEAD requests
POST requests/sec	The rate of HTTP POST requests
PUT requests/sec	The rate of HTTP PUT requests
OPTIONS requests/sec	The rate of HTTP OPTIONS requests
DELETE requests/sec	The rate of HTTP DELETE requests
COPY requests/sec	The rate of HTTP COPY requests
LOCK requests/sec	The rate of HTTP LOCK requests
MKOL requests/sec	The rate of HTTP MKOL requests
MOVE requests/sec	The rate of HTTP MOVE requests
TRACE requests/sec	The rate of HTTP TRACE requests
SEARCH requests/sec	The rate of HTTP SEARCH requests
404 errors/sec	The number of not found errors (HTTP 404 response code) per second since previous test probe
404 errors ratio (%)	not found errors / total requests ratio (%) Use this mode to trigger alerts if the fraction of 404 responses

	rises above a threshold. In theory, a 404 response is the user's fault, not the fault of the server. However, if many users are suddenly requesting missing pages, there's a good chance it's due to some changes on server side.
423 errors/sec	The number of locked errors (HTTP 423 response code) per second since previous test probe
423 errors ratio (%)	locked errors / total requests ratio (%) Use this mode to trigger alerts if the fraction of 423 responses rises above a threshold.
File Cache Hits %	The ratio of user-mode file cache hits to total file cache requests (since previous test probe). A low counter value combined with a low Kernel URI Cache Hits % value could mean that you need to check why your files are not being cached.
Metadata Cache Hits %	The ratio of Metadata cache hits to total Metadata cache requests (since previous test probe)
Kernel URI Cache Hits %	The ratio of Kernel URI cache hits to total cache requests (since previous test probe) Note: this counter reflects all HTTP.sys activity, not just IIS activity
URI Cache Hits %	The ratio of URI cache hits to total URI cache requests (since previous test probe)
Output Cache Hits %	The ratio of Output cache hits (since previous test probe)

Also you may setup additional tests: URL or HTTP test, Domain Expiration, Certificate Expiration, Network traffic, CPU Usage, Memory, Drive Free Space.

SMTP

Most Internet e-mail servers use the Simple Mail Transfer Protocol (SMTP) to transmit e-mail from server to server. HostMonitor monitors this type of server by sending an SMTP command to the server as if it were an e-mail client or another server verifying the existence of a user. By verifying the username, the program effectively tests the SMTP server`s mail database without generating unnecessary mail messages.
In addition to the common test parameters, the SMTP test has the following options:

Server
Here you should provide the host name (e. g. mail.ourdomain.com) or IP address (e. g. 204.71.200.68) of the mail server you want to test. Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) and specify hostname with suffixes ::ipv4 or ::ipv6 (e.g. mail.ourdomain.com::ipv4 or www.6bone.net::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.
Note: on Windows NT 4.0, Windows 2000 and Windows XP SP1 IPv6 protocol is not supported. You may use menu Tools -> Local Info to check is your system IPv6 ready.

Port
The default test port is 25, but you can specify a non-standard port. For a list of conventional port numbers click the button to the right of the port number box.

Timeout
This is the amount of time in seconds the program will wait for a response from the server before the request fails. Set this to 0 for no timeout (not recommended).

Perform 'VRFY' test
When checked, the test performs will include the verify ('VRFY') command, which is a complete test of the server's user database and its ability to respond to client requests. When this field is not checked, HostMonitor will log on to the mail server and then log off, but will not issue the "VRFY" command as part of the test. Skipping this command provides nearly the same level of server monitoring, since logging on and off effectively verifies that the mail server is accepting connections.
For mail servers that support the "VRFY" command, and have it enabled, we suggest that you use the complete test. However, some mail servers do not support the "VRFY" command, so turning this check off is required. In addition, for security reasons, the "VRFY" command is sometimes disabled on some servers, again requiring that this extra test would be turned off.

User Name
Enter a valid e-mail account name that exists on the server you are testing. HostMonitor will ask the server if this user exists. Most mail servers have "root" or "postmaster" accounts defined, even if the server is used only to forward outgoing mail. You can also use your own account name, assuming you have an account on that server.

POP3

E-mail is commonly posted and transferred between mail servers using SMTP, but access to mail is provided through POP3 (Post Office Protocol version 3). POP3 test can be used to test that your mail server's POP functions are functioning perfectly. To perform test HostMonitor login to the server and logout using specified user account. As an option HostMonitor can check number of messages and size of messages for a specified user. If messages count/size exceed specified limit, the program can start alert actions.
In addition to the common test parameters, the POP3 test has the following options:

Server
This is the name or IP address of the mail server you want to test, usually in the form "mail.yourcom.com".

Port
The default POP3 port for unencrypted connection is 110; POP3 servers that support secured SSL connections usually accept connections using TCP port 995. If your server configured to use some non-standard port, specify port number using this property.

TLS
This option allows you to use secured and encrypted connection (SSL). You may set “None” option to use unencrypted connection, select “Implicit” or “Explicit” to use encrypted connection.
Enabled protocols: TLS 1.1, 1.2 (and TLS 1.3 on Windows 11 and Windows Server 2022); in some cases TLS 1.0 and SSL 3.0 can be enabled.
Additional SSL/TLS options located on Misc page in the Options dialog.

Timeout
This is the amount of time in seconds the program will wait for a response from the server before the request fails. Set this to 0 for no timeout (not recommended).

User Name
HostMonitor will test the POP server by logging in to it using an existing account. In the user name field, supply the name of an account that can be used for testing. HostMonitor will log into the account and check the status of its mailbox without accessing, modifying or deleting any of the messages held in it.

Password
Supply the password for the user account HostMonitor will log into during the test.

Alert when mailbox contains more then [NN] messages
Mark this option and specify limit amount of messages in a mailbox. When this limit is reached, HostMonitor will change test status to Bad.

Alert when total size of messages bigger than [NN] MB
Mark this option and specify the size limit of all messages in a mailbox. When this limit is reached, HostMonitor will change test status to Bad.

Note: Value of the 'Reply' field depends on the test's settings:

- if test checks number of messages, HostMonitor will display number of messages
- if test checks total size of messages, HostMonitor will display total size of messages.
- if both these options disabled and test checks server status only (connect, login and logout), Reply value will contain the test execution time (that shows the reply speed of the server).
- Reply value is empty when the program cannot connect or login to server

IMAP

Some Internet mail servers support IMAP (Internet Message Access Protocol) for exchanging and manipulating e-mail. The IMAP test works much in the same way that POP3 test function to test IMAP compliant mail servers. The IMAP test performed by HostMonitor involves logging in to your mail server using an existing account and checking the status of the mailbox for that user. As option HostMonitor can check number of messages and size of messages for specified mailbox. If message count/size exceeds specified limit, the program can start alert actions.
In addition to the common test parameters, the IMAP test has the following options:

Server
This is the name or IP address of the mail server you want to test, usually in the form "mail.yourcom.com".

Port
The default IMAP port for unencrypted connection is 143; IMAP servers that support secured SSL connections usually accept connections using TCP port 993. If your server configured to use some non-standard port, specify port number using this property.

TLS
This option allows you to use secured and encrypted connection (SSL). You may set “None” option to use unencrypted connection, select “Implicit” or “Explicit” to use encrypted connection.
Enabled protocols: TLS 1.1, 1.2 (and TLS 1.3 on Windows 11 and Windows Server 2022); in some cases TLS 1.0 and SSL 3.0 can be enabled.
Additional SSL/TLS options located on Misc page in the Options dialog.

Timeout
This is the amount of time in seconds the program will wait for a response from the server before the request fails. Set this to 0 for no timeout (not recommended).

Login
HostMonitor will test the IMAP server by logging in to it using an existing account. In the user name field, supply the name of an account that can be used for testing. HostMonitor will log into the account and check the status of its mailbox without accessing, modifying or deleting any of the messages held in it.

Password
Supply the password for the user account HostMonitor will log into during the test.

Check mailbox
You may mark this combobox and select one of the folowing options to check mailbox parameters.

Mailbox
Specify name of the mailbox to check.

Filter
Here you may tell HostMonitor to scan all messages in the mailbox or scan for messages with specific flag by choosing one of the following options

- All messages
- Recent
- Answered
- Unanswered
- Flagged
- Unflagged
- Seen
- Unseen

Note: Recent option tells HostMonitor to check for messages that were received since last test probe (last check by HostMonitor).

Alert when mailbox contains more then [NN] messages
Select this option and specify the limit amount of messages in the mailbox. When this limit is reached, HostMonitor will change test status to Bad.

Alert when total size of messages bigger than [NN] MB
Select this option and specify the size limit of all messages in the mailbox. When this limit is reached, HostMonitor will change test status to Bad.

Alert when there are messages older than [NN] min
If you choose this option, HostMonitor will search for e-mail messages older than specified time limit. If any “old” e-mail detected, HostMonitor will set “Bad” test status and display number of such messages. Note: you may use “Optional status processing” options to modify test status depending on number of messages or some other conditions.

Note: Value of the 'Reply' field depends on the test settings:

- if test checks number of messages, HostMonitor will display number of messages.
- if test checks total size of messages, HostMonitor will display total size of messages
- if 'check mailbox' options disabled and test checks server status only (connect, login and logout), Reply value will contain the test execution time (that shows the reply speed of the server).
- Reply value is empty when the program cannot connect or login to the server

E-Mail

This versatile test may check mailbox on target server using POP3 or IMAP protocol including encrypted connections (TLS 1.1, TLS 1.2, etc).
You may setup test to check for "bad" and optionally for "good" e-mails by verifying sender's address, recipient's address, e-mail subject and body of the mail. You may check each parameter for specific string(s); also you may perform various check based on data retrieved from XML documents.

In addition to common test parameters, for this test you should specify the following options:

Server
The name or IP address of the mail server

Protocol
HostMonitor supports IMAP (Internet Message Access Protocol) and POP3 (Post Office Protocol version 3) protocols. Select the one supported by your server.
If both protocols supported by the server and a lot of mails can be stored in specified mailbox, we recommend to use IMAP protocol, it provides more efficient options for search operations.

Mailbox
Specify name of the mailbox to check (unused for POP3 servers).

Login
Provide account name that will be used for testing.

Password
Supply the password for the account specified above.

Port
The default POP3 port for unencrypted connection is 110; POP3 servers that support secured SSL connections usually accept connections using TCP port 995.
The default IMAP port for unencrypted connection is 143; IMAP servers that support secured SSL connections usually accept connections using TCP port 993.
If your server configured to use some non-standard port, specify port number using this property.

TLS
This option allows you to use secured and encrypted connection (SSL). You may set "None" option to use unencrypted connection, select "Implicit" or "Explicit" to use encrypted connection.
Enabled protocols: TLS 1.1, 1.2 (and TLS 1.3 on Windows 11 and Windows Server 2022); in some cases TLS 1.0 and SSL 3.0 can be enabled.
Additional SSL/TLS options located on Misc page in the Options dialog.

Timeout
This is the amount of time in seconds the program will wait for a response from the server before the request fails. Set this to 0 for no timeout (not recommended).

Filters for Bad and Good e-mails

When you setup E-Mail test item, you should setup filters that separate “Bad” and “Good” mails.

When HostMonitor detects new mail that fits “Bad” filter conditions, it changes status of the test item to “Bad”. Note: here “new” means mail that was received by mail server after last test probe. When test status changes back to “Ok”? This behavior depends on the following options:

- **set "Ok" status when no new "Bad" mails detected**
  HostMonitor will assign "Ok" status to the test item, when subsequent test probe will not detect any new "Bad" mail

- **set "Ok" status when new “Good” mails detected**
  Status of the test item will be changed to “Ok” when HostMonitor finds new mail that fits “Good” filter conditions.

- **set “Ok” status by acknowledgement (manually)**
  With this option chosen, test item will remain “Bad” until operator acknowledge status (then status will be changed to Ok)

If you choose “set Ok status when no new Bad mails detected” or “set Ok status by acknowledgement (manually)” options then “Good” filter is not used.
If you choose “set "Ok" status when new “Good” mails detected” option, you should specify both (“Bad” and “Good”) filters.

Filters:

There are 2 sets of conditions in the E-Mail Test Properties dialog - “Bad” and “Good” filters. If some mail matches neither “Bad” nor “Good” filter, mail is ignored by the test (however the same e-mail can be processed by another E-Mail test item that check the same mailbox with different filters in use). Mail passes the filter only when it matches ALL specified requirements of the filter.

Both filters provide exactly the same set of options. So, let’s describe the conditions for “Bad” filter. Here you may mark one or several of the following options

Check sender	Tells HostMonitor to check e-mail sender
Check recipient	Tells HostMonitor to check e-mail recipient
Check subject	Tells HostMonitor to check e-mail subject line for specific string(s)
Check body	Tells HostMonitor to check e-mail body for specific string(s) or specific data within XML document

For any of these options you may choose “check for string” or “check for expression” mode. Also, for e-mails with body that contains data in XML format, you may choose “check for XML data” mode, provide XPath and specify additional filters to check result set. You may check row count, check field value in 1st row, check value of any row or value of every row, check average value or sum of all values.

Check for string

With this mode selected HostMonitor simply checks e-mail parameter for specified string. When you check sender or recipient, you may use wildcard * at the beginning of the string (e.g. "*@microsoft.com").

If you check for subject or body, you may not use wildcard. Instead you may use "Whole words only" option, it tells HostMonitor to search for words only. With this option disabled, the search string might be found within longer words.

Check for expression

If you choose "check for expression" mode, HostMonitor will consider the specified string as boolean (logical) expression and evaluate expression using e-mail parameters. In the expression you may use strings (must be put in quotes (') or in double quotes ("")); round brackets; logical operators **and**, **or**, **not**.

For example if you set [Check body for expression ("<Price>" and "<Index>") and not ("Error" or "Warning")] option then e-mail will pass filter if mail body contains both strings "<Price>" and "<Index>", and doesn't contain either strings "Error" or "Warning".

If you specify expression like ('admin1@domain.com' or 'admin2@domain.com') for sender's address, e-mail will pass filter when sender is admin1@domain.com or admin2@domain.com.

Check for XML data

Using this mode you may provide XPath (that allows you to select some structures within XML document) and specify additional conditions to check result set. You may check row count, check data in 1st row, check any row or every row, check average value or sum of all values. E.g. you may setup HostMonitor to select all <temperature> fields and check temperature value for each item (e.g. "every row > than 50").

XPath

XPath (XML Path Language) is a query language for selecting nodes from an XML document. by a variety of criteria. Before checking "alert" conditions HostMonitor may process specified XPath, this allows you to setup very flexible queries.

Examples

/farm/server/drive[last()]	Selects the last "drive" element that is the child of the "server" element that in turn is child of the "farm" element
/farm/server/cpu[temperature>80]	Selects all "cpu" elements (child of the "server" element that in turn is child of the "farm" element) that have a temperature element with a value greater than 80
//drive[@type='fixed']	Selects all "drive" elements that have an attribute named "type" with a value of "fixed"

Alert when

This option specifies when exactly retrieved value(s) can pass "bad" (or "good") filter and appropriate alert actions should be started. There are 3 parameters should be provided: aggregation mode, compare mode and compare value.

Aggregation mode - specifies how HostMonitor should compare result data when query returns several rows. Choose one of the following option:

Row count	Tells HostMonitor to calculate row count and compare number of the rows to the specified number
1st row	Tells HostMonitor to check only 1st retrieved counter
Any row	Tells HostMonitor to check each retrieved counter. If ANY counter matches specified compare condition, e-mail passes this check
Every row	Tells HostMonitor to check all retrieved counters. If EVERY counter matches specified compare condition, e-mail passes this check
Average	Tells HostMonitor to calculate average value of the counters and compare calculated average value to the specified number.
Sum/Total	Tells HostMonitor to calculate sum of the counters and then compare total value to the specified number.

Notes:

- If there is single counter in result set then "1st row", "Any", "Every", "Average" and "Total" modes are equivalent (except "Average" and "Total" do not compare value to a string).
- You may use Average and Total mode only with numeric data

Compare mode: HostMonitor compares calculated value with a specified number or string. The following compare modes are supported:

- less than the specified number
- greater than the specified number
- equal to the specified value (number or string)
- different from the specified value (number or string)
- contains the specified string
- doesn't contain the specified string

Note: HostMonitor does not check mail body part when its size is over 128KB

Additional options

Report about latest bad/good mail

If several bad/good mails were received since previous test probe, this option tells HostMonitor to use most recent mail for test result.

Report about all bad/good mails

If several bad/good mails were received since previous test probe, this option tells HostMonitor to change test status according to each e-mail that passes filters.

Remove e-mail after test

This option tells HostMonitor to remove e-mails that fit specified filter (remove e-mail after test probe is complete).

Important note: If this option disabled and several "bad" or "good" e-mails can be received by the server within single second then HostMonitor will detect only 1st of these mails.

Display

Using this option you may choose what information should be displayed in Reply field of the test:

- Test time
- Sender address
- Recepient address
- Subject
- First line of the mail
- Last line of the mail
- Detected line (this option available when “check body” option is enabled)
- Previous (to detected) line
- Next (to detected) line
  (last 2 options available when you check mail body for a string, not XML data)

There are some variables specific to E-Mail test, you may use these variables as parameters of actions assigned to such test items.

Note: If you assign “Execute HM Script” action to E-Mail test, then you may send e-mail with HM Script commands to HostMonitor and HostMonitor will execute your e-mail as a script. So you may setup HostMonitor to inform you about problems by e-mail and you may respond to HostMonitor by e-mail as well. E.g. you may pause some test items or acknowledge status of failed items. Even more: HostMonitor may send you back confirmation. See HMScript and multiline variables for details.

Mail Relay

Mail Relay test method was designed to monitor a chain of mail servers. HostMonitor sends an e-mail through the specific mail server and then checks when the message becomes available in target mailbox. HostMonitor sends special mail using SMTP protocol and checks the target mailbox using POP3 or IMAP protocol.
In addition to common test parameters, for this test you should specify the following options:

Outgoing mail server
The following group of parameters specifies the mail server that receives e-mail from HostMonitor and sends message to a target mailbox (directly or through a chain of other mail servers).

Protocol
HostMonitor sends e-mail messages using SMTP protocol only.

Host
Provide the name or IP address of the mail server.

Port
The default ports for SMTP protocol is 25, 465 and 587. However you can specify a non-standard port (if it is known that your mail server uses such a port)

TLS
This option allows you to use secured and encrypted connection (SSL). You may set "None" option to use unencrypted connection, select "Implicit" or "Explicit" to use encrypted connection.

Timeout
This is the amount of time in seconds the program will wait for a response from the server before the request fails. Set this to 0 for no timeout (not recommended).

Authentication
HostMonitor supports and automatically recognizes Plain, Login and Cram-MD5 authentication schemes. It also works with SMTP servers that do not require any authorization.

Login
Specify the login name. You may create special e-mail account for testing purpose (an account that will be used by HostMonitor only), or you may use any of the existing user accounts. If your SMTP server does not require authorization, keep this field blank.

Password
Supply the password for the account specified above.

Incoming mail server
This group of parameters specifies the target server that should receive e-mail messages.

Protocol
HostMonitor supports IMAP (Internet Message Access Protocol) and POP3 (Post Office Protocol version 3) protocols. Select the one supported by your server.

Host
The name or IP address of the server that should receive test messages.

Port
The default POP3 port for unencrypted connection is 110; POP3 servers that support secured SSL connections usually accept connections using TCP port 995.
The default IMAP port for unencrypted connection is 143; IMAP servers that support secured SSL connections usually accept connections using TCP port 993.
If your server configured to use some non-standard port, specify port number using this property.

TLS
This option allows you to use secured and encrypted connection (SSL). You may set "None" option to use unencrypted connection, select "Implicit" or "Explicit" to use encrypted connection.
Enabled protocols: TLS 1.1, 1.2 (and TLS 1.3 on Windows 11 and Windows Server 2022); in some cases TLS 1.0 and SSL 3.0 can be enabled.
Additional SSL/TLS options located on Misc page in the Options dialog.

Timeout
This is the amount of time in seconds the program will wait for a response from the server before the request fails. Set this to 0 for no timeout (not recommended).

Mailbox
Specify name of the mailbox to check (unused for POP3 servers).

Login
HostMonitor tests the IMAP/POP3 server by logging in to it and checking status of the previously sent mail. In the Login field you should provide the name of an account that will be used for testing.
You may use an existing (user's) account - HostMonitor will log into the mailbox, check the status of special test mail and remove this mail without accessing, modifying or deleting any of the user's messages held in it.
However we recommend creating a special account to be used by HostMonitor only. In latter case test messages will not confuse users.

Password
Supply the password for the account specified above.

Mail

Here you should provide the e-mail addresses of the sender and recipient. In some cases you may use the same address in both fields.

From
Specify the email address of the sender (HostMonitor). You may create special account for testing purposes (an account that will be used by HostMonitor only), or you may use any valid address here (e.g. hostmonitor@our-domain.com).

To
Address of the recipient. You may use an e-mail address of existing user; HostMonitor will log into the mailbox, check the status of special mail and remove this mail without accessing, modifying or deleting any of the user's messages held in it.
However we recommend creating a special account to be used by HostMonitor only. In latter case testing messages will not confuse users (e.g. hostmonitor@our-remote-mail-box.com).

Alert
The following options define how HostMonitor should perform the test

Alert when incoming mail server does not receive mail within N sec
With this option selected HostMonitor will send e-mail through the specified SMTP server then wait N seconds and check the target mailbox on POP3 or IMAP server. If the target server has not received the mail then the status of the test item will be changed to "Bad" and appropriate action profile will be executed. If the mail has been received, HostMonitor sets "Ok" status and removes the message. Also it removes all obsolete messages (if any). "Obsolete messages" are those that were sent during previous test probes but were not delivered on time.
Use this option if your mail system is pretty fast and messages can be delivered within a minute or so.

Alert when incoming mail server does not receive mail before next checking cycle
With this option selected HostMonitor first logs into "incoming" server to check if the target mailbox has received the test mail that was sent by previous test probe. If the mail was received, HostMonitor sets "Ok" status and removes the message; otherwise "Bad" status will be set.
Then HostMonitor sends new mail that will be checked by next test probe. Time of the next probe depends on the test interval and assigned schedule (specified in Test Properties dialog). Note: if test item has been assigned as Master test for other test items, it might be executed more often (see "Consider status of the master test obsolete after N seconds" option on Behaviour page in the Options dialog). Also "Refresh" command will force HostMonitor to execute the test immediately.
So if you choose this option, each test probe will look for mail that was sent by previous probe.
Use this option when your mail system needs several minutes to deliver the mail.

Of course when incoming or outgoing server does not accept connection at all or it is impossible to pass server authentication using specified account, HostMonitor sets an appropriate test status and triggers assigned alert profile.

TCP

The TCP test provides you with the ability to monitor TCP based servers such as Whois, Finger, Telnet, Chargen, etc. Please note, that you may check SMTP, POP, IMAP, DNS, LDAP, HTTP/HTTPS, and FTP servers using dedicated SMTP, POP, IMAP, DNS, LDAP, URL, HTTP tests.
In addition to the common test parameters, the TCP test has the following options:

Host
Here you should provide the host name (e. g. www.yahoo.com) or IP address (e. g. 204.71.200.68) of the host that should process the TCP connection. Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) and specify hostname with suffixes ::ipv4 or ::ipv6 (e.g. www.google.com::ipv4 or www.6bone.net::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.
Note: on Windows NT 4.0, Windows 2000 and Windows XP SP1 IPv6 protocol is not supported. You may use menu Tools -> Local Info to check is your system IPv6 ready.
Also, a range of IPv4 addresses (e.g. 10.10.1.100 – 10.10.1.254) rather than a single address can be specified. In this case, HostMonitor will create a separate test for each of the addresses within that range.

Port
Specify the port number on which the host is listening for incoming TCP packets. E.g. Telnet servers use port #23, Whois servers uses port #43, etc. For a list of conventional port numbers click the button to the right of the port number box.

Timeout
Enter the amount of time (in seconds) that HostMonitor should wait for a response from the server. If this value is 0 (default value), HostMonitor uses the default Windows timeout.

The following optional parameters allow you not only to check whether the connection could be accepted by remote server but also allow to send some data to that server and check the response from it.

Send data
If you want to send data to the host (after TCP connection established), mark this option and enter the packet data. If you need to send binary data, use sequences formatted **%XX** where XX is a hexadecimal code of a character (byte). E.g. HELLO%0D%0A would send HELLO followed by a character ASCII 13 (line feed) and ASCII 10 (new line).

Alert when
To check the reply from the server, mark this option and choose one of the conditions to consider result of the test as “Bad”:

- no reply	HostMonitor will set “No answer” status when no reply from the server received and set test status to “Host is alive” when any reply received
- any reply	HostMonitor will set “Ok” status when no reply from the server received and set test status to “Bad” when any reply received
- reply contains	HostMonitor will set “Bad” status when reply from the server contains specified string (defined in “Compare with” field). If reply doesn’t contain the specified string, HostMonitor will set “Ok” status. The program sets status to “No answer” when no reply received.
- reply doesn’t contain	HostMonitor will set “Ok” status when reply from the server contains specified string (defined in “Compare with” field). If reply doesn’t contain the specified string, HostMonitor will set “Bad” status. The program sets status to “No answer” when no reply received.
- reply is equal to	HostMonitor will set “Bad” status when reply from the server equal to specified string (defined in “Compare with” field). If reply isn’t equal to the specified string, HostMonitor will set “Ok” status. The program sets status to “No answer” when no reply received.
- reply is not equal to	HostMonitor will set “Ok” status when reply from the server is equal to specified string (defined in “Compare with” field). If reply isn’t equal to the specified string, HostMonitor will set “Bad” status. The program sets status to “No answer” when no reply received.

Compare with
HostMonitor can compare data that were received from the server with specified string (use “Alert when” option to choose compare condition). As in “Send data” field you can use sequences formatted **%XX** where XX is a hexadecimal code of a character (byte). E.g. “October%00%00”

See also: variables specific to TCP and UDP tests

UDP

The UDP test provides you with the ability to monitor UDP based servers such as TFTP, SNTP, Daytime, etc. Please note, to check DNS, NTP, and RADIUS servers you can use dedicated DNS, NTP, and RADIUS tests.
In addition to the common test parameters, the UDP test has the following options:

Server
Here you should provide the host name (e. g. www.yahoo.com) or IP address (e. g. 204.71.200.68) of the host that should receive and process the UDP packet. Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) and specify hostname with suffixes ::ipv4 or ::ipv6 (e.g. www.google.com::ipv4 or www.6bone.net::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.
Note: on Windows NT 4.0, Windows 2000 and Windows XP SP1 IPv6 protocol is not supported. You may use menu Tools -> Local Info to check is your system IPv6 ready.

Port
Specify the port number on which the host is listening for incoming UDP packets. E.g. TFTP servers use port #69, SNTP servers use port #123, Daytime servers use port #13, etc

Retries
Set the number of times HostMonitor will resend data to the server before test fails.

Timeout
Enter the amount of time (in seconds) that HostMonitor should wait for a response from the server.

Packet to send
Enter the packet data that should be sent to the host. Because most UDP servers accept binary data, you may need to use sequences formatted **%XX** where XX is a hexadecimal code of a character (byte). E.g. HELLO%0D%0A would send HELLO followed by a character ASCII 13 (line feed) and ASCII 10 (new line).

Alert when
Choose one of the conditions to consider result of the test as “Bad”:

- no reply	HostMonitor will set “No answer” status when no reply from the server received and set test status to “Host is alive” when any reply is received
- any reply	HostMonitor will set “Ok” status when no reply from the server received and set test status to “Bad” when any reply is received
- reply contains	HostMonitor will set “Bad” status when reply from the server contains specified string (defined in “Compare with” field). If reply doesn’t contain the specified string,

HostMonitor will set “Ok” status. The program sets status to “No answer” when no reply is received.

- reply doesn’t contain — HostMonitor will set “Ok” status when reply from the server contains specified string (defined in “Compare with” field). If reply doesn’t contain the specified string, HostMonitor will set “Bad” status. The program sets status to “No answer” when no reply is received.
- reply is equal to — HostMonitor will set “Bad” status when reply from the server is equal to specified string (defined in “Compare with” field). If reply isn’t equal to the specified string, HostMonitor will set “Ok” status. The program sets status to “No answer” when no reply is received.
- reply not equal to — HostMonitor will set “Ok” status when reply from the server is equal to specified string (defined in “Compare with” field). If reply isn’t equal to the specified string, HostMonitor will set “Bad” status. The program sets status to “No answer” when no reply is received.

Compare with

HostMonitor can compare data that were received from the server with specified string (use “Alert when” option to choose compare condition). As in “Packet to send” field you can use sequences formatted **%XX** where XX is a hexadecimal code of a character (byte). E.g. “October%00%00”

Examples:

To check your TFTP server fill up test parameters with following values:

- Server — address of the server
- Port — 69
- Packet to send — %00%01filename%00%00netascii%00
  where filename is the name of the file on the server. We recommend provide incorrect (fake) name of the file.
- Alert when — no reply

To check SNTP server fill up test parameters with following values:

- Server — address of the server
- Port — 123
- Packet to send — %0B
  %00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00
  %00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00
  %00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00
  Yes, type such a long string, network packet must contain 48 bytes
- Alert when — no reply

NTP/SNTP

The Network Time Protocol (NTP) is widely used to synchronize computer clocks in the global Internet. Using NTP/SNTP test you can easily check you NTP/SNTP server.
In addition to the common test parameters, the NTP test has the following options:

Server
Here you should provide the host name (e. g. www.yahoo.com) or IP address (e. g. 204.71.200.68) of the destination host that should receive and process the request from HostMonitor. Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) and specify hostname with suffixes ::ipv4 or ::ipv6 (e.g. www.google.com::ipv4 or www.6bone.net::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.
Note: on Windows NT 4.0, Windows 2000 and Windows XP SP1 IPv6 protocol is not supported. You may use menu Tools -> Local Info to check is your system IPv6 ready.

Port
Specify the port number on which the host is listening for incoming packets. By default NTP servers use port #123.

Retries
Set the number of times HostMonitor will resend data to the server before test fails.

Timeout
Enter the amount of time (in seconds) that HostMonitor should wait for a response from the server.

Alert when difference in time is greater than XX sec
With this option enabled HostMonitor will mark test item as “Bad” when difference in time between the server and local system is greater than specified value. If this option is disabled HostMonitor will set test status to “Host is alive” when any correct response is received from the server.

Display mode
This parameter defines what HostMonitor will display in “Reply” field. Choose one of the following options:

Reply time	- display time required to send request and receive reply from the server
Remote time	- display server’s system time (Coordinated Universal Time)
Difference in time	- display difference in time between server and local system

DNS

The DNS test acts as a low-level resolver and connects directly to the target name server to perform a query. This means that the test is completely independent of the host files, DNR cache, etc.
In addition to the common test parameters, the DNS test has the following options:

Server
Here you should provide the domain name (e.g. DNS1.IU.EDU) or IP address (e. g. 204.71.200.68) of the machine running the DNS server that you wish to monitor. Using a domain name in the "Server" field requires that the domain name be resolved before the Domain Name Server can be tested, creating ambiguity in testing. It is better to enter the IP address of your Domain Name Server, as opposed to the domain name, so that the test will always report the correct error if the DNS fails.
Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) and specify hostname with suffixes ::ipv4 or ::ipv6 (e.g. DNS1.IU.EDU::ipv4 or NS-AOA.ES.NET::ipv6). If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.
Note: on Windows NT 4.0, Windows 2000 and Windows XP SP1 IPv6 protocol is not supported. You may use menu Tools -> Local Info to check is your system IPv6 ready.

Protocol
Select the protocol to use: TCP or UDP

Port
The default test port is 53, but you can specify a non-standard port. For a list of conventional port numbers click the button to the right of the port number box.

Timeout
This is the amount of time in seconds the program will wait for a response from the server before the request fails.

Request / Request type
Use these options to specify the domain name that should be requested from DNS server and type of the request. You may choose one of the following requests:

- A type request - request for IPv4 (IP version 4) address of the host
- AAAA request - request for IPv6 (IP version 6) address of the host
- CNAME - canonical name request
- NS - authoritative server request
- MX - mail routing information requests
- PTR - reverse DNS
- TXT - text records
- SPF - Sender Policy Framework records

Note: you may specify protocol used for communication (IPv4 or IPv6) and type of the request (A or AAAA) completely independently. E.g. HostMonitor may connect to DNS server 204.71.200.68 using IPv4 protocol and retrieve AAAA (IPv6) record or it may send request to host fe80::370:ff56:fed5:22 using IPv6 protocol and retrieve A (IPv4) record.

Test result for
If you are using "A" type request, you can define the IP address that will be compared with the address returned from the DNS server being tested. You can use "Test" button to have HostMonitor fill in this field, or you can enter the expected IP address yourself.
Similarly you may check results of CNAME, NS, MX, TXT and SPF requests.

See also: variables specific to DNS test

DHCP

The DHCP test allows you to monitor DHCP servers. HostMonitor verifies the DHCP server by sending request for IP address. HostMonitor sets "Host is alive" status when DHCP server properly responds within specified timeout, whatever it replies with NAK or ACK packet. Otherwise HostMonitor may set "Bad" (invalid reply from server) or "No answer" status.
In addition to the common test parameters, the DHCP test has the following options:

Host
This is the domain name or IP address of the machine running the DHCP server that you wish to monitor.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Request IP
Here you may specify IP address that will be requested or keep default value <current local IP>
Also you can manually specify which network interface should be used for testing - set RequestIP property of the DHCP test using a string like <request IP>/<interface IP>, e.g. 10.10.10.101/10.10.10.1

LDAP

This test is used to check Directory Servers using the LDAP (Lightweight Directory Access Protocol). To perform this test HostMonitor connects and binds to the directory server. If the Password property has a value, it is used for authentication. As an option HostMonitor can perform Search operation using specified base object and search filter.
In addition to the common test parameters, the LDAP test has the following options:

Server
This is the name or IP address of the LDAP server you want to test.
Note: when you setup LDAP test for LDAP server that accepts connection on non-standard port but does not support any SSL option, you may add "::sslnone" suffix to hostname (e.g. you may specify target hostname as primaryDC.mycompany.com::sslnone or 10.10.5.1::sslnone)

Port
The default LDAP port port for unencrypted connection is 389. LDAP servers that support secured SSL connections usually accept connections using TCP port 636. If your server configured to use some non-standard port, specify port number using this property.
Enabled protocols: TLS 1.1, 1.2 (and TLS 1.3 on Windows 11 and Windows Server 2022); in some cases TLS 1.0 and SSL 3.0 can be enabled.
Additional SSL/TLS options located on Misc page in the Options dialog.

Timeout
This is the amount of time in seconds the program will wait for a response from the server before the request fails.

Password
Specify the password used to authenticate to the LDAP server.

Perform Search operation
HostMonitor can perform search operation, to implement this behavior mark "Perform Search operation" option and define the following parameters:

Base object
The Distinguished Name used as the base for LDAP operations (in HostMonitor's case it's a base object during LDAP searches). The Distinguished Name is provided in string format as specified by RFC 1779.

Search filter
A string representation of the LDAP search filter used during searches. The format of the search filters is specified by RFC 1558 and is identical to the format used by most LDAP applications. The following are examples of search filters, as provided in the RFC:

- (cn=Babs Jensen)
- (!(cn=Tim Howes))
- (&(objectClass=Person)(|(sn=Jensen)(cn=Babs J*)))
- (o=univ*of*mich*)

Results limit

By default HostMonitor checks only result code returned by the server. If result code is 0 (success), HostMonitor sets “Host is alive” status. However if you want to check how many records server returns in response to search operation, use “Results limit” option. In this case HostMonitor will check number of records returned by the server and set “Bad contents” status when number of records is below specified limit.

RADIUS

RADIUS test allows you to check Remote Authentication Dial-In User Service (RADIUS).
In addition to the common test parameters, the RADIUS test has the following options:

Server
Here you should provide the host name (e. g. www.yahoo.com) or IP address (e. g. 204.71.200.68) of the destination host that should receive and process the request from HostMonitor. You RADIUS server must be configured to accept packets from the IP address of the machine on which HostMonitor is installed.
Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) and specify hostname with suffixes ::ipv4 or ::ipv6 (e.g. www.google.com::ipv4 or www.6bone.net::ipv6). If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.
Note: on Windows NT 4.0, Windows 2000 and Windows XP SP1 IPv6 protocol is not supported. You may use menu Tools -> Local Info to check is your system IPv6 ready.

Port
Specify the port number on which the host is listening for incoming packets. Usually RADIUS servers use port #1812. However some RADIUS servers are still using port 1645 even though RFC 2138 notes the conflict with "datametrics" services. You may need to change 1812 to 1645, this will depend on your RADIUS server configuration.

Retries
Set the number of times HostMonitor will resend data to the server before test fails.

Timeout
Enter the amount of time (in seconds) that HostMonitor should wait for a response from the server.

Login
Specify the name of the user to be authenticated. You can use invalid (fake) user name and set “Reject reply is Good” option. In this case HostMonitor will mark test as “bad” and start alert actions only when no reply received. If any reply from the server will be received, HostMonitor will mark test as “Host is alive”. Please note, for security reasons some RADIUS services will quietly discard invalid request packets. To check these servers you should specify correct user name and password.

Password
Specify the password of the user to be authenticated.

Secret
Provide a “shared secret”. Transactions between the client and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. User passwords are sent

encrypted between the client and RADIUS server, to eliminate the possibility that someone snooping on an unsecured network could determine user's password.

Reject reply is Good / Reject reply is Bad

Choose one of two options:

- "Reject" reply is Good
  with this option enabled HostMonitor will set test status to "Host is alive" when any reply received from the server
- "Reject" reply is Bad
  with this option enabled HostMonitor will set test status to "Ok" when "Access-Accept" packet received from the server (that means user was successfully authenticated on server). If any other response was received, the program will set "Bad" status. If no answer received, HostMonitor set status to "No answer"

Please note:

You RADIUS server must be configured to accept packets from the IP address of the machine on which HostMonitor is installed.

For some RADIUS servers you can use invalid (fake) user name and/or password and set "Reject reply is Good" option. In this case HostMonitor will mark test as "bad" and start alert actions only when no reply is received. If any reply from the server will be received, HostMonitor will mark test as "Host is alive".

However, for security reasons some RADIUS services will quietly discard invalid request packets. To check these servers you should specify correct user name and password.

DICOM

The Digital Imaging and Communications in Medicine (DICOM) standard was created by the National Electrical Manufacturers Association (NEMA) to aid the distribution and viewing of medical images, such as CT scans, MRIs, and ultrasound. https://www.dicomstandard.org
The DICOM test verifies end-to-end communications with a remote DICOM server by sending DIMSE C-Echo request to the remote host and listening for reply packets.
In addition to the common test parameters the DICOM test has the following options:

Host
Here you should provide the host name (e. g. medical.neman.org) or IP address (e. g. 204.71.200.68) of the remote DICOM server that you wish to monitor. Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) and specify hostname with suffixes ::ipv4 or ::ipv6 (e.g. medical.neman.org::ipv4 or medical.neman.org::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.
Note: on Windows NT 4.0, Windows 2000 and Windows XP SP1 IPv6 protocol is not supported. You may use menu Tools -> Local Info to check is your system IPv6 ready.

Port
Specify a port number that is used by the DICOM server to listening for incoming connections.

Timeout
Specify a timeout interval in seconds.

Called AE-Title
Specify the destination DICOM Application Name.

Calling AE-Title
Specify the source DICOM Application Name.

SIP

SIP test monitors target SIP server using Session Initiation Protocol REGISTER and OPTIONS requests. It may work over UDP, TCP and TLS protocols and can be used to monitor Voice over IP (VoIP) services. This test can send several requests and display average or maximum response time, percentage of lost packets, Jitter, response code.
In addition to the common test parameters the SIP test has the following options:

Address
Here you should provide the host name (e. g. sip2.domain.com) or IP address (e. g. 204.71.200.68) of the remote host that you wish to monitor. Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) and specify hostname with suffixes ::ipv4 or ::ipv6 (e.g. sip2.domain.com::ipv4 or sip33.domain.com::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.
Note: on Windows NT 4.0, Windows 2000 and Windows XP SP1 IPv6 protocol is not supported. You may use menu Tools -> Local Info to check is your system IPv6 ready.

Port
Specify port number used by target SIP server. The default SIP port for unencrypted connection is 5060. SIP servers that support secured TLS connections usually accept connections on port 5061.

Timeout
Specify a timeout interval in milliseconds.

Packets
Specify the number of OPTIONS requests for each test probe (if you need to check Jitter value, please set Packets property at least to 3)

Proto
Choose protocol, HostMonitor supports the following protocols for SIP test method
UDP (unencrypted)
TCP (unencrypted connection)
TCP+TLS (encrypted connection)

UserID / Password
Provide user ID and password. Some SIP services can be checked without REGISTER request, in such case you can keep these fields empty.

Alert if loss ratio >= N
A packet loss threshold can be specified for the test, based on which the test status is determined ("Host is alive" or "Bad"; "No answer" status means HostMonitor did not receive any response from the server).

Display mode

Tells HostMonitor what kind of data should be displayed in the Reply field:

Reply time (average)	- the "Reply" field will represent average reply time
Reply time (max)	- the "Reply" field will represent maximum reply time
Lost %	- display percentage of lost packets
Jitter	- amount of variation in response time, calculated by using the following formula Jitter = SquareRoot(SumOf((ReplyTime[i] - AverageReply)^2) / (ReceivedPacketCount-1)) (if you need to check Jitter, please set Packets property at least to 3)

SIP test can set the following statuses:

Host is alive	- connection established, server accepted REGISTER request and replied to OPTIONS requests (percentage of lost packets below specified threshold)
Bad	- connection established, server replied to SIP request with some error code (e.g. server does not accept authorization or returns code 480 - Service temporarily unavailable); OR connection established, server replied correctly to SIP requests but percentage of lost packets is above specified threshold
No answer	- server does not answer (TCP connection cannot be established or server does not respond to SIP requests)
Unknown host	- specified host name cannot be resolved to IP address
Unknown	- other errors, e.g. TLS handshake failure

You can adjust test behavior (e.g. ignore some SIP error codes) using Optional status processing options and %HttpCode%, %HttpHeader% variables

See also: variables specific to URL, HTTP, SOAP and SIP tests

RAS

The RAS check type is useful for monitoring remote RAS server. With this test HostMonitor tries to connect to the server using specified dial-up connection, sets status of the test (“Ok”, “Bad”, “No answer”, or “Unknown” depending on the connection result), and disconnects from the server. In addition to the common test parameters, the RAS test has the following options:

Connection
Select from drop down list the remote access entry to establish the connection.

User name
Specify the user's name. This parameter is used to authenticate the user's access to the remote access server. If the user name is empty string (""), HostMonitor uses the user name of the current logon context for authentication. For a user-mode application, RAS uses the credentials of the currently logged-on interactive user. For a Win32 service process, RAS uses the credentials associated with the service.

Password
Specify the user's password. This parameter is used to authenticate the user's access to the remote access server. If the password is empty string (""), HostMonitor uses the password of the current logon context for authentication. For a user-mode application, RAS uses the credentials of the currently logged-on interactive user. For a Win32 service process, RAS uses the credentials associated with the service.

Save password
This option has sense only if Password parameter is not an empty string. Specifies whether to save the password (in the phone-book entry) for the user indicated by User Name parameter or not. If "Save password" option is disabled, the password will be removed. Disabling option is equivalent to checking the "Unsave Password" checkbox in Dial-Up Networking dialog.

Retries
Set the number of times the dial-up connection is automatically redialed if the first attempt to connect fails. HostMonitor does not perform second attempt in case connection failed because of the wrong user name or password. If you setup HostMonitor to check several servers using the single modem connected to your computer, it is a good idea to set retries to 3 or more attempts and use **Wait between retries** option. In this case test that was started second (third, forth, etc) will wait for the first test to end and release modem.

Wait between retries
If attempt to dial fails, HostMonitor will wait specified amount of seconds before making another attempt. Of course this parameter makes sense only when Retries field is set to 2 or more attempts.

After execution of a test HostMonitor can set one of four statuses:
- “Ok” status HM sets when connection was successfully established (physical connection modem-to-modem, and network connection as well)

- “Bad”. There can be many reasons for this status, e.g. wrong user name or password, some problems with RAS server, etc.
- “No answer”. The program uses this status when modem does not receive answer from remote modem
- “Unknown”. This status HostMonitor sets when connection was not established because of a problem on local system, e.g. modem is used by another application. You can use “Treat Unknown status as Bad” option. With this option enabled, if test results cannot be obtained, actions are triggered by HostMonitor the same way as if the test returned a "Bad" status.

UNC

Check the UNC path (or local folder) for availability; for the total amount of free space; or for the amount of free space available to the current user (if the operating system implements per-user quotas, this value may be less than the total number of free bytes on the disk). For this test you have to specify the UNC path (or local folder) that you wish to be checked and select the condition for the alert:

- when the resource is unavailable
- when free space (for current user) is less than a specified value
- when the total free space is less than a specified value

If you want to perform the test using an agent installed on UNIX-like system, you should have in mind:

- use slash (/) in the path (instead of backslash (\) that you are using on Windows systems);
- on UNIX-like systems name of the file is case sensitive (so "/etc/RMA" and "/etc/rma" are different files).

See also common test parameters

Drive Free Space (Windows WMI / WinRM)

Both UNC and Drive Free Space test methods may check free disk space on local and remote systems but these methods work in different way and utilize different protocols.
Single UNC test may check single local or shared network resource using requests to file system.
Single Drive Free Space test may check several drives on target system and find drive with minimum free space or drive with minimal percentage of free space (e.g. you may setup test to check all removable drives plus disk C: and F:). Drive Free Space test method checks remote systems using WMI requests, this allows to check non-shared resources on remote Windows systems.

Normally this test uses WMI protocol; since version 15.80 this test method also supports WinRM mode. If you want to use the WinRM protocol for such tests, you should create an entry using the WinRM page of the Connection Manager.
Also you may check free space on Windows and UNIX systems using SNMP protocol, see Drive Free Space (SNMP)

In addition to the common test parameters, Drive Free Space test has the following options:

Target host
Provide the host name (e.g. mainserver) or IP address (e.g. 192.168.1.55) of the host that you wish to check. Keep this field empty or type localhost when you want to check drives on system where HostMonitor (or RMA) is running.
Note #1: Connection Manager provides one convenient place to store account information necessary to perform connections to remote systems.
Note #2: if HostMonitor or RMA is started on VMware virtual Windows system and you setup test to check space on local CD/DVD disk, system may show popup window "There is no disk in the drive" when disk ejected. Solution: specify hostname or external IP address of the system instead of using "localhost" or "127.0.0.1" as host.

Then you may select one or several of the following options
- **Check all local drives**
  tells HostMonitor to check all fixed drives on target system
- **Check all removable drives**
  check all removable drives on target system (not including CD/DVD drives)
- **Check listed drive(s)**
  mark this option and provide drive list when you want to check specific drive(s) on target system, e.g. C,D,E,M

Alert if free space less than <N> MB/GB/TB/%
When HostMonitor checks several drives it finds drive with smallest amount of free space (or drive with minimal percentage of free space when "%" alert options is selected) and sets Ok or Bad test status depending on amount of free space and value of this option.
Also %DiskID% and %DiskLabel% variables can be used as parameters of the actions, providing information about target drive.

See also: variables specific to Drive Free Space test

Drive Free Space (Win/UNIX: SNMP)

This test may check several drives on target system and find drive with minimum free space or drive with minimal percentage of free space (e.g. you may setup test to check all removable drives plus disk C: and F:). This version of Drive Free Space test method checks systems using SNMP requests, this allows to check non-shared resources on remote Windows or UNIX systems.
In addition to the common test parameters, Drive Free Space test has the following options:

Target host
Provide host name, IPv6 or IPv4 address (e.g. 10.10.1.55) of the system that you wish to monitor.
Optionally you may specify UDP port; port number has to be provided after a colon following the address(hostname) (e.g. 172.168.10.10**:161**).

SNMP profile
Choose profile that stores credentials necessary for communication with SNMP agent on target system. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout, Retries
Timeout - the amount of time in milliseconds the program will wait for a response from the server before the request fails.
Retries - specifies the communications retry count.
You may specify timeout and retries value in text field, type integer numbers separating values by space or colon or semicolon like "2000ms, 1" or "300,1" or "500 1"; also you may open "Connection parameters" window and choose Port, Timeout, Retries

Then you may select one or several of the following options
- **Check all local drives**
  tells HostMonitor to check all fixed drives on target system
- **Check all removable drives**
  check all removable drives on target system (not including CD/DVD drives)
- **Check listed drive(s)**
  mark this option and provide drive list when you want to check specific drive(s) on target system, e.g. C: D: E: M: or /var /dev/sda/. Note: wildcard * can be used at the end of disk name, e.g. /dev/sd*

Alert if free space less than <N> MB/GB/TB/%
When HostMonitor checks several drives it finds drive with smallest amount of free space (or drive with minimal percentage of free space when "%" alert options is selected) and sets Ok or Bad test status depending on amount of free space and value of this option.
Also %DiskID% and %DiskLabel% variables can be used as parameters of the actions, providing information about target drive.

See also: variables specific to Drive Free Space test

HDD SMART

S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) is a system included in hard drives, it provides various information regarding hard disk state and health.
Mechanical hard drive failures account for over 50% of all drive failures and most mechanical failures result from progressive wear. Usually there are certain indications that failure is imminent - these may include increased temperature, problems with reading and writing of data, increase in the number of damaged disk sectors, etc.
HostMonitor can check these parameters and warn you before catastrophic hard disk failure.
Note: usually its impossible to retrieve SMART data when HDD connected with USB or Firewire interface, also RAID controllers may monitor SMART data but do not provide SMART to upper level (OS, software).

In addition to the common test parameters, HDD SMART test offers the following options:

Basic options

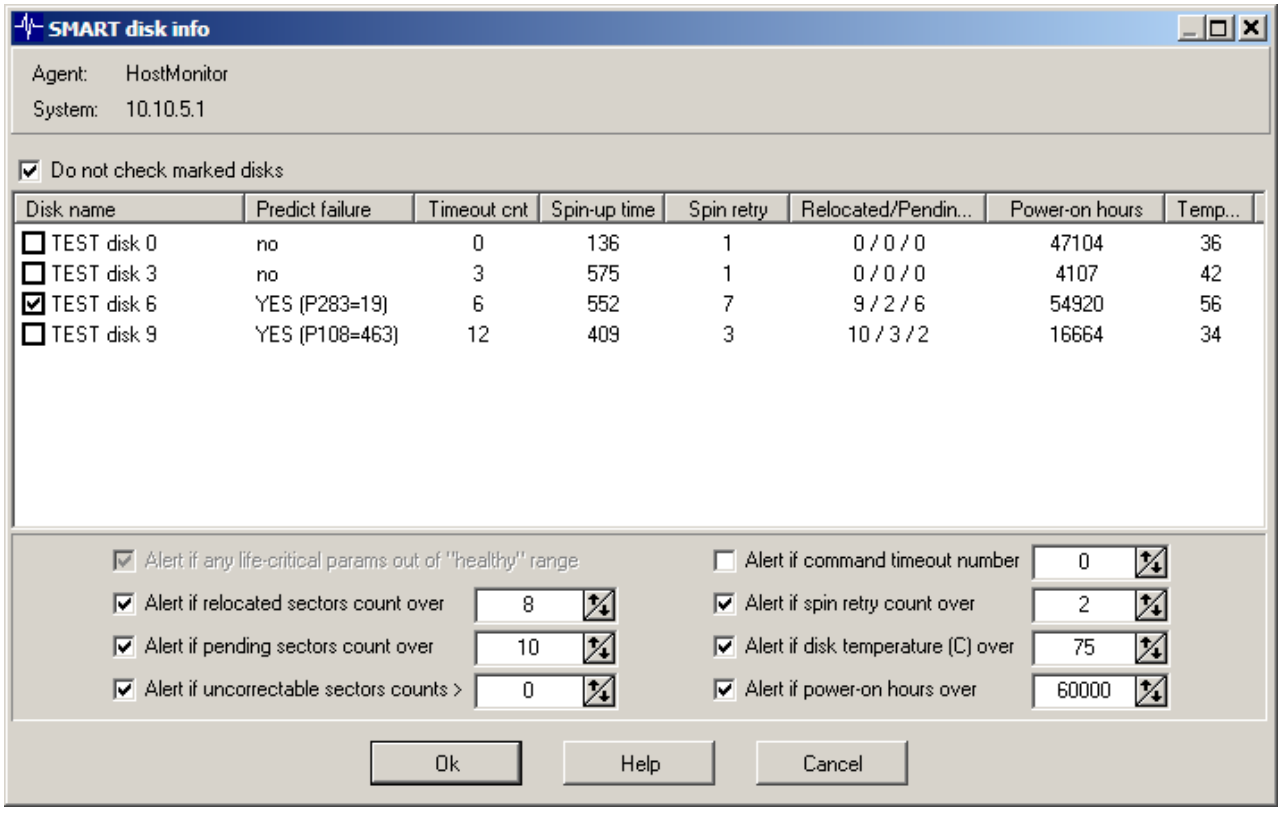
Target host
Provide the host name (e.g. mainserver) or IP address (e.g. 192.168.1.55) of the host that you wish to check. Keep this field empty or type localhost when you want to check drives on system where HostMonitor (or RMA) is running.
Note #1: Connection Manager provides one convenient place to store account information necessary to perform connections to remote systems.
Note #2: Target system should be running Windows, RPC and WMI services should be started.

Select disk with highest...
HostMonitor scans all disks that provide SMART data and checks various parameters marked by hard disk vendor as life-critical parameter. If ANY critical parameter is out of “healthy” range, HostMonitor will select this disk as “bad” - set “Bad” test status, set various macro variables using data retrieved from this hard disk, start actions specified in assigned alert profile, etc
This option tells HostMonitor which disk should be selected when all life-critical parameters on all disks within “healthy” range. In such case HostMonitor will select disk with “worst” parameter (e.g. disk with highest temperature), set macro variables but it will keep “Ok” test status so you can monitor this “worst” disk using logs or reports but no “bad” actions will be triggered.
You can choose one of the following parameters:

- Temperature (C)
- power-on hours
- read error rate
- spin-up time
- spin retry count
- # of command timeout errors
- # of relocation pending sectors
- # of relocated sectors
- # of uncorrectable errors

Extra options

Do not check marked disks
If you enable this option, you may mark some disks to exclude them from check



In addition to vendor-specific life-critical parameters you may set HostMonitor to check the following parameters and set your own “critical” threshold for each parameter.

Reallocated sectors count
Count of reallocated sectors represents a count of the bad sectors that have been found and remapped (this allows a drive with bad sectors to continue operation but affects performance). If reallocated sectors grow over time, you might encounter some serious problem.

Pending sectors count
Count of "unstable" sectors waiting to be remapped. If an unstable sector is subsequently read successfully, the sector is remapped and this value is decreased. Read errors on a sector will not remap the sector immediately (since the correct value cannot be read), instead, the drive firmware remembers sectors need to be remapped.
Some drives will not immediately remap such sectors; instead the drive will first attempt to write to the problem sector and if the write operation is successful then the sector will be marked good (in this case, the "Reallocated sectors count” will not be increased), as a result such drive may contain marginal sectors that consistently fail but the drive will never remap these problem sectors.

Uncorrectable sectors count
The total count of uncorrectable errors when reading/writing a sector. A rise in the value of this attribute indicates defects of the disk surface and/or problems in the mechanical subsystem.

Command timeout number
The count of aborted operations due to hard disk timeout. Normally this attribute value should be equal to zero and if the value is far above zero, then most likely there will be some serious problems with power supply or an oxidized data cable.

Spin retry count
Count of retry of spin start attempts. This attribute stores a total count of the spin start attempts to reach the fully operational speed (under the condition that the first attempt was unsuccessful). An increase of this attribute value is a sign of problems in the hard disk mechanical subsystem.

Disk Temperature
Current hard disk temperature (Celsius)

Power-on hours
Count of hours in power-on state. On some disks manufactured before 2005 this value may advance erratically and/or reset to zero periodically.

HostMonitor sets the following macro variables using data retrieved from selected hard disk
%DISK_NAME%
%DISK_TEMP%
%DISK_HOURS%
%DISK_RELOCATED%
%DISK_PENDING%
%DISK_UNCORRECTABLE%
%DISK_SPINUPTIME%
%DISK_SPINUPRETRIES%
%DISK_ERRORRATE%
%DISK_TIMEOUTS%
%DISK_ALERTREASON%
%DISK_ALERTVALUE%

Top Hosts may show list of "top" hard disks:
- oldest disks
- hottest disks
- worst disks – disks with highest number of relocated, pending and uncorrectable sectors

Known problems
Modern laptops and desktops (especially those running 10th-generation Intel processors or newer) ship with Intel RST (Rapid Storage Technology) / VMD (Volume Management Device) enabled in the BIOS by default. VMD acts as a hardware virtualization layer between the OS and the storage bus. It abstracts the disks so that Windows sees a unified Intel storage controller instead of individual physical NVMe/SATA drives.
If test item cannot retrieve data you may check Windows Device Manager, expand "Storage controllers" item. If you see Intel Premium Storage Indicator or Intel RST VMD Controller, the hardware configuration blocks raw passthrough.
There is no easy fix. For bare-metal machines, changing the storage controller mode in the motherboard BIOS from RAID/VMD to AHCI/NVMe natively exposes the raw disk registers to

WMI however changing this on an existing Windows installation can trigger a Blue Screen (BSOD).

Folder/File Size

HostMonitor can check folder or file size. To add this task select the test type "Folder/File Size", enter the folder name and specify a maximum size. You can manually type in the complete path to the folder that you wish to test, or click on the "Browse" button to select the folder.

If you select the option **"Include sub-folders"**, HostMonitor will calculate the size for the folder and all its sub-folders.
If you need to check some files that are dynamically created and do not have static name (e.g. some logs that are created on daily basis and have different file name every day), you may enable "**Translate macros**" options. With this option enabled you may use special date macro variables, file-specific variables and User Defined Variables in file name.

Windows tips
You can switch file scanner from typical Windows behavior to more logical behavior. For example, if you check a folder using wildcard mask like *.LOG, then Windows search will get all files with the extension .LOG, plus files with extension .LOGLOG, .LOG22, .LOG.zip, and so on. There are other weird nuances. You can switch to a more logical behavior where '?' matches a single character in a certain position, '*' matches any number of characters. In this case searching for *.LOG will only count files with the extention .LOG. In order to set HostMonitor scanning rules instead of Windows rules, add StrictMaskCheck=1 line into [Misc] section of the hostmon.ini file and restart HostMonitor.

UNIX tips
If you want to perform the test using an agent installed on UNIX-like system, you should have in mind:

- use slash (/) in the path (instead of backslash (\) that you are using on Windows systems);
- on UNIX-like systems name of the file is case sensitive (so "/etc/RMA" and "/etc/rma" are different files);
- on Windows system file masks '*' and '*.*' represent any file. On UNIX-like system only '*' represents any file; '*.*' can be used for any file that has dot (.) in the name.

See also common test parameters
See also: variables specific to file related test methods

Count Files

This test allows you to check number of files in the specified directory. Let`s say you have a mailserver that uses a spool directory. If the mail server is running correctly, it should deliver the mail within 5 minutes to the internet. Using Count Files test HostMonitor can check the number of files in the mail server`s spool directory and warn you when number of files exceed specified limit. In addition to the common test parameters, the Count Files test has the following options:

Folder
Specify the directory in which you want to count the amount of files.
File name mask
Specify file name mask. Usually mask contains wildcard characters, e.g. use '*.*' mask to count all files in the folder; use '*.eml' mask to count files with .EML extension.

If you want to perform the test using an agent installed on UNIX-like system, you should have in mind:

- use slash (/) in the path (instead of backslash (\) that you are using on Windows systems);
- on UNIX-like systems name of the file is case sensitive (so "/etc/RMA" and "/etc/rma" are different files);
- on Windows system file masks '*' and '*.*' represent any file. On UNIX-like system only '*' represents any file; '*.*' can be used for any file that has dot (.) in the name.

Translate macros
With this option enabled you can use special date macro variables and User Defined Variables in the folder name and in the file name mask.

Include sub-folders
If the option is disabled, HostMonitor will count files directly in the specified folder. If the option is enabled, files in the specified folder and in all of its descending subfolders will be counted.

Conditions to count files
Specify additional condition to count files. Choose one of the options:

- Count all files
- Count files older than NN min
- Count files newer than NN min
- Count files bigger than NN bytes
- Count files smaller than NN bytes
- Count subfolder only

Alert when folder contains more than NN files
Specify limit for the file amount. When this limit is reached, HostMonitor will change test status to "Bad". If you need to start alert actions when file amount become lower than specified, use "Reverse alert" option.

Folder/File Availability – FTP / FTPS / SFTP

HostMonitor can check for a file that MUST exist each time a test is run, or can check for a file that MUST NOT exist each time a test is run.
This test can check:
- files on local file system;
- files on shared network disk connected to HostMonitor system (using network client installed on local Windows system);
- files on system where Remote Monitoring Agent is running;
- files on shared network disk connected to the system where Remote Monitoring Agent is running;
- files on FTP and FTPS server (FTPS uses SSL);
- files on SFTP server (SFTP uses SSH protocol).

HostMonitor can check file modification time stamp, check for files that are dynamically created and so on.

In addition to the common test parameters, the Folder/File Availability test offers the following options:

File or folder name
Enter the file or folder name you wish to test (including full path, server name, protocol name).

If you check file on	path should be specified like
- local file system - or system where RMA for Windows is running;	<disk>:\<path>\<file> Examples: C:\folder\subfolder\error1.log C:\folder\log-%mmddyyyy%.txt D:\%newestfolder% D:\logs\%ddmmyy[-1d]%\%oldestfile%
- system where RMA for UNIX is running;	/<path>/<file> Examples: /var/logs/sql/ /var/logs/%newestfolder% Notes: - use slash (/) in the path (instead of backslash (\) that you are using on Windows systems); - on UNIX-like systems name of the file is case sensitive (so "/etc/RMA" and "/etc/rma" are different files); - on Windows system file masks '*' and '*.*' represent any file. On UNIX-like system only '*' represents any file; '*.*' can be used for any file that has dot (.) in the name.

- shared network disk connected to HostMonitor or Windows RMA agent	\\<hostname>\<path>\<file> Notes: - we recommend to use UNC path to the resource even if you set mapped disk drive. HostMonitor started as Windows service will not see mapped disks but will be able to check resource specified by UNC path
- SFTP server	sftp://<username>@<server>[:<port>]/<path>/<file> Examples: sftp://user1@ssh.microsoft.com:22/uploads/log.txt sftp://user1@ssh.microsoft.com:22/uploads/%oldestfile% sftp://user1@ssh.microsoft.com/uploads/%mmddyy[-1d]%
- FTP / FTPS server	ftp://<username>@<server>[:<port>]/<path>/<file> [<dateformat>] ftp**s**://<username>@<server>[:<port>]/<path>/<file> [<dateformat>] Examples: ftp://user1@microsoft.ftp.com:21/uploads/log.txt ftp://user1:pswd1@microsoft.ftp.com:21/uploads/ ftps://user1@microsoft.ftp.com:990/%newestfolder% [DMY] ftps://user1@microsoft.ftp.com/uploads/%ddmmyy% Notes: <dateformat> parameter is optional; if specified should be inside square brakets. Useful when you need to check file modification time (necessary for some servers due to limitations of FTP protocol. See details below) Available date formats: [MDY] – month, day, year, like 01/25/91 or 01-25-2005 [DMY] – day, month, year, like 25/11/91 or 25-11-2005 [YMD] – year, month, day, like 91/11/25 or 2005-11-25 [YDM] – year, day, month, like 91/25/01 or 2005-25-01

"Browse" button allows you to choose folder and file (cannot be used if you check files on FTP or SFTP servers).

Set password
HostMonitor enables this option when you check file on FTP, FTPS or SFTP server. Specify password for authentication on the server.
If you need to specify account for LAN connection, use Connection Manager.

Translate macros
If you need to check some files that are dynamically created and do not have static name (e.g. some logs that are created on daily basis and have a different file name every day), you may enable "Translate macros" options. With this option enabled you may use special date macro variables, file-specific variables and User Defined Variables in file name.

Alert when
You may set the following alert conditions:
- file doesn't exist
- file doesn't exist or older than N min
- file doesn't exist or newer than N min
- file exists
- file exists and older than N min
- file exists and newer than N min

Normally test sets Ok or Bad status. Unknown status indicates error (e.g. FTP server rejects login attempt with specified account), in such case error description will be displayed in Reply field of the test.
%FileName%, %FileSize%, %FileTime% and other variables provide file information and can be used as parameters of the actions assigned to the test.

FTP/FTPS related notes:

Unfortunately standard FTP protocol does not specify date format and does not provide a method for determining the server time zone. If you set File/Availability test to check file modification time, it can be hard to get correct time stamp of the file.
E.g.
- FTP servers that use UNIX directory structure do not include year information for files modified within the last 12 months. In such case HostMonitor appends current or last year to the file date (depending on file modification day and time). When HostMonitor system and the FTP server are in different time zones, the years may not match between December 31 and January 1; also year can be set incorrectly when the file is 1 year old (+- several hours).
- other FTP servers may provide date like 01/02/2016. Is it January 02 (USA) or February 01 (France)? In this case you may specify date format after file name, e.g.
  ftps://user1@ftp.big.com:990/%newestfolder% **[DMY]**

File Integrity

HostMonitor can check the integrity of your files and start alert actions when changes detected. This is done by calculating the CRC or MD5/SHA digest of the file and comparing it with a previously obtained value.
In addition to the common test parameters, the File Integrity test offers the following options:

File
You can manually type in the complete path and filename that you wish to monitor or click the "Browse" button to select the file
If you want to perform the test using an agent installed on UNIX-like system, you should have in mind:
- slash (/) should be used instead of backslash (\);
- on UNIX-like systems name of the file is case sensitive (so "/etc/RMA" and "/etc/rma" are different files).

Digest mode
- CRC32
- MD5
- SHA256
- SHA512

Use MD5, SHA256 or SHA512 when you need to check for unauthorized file modifications (SHA256 or SHA512 is preferred).
CRC32 can be used for legitimate modifications monitoring (not related to system security).

Hash
This field shows stored digest of the file. If you changed/updated the file, you may click "Calculate" button - the program will recalculate and store new digest.
You may setup test item using empty Hash field. In this case HostMonitor will calculate and set digest on 1st test probe. This saves your time when you need to setup tests for large files.

Recalculate Hash when file content changes are detected
With this option enabled, the new checksum will be recorded every time when changes in the file are detected, so the test will return to “Good” status until the checksum changes again.

Compare Files

You can use this test to compare two files or to search a string in the file. 6 alert conditions are available:

- alert when files are different
- alert when files are identical
- alert when 1st file contains 2nd (in any position)
- alert when 1st file does not contain 2nd
- alert when file contains a specified string

- alert when file does not contain a specified string

You can specify one or more parameters to compare files: compare time, compare size, and compare contents. If you set "compare contents" option but don't set "compare size" option, HostMonitor will consider two files to be identical when one file includes another one at offset 0 (one file can be smaller than another one).

If you need to check some files that are dynamically created and do not have static name (e.g. some logs that are created on daily basis and have different file name every day), you may enable "**Translate macros**" options. With this option enabled you may use special date macro variables, file-specific variables and User Defined Variables in file name.

When you use Compare Files test to check file for some specific string, you should tell HostMonitor what encoding was used for the file. HostMonitor supports several encoding methods:
- ASCII
- UTF-8
- UTF-16
- UTF-16 big endian
- UTF-32
- UTF-32 big endian

Note 1: file encoding
ASCII - each character represented by single byte;
UTF-8 - variable-length character encoding for Unicode;
UTF-16 - all characters in the Basic Multilingual Plane encoded by 2 bytes;
UTF-32 - each Unicode character is represented by exactly 4 bytes.

Note 2: Unicode support
HostMonitor gets information regarding current code page used on the system when you setup test item. If you check Unicode file, HostMonitor translates string to Unicode string using stored code page.

Note 3: UNIX
If you want to perform the test using an agent installed on UNIX-like system, you should have in mind:
- use slash (/) in the path (instead of backslash (\) that you are using on Windows systems);
- on UNIX-like systems name of the file is case sensitive (so "/etc/RMA" and "/etc/rma" are different files).

Also note: current version of RMA for UNIX supports ASCII encoding only. This will be improved in future version.

See also common test parameters
See also: variables specific to file related test methods

Text Log

This test is useful when you need to check log files created by another application. Unlike "Compare Files" test that warns you when any part of a file contains some specific string the Text Log test warns you only when the string is found in a NEW record. It means that if log file already has "bad' records when you started HostMonitor, you will not receive any alerts; but if any new "bad" record will be added to the log file while HostMonitor is running, you will receive a warning about the new problem. So the Text Log test works like NT Event Log test but it checks text files instead of NT Event Log Database.
In addition to the common test parameters, the Text Log test has the following options:

File
Provide name (with full path specified) of the file that has to be checked. You can manually type in the filename that you wish to monitor, or click on the "Browse" button to select the file. You may use wildcards in the name of the file (e.g. c:\logs\2004*.log), in this case 1st matched file will be checked.

Note: If you want to perform the test using an agent installed on UNIX-like system, you should have in mind:
- use slash (/) in the path (instead of backslash (\) that you are using on Windows systems);
- on UNIX-like systems name of the file is case sensitive (so "/etc/RMA" and "/etc/rma" are different files).

Translate macros
You may need this option if an application changes log file at regular intervals, e.g. daily or monthly. With this option enabled you may use special date macro variables and User Defined Variables in the file name (e.g. %dd% represents current day as a number with a leading zero 01..31)

Encoding
Use this option to tell HostMonitor what encoding is used for the file. HostMonitor supports several encoding methods:
- ASCII
- UTF-8
- UTF-16
- UTF-16 big endian
- UTF-32
- UTF-32 big endian

Note 1: file encoding
ASCII - each character represented by single byte;
UTF-8 - variable-length character encoding for Unicode;
UTF-16 - all characters in the Basic Multilingual Plane encoded by 2 bytes;
UTF-32 - each Unicode character is represented by exactly 4 bytes.

Note 2: Unicode support

HostMonitor gets information regarding current code page used on the system when you setup test item. If you check Unicode file, HostMonitor translates string to Unicode using stored code page.

Note 3: RMA for UNIX
current version of RMA for UNIX supports ASCII encoding only. This will be improved in future version.

Filters for Bad and Good records

When you setup Text Log test item, you should setup filters that separate "Bad" and "Good" records.

When HostMonitor finds new message that fits "Bad" filter conditions, it changes status of the test item to "Bad"

- Note1: here "new" means record that was recorded after last test probe.
- Note2: HostMonitor does not check records that were added while HostMonitor was not started or Text Log test item was not created yet.

When test status should be changed back to "Ok"? This behavior depends on the following options:

- **set "Ok" status when no new "Bad" records detected**
  HostMonitor will assign "Ok" status to the test item, when subsequent test probe does not detect new "Bad" event (event log does not contain new events at all or none of new events meet conditions of the "Bad" filter).

- **set "Ok" status when new "Good" records detected**
  Status of the test item will be changed to "Ok" when HostMonitor finds new event that fits "Good" filter conditions.

- **set "Ok" status by acknowledgement (manually)**
  With this option chosen, test item will remain "Bad" until operator acknowledge status (then status will be changed to Ok)

If you choose "set "Ok" status when no new "Bad" records detected" or "set "Ok" status by acknowledgement (manually)" options then "Good" filter is not used by the test item.
If you choose "set "Ok" status when new "Good" records detected" option, you should specify both ("Bad" and "Good") filters.

Filters:

There are 2 sets of conditions in the Text Log Test Properties dialog - "Bad" and "Good" filters. If some log record in the file matches neither "Bad" nor "Good" filter, record is ignored by the test item (however the same record can be processed by another Text Log test item that check the same file with different filters in use).

Both filters provide exactly the same set of options. So, let's describe the conditions for "Bad" filter:

Look for

- **string**: with this option selected HostMonitor will check records in a log file for a specified string. If new record contains specified data, HostMonitor will change status of the test to "Bad"

- **simple expression**: with this option selected HostMonitor will check log records using a boolean (logical) expression. Status of the test will be set to "Bad" when the text in the record satisfies the required conditions. In the expression you may use strings (must be concluded in quotes (') or double quotes ("")); round brackets; logical operators "and", "or", "not".
  For example: if you define expression like ('error' or 'warning') and not '16536', then HostMonitor will mark test as "Bad" when line in the log contains string 'error' or 'warning' and does not contain string '16536'

- **expression**: this mode allows to check each log record using
  - **%data%** variable (represents line from the file),
  - numbers and strings (in quotes). Strings that contain a number plus one of the following unit specificators [ms, Kb, Mb, Gb, %] are compared as numbers, so that '900 Kb' is equivalent to 921600. Also HostMonitor supports numbers in binary format, such number should contain only 0 and 1 and should be finished with 'B' character, e.g. '1110B' or '00101111B'.
  - arithmetical operators:
    div (integer division)
    mod (remainder)
    * (multiplication)
    + (addition)
    - (subtraction)
    and (bitwise and)
    or (bitwise or)
    xor (bitwise xor)
    Note: the value of (x div y) is the value of x divided by y and then rounded towards zero to the nearest integer; 'mod' operator returns the remainder obtained by dividing its operands (in other words, (x mod y) == x - (x div y) * y);
    For numbers in binary format you may use the same arithmetic operations that you are using for decimal numbers, plus you may use AND, OR and XOR operators to perform bitwise operations, e.g. ('%data%' and '010B')=='010B'
    When at least one operand of AND/OR/XOR operators specified in binary format, HostMonitor will use binary format for result as well. E.g. (6 and '11111111B') will return '110B'. If you want to convert number in binary format to decimal format, you may use addition (+), subtraction (-) or multiplication operations. E.g. '110B'+0 will return '6'.
    Note: HostMonitor always use decimal format for statistics, charts, etc.
  - relational operators are used to compare two operands
    > greater-than
    < less-than
    >= greater-than-or-equal-to

<= less-than-or-equal-to
<> inequality
== equality
not negation (one operand)

- string operators

getword	Expression like (‘string’ getword N) returns Nth word from text string counting from beginning; Example: ('40 10 50' getword 3) returns '50'
endword	Expression like (“string” endword N) returns Nth word from text string counting from end of the string Example: ('40 10 50' endword 3) returns '40'
csvfield	Retrieves field from CSV (comma-separated values) string. (‘string’ csvfield N) returns field #N. Examples: ('40,10 10,50' csvfield 2) returns '10 10' (”error 5”,”10,1,2”,10,50' csvfield 2) returns '10,1,2'
tsvfield	Retrieves field from TSV (tab-separated values) string. Works similar to csvfield command. (‘string’ tsvfield N) returns field #N.
getnumberwithdot	Usage <string> getnumberwithdot <num> This operator ignores all words and characters within <string> except integer numbers and numbers with the period, returns number #num and then replaces the period character with system decimal separator (so it may replace the period with comma when system decimal separator is the comma). Example ('wordA wordB 21.10,15.00' getnumberwithdot 2)=='15.00' ('wordA wordB 21 15.00' getnumberwithdot 2)=='15.00' ('15.00' will be replaced with '15,00' when system decimal separator is comma)
getnumberwithcomma	Usage <string> getnumberwithcomma <num> This operator ignores all words and characters within <string> except integer numbers and numbers with comma, returns number #num and then replaces comma with system decimal separator (so it may replace comma with the period when system decimal separator is the period). Example ('wordA wordB 21.10,15.00' getnumberwithcomma 2)=='10,15' ('wordA wordB 21 15.00' getnumberwithcomma 2)=='15' ('10,15' will be replaced with '15.10' when system decimal separator is the period)
getnumber	Usage <string> getnumber <num> This operator ignores all words and symbols within <string>

except integer numbers, returns number #num
('wordA wordB 21.10,15.00' getnumber 2)=='10'
('wordA wordB 21 15.00' getnumber 2)=='15'

Samples:

('%data%' csvfield 2) + ('%data%' csvfield 4) > 100
('%data%' tsvfield 2 > 50) and ('%data%' tsvfield 4 > 160)
('%data%' getword 1 == 'error') and ('%data%' getnumber 1 >= 500)

Note: "string" mode is the fastest one; "expression" mode the slowest

Options:

Case sensitive

With this option enabled search is case sensitive

Whole words only

Search for the whole words only. With this option disabled, the search string might be found as a part of a word.

Macros

With this option enabled you may use global (user defined) and date&time macro variables in the "look for" string/expression

Scanning mode

Warn of last new event

With this option enabled HostMonitor will scan (starting from the end of the log file) all events that were added into a log file since after the previous test. When the test finds the first "Bad" new record the test receives "Bad" status and HostMonitor performs specified alert action if it was specified. For example: if HostMonitor performs test every 10 minutes and 3 "Bad" events occurred within this time interval, HostMonitor will report only about the last one (because it scans starting from the end of file). This option is useful when you check for some specific event and don't need many messages about the same recurring error.

Warn of all new events

In opposite to previous mode, with this option enabled HostMonitor will inform you about each event that satisfies specified requirements. This option is useful when you use one test item to check for different error events (usually you will use "Repeat: until status changes" option for appropriate alert actions).

Consider, for example, there are 3 new records were added into log file: “bad”, “bad” and “good”. If all 3 records were added within short time interval (between 2 consecutive test probes), how the monitor behaves depending on test settings?

Used options	- Set "Ok" status when no new "Bad" records detected - Warn of last new event
Behavior	1) HostMonitor sets "Bad" status because there is "Bad" event detected; increments or resets Recurrences counter (depending on previous test status); if necessary, starts actions assigned to the test item (depending on action settings)
Used options	- Set "Ok" status when no new "Bad" records detected - Warn of all new events
Behavior	1) HostMonitor sets "Bad" status; increments or resets Recurrences counter (depending on previous test status); if necessary, starts actions assigned to the test (depending on action settings) 2) HostMonitor keeps "Bad" status, increments Recurrences counter because 2nd "Bad" event detected; starts actions if necessary
Used options	- Set "Ok" status when new "Good" records detected - Warn of last new event
Behavior	1) HostMonitor sets "Ok" status because last event fits "good" filter; increments or resets Recurrences counter (depending on previous test status); starts actions assigned to the test if necessary (depending on action settings)
Used options	- Set "Ok" status when new "Good" records detected - Warn of all new events
Behavior	1) HostMonitor sets "Bad" status; increments or resets Recurrences counter (depending on previous test status); if necessary, starts actions assigned to the test item (depending on action settings) 2) HostMonitor keeps "Bad" status, increments Recurrences counter because 2nd "Bad" event detected; starts actions if necessary 3) HostMonitor sets "Ok" status, resets Recurrences counter and starts actions if necessary

Info to display

Display
Specifies what information HostMonitor should display in the reply field of the test item when the "bad" (or the “good”) record is detected in the log file:

- found line
- offset of the found string in the file
- file size

Filter
When you chose "found line" mode you may apply additional filter to the select part of the line to display:

- display whole line
- display word #N
- display word #N counting from the end of line
- display text from word #N1 till word #N2
- display text from pos #N1 till pos #N2

Words separated by
This option allows you to choose word separator:

- space or tabs
- tabs
- comma
- semicolon

See also: Tune up Reply option
See also: variables specific to file related test methods

Process (Windows RPC / WinRM)

A process, in the simplest terms, is an executing program. HostMonitor can control specified process on local or remote computer and start alert actions if number of instances of the specified process is out of the defined range. To monitor processes on a remote computer you should use account from Performance Monitor or Administrators group.

This test method can check processes on Windows systems using RPC calls. Also you may check processes on Windows and UNIX systems using SNMP protocol, see Process (SNMP)

Since version 15.80 this test method also supports WinRM mode. If you want to use the WinRM protocol for such tests, you should create an entry using the WinRM page of the Connection Manager.

In addition to the common test parameters the Process test has the following options:

Computer name
Specify name of the target computer (the target computer name must be prefixed by "\\"), or select the "<local computer>" item. You can use the "Browse network" button to select a computer from the list.

Process
Type name of the process to check, or select a process from the drop-down list. Also select lower and/or upper limit amount of running instances of the specified process, when the limit is reached HostMonitor will mark the test status as Bad.

Connect as
To check process on remote Windows system you can mark this option and provide a user name and a password for a connection to the target computer. On the other hand, we recommend using the Connection Manager that provides one convenient place to store account information necessary to perform connections to remote systems.
This option disables WinRM mode for the test

Note #1 (Windows): make sure you have RPC and Remote Registry services started on the remote system. Windows NT 4.0 does not have this service installed by default, however you can find this service in the Resource Kit for Windows NT 4.0.

Note #2 (UNIX): To check UNIX systems you may use Remote Monitoring Agent installed on UNIX-machine (RMA for UNIX does not use "Computer" and "Connect as" parameters of the test and checks the system where agent is running). Also you may use Process (SNMP) test, this test method can check processes on remote Windows and UNIX systems using SNMP requests.

See also:
- Dominant Process test method
- Process Meter application

Process (Win/UNIX: SNMP)

HostMonitor can check processes on local or remote Windows and UNIX systems (Linux, FreeBSD, etc) using SNMP protocol.
In addition to the common test parameters the Process(SNMP) test has the following options:

Computer name
Provide host name, IPv6 or IPv4 address (e.g. 10.10.1.55) of the system that you wish to monitor.
Optionally you may specify UDP port; port number has to be provided after a colon following the address(hostname) (e.g. 172.168.10.10**:161**).

Process
Type name of the process to check, or select a process from the drop-down list. Also select lower and/or upper limit amount of running instances of the specified process, when the limit is reached HostMonitor will mark the test status as Bad.

SNMP profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

See also:
- Dominant Process test method
- Process Meter application

Service

Microsoft Windows NT* supports an application type known as a service. It can be started automatically at system boot, by a user through the Services control panel applet, or by an application that uses the service functions. Services can execute even when no user is logged on to the system.
* Here "Windows NT" means Windows system based on NT technology, including Microsoft Windows NT 4.0, Windows 2000/XP, Windows Vista, Windows 7-11, Windows Server 2003-2022.

Since version 15.80 this test method also supports WinRM mode. If you want to use the WinRM protocol for such tests, you should create an entry using the WinRM page of the Connection Manager.

In addition to the common test parameters the Service test has the following options:

Target host
Specify name (or IP address) of the target Windows system (name must be prefixed by "\\"), or select the "<local computer>" item. You can use the "Browse network" button to select a computer from the list.

Service test may work in 3 modes:

Alert when service not started
HostMonitor checks specific service state. If the service is not Running, HostMonitor will set Bad status and start the specified alert actions.
You may type name of the service to check, or select a service from the drop-down list. Note: when you setup NEW Service test item, you may specify several services; in such case HostMonitor will create separate test item for each selected Windows service.

Alert when service not started or does not respond
This mode used by default. HostMonitor checks service state and responsiveness. If the service has not been started or the service does not answer, HostMonitor will set Bad status and start the specified alert actions.
You may type name of the service to check, or select a service from the drop-down list.
Note 1: when you setup NEW Service test item, you may specify several services; in such case HostMonitor will create separate test item for each selected Windows service.
Note 2: WinRM protocol cannot be used for this mode.

Alert when some "Auto" services not running
HostMonitor will get list of ALL services with Automatic startup type and check state of each service. If some "auto" service is not running, HostMonitor will set Bad test status. You may specify comma separated list of the services that should not be checked, e.g. `MMCSS,sppsvc,UxSms`; you may use * wildcard at the end of the name, e.g. `clr*,spp*`

You may open "Choose service to monitor" dialog that displays list of all services on target system. It shows service name (short name), its long name, service status and type of the service. Also you may setup filters:
- Show running service
- Show stopped services
- Show running and stopped services
- Show 'Auto' services
- Show stopped 'Auto' services

Connect as
To check service on a remote system you can mark this option and provide a username and a password for a connection to the target computer. On the other hand, we recommend using the Connection Manager that provides one convenient place to store account information necessary to perform connections to remote systems.
Note: this option disables WinRM mode for the test

See also: variables specific to Service test

NT Events Log

Event logging in Microsoft Windows provides a standard, centralized way for applications (and the operating system) to record important software and hardware events. The event-logging service stores events from various sources in a single collection called an event log. HostMonitor can check this log and start alert actions if some specific events occur.
In addition to the common test parameters the NT Events Log test has the following options:

Compatibility
For each test item you may choose "Windows NT API" or "Windows Vista+ API" mode. If HostMonitor is started on Windows Vista, Windows 7-11, Windows Server 2008-2022 and target host uses one of these operational systems as well, we recommend using "Windows Vista API" mode. Otherwise you should use "Windows NT API" mode that works fine for Windows 2000, Windows XP and Windows Server 2003 as well.
Note: if you switch mode for existing test, HostMonitor will consider such modified test as new item and ignore “old” events.

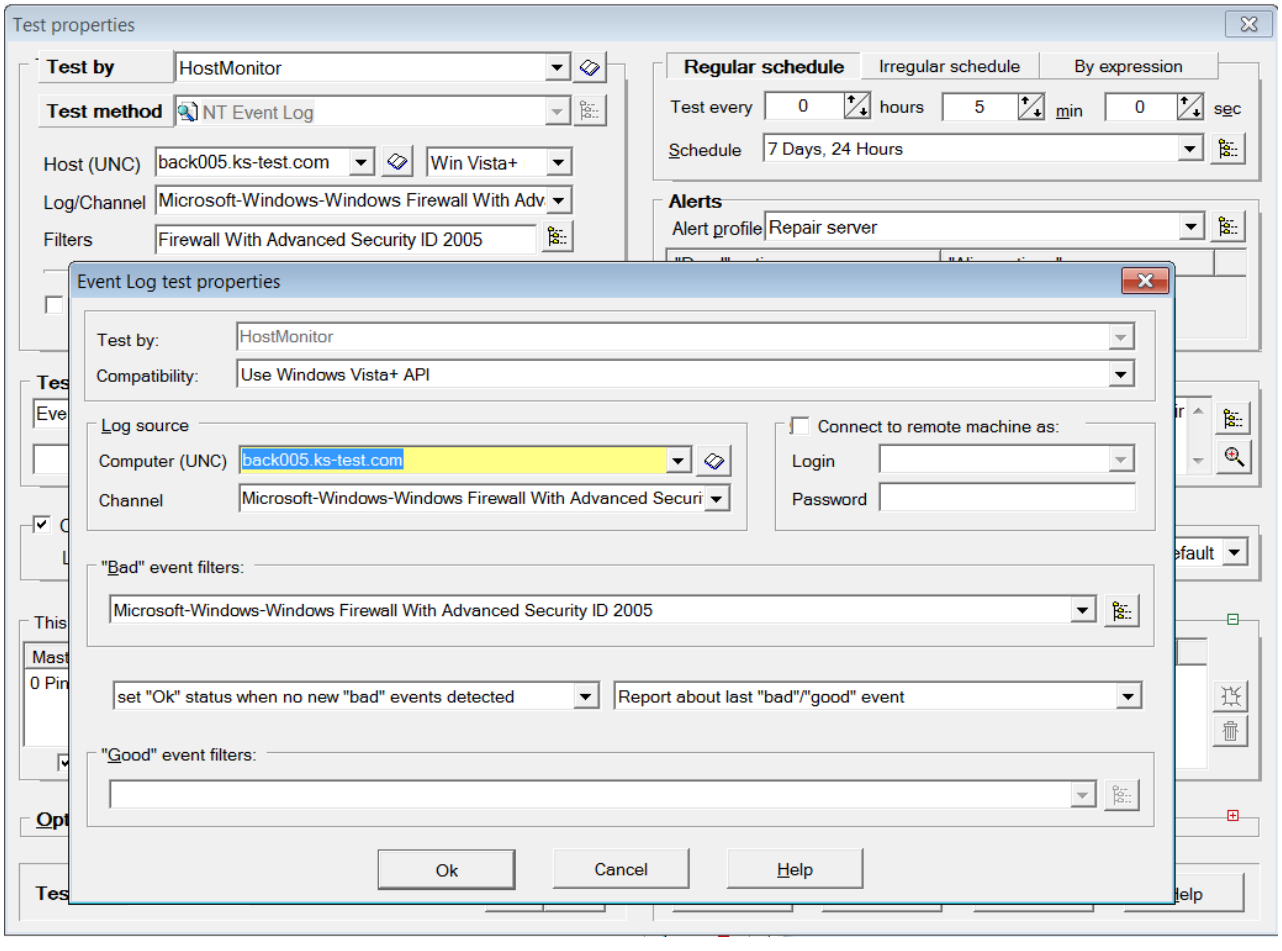
Computer
The Universal Naming Convention (UNC) name of the server on which the event log is to be opened (the target computer name must be prefixed by "\\"). Type the UNC or select the "<local computer>" item, also you can use the "Browse network" button to select a computer from the list.

Event Log (Channel)
Provide name of the event log that will be checked by HostMonitor. This can be the Application, Security, or System log, or a custom registered log.
Note: “Log” vs. “Channel”
Starting from Windows Vista, events use the concept of “event channels” instead of “event logs” used for downlevel platforms. From HostMonitor’s “poing of view” channels and logs are interchangeable. The Windows Vista/2008 backwards compatibility logs are named the same as they were on downlevel platforms (Application, Security, etc).
The only tricky thing to note about the channels in Vista/Server 2008 is that the folder structure in the Windows Event Viewer application does not necessarily match correct channel name (Windows Event Viewer changes channel names to present them in nicer form).

Connect as
To check an Event Log on the remote system you can mark this option and provide a username and a password for a connection to the target computer.

Filter profiles

Then you should select “bad” filters profile and optionally “good” filters profile. Each profile may have one or more filter records and each filter record sets one or more conditions to check. Event passes the filter only when it matches **ALL** specified requirements of the filter; when event passes **ANY** filter within selected filter profile, its counted by the test.
If some event matches neither “Bad” nor “Good” filter, event is ignored by the test item (however the same event can be processed by another NT Events Log test item with different filters in use).



When HostMonitor finds new* message that fits “Bad” filter conditions, it changes status of the test item to “Bad”

- Note1: here “new” means event was recorded after last test probe.
- Note2: HostMonitor does not check event log records that were added while HostMonitor was not started or NT Events Log test item was not created yet.

Bad/Ok modes

When test status should be changed back to “Ok”? This behavior depends on the following options:

- **set "Ok" status when no new "Bad" events detected**
  HostMonitor will assign “Ok” status to the test item, when subsequent test probe does not detect new* “Bad” event (event log does not contain new events at all or none of new events meet conditions of the “Bad” filter).

- **set "Ok" status when new “Good” event detected**
  Status of the test item will be changed to “Ok” when HostMonitor finds new event that fits “Good” filter conditions.

- **set “Ok” status by acknowledgement (manually)**
  With this option chosen, test item will remain “Bad” until operator acknowledge status (then status will be changed to Ok)

If you choose “set "Ok" status when no new "Bad" events detected” or “set “Ok” status by acknowledgement (manually)” options then “Good” filter is not used by the test item.
If you choose “set "Ok" status when new “Good” event detected” option, you should specify both (“Bad” and “Good”) filters.

Report modes

Report about last “Bad”/”Good” event
With this option enabled HostMonitor will scan (starting from the end of the log) all new* events till first** “Bad” event. If new “Bad” event is detected, HostMonitor marks test as “Bad” and may perform specified alert actions (if necessary). This option is useful when you check for some specific event and you don’t need many messages about the same recurring error.
**Note: here “first” means the most recent (last) “Bad” event as monitor scans the log from the end

Report about all events
In opposite to previous mode, with this option enabled HostMonitor will inform you about each event that satisfies specified requirements (filters). This option is useful when you use one test item to check for different error events (e.g. you are checking for any event with “Failure Audit” type).
Note: you may need to use “Repeat: until status changes” option for associated alert actions.

Consider, for example, there are 3 new events were added into NT Event Log: “bad”, “bad and “good”. If all 3 events were added within short time interval (between 2 consecutive test probes), how the monitor behaves depending on test settings?

Used options	- Set "Ok" status when no new "Bad" events detected - Report about last “Bad”/”Good” event

1) HostMonitor sets “Bad” status because there is “Bad” event detected;

Behavior	increments or resets Recurrences counter (depending on previous test status); if necessary, starts actions assigned to the test item (depending on action settings)
Used options	- Set "Ok" status when no new "Bad" events detected - Report about all events
Behavior	1) HostMonitor sets “Bad” status; increments or resets Recurrences counter (depending on previous test status); if necessary, starts actions assigned to the test (depending on action settings) 2) HostMonitor keeps “Bad” status, increments Recurrences counter because 2nd “Bad” event detected; starts actions if necessary
Used options	- Set "Ok" status when new “Good” event detected - Report about last “Bad”/”Good” event
Behavior	1) HostMonitor sets “Ok” status because last event fits “good” filter; increments or resets Recurrences counter (depending on previous test status); starts actions assigned to the test if necessary (depending on action settings)
Used options	- Set "Ok" status when new “Good” event detected - Report about all events
Behavior	1) HostMonitor sets “Bad” status; increments or resets Recurrences counter (depending on previous test status); if necessary, starts actions assigned to the test item (depending on action settings) 2) HostMonitor keeps “Bad” status, increments Recurrences counter because 2nd “Bad” event detected; starts actions if necessary 3) HostMonitor sets “Ok” status, resets Recurrences counter and starts actions if necessary

Report about last event but count ALL

This option works similar to “Report about last Bad/Good event” option, however it counts all new events that fit “bad” filter (and “good” filter if specified). If “Show events description in Reply field for NT Event Log test” option is disabled (Options dialog) then test will display number of detected “bad” events in Reply field of the test.

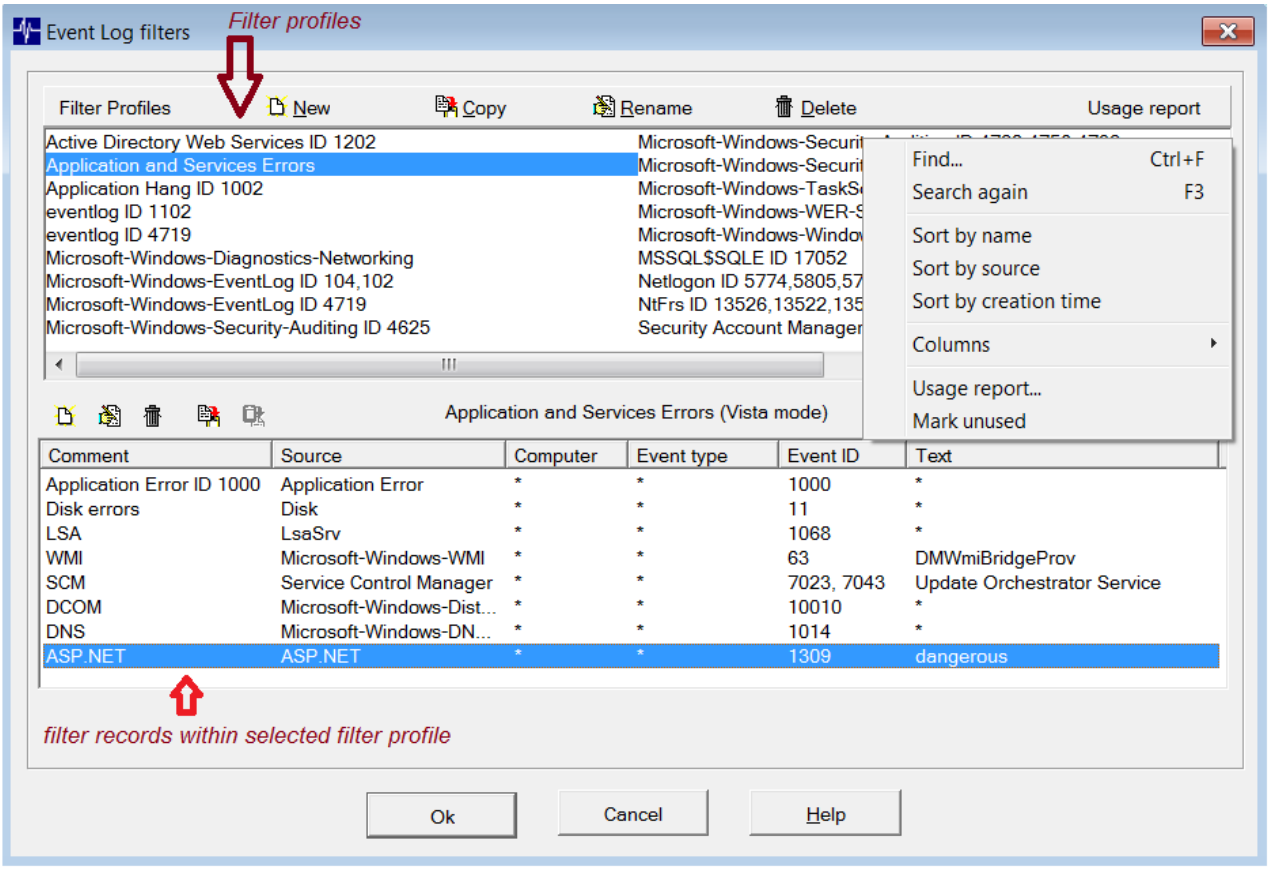
Also you may use %NTEvents_BadCnt% and %NTEvents_GoodCnt% variables for Optional status processing, actions or Custom HTML reports (regardless of “Show events description” option).

E.g.

- you may set Set Normal status if %NTEvents_BadCnt%<5 test option. This way HostMonitor will set Normal test status when there are NEW “bad” records in Event Log but number of such records below 5.
- or you may set Tune up Reply value, Reply = [%NTEvents_BadCnt%] test option, this way HostMonitor will display number of new “bad” events in Reply field of the test even if “Show events description” option” is enabled

Filters:

Each filter profile may have one or more filter records and each filter record sets one or more conditions to check. Event passes the filter only when it matches **ALL** specified requirements of the filter; when event passes **ANY** filter within selected filter profile, its counted by the test.



NOTE: All filter records within one profile should be related to the same event log (channel).

Copy/Paste – these buttons allow to copy filter record from one profile to another.
Find/SearchAgain - scan for specified text within profile name and within filter record properties (comment, source, computer names, event IDs, text).
Usage report - this option shows usage report for selected profile (list of test items that use selected profile).
Mark unused - if you enable this option, profiles that are not currently in use will be displayed in grey color and software will not ask confirmation when you want to remove such profiles.
Also you may sort profiles, set number of columns in the list.

Each filter record offers the following settings

Comment
Any text that can be useful for you or another administrator

Event Source (Publisher)
Select the source of events (application, service, driver, subsystem). You may specify event source using * as wildcard at the end of the string. E.g. if you type "MsExchange*", HostMonitor will check for events produced by "MsExchangeIS", "MSExhange ActiveSync", "MSExchange ADAccess", etc

Computer
Match against the computer that added the entry to the event log. You can provide list of the computers and choose one of the options:

- Any	name of the computer doesn't matter (event from any computer can be* considered as "Bad/Good")
- Any from the following	event can be* considered as "Bad/Good" when computer (that added the entry to the log) is specified in the list
- Any except the following	event can be* considered as "Bad/Good" when computer (that added the entry to the log) is not specified in the list

Note: to add a new line to the end of the list go to the last existing line and press Down Arrow button. Press INSERT button to insert new item. Press CTRL+DEL to remove item. Press F2 to edit item.

Event type / Event level
Match against the event type. Here you may choose "Any" option to skip this filter (any type of events can be considered as "Bad/Good") or choose "Any from the following" mode and then mark one or several items from the list.
When you use "Windows NT API" compatibility mode, you may mark one or several possible event types: Error, Warning, Information, Success Audit, and Failure Audit.
When you use "Windows Vista+ API" compatibility mode, you should choose one or several event levels: Audit, Critical, Error, Warning, Info and Verbose

Event ID
Match against the event ID (event ID is specific to the software that generated the event log entry). You can provide list of the ID codes and choose one of the options:

- Any	ID doesn't matter (event with any ID can be* considered as "Bad/Good")
- Any from the following	event can be* considered as "Bad/Good" when ID is specified in the list
- Any except the following	event can be* considered as "Bad/Good" when ID is not specified in the list

Description contains
Match against the event description. You can provide list of the text strings (phrases) and choose one of the options:

- Any text	event description doesn't matter (event with any description can be* considered as "Bad/Good")
- Any string from the list	event can be* considered as "Bad/Good" when description contains ANY string from the list
- Nothing from the list	event can be* considered as "Bad/Good" when description does not contain ANY string from the list
- All strings from the list	event can be* considered as "Bad/Good" when description contains ALL strings from the list

Note: to add a new line to the end of the list go to the last existing line and press Down Arrow button. Press INSERT button to insert new item. Press CTRL+DEL to remove item. Press F2 to edit item.

* Here “can be” means event WILL BE considered as “Bad/Good” WHEN IT MATCHES ALL specified requirements

Note: there are variables that provide information about current and previous detected event.

Known problems

3rd party DLLs version mismatch in Windows NT mode

When HostMonitor calls Windows API to format event description, Windows does not check the accordance between the number of variables in a template (that is stored in resource file) and the number of variables stored in an event log. This could lead to access violation errors when some software was installed or updated incorrectly (e.g. version mismatch between different DLLs).
HostMonitor checks the template (retrieved from the DLL) and verifies the number of insertion strings before calling Windows API. If problem detected, HostMonitor shows "Not enough insertion data for the message <dllname>" error in Reply field of the test.

Solution:
If there is DLLs version mismatch (described above), you may copy appropriate DLL (e.g. copy file from another system) into <HostMonitor>\EventLogDlls\ directory. If HostMonitor detects DLL in EventLogDlls subdirectory, this DLL will be used instead of installed DLL (installed DLL - DLL that is specified in the system registry under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\<log name>\<event source name> key).

Bugs in Windows Crypt32.DLL

There are some bugs in crypt32.dll that comes with Microsoft Windows Vista (including Service Pack 1 and 2) and Microsoft Windows Server 2008 (including Service Pack 2). According to Microsoft this may lead to application crash. We added some code to HostMonitor and RMA that should prevent application crash however some options will not work correctly on Windows Vista and Windows Server 2008.

Solution:
Looks like Microsoft fixed this problem in Windows 7. Also Microsoft provides hot fix for Windows Vista and Windows Server 2008: http://support.microsoft.com/kb/982416. Unfortunately this fix does not correct all problems related to this DLL.

CPU Usage

CPU Usage test checks the percentage of CPU utilization on the local or remote machine. This test method can monitor various systems and devices: Windows, Linux, AIX, FreeBSD, Cisco, etc.
In addition to the common test parameters the CPU Usage test has the following options:

Host[:port]
- Provide the host name, FQDN, UNC name (Universal Naming Convention), or IP address (e.g. 192.168.1.55) of the host that you wish to monitor.
- Type localhost when you want to check system where RMA agent is running ("Test by" property should point to this agent).
- Also you may type <local computer> or keep empty string when using the test for a local machine where HostMonitor is running.
- Specify a server name or NDS tree name (like ".bigcompany.ifx.department2.sever1") when using this test for Novell Netware server.

When SNMP protocol is used (see below), you may specify UDP port that is used by SNMP agent running on the target system. This parameter is optional; port number has to be provided after a colon following the target host address (e.g. 10.10.15.201**:161**).

OS (protocol)
Select the type of OS on the target host and prefered protocol (e.g. HostMonitor may check Windows systems using RPC or SNMP requests).

Windows (RPC / WinRM)	Target OS: Microsoft Windows NT 4.0, Windows 2000/XP, Windows Vista, Windows 7-11, Windows Server 2003-2022. In order to monitor CPU utilization on a remote Windows system, please make sure you have the RPC service and Remote Registry service started on the remote system. (Windows NT 4.0 does not have this service installed by default, however you can find this service in the Resource Kit for Windows NT 4.0) Since version 15.80 this test method also supports WinRM mode. If you want to use the WinRM protocol for such tests, you should create an entry using the WinRM page of the Connection Manager. **Connect as** In some cases you need to provide credentials for connection to the target system (e.g. system does not belong to the domain). You may use Connection Manager or you may provide a user name and password using this option. To monitor processes on a remote Windows system you should use account from "Performance Monitor" or "Administrators" group. Note: this option disables WinRM mode for the test
Novell Netware	Target OS: Novell Netware 4+ In this case HostMonitor uses the functionality of the Novell Netware client, therefore the Novell Netware client software has to

	be installed on the machine where HostMonitor is running. Note: this mode kept for backward compatibility, it was not tested recently.
UNIX (local RMA)	Target OS: Linux, FreeBSD, NetBSD, OpenBSD, Solaris, MacOS, AIX In this case HostMonitor sends request to Remote Monitoring Agent installed on target UNIX-machine. Agent name should be selected in "Test by" field.
UNIX (SNMP)	Target OS: Linux, FreeBSD, NetBSD, Solaris, AIX, ESXi and other HostMonitor checks the average of the percentage of time that CPU was not idle over the last minute. Different systems have different implementation related to CPU load statistics, may approximate this one minute smoothing period (on Linux system load <> CPU load). Test offers option to check either: - **average/cores** - checks all CPU cores, calculates average load - **max usage core** - finds CPU core with highest load Example: if system has 2 CPU cores with 90% load on 1st core and 10% load on 2nd core then average/cores=50%; max_usage_core=90%
Windows (SNMP)	Target OS: Microsoft Windows 2000/XP/2003, Windows 7-11, Windows Server 2008-2022. Test offers option to check either: - **average/cores** - checks all CPU cores, calculates average load - **max usage core** - finds CPU core with highest load Example: if system has 2 CPU cores with 90% load on 1st core and 10% load on 2nd core then average/cores=50%; max_usage_core=90%
Cisco	Target: Cisco IOS (software used on most Cisco routers and network switches). CPU Usage in this case is one minute exponentially-decayed moving average value
Juniper	Target: Junos OS (operating system used in Juniper Networks hardware routers). Here you may choose test mode: **check FPC,RE** modules or Packet Forwarding Engine modules (**SPU mode**). In any case HostMonitor will find module with highest CPU load
NetApp	Target: NetApp storage devices
QNAP	Target: QNAP storage devices
SonicWall	Target: SonicWall network devices
Synology	Target: Synology storage devices Test offers option to check either: - **average/cores** - checks all CPU cores, calculates average load

	- **max usage core** - finds CPU core with highest load Example: if system has 2 CPU cores with 90% load on 1st core and 10% load on 2nd core then average/cores=50%; max_usage_core=90%

Alert when CPU usage over N%
HostMonitor will set Bad test status and start specified alert actions when the percentage of CPU usage exceeds specified limit

The following parameters should be specified when SNMP protocol is used.

SNMP profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.

Timeout
This is the amount of time in miliseconds the program will wait for a response from the server before the request fails

Retries
Specifies the communications retry count

Memory

Memory test can check amount of free physical and virtual memory, size of unused swap space (page file) on local or remote Windows, Linux, BSD systems, Cisco routers and some other network devices.

In addition to the common test parameters, Memory test has the following options:

Protocol
HostMonitor can use 3 different protocols and several algorithms in order to retrieve data from remote systems. You may choose one of the following protocols:
- SNMP
- WMI / WinRM

WMI is an acronym for **W**indows **M**anagement **I**nstrumentation. WMI is the Microsoft's implementation of Web-Based Enterprise Management (WBEM)
System requirements:
- Windows 2000, XP and newer versions have the WMI components pre-installed:
- Windows 95, 98, and Windows NT 4.0 do not have WMI components preinstalled. The WMI Core software package for Windows 95/NT4 was available at Microsoft's web site but its not supported anymore.

WinRM: this test method also supports WinRM mode. If you want to use the WinRM protocol for such tests, you should create an entry using the WinRM page of the Connection Manager.

SNMP
The Simple Network Management Protocol is the Internet standard protocol for exchanging management information between management console applications and managed entities. It works faster and requires less resources than WMI; also using this protocol you may retrieve information from Windows, Linux, BSD systems, Cisco routers and other SNMP enabled devices.

Host
Provide the host name (e.g. mainserver) or IP address (e.g. 192.168.1.55) of the host that you wish to monitor. Type localhost when you want to check system where HostMonitor (or RMA) is running.
When SNMP protocol selected, you may specify UDP port that is used by target SNMP agent. This parameter is optional; port number has to be provided after a colon following the address of SNMP agent (e.g. 195.168.10.10**:161**).

If you prefer to use WMI protocol for Memory test, use Connection Manager to provide account information necessary to perform connections to remote systems.

If you chose SNMP protocol then you need to select SNMP Profile:

SNMP profile

Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.

Timeout
This is the amount of time in miliseconds the program will wait for a response from the server before the request fails (used for SNMP protocol only).
Retries
Specifies the communications retry count (used for SNMP protocol only)

Alert when
The following options allow you to choose what kind of memory should be monitored and when test status should be changed from Ok to Bad.

- **Free physical memory**
  Amount of physical memory in bytes available to processes running on the computer.
  Note: Linux and Windows may use most of free physical memory as disk cache, HostMonitor consider this cache as free memory because it can be assigned to processes without delay.

- **Free swap memory**
  Amount of swap space (page file) currently available (reserved but not used). If the paging file(s) are expanded, this limit increases accordingly.
  Note: this value cannot be retrieved if you are using SNMP protocol for Windows.

- **Free virtual memory**
  Total amount of free memory: free physical memory plus unused space of page file. If the paging file(s) are expanded, this limit increases accordingly.

You may tell HostMonitor to set Bad test status and start assigned actions when amount of free memory falls below specific limit (e.g below 1024 MB) or specific percentage (e.g. below 30%).

Known problems
HostMonitor uses different protocols and algorithms to make sure retrieved information is correct. We tested dozens of systems however there are hundreds different versions of Unix systems, for some of them test will not work correctly (e.g. we do not understand how to get correct data from FreeBSD 9.0 – sometimes even system utilities show information that does not make any sense; on Ubuntu 11.04 SNMP agent provides data that does not correlate with meminfo data).
In such case you may use alternative methods, like Shell Script test method performed by RMA for Unix

Performance Counter

Performance Counter test allows you to monitor specific aspects of work performed on local or remote computer by a system or a service. You can monitor a lot of important parameters of the system, such as:

Counter	Description
Processor\% Processor Time	% Processor Time is the percentage of time that the processor is executing a non-Idle thread
Processor\% Interrupt Time	% Interrupt Time is the percentage of time the processor spent receiving and servicing hardware interrupts during the sample interval
Processor\Interrupts/sec	Interrupts/sec is the average number of hardware interrupts the processor is receiving and servicing in each second
System\Processes	Processes is the number of processes in the computer at the time of data collection.
TCP\Connections Established	Connections Established is the number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
TCP\Segments/sec	Segments/sec is the rate at which TCP segments are sent or received using the TCP protocol.
Process\% Processor Time	% Processor Time is the percentage of elapsed time that all of the threads of specified process used the processor to execute instructions.
Process\Handle Count	The total number of handles currently open by specified process.
Printer Queue\Jobs	Current number of jobs in a print queue.
PhysicalDisk\% Disk Time	% Disk Time is the percentage of elapsed time that the selected disk drive is busy servicing read or write requests.
PhysicalDisk\Current Disk Queue Length	Current Disk Queue Length is the number of requests outstanding on the disk at the time the performance data is collected
Memory\Available Bytes	Available Bytes is the amount of physical memory available to processes running on the computer, in bytes.
NetworkInterface\Current Bandwidth	Current Bandwidth is an estimate of the interface current bandwidth in bits per second (BPS).

and much more…

To create Performance Counter test you need to define just 3 parameters (of course in addition to the common test parameters):

Performance Counter
Type name of the counter to monitor or use browse button to explore all performance counters available on the system.
Note: Each counter is uniquely identified through its name and its *path*, or location. In the same way that a file path includes drives, directories, subdirectories, and file names, a counter path consists of four elements: the machine, the object, the object instance, and the counter name.

The syntax of a counter path is:
\\Machine\PerfObject(ParentInstance/ObjectInstance#InstanceIndex)\Counter

Condition for alert

HostMonitor can compare value of the counter with a specified number and start alert actions if the returned value is:

- less than the specified value
- more than the specified value
- equal to the specified number
- different from the specified number

Also HostMonitor has 9 alert conditions to check how new value changes comparatively to the previous test results:

"increases by"	- HM sets "Bad" status when value increases by specified number or more
"decreases by"	- HM sets "Bad" status when value decreases by specified number or more
"changes by"	- HM sets "Bad" status when value changes by specified number or more
"increases by (%)"	- HM sets "Bad" status when value increases by specified (or greater) percentage
"decreases by (%)"	- HM sets "Bad" status when value decreases by specified (or greater) percentage
"changes by (%)"	- HM sets "Bad" status when value changes by specified (or greater) percentage
"increases /sec"	- HM sets "Bad" status when average increase of the counter (per second) is greater than the specified limit ((new value - old value)/elapsed time >= specified limit)
"decreases /sec"	- HM sets "Bad" status when average decrease of the counter (per second) is greater than the specified limit ((old value - new value)/elapsed time >= specified limit)
"changes /sec"	- HM sets "Bad" status when average change of the counter (per second) is greater than the specified limit (abs(new value - old value)/elapsed time >= specified limit)

HostMonitor can set status of the test to “Unknown” in case it cannot retrieve performance counter value (e.g. unable to connect to the remote machine or the specified counter could not be found). You can use “Treat Unknown status as Bad” option. With this option enabled, if test results cannot be obtained, actions are triggered by HostMonitor the same way as if the test returned a "Bad" status.

Display mode

This parameter defines information display method. You can select one of the following options:

as is	- do not perform any conversion
sec -> [days] hh:mm:ss	- converts received value in seconds to a "[days] hh:mm:ss" format
msec-> [days] hh:mm:ss	- converts received value in milliseconds to a "[days] hh:mm:ss" format
bytes -> Kb	- converts received value in bytes to kilobytes
bytes -> Mb	- converts received value in bytes to megabytes
bytes -> Gb	- converts received value in bytes to gigabytes

Important notes:

Note #1 (permissions): The security on the following registry key dictates which users or groups can gain access to the performance data: `HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Windows NT\ CurrentVersion\ Perflib`
In order to query performance data, account must have KEY_READ access to the above registry key. To change permissions to the registry key you can use the registry editor utility (Regedt32.exe).

Note #2 (bugs): Windows implementation of performance counters has bugs. E.g., PDH.DLL on Windows 2000 (Professional, Server, and Advanced Server editions) can lead to memory leakage. Also PDH.DLL does not work correctly in multithread environment on Windows XP.
That's why we have implemented several different methods to work with PDH.DLL:

- MultiThread - allows to start several tests in separate threads (fastest method)
- OneByOne - HostMonitor starts Performance Counter tests one by one
- Smart - multithreading model, HostMonitor tries to reload pdh.dll when error occurs
- External - HostMonitor uses external (perfobj.exe) utility to perform the tests. This is fast and most reliable method on Windows 2000/XP/2003 however it leads to higher system resources usage. You don't need this mode if you are running HostMonitor on Windows 7, Windows 8 or Windows Server 2008/2012 – Performance Counters API works more reliable on these systems

You can specify which test mode will be used on Miscellaneous page in the Options dialog

WMI

WMI is an acronym for **W**indows **M**anagement **I**nstrumentation. WMI is the Microsoft's implementation of Web-Based Enterprise Management (WBEM) - a new management technology that allows software to monitor and control managed resources throughout the network. Such managed resources include hard drives, file systems, settings of operating system, processes, services, shares, registry settings, networking components, event logs, users, groups, etc.
WMI allows monitoring of performance counters as well. Microsoft applications such as Exchange and SQL Server have WMI built-in. Many non-Microsoft applications utilize WMI and thus they could be monitored using Advanced Host Monitor as well.
WMI is already built into Windows 2000 or above, and can be installed on any other 32-bit Windows system. See also:

- System requirements
- Known problems
- Microsoft WMI FAQ
- WMI Explorer

Normally this test uses WMI protocol; since version 15.80 this test method also supports WinRM mode. If you want to use the WinRM protocol for such tests, you should create an entry using the WinRM page of the Connection Manager.

In addition to the common test parameters, the WMI test has the following options:

Host
Provide the host name (e.g. mainserver) or IP address (e.g. 192.168.1.55) of the host that you wish to monitor.
Please note: Connection Manager provides one convenient place to store account information necessary to perform connections to remote systems.

Authentication Level
This option is necessary for access to some namespaces. E.g. root\cimv2\TerminalServices namespace requires Packet Privacy authentication level.

Name space
WMI namespace is a container grouping child objects related to one another in some way. A namespace contains a hierarchy of classes and associations, which define either a machine's object or the relationship between two or more objects. The most commonly used namespace is CIMV2 (root\cimv2) - Common Information Model Version 2.
Also you may specify [:x32] or [:x64] suffix for name space parameter. E.g. root\cimv2[:x64] This option requests WMI to load a non-default provider (32-bit provider or 64-bit provider).
Note: Windows 8.1 and Windows Server 2012 works incorrectly - using this option in one application (e.g. HostMonitor) may effect another applications. If you run some other WMI related software on such system, then use this option with care.

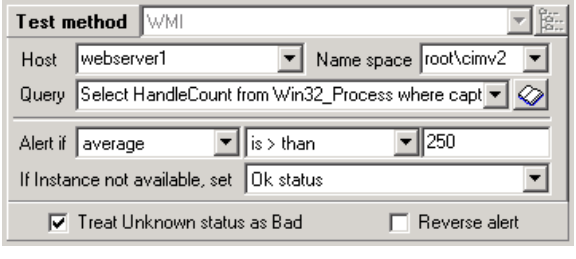
Query
Provide WQL (WMI Query Language) query. This query will be performed at test execution time and result data set will be checked by HostMonitor.

Examples:

1) If you want to monitor the number of handles used by all running instances of the Internet Explorer, use the query like this: `SELECT HandleCount FROM Win32_Process WHERE name='iexplore.exe'`
2) `If you need to monitor the number of processes which use more than 10 threads, use the following query: SELECT ThreadCount FROM Win32_Process WHERE ThreadCount>10`
3) The query: SELECT Name FROM Win32_Service WHERE Started=0 AND StartMode='Auto' shows all services which have not started and have the start mode configured to "Automatic".

You may click the right mouse button on the test item and choose "Explore WMI" item from the popup menu. When you do so, HostMonitor will start WMI Explorer in the Query mode, passing the query and information about the target host (such as the hostname, name space, login, etc) to the explorer. This allows you to check quickly hardware and software parameters on the target system and instantly see what is going on (e.g. why the test item has been failed).
Also, WMI Explorer may display full set of classes within the specified namespace, child objects and their properties.

Alert if
This option specifies when exactly test result(s) should be considered as "bad" and appropriate alert actions should be started. There are 3 parameters should be provided: aggregation mode, compare mode and compare value.



3) Aggregation mode. Specifies how HostMonitor should compare result data when WML query returns several rows. Choose one of the following option:

Any	Tells HostMonitor to compare data from EVERY row. If ANY row matches specified compare condition, HostMonitor will set "Bad" test status.
Average	Tells HostMonitor to calculate average value of the rows and compare average to the specified number.
Total	Tells HostMonitor to calculate sum of the rows and then compare total to the specified number.
Row count	Tells HostMonitor to calculate row count and compare number of rows to the specified number

Examples:

α) if you set the following test parameters:
- Query: `SELECT HandleCount FROM Win32_Process WHERE name='iexplore.exe'`
- `Alert if: Any`
- `Compare: > than 200`

HostMonitor will set "bad" status if any instance of Internet Explorer allocated more than 200 handles.

β) The same query but you chose "Alert if **Average** > 200" option. HostMonitor will set "bad" status when average handles usage is over 200 (e.g. there are 3 IE instances running on the system: 1st instance uses 120 handles, 2nd - 190 handles and 3rd – 310 handles. Average=206.6).

χ) The same query but this time you have chosen "Alert if **Total** > 200" option. HostMonitor will set "bad" status when total number of handles used by all instances of IE is over 200 (e.g. there are 3 IE instances running on the system: 1st instance uses 80 handles, 2nd - 50 handles and 3rd – 110 handles)

δ) If you choose "Alert if **Row count** > 200" then HostMonitor will start alerts when there are more than 200 instances of Internet Explorer is running

Notes:

- If WML query returns single row, then "Any", "Average" and "Total" modes are equivalent (except "Average" and "Total" do not compare value to a string).
- If you specify several fields in 'select' query (e.g. Select HandleCount, ThreadCount from Win32_Process), HostMonitor will check **only 1st field** (HandleCount).
- You may use Average and Total mode only with numeric data

4) Compare mode

HostMonitor compares received/calculated value of the counter with a specified number or string. The following compare modes are supported:

- less than the specified number
- greater than the specified number
- equal to the specified value (number or string)
- different from the specified value (number or string)
- contains the specified string
- doesn't contain the specified string

Also HostMonitor provides 9 compare modes to check how counter value changes in comparison to the previous test:

increases by	set "Bad" status when value increases by specified number or more
decreases by	set "Bad" status when value decreases by specified number or more
changes by	set "Bad" status when value changes by specified number or more
increases by (%)	set "Bad" status when value increases by specified (or greater) percentage
decreases by (%)	set "Bad" status when value decreases by specified (or greater) percentage
changes by (%)	set "Bad" status when value changes by specified (or greater) percentage
increases /sec	set "Bad" status when average increase of the counter (per second) is greater than the specified limit ((new value - old value)/elapsed time >= specified limit)
decreases /sec	set "Bad" status when average decrease of the counter (per second) is greater than the specified limit ((old value - new value)/elapsed time >= specified limit)
changes /sec	set "Bad" status when average change of the counter (per second) is greater than the specified limit (abs(new value - old value)/elapsed time >= specified limit)

Please note: You cannot use these "relative" compare modes if you have chosen "Any" aggregation mode.

3) And finally you should provide value to compare.

If instance no available, set [Unknown/Bad/Ok] status
This option allows you to choose test status that should be used when HostMonitor is able to connect to the system and execute WMI query but query returns empty data set. E.g. you have specified `SELECT HandleCount FROM Win32_Process WHERE name='iexplore.exe'` query; this query will return empty data set if 'iexplore.exe' process is not started. You may choose one of the following statuses: Unknown, Bad, Ok.
Please note: If HostMonitor cannot connect to the host or WMI query fails, HostMonitor will set Unknown status and display error description in Reply field of the test.

System requirements

The following versions of Windows **do** have the WMI pre-installed:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012
- Windows Server 2008
- Windows Server 2003
- Windows 7, 8, 10, 11
- Windows Vista
- Windows 2000
- Windows XP
- Windows ME

These versions of Windows **do not** have the WMI pre-installed:

- Windows NT
- Windows 98
- Windows 95

The WMI Core software package for Windows 95, 98, and Windows NT 4.0 available at Microsoft's web site. Please note: WMI CORE for Windows 95/98/NT requires Microsoft Internet Explorer version 5 or later.

Dominant Process

Unlike test methods that allow you to check specific process (Process test, Performance Counter, WMI) or total/average resource usage on the system (CPU Usage, WMI), Dominant Process test allows you to check on regular basis what process exactly uses the most of system resources. This test allows you to find out which process uses the most of CPU, Handles, Threads, Memory, Virtual memory or Address space.
HostMonitor provides information about "top process" – process that uses more resources than any other process on the system; it may display amount of allocated resources, process name and or process ID.

Normally this test uses WMI protocol; since version 15.80 this test method also supports WinRM mode. If you want to use the WinRM protocol for such tests, you should create an entry using the WinRM page of the Connection Manager.

In addition to the common test parameters the Dominant Process test has the following options:

Check processes on …
Specify name or an IP address of the target computer (the target computer name must be prefixed by "\\"), or select the "<local computer>" item. You can use the "Browse network" button to select a computer from the list.

Exclude process(es)c
Here you may tell HostMonitor to exclude some processes from check by providing comma separated list of such processes, e.g. iexplore.exe, avp.exe, sql.exe If some process name includes comma, use quotation marks for such process. E.g. "test,alert.exe" – name of single process.
Also you may use expression like firefox.exe[800 MB], oracle.exe[8 GB]. Expressions in square brackets tell HostMonitor to exclude firefox.exe and oracle.exe processes from check UNLESS firefox uses over 800 MB or oracle uses over 8 GB (memory). Similar expressions can be applied when the test checks for processes are using the most CPU, Handles or Threads; e.g. svchost.exe[30 %] or chrome.exe[4000]
When you need to monitor many instances of some specific application, you may use "Exclude processes" option to exclude ALL but specified process(es). Type string like all but processname.exe You may check several processes using string like all but iexplore.exe, avp.exe

Alert if process utilizes over …
Here you should specify what kind of resources should be monitored and the maximum limit of resources. If any process uses resources over the limit, HostMonitor will change test status from Ok to Bad and start alerts if necessary (e.g. you may setup HostMonitor to use "kill" utility to terminate or restart any application that uses 60 or more percents of CPU).
You may check the following resources:
- CPU load
- Handles
- Threads
- Memory

- Virtual memory
- Address space

Top process info:
HostMonitor provides information about "top process" (process that uses more resources than any other process on the system) using Reply field of the test item. You may choose one of the following options:
- process ID
- process name
- process name and process ID
- value (amount of resources used by the process)
- value and process ID
- value and process name
- value, process name and process ID

Also, there are 3 macro variables that can be used as parameters of the action (%ProcessName% and %ProcessID%. %ProcessOwner%).

Connect as
To check processes on remote Windows system you can mark this option and provide a username and a password for a connection to the target computer. On the other hand, we recommend using the Connection Manager that provides one convenient place to store account information necessary to perform connections to remote systems.
Note: this option disables WinRM mode for the test

Note: To monitor processes on local or remote Windows system, make sure you have the WMI Core software package installed on the system. WMI Core is installed by default on Windows ME/2000/XP, Windows Vista, Windows 7-11, Windows Server 2003-2022.
The WMI Core software package for Windows 95, 98, and Windows NT 4.0 is available at Microsoft's web site. Please note: WMI CORE for Windows 95/98/NT requires Microsoft Internet Explorer version 5 or later.

See also: Process Meter application
See also: variables specific to Dominant Process test

Registry

This test can retrieve specified Registry counter from local or remote Windows system and compare counter value with specified string, a number or a date.
In addition to common test parameters, for this test you should specify the following options:

Check registry on...
Specify name or an IP address of the target computer or select the "<local computer>" item. You can use the "Browse network" button to select a computer from the list.

Path to the key/value
The Registry path is the location in the Registry that is described by series of nested keys. For example, if you're looking for InstallationDirectory counter in the MessengerService key, which is under Microsoft, which is under SOFTWARE, which is under HKEY_LOCAL_MACHINE, the registry path would be:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MessengerService\InstallationDirectory

Use Win32 registry
Use Win64 registry
Under WOW64, certain registry keys are redirected. When a 32-bit or 64-bit application makes a registry call for a redirected key, the registry redirector intercepts the call and maps it to the key's corresponding physical registry location. For more information, see the following Microsoft articles:
http://msdn.microsoft.com/en-us/library/aa384253(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/aa384232(v=vs.85).aspx
That's why Registry test offers 2 options that tell HostMonitor to accesses the 32-bit registry view or 64-bit registry view.
Note: these options do not work on Windows 2000, HostMonitor will be able to work with 32-bit registry view only.

Alert if key/value absent
This option tells HostMonitor what test status should be set when specified registry counter does not exist. If counter absent and this option enabled, HostMonitor will set Bad test status regardless of "compare mode" and previous value of the counter.
If counter absent and this option disabled, then
- If you are using "any change detected" alert mode, HostMonitor will set Bad or Ok status depending on previous value of the counter (e.g. if counter does not exist now and it was not present earlier then test status will be Ok)
- For other alert modes, HostMonitor will set Unknown test status.

Alert when
This option specifies when exactly test result should be considered as "bad" and appropriate alert actions should be started. There are 2 parameters should be provided: compare mode and compare value.
Compare mode: HostMonitor compares retrieved value of the counter with a specified number, a string or a date. The following compare modes are supported:

- any change detected
- less than the specified value (number, string or date)
- greater than the specified value (number, string or date)
- equal to the specified value
- different from the specified value
- contains the specified string (date macros cannot be used)
- doesn't contain the specified string (date macros cannot be used)

Registry test allows you to check registry data using date macro variables and date expressions. Date format depends on system "short date" format; in addition HostMonitor checks for similar formats. E.g. if short date format = yy/MM/dd, then HostMonitor will translate date specified in one of the following formats: yy/m/d, yy/m/d, yy/mm/d, yy/m/dd, yy/mm/dd, yyyy/m/d, yyyy/m/d, yyyy/mm/d, yyyy/m/dd, yyyy/mm/dd

Connect as

To check registry on remote Windows system you can mark this option and provide a username and a password for a connection to the target computer. On the other hand, we recommend using the Connection Manager that provides one convenient place to store account information necessary to perform connections to remote systems.

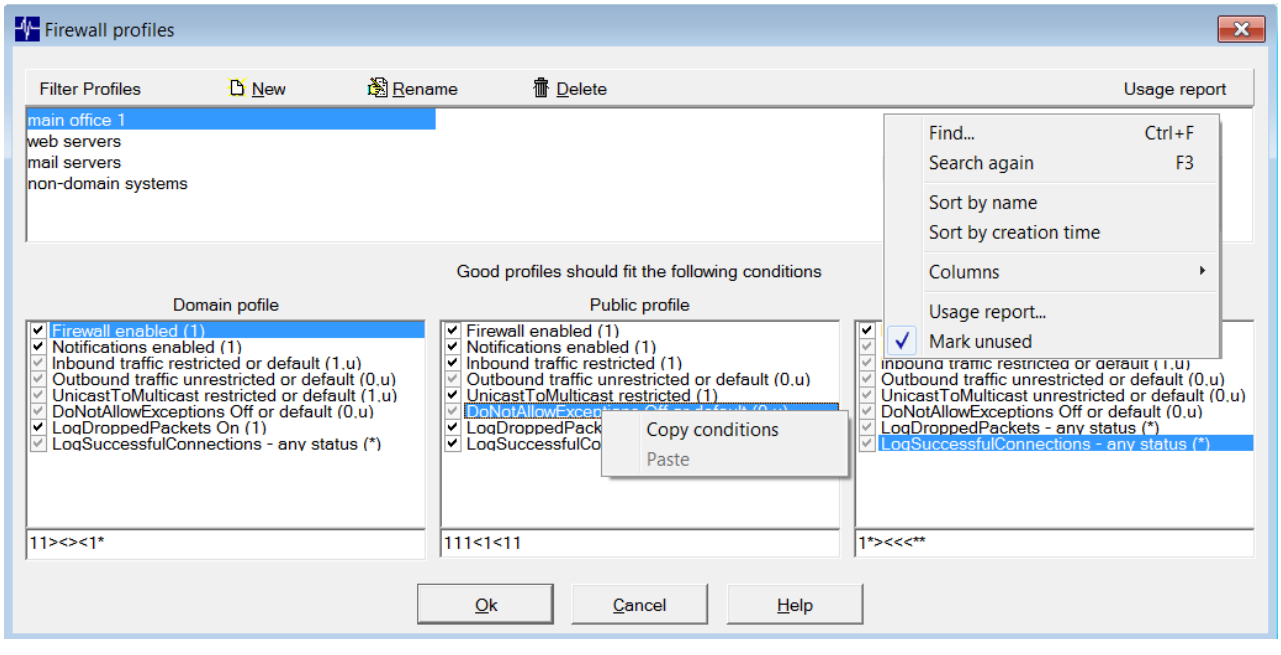
Firewall Status

This test checks the firewall settings on local or remote Windows systems.
In addition to common test parameters, the following parameters must be specified for this test:

Host
Specify the hostname, FQDN or IP address of the target computer. You can use the "Browse network" button to select a computer from the list. Type localhost when you want to check the system where HostMonitor (or RMA) is running.

Mode
Choose one of the following available modes:
- Local profiles
- Group policies
Group policies may override local settings when a system joins a domain.

Checks
Here you should select a HostMonitor profile with "good" conditions for domain, public and private Windows profiles.
Also you may open "Firewall profiles" window and adjust profile settings, create new profiles, sort profiles, get a list of tests that use a specific profile and more.



You may adjust the profile settings using checkbox lists:
- unchecked (0): the rule should be disabled;
- checked (1): the rule set by Windows firewall profile should be enabled (e.g. firewall enabled, notifications enabled, DoNotAllowExceptions rule enabled, etc). Otherwise HostMonitor will set "Bad" test status and trigger the alert actions assigned to the test item;
- grey out (<, >, u, *): this switch state is more complex and depends on the mask located below each list. You can change this mask by using the following symbols in each of the eight positions:
  0 - the rule should be disabled
  1 - the rule should be enabled

< - the rule should be disabled OR unset (unset means the default behavior of Windows firewall, e.g. Inbound traffic is restricted by default while Outbound traffic is unrestricted by default)
> - the rule should be enabled OR unset
u - the rule should be unset
* - any state, HostMonitor will not check the status of the rule
Note: only 0,1,u allowed for "firewall enabled/disabled" rule (1st character)

Connect as
To check firewall settings on remote Windows system you can mark this option and provide a username and a password for a connection to the target computer. On the other hand, we recommend using the Connection Manager that provides one convenient place to store account information necessary to perform connections to remote systems.

DHCP Pool

This test checks percentage of available IP addresses (IP addresses available for the allocation by Windows DHCP server) and alerts when it falls below specified limit. E.g. if DHCP server allocated 200 addresses from 192.168.1.11-192.168.1.254 range, then 18% is available.
In addition to common test parameters, for this test you should specify the following options:

Host
Provide the host name (e.g. mainserver) or IP address (e.g. 10.10.5.55) of DHCP Server you wish to monitor (Windows DHCP server). Type localhost when you want to check system where HostMonitor (or RMA) is running.

Port
Specify the port number on which target SNMP agent is listening for incoming requests. By default SNMP agents use port 161.

Profile
Choose SNMP profile that stores credentials necessary for communication with SNMP agent on DHCP server. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.

Timeout
This is the amount of time in miliseconds the program will wait for a response from the server before the request fails

Retries
Specifies the communications retry count

DHCP Pool
DHCP servers are configured with one or several ranges of IP addresses, HostMonitor may check specific range or check all DHCP scopes and find subnet with lowest percentage of available IP addresses. Here you can specify subnet that you wish to monitor (e.g. 192.168.68.0) or type **all** when all DHCP scopes should be checked by single test item.

Alert when percentage of free addresses fails below N %
HostMonitor will set Bad test status and trigger assigned actions when percentage of available IP addresses falls below this limit.

Antivirus status

This test can check built-in or 3rd party antivirus and antispyware software running on local or remote Windows 7, Windows 10 or Windows Server systems (starting from Windows Server 2012 R2).
In addition to common test parameters, for this test you should specify the following options:

Def/KAV/ESET
Use this switch to set test mode:
- Default/Defender - check Windows Defender, also this mode allows to check 3rd party antiviruses running on Windows 7, Windows 9 and Windows 10 systems
- KAV - check Kaspersky Security for Windows Servers
- ESET - check the following antivirus software:
  ESET Endpoint Security
  ESET Mail Security for Microsoft Exchange
  ESET File Security For Windows Server

Host
Specify name or an IP address of the target computer or select the "<local computer>" item. You can use the "Browse network" button to select a computer from the list.

Defender

Check antivirus/antispyware status, uptodate state (Win 7-10)
This option tells HostMonitor to check built-in or 3rd party antivirus and antispyware software running on Windows 7, 8.1 or Windows 10 systems. Test will set Bad status when all antivirus products disabled or some software is out of date.

Check Defender: pending reboot/manual steps, critical failure
With this option enabled HostMonitor will check Defender running on Windows 8.1, Windows 10 or Windows Server systems (starting from Windows Server 2012 R2) and set Bad status when Defender requires reboot or some manual steps or critical failure detected.

Check Defender: alert if signatures age >= N days
With this option enabled HostMonitor will check Defender running on Windows 8.1, Windows 10 or Windows Server systems (starting from Windows Server 2012 R2) and set Bad status when Defender database is too old.

KAV or ESET modes

HostMonitor may check status, license expiration and database age. Set threshould limits using two options:
Alert when database age is over N days
Alert when license expires within M days
Also HostMonitor will set Bad test status when license expired or software is not activated and provide details in Reply field of the test.
Note: ESET antivirus software may set "kernel not running" status while antivirus service is running and working properly. Antivirus Status test in "ESET" testing mode ignores "kernel not running" error and sets Ok status (unless other problems detected).

Connect as
To check remote Windows system you can mark this option and provide a username and a password for a connection to the target computer. On the other hand, we recommend using the Connection Manager that provides one convenient place to store account information necessary to perform connections to remote systems.

Windows updates (time since last update)

This test can check system updates on local or remote Windows hosts. Normally WMI protocol is used; since version 15.80 this test method also supports WinRM mode. If you want to use the WinRM protocol for such tests, you should create an entry using the WinRM page of the Connection Manager.

In addition to common test parameters, for this test you should specify the following options:

Check updates on
Specify name or an IP address of the target computer or select the "<local computer>" item. You can use the "Browse network" button to select a computer from the list.

Check for
Choose one of the following options
- any update
- security update
- hotfix

Also HostMonitor always checks for “pending reboot” system flags and sets “Bad” test status when reboot is requires.

Alert if no updates for N days or more
Set alert threshold

Connect as
To check remote Windows system you can mark this option and provide a username and a password for a connection to the target computer. On the other hand, we recommend using the Connection Manager that provides one convenient place to store account information necessary to perform connections to remote systems.
This option disables WinRM mode for the test

Note1: Windows does not provide information about some system updates.

Note2: This test method uses significant amount of system resources. If you need 20 or more of "Windows update" tests, we would suggest to put all such tests into one folder and mark "Non-simultaneously test execution" option located in Folder Properties dialog. With this option enabled tests that located in the folder will not be executed at the same time.

VM Host status

This test checks config and overall status of VMware ESXi host or Microsoft Hyper-V systems health state
In addition to common test parameters, for this test you should specify the following options:

VM system
Choose type of the hypervisor: VMware ESXi or Microsoft Hyper-V

Host[:port]
Target host name or IP address (if target system is VMware ESXi, you may specify TCP port used for connections to MOB service over HTTPS protocol)

Timeout
Communication timeout (this option available for VMware ESXi only)

For Hyper-V systems HostMonitor will set Bad test status either for “major” or “critical” failure.

For VMware ESXi systems HostMonitor will set one of the following statuses:
- Bad status if config or overall status is “red”
- Warning status if config or overall status is “yellow”
- Unknown status if config or overall status is “grey”
- Ok status if config AND overall statuses are “green”

Check sensors
WMWare: with this option enabled, HostMonitor will check additional hardware and software status sensors (battery, processor, VMware drivers, etc)

Connect as
You may mark this option and provide a username and a password for a connection to the target computer. On the other hand, we recommend using the Connection Manager that provides one convenient place to store account information necessary to perform connections to remote systems.

Supported VMware hypervisors:
VMware ESXi 4.1
VMware ESXi 5.0
VMware ESXi 5.1
VMware ESXi 5.5
VMware ESXi 6.0
VMware ESXi 6.5
Supported Microsoft hypervisors:
Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2
Microsoft Hyper-V Server 2008, Microsoft Hyper-V Server 2008 R2
Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2
Microsoft Hyper-V Server 2012, Microsoft Hyper-V Server 2012 R2
Microsoft Hyper-V Server 2016, Microsoft Windows Server 2016
Microsoft Hyper-V Server 2019, Microsoft Windows Server 2019

System requirements:
- HostMonitor (RMA) should be started on Windows 7 or higher;
- MOB should be enabled on VMWare host system How to enable MOB

Known problems:
VMware MOB service is not very reliable, if you perform tests often, service may stop responding. In such case you may restart Management Agents using command /sbin/services.sh (execute command using SSH interface)
How to enable Secure Shell
If you experience this problem, please contact VMware team. We hope they will fix the problem

VM Host CPU usage

This test checks CPU load on VMware ESXi host or Microsoft Hyper-V system.
In addition to common test parameters, for this test you should specify the following options:

VM system
Choose type of the hypervisor VMware ESXi or Microsoft Hyper-V

Host[:port]
Target host name or IP address (if target system is VMware ESXi, you may specify TCP port used for connections to MOB service over HTTPS protocol)

Timeout
Communication timeout (this option available for VMware ESXi only)

Alert when CPU usage is over N%
HostMonitor will set "Bad" status and start assigned alert actions when CPU load is over specified limit.

Check CPU load by Hypervisor only
If you check Microsoft Hyper-V system, this option tells HostMonitor to check CPU usage by hypervisor only (like Windows Task Manager does). Otherwise HostMonitor will check CPU load caused by hypervisor and running virtual systems.

Connect as
You may mark this option and provide a username and a password for a connection to the target computer. On the other hand, we recommend using the Connection Manager that provides one convenient place to store account information necessary to perform connections to remote systems.

Supported VMware hypervisors:
- VMware ESXi 4.1
- VMware ESXi 5.0
- VMware ESXi 5.1
- VMware ESXi 5.5
- VMware ESXi 6.0

VMware ESXi 6.5

Supported Microsoft hypervisors:

Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2
Microsoft Hyper-V Server 2008, Microsoft Hyper-V Server 2008 R2
Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2
Microsoft Hyper-V Server 2012, Microsoft Hyper-V Server 2012 R2
Microsoft Hyper-V Server 2016, Microsoft Windows Server 2016
Microsoft Hyper-V Server 2019, Microsoft Windows Server 2019

System requirements:

- HostMonitor (RMA) should be started on Windows 7 or higher;
- MOB should be enabled on VMWare host system How to enable MOB

Known problems:

VMware MOB service is not very reliable, if you perform tests often, service may stop responding. In such case you may restart Management Agents using command /sbin/services.sh (execute command using SSH interface)

How to enable Secure Shell

If you experience this problem, please contact VMware team. We hope they will fix the problem

VM Host free memory

This test checks free memory percentage on VMware ESXi host or Microsoft Hyper-V system (physical memory).
In addition to common test parameters, for this test you should specify the following options:

VM system
Choose type of the hypervisor VMware ESXi or Microsoft Hyper-V

Host[:port]
Target host name or IP address (if target system is VMware ESXi, you may specify TCP port used for connections to MOB service over HTTPS protocol)

Timeout
Communication timeout (this option available for VMware ESXi only)

Alert when memory below N %
HostMonitor will set "Bad" status and start assigned alert actions when free memory falls below specified limit.

Connect as
You may mark this option and provide a username and a password for a connection to the target computer. On the other hand, we recommend using the Connection Manager that provides one convenient place to store account information necessary to perform connections to remote systems.

Supported VMware hypervisors:
VMware ESXi 4.1
VMware ESXi 5.0
VMware ESXi 5.1
VMware ESXi 5.5
VMware ESXi 6.0
VMware ESXi 6.5
Supported Microsoft hypervisors:
Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2
Microsoft Hyper-V Server 2008, Microsoft Hyper-V Server 2008 R2
Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2
Microsoft Hyper-V Server 2012, Microsoft Hyper-V Server 2012 R2
Microsoft Hyper-V Server 2016, Microsoft Windows Server 2016
Microsoft Hyper-V Server 2019, Microsoft Windows Server 2019

System requirements:
- HostMonitor (RMA) should be started on Windows 7 or higher;
- MOB should be enabled on VMWare host system How to enable MOB

Known problems:

VMware MOB service is not very reliable, if you perform tests often, service may stop responding. In such case you may restart Management Agents using command /sbin/services.sh (execute command using SSH interface)
How to enable Secure Shell
If you experience this problem, please contact VMware team. We hope they will fix the problem.

VM Host Datastore space

This test checks data storage(s) on VMware ESXi system, finds storage with minimum free space ratio.
In addition to common test parameters, for this test you should specify the following options:

VM system: VMware ESXi

Host[:port]
Target host name or IP address. Optionally, you may specify TCP port used for connections to MOB service over HTTPS protocol

Timeout
Communication timeout

Datastores
This option allows you to check some specific datastores. You may specify single datastore to check, select datastores from the list or provide comma separated list. If you keep this field empty or type * then HostMonitor will check ALL available stores and find the store with minimum free space

Alert when disk space below N %
HostMonitor will set "Bad" status and start assigned alert actions when free space falls below specified limit.

Connect as
You may mark this option and provide a username and a password for a connection to the target computer. On the other hand, we recommend using the Connection Manager that provides one convenient place to store account information necessary to perform connections to remote systems.

Supported VMware hypervisors:
- VMware ESXi 4.1
- VMware ESXi 5.0
- VMware ESXi 5.1
- VMware ESXi 5.5
- VMware ESXi 6.0
- VMware ESXi 6.5

System requirements: HostMonitor (RMA) should be started on Windows 7 or higher.

System requirements:
- HostMonitor (RMA) should be started on Windows 7 or higher;

- MOB should be enabled on VMWare host system How to enable MOB

Known problems:

VMware MOB service is not very reliable, if you perform tests often, service may stop responding. In such case you may restart Management Agents using command /sbin/services.sh (execute command using SSH interface)

How to enable Secure Shell

If you experience this problem, please contact VMware team. We hope they will fix the problem.

VM guests status

This test checks all virtual systems (guests) running on VMware ESXi host or Microsoft Hyper-V system, sets Bad or Warning status when guest heartbeat status (health state) indicates failure, provides name of such guest system.
In addition to common test parameters, for this test you should specify the following options:

VM system
Choose type of the hypervisor VMware ESXi or Microsoft Hyper-V

Host[:port]
Target host name or IP address (if target system is VMware ESXi, you may specify TCP port used for connections to MOB service over HTTPS protocol)

Timeout
Communication timeout (this option available for VMware ESXi only)

Ignore unknown (grey) status
VMware: with this option enabled HostMonitor will not set Unknown test status when some guest system cannot report its state (heartbeat status is unknown - this may happen when VMware Tools are not installed or not running).
Hyper-V: with this option enabled HostMonitor will not set Bad test status when EnabledState of the guest system cannot be determined.

Alert if guest powered off
With this option enabled HostMonitor will set Bad test status if stopped virtual system detected

Skip guests
This option tells HostMonitor to ignore some virtual systems, you may specify several systems using comma as separator

Connect as
You may mark this option and provide a username and a password for a connection to the target computer. On the other hand, we recommend using the Connection Manager that provides one convenient place to store account information necessary to perform connections to remote systems.

Supported VMware hypervisors:
- VMware ESXi 4.1
- VMware ESXi 5.0
- VMware ESXi 5.1
- VMware ESXi 5.5
- VMware ESXi 6.0
- VMware ESXi 6.5

Note: HostMonitor may display list of all guests with the "worst" (red, yellow, gray) status. To enable this option, you may add vmShowManyGuests=1 line to the [Misc] section of hostmon.ini file and restart HostMonitor

Supported Microsoft hypervisors:
Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2
Microsoft Hyper-V Server 2008, Microsoft Hyper-V Server 2008 R2
Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2
Microsoft Hyper-V Server 2012, Microsoft Hyper-V Server 2012 R2
Microsoft Hyper-V Server 2016, Microsoft Windows Server 2016
Microsoft Hyper-V Server 2019, Microsoft Windows Server 2019

System requirements:
- HostMonitor (RMA) should be started on Windows 7 or higher;
- MOB should be enabled on VMWare host system How to enable MOB

Known problems:
VMware MOB service is not very reliable, if you perform tests often, service may stop responding. In such case you may restart Management Agents using command /sbin/services.sh (execute command using SSH interface)
How to enable Secure Shell
If you experience this problem, please contact VMware team. We hope they will fix the problem.

VM guests CPU usage

This test checks all virtual systems (guests) running on VMware ESXi host or Microsoft Hyper-V system and finds guest system with highest CPU usage
In addition to common test parameters, for this test you should specify the following options:

VM system
Choose type of the hypervisor VMware ESXi or Microsoft Hyper-V

Host[:port]
Target host name or IP address (if target system is VMware ESXi, you may specify TCP port used for connections to MOB service over HTTPS protocol)

Timeout
Communication timeout (this option available for VMware ESXi only)

Alert when CPU usage is over N%
HostMonitor will set “Bad” status and start assigned alert actions when CPU load is over specified limit.
You may use variables like %VMName%, %VMCPUusage% as parameters of the actions.

Skip guests
This option tells HostMonitor to ignore some virtual systems, you may specify several systems using comma as separator

Connect as

You may mark this option and provide a username and a password for a connection to the target computer. On the other hand, we recommend using the Connection Manager that provides one convenient place to store account information necessary to perform connections to remote systems.

Supported VMware hypervisors:
- VMware ESXi 4.1
- VMware ESXi 5.0
- VMware ESXi 5.1
- VMware ESXi 5.5
- VMware ESXi 6.0
- VMware ESXi 6.5

Supported Microsoft hypervisors:
- Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2
- Microsoft Hyper-V Server 2008, Microsoft Hyper-V Server 2008 R2
- Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2
- Microsoft Hyper-V Server 2012, Microsoft Hyper-V Server 2012 R2
- Microsoft Hyper-V Server 2016, Microsoft Windows Server 2016
- Microsoft Hyper-V Server 2019, Microsoft Windows Server 2019

System requirements:
- HostMonitor (RMA) should be started on Windows 7 or higher;
- MOB should be enabled on VMWare host system How to enable MOB

Known problems:
VMware MOB service is not very reliable, if you perform tests often, service may stop responding. In such case you may restart Management Agents using command /sbin/services.sh (execute command using SSH interface)
How to enable Secure Shell
If you experience this problem, please contact VMware team. We hope they will fix the problem.

VM guests free memory

This test checks all virtual systems (guests) running on VMware ESXi host or Microsoft Hyper-V system and finds guest system with lowest percentage of free memory
In addition to common test parameters, for this test you should specify the following options:

VM system
Choose type of the hypervisor VMware ESXi or Microsoft Hyper-V

Host[:port]
Target host name or IP address (if target system is VMware ESXi, you may specify TCP port used for connections to MOB service over HTTPS protocol)

Timeout
Communication timeout (this option available for VMware ESXi only)

Alert when free memory below N %
HostMonitor will set "Bad" status and start assigned alert actions when free memory falls below specified limit.
You may use variables like %VMName%, %VMFreeMem% as parameters of the actions.

Microsoft Hyper-V notes: HostMonitor checks guest systems with dynamic memory allocation support, finds system with lowest amount of free memory, shows free memory percentage using formula like `(1 - (amount of memory the VM wants) / (amount of memory the VM has)) *100`
As long as this number stays above 0, host has enough available memory to service all virtual systems. If test shows 0, this means VM doing paging operations and you will see performance degradation. For best performance with low risk of paging operations, this number should consistently be above 0, ideally around 10-20.

Skip guests
This option tells HostMonitor to ignore some virtual systems, you may specify several systems using comma as separator

Connect as
You may mark this option and provide a username and a password for a connection to the target computer. On the other hand, we recommend using the Connection Manager that provides one convenient place to store account information necessary to perform connections to remote systems.

Supported VMware hypervisors:
- VMware ESXi 4.1
- VMware ESXi 5.0
- VMware ESXi 5.1
- VMware ESXi 5.5
- VMware ESXi 6.0
- VMware ESXi 6.5

(In order to check VM guests free space VM Ware Tools should be installed in guest OS)

Supported Microsoft hypervisors:
Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2
Microsoft Hyper-V Server 2008, Microsoft Hyper-V Server 2008 R2
Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2
Microsoft Hyper-V Server 2012, Microsoft Hyper-V Server 2012 R2
Microsoft Hyper-V Server 2016, Microsoft Windows Server 2016
Microsoft Hyper-V Server 2019, Microsoft Windows Server 2019

System requirements:
- HostMonitor (RMA) should be started on Windows 7 or higher;
- MOB should be enabled on VMWare host system How to enable MOB

Known problems:
VMware MOB service is not very reliable, if you perform tests often, service may stop responding. In such case you may restart Management Agents using command /sbin/services.sh (execute command using SSH interface)
How to enable Secure Shell
If you experience this problem, please contact VMware team. We hope they will fix the problem.

VM guests free disk space

This test checks all virtual systems (guests) running on VMware ESXi host and finds system and disk with minimum free/total space ratio, provides name of the guest, volume name and free space percentage.
In addition to common test parameters, for this test you should specify the following options:

VM system: VMware ESXi

Host[:port]
Target host name or IP address (also you may specify TCP port used for connections to MOB service over HTTPS protocol)

Timeout
Communication timeout

Alert when disk space below N %
HostMonitor will set “Bad” status and start assigned alert actions when disk space falls below specified limit.
You may use variables like %VMName%, %VMVolume%, %VMFreeDisk% as parameters of the actions.

Skip guests
This option tells HostMonitor to ignore some virtual systems, you may specify several systems using comma as separator

Connect as
You may mark this option and provide a username and a password for a connection to the target computer. On the other hand, we recommend using the Connection Manager that provides one convenient place to store account information necessary to perform connections to remote systems.

Supported VMware hypervisors:
- VMware ESXi 4.1
- VMware ESXi 5.0
- VMware ESXi 5.1
- VMware ESXi 5.5
- VMware ESXi 6.0
- VMware ESXi 6.5

System requirements:
- HostMonitor (RMA) should be started on Windows 7 or higher;
- MOB should be enabled on VMWare host system How to enable MOB

Known problems:
VMware MOB service is not very reliable, if you perform tests often, service may stop responding. In such case you may restart Management Agents using command /sbin/services.sh (execute command using SSH interface)
How to enable Secure Shell
If you experience this problem, please contact VMware team. We hope they will fix the problem.

RMCP Ping

RMCP Ping test uses Remote Management Control Protocol (RMCP) to verify connection to remote servers. Unlike Ping(ICMP Ping) this test method may check powered off servers. Note: not every server supports RMCP and IPMI protocols.
RMCP subsystem may use separate network interface with its own IP address to which HostMonitor can connect.
In addition to the common test parameters, the RMCP Ping test has the following options:

Host
Here you should provide the domain name (e. g. server55.msinternal.com) or IP address (e. g. 204.71.200.68) of the host that you wish to monitor. Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) and specify hostname with suffixes ::ipv4 or ::ipv6 (e.g. server55.msinternal.com::ipv4 or www.6bone.net::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.
Note: on Windows NT 4.0, Windows 2000 and Windows XP SP1 IPv6 protocol is not supported. You may use menu Tools -> Local Info to check is your system IPv6 ready.
Also, a range of IPv4 addresses (e.g. 10.10.1.100 – 10.10.1.254) rather than a single address can be specified. In this case, HostMonitor will create a separate test for each of the addresses within that range.

Port
Specify the port number on which the host is listening for incoming RMCP/IPMI requests. Usually port 623 is used.

Timeout
Specify a timeout interval in milliseconds.

Packets
Specify the number of ping requests (at least 3 packets required for Jitter check).

Alert if loss ratio N% or more
A packet loss threshold can be specified for the test, based on which the test status is determined.

Alert if Jitter over N ms
Jitter - amount of variation in response time, calculated by using the following formula Jitter = SquareRoot(SumOf((ReplyTime[i] - AverageReply)^2) / (ReceivedPacketCount-1))
(when this option enabled, HostMonitor will send at least 3 ICMP packets)

Display mode
Tells HostMonitor what kind of data should be displayed in the Reply field:
- Reply time - the "Reply" field will represent average reply time
- % of lost - display percentage of lost packets,

- % of received - display percentage of received packets.
- Jitter - amount of variation in response time

Note: Test Info window may show Loss ratio and Jitter in addition to selected "reply" value

HostMonitor may set 6 statuses for RMCP Ping tests:

"Ok"	this status used when Jitter" option is enabled and Jitter time within specified limit (when "Alert if lost ratio" option enabled, it should be within specified limit as well)
"Host is alive"	this status used when "Jitter" option was not enabled and loss ratio within specified limit
"Bad"	this status means either Jitter or Loss ratio is out of the limits
"No answer"	HostMonitor sets "no answer" status when does not receive any response from target system
"Unknown host"	host name could not be resolved to IP address
"Unknown"	test performed by Remote Monitoring Agent and there is some RMA related error (e.g. HostMonitor cannot connect to the agent)

IPMI Health

IPMI (Intelligent Platform Management Interface) is a set of computer interface specifications for out-of-band management of computer systems. IPMI subsystem works independently of the host CPU, firmware and operating system. IPMI provides a way to manage a computer that may be powered off or otherwise unresponsive by using a network connection to the hardware rather than to an operating system.
IPMI subsystem may use separate network interface with its own IP address to which HostMonitor can connect.

This test method uses IPMI protocol in order to check target server for power related problems, fans and drives faults, detect chassis intrusion.
NOTE: some servers do not set error bits in chassis status record regardless of various hardware problems. You may need to set IPMI Discrete tests in order to check for hardware problems.

In addition to the common test parameters, the IPMI Health test has the following options:

Host
Here you should provide the domain name (e. g. server55.msinternal.com) or IP address (e. g. 204.71.200.68) of the host that you wish to monitor. Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) and specify hostname with suffixes ::ipv4 or ::ipv6 (e.g. server55.msinternal.com::ipv4 or www.6bone.net::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.
Note: on Windows NT 4.0, Windows 2000 and Windows XP SP1 IPv6 protocol is not supported. You may use menu Tools -> Local Info to check is your system IPv6 ready.
Also, a range of IPv4 addresses (e.g. 10.10.1.100 – 10.10.1.254) rather than a single address can be specified. In this case, HostMonitor will create a separate test for each of the addresses within that range.

Port
Specify the port number on which the host is listening for incoming IPMI requests. Usually port 623 is used.

Cipher
Choose cipher mode (set of authentication, integrity and encryption algorithms). The following cipher modes are supported

00: None
01: RAKP-HMAC-SHA1 authentication (**SHA1**)
02: RAKP-HMAC-SHA1 authentication + HMAC-SHA1-96 integrity (**SHA1/96**)
03: RAKP-HMAC-SHA1 + AES128CBC encryption + HMAC-SHA1-96 integrity (**SHA1/AES**)
15: RAKP-HMAC-SHA256 authentication (**SHA256**)
16: RAKP-HMAC-SHA256 authentication + HMAC-SHA256-128 integrity (**SHA256/128**)
17: RAKP-HMAC-SHA256 + AES128CBC encryption + HMAC-SHA256-128 integrity (**SHA256/AES**)

Retries
Specifies the communications retry count.

Timeout
Specify a timeout interval in milliseconds.

You may mark one or several of the following option
Alert when power off
Alert when chassis intrusion detected
Alert on power/fan/drive failures

Connection Manager
You may use this button to start Connection Manager and provide user name and password for specific IPMI-enabled server or set of servers using IP address range like 10.10.1.120-10.10.1.160

IPMI Browser
You may use this button to start IPMI Browser and verify that connection and account settings are correct and target host accepts requests.
If you are using RCC (Remote Control Console) started on remote system, make sure ipmibrowser.exe module is installed as well.

IPMI Temperature, Fans, Voltage, Current (Analog tests)

IPMI (Intelligent Platform Management Interface) is a set of computer interface specifications for out-of-band management of computer systems. IPMI subsystem works independently of the host CPU, firmware and operating system. IPMI provides a way to manage a computer that may be powered off or otherwise unresponsive by using a network connection to the hardware rather than to an operating system.
IPMI Temperature, IPMI Fans, IPMI Voltage and IPMI Current test methods use IPMI protocol in order to monitor analog sensors.
In addition to the common test parameters, the IPMI analog tests offer the following options:

Host
Here you should provide the domain name (e. g. server55.msinternal.com) or IP address (e. g. 204.71.200.68) of the host that you wish to monitor. Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) and specify hostname with suffixes ::ipv4 or ::ipv6 (e.g. server55.msinternal.com::ipv4 or www.6bone.net::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.
Note: on Windows NT 4.0, Windows 2000 and Windows XP SP1 IPv6 protocol is not supported. You may use menu Tools -> Local Info to check is your system IPv6 ready.
Also, a range of IPv4 addresses (e.g. 10.10.1.100 – 10.10.1.254) rather than a single address can be specified. In this case, HostMonitor will create a separate test for each of the addresses within that range.

Port
Specify the port number on which the host is listening for incoming IPMI requests. Usually port 623 is used.

Cipher
Choose cipher mode (set of authentication, integrity and encryption algorithms). The following cipher modes are supported

00: None
01: RAKP-HMAC-SHA1 authentication (**SHA1**)
02: RAKP-HMAC-SHA1 authentication + HMAC-SHA1-96 integrity (**SHA1/96**)
03: RAKP-HMAC-SHA1 + AES128CBC encryption + HMAC-SHA1-96 integrity (**SHA1/AES**)
15: RAKP-HMAC-SHA256 authentication (**SHA256**)
16: RAKP-HMAC-SHA256 authentication + HMAC-SHA256-128 integrity (**SHA256/128**)
17: RAKP-HMAC-SHA256 + AES128CBC encryption + HMAC-SHA256-128 integrity (**SHA256/AES**)

Retries
Specifies the communications retry count.

Timeout
Specify a timeout interval in milliseconds.

Name filter
Use this filter when you need to check single sensor or some set of sensors, e.g. type CPU in order to check all sensors with "CPU" in the name; or type CPU5, then any sensor that contains "CPU5" in the name will fit the filter. You may use IPMI Browser in order to check all sensors available on target server.
If you keep this field empty, HostMonitor will check all available sensors (i.e. all analog temperature sensors for IPMI Temperature test; all voltage sensors for IPMI Voltage test; etc).

Display: Highest value / Lowest value
HostMonitor checks sensors readings against thresholds set on the server for each sensor. If some value falls below (or rises above) critical or non-repairable thresholds, HostMonitor will set Bad test status and display sensor value and sensor name in Reply field of the test. If one sensor value rises above critical threshold and another sensor value rises above non-repairable threshold then HostMonitor will show the "worst" sensor.
"Display" option is used when there is no bad sensor. If all readings fit within "healthy" range, this option tells HostMonitor to display sensor with highest or lowest value.

Warning if non-critical limits reached
There are non-critical limits specified for some sensors. If you mark this option and sensor reading falls below (or rises above) non-critical limit, HostMonitor will set Warning test status and display sensor value and sensor name in Reply field of the test (unless there is another sensor with critical or non-repairable value).

Note: some HPE servers set upper non-repairable threshold for fans at 999 RPM, this is invalid threshold. You may adjust thresholds on server side or use Optional status processing options, e.g.
use Normal status if ("%SuggestedStatus%"=="Bad") and ("%SuggestedReply%" getnumber 1 > 500)

Connection Manager
You may use this button to start Connection Manager and provide user name and password for specific IPMI-enabled server or set of servers using IP address range like 10.10.1.120-10.10.1.160

IPMI Browser
You may use this button to start IPMI Browser and verify that connection and account settings are correct and target host accepts requests.
If you are using RCC (Remote Control Console) started on remote system, make sure ipmibrowser.exe module is installed as well.

Known problems
The IPMI subsystem operates with limited resources and may not be able to handle many requests at the same time. If you have configured many tests for a particular server and the tests fail from time to time, we recommend to place all IPMI related tests related to the server in one folder and enable **Non-simultaneously test execution** option located on the Specials page in the Test Properties window.
With this option enabled tests that located in the folder will not be executed simultaneously. Test items located in different folders may be executed simultaneously, even if this option is set for all of these folders.

IPMI Discrete

IPMI (Intelligent Platform Management Interface) is a set of computer interface specifications for out-of-band management of computer systems. IPMI subsystem works independently of the host CPU, firmware and operating system. IPMI provides a way to manage a computer that may be powered off or otherwise unresponsive by using a network connection to the hardware rather than to an operating system.

IPMI Discrete test uses IPMI protocol in order to check set of discrete sensors and alert when specific state is asserted. HostMonitor checks all sensors that match "check" mode and name filter and have asserted state(s) matched bitmask (bit 0 tells HostMonitor to ignore state); sets Bad status when there are such sensor(s) detected; displays sensor name and error description in Reply field of the test. E.g. when you are checking Drive Slot sensors HostMonitor may display reply like:
C1P1 Bay 1 Predictive Failure, Parity Check In Progress <LF> C1P2 Bay 6 Rebuild Aborted
See deteils below

In addition to the common test parameters, this test offers the following options:

Host
Here you should provide the domain name (e. g. server55.msinternal.com) or IP address (e. g. 204.71.200.68) of the host that you wish to monitor. Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) and specify hostname with suffixes ::ipv4 or ::ipv6 (e.g. server55.msinternal.com::ipv4 or www.6bone.net::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6

protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.
Note: on Windows NT 4.0, Windows 2000 and Windows XP SP1 IPv6 protocol is not supported. You may use menu Tools -> Local Info to check is your system IPv6 ready.
Also, a range of IPv4 addresses (e.g. 10.10.1.100 – 10.10.1.254) rather than a single address can be specified. In this case, HostMonitor will create a separate test for each of the addresses within that range.

Port
Specify the port number on which the host is listening for incoming IPMI requests. Usually port 623 is used.

Cipher
Choose cipher mode (set of authentication, integrity and encryption algorithms). The following cipher modes are supported

00: None
01: RAKP-HMAC-SHA1 authentication (**SHA1**)
02: RAKP-HMAC-SHA1 authentication + HMAC-SHA1-96 integrity (**SHA1/96**)
03: RAKP-HMAC-SHA1 + AES128CBC encryption + HMAC-SHA1-96 integrity (**SHA1/AES**)
15: RAKP-HMAC-SHA256 authentication (**SHA256**)
16: RAKP-HMAC-SHA256 authentication + HMAC-SHA256-128 integrity (**SHA256/128**)
17: RAKP-HMAC-SHA256 + AES128CBC encryption + HMAC-SHA256-128 integrity (**SHA256/AES**)

Retries
Specifies the communications retry count.

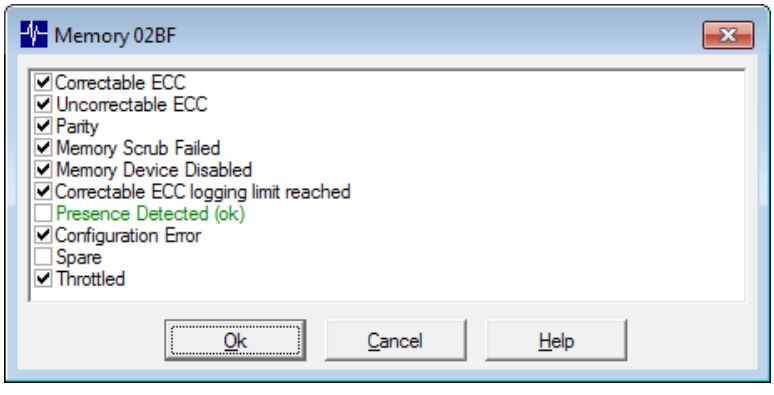
Timeout
Specify a timeout interval in milliseconds.

Check
Choose what kind of discrete sensors should be checked by HostMonitor:
- Management system health
- Physical Security
- Platform Security
- Firmware Errors
- Power supply
- Power unit
- Battery
- Cooling
- Processor
- Memory
- Drive Slot

Name filter
Use this filter when you need to check single sensor or some set of sensors, e.g. type CPU in order to check all sensors with “CPU” in the name; or type CPU5, then any sensor that contains “CPU5” in the name will fit the filter. You may use IPMI Browser in order to check all sensors available on target server.

If you keep this field empty, HostMonitor will check all available sensors (e.g. all Drive Slot sensors).

Alert bitmask
Here you should provide hex or binary number with ‘h’ or ‘b’ suffix accordingly, e.g. 17Fh or 101111111b. HostMonitor checks all sensors that match “check” mode and name filter and have asserted state(s) matched bitmask (bit 0 tells HostMonitor to ignore state).
HostMonitor sets default mask depending on sensor type (check type), also you may adjust bitmask either manually or using “Alert mask” window – it shows possible error states and calculates bitmask.
Note: “good” items displayed in green, usually you don’t need to mark such items



HostMonitor may detect and report the following states:

Management Subsystem Health
Sensor access degraded or unavailable
Controller access degraded or unavailable
Management controller off-line
Management controller unavailable
Sensor failure
FRU failure

Physical Security
General Chassis intrusion
Drive Bay intrusion
I/O Card area intrusion
Processor area intrusion
System unplugged from LAN
Unauthorized dock
FAN area intrusion

Platform Security
Front Panel Lockout violation attempted
Pre-boot user password violation
Pre-boot setup password violation
Pre-boot network password violation
Pre-boot password violation
Out-of-band access password violation

Firmware Errors
System Firmware Error
System Firmware Hang
System Firmware Progress

Power supply
Presence detected
Failure detected
Predictive failure
Power Supply AC lost
AC lost or out-of-range
AC out-of-range, but present
Config Error
Inactive

Power unit
Power off/down
Power cycle
240VA power down
Interlock power down
AC lost
Soft-power control failure
Failure detected
Predictive failure

Battery
Low
Failed

Processor
IERR
Thermal Trip
FRB1/BIST failure
FRB2/Hang in POST failure
FRB3/Processor startup/init failure
Configuration Error
SM BIOS Uncorrectable CPU-complex Error
Presence detected
Disabled
Terminator detected
Throttled
Machine Check Exception (Uncorrectable)
Correctable Machine Check Error

Memory
Correctable ECC
Uncorrectable ECC
Parity
Memory Scrub Failed
Memory Device Disabled
Correctable ECC logging limit reached
Presence detected
Configuration Error
Spare
Throttled

Drive Slot
Presence detected
Drive Fault
Predictive Failure
Hot Spare
Parity Check In Progress
In Critical Array
In Failed Array
Rebuild In Progress
Rebuild Aborted

Connection Manager

You may use this button to start Connection Manager and provide user name and password for specific IPMI-enabled server or set of servers using IP address range like 10.10.1.120-10.10.1.160

IPMI Browser

You may use this button to start IPMI Browser and verify that connection and account settings are correct and target host accepts requests.
If you are using RCC (Remote Control Console) started on remote system, make sure ipmibrowser.exe module is installed as well.

Known problems

The IPMI subsystem operates with limited resources and may not be able to handle many requests at the same time. If you have configured many tests for a particular server and the tests fail from time to time, we recommend to place all IPMI related tests related to the server in one folder and enable **Non-simultaneously test execution** option located on the Specials page in the Test Properties window.
With this option enabled tests that located in the folder will not be executed simultaneously. Test items located in different folders may be executed simultaneously, even if this option is set for all of these folders.

HP iLO Health

Integrated Lights-Out (iLO) - server management technology by Hewlett-Packard. iLO is available on HP ProLiant and Integrity servers and provides system information, such as fans, temperatures, and power supplies status. Usually the iLO card has a separate network connection and its own IP address to which HostMonitor can connect.

Please note: marketing name "HP iLO" can be misleading as "HP iLO"-compatible servers actually can support at least 3 different protocols: IPMI, iLO and Redfish.
- HP iLO versions 1, 2 and 3 do not use the Redfish protocol, but the older HPE "iLO" protocol (IPMI is also usually supported).
- HP iLO version 4 and 5 - can use either the older HPE protocol or the Redfish protocol (IPMI is also usually supported). As we know, this depends on the firmware version, HPE switched to Redfish protocol in iLO 5 v2.30
- HP iLO version 6 - can use either the older HPE protocol or the Redfish protocol (IPMI is also usually supported). As we know, HPE switched to Redfish protocol in iLO 6 v1.05

If HP iLO tests do not work with your HPE server, you may try IPMI and Redfish tests

This test checks BIOS status, fans, temperature sensors, power supplies status, memory, processor, network and storage status using HTTPS protocol for iLO requests.
In addition to common test parameters, HP iLO Health test has the following options:

Host
Provide target host name or IP address (e.g. 10.20.5.101).
Optionally you may specify TCP port; port number has to be provided after a colon following the host address (e.g. 172.168.10.10**:443**).

Login/Pswd
Provide valid iLO user account and password

If some problem detected, HostMontor sets Bad test status and shows problem description like "STORAGE STATUS: Degraded" in Reply field of the test.
Also, it sets %HealthData% variable (can be used as parameter of some actions assigned to the test). When no problem detected this variable will reports status of all checked components, e.g.

```
BIOS HARDWARE: OK
FANS: OK
TEMPERATURE: OK
POWER SUPPLIES: OK
PROCESSOR: OK
MEMORY: OK
STORAGE: OK
```

See also: variables specific to HP iLO tests

HP iLO Temperature

Integrated Lights-Out (iLO) - server management technology by Hewlett-Packard. iLO is available on HP ProLiant and Integrity servers and provides system information, such as fans, temperatures, and power supplies status. Usually the iLO card has a separate network connection and its own IP address to which HostMonitor can connect.
This test checks temperature sensors installed in the server using HTTPS protocol for iLO requests.

In addition to common test parameters, HP iLO Temperature test has the following options:

Host
Provide target host name or IP address (e.g. 10.20.5.101).
Optionally you may specify TCP port; port number has to be provided after a colon following the host address (e.g. 172.168.10.10**:443**).

Login/Pswd
Provide valid iLO user account and password

If some problem detected, HostMontor sets Bad test status and shows problem description (status, temperature, limit, sensor name and location) in Reply field of the test.

If critical temp not reached, display
- sensor closest to critical temp (%)
- hottest sensor, name or location matches

If no problems detected, these options allow you to choose Reply field mode. E.g. you may specify location: Ambient, System, CPU, I/O Board, Memory or Power Supply. Also you may provide specific sensor name, e.g. "02-CPU 1" or "04-P1 DIMM 1-6"

HP iLO Fans

Integrated Lights-Out (iLO) - server management technology by Hewlett-Packard. iLO is available on HP ProLiant and Integrity servers and provides system information, such as fans, temperatures, and power supplies status. Usually the iLO card has a separate network connection and its own IP address to which HostMonitor can connect.
This test checks fans installed in the server using HTTPS protocol for iLO requests.

In addition to common test parameters, HP iLO Fans test has the following options:

Host
Provide target host name or IP address (e.g. 10.20.5.101).
Optionally you may specify TCP port; port number has to be provided after a colon following the host address (e.g. 172.168.10.10**:443**).

Login/Pswd
Provide valid iLO user account and password

If some problem detected, HostMontor sets Bad test status and shows problem description (fan status, location, name, speed) in Reply field of the test.

If no failed fan detected, display fastest fan in zone
If no problems detected, this option allows you to choose Reply field mode. E.g. you may type "any" to display fastest fan speed; specify location zone like "System" or provide fan name like "Fan 2"

HP iLO Power

Integrated Lights-Out (iLO) - server management technology by Hewlett-Packard. iLO is available on HP ProLiant and Integrity servers and provides system information, such as fans, temperatures, and power supplies status. Usually the iLO card has a separate network connection and its own IP address to which HostMonitor can connect.
This test checks power supply status using HTTPS protocol for iLO requests.

In addition to common test parameters, HP iLO Power test has the following options:

Host
Provide target host name or IP address (e.g. 10.20.5.101).
Optionally you may specify TCP port; port number has to be provided after a colon following the host address (e.g. 172.168.10.10**:443**).

Login/Pswd
Provide valid iLO user account and password

If some problem detected, HostMontor sets Bad test status and shows problem description in Reply field of the test.

Display
- Present power consumption
- Average power consumption
- Maximum power consumption

This option allows you to choose Reply field mode. Note: Average and Maximum modes require HPE iLO Advanced license from Hewlett-Packard

Alert if no redundancy
With this option enabled test will set Bad status when system has no redundant power supply

HP iLO Disks

Integrated Lights-Out (iLO) - server management technology by Hewlett-Packard. iLO is available on HP ProLiant and Integrity servers and provides system information, such as fans, temperatures, and power supplies status. Usually the iLO card has a separate network connection and its own IP address to which HostMonitor can connect.
This test checks controller and disks status using HTTPS protocol for iLO requests.

In addition to common test parameters, HP iLO Disks test has the following options:

Host
Provide target host name or IP address (e.g. 10.20.5.101).
Optionally you may specify TCP port; port number has to be provided after a colon following the host address (e.g. 172.168.10.10**:443**).

Login/Pswd
Provide valid iLO user account and password

If no degraded/failed drive detected, display
- Total logical size
- Total physical size

If some problem detected, HostMontor sets Bad test status and shows problem description in Reply field of the test. Otherwise HostMonitor shows total logical or physical capacity of the system

Note: HP iLO 5 firmware 1.10 does not work correctly, it sets “degraded” disk status when predicted life left percentage is less than 100% (e.g. 99% of media life left == “degraded” disk)
https://support.hpe.com/hpesc/public/docDisplay?docId=a00026408en_us&docLocale=en_US

Redfish Health

Redfish is a set of specifications for out-of-band management of computer systems. Redfish subsystem operates independently of the host CPU, firmware and operating system (similar to IPMI and HP iLO). Redfish allows you to manage a computer that may be powered off or otherwise unresponsive by using a network connection to the hardware rather than to an operating system. Redfish is supported by a variety of vendors, including Cisco, Dell, HPE, Lenovo, IBM, Supermicro, and others.
Redfish subsystem may use a separate network interface with its own IP address to which HostMonitor can connect.

Please note: marketing names such as "iDRAC" or "HP iLO" can be misleading as "HP iLO"-compatible servers can actually support at least 3 different protocols: IPMI, iLO and Redfish.
- HP iLO versions 1, 2 and 3 do not use the Redfish protocol, but the older HPE "iLO" protocol (IPMI is also usually supported).
- HP iLO version 4 and 5 - can use either the older HPE protocol or the Redfish protocol (IPMI is also usually supported). As we know, this depends on the firmware version, HPE switched to Redfish protocol in iLO 5 v2.30
- HP iLO version 6 - can use either the older HPE protocol or the Redfish protocol (IPMI is also usually supported). As we know, HPE switched to Redfish protocol in iLO 6 v1.05

Dell servers with iDRAC can also support several different protocols: IPMI and Redfish.

Also Redfish specifications change slightly every year. HostMonitor supports several versions and should be able to work with older and newer servers. If it does not work with your server, please contact us by e-mail.

Redfish Health test checks the overall system health, CPU and memory health, TPM status, storage and battery health and more
In addition to the common test parameters, the Redfish Health test has the following options:

Host
Here you should specify the domain name or IP address of the host you want to monitor. You can also specify the TCP port (default is 443), for example 10.10.10.1:8000.
You can also set the prefix http://, in which case the regular HTTP protocol will be used without encryption, and the default TCP port will be changed to port 80.
E.g.
server55.msinternal.com
204.71.200.68
204.71.200.68:8000
http://10.10.10.1:8002

Timeout
Specify a timeout interval in milliseconds.

If no health problems are detected, display
Here you can choose one of the following options:
- response time
- battery: health percentage (battery with the lowest value)
- disk: predicted life percentage (disk with the lowerst value)

If any issue are detected, HostMonitor will set Warning or Bad test status and provide a description in the Reply field of the test.

Macro variables can provide additional information about the target system (for example, you can use variables in the e-mail template used by the "Send e-mail" action assigned to the test item or use variables in Optional status processing expressions)

%RF_SysInfo%	- detailed information about system
%RF_SysModel%	- system model
%RF_SysName%	- system name
%RF_HostName%	- host name
%RF_Description%	- description
%RF_Manufacturer%	- manufacturer
%RF_BIOS%	- BIOS version
%RF_SystemID%	- system ID
%RF_PowerState%	- power state
%RF_LastResetTime%	- last reset time
%RF_LastBoot%	- last boot
%RF_SysStatus%	- system status
%RF_CPUModel%	- CPU model
%RF_CPUCores%	- CPU cores
%RF_CPUStatus%	- CPU status
%RF_MemMirroring%	- memory mirroring
%RF_MemTotal%	- total amount of memory
%RF_MemStatus%	- memory status
%RF_TPMType%	- TPM type
%RF_TPMStatus%	- TPM status
%RF_Devices%	- information about storage devices

Connection Manager
You can use this button to launch Connection Manager and spacify the username and password for specific Redfish-enabled server or group of servers using an IP address range like 10.10.1.120-10.10.1.160

Redfish Meter
You can use this button to launch Redfish Meter and verify that the connection and account settings are correct and that the target host is accepting requests.
If you are using RCC (Remote Control Console) started on a remote system, make sure that RfMeter.exe module is also installed.

Redfish Temperature, Fans, Voltage, Current and Power tests

Redfish is a set of specifications for out-of-band management of computer systems. Redfish subsystem operates independently of the host CPU, firmware and operating system (similar to IPMI and HP iLO). Redfish allows you to manage a computer that may be powered off or otherwise unresponsive by using a network connection to the hardware rather than to an operating system. Redfish is supported by a variety of vendors, including Cisco, Dell, HPE, Lenovo, IBM, Supermicro, and others.
Redfish subsystem may use separate network interface with its own IP address to which HostMonitor can connect.

Redfish Temperature, Redfish Fans, Redfish Voltage, Redfish Current and Redfish Power test methods use Redfish protocol in order to monitor temperature sensors, speed of the fans, voltage, current and power consumption.

In addition to the common test parameters, these tests offer the following options:

Host
Here you should specify the domain name or IP address of the host you want to monitor. You can also specify the TCP port (default is 443), for example 10.10.10.1:8000.
You can also set the prefix http://, in which case the regular HTTP protocol will be used without encryption, and the default TCP port will be changed to port 80.
E.g.
server55.msinternal.com
204.71.200.68
204.71.200.68:8000
http://10.10.10.1:8002

Timeout
Specify a timeout interval in milliseconds.

Check sensors with name/context matches
Use this filter when you need to check a single sensor or a specific set of sensors. For example, type CPU in order to check all sensors with "CPU" in the name or "CPU" in description of the physical context (location); or type CPU5, then any sensor that contains "CPU5" in the name will match the filter. You can use Redfish Meter in order to check all sensors available on the target server.
If you keep this field empty or use "* (any)" item, then HostMonitor will check all available sensors (i.e. all temperature sensors for Redfish Temperature test; all voltage sensors for Redfish Voltage test; etc).

If the thresholds are not reached, display
- sensor with **highest** value
- sensor with **lowest** value

HostMonitor checks the status and readings of the sensors. If some value falls below (or rises above) warning or critical thresholds set on the server, HostMonitor will set Warning or Bad test status and display the sensor value and sensor name in the Reply field of the test. If one sensor

value rises above the warning threshold and another sensor value rises above the critical threshold then HostMonitor will show the “worst” sensor.
“Display” option is used when there are no bad sensors. If all readings are within “healthy” range, this option tells HostMonitor to display the sensor with the highest or lowest value.

Macro variables can provide additional information about the sensor (e.g. you may use variables in the e-mail template used by the “Send e-mail” action assigned to the test item or use variables in Optional status processing expressions)
%RF_CHASSI% - name of the chassi where the sensor is located
%RF_CONTEXT% - context (location) of the sensor

Connection Manager
You can use this button to launch Connection Manager and spacify the username and password for specific Redfish-enabled server or group of servers using an IP address range like 10.10.1.120-10.10.1.160

Redfish Meter
You can use this button to launch Redfish Meter and verify that the connection and account settings are correct and that the target host is accepting requests.
If you are using RCC (Remote Control Console) started on a remote system, make sure that RfMeter.exe module is also installed.

Known problems:

Some versions of Dell iDRAC firmware cause the Redfish ThermasSubsystem/Fans endpoint to return malformed data (e.g. PowerEdge R7715, Redfish ver 1.20.1). In this case Redfish Fans test method does not work.

The Redfish subsystem operates with limited resources and may not be able to handle many requests at the same time. If you have configured many tests for a particular server and the tests fail from time to time, we recommend to place all Redfish related tests related to the server in one folder and enable **Non-simultaneously test execution** option located on the Specials page in the Test Properties window.
With this option enabled tests that located in the folder will not be executed simultaneously. Test items located in different folders may be executed simultaneously, even if this option is set for all of these folders.

Redfish Sensor

Redfish is a set of specifications for out-of-band management of computer systems. Redfish subsystem operates independently of the host CPU, firmware and operating system (similar to IPMI and HP iLO). Redfish allows you to manage a computer that may be powered off or otherwise unresponsive by using a network connection to the hardware rather than to an operating system. Redfish is supported by a variety of vendors, including Cisco, Dell, HPE, Lenovo, IBM, Supermicro, and others.
Redfish subsystem may use separate network interface with its own IP address to which HostMonitor can connect.

Redish Sensor test may check any type of the sensor, inluding temperature, voltage, current and power sensors as well.
In addition to the common test parameters, the Redfish Sensor tests offer the following options:

Host
Here you should specify the domain name or IP address of the host you want to monitor. You can also specify the TCP port (default is 443), for example 10.10.10.1:8000.
You can also set the prefix http://, in which case the regular HTTP protocol will be used without encryption, and the default TCP port will be changed to port 80.
E.g.
server55.msinternal.com
204.71.200.68
204.71.200.68:8000
http://10.10.10.1:8002

Timeout
Specify a timeout interval in milliseconds.

Sensor type
Use this filter to set the type of sensors to be checked:
* (any)
AbsoluteHumidity
AirFlow
AirFlowCMM
Altitude
Barometric
ChargeAh
Current
EnergyJoules
EnergyWh
Frequency
Heat
Humidity
LiquidFlow
and more...

Name filter
Use this filter when you need to check a single sensor or a specific set of sensors. For example, type CPU in order to check all sensors with “CPU” in the name; or type CPU5, then any sensor that contains “CPU5” in the name will match the filter. You can use Redfish Meter in order to check all sensors available on target server.

Context filter
Use this filter when you need to check sensors at a specific location, such as “Battery”, “Intake”, “Memory” or “Exhaust”. You can use Redfish Meter in order to check all sensors available on target server.

You may set one, two or three filters, for example, tell HostMonitor to check temperature sensors associated with the "Memory" context, with the string “DIMM” in the sensor name.

Thresholds
Unlike Redfish Temperature or Redfish Power test methods, which check sensors readings against thresholds set on the server, Redfish Sensor test checks sensors readings against user-defined thresholds. Therefore, you should set minimum and maximum limits for the test.
If a sensor value falls below (or rises above) the limit, HostMonitor will set the test status to "Bad". Otherwise the sensor with the value closest to the limit will be used for the result. HostMonitor will display the sensor value and sensor name in the Reply field of the test in both cases (test status "Ok" or "Bad").

Macro variables can provide additional information about the sensor (e.g. you may use variables in the e-mail template used by the “Send e-mail” action assigned to the test item or use variables in Optional status processing expressions)
%RF_CHASSI% - name of the chassi where the sensor is located
%RF_CONTEXT% - context (location) of the sensor

Connection Manager
You can use this button to launch Connection Manager and spacify the username and password for specific Redfish-enabled server or group of servers using an IP address range like 10.10.1.120-10.10.1.160

Redfish Meter
You can use this button to launch Redfish Meter and verify that the connection and account settings are correct and that the target host is accepting requests.
If you are using RCC (Remote Control Console) started on a remote system, make sure that RfMeter.exe module is also installed.

Known problems
The Redfish subsystem operates with limited resources and may not be able to handle many requests at the same time. If you have configured many tests for a particular server and the tests fail from time to time, we recommend to place all Redfish related tests related to the server in one

folder and enable **Non-simultaneously test execution** option located on the Specials page in the Test Properties window.
With this option enabled tests that located in the folder will not be executed simultaneously. Test items located in different folders may be executed simultaneously, even if this option is set for all of these folders.

Cisco Health

For Cisco devices with environmental monitor this test checks fans, temperature sensors, power supplies status. Also test can check UCS faults and find all faults with specified severity (and above, e.g. minor, major and critical events).
HostMonitor retrieves data from Cisco devices using SNMP protocol.
In addition to common test parameters, Cisco Health test has the following options:

Host
Provide a string specifying either a dotted-decimal IP address (e.g. 195.168.10.10) or a host name that can be resolved to an IP address.
Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) or specify hostname with suffixes **::ipv4** or **::ipv6** (e.g. www.google.com::ipv4 or www.6bone.net::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.

Port
Specify the port number on which the host is listening for incoming requests. Usually Cisco SNMP agents listen on port 161.

Profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

Environmental check
With this option enabled HostMonitor will check statuses maintained by the environmental monitor: the table of voltage status, the table of temperature status, the table of fan status, the table of power supply status.

UCS faults check, ignore severity before <severity>
Tells HostMonitor to check for events in UCS fault table, find all events with specified severity (and above), igone events with lower severity. E.g. "ignore severity before Warning" option tells HostMonitor to find Warning, Minor, Major and Critical events, ignore events with status Unknown, Info or Cleared.

If some problems detected, HostMonitor will show error desctiption in Reply field of the test.

Cisco Temperature

HostMonitor may check all temperature sensors installed on Cisco devices; if no problem detected HostMonitor may display unit with temperature closest to critical. Also it may show temperature of specific unit, e.g. hottest intake or CPU unit with highest temperature.
In addition to common test parameters, Cisco Temperature test has the following options:

Host
Provide a string specifying either a dotted-decimal IP address (e.g. 195.168.10.10) or a host name that can be resolved to an IP address.
Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) or specify hostname with suffixes **::ipv4** or **::ipv6** (e.g. www.google.com::ipv4 or www.6bone.net::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.

Port
Specify the port number on which the host is listening for incoming requests. Usually Cisco SNMP agents listen on port 161.

Profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

HostMonitor checks status and temperature of each sensor. If some problems detected, HostMonitor finds unit with worst status and show its temperature in Reply field (e.g. if there are 2 units, one with Warning status another with Critical status, HostMonitor will show unit with Critical status). If units have the same status, HostMonitor will find unit with "worst" temperature comparing temperature to threshold specified for the unit.

If critical temp not reached, display
- sensor closest to critical temp (%)
- hottest sensor, name matches (e.g. "Intake" or "CPU")
If no problems detected, these options allow you to choose Reply field mode.

Cisco Fans

This test checks status of all fans on target Cisco system, displays Ok status when no problems detected. Otherwise it sets Bad status with reply like "Fan 1: warning, Fan 5: critical".
In addition to common test parameters, Cisco Fans test has the following options:

Host
Provide a string specifying either a dotted-decimal IP address (e.g. 195.168.10.10) or a host name that can be resolved to an IP address.
Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) or specify hostname with suffixes **::ipv4** or **::ipv6** (e.g. www.google.com::ipv4 or www.6bone.net::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.

Port
Specify the port number on which the host is listening for incoming requests. Usually Cisco SNMP agents listen on port 161.

Profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

Cisco Power

This test checks all power supplies; if no problem detected may display unit with voltage closest to critical value. Also may show voltage on specific power supply, e.g. "12V" or "3.3V" line.
In addition to common test parameters, Cisco Power test has the following options:

Host
Provide a string specifying either a dotted-decimal IP address (e.g. 195.168.10.10) or a host name that can be resolved to an IP address.
Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) or specify hostname with suffixes **::ipv4** or **::ipv6** (e.g. www.google.com::ipv4 or www.6bone.net::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.

Port
Specify the port number on which the host is listening for incoming requests. Usually Cisco SNMP agents listen on port 161.

Profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

HostMonitor checks status and voltage of each power supply. If some problems detected, HostMonitor finds unit with worst status and show its voltage in Reply field (e.g. if there are 2 power supplies, one with Warning status another with Critical status, HostMonitor will show unit with Critical status). If units have the same status, HostMonitor will find unit with "worst" voltage comparing voltage level to low and high thresholds specified for each unit.

If critical voltage not reached, display
- voltage closest to critical level (%)
- specific power supply (e.g. 12V or 5V)
If no problems detected, these options allow you to choose Reply field mode.

Cisco CPU Usage

This test checks the percentage of CPU utilization on routers and network switches running Cisco IOS.
In addition to common test parameters, CPU Usage test has the following options:

Host[:port]
Provide the host name or IP address (e.g. 192.168.1.55) of the host that you wish to monitor.
Optionally you may specify UDP port that is used by Cisco SNMP agent. Port number has to be provided after a colon following the target host address (e.g. 10.10.15.2**:161**).

OS (protocol)
Choose "Cisco" option

Alert when CPU usage over N%
HostMonitor will set Bad test status and start specified alert actions when the percentage of CPU usage exceeds specified limit.
CPU usage in this case is one minute exponentially-decayed moving average value.

Profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

Cisco Memory

This test checks memory usage on Cisco devices.
In addition to common test parameters, Memory test has the following options:

OS (protocol)
Choose "Cisco (SNMP) option

Host
Provide the host name (e.g. mainserver), IPv6 or IPv4 address (e.g. 192.168.1.55) of the host that you wish to monitor.
Optionally you may specify UDP port; port number has to be provided after a colon following the address of SNMP agent (e.g. 195.168.10.10**:161**).

Profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

Alert when CPU memory < N%
Tells HostMonitor to set Bad status when percentage of free processor associated heap memory falls below the specified limit

Alert when I/O memory < N%
Tells HostMonitor to set Bad status when percentage of free shared memory for buffer data falls below the specified limit
(note: not all Cisco devices provide I/O memory related data)

Juniper Health

This test checks overall health status, PIC, FPC, Routing Engine, Flow and CP sessions. When some problem detected, HostMonitor sets Bad status and provides error description in Reply field of the test. E.g. "Left Fan Tray: down; High # of CP sessions: 200"
(HostMonitor warns about high number of CP sessions when
current_CP_session_usage / max_CP_sessions rate is over 85%).
Software retrieves data from Juniper devices using SNMP protocol.

In addition to common test parameters, Juniper Health test has the following options:

Host
Provide a string specifying either a dotted-decimal IP address (e.g. 195.168.10.10) or a host name that can be resolved to an IP address.
Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) or specify hostname with suffixes **::ipv4** or **::ipv6** (e.g. juniper-gate.block5.com::ipv4 or www.6bone.net::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.

Port
Specify the port number on which the host is listening for incoming requests. Usually Juniper SNMP agents listen on port 161.

Profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

Juniper Temperature

HostMonitor checks all or specific units, sets Bad status when temperature exceeds specified limit.
In addition to common test parameters, Juniper Temperature test has the following options:

Host
Provide a string specifying either a dotted-decimal IP address (e.g. 195.168.10.10) or a host name that can be resolved to an IP address.
Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) or specify hostname with suffixes **::ipv4** or **::ipv6** (e.g. juniper-gate.block5.com::ipv4 or www.6bone.net::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.

Port
Specify the port number on which the host is listening for incoming requests. Usually Juniper SNMP agents listen on port 161.

Profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

Check temp of the following unit(s)
This option tells HostMonitor what units should be checked. E.g.
any - check all available temperature sensors
PEM - check all PEM modules
Routing engine - check all "Routing engine" modules (Routing engine 0, Routing engine 1, etc)
Routing engine 1 - check specific module "Routing engine 1"

Alert when temperature exceeds
Specify limit; HostMonitor will set Bad test status when temperature is over specific limit

Juniper Fans

This test checks installed fans.
In addition to common test parameters, Juniper Fans test has the following options:

Host
Provide a string specifying either a dotted-decimal IP address (e.g. 195.168.10.10) or a host name that can be resolved to an IP address.
Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) or specify hostname with suffixes **::ipv4** or **::ipv6** (e.g. juniper-gate.block5.com::ipv4 or www.6bone.net::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.

Port
Specify the port number on which the host is listening for incoming requests. Usually Juniper SNMP agents listen on port 161.

Profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

Consider fans at full speed - Bad/Ok
The following statuses considered as "good":
- running (as active primary)
- standby (as a standby backup)
- ready (ready to run, not running yet)

If you set "Consider fans at full speed - Ok" option, then "run at full speed" status will be considered as good.
"Down" fan status always considered as failure.

Display # of operations/failed fans
You may set the test to show number of good(operational) fans in Reply field of the test; or number of failed fans

Juniper CPU Usage

This test checks the percentage of CPU utilization on Juniper Networks hardware routers.
In addition to common test parameters, CPU Usage test has the following options:

Host[:port]
Provide the host name or IP address (e.g. 192.168.1.55) of the host that you wish to monitor.
Optionally you may specify UDP port that is used by SNMP agent on target router. Port number has to be provided after a colon following the target host address (e.g. 10.10.15.2**:161**).

OS (protocol)
Choose "Juniper" option

max FPC,REc
max SPU
If you choose 1st option, HostMonitor will check all FPC and RE modules and find module with highest CPU usage. If you select "max SPU" then HostMonitor will check all Packet Forwarding Engine modules and find module with highest CPU usage.

Alert when CPU usage over N%
HostMonitor will set Bad test status and start specified alert actions when the percentage of CPU usage exceeds specified limit.

Profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

Juniper Memory

This test checks memory usage on Juniper devices.
In addition to common test parameters, Memory test has the following options:

OS (protocol)
Choose "Juniper (SNMP) option

Host
Provide the host name (e.g. mainserver), IPv6 or IPv4 address (e.g. 192.168.1.55) of the device that you wish to monitor.
Optionally you may specify UDP port; port number has to be provided after a colon following the address of SNMP agent (e.g. 195.168.10.10**:161**).

Profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

Alert when free buffer pool < N%
Checks buffer pool usage. If there are several Routing Engine units, HostMonitor will find init with lowest percentage of free memory.
Memory usage may impact system updates (such as IDP route table additions) when free percentage below 20%.
Juniper device will begin active memory clean up attempts when free percentage below 5%.

Alert when free heap < N%
Checks heap utilization.

Alert when free SPU memory < N%
Checks Packet Forwarding memory usage. If there are several SPU units, HostMonitor will find init with lowest percentage of free memory.
Juniper recommends to start investigation when free SPU memory percentage below 20%. If amount of free memory falls below 5% then transit traffic may be impacted due to inability for forwarding operations.

Big-IP Health

This test checks overall health of the device: status of the disks, power supply status, fans status, failover and sync statuses; in case of failure HostMonitor sets Bad test status and describes the problem using Reply field of the test.
In addition to common test parameters, Big-IP Health test has the following options:

Host
Provide a string specifying either a dotted-decimal IP address (e.g. 195.168.10.10) or a host name that can be resolved to an IP address.
Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) or specify hostname with suffixes **::**ipv4 or **::**ipv6 (e.g. www.balancer.domain.com**::**ipv4 or www.6bone.net**::**ipv6). If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.

Port
Specify the port number on which the host is listening for incoming requests (default port for SNMP agents: 161).

Profile
Choose profile that stores credentials necessary for communication with BIG-IP device (SNMP agent). You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

Optionally you may select one or several of the following settings (tell HostMonitor to set Bad status):
Warn when system functioning suboptimally (failover status)
Warn when status is unknown/incomplete (failover,sync)
Warn when the system is intentionally not functioning (offline)

Big-IP Temperature

This test can check temperature sensors on F5 Big-IP devices.
In addition to common test parameters, Big-IP Temperature test has the following options:

Host
Provide a string specifying either a dotted-decimal IP address (e.g. 195.168.10.10) or a host name that can be resolved to an IP address.
Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) or specify hostname with suffixes **::**ipv4 or **::**ipv6 (e.g. www.balancer.domain.com**::**ipv4 or www.6bone.net**::**ipv6). If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.

Port
Specify the port number on which the host is listening for incoming requests (default port for SNMP agents: 161).

Profile
Choose profile that stores credentials necessary for communication with BIG-IP device (SNMP agent). You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

You may select one or several of the following options and set temperature limit for each option. HostMonitor will set Bad test status and start specified alert actions when temperature exceeds specified limit.
When all values below threshold then HostMonitor will show temperature of the hottest sensor.

- **Check chassis temperature**
- **Check CPU temperature**
- **Check blade temperature**

Big-IP Statistics

This test can monitor various parameters on F5 Big-IP devices.
In addition to common test parameters, Big-IP Temperature test has the following options:

Host
Provide a string specifying either a dotted-decimal IP address (e.g. 195.168.10.10) or a host name that can be resolved to an IP address.
Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) or specify hostname with suffixes **::**ipv4 or **::**ipv6 (e.g. www.balancer.domain.com**::**ipv4 or www.6bone.net**::**ipv6). If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.

Port
Specify the port number on which the host is listening for incoming requests (default port for SNMP agents: 161).

Profile
Choose profile that stores credentials necessary for communication with BIG-IP device (SNMP agent). You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

Alert when <parameter> below X or above Y
Choose what exactly metric should be monitored and set lower and upper limits. HostMonitor will set Bad test status and start specified alert actions when parameter value will be out of the range.

- Failover status summary -no limits can be specified for this parameter, this is text parameter
- Current connections
- Client connections
- Server connections
- SSL connections to clients
- SSL connections to servers
- PVA connections to clients
- PVA connections to servers
- Connections/sec
- Client connections/sec
- Server connections/sec

- SSL connections/sec
- SSL connections ratio
- SSL invalid certificates ratio
- SSL handshake errors ratio
- PVA connections/sec
- PVA connections ratio
- Traffic
- Clients traffic
- Servers traffic
- Dropped packets/sec
- Dropped packets ratio
- HTTP requests/sec
- HTTP 3xx errors ratio
- HTTP 4xx errors ratio
- HTTP 5xx errors ratio
- HTTP errors ratio
- HTTP compression ratio
- HTTP Cache hits ratio
- HTTP Cache hits ratio (for cacheable data)
- DNS requests/sec
- FTP logins/sec
- FTP downloads/sec

Big-IP Disk Free Space

Using SNMP protocol HostMonitor may check free disk space on F5 BIG-IP device and find disk with minimum free space or disk with minimal percentage of free space.
In addition to common test parameters, Big-IP Free Space test has the following options:

Host
Provide the host name or IP address (e.g. 192.168.1.55) of the host that you wish to monitor.
Optionally you may specify UDP port that is used by SNMP agent on target router. Port number has to be provided after a colon following the target host address (e.g. 10.10.15.2**:161**).

SNMP Profile
Choose profile that stores credentials necessary for communication with Big-IP device (SNMP agent). You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.

Timeout, Retries
Timeout - the amount of time in milliseconds the program will wait for a response from the server before the request fails.
Retries - specifies the communications retry count.

You may specify timeout and retries value in text field, type integer numbers separating values by space or colon or semicolon like "2000ms, 1" or "300,1" or "500 1"; also you may open "Connection parameters" window and choose Port, Timeout, Retries

Then you should mark at least one of the following options:

- **Check all local drives** tells HostMonitor to check all disks on target device
- **Check all removable drives** tells HostMonitor to check removable drives
- **Check listed drive(s)** if you need to check specific drive on target system, mark this option and provide list of the volumes; e.g. /shared/* Note: wildcard * can be used at the end of disk name

Alert if free space less than N MB/GB/TB/%
When HostMonitor checks several drives it finds drive with smallest amount of free space (or drive with minimal percentage of free space when "%" alert options is selected) and sets Ok or Bad test status depending on amount of free space and value of this option. Also %DiskID% variable can be used as parameters of the actions, providing information about target drive.

Big-IP CPU Usage

This test checks the percentage of CPU utilization on F5 Big-IP networks devices.
In addition to common test parameters, CPU Usage (Big-IP) test has the following options:

Host[:port]
Provide the host name or IP address (e.g. 192.168.1.55) of the host that you wish to monitor.
Optionally you may specify UDP port that is used by SNMP agent on target router. Port number has to be provided after a colon following the target host address (e.g. 10.10.15.2**:161**).

OS (protocol)
Choose "Big-IP" option

Alert when CPU usage over N%
HostMonitor may check the average CPU load over the 5 or 60 seconds or current CPU usage ratio, depending on time elapsed since previous test probe.
HostMonitor will set Bad test status and start specified alert actions when the percentage of CPU usage exceeds specified limit.

Profile
Choose profile that stores credentials necessary for communication with Big-IP device (SNMP agent). You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries

Specifies the communications retry count.

Big-IP Memory

This test checks memory usage on F5 Big-IP devices.
In addition to common test parameters, Memory test has the following options:

OS (protocol)
Choose "Big-IP (SNMP)" option

Host
Provide the host name (e.g. mainserver), IPv6 or IPv4 address (e.g. 192.168.1.55) of the device that you wish to monitor.
Optionally you may specify UDP port; port number has to be provided after a colon following the address of SNMP agent (e.g. 195.168.10.10**:161**).

Profile
Choose profile that stores credentials necessary for communication with Big-IP device (SNMP agent). You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

Choose one of the following modes and set threshold limit (Megabytes or percentage):

Alert when Total < N MB / %
Check the total host memory

Alert when TTM < N MB / %
Check the total memory available for TMM (Traffic Management Module)

Alert when Non-TTM < N MB / %
Check the total other (non-TMM) memory

Alert when SWAP < N MB / %
Check awailable SWAP memory

Netscaler Temperature

This test can check temperature sensors on Citrix Netscaler devices.
In addition to common test parameters, Netscaler Temperature test has the following options:

Host
Provide a string specifying either a dotted-decimal IP address (e.g. 195.168.10.10) or a host name that can be resolved to an IP address.
Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) or specify hostname with suffixes **::**ipv4 or **::**ipv6 (e.g. www.balancer.domain.com**::**ipv4 or www.6bone.net**::**ipv6). If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.

Port
Specify the port number on which the host is listening for incoming requests (default port for SNMP agents: 161).

Profile
Choose profile that stores credentials necessary for communication with Netscaler device (SNMP agent). You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

You may select one or several of the following options and set temperature limit for each option. HostMonitor will set Bad test status and start specified alert actions when temperature exceeds specified limit.
When all values below threshold then HostMonitor will show temperature of the hottest sensor.

- **Check internal temperature**
- **Check CPU temperature**
- **Check auxiliary temperature**

Netscaler Statistics

This test can monitor various parameters on popular Citrix Netscaler devices.
In addition to common test parameters, Netscaler Statistics test has the following options:

Host
Provide a string specifying either a dotted-decimal IP address (e.g. 195.168.10.10) or a host name that can be resolved to an IP address.
Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) or specify hostname with suffixes **::**ipv4 or **::**ipv6 (e.g. www.balancer.domain.com**::**ipv4 or www.6bone.net**::**ipv6). If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.

Port
Specify the port number on which the host is listening for incoming requests (default port for SNMP agents: 161).

Profile
Choose profile that stores credentials necessary for communication with Netscaler device (SNMP agent). You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

Alert when <parameter> below X or above Y
Choose what exactly metric should be monitored and set lower and upper limits. HostMonitor will set Bad test status and start specified alert actions when parameter value will be out of the range.

- Current connections
- Connections to clients
- Connections to servers
- Current SSL sessions
- Connections/sec
- Client connections/sec
- Server connections/sec
- SSL connections/sec
- SSL connections ratio
- SSL cache hit ratio
- SSL current queue size
- Traffic

- HTTP requests/sec
- HTTP 5xx errors ratio
- HTTP compression ratio
- Cache hit ratio
- Cache memory usage
- DNS requests/sec

Netscaler CPU Usage

This test checks the percentage of CPU utilization on Citrix Netscaler networks devices.
In addition to common test parameters, CPU Usage (Netscaler) test has the following options:

Host[:port]
Provide the host name or IP address (e.g. 192.168.1.55) of the host that you wish to monitor. Optionally you may specify UDP port that is used by SNMP agent on target router. Port number has to be provided after a colon following the target host address (e.g. 10.10.15.2**:161**).

OS (protocol)
Choose "Netscaler" option

CPU / Crypto CPU
You may choose test mode: check the percentage of CPU utilization; or check utilization of the hardware crypto chip (N3 chip, if installed)

Alert when CPU usage over N%
HostMonitor will set Bad test status and start specified alert actions when the percentage of CPU (or N3 chip) usage exceeds specified limit.

Profile
Choose profile that stores credentials necessary for communication with Citrix Netscaler device (SNMP agent). You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

Netscaler Memory

This test checks memory usage on Citrix Netscaler devices.
In addition to common test parameters, Memory test has the following options:

OS (protocol)
Choose "Netscaler" option

Host
Provide the host name (e.g. mainserver), IPv6 or IPv4 address (e.g. 192.168.1.55) of the device that you wish to monitor.
Optionally you may specify UDP port; port number has to be provided after a colon following the address of SNMP agent (e.g. 195.168.10.10**:161**).

Profile
Choose profile that stores credentials necessary for communication with Netscaler device (SNMP agent). You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

Alert when free memory < N MB / %
Tell HostMonitor to set Bad test status and start assigned actions when amount of free memory falls below specific limit (e.g below 1024 MB) or specific percentage (e.g. below 20%).

NetApp Health

HostMonitor checks temperature indicators, failed fans, power supplies, overall file system status, NVRAM status. If any problem detected, HostMonitor sets Bad status and shows error description in Reply field.
HostMonitor retrieves data from NetApp devices using SNMP protocol.
In addition to common test parameters, NetApp Health test has the following options:

Host
Provide a string specifying either a dotted-decimal IP address (e.g. 195.168.10.10) or a host name that can be resolved to an IP address.
Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) or specify hostname with suffixes **::ipv4** or **::ipv6** (e.g. netapp.block5e.com::ipv4 or netapp.bone.net::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.

Port
Specify the port number on which the host is listening for incoming requests. Usually NetApp SNMP agents listen on port 161.

Profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

See also: variables specific to NetApp Health test

NetApp CPU Usage

This test checks the percentage of CPU utilization on NetApp storage devices.
In addition to common test parameters, CPU Usage test has the following options:

Host[:port]
Provide the host name or IP address (e.g. 192.168.1.55) of the host that you wish to monitor. Optionally you may specify UDP port that is used by SNMP agent on target host. Port number has to be provided after a colon following the target host address (e.g. 10.10.15.2**:161**).

OS (protocol)
Choose "NetApp" option

Alert when CPU usage over N%
HostMonitor will set Bad test status and start specified alert actions when the percentage of CPU usage exceeds specified limit.

Profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

NetApp Temperature

HostMonitor may check temperature sensors installed on NetApp devices; if no problem detected HostMonitor may display unit with temperature closest to critical or max ambient temperature.
In addition to common test parameters, NetApp Temperature test has the following options:

Host
Provide a string specifying either a dotted-decimal IP address (e.g. 195.168.10.10) or a host name that can be resolved to an IP address.
Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) or specify hostname with suffixes **::ipv4** or **::ipv6** (e.g. netapp.block5e.com::ipv4 or netapp.bone.net::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.

Port
Specify the port number on which the host is listening for incoming requests. Usually NetApp SNMP agents listen on port 161.

Profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

If no problems detected, the following options allow you to choose Reply field mode:
- sensor closest to critical temp (%)
- max ambient temperature

NetApp RAID

This test may check status of the disks installed on NetApp storage device. It checks the number of disks which are currently broken, number of "prefailed" disks, number of available spare disks and so on.
In addition to common test parameters, NetApp RAID test has the following options:

Host
Provide a string specifying either a dotted-decimal IP address (e.g. 195.168.10.10) or a host name that can be resolved to an IP address.
Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) or specify hostname with suffixes **::ipv4** or **::ipv6** (e.g. www.google.com::ipv4 or www.6bone.net::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.

Port
Specify the port number on which the host is listening for incoming requests. Usually NetApp SNMP agents listen on port 161.

Profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

You may set 2 conditions, e.g. "Alert if Spare disks count below 2" and "Alert if Out Of Date disks count over 0". HostMonitor will set Bad test status when any if these conditions are met.
The following options available:

- Spare disks count below N
- Failed disks count over N
- Failed+Prefailed disks count over N
- Out Of Date disks count over N
- Reconstructing+Verifying+Scrubbing disks count over N

Also test sets the following macro variables

%DS_ActiveCount%	The number of disks which are currently active, including parity disks
%DS_ReconstructingCount%	The number of disks which are currently being reconstructed
%DS_ReconstrparityCount%	The number of parity disks which are currently being reconstructed
%DS_VerifyingparityCount%	The number of parity disks which are currently being verified
%DS_ScrubbingCount%	The number of parity disks which are currently being scrubbed
%DS_FailedCount%	The number of disks which are currently broken
%DS_SpareCount%	The number of available spare disks
%DS_AddingSpareCount%	The number of spare disks which are currently being added into a RAID group
%DS_PrefailedCount%	The number of prefailed disks marked for rapid raid recovery
%DS_OutdatedCount%	The number of outdated disks

NetApp Free Space

This test may check (using SNMP requests) volumes and snapshots on NetApp storage device and find volume or snapshot with minimum free space or volume with minimal percentage of free space.
In addition to common test parameters, NetApp Free Space test has the following options:

NetApp host
Provide host name, IPv6 or IPv4 address (e.g. 10.10.1.55) of the system that you wish to monitor. Optionally you may specify UDP port; port number has to be provided after a colon following the address(hostname) (e.g. 172.168.10.10**:161**).

Profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout, Retries
Timeout - the amount of time in milliseconds the program will wait for a response from the server before the request fails.
Retries - specifies the communications retry count.
You may specify timeout and retries value in text field, type integer numbers separating values by space or colon or semicolon like "2000ms, 1" or "300,1" or "500 1"; also you may open "Connection parameters" window and choose Port, Timeout, Retries

Then you should mark at least one of the following options:
- **Check all volumes**
  tells HostMonitor to check all volumes on target device
- **Check all snapshots**
  tells HostMonitor to check snapshots on target device
- **Check listed drive(s)**
  if you need to check specific volumes/snapshots on target system, mark this option and provide list of the volumes.
  Note1: wildcard * can be used at the end of disk name, e.g. /dev/web* /vol/vol2/
  Note2: 0 size shapshots will be counted only if you set **.**snapshot keyword in "listed drives" field. E.g. if you set "listed drives" using pattern /vol* then test will count snapshots but will skip 0 size snapshots

Alert if free space less than <N> MB/GB/TB/%
When HostMonitor checks several drives it finds drive with smallest amount of free space (or drive with minimal percentage of free space when "%" alert options is selected) and sets Ok or Bad test status depending on amount of free space and value of this option.
Also %DiskID% variable can be used as parameters of the actions, providing information about target drive.

QNAP Health

HostMonitor may check QNAP NAS storages using SNMP protocol.
QNAP Health test method checks disks status, power status, volumes, pools, fans status (some devices do not provide fans status but provide fans speed data; in such case you may use QNAP Fans test method). If any problem detected, HostMonitor sets Bad status and shows error description in Reply field.
In addition to common test parameters, QNAP Health test has the following options:

Host
Provide a string specifying either a dotted-decimal IP address (e.g. 195.168.10.10) or a host name that can be resolved to an IP address.
Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) or specify hostname with suffixes **::ipv4** or **::ipv6** (e.g. app.block5e.com::ipv4 or app.bone.net::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.

Port
Specify the port number on which the host is listening for incoming requests (usually port 161).

Profile
Choose profile that stores credentials necessary for communication with QNAP device. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

Check for uninitialized volumes
Enable this option when uninitialized volumes should trigger Bad test status

QNAP Temperature

Using SNMP protocol HostMonitor may check temperature sensors installed on QNAP devices.
In addition to common test parameters, QNAP Temperature test has the following options:

Host
Provide a string specifying either a dotted-decimal IP address (e.g. 195.168.10.10) or a host name that can be resolved to an IP address.
Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) or specify hostname with suffixes **::ipv4** or **::ipv6** (e.g. app.block5e.com::ipv4 or app.bone.net::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.

Port
Specify the port number on which the host is listening for incoming requests (usually port 161).

Profile
Choose profile that stores credentials necessary for communication with QNAP device. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

Alert when
You may choose one of the following options:
- Alert when **CPU** temperature over specified limit (C)
- Alert when **system** temperature over specified limit (C)
- Alert when **hottest disk** temperature over specified limit (C)
  (in this case HostMonitor will display temperature and disk name)

QNAP Fans

HostMonitor may check fans, find fastest and slowest fans, check if speed within specified range.
In addition to common test parameters, QNAP Fans test has the following options:

Host
Provide a string specifying either a dotted-decimal IP address (e.g. 195.168.10.10) or a host name that can be resolved to an IP address.
Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) or specify hostname with suffixes **::ipv4** or **::ipv6** (e.g. app.block5e.com::ipv4 or app.bone.net::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.

Port
Specify the port number on which the host is listening for incoming requests (usually port 161).

Profile
Choose profile that stores credentials necessary for communication with QNAP device. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

Alert when fan speed below X or above Y (RPM)
Provide minimum and maximum limits. HostMonitor will set Bad test status and trigger specified actions when fan speed is out of specified range.

QNAP Free Space

Using SNMP protocol HostMonitor may check free space on QNAP storage device and find disk with minimum free space or disk with minimal percentage of free space.
In addition to common test parameters, QNAP Free Space test has the following options:

QNAP host
Provide host name, IPv6 or IPv4 address (e.g. 10.10.1.55) of the system that you wish to monitor.
Optionally you may specify UDP port; port number has to be provided after a colon following the address(hostname) (e.g. 172.168.10.10**:161**).

Profile
Choose profile that stores credentials necessary for communication with QNAP storage. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout, Retries
Timeout - the amount of time in milliseconds the program will wait for a response from the server before the request fails.
Retries - specifies the communications retry count.
You may specify timeout and retries value in text field, type integer numbers separating values by space or colon or semicolon like "2000ms, 1" or "300,1" or "500 1"; also you may open "Connection parameters" window and choose Port, Timeout, Retries

Then you should mark at least one of the following options:
- **Check all local drives**
  tells HostMonitor to check all disks on target device
- **Check all removable drives**
  tells HostMonitor to check removable drives
- **Check listed drive(s)**
  if you need to check specific drive on target system, mark this option and provide list of the volumes; e.g. /share/* Note: wildcard * can be used at the end of disk name

Alert if free space less than <N> MB/GB/TB/%
When HostMonitor checks several drives it finds drive with smallest amount of free space (or drive with minimal percentage of free space when "%" alert options is selected) and sets Ok or Bad test status depending on amount of free space and value of this option.
Also %DiskID% variable can be used as parameters of the actions, providing information about target drive.

QNAP CPU Usage

This test checks the percentage of CPU utilization on QNAP storage devices.
In addition to common test parameters, CPU Usage test has the following options:

Host[:port]
Provide the host name or IP address (e.g. 192.168.1.55) of the host that you wish to monitor. Optionally you may specify UDP port that is used by SNMP agent on target host. Port number has to be provided after a colon following the target host address (e.g. 10.10.15.2**:161**).

OS (protocol)
Choose "QNAP" option

Alert when CPU usage over N%
HostMonitor will set Bad test status and start specified alert actions when the percentage of CPU usage exceeds specified limit.

Profile
Choose profile that stores credentials necessary for communication with QNAP device. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

QNAP Memory

This test checks memory usage on QNAP devices.
In addition to common test parameters, Memory test has the following options:

OS (protocol)
Choose "QNAP" option

Host
Provide the host name (e.g. mainserver), IPv6 or IPv4 address (e.g. 192.168.1.55) of the device that you wish to monitor.
Optionally you may specify UDP port; port number has to be provided after a colon following the address of SNMP agent (e.g. 195.168.10.10**:161**).

Profile
Choose profile that stores credentials necessary for communication with QNAP device. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

Alert when free memory < N (MB or %)
You may tell HostMonitor to set Bad test status and start assigned actions when amount of free memory falls below specific limit (e.g below 1024 MB) or specific percentage (e.g. below 30%).

Synology Health

HostMonitor may check Synology NAS storages using SNMP protocol.
Synology Health test method checks disks status, RAID status, power supply status, fans status. If any problem detected, HostMonitor sets Bad test status and shows error description in Reply field.
In addition to common test parameters, Synology Health test has the following options:

Host
Provide a string specifying either a dotted-decimal IP address (e.g. 195.168.10.10) or a host name that can be resolved to an IP address.
Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) or specify hostname with suffixes **::ipv4** or **::ipv6** (e.g. app.block5e.com::ipv4 or app.bone.net::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.

Port
Specify the port number on which the host is listening for incoming requests (usually port 161).

Profile
Choose profile that stores credentials necessary for communication with Synology device. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

Check fans, power supply, disks, RAID status
These checks always active
Check for not initialized disks, RAID repairing, migrating, canceling
If you disable this option, HostMonitor will not set Bad test status when some disks not initialized or RAID status set to Repairing, Migrating or Canceling (while Degrade and Crashed status will trigger alerts regardless of this option)
Check for software updates
With this option enabled, HostMonitor will set Bad test status when updates available for this Synology device

Synology Temperature

Using SNMP protocol HostMonitor may check temperature sensors installed on Synology devices. In addition to common test parameters, Synology Temperature test has the following options:

Host
Provide a string specifying either a dotted-decimal IP address (e.g. 195.168.10.10) or a host name that can be resolved to an IP address.
Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) or specify hostname with suffixes **::ipv4** or **::ipv6** (e.g. app.block5e.com::ipv4 or app.bone.net::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.

Port
Specify the port number on which the host is listening for incoming requests (usually port 161).

Profile
Choose profile that stores credentials necessary for communication with Synology device. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

Alert when
You may choose one of the following options:
- Alert when **system** temperature over specified limit (C)
- Alert when **hottest disk** temperature over specified limit (C)
  (in this case HostMonitor will display temperature and disk name)

Synology Disk Load

HostMonitor may check Synology storage disks load, find busiest disk, set Bad test status and trigger actions when load is over specified limit
In addition to common test parameters, Synology Disk Load test has the following options:

Host
Provide a string specifying either a dotted-decimal IP address (e.g. 195.168.10.10) or a host name that can be resolved to an IP address.
Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) or specify hostname with suffixes **::ipv4** or **::ipv6** (e.g. app.block5e.com::ipv4 or app.bone.net::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.

Port
Specify the port number on which the host is listening for incoming requests (usually port 161).

Profile
Choose profile that stores credentials necessary for communication with Synology device. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

Alert when load of busiest disk is over N %
You may set HostMonitor to check for 1 minute average load, 5 min average load or 15 min average load and provide maximum limit. HostMonitor will set Bad test status and trigger specified actions when disk load exceeds the limit.

Synology Free Space

Using SNMP protocol HostMonitor may check free space on Synology storage device and find disk with minimum free space or disk with minimal percentage of free space.
In addition to common test parameters, Synology Free Space test has the following options:

Target host
Provide host name, IPv6 or IPv4 address (e.g. 10.10.1.55) of the system that you wish to monitor.
Optionally you may specify UDP port; port number has to be provided after a colon following the address(hostname), e.g. 172.168.10.10**:161**

Profile
Choose profile that stores credentials necessary for communication with Synology storage. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout, Retries
Timeout - the amount of time in milliseconds the program will wait for a response from the server before the request fails.
Retries - specifies the communications retry count.
You may specify timeout and retries value in text field, type integer numbers separating values by space or colon or semicolon like "2000ms, 1" or "300,1" or "500 1"; also you may open "Connection parameters" window and choose Port, Timeout, Retries

Then you should mark at least one of the following options:
- **Check all local drives**
  tells HostMonitor to check all disks on target device
- **Check all removable drives**
  tells HostMonitor to check removable drives
- **Check listed drive(s)**
  if you need to check specific volumes on target system, mark this option and provide list of the volumes; e.g. /volume* Note: wildcard * can be used at the end of disk name

Alert if free space less than <N> MB/GB/TB/%
When HostMonitor checks several drives it finds drive with smallest amount of free space (or drive with minimal percentage of free space when "%" alert options is selected) and sets Ok or Bad test status depending on amount of free space and value of this option.
Also %DiskID% variable can be used as parameters of the actions, providing information about target drive.

Synology CPU Usage

This test checks the percentage of CPU utilization on Synology storage devices.
In addition to common test parameters, CPU Usage test has the following options:

Host[:port]
Provide the host name or IP address (e.g. 192.168.1.55) of the host that you wish to monitor. Optionally you may specify UDP port that is used by SNMP agent on target host. Port number has to be provided after a colon following the target host address, e.g. 10.10.15.2**:161**

OS (protocol)
Choose "Synology" option

Alert when CPU usage over N%
HostMonitor will set Bad test status and start specified alert actions when the percentage of CPU usage exceeds specified limit.

Profile
Choose profile that stores credentials necessary for communication with Synology device. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

Test offers option to check either:
- **average/cores** - checks all CPU cores, calculates average load
- **max usage core** - finds CPU core with highest load
Example: if system has 2 CPU cores with 90% load on 1st core and 10% load on 2nd core then average/cores=50%; max_usage_core=90%

Synology Memory

This test checks memory usage on Synology devices.
In addition to common test parameters, Memory test has the following options:

OS (protocol)
Choose "Synology" option

Host
Provide the host name (e.g. mainserver), IPv6 or IPv4 address (e.g. 192.168.1.55) of the device that you wish to monitor.
Optionally you may specify UDP port; port number has to be provided after a colon following the address of SNMP agent, e.g. 10.10.15.2**:161**

Profile
Choose profile that stores credentials necessary for communication with Synology device. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

Alert when
The following options allow you to choose what kind of memory should be monitored and when test status should be changed from Ok to Bad.

- **Free physical memory**
  Amount of physical memory in bytes available to processes running on the device.

- **Free swap memory**
  Amount of swap space (page file) currently available (reserved but not used). If the paging file(s) are expanded, this limit increases accordingly.

- **Free virtual memory**
  Total amount of free memory: free physical memory plus unused space of page file. If the paging file(s) are expanded, this limit increases accordingly.

You may tell HostMonitor to set Bad test status and start assigned actions when amount of free memory falls below specific limit (e.g below 1024 MB) or specific percentage (e.g. below 30%).

SonicWall CPU Usage

This test checks the percentage of CPU utilization on SonicWall network devices.
In addition to common test parameters, CPU Usage test has the following options:

Host[:port]
Provide the host name or IP address (e.g. 192.168.1.55) of the host that you wish to monitor. Optionally you may specify UDP port that is used by SNMP agent on target host. Port number has to be provided after a colon following the target host address, e.g. 10.10.15.2**:161**

OS (protocol)
Choose "SonicWall" option

Profile
Choose profile that stores credentials necessary for communication with SonicWall device. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

Alert when CPU usage over N%
HostMonitor will set Bad test status and start specified alert actions when the percentage of CPU usage exceeds specified limit.

SonicWall Memory

This test checks memory usage on SonicWall devices.
In addition to common test parameters, SonicWall Memory test has the following options:

OS (protocol)
Choose "SonicWall" option

Host
Provide the host name (e.g. mainserver), IPv6 or IPv4 address (e.g. 192.168.1.55) of the device that you wish to monitor.
Optionally you may specify UDP port; port number has to be provided after a colon following the address of SNMP agent, e.g. 10.10.15.2**:161**

Profile
Choose profile that stores credentials necessary for communication with SonicWall device. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

Alert when free memory < N%
You may tell HostMonitor to set Bad test status and start assigned actions when percentage of free memory falls below specific limit (e.g below 20%)

UPS Health

Using SNMP protocol HostMonitor may monitor various uninterruptible power supply devices, check battery status, retrieve active alarm conditions (when device supports such option). If some problem detected HostMonitor will set Bad test status and display problem description in Reply field of the test, you may see messages like 'Battery needs replacing' or 'Battery depleted'.
In addition to common test parameters, UPS Health test has the following options:

UPS
Choose type of the uninterruptible power supply, there are several options:

Generic	- Various devices support standard requests, e.g. TrippLite, OneAC devices
APC	- American Power Conversion units
CyberPower	- CyberPower systems
HP	- Hewlett-Packard Company
Powerware	- Powerware, Eaton, IBM

Alert when on battery for N sec
With this option enabled HostMonitor will set Bad test status and trigger specified actions when UPS running on battery power for N seconds (or more)

Host
Provide IP address or host name of the UPS device. If UPS supports IP v6 then you may provide IPv6 address, e.g. fe80::370:ff56:fed5:22. If you specify hostname with **::ipv4** or **::ipv6** suffix (e.g. npower.bone.net::ipv6), HostMonitor will use specified protocol (IPv6 in this case).

Port
Specify the port number on which UPS is listening for incoming requests. Usually port 161 is used.

Profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the UPS before the request fails.

Retries
Specifies the communications retry count.

UPS Load

HostMonitor may check current UPS load and set Bad test status when output load is out of specified range. SNMP protocol used for this test.
In addition to common test parameters, UPS Load test has the following options:

UPS
Choose type of the uninterruptible power supply, there are several options:

Generic	- Various devices support standard requests, e.g. TrippLite, OneAC devices
APC	- American Power Conversion units
CyberPower	- CyberPower systems
HP	- Hewlett-Packard Company
Powerware	- Powerware, Eaton, IBM

Alert when load below X% or above Y%
Provide minimum and maximum limits. HostMonitor will set Bad test status and trigger specified actions when UPS output load is out of specified range.

Host
Provide IP address or host name of the UPS device. If UPS supports IP v6 then you may provide IPv6 address, e.g. fe80::370:ff56:fed5:22. If you specify hostname with **::ipv4** or **::ipv6** suffix (e.g. npower.bone.net::ipv6), HostMonitor will use specified protocol (IPv6 in this case).

Port
Specify the port number on which UPS is listening for incoming requests. Usually port 161 is used.

Profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the UPS before the request fails.

Retries
Specifies the communications retry count.

UPS Charge level

HostMonitor may check battery charge level and set Bad test status when charge level falls below specified limit. SNMP protocol used for this test.
In addition to common test parameters, UPS Charge Level test has the following options:

UPS
Choose type of the uninterruptible power supply, there are several options:

Generic	- Various devices support standard requests, e.g. TrippLite, OneAC devices
APC	- American Power Conversion units
CyberPower	- CyberPower systems
HP	- Hewlett-Packard Company
Powerware	- Powerware, Eaton, IBM

Alert when charge level below N%
Specify charge level limit. HostMonitor will set Bad test status and trigger specified actions when UPS battery charge level falls below this limit.

Host
Provide IP address or host name of the UPS device. If UPS supports IP v6 then you may provide IPv6 address, e.g. fe80::370:ff56:fed5:22. If you specify hostname with **::ipv4** or **::ipv6** suffix (e.g. npower.bone.net::ipv6), HostMonitor will use specified protocol (IPv6 in this case).

Port
Specify the port number on which UPS is listening for incoming requests. Usually port 161 is used.

Profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the UPS before the request fails.

Retries
Specifies the communications retry count.

UPS Input voltage

HostMonitor may check current input voltage on all input lines and set Bad test status when input voltage is out of specified range. SNMP protocol used for this test.
In addition to common test parameters, UPS Input Voltage test has the following options:

UPS
Choose type of the uninterruptible power supply, there are several options:

Generic	- Various devices support standard requests, e.g. TrippLite, OneAC devices
APC	- American Power Conversion units
CyberPower	- CyberPower systems
HP	- Hewlett-Packard Company
Powerware	- Powerware, Eaton, IBM

Alert when voltage below X or over Y
Provide minimum and maximum limits. HostMonitor will set Bad test status and trigger specified actions when input voltage is out of specified range.

Host
Provide IP address or host name of the UPS device. If UPS supports IP v6 then you may provide IPv6 address, e.g. fe80::370:ff56:fed5:22. If you specify hostname with **::ipv4** or **::ipv6** suffix (e.g. npower.bone.net::ipv6), HostMonitor will use specified protocol (IPv6 in this case).

Port
Specify the port number on which UPS is listening for incoming requests. Usually port 161 is used.

Profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the UPS before the request fails.

Retries
Specifies the communications retry count.

UPS Output voltage

HostMonitor may check current output voltage and set Bad test status when voltage is out of specified range. SNMP protocol used for this test.
In addition to common test parameters, UPS Output Voltage test has the following options:

UPS
Choose type of the uninterruptible power supply, there are several options:

Generic	- Various devices support standard requests, e.g. TrippLite, OneAC devices
APC	- American Power Conversion units
CyberPower	- CyberPower systems
HP	- Hewlett-Packard Company
Powerware	- Powerware, Eaton, IBM

Alert when voltage below X or over Y
Provide minimum and maximum limits. HostMonitor will set Bad test status and trigger specified actions when output voltage is out of specified range.

Host
Provide IP address or host name of the UPS device. If UPS supports IP v6 then you may provide IPv6 address, e.g. fe80::370:ff56:fed5:22. If you specify hostname with **::ipv4** or **::ipv6** suffix (e.g. npower.bone.net::ipv6), HostMonitor will use specified protocol (IPv6 in this case).

Port
Specify the port number on which UPS is listening for incoming requests. Usually port 161 is used.

Profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.
Note: HostMonitor may retrieve data faster when SNMP v2c or SNMP v3 is used.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the UPS before the request fails.

Retries
Specifies the communications retry count.

UPS Temperature

HostMonitor may check battery and ambient temperature sensors (some UPS devices do not have battery temperature sensor) and set Bad test status when temperature is out of specified range. SNMP protocol used for this test.
In addition to common test parameters, UPS Temperature test has the following options:

UPS
Choose type of the uninterruptible power supply, there are several options:

Generic	- Various devices support standard requests, e.g. TrippLite, OneAC devices
APC	- American Power Conversion units
CyberPower	- CyberPower systems
HP	- Hewlett-Packard Company
Powerware	- Powerware, Eaton, IBM

Alert when temp below X or over Y(C)
Provide minimum and maximum limits. HostMonitor will set Bad test status and trigger specified actions when UPS temperature is out of specified range.

Host
Provide IP address or host name of the UPS device. If UPS supports IP v6 then you may provide IPv6 address, e.g. fe80::370:ff56:fed5:22. If you specify hostname with **::ipv4** or **::ipv6** suffix (e.g. npower.bone.net::ipv6), HostMonitor will use specified protocol (IPv6 in this case).

Port
Specify the port number on which UPS is listening for incoming requests. Usually port 161 is used.

Profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the UPS before the request fails.

Retries
Specifies the communications retry count.

UPS Remaining time

HostMonitor may check the UPS and set Bad test status when remaining run time (before battery exhaustion) below the threshold value. SNMP protocol used for this test.
In addition to common test parameters, UPS Remaining Time test has the following options:

UPS
Choose type of the uninterruptible power supply, there are several options:

Generic	- Various devices support standard requests, e.g. TrippLite, OneAC devices
APC	- American Power Conversion units
CyberPower	- CyberPower systems
HP	- Hewlett-Packard Company
Powerware	- Powerware, Eaton, IBM

Alert if remaining time N min or less
Specify threshold value (minutes). HostMonitor will set Bad test status and trigger specified actions when the UPS remaining run time below this limit.

Host
Provide IP address or host name of the UPS device. If UPS supports IP v6 then you may provide IPv6 address, e.g. fe80::370:ff56:fed5:22. If you specify hostname with **::ipv4** or **::ipv6** suffix (e.g. npower.bone.net::ipv6), HostMonitor will use specified protocol (IPv6 in this case).

Port
Specify the port number on which UPS is listening for incoming requests. Usually port 161 is used.

Profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the UPS before the request fails.

Retries
Specifies the communications retry count.

Printer Status

This test method checks various counters and alert flags provided by printers using SNMP protocol. When some problems detected, HostMonitor will set Bad test status and display error(s) description in Reply field of the test (see also %Reply% variable). Also you may use %PrinterDetails% variable as a parameter of the actions triggered by this test, HostMonitor will provide name of the printer, description, location and information about the problem(s).
In addition to common test parameters, Printer Status test has the following options:

Host
Provide IP address or host name of the Printer. If Printer supports IP v6 then you may provide IPv6 address, e.g. fe80::370:ff56:fed5:22. If you specify hostname with **::ipv4** or **::ipv6** suffix (e.g. npower.bone.net::ipv6), HostMonitor will use specified protocol (IPv6 in this case).
Port
Specify the port number on which Printer is listening for incoming requests. Usually port 161 is used.

Profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the Printer before the request fails.
Retries
Specifies the communications retry count.

Ignore open door, cover, interlock status
With this option enabled HostMonitor will ignore the DoorOpen, CoverOpen and InterlockOpen statuses and will set Ok test status if just these problems are detected

Ignore almost full/empty warnings
With this option enabled HostMonitor will ignore "warning" flags such as inputMediaSupplyLow, outputMediaTrayAlmostFull, markerTonerAlmostEmpty, markerWasteInkReceptacleAlmostFull, markerDeveloperAlmostEmpty, mediaPathMediaTrayAlmostFull

Ignore other non-critical problems
With this option enabled all non-critical issues will be ignored by HostMonitor. A critical alert is one that stops the printer from printing immediately and printing can not continue until the critical alert condition is eliminated. Non-critical alerts are those that do not stop printing but may at some future time.

We tested various models of Brother, Canon, HP, Konica, Lexmark, Ricoh, Xerox printers. Printers from other manufacturers may support SNMP protocol and necessary counters as well.

Printer supply levels

This test method checks various counters provided by printers using SNMP protocol. When the level of some supply falls below the specified limit, HostMonitor will set Bad test status and display level(%) and description of the supply type in Reply field of the test (see also %Reply% variable). Also you may use %PrinterDetails% variable as a parameter of the actions triggered by this test, HostMonitor will provide name of the printer, description, location and information about all avilable supplies.
In addition to common test parameters, Printer Supply Levels test has the following options:

Host
Provide IP address or host name of the Printer. If Printer supports IP v6 then you may provide IPv6 address, e.g. fe80::370:ff56:fed5:22. If you specify hostname with **::ipv4** or **::ipv6** suffix (e.g. npower.bone.net::ipv6), HostMonitor will use specified protocol (IPv6 in this case).
Port
Specify the port number on which Printer is listening for incoming requests. Usually port 161 is used.

Profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the Printer before the request fails.
Retries
Specifies the communications retry count.

You can set a minimum threshould for each group of supplies
Check toner, ink levels
HostMonitor will check the toner and ink levels, ribbon and wax (if printer uses such supplies and provides the necessary data)

Check waste, water, binding levels
HostMonitor will check the waste space for toner, ink, wax, water, waste paper, level of binding supplies, staples, covers, etc (if printer uses such supplies and provides the necessary data)

Check OPC, corona wire, transfer units
HostMonitor will check OPC, developer units, fuser oil, cleaner unit, transfer unit, fuser oiler

We tested various models of Brother, Canon, HP, Konica, Lexmark, Ricoh, Xerox printers. Printers from other manufacturers may support SNMP protocol and necessary counters as well.
Note: many Brother printers do not provide toner level data, just drum status and warning flags related to low level

Database test

HostMonitor can test your SQL servers. It supports Interbase, Firebird, MS SQL, MySQL, MariaDB, Oracle, Postgre and Sybase servers. Servers are checked by logging into (and out) of the server. You should specify the server name (the TNS alias for Oracle), database, user name and password. For Interbase you can specify the protocol (TCP, SPX, or NetBEUI).
See also common test parameters

To monitor Oracle servers HostMonitor uses the Oracle Call Interface (OCI.DLL), this means you should have the Oracle client software installed on the computer. The same is true for other SQL servers, install the client software for testing your SQL server. HostMonitor uses the following DLLs:

- gds32.dll to monitor Interbase connections
- fbclient.dll to check Firebird SQL server
- ntwdblib.dll to monitor MS SQL
- libmysql.dll to monitor MySQL
- libmariadb.dll to check MariaDB
- oci.dll to check Oracle
- libpq.dll to monitor PostgreSQL
- libsybdb.dll to monitor Sybase

MS SQL notes: ntwdblib.dll does not allow connection to modern MS SQL servers using Windows Authentication; only SQL Server Authentication can be used (the user name and the password are created by using SQL Server and stored in SQL Server; not based on Windows user accounts). If you need Windows Authentication, then you may use ODBC Query test method instead.

MySQL v8 notes: libmySQL.dll from MySQL Connector v8 is not supported yet; libmySQL.dll version 5.x can be used for connection to MySQL v8 but in this case you have to create a user account using mysql_native_password plugin (because default MySQL v8 caching_sha2_password authentication is not supported by MySQL 5.x)
MySQL known problems: MySQL Connectors prior version 5.26 have bugs and may cause HostMonitor to crash. You may download stable version of MySQL library or at least place all MySQL test items into one folder and use "Non-simultaneously test execution" folder-specific option.

Oracle: its hard to find Oracle client software without critical bugs. Version 8, 11 and especially version 10 have many, many, many bugs. ODBC driver may lead to high CPU usage, handles and memory leakage and may crash application. Please do not use these versions of Oracle client software. New versions are not bug-free either. We can suggest you to use one of the following versions: 9.2.0.8.0, 12.2.0.0 or 19.3.0.0

Interbase/Firebird, MS SQL, MySQL/MariaDB, Oracle, PostgreSQL and Sybase tests may display "unknown" status and appropriate error message in the Reply field when it was impossible to perform the check (e.g. when client library is not installed).

ODBC Query

This test allows you to check the availability of an ODBC data source, run an SQL query, and analyze the value of a specified data field in the result set returned. To set up a test, simply pick one of the ODBC data sources defined in your system, and fill in the Login, Password and Timeout fields. Optionally, provide an SQL query and a condition to check. If no condition is specified, the two possible test status values are "Alive" and "No answer". If a condition is provided, test status can be either:

- "Ok" - if the condition is met;
- "Bad" - if the condition is not met;
- "Unknown" - if the query fails, or the data field specified is not found in the result set.

If field is unavailable, set status
You can use above option to define status of the test in case SQL query was executed without errors but result data set does not contain specified field (specified by row and col parameters). Choose one of the following statuses:

- Unknown
- Bad
- Ok

Retrieve 2nd field
With this option enabled test may retrieve 2 different fields. HostMonitor may check value of field1 and display value of field2 or display field1, also it may display both fields. Also variables %ODBCField1% and %ODBCField2% provide access to retrieved data; variables can be used in Optional status processing expressions or as parameters of actions assigned to ODBC Query test

Note: some ODBC drivers (e.g. MS SQL ODBC Driver version 13.1+) support Integrated Windows authentication and Active Directory Integrated authentication. In this case you may type WindowsAuth instead of login name (for Integrated Windows authentication) or set ADAuth as login name (for Active Directory Integrated authentication). Password field is not used in such case.

See also

- common test parameters
- DSN options (options located on Misc page in the Options dialog)

Windows x64
HostMonitor is 32bit application that can be started on 64bit Windows OS. If you are using Windows x64 Edition and you want to setup ODBC Logging or ODBC test method, you should setup ODBC datasources using 32-bit ODBC Data Source Administrator (e.g. C:\WINDOWS\SysWOW64\odbcad32.exe).
There are x86 and x64 versions of RMA (Remote Monitoring Agent) available, so you may use 32-bit or 64-bit version of ODBC Data Source Administrator depending on RMA version.

Reliability / Known problems

If you are using ODBC Query test method or you have setup ODBC logging, you must be sure that ODBC driver (provided by 3rd party) works reliable and will not cause HostMonitor to crash.

Some bad ODBC drivers:

- Microsoft **dBase** Driver v 4.00 causes resource leakage;

- Old **MySQL** ODBC drivers v3 cause handles leakage in multithreaded environment. If you have several ODBC Query test items that check MySQL servers, we recommend to place these test items in separate folder and use "Non-simultaneously test execution" folder-specific option.

- **MySQL** ODBC drivers version 8.00.11 – 8.00.15 may lead to various problems as well, including memory access violations. If you need to use MySQL ODBC driver version 8.x, please set two options in hostmon.ini file, [Misc] section:

```
[Misc]
ODBC_UseSharedEnvHandle=1
ODBC_KeepSharedEnvHandle=1
```

- Oracle: its hard to find Oracle client software without critical bugs. Version 8, 11 and especially version 10 have many, many, many bugs. ODBC driver may lead to high CPU usage, handles and memory leakage and may crash application. Please do not use these versions of Oracle client software. New versions are not bug-free either. We can suggest you to use one of the following versions: 9.2.0.8.0, 12.2.0.0 or 19.3.0.0

Using this test method you may retrieve information about SQL server status as well.
There are some useful SQL queries:

Firebird: The number of established connections
SELECT COUNT(*) FROM MON$ATTACHMENTS

Interbase: Number of active connections (SMALLINT)
SELECT TMP$ATTACHMENTS FROM TMP$DATABASE

Interbase: Active threads in database (SMALLINT)
SELECT TMP$ACTIVE_THREADS FROM TMP$DATABASE

Interbase: Current memory allocated database (INTEGER)
SELECT TMP$CURRENT_MEMORY FROM TMP$DATABASE

Interbase: Maximum memory ever allocated (INTEGER)
SELECT TMP$MAXIMUM_MEMORY FROM TMP$DATABASE

Interbase: Number of active transactions (SMALLINT)
SELECT TMP$TRANSACTIONS FROM TMP$DATABASE

Interbase: Number of transaction deadlocks (INTEGER)
SELECT TMP$TRANSACTION_DEADLOCKS FROM TMP$DATABASE

Interbase: Number of transaction update conflicts (INTEGER)
SELECT TMP$TRANSACTION_CONFLICTS FROM TMP$DATABASE

Interbase: Records inserted into database (INTEGER)
SELECT TMP$RECORD_INSERTS FROM TMP$DATABASE

Interbase: Records updated to database (INTEGER)
SELECT TMP$RECORD_UPDATES FROM TMP$DATABASE

Interbase: Records deleted from database (INTEGER)
SELECT TMP$RECORD_DELETES FROM TMP$DATABASE

MS SQL: Number of active connections:
SELECT COUNT(DBID) AS TOTALCONNECTIONS FROM SYS.SYSPROCESSES

MySQL: The number of failed attempts to connect to the MySQL server.
SHOW GLOBAL STATUS LIKE 'Aborted_connects'

MySQL: The number of connections that were aborted
because the client died without closing the connection properly
SHOW GLOBAL STATUS LIKE 'Aborted_clients'

MySQL: The maximum number of connections that have been in use simultaneously since the server started.

SHOW GLOBAL STATUS LIKE 'Max_used_connections'

MySQL: The number of files that are open.
SHOW GLOBAL STATUS LIKE 'Open_files'

MySQL: The number of tables that are open.
SHOW GLOBAL STATUS LIKE 'Open_tables'

Oracle: CPU Usage Per Sec.
SELECT value FROM sys.v_$sysmetric WHERE metric_name = 'CPU Usage Per Sec'
The CPU Time Per Sec Oracle metric shows the amount of CPU usage per second for the specific task, SQL statement or session.

Oracle: Current Logons Count.
SELECT value FROM sys.v_$sysmetric WHERE metric_name = 'Current Logons Count'
The Current Logons Count Oracle metric is the total number of current logons.
Measurement unit: Logons

Oracle: Current Open Cursors Count.
SELECT value FROM sys.v_$sysmetric WHERE metric_name = 'Current Open Cursors Count'
The Current Open Cursors Count Oracle metric refers to the current number of open cursors; whether they are being utilized or not.

Oracle: Current OS Load (Number Of Processes)
SELECT value FROM sys.v_$sysmetric WHERE metric_name = 'Current OS Load'

Oracle: Cursor Cache Hit Ratio.
The Cursor Cache Hit Ratio Oracle metric is determined by the ratio of the number of times an open cursor was found divided by the number of times a cursor was sought.
SELECT value FROM sys.v_$sysmetric WHERE metric_name = 'Cursor Cache Hit Ratio'

Oracle: Database CPU Time Ratio.
Measurement unit: % Cpu/DB_Time
SELECT value FROM sys.v_$sysmetric WHERE metric_name = 'Database CPU Time Ratio' order by group_id

Oracle: Host CPU Utilization (%).
SELECT value FROM sys.v_$sysmetric WHERE metric_name = 'Host CPU Utilization (%)' order by group_id

Sybase: Number of active connections:
SELECT COUNT(*) FROM MASTER.DBO.SYSPROCESSES

There are more useful SQL queries for most popular SQL servers listed in Appendix #1 of the manual.

SNMP Get

The Simple Network Management Protocol is the Internet standard protocol for exchanging management information between management console applications and managed entities (hosts, routers, bridges, hubs). Using this powerful test HostMonitor can control many different parameters of network devices.
In addition to the common test parameters, the SNMP test has the following options:

Agent address
Here you should provide a string specifying either a dotted-decimal IP address (e.g. 195.168.10.10) or a host name that can be resolved to an IP address, an IPX address (in 8.12 notation), or an Ethernet address.
Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) and specify hostname with suffixes ::ipv4 or ::ipv6 (e.g. www.google.com::ipv4 or www.6bone.net::ipv6). If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.
Note: on Windows NT 4.0, Windows 2000 and Windows XP SP1 IPv6 protocol is not supported. You may use menu Tools -> Local Info to check is your system IPv6 ready.
Also you may specify port that is used by target SNMP agent. This parameter is optional; port number has to be provided after a colon following the address of SNMP agent. (E.g. 195.168.10.10**:161**). You cannot specify port number when target host specified by IPv6 address.

SNMP profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

OID (object identifier)
The name that uniquely identifies the object for testing.
For example OID "1.3.6.1.2.1.2.1.0" represents the number of network interfaces on which your system can send/receive IP datagrams; OID "1.3.6.1.2.1.6.9.0" represents the number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT; etc. To get a list of valid OIDs for your SNMP enabled devices you should contact the vendor of the device. They should be able to give you a MIB file that contains all the OIDs for the device. If you cannot contact the vendor, try to find the file on the Internet. Numerous free resources offer wide lists of MIB files for various devices (e.g. http://www.mibdepot.com/index.shtml)

When you are configuring SNMP Get test method with MIB Browser installed HostMonitor allows you to specify SNMP variables by a name (e.g. iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0) as well as by an OID in numeric format (e.g. 1.3.6.1.2.1.1.3.0). If you click on "Browse MIBs" button next to "OID" field, HostMonitor will launch MIB Browser displaying the hierarchy tree of SNMP variables. The specified variable (if any) is highlighted and additional information is displayed for it (such as status, access mode, description). Now you may browse variables, choose another variable if needed and click [Ok] button to use the selected variable by HostMonitor.

Starting from version 9.18 HostMonitor allows you to use expressions like
TotalTraffic1 = [1.3.6.1.2.1.2.2.1.10.1] + [1.3.6.1.2.1.2.2.1.16.1]
In such case HostMonitor will retrieve 2 counters (1.3.6.1.2.1.2.2.1.10.1 - total number of octets received on interface #1; 1.3.6.1.2.1.2.2.1.16.1 - total number of octets transmitted out of interface #1) calculate sum of these counters and check result.

When you are using this expression, %MIBNAME%, %MIBNAMESHORT% and %PATH% variables will be set to TotalTraffic1 (name of the variable specified in this expression); while %OBJECT% variable will be set to [1.3.6.1.2.1.2.2.1.10.1] + [1.3.6.1.2.1.2.2.1.16.1]

Also you may use folder-level variables instead of expression. In such case variable should be specified using Folder Properties dialog and it should contain valid expression.
For example you may use [1.3.6.1.2.1.2.2.1.10.1]+[1.3.6.1.2.1.2.2.1.16.1] string for %fvar_totaltraffic1% folder variable and then just type %fvar_totaltraffic1% when setup SNMP Get test item. In such case %MIBNAME%, %MIBNAMESHORT% and %PATH% variables will be set to totaltraffic1 while %OBJECT% variable will be set to [1.3.6.1.2.1.2.2.1.10.1]+[1.3.6.1.2.1.2.2.1.16.1]

When you are using expression for SNMP Get test, counters should be specified by OID numbers enclosed in square brackets. MIB names cannot be used in expressions.
Also you may use round brackets (to change common rules of precedence) and the following operators:

div	integer division, the value of (x div y) is the value of x divided by y and then rounded in the direction of zero to the nearest integer
mod	remainder
*	multiplication
+	addition
-	subtraction
or	bitwise OR operation
and	bitwise AND operation
xor	bitwise XOR operation

Note: When at least one operand of AND/OR/XOR operators specified in binary format, HostMonitor will use binary format for result as well. E.g. (6 and '11111111B') will return '110B'. If you want to convert number in binary format to decimal format, you may use addition (+), subtraction (-) or multiplication operations. E.g. '110B'+0 will return '6'.
Example:
var1 = (([1.3.6.1.2.1.2.2.1.10.1]+[1.3.6.1.2.1.2.2.1.16.1]) div ([1.3.6.1.2.1.2.2.1.14.1]+[1.3.6.1.2.1.2.2.1.20.1]+1) AND 11110000B) +0

Condition for alert

HostMonitor can compare values returned by the device with a specified string and start alert actions if the returned value is:

- less/more than the specified value
- equal to/different from the specified number or string
- contains/doesn't contain the specified string

Also HostMonitor offers 9 alert conditions to check how new value changes comparatively to the previous test results:

"increases by"	-	HM sets "Bad" status when value increases by specified number or more
"decreases by"	-	HM sets "Bad" status when value decreases by specified number or more
"changes by"	-	HM sets "Bad" status when value changes by specified number or more
"increases by (%)"	-	HM sets "Bad" status when value increases by specified (or greater) percentage
"decreases by (%)"	-	HM sets "Bad" status when value decreases by specified (or greater) percentage
"changes by (%)"	-	HM sets "Bad" status when value changes by specified (or greater) percentage
"increases /sec"	-	HM sets "Bad" status when average increase of the counter (per second) is greater than the specified limit ((new value - old value)/elapsed time >= specified limit)
"decreases /sec"	-	HM sets "Bad" status when average decrease of the counter (per second) is greater than the specified limit ((old value - new value)/elapsed time >= specified limit)
"changes /sec"	-	HM sets "Bad" status when average change of the counter (per second) is greater than the specified limit (abs(new value - old value)/elapsed time >= specified limit)

Note: if OCTET STRING returned by SNMP agent contains non-printable characters, HostMonitor displays them using %XX format where "XX" is a hexadecimal code of a character (byte). This is useful when you need to check MAC address or some other binary counters.

When MIB Browser installed and SNMP agent tested directly by HostMonitor then you may use “Real time chart” option (main window popup menu) to monitor numeric counters.

SNMP Credentials

SNMP Credentials dialog allows you to setup list of SNMP profiles (accounts). Profiles store login or community string and other information necessary for communication with SNMP agent.
For each profile you should specify name of the profile (your choice) and version of SNMP protocol used by SNMP agent. HostMonitor supports SNMP v1, v2c and v3.

Community
If SNMP agent uses SNMP v1 or v2c protocol, specify the SNMP community name (often SNMP agents use "public" as community string).

If SNMP agent is configured to use SNMP v3, you should specify the following parameters:

Username
Enter the username that is configured for the SNMP agent(s). An SNMP device, upon reception of a request, uses this username to look for configured authentication and encryption parameters and applies them to the received request message.

Context
Specify the context needed to identify specific SNMP instances. This parameter is optional.

Authorization
You may choose one of the following authorization methods: None (no authorization), MD5, SHA-1, SHA256, SHA384 or SHA512.
Only MD5 and SHA1 algorithms are defined in SNMP standards however many manufacturers use more strong "unofficial" SHA256/384/512 hashes.

Authorization password
If authorization is used, use this field to specify authorization password.

Privacy type
Specify encryption mode: None, DES, 3DES, AES128, AES192, AES256, AES192C, AES256C.
Note1: AES192, AES256, AES192C and AES256C are not defined in SNMP standards however many manufacturers use these algorithms.
Note2: AES192C and AES256C modes used by Cisco, they are equivalent to AES192/AES256 when SHA256, SHA384 or SHA512 authorization mode is used. We would not recommend to use MD5+AES192C/AES256C or SHA1+AES192C/AES256C.
Note3: we do not recommend DES or 3DES encryption mode. DES is not secure. 3DES slower and less secure than AES encryption.

Privacy password
Specify key for encryption

Check OPAQUE data for float numbers
This option tells HostMonitor to check for single and double precision floating-point numbers that can be encoded as OPAQUE SNMP data and compare such numbers with specified value (number that specified as alert condition for each specific test item)

SNMP Trap

SNMP Trap test method allows you to receive SNMP Trap messages - unsolicited messages from a device (such as router, server) to an SNMP console. Traps might indicate power-up or link-up/down conditions, temperatures exceeding certain thresholds, high traffic, etc. Traps provide an immediate notification for events that otherwise might only be discovered during occasional polling.

This test method is different from any other. Unlike the rest of tests that really test some devices (by sending request and receiving response), SNMP Trap test method was implemented as listener - it does not send any requests. HostMonitor listens for incoming messages from network hosts and reacts in real-time.
That is why time interval fields for this test method are disabled; however you still may use Schedule as well as for any other method. HostMonitor simply ignores messages that come within restricted time period.

Active RMA agent is able to collect, filter and forward SNMP Trap messages from remote networks to HostMonitor. Some notes regarding Active RMA:

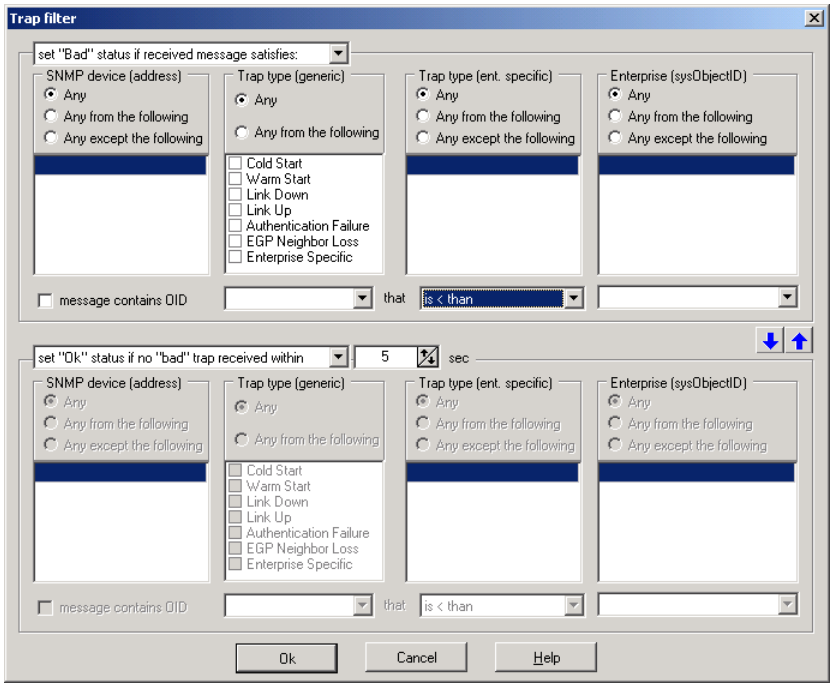
- RMA encrypts Trap messages like any other traffic between HostMonitor and RMA
- When you setup SNMP Trap test item and choose remote active agent using "Test by" property, HostMonitor send filter settings to the agent. This allows filtering incoming trap messages on remote site and sending to HostMonitor only messages that satisfy specified requirements.
- HostMonitor does not use "Backup RMA" for SNMP Trap test items.

In addition to the common test parameters, the SNMP Trap test has the following options:

- Bad message filter
- Good message filter
- Display

In the Options dialog (Miscellaneous : SNMP Trap test settings page) you may specify general Trap Watcher settings (e.g. set UDP port number, disable certain versions of SNMP Trap messages) and provide special instructions to warn about high SNMP traffic from network devices.

SNMP v3 notes: If you need to receive encrypted SNMP Trap messages, you should set "Engine ID" field for some accounts using SNMP Credentials window. For example, if you are already using an SNMP account with authentication and privacy settings (algorithms, username, password) to check traffic, fans or CPU usage on your router, then you can set only Engine ID parameter for that account and it will be used by HostMonitor when SNMP Trap test method receives an encrypted trap message from that router.



Filters:

When you setup SNMP Trap test item, you should provide filters (one or more conditions) that will separate “Bad” and “Good” messages. Message passes the filter only when it matches **ALL** specified requirements of the filter.
When HostMonitor receives message that fits “Bad” filter conditions, it changes status of the test item to “Bad”. If HostMonitor receives message that fits “Good” filter conditions, it changes status of the test item to “Ok”.
Different test items may react on different trap messages. For example one test item may react on router configuration changes, while another test reacts on incoming connections received by your firewall.
It is also possible to change status of the test if no “Bad” (or “Good”) trap messages were received within specified time interval. For example, you may setup 3rd test item alerting you when a temperature-monitoring device does not send any messages for 5 min.

Following options define which situation will be reported as “bad”:

- **set "Bad" status if received message satisfies:**
  with this option selected HostMonitor will set “Bad” status when received trap message meets all conditions of the “Bad” filter.

- **set "Bad" status if no "Good" trap received within NN sec**
  with this option selected HostMonitor will assign “Bad” status to the test item when there were no messages received within specified interval of time or when received messages don’t meet conditions of the “Good” filter.

The same 2 options are available for “Good” messages:

- set "Ok" status if received message satisfies:

- set "Ok" status if no "Bad" trap received within NN sec

Plus there is one more option for “Good” status:

- Set Ok status by acknowlegement (manually)
  With this option enabled, test item will remain “Bad” until operator Acknowledge status (then status will be changed to Ok)

You should provide at least one filter (“Bad” or “Good) or both.

Filter conditions:

There are 2 sets of conditions in the Trap Filter dialog - “Bad” and “Good” filters. Message passes the filter only when it matches ALL specified requirements. If received message does not match neither “Bad” nor “Good” filter, trap message is ignored by the test item (but of course it can be processed by another SNMP Trap test item with different filter).

So, let’s describe the conditions:

SNMP device

Match against the source device – device that has sent message. You can provide list of IP addresses and choose one of the following options:

• Any	messages from any device will be accepted
• Any from the following	messages only from specified devices will be accepted
• Any except the following	messages from any devices except specified will be accepted

List editing tips

- To add new items to the end of the list go to the last existing line and press Down Arrow key.
- Press INSERT key to insert new item.
- Press CTRL+DEL to remove item.
- Press F2 to edit item.

Note: also you may specify ranges of IP addresses from which SNMP Trap message may be accepted. E.g. 192.168.1.1 - 192.168.1.100

Trap type (generic)

Match against the generic type of the trap:

• Any	select this option to accept messages of any type.
• Any from the following	if you want to accept just some type of messages, select this option and mark one or several possible event types: Cold Start, Warm Start, Link Down, Link Up, Authentication Failure, EGP Neighbor Loss, Enterprise Specific ○ Cold Start - the sender is reinitializing and its configuration may change ○ Warm Start - the sender is reinitializing but its configuration will not change ○ Link Down - failure in one of the agent’s links ○ Link Up - one of the agent’s links has come up ○ Authentication Failure - the agent received a protocol message improperly authenticated

	○ EGP Neighbor Loss - an Exterior Gateway Protocol neighbor is down ○ Enterprise Specific - The trap is identified as not being one of the basic one

Trap type (specific)
You can provide list of enterprise specific codes (numbers) and choose one of the following options:

• Any	accept messages of any type
• Any from the following	accept only messages that have one of the specified enterprise specific types
• Any except the following	accept messages with any enterprise specific type except those that are specified in the list.

List editing tips
- To add new items to the end of the list go to the last existing line and press Down Arrow key.
- Press INSERT key to insert new item.
- Press CTRL+DEL to remove item.
- Press F2 to edit item.

Enterprise
Enterprise field of the trap contains an OBJECT IDENTIFIER, which names the device that sends the trap. Here you may provide list of OIDs and choose one of the following options:

• Any	do not check Enteprise field of the traps
• Any from the following	accept only messages from listed devices.
• Any except the following	accept all messages except from the devices on the list

Message contains OID
This option allows you to check incoming trap messages for some specific variable and
- compare its value to some constant (string or number)
- compare current value of the variable with previous value of this variable

Just provide OID (OBJECT IDENTIFIER) of the variable and choose one of the following compare conditions:

Condition for alert

is < than	-	message fits the condition when value of the variable is less than specified number
is > than	-	message fits the condition when value of the variable is greater than specified number
is = to	-	message fits the condition when value of the variable is equal to specified number or string
is <> from	-	message fits the condition when value of the variable is not equal to specified number or string
contains	-	message fits the condition when value of the variable contains specified string
does not contain	-	message fits the condition when value of the variable does not contain specified string

Also HostMonitor supports 9 conditions that allow you to check how new value had changed versus its previous value:		
"increases by"	-	trap message fits the condition when new value is greater then the old one by specified number or more
"decreases by"	-	message fits the condition when new value is less then old one by specified number or more
"changes by"	-	message fits the condition when absolute difference between new and old value is equal or greater then specified number
"increases by (%)"	-	message fits the condition when new value had increased by specified (or greater) percentage versus the old one
"decreases by (%)"	-	message fits the condition when new value had decreased by specified (or greater) percentage versus the old one
"changes by (%)"	-	message fits the condition when an absolute difference between new and old values measured as a percentage of an old value is equal or greater then specified percentage number
"increases /sec"	-	message fits the condition when average increase of the counter (per second) is greater than the specified limit ((current value - old value)/elapsed time >= specified limit)
"decreases /sec"	-	message fits the condition when average decrease of the counter (per second) is greater than the specified limit ((old value - current value)/elapsed time >= specified limit)
"changes /sec"	-	message fits the condition when average absolute difference (change) of the counter (per second) is greater than the specified limit (abs(current value - old value)/elapsed time >= specified limit)

Note 1: When you are configuring SNMP Trap test method with MIB Browser installed HostMonitor allows you to specify SNMP variables by a name (e.g. iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0) as well as by an OID in numeric format (e.g. 1.3.6.1.2.1.1.3.0). If you click on "Browse MIBs" button next to "OID" field, HostMonitor will launch MIB Browser displaying the hierarchy tree of SNMP variables. The specified variable (if any) is highlighted and additional information is displayed for it (such as status, access mode, description). Now you may browse variables, choose another variable if needed and click [Ok] button to use the selected variable by HostMonitor.

Note 2: You may type "any" instead of specific object identifier. In such case HostMonitor will check every object contained in the Trap message.
Also you may use trailing wildcard * for "Message contains OID" test property. E.g. 1.3.6.1.2.1.1.3*

Note 3: If you use relative compare modes (increases by .. decreases by .. changes by .. increases by ..(%) decreases by ..(%) changes by ..(%) increases /sec decreases /sec changes /sec) and various network sources can send the same variable, you should restrict the filter to accept SNMP Trap messages from a single source only. Otherwise HostMonitor could compare variables that were received from different sources (that usually does not make any sense). Create several test items (one item for each network source) if you have to use relative compare mode for some variable.

Counters fit expression

Instead of “Message contains OID” option you may mark “Counters fit expression” checkbox and provide logical expression that will be applied to incoming trap messages. This option allows you to check several parameters (counters) of the message using expressions like the following:

('gmail.com' in '%1.3.6.1.4.1.3093.1.1.0%') and (%1.3.6.1.4.1.3093.1.3.0% > 995)

Such expression means - trap message will pass verification when it contains OID 1.3.6.1.4.1.3093.1.1.0 and its value contains ‘gmail.com’ string; also trap message contains OID 1.3.6.1.4.1.3093.1.3.0 with numeric value above 995.

In these expressions you can use:

- constant numbers and strings (in quotes). Strings that contain a number plus one of the following unit specificators [ms, Kb, Mb, Gb, %] are compared as numbers, so that '900 Kb' is less than '9 Mb'
- variables that represent trap message OIDs. Such variables should be marked by % signs. HostMonitor resolves OID variables using values from received trap message. If received SNMP Trap message does not contain specified OID, HostMonitor sets variable to empty string ‘’ before logical expression evaluation;
- logical operators [and, or, xor, not, <, >, >=, <=, ==, <>];
- arithmetic operators [div, mod, +, -]
  div (integer division)
  mod (remainder)
  + (addition)
  - (subtraction)
  Note: The value of (x div y) is the value of x divided by y and then rounded in the direction of zero to the nearest integer; 'mod' operator returns the remainder obtained by dividing its operands (in other words, (x mod y) == x - (x div y) * y);
- operator [in]. Expression ‘Substr’ in ‘Str’ searches for a sub string, Substr, in a string Str. Operator returns True when Str contains Substr; otherwise operator returns False
- parentheses. In complex expressions, common rules of precedence determine the order in which operations are performed:

Operators	Precedence
not	first (highest)
div, mod	second
+, -, in	third
<, >, >=, <=, ==, <>	fourth
and, or, xor	fifth (lowest)

An operator with higher precedence is evaluated before an operator with lower precedence, while operators of equal precedence associate to the left. You can use parentheses to override precedence rules. An expression within parentheses is evaluated first and then its result is treated as a single operand.

Display
This option defines what information will be displayed in the Reply field of the test item. Choose one of the following options:

• Agent address	Represents IP address of the host that have sent the message
• Trap type	Represents type of the trap. It provides information about generic type and enterprise specific number. Generic type could be one of the following: Cold Start, Warm Start, Link Down, Link Up, Auth Failure, EGP Loss, Specific. o Cold Start - the sender is reinitializing and its configuration may change o Warm Start - the sender is reinitializing but its configuration will not change o Link Down - failure in one of the agent's links o Link Up - one of the agent's links has come up o Authentication Failure - the agent received a protocol message improperly authenticated o EGP Neighbor Loss - an Exterior Gateway Protocol neighbor is down o Enterprise Specific - the trap is identified as not being one of the basic traps Enterprise specific number is only applicable when generic trap type is Enterprise Specific, otherwise enterprise specific number is 0
• Enterprise	Enterprise field contains an OBJECT IDENTIFIER which names the device that have sent the trap
• OID	Variable name (OID)
• Counter value	Variable value
• Relative value	Relative value of the variable. This is could be useful when you check incoming trap messages for some specific variable and compare current value of the variable with its previous value (see "Message contains OID…" option in the Trap Filter dialog). Depending on the test settings HostMonitor may display: o simple difference between current and previous value (if you use "increases by", "decreases by" or "changes by" compare option) o relative difference as a percentage of previous value (if you use "increases by (%)", "decreases by (%)" or "changes by (%)" compare option) o average increase/decrease of the counter per second since previous message (if you use "increases /sec", "decreases /sec" or "changes /sec" compare option)
• OID & Value	Display variable name (OID) and variable value

Increment counters when no messages received

If you are using SNMP Trap test items with “Set Ok status if no Bad trap received within N sec” option, HostMonitor sets "Ok" status to the test item when there are no messages received within specified time interval or when received messages don't meet conditions of the "Bad" filter.
With “Increment counters when no messages received” option enabled HostMonitor sets the status AND increments Recurrences and statistical counters every N seconds. This allows the use of escalation alerts even if HostMonitor does not receives any messages from monitoring device. Of course the same rule applies to “Set **Bad** status if no Ok trap received within N sec”.

See also: variables specific to SNMP Trap test

SNMP Table

This test uses SNMP protocol, like SNMP Get test method. The Simple Network Management Protocol (SNMP) is the Internet standard protocol for exchanging management information between management console applications and managed entities (hosts, routers, bridges, hubs). Using SNMP protocol, HostMonitor can control many different parameters of various network devices.
While single SNMP Get test item allows you to check just one counter provided by specified SNMP agent, single SNMP Table test item may check hundreds counters at once. Single SNMP Table test item cannot check various SNMP agents (check different hosts) but it can retrieve set of counters from target agent and perform various checks. E.g. you may setup HostMonitor to look for a maximum or minimum counter within some table, check average value or look for most rapidly changing counter.
In some cases you may replace thousand of you SNMP Get test items with single SNMP Trap test. E.g. if you want to receive alert when any network interface on your router changes status, you may easily do this using single SNMP Table test.
In addition to the common test parameters, the SNMP Table test has the following options:

Host
Specify target host name or address. You may provide either a dotted-decimal IP address or a host name that can be resolved to an IP address, an IPX address (in 8.12 notation), or an Ethernet address.
Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) and specify hostname with suffixes ::ipv4 or ::ipv6 (e.g. www.google.com::ipv4 or www.6bone.net::ipv6). If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.
Note: IPv6 protocol is not supported on Windows NT 4.0, Windows 2000 and Windows XP SP1. You may use menu Tools -> Local Info to check is your system IPv6 ready.

Port
Specify the port number on which target SNMP agent is listening for incoming requests. By default SNMP agents use port 161.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

SNMP profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.

Table OID
Here you specify what exactly information should be requested from target SNMP agent by providing object identifier. In contrast to SNMP Get test method (where you should specify OID of single instance counter or specific instance of multi-instance counters), here you should provide OID that identifies multi-instance counter. E.g. when the following OIDs identify current operational state for 64 interfaces on target router
- 1.3.6.1.2.1.2.2.1.8.1
- 1.3.6.1.2.1.2.2.1.8.2
....
- 1.3.6.1.2.1.2.2.1.8.64
SNMP Table test allows you to specify OID 1.3.6.1.2.1.2.2.1.8 when you want to check state of all network interfaces on target device.
When you are configuring SNMP Table test method with MIB Browser installed HostMonitor allows you to specify SNMP variables by a name (e.g. iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInErrors) as well as by an OID in numeric format (e.g. 1.3.6.1.2.1.2.2.1.14). If you click on "Browse MIBs" button next to "OID" field, HostMonitor will launch MIB Browser displaying the hierarchy tree of SNMP variables. The specified variable (if any) is highlighted and additional information is displayed for it (such as status, access mode, description).

Max rows
In some cases table provided by SNMP agent can be huge but it's enough to check just part of the table. You may use this option to set maximum number of rows (counters) that should be retrieved from target host and checked by HostMonitor thus you may save system resources and increase performance.

Apply filter
Also you may provide additional filter based on counter values. For example if you want to find minimum **nonzero** counter, you should use "Apply filter: skip items are = to 0" option.

Alert when
The following options specify how exactly retrieved data should be checked and when HostMonitor should set "bad" test status and start alerts assigned to the test item. There are 6 summation modes and 15 comparison modes offered by HostMonitor.

First you should choose **summation mode**:

- any item	check every retrieved counter
- min	check counter with minimum value
- max	check counter with maximum value
- average	check average value of all counters
- total	check total (cumulative) value of all counters
- row count	check number of retrieved counters

Then you should set **comparison mode** and threshold value. HostMonitor can compare counter values retrieved from SNMP agent with a specified number (or string) and set "Bad" status if counter value is:

- less or more than the specified number (string) ;
- equal to or different from the specified number (string)
- contains or does not contain the specified string

Also HostMonitor offers 9 alert conditions that allow you to check how counter values change comparatively to the values received by previous test probe:

- increases by	- HostMonitor sets "Bad" status when counter value increases by (or over) the specified limit
- decreases by	- HostMonitor sets "Bad" status when counter value decreases by (or over) the specified limit
- changes by	- HostMonitor sets "Bad" status when counter value either increases or decreases by (or over) the specified limit

The following options allow you to check how counter value changes relatively to previous value of the same counter percentage wise

- increases by (%)	- HostMonitor sets "Bad" status when counter value increases by (or over) the specified percentage
- decreases by (%)	- HostMonitor sets "Bad" status when counter value decreases by (or over) the specified percentage
- changes by (%)	- HostMonitor sets "Bad" status when counter value changes by (or over) the specified percentage

Other options allow you to check how fast counter value changes over time

- increases /sec	- HostMonitor sets "Bad" status when average increase of the counter (per second) is greater than the specified limit. I.e. (new value - old value)/elapsed time >= specified limit
- decreases /sec	- HostMonitor sets "Bad" status when average decrease of the counter (per second) is greater than the specified limit. I.e. (old value - new value)/elapsed time >= specified limit
"changes /sec"	- HostMonitor sets "Bad" status when average change of the counter (per second) is greater than the specified limit. I.e. abs(new value - old value)/elapsed time >= specified limit

Note 1: If you are using “Alert if **any item**” mode for SNMP Table test, HostMonitor checks entire table (all counters passed thru filter) and finds not just a value that fits specified alert threshold but finds the counter that maximally satisfies specified condition.
For example:

- if you setup “Alert if any item < than 1000” condition and SNMP agent returns numbers 2222, 100, 50, 5000 then HostMonitor will report 50 as test result (1st number that fits condition is 100 but HostMonitor will continue scanning and find minimal number 50).
- If you setup “Alert if any item > than 1000” condition and SNMP agent returns numbers 2222, 100, 50, 5000 then HostMonitor will report 5000 as test result (not 2222)

The same rule works when you use “increases by”, “decreases by”, “changes by %” and other comparative modes - HostMonitor will find counter that increased or decreased maximally (or increased/decreased maximally percentage wise).
This way you may find not just network interface with new errors but find interface that has the highest number of new errors; or find interface where growth of incoming network traffic has the highest rate.

Note 2: Test Info dialog shows table with all counters retrieved from target host; it shows OID, current counter value, old counter value and difference for each row. Also you may view this information using Web Service.

Note 3: There are variables specific to SNMP Table test; you may use these variables as parameters of some actions assigned to such test items.

Active Script

Starting from HostMonitor version 3.40 you can create your own tests using different script languages such as Visual Basic Script or Java Script. HostMonitor uses Microsoft ActiveScripting technology to execute scripts that were written by you or somebody else. Theoretically using this type of test you can check anything what is possible to check (if it's impossible to retrieve some information using script language, you can create ActiveX object (e.g. using C++) and use this object in the script). So, you are the one who can improve HostMonitor to suit all your needs. BTW you can create your own script language…
In addition to the common test parameters, the Active Script test has the following options:

Run script from external file
Set this option and specify script file name that HostMonitor will load and execute every time test is performed. This option allows you to change script any time without changing HostMonitor's settings. E.g. HostMonitor can be loaded on server machine and execute scripts located on workstations

Store script inside HML file
With this option enabled HostMonitor will store script inside HML file with test settings. You can protect HostMonitor's settings by password and be sure nobody read or modify your scripts.

Language
The Language property determines language in which a script is written. HostMonitor can use any script engine that is installed on your system. VBScript and JScript installed by default on Windows 2000/XP. Also you can download and install additional script languages, for more information please refer to Technical requirements paragraph.

Timeout
The Timeout property offers a safety shield to prevent a script program from going into an infinite loop and locking up the system. It specifies the maximum number of seconds the script will run before an error will be generated.

Alow UI
When this option enabled the script program can display user interface (UI) elements such as a MsgBox

Translate macros
With this option enabled you can use special macro variables in your script.

Also Test Properties dialog contains Edit and Test buttons. First button opens Script Editor window that allows you to view, modify, and execute script. Test button executes script and displays result or an error message.

Requirements to the script:
HostMonitor has just a few requirements:

1) script must contain “performtest” function. HM always calls function with this name
2) “performtest” function must not have any parameters
3) “performtest” function must return string value. This string contains two parts separated by colon (:). First obligatory part contains test status, it can take following values:
   - Host is alive
   - No answer
   - Unknown
   - Unknown host
   - Ok
   - Bad
   - Bad contents

   Second optional part contains Reply value, HostMonitor displays this value in Reply field, writes to log files, uses to displays charts (Log Analyzer), etc.
   Several examples:

return “Host is alive:1000 ms”	Jscript;	Status: Host is alive;	Reply: 1000 ms
return “Unknown host:”	Jscript;	Status: Unknown host;	Reply: empty
performtest = “Ok:300 Kb”	VBscript;	Status: Ok;	Reply: 300 Kb
performtest = “Bad:90 %”	VBscript;	Status: Bad;	Reply: 90 %

3a) If you want Log Analyzer to be able correctly process Reply values and display charts, use one of following formats for Reply value:

- decimal_number (like ‘123’, ‘0’, ‘6456.45’. as decimal separator use symbol that is specified on your system, usually a dot (.) or a comma (,))
- decimal_number + space + ‘Kb’ (like ‘512 Kb’, ’64 Kb’)
- decimal_number + space + ‘Mb’ (like ‘1024 Mb’, ’5 Mb’)
- decimal_number + space + ‘Gb’ (like ‘12 Gb’, ’4 Gb’)
- decimal_number + space + ‘%’ (like ’50 %’, ’99 %’)
- decimal_number + space + ‘ms’ (like ‘100 ms’, ’5400 ms’)

That’s it. Everything else is entirely up to you

When you create new script HostMonitor provides template with constants which describe test statuses and with empty “performtest” function.
Also you can find several simple examples of scripts in HostMonitor’s directory “Examples\”.

DrivesList.vbs	VBScript, checks list of disk drives on local system. Set test’s status to “Bad” when list of drives changes. E.g. when user map/unmap network drive.
DrivesList.js	JScript, analogue of DrivesList.vbs
DiskSpaces.vbs	VBScript, checks difference between free disk space on drive C: and drive D: Sets status to “Bad” when drive C: has less amount of free space than drive D:
DiskSpaces.js	JScript, analogue DiskSpaces.vbs
CheckWord.vbs	VBScript, statrs MS Word, opens document and returns number of characters in the document. If MS Word is not installed or document does not exist, test’s status will be “Uknown”
RegRead.vbs	VBScript, reads registry data. Sets test’s status to “Bad” when some application (or a user) changes address to a web page that Internet Explorer uses as home page
RegRead.js	JScript, analogue RegRead.vbs

Technical requirements:
As we have already said HostMonitor uses Microsoft ActiveScripting technology to execute scripts. Microsoft ActiveScript is basically 2 related COM objects: the scripting engine and the scripting host.
The scripting host is responsible for the interaction between application and the scripting engine. HostMonitor uses MS Script Control as scripting host. It means MS Script Control must be installed on your system to perform script tests. Normally, this control is installed on Windows 2000, Windows XP, Windows Server 2003 and all newer systems.

The scripting engine is the COM object that actually processes the scripts, e.g. VBScript, JScript, etc. These COM objects are usually provided by a third party (in the case of VBScript it's provided by Microsoft). On Windows 2000/XP VBScript and Jscript installed by default, also you can download and install additional script languages. If you have old version of Windows or if you want to use another script language, the following links can be useful for you:

- Perl is available from www.activestate.com
- Python is available at the same site www.activestate.com
- Haskell is available at http://www.haskell.org/haskellscript

Of course we don't know about all script languages available on the Internet, these are just the most popular that we know about.

Useful links:
There are some useful links:

Scripting FAQ: docs.microsoft.com
Microsoft Java Script documentation available at msdn.microsoft.com
Microsoft Visual Basic Script documentation available at docs.microsoft.com

Shell Script

Shell Script method combines the versatility of "External" and convenience of "Active Script" method.
Both "External" and "Shell Script" test methods execute specified commands as new processes. Due to this nature it is possible to use any programming tool for test creation. E.g. you may use Visual Basic script, Java script, create real executable file using C++ compiler or use simple BAT file or shell script.
On the other hand this test method allows passing of any valid Status and Reply values back to HostMonitor. Just like "Active Script test method.
In addition to the common test parameters, the Shell Script test has the following options:

Script
Choose script profiles from drop down list box or click "Script Manager" button to view/modify/select the script. Script Manager allows you to view and modify scripts; check script comments, version and history; import and export existing scripts; create and test new scripts.
Some useful UNIX-specific scripts are included into the package.

Params
If script requires some parameters, "Hint" field will show you the list of parameters. E.g. "SYSTEM: Average Load - 1 min" script requires single parameter: <alert threshold>. If you specify "50" as the script parameter and script detects that system load is over 50%, it will set "Bad" status for the test. Otherwise status of the test will be "Ok".
Translate macros
With this option enabled you can use global macro variables as script parameters.

Timeout
The Timeout property offers a safety shield to prevent a script program from going into an infinite loop and locking up the system. It specifies the maximum number of seconds the script can run before HostMonitor (or RMA) terminates the script and sets "Unknown" status for the test.
If you set Timeout to 0, HostMonitor will not terminate script.

Knows problems
If you need to pass parameters with quotation marks to powershell script, you may need to use escape character. Microsoft says escape character is backtick (`) but it only interpreted when contained in double-quoted (") strings. So you should use backslash (\) or backslash plus backtick (\`). E.g. you can type '123\"text\"456' instead of '123"text"456'

If you are using Windows Vista or newer version of the system, UAC is enabled and HostMonitor running as Win32 service cannot start external applications, you may need to assign "Replace a process level token" right to the account (user account used for HostMonitor service). Local Computer Policy -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> Replace a process level token -> Properties -> Add User or Group, then restart system.

Some useful UNIX-specific scripts that are included into the package.

SYSTEM: number of processes (runnable)	
Purpose:	Checks how many processes are on run queue.
Parameters:	
- MaxLimit	script sets “Bad” status when number of runnable processes is greater than specified limit.
Platform:	AIX/BSD/Linux/Solaris
Tested on:	AIX 5.3, Linux Mandrake 9.1, FreeBSD 4.5, NetBSD 3.0.1, OpenBSD 3.9, Solaris 9
See also:	Shell Script test method, Test Properties dialog, Script Manager

SYSTEM: number of processes (total)	
Purpose:	Checks how many processes (in total) exist on the system.
Parameters:	
- MaxLimit	script sets “Bad” status when number of processes is greater than specified limit.
Platform:	AIX/BSD/Linux/Solaris
Tested on:	AIX 5.3, Linux Mandrake 9.1, FreeBSD 4.5, NetBSD 3.0.1, OpenBSD 3.9, Solaris 9
See also:	Shell Script test method, Test Properties dialog, Script Manager

SYSTEM: number of processes (zombie)	
Purpose:	Checks how many zombie processes exist on the system.
Parameters:	
- MaxLimit	script sets “Bad” status when number of defunct processes is greater than specified limit.
Platform:	AIX/BSD/Linux/Solaris
Tested on:	AIX 5.3, Linux Mandrake 9.1, FreeBSD 4.5, NetBSD 3.0.1, OpenBSD 3.9, Solaris 9
See also:	Shell Script test method, Test Properties dialog, Script Manager

SYSTEM: number of user sessions	
Purpose:	Checks how many user sessions are opened on the system.
Parameters:	
- MinLimit	script sets “Bad” status when number of sessions is less than specified limit.
- MaxLimit	script sets “Bad” status when number of sessions is greater than specified limit.
Platform:	UNIX
Tested on:	AIX 5.3, Linux Mandrake 9.1, FreeBSD 4.5, NetBSD 3.0.1, OpenBSD 3.9, Solaris 9
See also:	Shell Script test method, Test Properties dialog, Script Manager

SYSTEM: Average Load for the last 1, 5 or 15 min	
Purpose:	Checks an average load of the system during the last 1, 5, or 15 minutes.
Parameters:	
- MaxLimit	script sets “Bad” status when system load is over specified limit.
Platform:	UNIX
Tested on:	AIX 5.3, Linux Mandrake 9.1, FreeBSD 4.5, NetBSD 3.0.1, OpenBSD 3.9, Solaris 9
See also:	Shell Script test method, Test Properties dialog, Script Manager

SYSTEM: Mem Free	
Purpose:	Checks the amount of free memory on the system.
Parameters:	
- MinLimit	script sets “Bad” status when amount of free memory is less than specified limit (Kb)
Platform:	AIX/BSD/Linux/Solaris
Tested on:	AIX 5.3, Linux Mandrake 9.1, FreeBSD 4.5, NetBSD 3.0.1, OpenBSD 3.9, Solaris 9
See also:	Shell Script test method, Test Properties dialog, Script Manager

SYSTEM: Swap Free	
Purpose:	Checks the amount of available swap space on the system.
Parameters:	
- MinLimit	script sets “Bad” status when amount of available swap space is less than specified limit (Kb)
Platform:	FreeBSD/Linux/Solaris
Tested on:	Linux Mandrake 9.1, FreeBSD 4.5, and Solaris 9
See also:	Shell Script test method, Test Properties dialog, Script Manager

Process: number of instances	
Purpose:	Checks the number of instances of the specified process.
Parameters:	
- ProcessName	name of the process that has to be checked. On Solaris you should specify first 8 characters of the base name of the process executable file name
- MaxLimit	script sets "Bad" status when number of running instances is over specified limit
Platform:	AIX/BSD/Linux/Solaris
Tested on:	AIX 5.3, Linux Mandrake 9.1, FreeBSD 4.5, NetBSD 3.0.1, OpenBSD 3.9, Solaris 9
See also:	Shell Script test method, Test Properties dialog, Script Manager

Process: %CPU usage (average)	
Purpose:	Checks an average (percentage for the last minute) CPU usage for the

	specified process. If there are several processes with the same name, script chooses process that loads CPU more than other instances.
Parameters:	
- ProcessName	name of the process that has to be checked. On Solaris you should specify first 8 characters of the base name of the process's executable file name
- MaxLimit	script sets “Bad” status when CPU usage by the process is over specified limit (%)
Platform:	AIX/BSD/Linux/Solaris
Tested on:	AIX 5.3, Linux Mandrake 9.1, FreeBSD 4.5, NetBSD 3.0.1, OpenBSD 3.9, Solaris 9
See also:	Shell Script test method, Test Properties dialog, Script Manager

Process: %CPU usage (raw)	
Purpose:	Checks current (raw) CPU usage in percents by the specified process. If there are several processes with the same name, script chooses process that loads CPU more than other instances.
Parameters:	
- ProcessName	name of the process that has to be checked. On Solaris you should specify first 8 characters of the base name of the process's executable file name
- MaxLimit	script sets “Bad” status when CPU usage by the process is over specified limit (%)
Platform:	Linux
Tested on:	Linux Mandrake 9.1
See also:	Shell Script test method, Test Properties dialog, Script Manager

Process: Memory usage	
Purpose:	Checks memory usage for the specified process. If there are several processes with the same name, script chooses process with max amount of memory usage.
Parameters:	
- ProcessName	name of the process that has to be checked. On Solaris you should specify first 8 characters of the base name of the process's executable file name
- MaxLimit	script sets “Bad” status when memory usage by the process is over specified limit (Kb)
Platform:	BSD/Linux/Solaris
Tested on:	Linux Mandrake 9.1, FreeBSD 4.5, NetBSD 3.0.1, OpenBSD 3.9, Solaris 9
See also:	Shell Script test method, Test Properties dialog, Script Manager

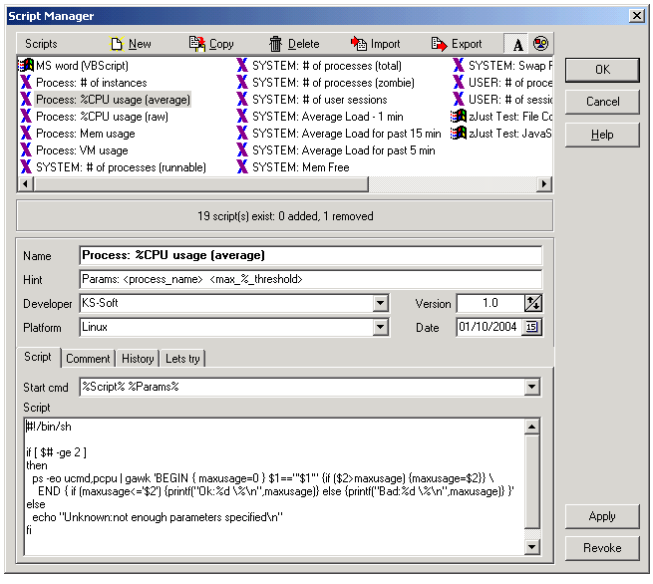
Process: Virtual Memory usage	
Purpose:	Checks virtual memory usage for the specified process. If there are several processes with the same name, script chooses process with max amount of memory usage.
Parameters:	
- ProcessName	name of the process that has to be checked. On Solaris you should specify first

	8 characters of the base name of the process's executable file name
- MaxLimit	script sets “Bad” status when virtual memory usage by the process is over specified limit (Kb)
Platform:	AIX/BSD/Linux/Solaris
Tested on:	AIX 5.3, Linux Mandrake 9.1, FreeBSD 4.5, NetBSD 3.0.1, OpenBSD 3.9, Solaris 9
See also:	Shell Script test method, Test Properties dialog, Script Manager

USER: number of processes	
Purpose:	Checks the number of processes started by specified user.
Parameters:	
- UserName	user's login name
- MaxLimit	script sets “Bad” status when the user has more running processes than specified limit
Platform:	AIX/BSD/Linux/Solaris
Tested on:	AIX 5.3, Linux Mandrake 9.1, FreeBSD 4.5, NetBSD 3.0.1, OpenBSD 3.9, Solaris 9
See also:	Shell Script test method, Test Properties dialog, Script Manager

USER: number of sessions	
Purpose:	Checks the number of sessions opened by specified user.
Parameters:	
- UserName	user's login name
- MinLimit	script sets “Bad” status when the user has less opened sessions than specified limit
- MaxLimit	script sets “Bad” status when the user has more opened sessions than specified limit
Platform:	UNIX
Tested on:	AIX 5.3, Linux Mandrake 9.1, FreeBSD 4.5, NetBSD 3.0.1, OpenBSD 3.9, Solaris 9
See also:	Shell Script test method, Test Properties dialog, Script Manager

Script Manager



You may reach Script Manager dialog from the Test Properties dialog (as described above) or use main window menu “Test”->”New”->”Shell Script test”->”Script Manager”

How to manage a list of script profiles?

In the upper part of the dialog you see the list of **script profiles**. To manage the list of profiles, use following buttons on toolbar:

New
Creates new profile.

Copy
Makes a copy of the selected profile. You will need to change either the name of profile or the target platform. HostMonitor does not allow having several scripts with the same name for the same target platform. However you may have several scripts with the same name for different platforms (e.g. “CPU Usage” script for Linux, “CPU Usage” script for Solaris and “CPU Usage” script for Windows).

Delete
Removes selected profile. Tests that were using deleted profile will not function properly after profile deletion and will return “Unknown” status.

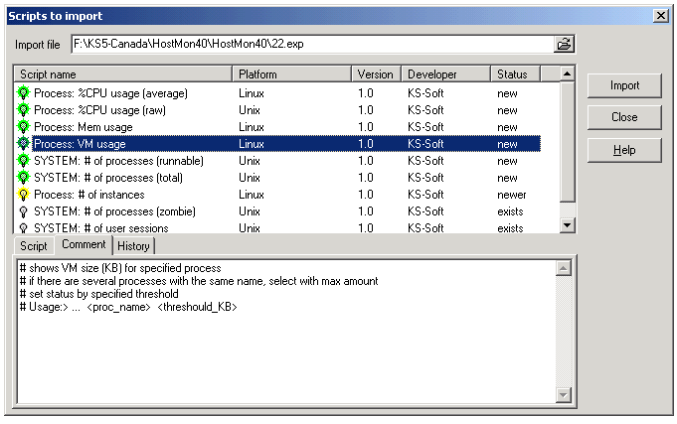
Revoke
Revokes changes that were made in selected profile. To cancel all changes that were made in the list of profiles use Cancel button instead.

Usage report
This option shows usage report for selected script. It tells you where script is used.

You may sort script profiles in different orders. Menu items for the appropriate test methods will be arranged in the same order (menu items that located in the menu Test->New->Shell Script and in the pop-up menu Add->Shell Script).

Sort by name
Allows you to sort profiles by name in alphabetical order.
Sort by platform
Groups profiles by target platform, sorts profiles alphabetically within each group.

Import



Brings up "Import" dialog window that allows you to select file with script profiles, view profiles, select some of them and import into current list.

To avoid accidental script replacement a dialog shows the status of scripts (new, newer, exists, older) and uses different icons for the scripts.
Script statuses have the following meanings:

- new	Script that is going to be imported does not exist in the current list. It is marked by green icon that means you can import script without any fear of losing existing settings.
- newer	Script that is going to be imported already exists in the list, however it has more recent modification date and higher version number than existing script. Marked by yellow, probably you should check the list of modifications that has been made to this script.
- exists	Script already exists in the list; it has the same modification date and version number. Marked by grey.
- older	Script that is going to be imported already exists in the list, however it has older modification date and lower version number than existing one. Marked by red - risk of losing some functionality if you import this script
- ??	Script that is going to be imported already exists in the list. HostMonitor is confused because script's modification date and version number are not correlating (e.g. "import" script has more recent modification date than current script but has lower version than current script. Or vice versa.)

If you click "Import" button and some of the current scripts are going to be replaced, HostMonitor will ask for confirmation.
By the way: you may select another file for importing without closing the dialog. Use "Import file" control for this purpose.

Export

This function brings up "Export" dialog that allows you to select some (or all) scripts from the current list and export them into specified file.

Find/Search again

You can use "Find" and "Search again" pop-up menu items to check the list of profiles looking for the specified text in each field: name, hint, platform, script code, comments, history, etc

Revoke

Revokes changes that were made in selected profile. To cancel all changes that were made in the list of profiles use Cancel button instead.

How to create your own script?

Now the most interesting part: how to create scripts profiles.
Script profile is not just a command for execution. It is recommended to specify comments, the list of parameters (if any) and version for each profile.

General script information:

Name
Provide the name of the script. This name will be displayed in drop down list in the Test Properties dialog, also HostMonitor will create menu item (with the same title) in "Shell Script" submenu. If you click on that item, HostMonitor will create new test with preselected script.
Please note HostMonitor does not allow you to have several scripts with the same name for the same target platform. However you may have several scripts with the same name for different platforms (e.g. "CPU Usage" script for Linux, "CPU Usage" script for Solaris and "CPU Usage" script for Windows).

Hint
List of script parameters (if any). This parameter is optional however we recommend using it. It will be displayed in the Test Properties dialog as a reminder – which parameters should be specified for the script. E.g. "Process: %CPU usage (average)" script has 2 parameters: <process_name> and <maximum threshold (%)>

Developer
Select name of the developer from drop down list. If your name is not in the list yet, just type the name and HostMonitor adds it to the list.

Platform
Choose the platform on which a script can be executed. E.g. Windows, Linux, or UNIX (if script can be executed on any UNIX-like system). If the script can be executed on several platforms (e.g. Linux and FreeBSD), please separate platforms by slash (e.g. FreeBSD/Linux).

Version
Script version. Import manager uses information about version and modification date (see above). If you change script that was developed by somebody else, please, change version number.

Date
Date of the last modification. HostMonitor updates this field automatically when you modify the script. Import manager uses information about version and modification date (see above).

Optional fields:

Comment
Any comment that makes sense for you and could be helpful for you or other administrators. It is useful to describe the purpose of the script, version of the operating system(s) where script was tested, list of parameters, or other essential information.

History
If you made changes to some script developed by KS-Soft or somebody else, please, make report about this modification in History section. If you modify your own script, this section can be useful as well. Please provide the date of the modification, version number, who made the changes, comments about modification (HostMonitor adds date and version number automatically, however you may change it).

Script section

This is the most important section; here you define the script and the command that HostMonitor/RMA will use to start the script.

Start cmd
This is an obligatory parameter. Please provide the command that HostMonitor/RMA will use to start the script. In this command you can use 2 special variables:
- %Script%

Before execution of the script HostMonitor/RMA will save the script into temporary file. %Script % variable will be replaced by the name of this temporary file. This variable doesn't have sense when you do not provide any script and use script profile just to start external executable module.
- %Params%

Scripts often require some parameters, you can specify the list of parameters in the Test Properties dialog for each test item separately. This allows using the same script to check different parameters on different target systems. To pass parameters to the script use %Params% variable, HostMonitor will replace this variable by parameters specified for the test item.

Examples:
- If script is designed as BAT file for Windows NT system (like "File Compare" sample script), you can use command line like "cmd /c %Script% %Params%"
- If script is Visual Basic Script for Windows system, use command line like "cmd /c cscript /B /E:VBScript %Script% %Params%"
- If script is Java Script for Windows system, use command line like "cmd /c cscript /B /E:JScript %Script% %Params%"
- If script is shell script for UNIX-like system, you may use simple command like "%Script% %Params%" or you may use more complicated command like "/bin/sh -c "%Script% %Params %""
- If you want to execute Power Shell script, use command line like "powershell %Script% %Params%"

- If you do not provide script and use profile to start your executable module or if you want to store script in external file, command line may look like "c:\HostMonitor4\myscripts\MyPowerfulScript %Params%"

Script

In some cases you will not provide script body, just a command for execution (e.g. you have created an executable module using some compiler such as C++ or you want to store script in some external file).
However in most cases script body can be stored within script profile. Use "Script" field to store your script.

Requirements to the script:

The following rules must be obeyed when creating a script:

The script or external program must write to **stdout** (standard output stream) single result string. This string should contain 3 parts separated by colon (**:**).

1) First obligatory part - marker "**scriptres**" tells to HostMonitor or RMA that this string is the result string.

2) Second obligatory part represents the test status, it can take one of the following values (case insensitive):

Status string	Comment
Host is alive	status means "script executed successfully, target system responds correctly"
No answer	script executed successfully, target system does not respond
Unknown	status means "test cannot be performed for some reason".
Unknown host	use this status when script cannot resolve target host name into IP address
Ok	script executed, result satisfies (some) requirements
Bad	script executed, result does not satisfy (some) requirements
Bad contents	use this status if script found some error in monitored file, web page, etc
Warning	you may use this status when some service still works but needs attention
Normal	you may use this status when you need distinguish some different "good" conditions

3) Third optional part contains Reply value, HostMonitor displays this value in Reply field, writes to log files, uses to displays charts (Log Analyzer), etc.
If you want Log Analyzer to process Reply values correctly and display charts, use one of the following formats for Reply value:
   - decimal_number (like “123”, “0”, “6456.45”. as decimal separator use symbol that is specified on your system, usually a dot (.) or a comma (,))
   - decimal_number + space + “Kb” (like “512 Kb”, “64 Kb”)
   - decimal_number + space + “Mb” (like “1024 Mb”, “5 Mb”)
   - decimal_number + space + “Gb” (like “12 Gb”, “4 Gb”)
   - decimal_number + space + “%” (like “50 %”, “99 %”)
   - decimal_number + space + “ms” (like “100 ms”, “5400 ms”)

Several examples:

String printed by script	“Status” of the test	“Reply” field of the test
scriptres:Host is alive:1000 ms	Host is alive	1000 ms
scriptres:Unknown host:	Unknown host	
scriptres:Ok:300 Kb	Ok	300 Kb
scriptres:Bad:90 %	Bad	90 %

That’s it. Everything else is entirely up to you

BTW: HostMonitor offers dozen of scripts for Unix and Windows, they are pretty simple and you can use these scripts as basis for your own development.

Let’s try

This tab allows you to test script before using it for real monitoring.

Test by
Test can be performed by HostMonitor itself (by default) or by Remote Monitoring Agent. To specify what application should execute script, select an agent from drop down list.
Please note script is executed on system where HostMonitor (or RMA) is running. It means if you have created some script for Linux, you should select appropriate agent that is running on Linux system to execute this script.

Params
If script requires some parameters, provide them here.

Timeout
The Timeout property offers a safety shield to prevent a script program from going into an infinite loop and locking up the system. It specifies the maximum number of seconds the script can run before HostMonitor (or RMA) terminates the script and sets "Unknown" status for the test. If you set Timeout to 0, HostMonitor will not terminate script.

Display N lines
If script doesn't work properly, it may display various error messages. This option allows you to check messages displayed by script; it defines how many lines of the result to display.

Test
Click this button to execute the script. HostMonitor will execute the script (by itself or with the help of selected agent) and display result.
Unlike normal test execution mode (when HostMonitor displays status and single reply string), this test sends special flag to the agent and displays complete script response if the result string of correct format was not received. It helps to find errors in the script.

Clear old res
With this option enabled HostMonitor clears previous outputs.

External

HostMonitor has many built-in check types, but it can not support all possible check types. That's why the program contains an External Test. With the External Test, HostMonitor uses an external application to perform a test and, based on the returned errorlevel, will flag the test entry as being up or down.
In addition to the common test parameters, the External test has the following options:

External program
Specify command line to launch external application

Condition
Choose condition to mark test as failed (and start alert action):

- is < than - alert if the errorlevel returned by the program is less than a specified code.
- is > than - alert if the errorlevel returned by the program is greater than a specified code.
- is = to - alert if the errorlevel returned by the program is equal to a specified code.
- is <> from - alert if the errorlevel returned by the program is different than a specified code.

Window mode
This parameter specifies how the application window is going to 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.

Kill application if not answer after N sec
You may select the "Kill application after N sec" option and specify a timeout. In this case if the external application hasn't returned an error level to HostMonitor within the given timeout, HostMonitor will flag the test entry as down and "kill" the external application.

Knows problems
If you are using Windows Vista or newer version of the system, UAC is enabled and HostMonitor running as Win32 service cannot start external applications, you may need to assign "Replace a process level token" right to the account (user account used for HostMonitor service). Local Computer Policy -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> Replace a process level token -> Properties -> Add User or Group, then restart system.

SSH

Secure Shell or SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices. Used primarily on UNIX based systems to access shell accounts, SSH was designed as a replacement for TELNET and other insecure remote shells
SSH is typically used to log into a remote machine and execute commands. The encryption used by SSH provides confidentiality and integrity of data over an insecure network, such as the Internet.

HostMonitor can connect and login to specified remote system running the SSH daemon and execute a command or shell script. This allows you to perform some tests on UNIX systems without using Remote Monitoring Agent for UNIX.
HostMonitor may perform SSH test directly or using RMA for Windows.

In addition to the common test parameters, the SSH test has the following options:

Host
Host name or IP address of the system that provides SSH service

Port
Specify TCP port used by SSH server (SSH server, by default, listens on TCP port 22)

Timeout
Specify timeout in miliseconds

Command
Specify command line that should be executed on target server

Translate macros
With this option enabled you may use special date macro variables in the command line

Check for
SSH test allows you to check result of the command execution in 3 different ways:

a) **Check for exit code** (just like External test method does)
In such case HostMonitor checks errorlevel returned by the command. You should choose one of the following conditions:
Alert if exit code
- is < than — alert if the errorlevel returned by the program is less than a specified code
- is > than — alert if the errorlevel returned by the program is greater than a specified code
- is = to — alert if the errorlevel returned by the program is equal to a specified code
- is <> from — alert if the errorlevel returned by the program is different than a specified code

b) **Check for text output**

Text (show code) - reply field will show exit code (error level)
Text output - reply field will show command output
HostMonitor can search for a string in the command output and start alert actions when the string exists (or doesn't exist). You should specify a string and condition to alert using the following options:
Alert if

- string present HostMonitor will set "Bad" status when output contains specified string

- string absent HostMonitor will set "Bad contents" status when output does not contain specified string

- expression true HostMonitor will consider provided text as boolean (logical) expression, evaluate this expression using data received from the server, and set "Bad" status when retrieved data does not satisfy the required conditions. For example: if you define expression like "'No errors' and not ('Error' or 'Warning')", then HostMonitor will mark test as "Ok" when command output contains string 'No error' and does not contain either 'Error' or 'Warning'

In the expression you may use strings (must be put in quotes (') or in double quotes ("")); round brackets; logical operators "and", "or", "not".

Additional options:
Case sensitive
With this option enabled search is case sensitive
Whole words only
Searches are for words only. With this option disabled, the search string might be found within longer words.
Macros
This option allows you to use date & time variables in the search string. E.g. if you provide "%mm%-%dd%-%yyyy%" in the search string, HostMonitor will check retrieved data for the presence of a current date and will set "Bad" status for output without current date stamp.

c) **Check for Shell Script result**
HostMonitor checks output text for specially formatted result string. I.e. result of the command execution should follow the same rules as Shell Script

Authentication
Connection Manager allows you to setup user name and password for each remote system (also you may use some default account information for all target systems)
Also private key authentication can be used instead of password authentication. If the private key for the target server is set in SSH Key Manager, this key will be used for authentication. Otherwise the password specified in Connection Manager will be used.

Public host keys
HostMonitor and RMA send public keys retrieved from servers to SSH Key Manager. You can also choose the behavior of the software when the host public key changes. SSH Key Manager offers 3 options:
- set Warning status once, automatically approve new key
- don't connect to the host until operator approves new key

- automatically approve new key
If you choose the "don't connect to the host until operator approves new key" option and the host key changes for any reason then HostMonitor/RMA will not perform SSH tests related to the server until you open SSH Key Manager, verify the fingerprint of the new pubic key and confirm that this new key is legitimate
(note: new unapproved public keys marked in red).

IT Temperature Monitor

When you utilize temperature-sensing units from Sensatronics, this test provides you with the ability to monitor the temperature and to start alert actions when the temperature is out of the specified range. HostMonitor supports following unit models:

- Model E (temperature monitor)
- Model EM1 (environmental monitor)*
- Model CM (cryo low temperature monitor)
- Model U16 (universal temperature monitor)

In addition to the common test parameters, IT Temperature Monitor test has the following options:

IP
Provides IP address of the temperature-sensing unit

Port
Specifies TCP port that is used by the unit. By default it uses port #80

Probe
After you have specified IP address and TCP port, select which Probes you want to monitor. There are two special (in addition to the list of probes) options available in the drop down list:

- **<All probes>**
  HostMonitor will check all available probes (on the specified unit) and will start alarm action when the temperature on ANY probe(s) is out of specified upper/lower limits (status of the test item will then be set to "Bad"). If some probes are not connected or there is a shortcut in the circuit, HostMonitor sets "Unknown" status of the test (and starts alarm actions if "Treat Unknown status as Bad" option is enabled).
- **<All operable probes>**
  if you choose this item, HostMonitor will check all operable probes. Operable, means all those probes that work correctly, shortcut or not connected probes will be ignored.

Scale
This option sets F° (Fahrenheit) or C° (Celsius) scale to display temperatures.

Low temp alarm
Use this option to set lower temperature limit. If temperature goes below this limit, HostMonitor sets test status to "Bad" (and starts alert actions if specified so)

High temp alarm
Use this option to set upper temperature limit. If temperature goes above this limit, HostMonitor sets test status to "Bad" (and starts alert actions if specified so)

* EM1 Environmental Monitor may measure wetness and humidity as well as temperature. To monitor wetness and humidity with HostMonitor you should use SNMP Get test method.

Traffic Monitor

This test allows you to check the traffic on network interfaces of SNMP enabled devices. It has the following advantages over the SNMP Get test:

- you don't need to know much about OIDs. Connection to the specified network device is established with the help of Test Properties dialog which displays the list of available interfaces. You only have to select the interface that you want to monitor;
- using single test item you may monitor total (both incoming and outgoing) traffic on the selected interface;
- with single test item you may monitor summarized total of the traffic or some other parameters (like queue length) for all interfaces of selected device. For example you may monitor the traffic on all ports of the network router.

In addition to the common test parameters, Traffic Monitor test has the following options:

Host
Here you should provide either a dotted-decimal IP address or a host name that can be resolved to an IP address, an IPX address (in 8.12 notation), or an Ethernet address.
Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) and specify hostname with suffixes ::ipv4 or ::ipv6 (e.g. www.google.com::ipv4 or www.6bone.net::ipv6). If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.
Note: on Windows NT 4.0, Windows 2000 and Windows XP SP1 IPv6 protocol is not supported. You may use menu Tools -> Local Info to check is your system IPv6 ready.

Port
Specify the port number on which the host is listening for incoming requests. By default SNMP agent uses port 161.

Profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.

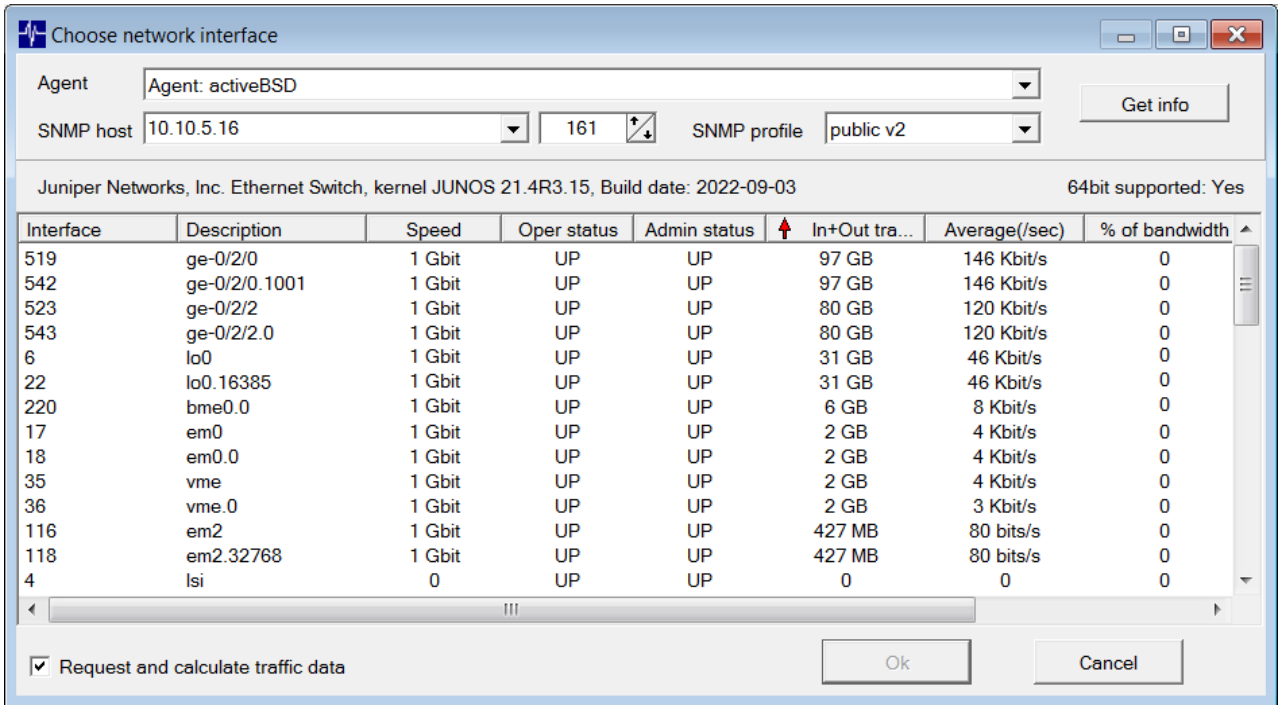
Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

Check (interface)
You may open "Network interfaces" window and select interface(s) that you want to monitor. For each available interface HostMonitor displays the index, description, speed and status (optionally

traffic since reboot, bandwidth utilization, etc). If you choose “Monitor traffic on all interfaces”, HostMonitor will check summarized traffic for each network interface available on the device.

When you are creating a new Traffic Monitor test item, then you may select many interfaces in the list; HostMonitor will create separate test item for each selected interface. E.g. you may sort interfaces by speed, select all 10Gbit interfaces and set the same alert limit for set of new tests.



Interface	Description	Speed	Oper status	Admin status	In+Out tra...	Average(/sec)	% of bandwidth
519	ge-0/2/0	1 Gbit	UP	UP	97 GB	146 Kbit/s	0
542	ge-0/2/0.1001	1 Gbit	UP	UP	97 GB	146 Kbit/s	0
523	ge-0/2/2	1 Gbit	UP	UP	80 GB	120 Kbit/s	0
543	ge-0/2/2.0	1 Gbit	UP	UP	80 GB	120 Kbit/s	0
6	lo0	1 Gbit	UP	UP	31 GB	46 Kbit/s	0
22	lo0.16385	1 Gbit	UP	UP	31 GB	46 Kbit/s	0
220	bme0.0	1 Gbit	UP	UP	6 GB	8 Kbit/s	0
17	em0	1 Gbit	UP	UP	2 GB	4 Kbit/s	0
18	em0.0	1 Gbit	UP	UP	2 GB	4 Kbit/s	0
35	vme	1 Gbit	UP	UP	2 GB	4 Kbit/s	0
36	vme.0	1 Gbit	UP	UP	2 GB	3 Kbit/s	0
116	em2	1 Gbit	UP	UP	427 MB	80 bits/s	0
118	em2.32768	1 Gbit	UP	UP	427 MB	80 bits/s	0
4	lsi	0	UP	UP	0	0	0

"Request and calculate traffic data"
If you enable this option HostMonitor will show additional information for each network interface:
- amount of total received and transmitted traffic;
- average amount of data per second;
- bandwidth utilization (%);
- bandwidth utilization by income traffic;
- bandwidth utilization by outgoing traffic

Notes:
- Bandwidth utilization: amount of data transferred through a network relative to its total capacity.
- In this case average traffic and utilization percentage calculated based on total traffic thru interface since device reboot (not a current utilization measured for last second or minute)
- This option is available for SNMP v2c, SNMP v3 enabled devices with 64bit traffic counters

Alert if

Here you should specify which parameter of the interface to check together with its minimum or maximum value beyond which an alert action will be started.

Parameter	**Comment**	**Alert threshold unit(s)**
- In/Out traffic	total of incoming and outgoing traffic	Kbit/sec,

		Kbit/min KB/sec, KB/min Mbit/sec, Mbit/min MB/sec, MB/min
- Income traffic	income traffic only	Kbit/sec, Kbit/min KB/sec, KB/min Mbit/sec, Mbit/min MB/sec, MB/min
- Outgoing traffic	outgoing traffic only	Kbit/sec, Kbit/min KB/sec, KB/min Mbit/sec, Mbit/min MB/sec, MB/min
- In Discards	the number of inbound packets which were chosen to be discarded (e.g. because of an unknown or unsupported protocol)	pkt/sec pkt/min
- In Errors	the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol	pkt/sec pkt/min
- Out Discards	the number of outbound packets which were chosen to be discarded	pkt/sec pkt/min
- Out Errors	the number of outbound packets that could not be transmitted because of errors.	pkt/sec pkt/min
- Output queue	the length of the output packet queue	pkt

Note #1: even though you specify traffic (or errors) limit in Kb/sec, Mb/min, etc, it doesn't mean that HostMonitor will check network interface every second or every minute. It checks the device by specified schedule and then calculates average traffic between 2 consecutive probes.

Note #2: options located on Misc page in the Options dialog allow you to select units used to report amount of network traffic (KB/MB or Kbit/Mbit).

Note #3: since version 7.06 HostMonitor does not use Microsoft's mgmtapi.dll anymore, this helps to avoid various problem caused by bugs in some versions of this DLL

Network Interfaces Status (NIS)

This test allows you to check all or some specific interfaces on SNMP enabled device (server, router, etc). HostMonitor may warn you when network interface goes down or changes its administrative and/or operative status.

In addition to the common test parameters, NIS test has the following options:

Host
Provide either a dotted-decimal IP address or a host name that can be resolved to an IP address.
You may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) and specify hostname with suffixes ::ipv4 or ::ipv6 (e.g. www.google.com::ipv4 or www.6bone.net::ipv6). If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.
Note: on Windows NT 4.0, Windows 2000 and Windows XP SP1 IPv6 protocol is not supported. You may use menu Tools -> Local Info to check is your system IPv6 ready.

Port
Specify the port number on which the host is listening for incoming requests. By default SNMP agent uses port 161.

Profile
Choose profile that stores credentials necessary for communication with SNMP agent. You may select profile from drop-down list or click button beside the list to bring up SNMP Credentials dialog.

Timeout
This is the amount of time in milliseconds the program will wait for a response from the server before the request fails.

Retries
Specifies the communications retry count.

Known problems

Cisco devices can provide a corrupted network interface table, the problem seems to be getting worse after some Cisco updates in 2026.
Solution?
a) Sometimes device restart may fix the problem;
b) Network Interfaces Status (NIS) test can analyze such broken tables if you add snmpTests_CheckBrokenInterfaceTables=1 line into the [Misc] section of the hostmon.ini file and restart HostMonitor. In such case NIS test will skip interfaces with invalid data without reporting an error.
Note: this option does not apply if you are using SNMP version 1.

Check
Use this option to choose which status should be checked for each network interface.

admin status only	HostMonitor will check the desired (administrative) state of the interface and show number of interfaces with administrative_status<>UP
admin and operative statuses	HostMonitor will check administrative and current operational state of the interface and show number of interfaces that fits the following condition: (administrative_status<>UP) OR (operational_status<>UP)
operative status (all interfaces)	HostMonitor will check the current (operative) state of the interface and show number of interfaces with operative_status<>UP
operative status (when admin status UP)	HostMonitor will check administrative and current operational state of the interface and show number of interfaces that fits the following condition: (administrative_status==UP) AND (operational_status<>UP) **Lets call these selected interfaces "bad" interfaces**

The following options tells HostMonitor when "Bad"/"Ok" test status should be set and when actions should be triggered

Alert if

N or more interfaces down	HostMonitor will set "Bad" test status when number of "bad" interfaces over specified number. HostMonitor will restore "Ok" test status when number of "bad" interfaces <= specified limit.
any new interface down	HostMonitor keeps list of all interfaces. If any interface changes status from UP to DOWN, HostMonitor sets "Bad" test status. The following options tell HostMonitor when "Ok" status should be restored: **- set Ok: auto** the following test probe may set Ok status if no other interface changed its status from UP to DOWN **- set Ok: user** HostMonitor will keep "Bad" status until operator acknowledge item
any change in status detected	HostMonitor keeps list of all interfaces. If any interface changes status (UP to DOWN or DOWN to UP), HostMonitor sets "Bad" test status. The following options tell HostMonitor when "Ok" status should be restored: **- set Ok: auto**

the following test probe may set Ok status if no other interface changed its status

- set Ok: user
HostMonitor will keep "Bad" status until operator acknowledge item

When NIS test performs HostMonitor sets the following macro variables

%InterfacesDOWN_Index% "Bad" interfaces: list of interfaces indexes separated by commas
%InterfacesDOWN_Name% "Bad" interfaces: list of interfaces descriptions separated by CRLF

Value of the following "**InterfacesChanged"** variables depends on above options

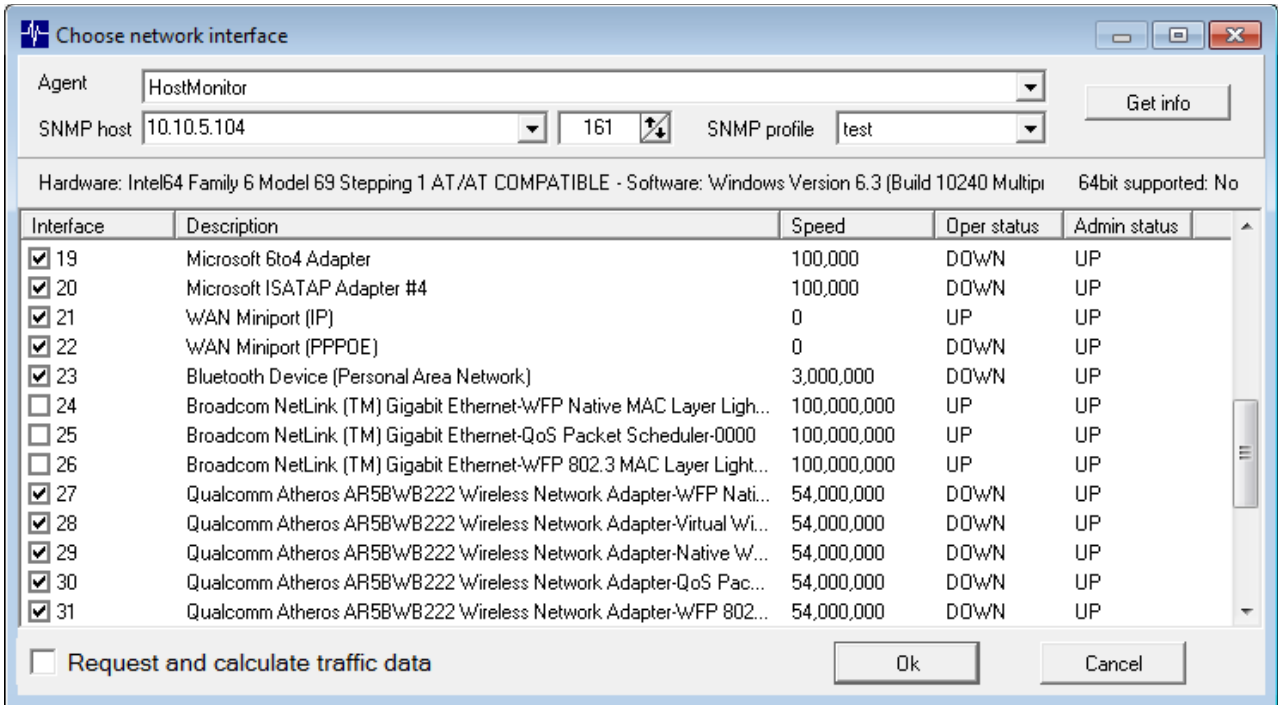
- set Ok: auto with this option selected "**InterfacesChanged"** variables will provide list of interfaces whose status changed between last 2 probes

- set Ok: user with this option selected "**InterfacesChanged"** variables will provide list of interfaces whose status changed since last user acknowledgement

%InterfacesChanged_Index% List of interfaces indexes which status has been changed (separated by commas)

%InterfacesChanged_Name% List of interfaces descriptions which status has been changed (separated by CRLF)

Ignore interfaces
Select interface(s) you want to skip from monitoring. You may specify comma separated list of interface indexes or open "Choose network interface" window, view interfaces list (index, description, speed, status, etc) and mark some interfaces.



"Request and calculate traffic data"

If you enable this option HostMonitor will show additional information for each network interface:
- amount of total received and transmitted traffic;
- average amount of data per second;
- bandwidth utilization (%);
- bandwidth utilization by income traffic;
- bandwidth utilization by outgoing traffic

Notes:
- Bandwidth utilization: amount of data transferred through a network relative to its total capacity.
- In this case average traffic and utilization percentage calculated based on total traffic thru interface since device reboot (not a current utilization measured for last second or minute)
- This option is available for SNMP v2c, SNMP v3 enabled devices with 64bit traffic counters

HM Monitor

Lets say you have installed HostMonitor on the server and setup thousand test items to monitor entire network (or several networks). HostMonitor will inform you in case of any problem. Unless... unless something happens to system where HostMonitor is running. What if power supply dies, motherboard fries or Windows crashes due to some buggy driver?
You may install another instance of HostMonitor on different system and use 2nd copy of HostMonitor to check your primary monitor! Also there is another good feature: primary HostMonitor may monitor backup HostMonitor so each system will monitor colleague!

Note 1: If you want to install HostMonitor on 2 systems (physical or virtual), you need to order 2 licenses.
Note 2: In order to monitor HostMonitor "A" by HostMonitor "B" you need to enable RCI interface on HostMonitor "A". If you want to use 2 HostMonitors to monitor each other, you need to enable RCI interface on both systems (HostMonitor "A" and HostMonitor "B"). RCI license included into Enterprise package; holders of a Lite, Standard or Professional licenses may purchase RCI license separately.
Note 3: There is WatchDog application included into Enterprise package. It allows you to monitor HostMonitor remotely and start alerts as well. While WatchDog provides charts and alerts in one application at no additional cost, 2nd instance of HostMonitor will provide great flexibility and reliability.

HM Monitor test method offers more that simple check: HostMonitor is on-line or not. It may monitor many parameters of HostMonitor. For example

- it may warn you when alerts disabled or monitoring stopped;
- it may show how many tests per second performed by primary monitor and start alerts if less than 5 tests per second were performed over period of time;
- it may inform you that test list was modified and modifications were not stored (saved in the file);
- it may warn you when ODBC driver (selected for ODBC logging function) uses too much time;
- it may tell you how many actions were executed by primary monitor and how many log records were recorded;
- and much more.

In addition to the common test parameters, the HM Monitor test has the following options:

Host
Domain name or IP address of the machine running HostMonitor you wish to monitor.

Password
Password specified for "watchdog" account. You need to setup this account on HostMonitor that you wish to monitor. Basically you just need to specify password and a list of IP addresses authorized for remote connections. See RCI: Operators section of the manual

TCP Port

TCP port used by “primary” HostMonitor for RCI Interface
Note: Remote Control Interface should be enabled on HostMonitor that you wish to monitor.

Timeout
Here you may specify amount of time in milliseconds the program will wait for a response from the server before the request fails.

Set Bad status if monitoring stopped or alerts disabled
With this option enabled HM Monitor test will set Bad status when someone stopped monitoring or disabled alerts on target system.
BTW: There are some options that allow you to execute action profile every time monitoring is stopped or alerts getting disabled without using external monitor. See “Pause monitoring/alerting” dialog. However external monitoring provides extra flexibility: for example you may start alerts only if monitoring paused/stopped for more than 20 minutes.
Note: HM Monitor test will not inform you when monitoring is stopped due to “evaluation pause”

Display
This option defines what kind of information should be displayed in Reply field of the test. You may choose one of the following options:

- response time
- tests performed (since last probe)
- tests failed (since last probe)
- actions performed (since last probe)
- log records added (since last probe)
- tests per second
- actions per second
- log records per second
- actions: average time consumption.
  Actions ATC (Average Time Consumption). Time used by HostMonitor for actions (milliseconds per action). This time does not include time used by auxiliary threads, its not so important
- logging: average time consumption
  Time used by HostMonitor for logging (milliseconds per record). This time does not include time used by auxiliary threads, its not so important. This option can be useful for investigation of some 3rd party software related problems (e.g. if ODBC driver specified for ODBC logging consumes too much time)

As you see basic setup is pretty simple and allows you to setup test that will alert you when “primary” HostMonitor does not respond or monitoring/alerts were disabled.
However this test supports common macro variables plus dozen of HM Monitor specific variables. Using these variables with “Optional status processing” test property you may setup various additional alerts.
Several examples:

1) if you want to receive alert when test list was changed and modifications were not saved, mark “Use Warning status if” option and provide the following expression: ‘modifications not stored’ in ‘%HMStatusString%’. If you setup such condition, we recommend starting alerts after several failed probes so operator that manages test items will have time to store results. E.g. if you use “Start when 6 consecutive Bad results occur” alert condition for test

performed every 5 min; alert will be triggered if modifications not stored within 30 min. BTW: There is “Autosave testlist after any changes” option located on Preferences page in the Options dialog

2) if you want to receive alert when logging module requires too much time due to some problems with ODBC driver or antivirus monitor, mark “Use Warning status if” option and provide expression like: ‘%HMLogsATC%’ > 50 (note: usually 50 milliseconds per 1 log record is too much however it can be normal when you are using shared network drive for logging. Not recommended)
3) you may check several conditions. E.g. you may check is monitoring started, check average time consumption by logging and actions, check how many tests are performed by HostMonitor. Disable “Set Bad status if monitoring stopped or alerts disabled” option (so disabled alerts will not trigger “Bad” test status), mark “Use Warning status if” option and provide expression like (‘monitoring stopped’ in ‘%HMStatusString%’) or (‘%HMLogsATC%’ > 50) or (‘%HMActionsATC%’ > 500) or (%HMTestsDone%<10)

In the same way “Tune up Reply value” option allows you to display various parameters of the HostMonitor using single test item. E.g. expression like “%HMVersionText% %HMTestsDone% (%HMTestsFailed%), %HMActionsDone% / %HMLogsDone%” will show version of HostMonitor, number of test probes performed since last check, number of failed test items, how many actions were executed and log items recorded (since last check).
Note: in such case Log Analyzer will not be able to generate charts for the test

Macros

When you setup "Folder/File Size", "File/Folder Availability", “Count Files”, or "Compare Files" tests you can set "Translate macros" option and use special macro variables in the file name:

%d%	Current day as a number without a leading zero (1-31)
%dd%	Current day as a number with a leading zero (01-31)
%ddd%	Current day as an abbreviation (Sun-Sat) using system regional settings.
%jjj%	Current day of the year as a three digit decimal number in the range of 001 to 366
%uuu%	UnixTimeStamp (seconds since 1970)
%dddd%	Current day as a full name (Sunday-Saturday) using system regional settings.
%ddddd%	Current date using the short date format (see Windows Regional Options).
%dddddd%	Current date using the long date format.
%w%	Current week number (1-54).
%ww%	Current week as two-digit number with a leading zero (01-54).
%www%	Current week number according to ISO 8601 specification (1st week of the year is the week with the year's first Thursday in it)
%m%	Current month as a number without a leading zero (1-12).
%mm%	Current month as a number with a leading zero (01-12).
%mmm%	Current month as an abbreviation (Jan-Dec) using system regional settings.
%mmmm%	Current month as a full name (January-December) using system regional settings.
%yy%	Current year as a two-digit number (00-99)
%yyyy%	Current year as a four-digit number (0000-9999)
%h%	Current hour without a leading zero (0-23)
%hh%	Current hour with a leading zero (00-23)
%h12%	Current hour using 12-hour clock (0-12,1-11)
%hh12%	Current hour using 12-hour clock with a leading zero
%n%	Current minute without a leading zero (0-59)
%nn%	Current minute with a leading zero (00-59)
%t%	Current time using the short time format.
%tt%	Current time using the long time format.
%am/pm%	Uses the 12-hour clock for the preceding h or hh specifier, and displays 'am' for any hour before noon, and 'pm' for any hour after noon. The am/pm specifier can use lower, upper, or mixed case, and the result is displayed accordingly.
%a/p%	Uses the 12-hour clock for the preceding h or hh specifier, and displays 'a' for any hour before noon, and 'p' for any hour after noon. The “a/p” specifier can use lower, upper, or mixed case, and the result is displayed accordingly.
%/%	Displays the date separator character given by the DateSeparator global variable.
%:%	Displays the time separator character given by the TimeSeparator global variable.

%NewestFile%	Name of the newest file in specified folder
%NewestFolder%	Name of the newest sub-folder in specified folder
%OldestFile%	Name of the oldest file in specified folder
%OldestFolder%	Name of the oldest sub-folder in specified folder
%SmallestFile%	Name of the smallest file in specified folder
%LargestFile%	Name of the largest file in specified folder

There is also a different, more flexible format. If you use the variable %NewestFile%, HostMonitor will check all files in the folder to find the newest file. If you use the variable %NewestFile(*.TXT)%, HostMonitor will only check files with the .TXT extension and find the newest .TXT file. The same format can be used for other variables.
This format is not supported for FTP related tests.

Format	Example
%NewestFile(<filemask>)%	%NewestFile(*.log)%
%OldestFile(<filemask>)%	%OldestFile(LOG*)%
%LargestFile(<filemask>)%	%LargestFile(????2026*)%
%SmallestFile(<filemask>)%	%SmallestFile(*.DAT)%
%NewestFolder(<filemask>)%	%NewestFolder(Reports*)%
%OldestFolder(<filemask>)%	%OldestFolder(User*.REP)%

For example, you can specify a path like
C:\Firewall\LogsAndReports\%NewestFolder(Logs*)%\%LargestFile(*.txt)%

Macro specifiers may be written in upper case as well as in lower case letters - both produce the same result.
Examples:
c:\database\archives**%DDMMYYYY%**.zip
c:\database\archives**%dd%-%mm%-%yy%**.zip
c:\application\logs**%mmyyyy%\%NewestFile%**
c:\application\logs**%NewestFolder%\%OldestFile%**

Expressions

What if you need to use yesterday's date? Or the date that specifies last month? In this case you may use expressions. For example when you need to create the test that will compare two log files created by some application every day – compare 2 days old log file to yesterday's log file. Use expression like **%mmddyyyy[-2d]%.log** to describe the first file and **%mmddyyyy[-1d]%.log** to describe the second one.

Rules:

1) to subtract a number of days from current date, use expression like [-NNd]
   (e.g. %dd[-1d]%)
2) to add a number of days to current date, use expression like [+NNd]
   (e.g. %ddd[+22d]%)
3) to subtract a number of months from current date, use expression like [-NNm]
   (e.g. %dm[-24m]%)

4) to add a number of month to current date, use expression like [+NNm]
   (e.g. %ddmm[+1m]%)
5) to subtract a number of years from current date, use expression like [-NNy]
   (e.g. %dmyy[-2y]%)
6) to add a number of years to current date, use expression like [+NNy]
   (e.g. %ddmmyyyy[+10y]%)
7) [-0u] converts local time to UTC time (e.g. %yymmdd-hhnn[-0u]%)
8) expression must be concluded in the same percent signs (%) that concludes date variables
9) expression must be specified after regular date variables
   (e.g. %dd[-1d]% - correct expression, %[-1d]dd% - incorrect expression)
10) you may use only one expression in each macro variable.

Examples:

%ddmm[-1m]%	- correct expression (one variable and one expression)
%dd[-1d]%%mm[-1m]%	- correct expression (2 variables, 1 expression in each variable)
%ddmm[-1d][-1m]%	- incorrect expression (2 expressions in one variable)

Templates

Templates
You may use folder related user defined variables as parameters of tests (target host, path to the file, etc). E.g. you may define %fvar_IPaddress% variable and use this variable for various test items. You may specify %fvar_IPaddress% as target address for Ping and Trace tests, use string like http://%fvar_IPaddress%/database/index.cgi as URL specified for HTTP test, check drive free space using \\%fvar_IPaddress%\driveC and \\%fvar_IPaddress%\driveD paths for UNC tests, etc.
Note: %folder% variable allows you to use name of the folder as parameter of the test item.
HostMonitor will resolve variable and use its current value for test item parameters. If you change value of such folder variables, test items located in this folder will apply new values automatically. This allows you to modify parameters of many test items within folder (and subfolder, if subfolders inherit variable list from parent folder) by changing single folder-level variable! E.g. if you setup 20-30 test items for some server and then you need to change server address, hostname or some other important parameter, you can make these changes in less than 1 minute.
Also, if you copy test items from one folder to another, HostMonitor will apply changes to new test items according to values of the variables that were specified for target folder. This means you may easily apply/create set of tests for new servers by using single copy operation without any following modifications.
The same rules are applicable for other operations:

- you can move test items from one folder to another and HostMonitor will change test parameters and names according to template
- you can rename folder and HostMonitor will apply changes to test items if you have used %folder% variable as parameter of the tests
- if you move folder from one node to another (folder changes its parent) and folder inherit variables from parent, HostMonitor will apply changes to items according to new values

If you spend some time to prepare templates and folders then you will be able to create dozens of new checks for new set of servers in a minute.
See also Template folders

You may use variables while specifying test name, comment and the following test-specific parameters

Test method	Template is applicable*	Variables can be used as
Ping	Yes	Target host (host name or IP address)
Trace	Yes	Target host (host name or IP address)
URL request	Yes	URL
HTTP	Yes	URL
SOAP/XML	No	-
OPC	No	-
Certificate expiration	Yes	Target host (host name or IP address)
Domain expiration	Yes	Domain name
Apache	Yes	Status URL
NGINX	Yes	Status URL
Tomcat	Yes	Status URL
IIS	Yes	Target host (host name or IP address)

TCP	Yes	Target host (host name or IP address)
UDP	Yes	Target host (host name or IP address)
NTP	Yes	Target host (host name or IP address)
SMTP	Yes	Target host (host name or IP address)
POP3	Yes	Target host (host name or IP address)
IMAP	Yes	Target host (host name or IP address)
E-Mail	No	-
Mail Relay	No	-
DNS	Yes	Target host (host name or IP address)
DHCP	Yes	Target host (host name or IP address)
LDAP	Yes	Target host (host name or IP address)
RADIUS	Yes	Target host (host name or IP address)
DICOM	Yes	Target host (host name or IP address)
RAS	Yes	Connection name
UNC	Yes	UNC path
Disk free space	Yes	Target host (host name or IP address)
HDD SMART	Yes	Target host (host name or IP address)
Folder/File size	Yes	Path (UNC path, file or folder name)
Count Files	Yes	Path (folder name)
File/Folder Availability	Yes	Path (UNC path, file or folder name)
Compare files	Yes	Path to 1st file (UNC path, file or folder name)
File Integrity	Yes	Path (UNC path, file or folder name)
Text Log	Yes	Path (UNC path, file or folder name)
Interbase	Yes	Target host (host name or IP address)
MS SQL	Yes	Target host (host name or IP address)
MySQL	Yes	Target host (host name or IP address)
Oracle	Yes	Server (TNS alias)
PostgreSQL	Yes	Target host (host name or IP address)
Sybase	Yes	Target host (host name or IP address)
ODBC Query	Yes	SQL Query
Process	Yes	Target host (host name or IP address)
Service	Yes	Target host (host name or IP address)
SNMP Get	Yes	Target host (host name or IP address)
SNMP Table	Yes	Target host (host name or IP address)
SNMP Trap	No	-
NT Events Log	Yes	Target host (host name or IP address)
CPU Usage	Yes	Target host (host name or IP address)
Memory	Yes	Target host (host name or IP address)
Performance Counter	Yes	Target counter (target host, counter name)
WMI	Yes	Target host (host name or IP address)
Dominant Process	Yes	Target host (host name or IP address)
Registry	Yea	Target host (host name or IP address)
External test	Yes	Command line
Active Script	No	-

Shell Script	Yes	Script parameters
Temperature Monitor	Yes	Target host (host name or IP address)
Traffic Monitor	Yes	Target host (host name or IP address)
Interfaces status	Yes	Target host (host name or IP address)
HM Monitor	No	
Cisco Health	Yes	Target host (host name or IP address)
Cisco Temp	Yes	Target host (host name or IP address)
Cisco Fans	Yes	Target host (host name or IP address)
Cisco Power	Yes	Target host (host name or IP address)
Cisco CPU Usage	Yes	Target host (host name or IP address)
Cisco Memory	Yes	Target host (host name or IP address)
Juniper Health	Yes	Target host (host name or IP address)
Juniper Temp	Yes	Target host (host name or IP address)
Juniper Fans	Yes	Target host (host name or IP address)
Juniper CPU Usage	Yes	Target host (host name or IP address)
Juniper Memory	Yes	Target host (host name or IP address)
Big-IP Health	Yes	Target host (host name or IP address)
Big-IP Temp	Yes	Target host (host name or IP address)
Big-IP Statistics	Yes	Target host (host name or IP address)
Big-IP Free Space	Yes	Target host (host name or IP address)
Big-IP CPU Usage	Yes	Target host (host name or IP address)
Big-IP Memory	Yes	Target host (host name or IP address)
Netscaler Temp	Yes	Target host (host name or IP address)
Netscaler Statistics	Yes	Target host (host name or IP address)
Netscaler CPU Usage	Yes	Target host (host name or IP address)
Netscaler Memory	Yes	Target host (host name or IP address)
NetApp Health	Yes	Target host (host name or IP address)
NetApp CPU Usage	Yes	Target host (host name or IP address)
NetApp Temperature	Yes	Target host (host name or IP address)
NetApp RAID	Yes	Target host (host name or IP address)
NetApp Free Space	Yes	Target host (host name or IP address)
QNAP Health	Yes	Target host (host name or IP address)
QNAP Temperature	Yes	Target host (host name or IP address)
QNAP Fans	Yes	Target host (host name or IP address)
QNAP CPU Usage	Yes	Target host (host name or IP address)
QNAP Memory	Yes	Target host (host name or IP address)
QNAP Free Space	Yes	Target host (host name or IP address)
Synology Health	Yes	Target host (host name or IP address)
Synology Temp	Yes	Target host (host name or IP address)
Synology Disk Load	Yes	Target host (host name or IP address)
Synology CPU Usage	Yes	Target host (host name or IP address)
Synology Memory	Yes	Target host (host name or IP address)
Synology Free Space	Yes	Target host (host name or IP address)
HP iLO Health	Yes	Target host (host name or IP address)
HP iLO Temp	Yes	Target host (host name or IP address)
HP iLO Fans	Yes	Target host (host name or IP address)

HP iLO Power	Yes	Target host (host name or IP address)
HP iLO Disks	Yes	Target host (host name or IP address)
UPS Health	Yes	Target host (host name or IP address)
UPS Load	Yes	Target host (host name or IP address)
UPS Charge level	Yes	Target host (host name or IP address)
UPS Input voltage	Yes	Target host (host name or IP address)
UPS Output voltage	Yes	Target host (host name or IP address)
UPS Temperature	Yes	Target host (host name or IP address)
UPS Remaining time	Yes	Target host (host name or IP address)
Printer status	Yes	Target host (host name or IP address)
Printer supply levels	Yes	Target host (host name or IP address)

When you specify test item Name, Comment, Related URL and Private Log path you may use folder-related variables plus you may use variables that represent parameters of the test (test-properties variables):

Variable	Variable can be used for the following tests	Variable represents
%MethodName%	Any	Name of test method (e.g. Ping, TCP, Traffic Monitor)
%Folder%	Any	The name of the folder containing the test
%FolderFullPath%	Any	The full folder path name (e.g. Root\USA\Main office)
%FolderParent%	Any	Parent folder name
%Agent%	Any	Represents a name of the remote agent that performs the test, this variable returns the string "*HostMonitor*" when the test is performed by HostMonitor
%host% or %hostaddr%	Most of the test methods, except ODBC Query, RAS, Active Script, Shell Script, External	Represents the host name (or IP address) of the target system
	Count Files Text Log Compare Files File Integrity Folder/File size File/Folder Availability	Name of target server or "localhost" when test item checks local file. Note: if you setup test using path to mapped network drive (instead of using UNC path), this variable will return "localhost".
%HostAddrB%	-//-	Variable works similar to %HostAddr% variable but returns host name without back slashes. E.g. if path to the file specified as \\sqlserver5\share\file5 then %HostAddr% will return \\sqlserver5 while %HostAddrB% will return sqlserver5
%Path%	URL	URL

	HTTP	URL
	SOAP/XML	URL specified for request
	UNC	UNC path
	Drive Free Space	List of drives, including "local" and "removable" (if such options were selected for the test)
	Folder/File size	Full path to the folder/file
	File/Folder Availability	Full path to the folder/file
	Count Files	Full path to the folder plus file mask
	Compare files	Full path to the file (1st file)
	File Integrity	Full path to the file
	Text Log	Full path to the file
	ODBC Query	SQL Query
	SNMP Get, SNMP Table	Using the database of compiled MIB files HostMonitor translates specified OID from its numeric form to a MIB name. E.g. - %Path% = iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOperStatus.1 - %Object% = .1.3.6.1.2.1.2.2.1.8.1 If you need to extend the database by including information about MIBs supported by some specific SNMP enabled device, use MIB Browser.
	Service	"Display name" property of the service
	NT Events Log	Event log \ Event source
	Registry	Full path to registry key
	External test	Command line
	Active Script	Full path to the script or '*Internal active script*' string if script is stored in HML file
	Shell Script	Name of the script
	Performance Counter	Full path to the counter
	WMI	WMI Query
	E-Mail	Login and server (e.g. hmonitor@mailserv.com)
	Mail Relay	Source e-mail address + destination address
%Object%	URL	Target page with optional parameters E.g. - %Path% = http://www.google.com/search/advanced.cgi?hl=en - %Object% = /advanced.cgi?hl=en
	HTTP	Target page with optional parameters
	SOAP/XML	SOAP method
	Domain expiration	Domain
	NGINX	Zone name
	Tomcat	Memory pool name or Connector name
	IIS	Site name (instance)
	SMTP	Username if "Perform VRFY test" option is enables, otherwise %object% variable returns empty string

	POP3	Username
	IMAP	Username
	E-Mail	“Bad” filter: short text description
	Mail Relay	Destination e-mail address
	DNS	Requested domain name
	LDAP	Base object if “Perform search” option is enabled, otherwise variable returns empty string
	RAS	Dial-up connection name
	UNC	Target resource (file, folder, etc) E.g. - %Path% = \\primary_host\shareddrive1\logs\log1.txt - %Object% = log1.txt
	Disk free space	List of drives (only if "check listed drives" option is selected)
	Folder/File size	Folder/File name (no path, just name and extension)
	Count Files	Folder name
	File/Folder Availability	Folder/File name (name and extension)
	Compare files	File name (1st file)
	File Integrity	File name (name and extension)
	Text Log	File name (name and extension)
	Interbase	Database name
	MS SQL	Database name
	MySQL	Database name
	Oracle	Server (TNS alias)
	PostgreSQL	Database name
	Sybase	Database name
	ODBC Query	Data source
	Process	Process name
	Service	Service name (“short name” property of the service)
	SNMP Get	OID (object identifier)
	SNMP Table	OID (object identifier)
	SNMP Trap	OIDs used as test filters
	NT Events Log	If test was setup to checks specific source, variable represents source name, otherwise it shows log name
	Memory	Memory type checked by the test item *Swap* *Physical memory* *Virtual memory*
	Performance Counter	Counter name
	WMI	Name of 1st field listed in the query
	Registry	Counter name
	DHCP Pool	DHCP scope

	External test	File name (without path and parameters)
	Active Script	File name (script) or '*Internal active script*' string if script is stored in HML file
	Shell Script	1st parameter of the script (if any)
	Temperature Monitor	Temperature probe name
	Traffic Monitor	Network interface description
	HM Monitor	Name of target HostMonitor parameter selected for Reply value
	IPMI Temperature IPMI Fans IPMI Voltage IPMI Current IPMI Discrete	Name filter value
	Redfish Temperature Redfish Fans Redfish Voltage Redfish Current Redfish Power Redfish Sensor	Name/context filter value
%Object2%	SOAP/XML	Value specified for XML comparison or text string used for search
	DNS	Represents string (IP address) specified for results comparison
	E-Mail	If "good" filter specified, shows short text description
	File/Folder Availability	target path without file name
	Count Files	File mask specified for the test
	Compare Files	2nd file name if you compare 2 files, otherwise variable returns search string specified for the test
	Text Log	Search string specified for the test
	SNMP Get, SNMP Table	Value specified for comparison
	Performance Counter	Value specified for comparison
	WMI	Value specified for comparison
	Registry	Value specified for comparison
	Shell Script	2nd parameter of the script (if any)
	IPMI Discrete	Bitmask
	Redfish Sensor	Sensor type
%TargetPort%	TCP, UDP, SMTP, POP3, IMAP, E-Mail, LDAP, DSN, NTP/SNTP, DICOM, Radius, Certificate Expiratiom, Domain Expiration, SNMP	TCP (UDP) port specified for the test

	Table, Traffic Monitor, SSH, HM Monitor, NetApp, QNAP, Synology, Cisco, Juniper, F5 Big-IP, Citrix Netscaler and UPS related tests, IPMI tests	
%TestMode%	DNS	Type of DNS request - one of the following: *A* *AAAA* *CNAME* *MX* *NS*
	SOAP/XML	Information about CRC, Text or XML check modes
	Apache	Test mode, one of the following: *Connections/sec* *Bytes/sec* *BusyWorkers* *IdleWorkers*
	NGINX	Test mode
	Tomcat	Test mode
	IIS	Test mode
	Compare Files	Comparison mode - one of the following: *FilesDifferent* *FilesIdentical* *ContainsFile* *DoesntContainFile* *ContainsString* *DoesntContainString*
	Count Files	One of the following: *AllFiles* *OlderThan N min* *NewerThan N min* *BiggerThan N bytes/KB/MB/GB* *SmallerThan N bytes/KB/MB/GB* *SubFolders*
	Dominant Process	Shows what kind of resources is checked by the test item - one of the following: *CPU Usage* *Handles* *Threads* *Memory* *VMem* *Address space*
	SNMP GET, SNMP Table	Comparison mode – one of the following: *LessThan*

		MoreThan *EqualTo* *DifferentFrom* *Contain* *NotContain* *IncreaseBy* *DecreaseBy* *ChangeBy* *IncreaseBy%* *DecreaseBy%* *ChangeBy%* *Increase/Sec* *Decrease/Sec* *Change/Sec*
	Network Traffic	Shows what check mode is used - one of the following: *Traffic* *Traffic in* *Traffic out* *Discards in* *Errors in* *Discards out* *Errors out* *Queue*
	Memory	Protocol used for the test *SNMP* *WMI*
	Performance Counter WMI	Comparison mode – one of the following: *LessThan* *MoreThan* *EqualTo* *DifferentFrom* *IncreaseBy* *DecreaseBy* *ChangeBy* *IncreaseBy%* *DecreaseBy%* *ChangeBy%* *Increase/Sec* *Decrease/Sec* *Change/Sec*
	Registry	Comparison mode – one of the following: *Any change* *LessThan* *MoreThan* *EqualTo* *DifferentFrom* *Contain*

		NotContain
	Firewall status	One of the following: *Local profiles* *Group policies*
	Antivirus status	Test mode - one of the following strings: Windows Kaspersky ESET
	QNAP Temperature	One of the following strings: *CPU temperature* *System temperature* *Disk temperature*
	Synology Temperature	One of the following strings: *System temperature* *Disk temperature*
	Synology Disk Load	One of the following strings: *1 min average* *5 min average* *15 min average*
	Active Script	Script langauge (VBScript, JScript, etc)
	IPMI Temperature IPMI Fans IPMI Voltage IPMI Current IPMI Discrete	Sensor type
	Printer supply levels	String like “Toner,supplies,waste,units”
%AllParams%	ShellScript	Parameters of the script
%MibName%	SNMP Get, SNMP Table	Using the database of compiled MIB files HostMonitor translates specified OID from its numeric form to a MIB name. If you need to extend the database by including information about MIBs supported by some specific SNMP enabled device, use MIB Browser.
%MibNameShort%	SNMP Get, SNMP Table	Similar to %MibName% but shows the name of the variable (plus possible index) without names of parent nodes. E.g. - %Object% = .1.3.6.1.2.1.2.2.1.8.1 - %MibName% = iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOperStatus.1 - %MibNameShort% = ifOperStatus.1

There are several variables that allow you to disguise part of data:
- %DisguisedFolderFullPath%
- %DisguisedHost%
- %DisguisedPath%
- %DisguisedObject%

These variables similar to %FolderFullPath%, %Host%, %Path% and %Object% variables but some symbols will be replaced with DisguiseChar ('?' by default). You may add [DORA] section into hostmon.ini file and set the following options:

[DORA]

DisguiseMode=0|1|2|3	0 – disguise mode off 1 – replace characters on the left 2 – replace characters on center 3 – replace characters on the right
DisguiseChar=<symbol>	Replace the actual characters with the specified symbol. The default symbol is '?'
DisguiseLen=<number>	The number of DisguiseChar symbols in the result string. If you set it to 0, each replaced character will be displayed (as '?'), so the number of '?' characters will be equivalent to the actual number of replaced characters
DisguiseRatio=<number>	Percentage of characters that should be disguised
NonDisguiseMin=<number>	Minimum number of characters that should not be disguised
NonDisguiseMax=<number>	Maximum number of characters that should not be disguised

Examples

DisguiseMode=3 DisguiseChar=* DisguiseLen=3 DisguiseRatio=50 NonDisguiseMin=10 NonDisguiseMax=20	server5 → server5 server_store_150 → server_sto*** server1255.goverment.gov → server1255.g*** Root\Texas\WebServers\3rdcluster\Apache305128E\ → Root\Texas\WebServer***
DisguiseMode=1 DisguiseChar=? DisguiseLen=0 DisguiseRatio=50 NonDisguiseMin=10 NonDisguiseMax=20	server5 → server5 server_store_150 → ??????_store_150 server1255.goverment.gov → ????????????overment.gov Root\Texas\WebServers\3rdcluster\Apache305128E\ → ????????????????????????uster\Apache305128E\

All these variables allow you to configure HostMonitor to assign test name and comment automatically (see Patterns dialog)

When you edit test properties using Test Properties dialog HostMonitor displays template used for the field (if any) every time you enter the field and resolves template when you leaving the field. Active field with template in use will be displayed in yellow background color. When you see template (field is active) you may check correspondent value while moving mouse over the field (HostMonitor will show popup "hint", also value will be displayed on status bar). And vice versa: when field is not active you will see resolved value as text written in the field and you may check template that was used for the field by moving mouse over the text.

Template folders / Default templates

Ok, you created set of tests using variables and you plan to use these tests as templates for many hosts to monitor. You may place these tests into some folder (plus sub-folders) and mark such folder using popup menu "**Set as templates**". Note: only one folder (with all sub-folders) can be used for templates.
HostMonitor applies special rules related to tests and folders marked as templates:
- HostMonitor uses special color for template folders and tests (you may adjust palette using Color Profiles dialog)
- HostMonitor uses special icons for template test items
- HostMonitor does not perform template test items so now you don't need to disable such items and then enable newly created items after replication
- License check does not count template test items. E.g. if you have Advanced license you may monitor 5000 "normal" test items plus setup hundreds of template items at no additional cost (this is especially useful when you have the simplest Starter license)
- "Append from HML file" function merges "normal" folders and separately merges template folders
- Auditing Tool does not check template test items for unresolved folder-level variables (HostMonitor will check for unresolved variables when you create "normal" tests using templates)
- Auditing Tool checks if "normal" test depends on template master item (you should not set such relations because test will not be performed)
- HostMonitor does not include template folders and tests into reports (unless template folder is selected as main folder for the report)
- HostMonitor does not show template folders and tests on screen (even if "show tests in sub-folder" option is enabled and Root folder selected), unless you choose Template folder as current folder
- When you choose Master test for "normal" dependent item, HostMonitor will not show Template tests in the list
- Web Service does not show Template folders and tests on screen (even if "display tests from current folder and from all sub-folders" option enabled and Root folder selected), unless you select Template folder as current folder

Special template sub-folders
You may create any sub-folders within main Template folder. If you create sub-folder with one of the following names, then HostMonitor will add corresponding menu item into main menu (Tests->New) and into "Add" popup menu:

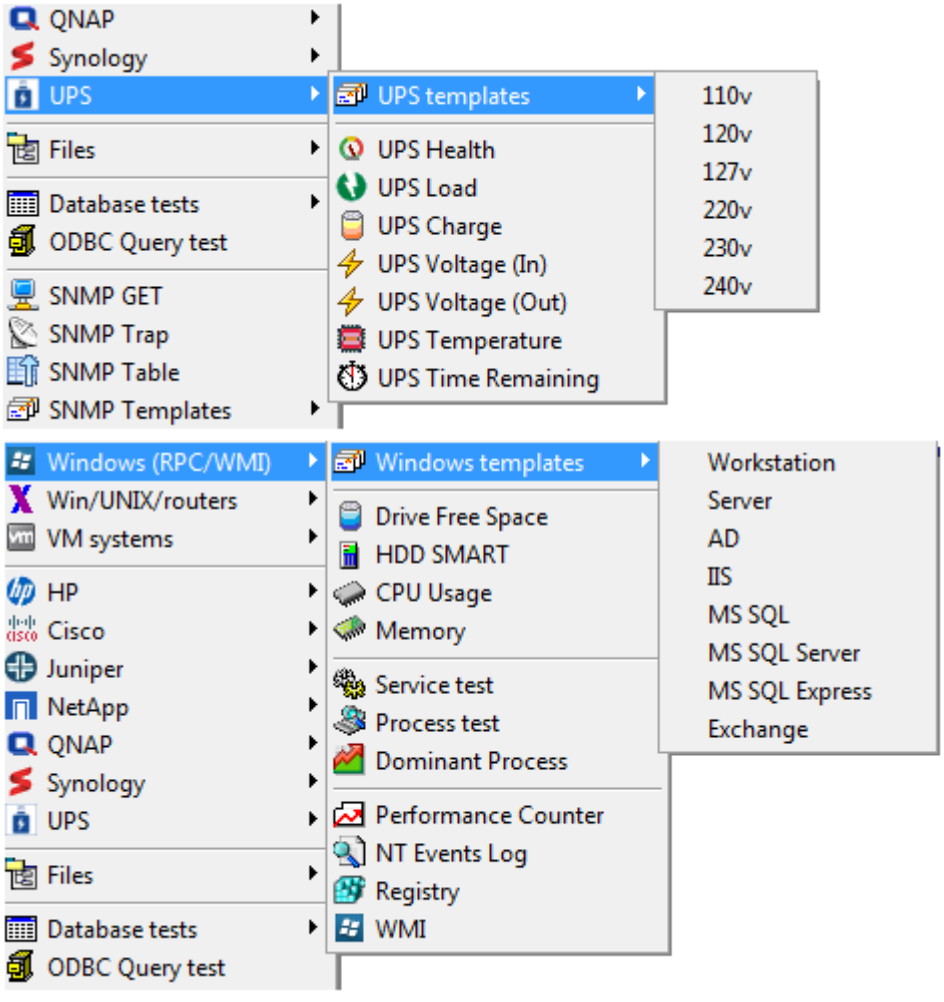
Lan
Email
Web
IIS
Apache
Nginx
Tomcat

Windows
Unix
VMWare
HyperV
HP iLO
IPMI
Redfish

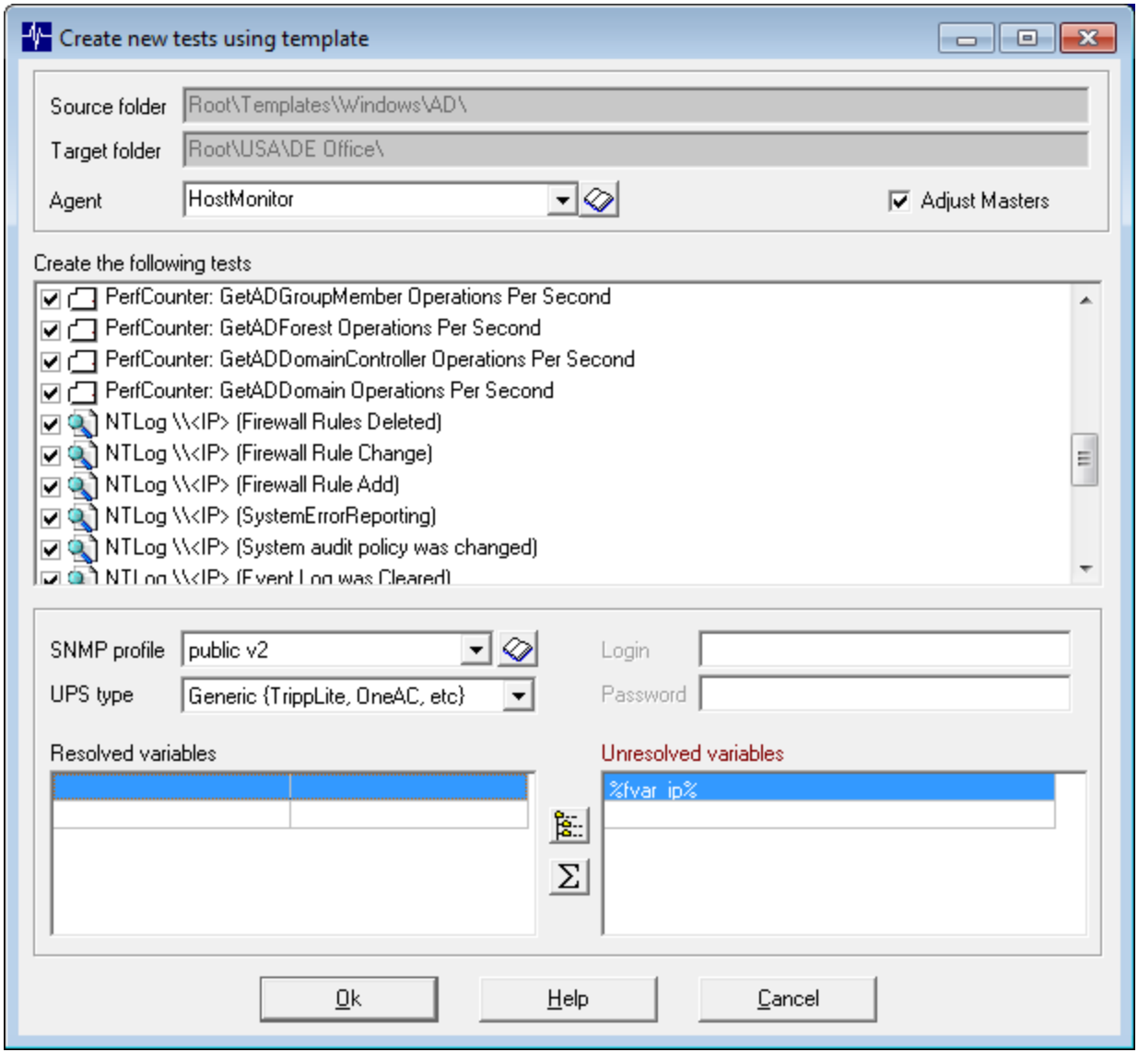
Cisco
Juniper
BigIP
Netscaler
Netapp
QNAP
Synology
BigIP
Netscaler
UPS

Files
Interbase
MsSql
MySql
Oracle
Postgree
Sybase

SNMP
External



When you use such menu item, HostMonitor will show all tests related to the corresponding template folder



Then you may unmark some tests, change monitoring agent, set SNMP profile for SNMP related tests, change type of UPS device (for UPS related tests), set login and password for tests that require account information (see also: Connection Manager). If some test depends on master(s), HostMonitor checks if master template test items selected and shows warning if such items located in different template folder or master test is unmarked by operator. Also HostMonitor checks if all variables will be resolved after replication - if there are some missed variables, you may define variables using Folder Properties dialog.
Also there is "**Adjust Masters**" option. With this option enabled, if dependent tests copied with master(s) then HostMonitor adjusts master-dependant relations for newly created tests. E.g. if you copy 6 tests (5 UPS tests that depends on 1 Ping test) then new UPS tests will depend on new Ping test (if you are using folder-related variables for target IP address, then new tests will start to monitor new device without any manual adjustments).
If you create just dependent tests without related master template test, then HostMonitor will unlink newly created (replicated) dependent tests from this "missed" master.

Predefined templates

HostMonitor comes with some predefined templates: over 600 items for Windows and UNIX systems, Cisco, Juniper, QNAP, NetApp and Synology devices, HP servers, MS SQL, MySQL, Oracle databases and so on. You may adjust items for your needs (e.g. set alert profiles, change time interval, schedule and logging options, adjust alert), adjust alert thresholds, add more folders and test items or remove them.
Many template tests will be able to monitor your servers without modifications – just create folder, setup %fvar_ip% variable (IP address or host name of the server) and you may add set of tests using templates;
some tests require user account information, you may provide default account or accounts for each server using Connection Manager;
other template tests will require modifications, e.g. if you need to check database size, you need to set database name in SQL query (ODBC Query tests); also you may need to modify class name used in MS SQL related WMI queries.

Update
If you already use your own templates and you updated HostMonitor to version with predefined templates, you have several options:
- remove default templates that come with HostMonitor (remove Templates folder) then select your main template folder and use "Set as Templates" popup menu item;
- you may merge our templates with your items – simply drag&drop your folders (or some selected test items) into Templates folder

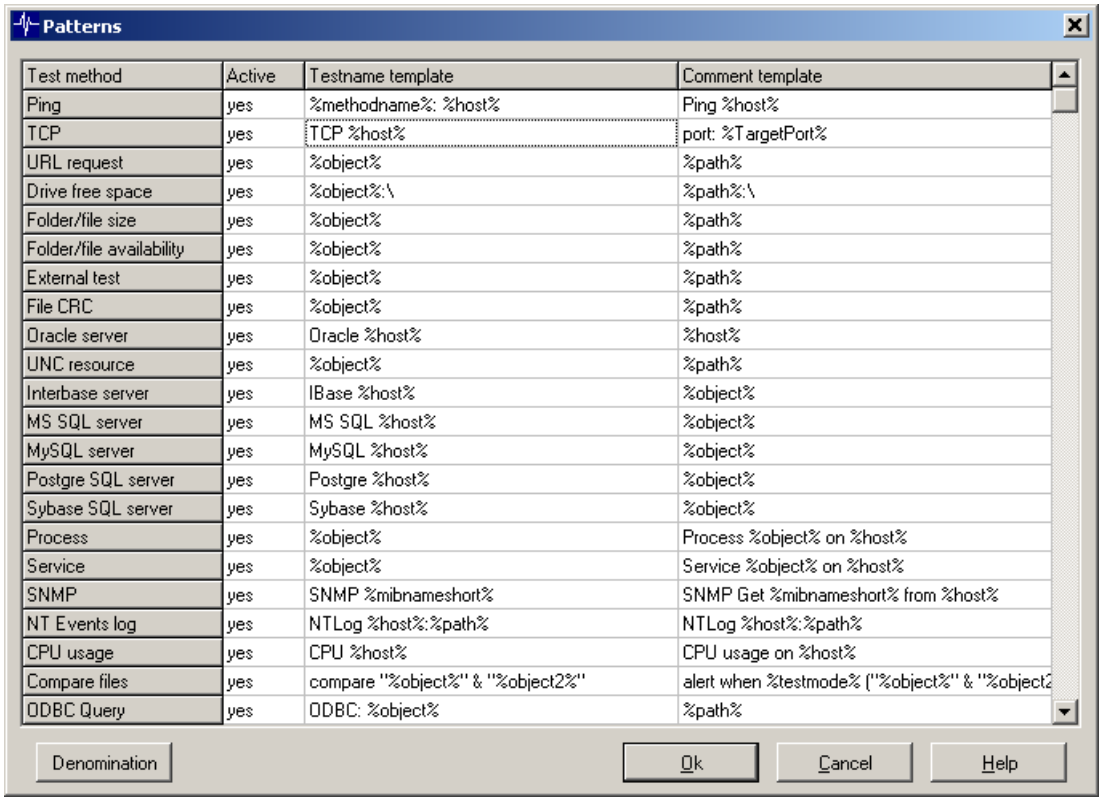
Probably your old template test items are disabled? You may enable test items – now HostMonitor does not execute template test items.

Save Templates as default
This menu (File -> Save Templates as default) tells HostMonitor to save all template folders and tests into special file (deftemplates.lst). If you load some old testlist (HML file) without templates or create new test list, then default templates will be added to the list automatically.
(option not available for remote RCC operators)

Patterns dialog

"Patterns" menu item (located in menu Profiles) allows you to configure patterns that tell HostMonitor how to automatically assign test name and comments for new test items. There are 3 options can be specified for each test method:

- pattern active / not active
- testname template
- comment template



If you create new test item and there are active templates specified for this test method, HostMonitor will assign templates automatically so you don't need to type name and comment for each new item.

We recommend using special test-properties variables for name and comment templates. In such case test name may depend on test settings. E.g. you may use "Ping: %host%" template for Ping test name and "SNMP %mibnameshort%" template for SNMP Get tests. In such case if you change target host name for Ping test, HostMonitor will change test name automatically. If target host name contains some variables as well, HostMonitor may change test properties, name and comment when you move or copy test items from one folder to another. See Templates for details.

You may use folder-related variables in templates as well. In such case tests in various folders may have distinguished names.

In spite of automatically assigned test name and/or comment, you may override assigned name at any time. You may set different template for some specific test item or use static text.

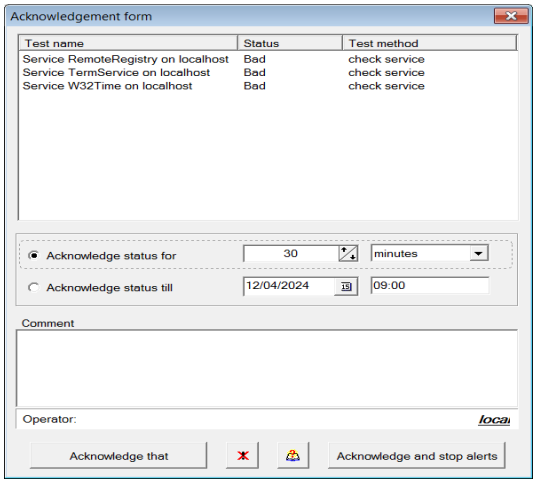
There is “Denomination” button that allows you to rename all test items within loaded testlist at once. HostMonitor will apply pattern list for all items so you will have great consistency in test names.
Note: We would not recommend playing with “denomination” option without necessity as Log Analyzer separate test items by name (not only name but name is one of the keys). If you rename test item, log file will contain records with different names related to the same test item. As result Log Analyzer will show 2 statistical records for the same test item. We plan to redesign Log Analyzer in version 8.

Note: Any operator that has access to “Root“ folder (in other words has access to all test items) and owns right to configure tests and folders may modify patterns.

Acknowledgement

Menu item "Acknowledge" provides access to "Acknowledgment form" window (menu item available thru main menu [Test] and popup menu in Test Detail Area).
When you click on the "Acknowledge that" or "Acknowledge and stop alerts" button, HostMonitor will mark selected test item(s) as "acknowledged". What does that mean?

It means:



1. "Acknowledged" test items can be displayed in different color (different from non-acknowledged "bad" or "unknown" tests). There is item in "Color profiles" dialog which allows you to select specific color for "acknowledged" items within each color scheme. This applies to GUI, HTML reports and HTML log files.
2. Same color will be used for folders containing some "unknown" and/or "bad" test items when all of them are "acknowledged" (this applies only to GUI interface).
3. HostMonitor's system tray icon: HostMonitor displays such icon when there are some "unknown" and/or "bad" test items but all of them are "acknowledged".

4. HostMonitor adds the record into the log file, with information about acknowledgement (date and time, name of the user who acknowledged test status).
5. Also you may see this information in Quick Log
   Note: You may setup HostMonitor to include acknowledgement comments into log file/database (1st line of the comment will be displayed in Reply field). This option is not accessible thru GUI however you may add line like ReplyIncludeAckComment=1 into [Logging] section of hostmon.ini file and restart HostMonitor

6. If you have used "Acknowledge and stop alerts" button, HostMonitor will suspend all alerts triggered by "acknowledged" test item(s) until the test(s) restores "good" status - then HostMonitor will resume normal actions behavior ("ack" flag could also be cleared when test changes the status from "unknown" to "bad", unless you have marked "Treat Unknown status as Bad" option for this test item). Exception: advanced action with **%AcknowledgedJustNow%** variable may be triggered regardless of "stop alerts" flag
7. If you have used "Acknowledge that" button, HostMonitor will not suspend alerts. However you may configure the alert profile to launch different actions for "non-acknowledged" and "acknowledged" test items (using "advanced mode" actions and "acknowledged" macro variables).

8. There are 3 fields that display information about acknowledged test items:
   Acknowledged At - shows the time of the test acknowledgment

Acknowledged By - shows name of the user (operator) who have acknowledged the test status

ACK Comment - displays 1st line of the comment provided for "acknowledge" operation; if later operator adds 2nd or 3rd acknowledgment comment then GUI shows last comment line (so you will see newest comment)

These fields could be displayed in main HostMonitor's window (use the Columns page in the Options dialog to setup the list of visible fields); also these fields can be displayed in reports (see Report Manager section of the manual for details). As well, you may see information about "acknowledgment" in the Info Pane, where the detailed "acknowledgment" comment is included.

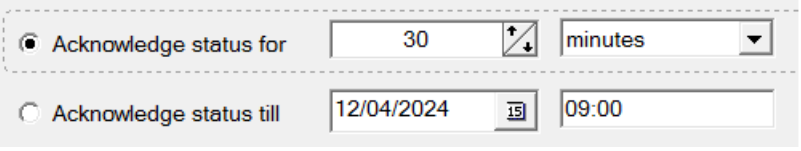
When test changes its status back to "good", all these fields are automatically cleared by HostMonitor.

9. There are 6 macro variables that provide information about acknowledged tests:

%AcknowledgedAt%	Represents the date and time when test status was acknowledged
%AcknowledgedDate%	Represents the date when test status was acknowledged
%AcknowledgedTime%	Represents the time when test status was acknowledged
%AcknowledgedBy%	Shows the name of the operator who has acknowledged the test status
%AckComment%	Shows the comment which was provided for "acknowledge" operation
These 5 variables return empty string for non-acknowledged test items.	
%AckRecurrences%	Represents the number of test probes which have returned similar (bad or unknown) result after it was already acknowledged. Returns 0 for non-acknowledged test items. For example if the test returned "bad" status during five consecutive probes, then %Recurrences% variable will be equal to 5. If the user has acknowledged the bad status after the second probe then %AckRecurrences% will be equal 3 (5-2=3). This variable is useful when you want to configure alert profile to launch different actions for "non-acknowledged" and "acknowledged" test items. E.g. if condition to trigger action execution looks like ('%SimpleStatus%=='DOWN') and (%AckRecurrences%==1), HostMonitor will start action when user confirmed status and test failed once again (after acknowledgement).
%AcknowledgedJustNow%	Advanced mode action and variables like %AckRecurrences %, %AckComment% allow starting special actions when Bad test status was acknowledged by the operator. Such actions could be started after the following test probes while sometimes you may need to start action right after acknowledgment. If you set advanced mode action using **%AcknowledgedJustNow%** variable, then HostMonitor may trigger action when operator acknowledges test status without

	waiting for the next test probe. This way you may pause or disable test (if you need) right after acknowledgement and still trigger special action(s). For example, you may use expressions like %AcknowledgedJustNow% and ("%Reply%" > "90 %") %AcknowledgedJustNow% and (("%AckComment%" getword 1)=="Attention") Note: HostMonitor may trigger such action even if operator chooses "acknowledge and STOP alerts" option; "New ack comment" operation may trigger such alerts as well.

10. Report Manager provides filtering options that allow you to display "acknowledged" and "non-acknowledged" items in separate reports (if you want to do so)



You can acknowledge an issue (Bad or Unknown test status) for N minutes/hours/days or until a specific time such as October 25, 2027. This time can be adjusted later by the operator. When the specified time expires, HostMonitor will change the test color to "red" (after the following test probe, unless this time test will return to "good" status). If "stop alerts" acknowledgement option was used, the actions will be resumed after the specified time expires. Also, if you set ResetRecurrencesOnExpiredAck=1 option ([HostMon] section of the hostmon.ini file), then HostMonitor will reset Recurrences counter after the acknowledgement period expires, even if the test status remains the same. This allows to start predefined sequence of actions from the beginning (for example, if you setup alert profile to send an e-mail to the administrator only once when the test status changes from "good" to "bad", then HostMonitor will start this action again after the acknowledgement period expires)

Note 1: after initial acknowledgment of test status, other local and remote operators can amplify “acknowledgment” comment and/or change expiration time.
Note 2: HM Script provides command for automatic acknowledgment

Note 3: Normally HostMonitor resets operators comments when test status changes from “bad” to “good”. However you may change this behavior. If you insert KeepAckCommentNDays=3 line into [Logging] section of hostmon.ini file and restart HostMonitor, it will keep comments that are up to 3 days old (you may use different number, e.g. keep comments for 5 or 15 days)

Accounts

Some test methods do not require any authorization, e.g. Ping test, TCP, UDP, DHCP; some tests may require account information, e.g. Process test, Service, NT Event Log, CPU Usage (if you do not specify accounts for specific tests and hosts, the account under which the program is run will be used); some test methods always require authorization and you must specify which account should be used, e.g. SNMP Get, SNMP Table, Cisco, Juniper, QNAP and NetApp related test methods, WMI and Dominant Process test methods.

Accounts menu provides access to necessary tools:

Connection Manager	- provides one convenient place where you may store account information necessary to perform connections to the remote systems. Built-in Password Generator allows you to generate new passwords for set of multiple accounts with a single click.
SSH Key Manager	- this tool allows you to manage private and public keys used for SSH test authentication. Private key authentication has priority over password authentication.
SNMP Credentials	- SNMP Credentials dialog allows you to setup list of SNMP profiles (accounts). Profiles store login or community string and other information necessary for communication with SNMP agent.
Change Master password	- this option allows you to change the master password used to encrypt files with sensitive information

Master password

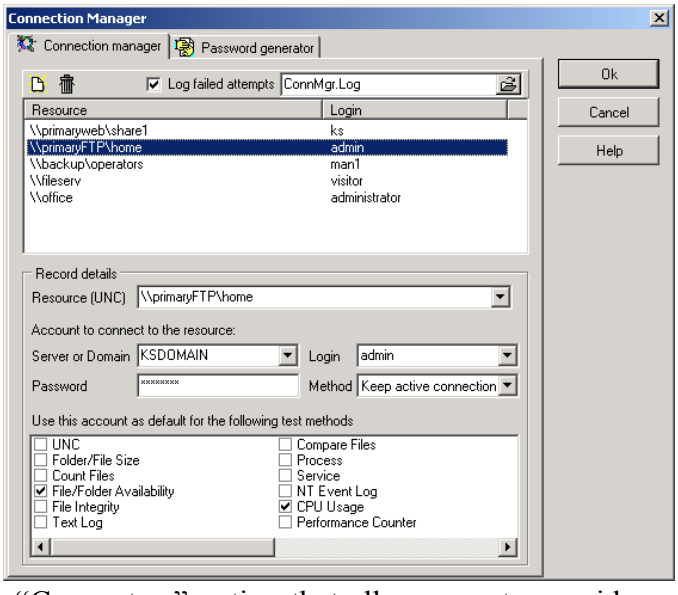
Set/Change Master password

This option allows you to change the master password used to encrypt files with sensitive information, e.g. private SSH keys, accounts used to connect to remote systems, etc. If you move HostMonitor and configuration files to another system, you will need to enter this password the first time you start the software (if you start HostMonitor as a service right away, then use RCC to enter the master password)

Connection Manager and Password Generator

Connection Manager

When you check the remote system, some test methods (like CPU Usage, Process, Service, NT Event Log and several others) need to establish connection with that remote system using a user name and password. Connection Manager provides one convenient place to store account information necessary to perform connections to remote systems.



Note: in many cases, when HostMonitor or RMA agent runs under a domain account and checks other members of the same domain, you don't need to configure accounts here.

As you already have noticed, many tests have "Connect as" option that allows you to provide an account name and password necessary to establish communication. But if, for example, you need to check 20 different processes on the same server, you will need to specify that password for every test separately. With the help of Connection Manager you only need to create a single record for the account. This is also very convenient when the password for that account is changed from time to time (check also Password Generator).

Another advantage of Connection Manager – it allows you to provide account information for test methods that normally were designed to work with local files but may also be used to test remote shares as well. Test methods Folder/File Size, Count Files, File Availability, File Integrity, Text Log, and Compare Files do not have "Connect as" option. However when the path to the file/folder is specified in UNC format, Connection Manager may establish connection prior to the execution of these tests.

Also you may specify "Reconnect if necessary" option for an account. With this option selected when the system (where HostMonitor is running) is already connected to the remote system with a user account that doesn't have enough permissions to perform the test, Connection Manager may reconnect the system using specified account.

And one more advantage: if HostMonitor is unable to establish connection with the remote system, Connection Manager may log the response from that remote system; information such as why the connection was rejected will be stored.

So, what information you need to provide for each record:

Agent

Use this field to specify Remote Monitoring Agent (or HostMonitor) that will check target host or LAN. If you set "Any" option, then account can be used for any agent and HostMonitor itself.
Please see notes below

Resource (UNC)
Specifies an UNC path to the resource with which HostMonitor are going to establish the connection. E.g. if you plan to use an account for CPU Usage, Process or Service test methods that require a connection to the remote system, you may use just the name of target system (like \\primaryserver). Or you may specify a full path to the share (e.g. \\primaryserver\web\sharefolder1), this makes more sense for file related tests such as Folder Size or File Integrity.

Server or Domain
Specifies the DNS or NetBIOS name of a remote server or domain that will authorize connection.

Login
Provides a user name that is used for the connection.

Password
Specifies a password to be used when establishing the network connection.

Method
This parameter defines HostMonitor's behavior in case when the connection with specified remote system is already established but with different (than specified) account.
Choose one of the options:
- Keep active connection
- Reconnect if necessary

With the 1st option selected HostMonitor will not drop current connection and will not establish another one. This method is guaranteed not to interfere with other applications or users already using the same connection. But on the other hand if an account that is used for connection does not have all required permissions the test may fail.
With 2nd option selected, Connection Manager will drop current connection and establish new one using specified account.

Use this account as default for the following test methods (list of test methods)
Here you select test methods that will use specified account as default. "Default" means that this account will be used unless another account is specified directly for the test item (using "Connect as" option).

Special accounts:

- You may provide "default" account that will be used by HostMonitor for every resource not included in the list. To do so, type * as resource name. Then you may provide name of the server/domain or type * instead of server name. In 1st case HostMonitor will send authentication information to the specified server; in 2nd case (unc=* and sever=*) HostMonitor will connect to the server that was specified as test parameter.

- In addition to default and host-specific accounts, you may specify accounts based on IP address ranges (e.g. you may specify one user account for 10.10.1.5-10.10.1.55 range, another account for 10.10.1.200-10.10.1.235 range)

Connection Manager may use account specified for some specific IP or IP range even if you are using hostname (not IP) for the test item target. When HostMonitor tries to find account for target server, it checks records trying to find specified resource or hostname; if such resource/hostname not found, HostMonitor resolves hostname to IP address and check Connection Manager records for this IP. If account for specific IP address could not be found either, HostMonitor will try to find appropriate account within "IP range" accounts. Only when all attempts fail, HostMonitor will use "default" account.
Note: some "hostname to IP" conversions related to UNC resources is not supported. E.g. if you setup file related test method using target resource like \\hostname\resource\folder\file and you have specified one or several accounts using IP or \\IP or IP range, this will work fine. But if you specified only one Connection Manager account using \\IP\resource path (e.g. \\192.168.1.100\C$), then HostMonitor will not use this record for connection (even if "hostname" can be resolved to "192.168.1.100" IP).

HostMonitor version 10 introduces "agent" property, this option changed the way HostMonitor chooses account for remote connection:

Step 1

1-a) highest priority has record for specific agent and specific resource. E.g. If "Folder Size" test performed by "NY-agent" checks \\dbase_server5\tables\root\ folder, then HostMonitor will try to find account record with enabled "Folder/File size" test method for NY-agent with resource field set to \\dbase_server5\tables\root
1-b) if such record not found, then HostMonitor checks for account record with the same properties but with agent field set to "Any" (any RMA or HostMonitor)

Not found? go to Step 2

2-a) HostMonitor will try to find account record with enabled "Folder/File size" test method for NY-agent with resource field related to target host (e.g. \\dbase_server5\tables or dbase_server5 will match)
2-b) if such record not found, then HostMonitor checks for account record with the same properties but with agent field set to "Any"

No such records? go to Step 3

3-a) HostMonitor will use IP address of target system to check for appropriate record (resource for specific IP or IP range) specified for "NY-agent"
3-b) if such record not found, then HostMonitor checks for specific IP or IP range specified for "Any"

If there is no record for target host, go to Step 4

4-a) Get "default" account (resource specified as *) for "NY-agent"
4-b) Finally (lowest priority), use "default" account specified for "Any"

So, now we have 8 priority levels.

Note: If you provide some account just for primary agent and primary RMA agent fails and there is backup agent installed, same account will be used.

LAPS

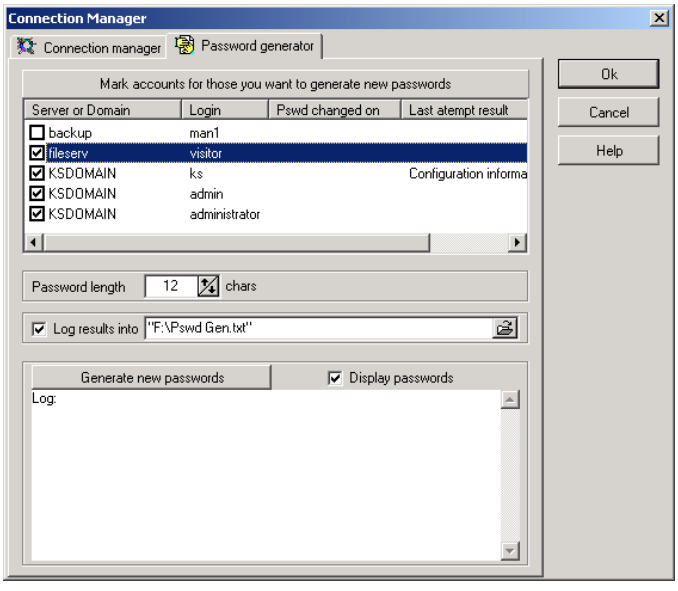
The Local Administrator Password Solution (LAPS) provides management of local account passwords of domain joined computers. Passwords are stored in Active Directory (AD) and protected by ACL. Connection Manager may retrieve up to date local administrator passwords from Active Directory and update records in HostMonitor database.
By default "administrator" account name is used; if you set LAPS for other account (using LAPS GPO policy), change account name on HostMonitor side as well using Connection Manager popup menu LAPS → Set default account name.

You may update password for single selected item using menu LAPS → Update password for selected item.
You may update passwords for all items using menu LAPS → Update passwords for ALL administrator accounts (please check Note1 and Note2).

Note 1: Remote Monitoring Agents do not support LAPS options yet. So Connection Manager may update records related to hosts within local HostMonitor/RCC domain.
Note 2: domain/server field of the record should point to specific server, default account (*) and accounts for IP ranges are not updated.
Note 3: Microsoft LAPS modules should be installed on system where HostMonitor (and/or RCC) is running
https://www.microsoft.com/en-us/download/details.aspx?id=46899
Note 4: in order to get passwords using LAPS HostMonitor/RCC account requires "All extended rights" permission. Please make sure regular users, groups or computer objects do not own this permission. To restrict the ability to view the password to specific users and groups you need to remove "All extended rights" from users and groups that are not allowed reading the value of attribute ms-Mcs-AdmPwd. This is important because the "All Extended rights" permission gives permission to read confidential attributes.

Other options
- Export to CSV file
- Import from CSV file
- "Find" and "Search again" popup menu items (Ctrl+F, F3). Application may check for IP address within IP range, e.g. it may find "10.10.5.55" in records like "10.10.5.11-10.10.5.99"

Password Generator



Another page in the same dialog represents Password Generator utility. This utility allows you to generate new passwords for the set of accounts with a single click.
Note: domain admin rights requires.

Every time you change records in Connection Manager utility (add new record, modify or remove existing one) these changes are automatically applied in Password Generator utility (as you add new record in Connection Manager, you will see that new record appears in Password Generator utility as well).

To generate new passwords follow these steps:

- Mark accounts for which you want to change passwords (if you already used Password Generator some time ago, it will remember the list of marked accounts and you may skip this step). If you want to mark multiple accounts, hold the Shift key while selecting the first and the last items to select a range of records and then press Space to mark/unmark selected records.
- Specify the length of passwords. Password Generator will generate random passwords (of specified length) using upper and lower case letter characters 'A'..'Z'; 'a'..'z', and numbers '0'..'9'
- Optionally you may mark "Log results into" selector and provide a file name that will be used for the log.
- Also you may use "Display passwords" option. In this case Password Generator will display new passwords for each account.
- Click "Generate new passwords" button

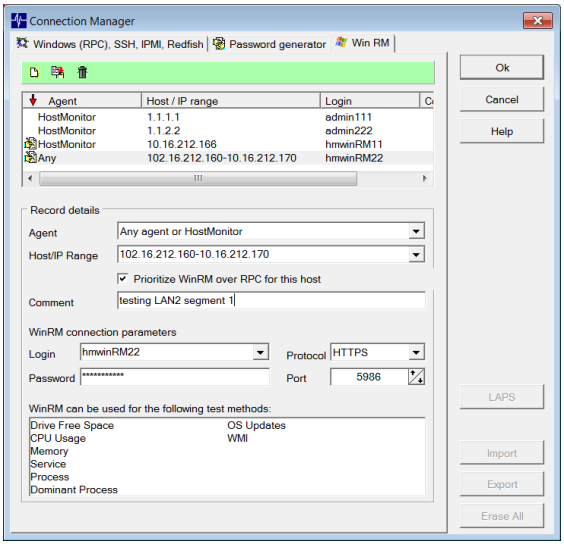
When Password Generator connects to the server and successfully changes a password, it also changes the password for the account that was specified in Connection Manager utility. This way, all accounts will be synchronized.
However it will not change passwords for test items that use "Connect As" option.

IMPORTANT: When you click "Generate new passwords" button you should remember that:

1) All changes that were made in Connection Manager utility will be saved
2) You will not be able to restore old passwords automatically (THERE IS NO UNDO)!
3) If selected accounts are in use by some users (or other applications), they will not be able to use these accounts after new passwords are generated!

WinRM

Windows Remote Management (WinRM) uses the WS-Management protocol, it transfers requests over the network using SOAP (Simple Object Access Protocol) messages sent over standard web protocols



Since version 15.80 some test methods support WinRM mode in addition to RPC, WMI and SNMP:
- Drive Free Space
- CPU Usage
- Memory
- Service test
- Process test
- Dominant Process
- OS updates
- WMI

Various **GUI** function can use WinRM as well, for example

- Test Properties dialog → Service test → 'Choose service to monitor' window can retrieve a list of services on the target system using WinRM protocol (directly or thru the RMA agent)
- Test Properties dialog → Process test → 'Copies of the following process' drop-down list can retrieve a list of the processes on the target system using WinRM protocol (directly or thru the RMA agent)
- System Info tool can retrieve various data using WinRM protocol (in addition to RPC, WMI, SNMP)

If you want to use the WinRM protocol for such tests, you should create the record(s) using the WinRM page.

Agent
Use this field to specify Remote Monitoring Agent (or HostMonitor) that will check target host or LAN. If you set "Any" option, then account can be used for any agent and HostMonitor itself.

Host/IP
Specify target system(s) using either
- hostname or FQDN (highest priority)
- IP address
- IP address range (e.g. you may specify one user account for 10.10.1.5-10.10.1.55 range, another account for 10.10.1.200-10.10.1.235 range)
- * specifies "default" account that will be used by HostMonitor for every resource not included in the list (lowest priority)

Prioritize WinRM over RPC for this host
If there are 'RPC' records and 'WinRM' entries (with the same priority level, e.g. specific hostname set for both records), then RPC takes precedence, unless you have set "Prioritize WinRM over RPC for this host" option.

For example
- if there are matched records with **specific hostname** in RPC section and WinRM section, and the "Prioritize WinRM over RPC for this host" option is not set, then RPC mode will be used;
- if there is a match for an IP **address range** in the RPC section and a match for a **specific hostname** in the WinRM section, then WinRM mode will be used, because the "specific host" entry takes precedence over the "IP range" entry (regardless of the "Prioritize WinRM over RPC for this host" option);
- if there is a match for a **specific hostname** in the RPC section and a match for an IP **address range** in the WinRM section, then RPC mode will be used, because the "specific host" entry takes precedence over the "IP range" entry (regardless of "Prioritize WinRM over RPC for this host" option)

Login
Provides a user name for authentication

Password
Specifies a password for authentication

Protocol
Select HTTP or HTTPS. HTTP without encryption is not recommended.

Port
TCP port used by the WinRM server(s). Typically, TCP port 5985 is used for unencrypted WinRM traffic; TCP port 5986 is used for encrypted WinRM connections.

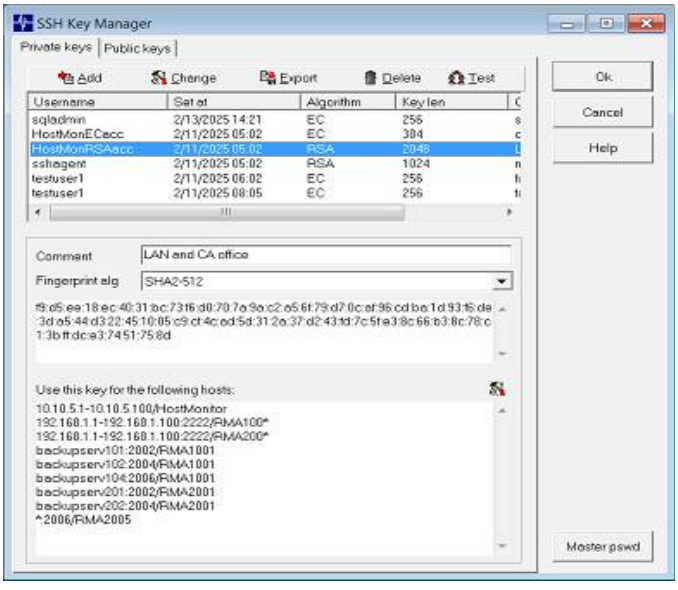
Useful Microsoft articles

Installation and configuration for Windows Remote Management

How to configure WINRM for HTTPS

SSH Key Manager

This tool allows you to manage private and public keys used for SSH test authentication. Private key authentication has priority over password authentication. This means that if the private key for the target server is set in SSH Key Manager, that key will be used to authenticate to the target server; otherwise, the password specified in the Connection Manager will be used for authentication. With SSH Key Manager you can import and export keys, verify fingerprints, approve a new public key when the host key changes and delete keys.



Each private key entry stores the private and public key, a user name, an optional comment, an optional command that can be used for a test connection (e.g. "uname" UNIX command), and one or more **host[:port]/agent** lines that specify which servers this username and private key can be used with.
For example

#17.16.212.174/HostMonitor	a line starting with # will be ignored by the software, such lines can be used as comment or you can use # to temporarily disable an item
17.16.212.190/agent5	this line means that the private key can be used for host 17.16.212.190 if the host is verified by RMA agent named agent5
17.16.212.190:2002/agent6	the key can be used for host 17.16.212.190 only if the SSH server uses port 2002 and the test is performed by RMA named agent6
1.1.21.1-1.1.21.90:22/HostMonitor	the key can be used for any host in the IP address range 1.1.21.1-1.1.21.90 but only if the SSH server uses port 22 and the test is performed by HostMonitor itself
mailserver1.dom.com/HostMonitor	the key can be used for mailserver1.dom.com when the test is performed by HostMonitor
*:2222/Factory5	the key can be used for any SSH server on port 2222 checked by RMA agent named Factory5
10.10.1.1-10.10.1.254/ANY	the key can be used for any host in the IP range 10.10.1.1-10.10.1.254 when the test is performed by any RMA agent or HostMonitor
10.10.1.1-10.10.1.99/Store100*	the key can be used for any host in the IP range 10.10.1.1-10.10.1.99 if the SSH test is performed by an RMA agent

	whose name starts with Store100, e.g. Store100, Store1001, Store100555

Different types of host records have different priorities.

hostname[:port]/agent IP[:port]/agent	The highest priority 0. HostMonitor initially tries to find a matching host entry in this format
IP1-IP2[:port]/agent	Lower priority 1. HostMonitor then tries to find the entry corresponding to the host by checking entries with a range of IP addresses.
*[:port]/agent	Priority 2
hostname[:port]/agentwildcard* IP[:port]/agentwildcard*	Priority 3
IP1-IP2[:port]/agentwildcard*	Priority 4
hostname[:port]/ANY IP[:port]/ANY	Priority 5
IP1-IP2[:port]/ANY	Priority 6
*[:port]/ANY	Lowest priority 7. These entries will only be checked if the target host/port/agent combination does not match any records with higher priority

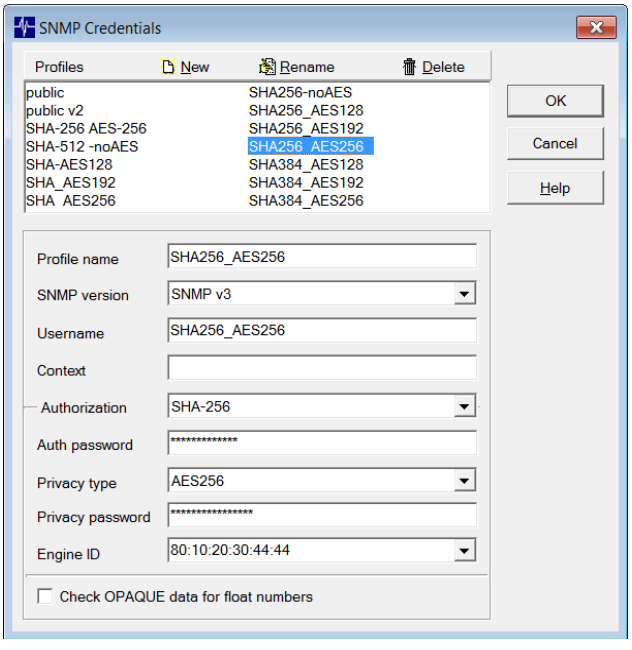
Public keys

HostMonitor and RMA send public keys retrieved from servers to SSH Key Manager. You can also choose the behavior of the software when the host public key changes. SSH Key Manager offers 3 options:

- set Warning status once, automatically approve new key
- don't connect to the host until operator approves new key
- automatically approve new key

If you choose the "don't connect to the host until operator approves new key" option and the host key changes for any reason then HostMonitor/RMA will not perform SSH tests related to the server until you open SSH Key Manager, verify the fingerprint of the new pubic key and confirm that this new key is legitimate (note: new unapproved public keys marked in red).

SNMP Credentials



SNMP Credentials dialog allows you to setup list of SNMP profiles (accounts). Profiles store login or community string and other information necessary for communication with SNMP agent. For each profile you should specify name of the profile (your choice) and version of SNMP protocol used by SNMP agent. HostMonitor supports SNMP v1, v2c and v3.

Community
If SNMP agent uses SNMP v1 or v2c protocol, specify the SNMP community name (often SNMP agents use "public" as community string).

If SNMP agent is configured to use SNMP v3, you should specify the following parameters:

Username
Enter the username that is configured for the SNMP agent(s). An SNMP device, upon reception of a request, uses this username to look for configured authentication and encryption parameters and applies them to the received request message.

Context
Specify the context needed to identify specific SNMP instances. This parameter is optional.

Authorization
You may choose one of the following authorization methods: None (no authorization), MD5, SHA-1, SHA256, SHA384 or SHA512.
Only MD5 and SHA1 algorithms are defined in SNMP standards however many manufacturers use more strong "unofficial" SHA256/384/512 hashes.

Authorization password
If authorization is used, use this field to specify authorization password.

Privacy type
Specify encryption mode: None, DES, 3DES, AES128, AES192, AES256, AES192C, AES256C.
Note1: AES192, AES256, AES192C and AES256C are not defined in SNMP standards however many manufacturers use these algorithms.
Note2: AES192C and AES256C modes used by Cisco, they are equivalent to AES192/AES256 when SHA256, SHA384 or SHA512 authorization mode is used. We would not recommend to use MD5+AES192C/AES256C or SHA1+AES192C/AES256C.

Note3: we do not recommend DES or 3DES encryption mode. DES is not secure. 3DES slower and less secure than AES encryption.

Privacy password
Specify key for encryption

Engine ID
If you need to receive encrypted SNMP Trap messages version 3 using SNMP Trap test items, you should set Engine ID field for some accounts. For example, if you are already using an SNMP account with authentication and privacy settings (algorithms, username, password) to check traffic, fans or CPU usage on your router, then you can set only Engine ID parameter for that account and it will be used by HostMonitor when SNMP Trap test method receives an encrypted trap message from that router.
If a single SNMP account is to be used for multiple SNMP-enabled target devices with the same username and password but different Engine IDs, then you can set "* (any)" as the Engine ID. Accounts with a specific Engine ID take precedence over entries with an Engine ID set to "*".

Check OPAQUE data for float numbers
This option tells HostMonitor to check for single and double precision floating-point numbers that can be encoded as OPAQUE SNMP data and compare such numbers with specified value (number that specified as alert condition for each specific test item)

Profiles

HostMonitor provides set of profiles to make configuration easy and flexible:

Schedules	- used as a time restriction for the test or action execution.
Color schemes	- customizable color palettes for the interface of the program, HTML logs, and reports.
Mail templates	- multiple message templates are used for the e-mail, pager and ICQ notification.
Report profiles	- allows you to create and customize reports in a variety of ways.
Action profiles	- defines set of actions to respond to failed services.

To configure profiles use Profiles menu in HostMonitor's main window.

Schedules

Purpose of schedules: time restriction for a test or an action execution.
For example, if you want to check your server only from Monday to Friday select the "Monday-Friday, 24 hours" schedule in the Test Properties dialog. If you do not specify a schedule for a test, HostMonitor will check the host 24 hours per day, 7 days per week (using the interval specified when you created the test).

Also Schedules can be applied to actions the same way they were used for tests. With schedules, actions can be customized per time of the day. For instance, an action profile can be set up to page both the IT manager and the network administrator during regular office hours, and to page the administrator alone the rest of the time, while doing nothing else but writing to the log at the weekends. To make this possible, simply check the "Time restriction" option in the Action Properties dialog and select an appropriate schedule.

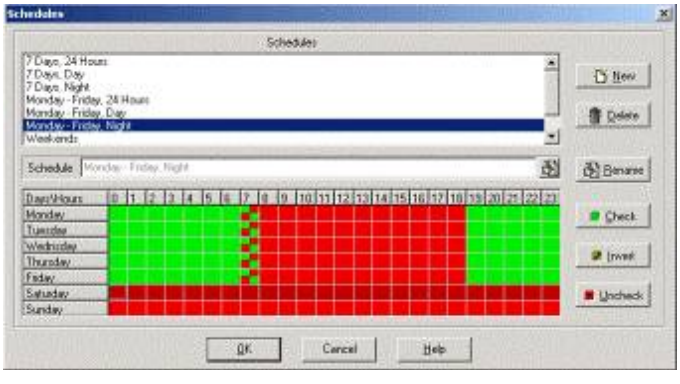
You can create your own schedules and modify standard schedules using Schedules dialog. To bring up this dialog use menu Profiles->Schedules or appropriate buttons in the Test Properties and Action Properties dialogs.

As you can see, editing schedules is very easy. To manipulate with the list of schedules use 4 buttons:

New
Create new schedule

Copy
Make a copy of selected schedule

Rename
Change name of the schedule. You can rename schedules without having to worry that the link between the test and the profile will be broken. To link tests, actions and profiles HostMonitor uses internal IDs that are unique and non-changeable throughout the lifetime of an object.



Delete
Remove selected schedule

Popup menu items provide access to additional options:

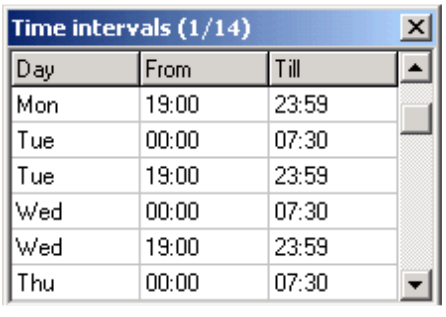
Sort by	Option allows you to sort schedules by name or creation time.
Columns	You may change the number of columns (1,2 or 3) for the list of profiles.
Usage report	Such report tells you what test items and actions use selected schedule.
Mark unused	With this option enabled schedules that are not used by any test item (nor action profile) displayed in grey color.

To edit a schedule, select the time region (using the left mouse button) and click one of the following buttons:

Check	Marks the selected time interval as 'Allowed' for the start of tests and actions (highlighted in green)
Uncheck	Marks the selected time interval as 'Not allowed' for the start of tests and actions (highlighted in red)
Invert	Changes time interval to an opposite ('Allowed' becomes 'Not allowed' and the other way around)

Tune

You may define schedules with up-to-the-minute precision. To use this feature click on "Tune" button or select "Edit intervals" item from popup menu. In a popup window appearing, you will be able to check and modify list of time intervals. To change "From" or "Till" time just type new time, to change day of the week press F2 and select day from drop-down list or type one of the following words to specify day of the week:



- Mon, Tue, Wed, Thu, Fri, Sat, San, Holiday
- type the word 'any'. HostMonitor will replicate time interval for every day of the week (including holidays)
- type the word 'work'. HostMonitor will replicate time interval for Monday-Friday
- type set of day numbers, e.g.'123'(Monday..Wednesday) or '12345678' (Monday-Sunday and Holidays) and so on

To append a new interval to the list go to the last existing line and press Down Arrow button, to insert new line anywhere in the list press INSERT button. To remove line press CTRL+DEL.

Holidays

Also you may specify separate schedules for holidays. The list of holidays is available for modifications for years ahead. Click “Holidays” button and HostMonitor brings up dialog window with the one year calendar that has all holidays marked by red background. To mark or unmark any day as a holiday select a day and press Space key. To see/modify holidays for another year, select a year using “up-down” control at the bottom of dialog. Use “Clear All” button to clear the list of holidays (holidays for current, all past and future years will be unmarked).

Color palettes

You can use fully customizable color schemes for the program's interface, for HTML log files and HTML reports. For different folders and reports you can use different color palettes. For example, a report designed for the IT manager might have an entirely different look and feel as compared to the one intended for use by the network administrator. Similarly, reports designed for the field offices may differ in palette from those used by the headquarters

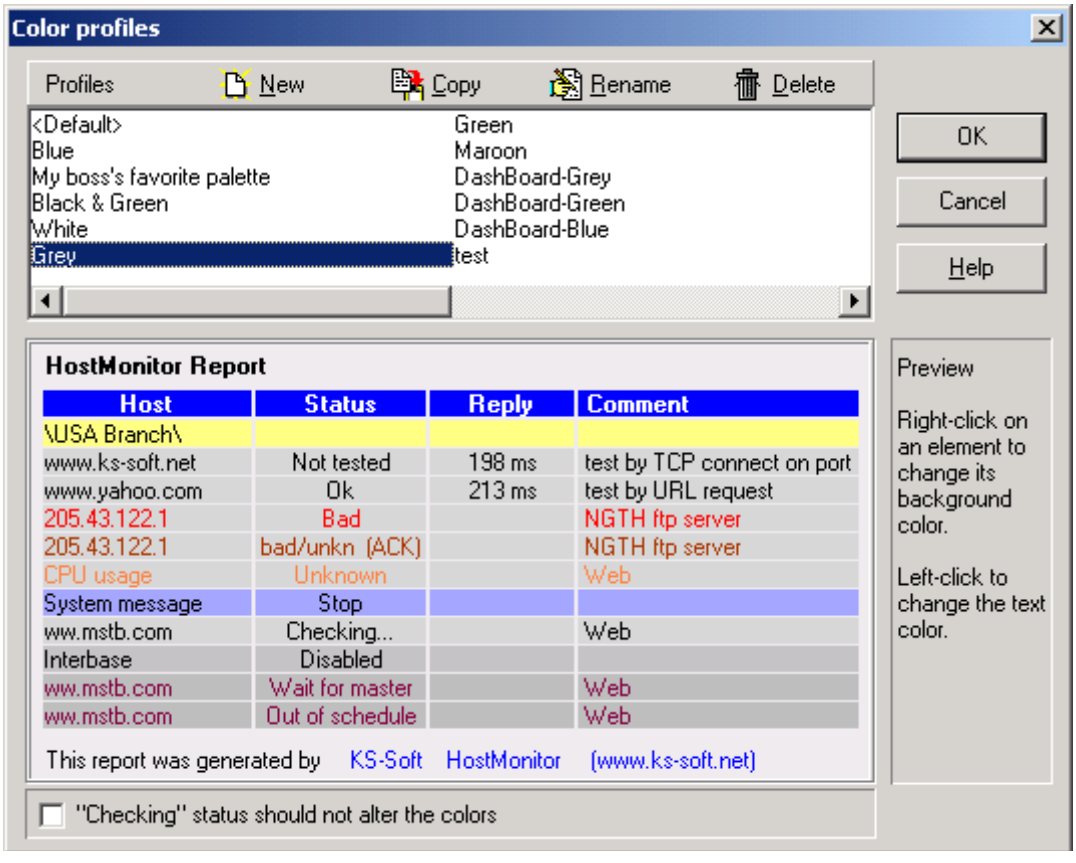
The following elements have customizable color attributes (you can change both fore- and background colors):

- underlying layer;
- table header (HTML reports/logs only);
- folders;
- system messages (HTML logs only);
- HTML links (HTML reports/logs only);
- test colors are status-dependent, so you can use different colors to display tests with different statuses:
  - "Not tested";
  - "Good" items;
  - "Bad" items;
  - "Unknown" tests;
  - "Warning" test items;
  - Acknowledged "Bad", Unknown" or "Warning" test items;
  - "Checking..." items (when "Checking status should not alter the colors" option is disabled);
  - "Disabled" tests;
  - "Waiting for master";
  - "Out of schedule" test items.

If you plan to use palette for **SLA reports with charts**, set profile name starting with "SLA " or "SLA-" (case insensitive, e.g. "Sla Blue palette", "SLA-White"). In such case HostMonitor will show special sample.

To choose a palette that will be used in the program's interface, use Interface page in the User Preferences dialog; you can select the palette for HTML logs on the HTML Colors page in the Options dialog; use Report Manager to choose color schemes for HTML reports.

Color schemes are created and edited in the Color Profiles dialog:



To manipulate with color schemes use the following options:

New Create new palette.

Copy Copy selected palette. This is useful if you want to make small modifications for the existing color palette.

Rename Change palette's name. You can rename palettes without having to worry that the program will lose the link to the palette; HostMonitor uses internal IDs that are unique and non-changeable throughout the lifetime of an object.

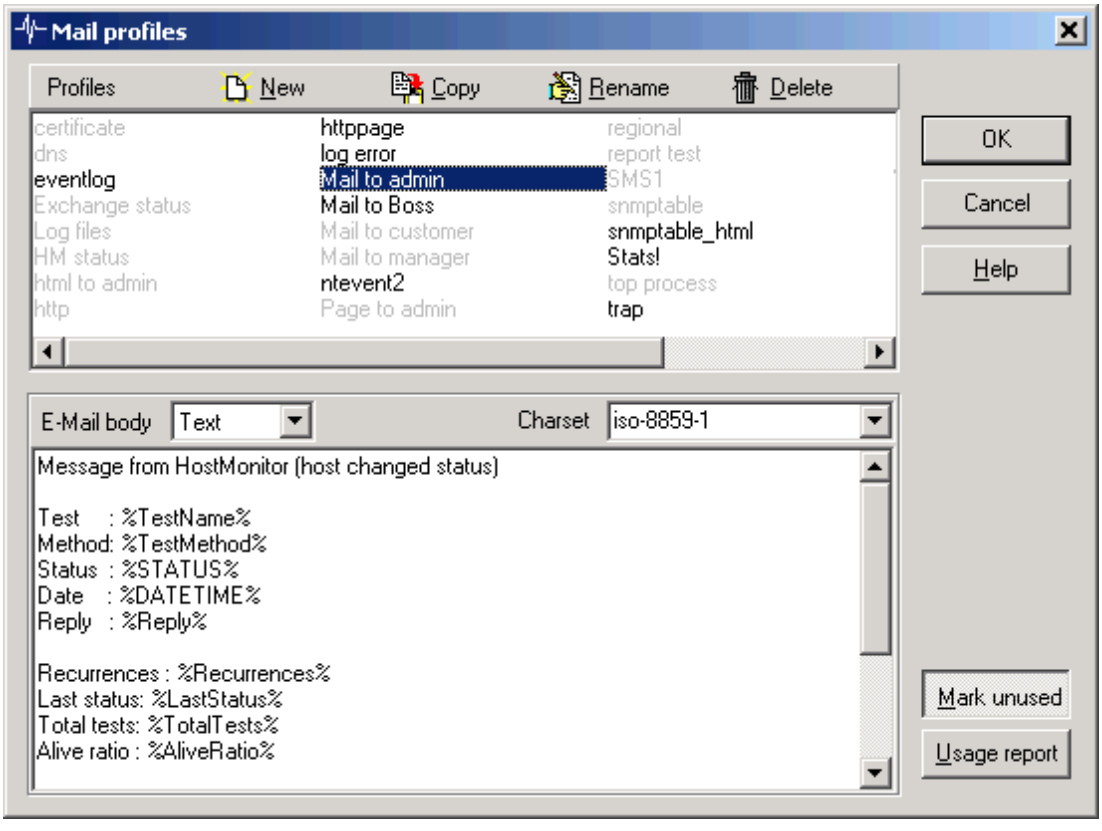
Delete Remove selected palette (you can remove any color scheme except 1st one 'default')

Note: “Sort by” popup menu allows you to sort profiles by name or creation time. “Columns” popup menu allows the changing of the number of columns (1,2 or 3) for the list of profiles.

To change the color for the selected palette, click mouse on an element that you want to change color for. Use right-click on an element to change its background color, and left-click to change the text color.

Mail templates

Multiple message templates can be created for the e-mail, pager and ICQ notification. For instance, you can set up HostMonitor to send general server status emails to the manager, and fire off an elaborate problem report to the administrator in case of a network failure.



Macro variables are supported in message templates to be substituted with their actual values at the message generation time. This way you may use single template for thousands of test items.

If template is used for "Send e-mail" action, you may use special directive like <<IncludeFile=path_to_the_file>> (e.g. <<IncludeFile=c:\HostMonitor\template1.htm>> or <<IncludeFile=%CommentLine3%>>). When HostMonitor detects such directive, it inserts content of the file into mail and then resolves macro variables (it means you may use macro variables in external file as well).
Note: normally size of the file should not exceed 48K however you may tell HostMonitor to include just top of the file, from line 1 to line N. E.g. if you add EMailIncludeNLines=15 line into [Misc] section of hostmon.ini file, then HostMonitor will include up to 15 lines from top of the file into e-mail body (maximum 256 lines).

For each mail template you may choose content type: Text or HTML. If you choose HTML, HostMonitor will resolve test related macro variables according to HTML encoding rules. For example test name "<local comp>" will be translated to "<local comp>". User defined variables and folder related variables are substituted as it is. This allows you to use folder comments and user defined macro variables to store certain elements of HTML code (can be used as styles).

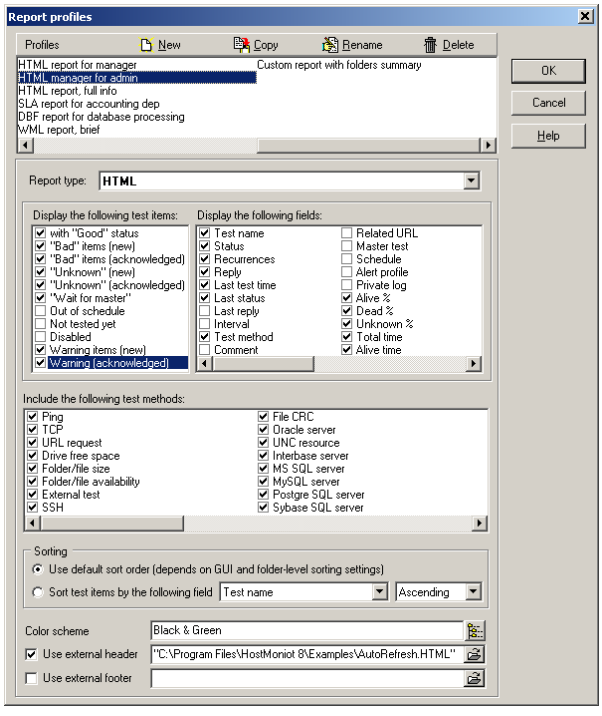
Also you can specify a particular character set for your templates. This comes in especially handy if you work in a multilingual environment.

Commands:

New	Create new template.
Copy	Copy selected template. This is useful if you want to make small modifications for the existing template.
Rename	Change name of the template. You can rename mail templates without having to worry that the program will lost the link to the template; HostMonitor uses internal IDs that are unique and non-changeable throughout the lifetime of an object.
Delete	Remove selected template.
Usage report	Such reports tell you which action profiles use selected mail template
Mark unused	With this option enabled templates that are not used by any action profile will be displayed in grey color.

Note: “Sort by” popup menu allows you to sort profiles by name or creation time. “Columns” popup menu allows the changing of the number of columns (1,2 or 3) for the list of profiles.

Report manager



HostMonitor can generate reports at regular intervals and/or when some tests change their status. It is also worth noting that each folder may contain its own list of reports, and each of the reports can be set up with a launching schedule specific to that folder. Also reports can be generated at user request at any time through the Reports menu in HostMonitor's main window. Reports can be in either HTML, DBF, WML, or Text formats. With reports, you can easily check the status of your network from anywhere using a Web browser or your WAP cell phone. Example
For more information how to use reports please, refer to "Logs&Reports" section of this documetation.

The highly flexible Report Manager allows you to create and customize reports to your preferences in a variety of ways.

The configurable report parameters include:

Report type
Choose one of the available report types:

- HTML — HTML file format. Test items will be represented in the table, each test item will be recorded as one row in the table.
- WML — WML (Wireless Markup Language) file format
- DBF — DBF (Data Base File) format
- Text — Text file
- Dashboard — HTML file format. Every folder is represented by a row in the table. Each cell of the row represents tests of a certain type from within that folder (e.g. Ping, CPU Load, Service, Drive Free Space).
- Compact HTML — HTML file format. Each test will be represented by small button. You will be able to click mouse on those buttons to retrieve detailed information about the test.
- Custom HTML — HTML file format. HostMonitor will use HTML templates provided by you to create report.
- SLA — SLA reports in HTML or XML format

All reports have some common properties:

Test method filter
"Include the following test methods" list allows you to select the test types that should be included in the report (e. g., you may select all test methods except Ping and CPU Usage tests). Click the mouse button on the check box next to a field name to mark/unmark the item. Use "Mark all" popup menu item to select all available fields, use "Clear all" popup menu item to deselect all items.
To exclude some specified tests from the report use "Exclude from reports" test property (located in Test Properties dialog).

Sorting mode
You may setup HostMonitor to sort test items in the report in the same way it sorts test items on screen (this option is selected by default). So, test items will be sorted in the order specified on Columns page in the Options dialog, unless the folder overrides global options and uses its own sorting mode (e.g. different folders may use the same set of report profiles but different sort orders).
Or you may directly specify sort method for the report profile. In such case test items will be sorted by specified field regardless of global and folder-level options.

The following properties are applicable for any report except DBF, WML and Text reports:

Color scheme
Use this option to choose a color scheme you like from a drop down list, or use button to bring up Color Palettes dialog and create the color scheme to your personal preferences.

External Header
Specify an HTML file that will be used as a header for the report. You need to specify this option only if you want to change the standard header of the report. In HostMonitor's directory "Examples\" you can find several examples of the external header:

File	Target report type	Purpose
AutoRefresh.html	HTML	file contains command to auto refresh HTML page. Your browser will be refreshing the page's contents at regular intervals (by default 60 seconds, but you can change the interval).
Summary.html	HTML	external header with test statuses summary.
StdHeader.html	HTML	this external header is similar to the one that HostMonitor is using, can be used as a base for the creation of your own headers.
CompactHeader.html	Compact HTML	this external header is similar to the one that HostMonitor is using for Compact HTML reports, can be used as a base for the creation of your own headers.
DbHeader.html	Dashboard	this external header is similar to the one that HostMonitor is using for Dashboard reports, can be used as a base for the creation of your own headers.

Use macro variables to show current date, time, colors of selected palette, etc.

External footer
Specify an HTML file that will be used as a footer for the report. You need to specify this option only if you want to change the standard footer of the report. HostMonitor's directory "Examples\" contains 2 samples of the footer:
StdHeader.html - this external footer is similar to the one that HostMonitor is using, can be used as a base for creating your own footers.
Summary2.html – contains external footer with tests' statuses summary
Use macro variables to show current date, time, colors of selected palette, etc.

To manipulate with profiles use 4 buttons:

New	Create new report profile.
Copy	Copy selected profile. This is useful if you want to make small modifications for the existing profile.
Rename	Change profile's name. You can rename profiles without having to worry that the program will loose the link to the profile; HostMonitor uses internal IDs that are unique and non-changeable throughout the lifetime of an object.
Delete	Remove selected profile.

Popup menu items provide access to additional options:

Sort by	Option allows you to sort profiles by name, report type or creation time
Columns	Use this option to change the number of columns (1,2 or 3) for the list of profiles.
Usage report	This option shows usage report for selected profile. Such report tells you what folders (within loaded HML file) use selected report profile.
Mark unused	With this option enabled profiles that are not used by any folder (within current HML file) will be displayed in grey color. Note: this option does not check if report profile is used by some external HM Scripts

Other reports have some unique properties.

"Simple" HTML, WML, DBF, TXT reports

These reports show simple list of tests (table) and test properties. You may define the following properties for each report:

Status filter
Use left listbox to select the status set. To create the report HostMonitor will use tests with the selected statuses only (e. g., include tests with a "No answer" or "Unknown" status only). Click mouse button on the check box next to a field name to mark/unmark the item. Use "Mark all" popup menu item to select all available fields, use "Clear all" popup menu item to deselect all items.
To exclude some specific test items from the report use "Exclude from reports" test property (located in Test Properties dialog).

Fields list
The right listbox in the Report Profiles dialog contains list of fields that you can include in the report (e. g., test name, status, average response time, downtime, comment, related URL, etc.). Click mouse button on the check box next to a field name to mark/unmark the item. Use "Mark all" popup menu item to select all available fields, use "Clear all" popup menu item to deselect all items.
You can change fields order in the report by dragging items with a mouse (click left mouse button on the item and drag it to a new place). Also you can change the name of the field, using Columns page in the User Preferences dialog (use <Default> profile for such operation!).

Dashboard reports

Dashboard is actually an indicator panel. One glance at the dashboard will give you comprehensive overview of all tests in all folders.
Every folder is represented by a row on the dashboard. Each cell of the row represents tests of a certain type from within that folder (e.g. Ping, CPU Load, Service, Drive Free Space). Number inside cell and their color depend on the tests results:

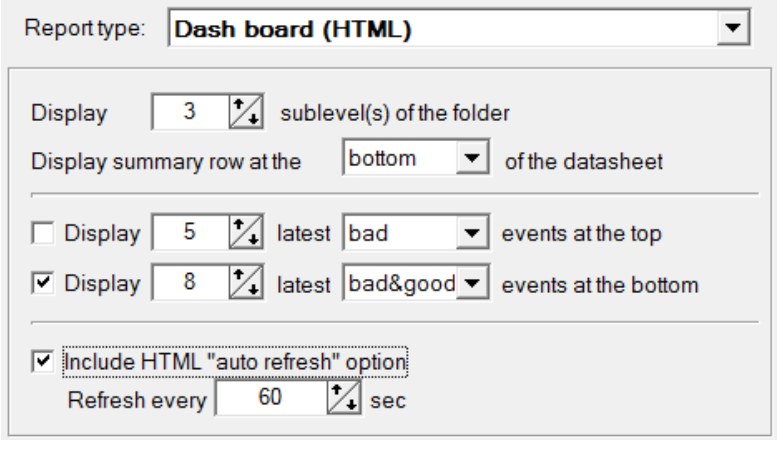
Color*	Meaning of the color of the cell	Meaning of the number in the cell
N	Some test(s) have "bad" status (non-acknowledged)	Number of "bad" test items
N	No "bad" tests but some test(s) have "warning" status (non-acknowledged)	Number of "warning" tests
N	No "bad" or "warning" tests but some test(s) have "unknown" status (non-acknowledged)	Number of "unknown" tests
N	There are some "bad", "warning" or "unknown" items, all of them acknowledged	Number of acknowledged tests
N	No "bad"/"unknown" tests but there are "WaitForMaster" test(s)	Number of tests with "Wait.." status

N	ALL tests are disabled	Number of disabled tests
N	All tests have “OutOfSchedule” status	Number of “OutOfSchedule” tests
N	No “bad”/”unknown”/”wait” items, some (all) tests are “good”	Number of “good” test items
0	No tests of this type in the folder	0 – no tests

* Of course colors used for report depend on color palette you have chosen.

Click on the cell to see the list of tests of specific method (Ping, Process, etc) that have "bad", "unknown", or "WaitForMaster" status (from the specific folder of course). Report may display up to 10 test items of each status. E.g. if you click on "red" cell that represents Ping tests for "USA Office" folder, you will see "bad" (as well as "unknown" and "waitformaster", if any) ping tests within that folder.

Dashboard report has a few more parameters (than regular HTML report):



Display N sublevel(s) of the folder
This parameter defines how many sublevels of the folder tree will be displayed.
For example if you create report for the root folder with "Display 2 sublevel(s) of the folder" option, HostMonitor will create a table that displays tests of the root folder, it's direct descendants (1st sublevel) and descendants of root descendants (2nd sublevel). If the folder tree contains more levels of subfolders, information about test items from deeper subfolders will be included in the last displayed level of subfolders.

Display summary row at the top/bottom of the datasheet
Choose where the summary row will be displayed

Display N latest "bad" / "good" / "bad&good" / "any" events at the top
Display N latest "bad" / "good" / "bad&good" / "any" events at the bottom
These optional settings allow placing information about latest events of specified kind at the top and/or at the bottom of the report. You may choose what kind of events will be displayed. E.g. "bad" event records provide information about failed tests; "good" events provide information about recovered items, and so on.

The term "event" means a log record that was added with every test status change. If logging mode for some test is set to "Reply" or "Full", HostMonitor adds new record when either the test status or "Reply" field value the test changes.

Include "AutoRefresh" option
With this option enabled report will include command for web browser to refresh the page every N sec.

If you want to create a customized external header for Dashboard report, please note:

- HTML header must contain list of styles for the table header, folder items and for each possible test status

```
<style type="text/css">
 td.Header1          { ..style definition.. }
 td.Header           { ..style definition.. }
 td.Folder           { ..style definition.. }
 td.NotTested        { ..style definition.. }
 td.Ok               { ..style definition.. }
 td.Bad              { ..style definition.. }
 td.ClassWarn        { ..style definition.. }
 td.Unknown          { ..style definition.. }
 td.ClassACK         { ..style definition.. }
 td.Disabled         { ..style definition.. }
 td.WaitForMaster    { ..style definition.. }
 td.OutOfSchedule    { ..style definition.. }
 td.NoTests          { ..style definition.. }
 td.BadLog           { ..style definition.. }
 td.OkLog            { ..style definition.. }
</style>
```

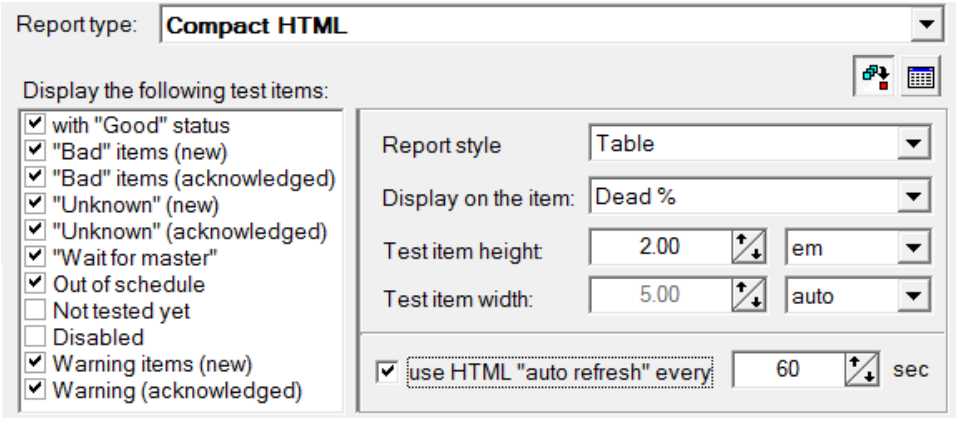
- Header should contain "showinfo" function, called every time user clicks on an element and shows the list of test items. E.g.

```
<script language="JavaScript"> <!--
function showinfo(info) { alert(info); }
--> </script>
```

You may find the example of the header for Dashboard report in "Examples\" directory. File dbHeader.html

Compact HTML reports

Compact HTML report useful when you monitor hundreds or thousands of servers. Each test in the report will be represented by rectangle element.
Compact HTML Report has a few more parameters:



Display the following test items
This list allows you to explude tests with some specific status, e.g. “Out of schedule” or “Disabled” test items. Click mouse button on the check box next to a field name to mark/unmark the item. Use "Mark all" popup menu item to select all available fields, use "Clear all" popup menu item to deselect all items.
To exclude some specified tests from the report use "Exclude from reports" test property (located in Test Properties dialog).

Report mode
Choose one of the following options:

- Group tests by folders
- Table
- All tests in one block

Note: report header may show name, status and reply value of the current element (element near mouse pointer). You may click on any element in order to check detailed information about the test; you may close popup window with details using ESC key or click on Ok button or click on window header

Display on each item
Select what information HM should display on each button. You can select any field (like "Test name", "Status", "Reply", "Comment", etc), or choose "<nothing>" to display items without any text.

Size of test item
Specify width and height of the elements using standard CSS units (px, pt, in, em, ch, etc) or set auto mode, in this case size of the elements will depend on content

Include "AutoRefresh" option
With this option enabled report will include command for web browser to refresh the page every N sec.

Fields button
Set list of fields displayed by popup window (this window displayed when you click on the element), e.g. test name, status, reply value, previous status, schedule, alert profile, comments and much more. You can re-order fields by dragging and dropping items

When you create external header for Compact HTML report please note:

- header must contain list of styles for the folder items and each possible test status

```
<style type="text/css">
 input.Folder          { ..style definition.. }
  input.NotTested      { ..style definition.. }
  input.Alive          { ..style definition.. }
  input.Ok             { ..style definition.. }
  input.Normal         { ..style definition.. }
  input.Bad            { ..style definition.. }
  input.NoAnswer       { ..style definition.. }
  input.BadContents    { ..style definition.. }
  input.Warning        { ..style definition.. }
  input.Unknown        { ..style definition.. }
  input.UnknownHost    { ..style definition.. }
  input.Checking       { ..style definition.. }
  input.Resolving      { ..style definition.. }
  input.ACK            { ..style definition.. }
  input.Disabled       { ..style definition.. }
  input.WaitForMaster  { ..style definition.. }
  input.OutOfSchedule  { ..style definition.. }
</style>
```

- in order to display detailed test information header should contain 2 functions:
  "showHint" called when the mouse pointer is moved onto an element
  "showInfo" called every time user clicks on an element

Custom HTML reports

Custom HTML report is the most flexible report type. However it takes more time on your part to configure the report profile. HTML and Compact HTML reports allow you to change header and footer of the reports, custom HTML report allows you to change everything. Define your own HTML template using special macro variables and HostMonitor will generate HTML report using parameters of the tests and folders instead of macro variables.

Each section (header, summary, gap, etc) allows you to use following macro variables:

- Regular macro variables (the same varaibles those used for external header/footer for regular HTML report);
- User defined variables
- Date & time variables

Header
Specify header of the report, this template will be used once for the report.

Folder title
Provide HTML code that will be used to display Folders. Here you may use Folder Specific macro variables (in addition to regular, user defined and date variables).
If you do not want to display folders in the report, leave "Folder title" field empty.

Test items
Provide HTML code for each test status. You can use regular macro variables plus macro variables those represent test parameters (e.g. %TestName%, %Status%, %Reply%, %MinReply%, %MaxReply%, etc). Full list of test specific macro variables available here

Folder summary
Provide HTML code that will be used to display summary information about each Folder. Here you may use Folder Specific macro variables (in addition to regular, user defined and date variables).
If you do not want to display any summary information, keep "Folder summary" field empty.

Gap between folders
Provide HTML code that will be inserted between last test item (from current folder) and next folder. In other words this code will be used before each folder item except 1st one.

Footer
Specify footer of the report, this template will be used once for the report.

SLA Reports

When "Store historical data in the file" option (located in "Test list properties" dialog) is enabled, HostMonitor collects additional statistical information for each test item. Such information can be displayed by SLA reports, "Test history" window, Web Service interface, etc.

You may setup HostMonitor to generate SLA reports using XML or HTML file formats. HTML SLA report can be created in forms of text table or list of charts.
Examples:
- Table report 1
- Table report 2
- Performance charts
- Availability charts
- Availability prediction

SLA report profiles provide additional properties:

Mode
Select file type for the report: XML or HTML

Chart
When you setup HTML SLA report, you may setup report without charts or choose one of several types of charts:
- Availability
- Performance
- Availability + average reply

Folder summary
With this option enabled HostMonitor will calculate average alive/dead ratio and average reply values for each folder included into the report; folder summary information is based on each test item within the folder.

Show folder comment
With this option enabled HostMonitor will display comments assigned to each folder included into the report. You may specify number of specific line of the comment (as folder comment is multy-line text).

Show test comment
With this option enabled HostMonitor will display comments assigned to each test item included into the report. You may specify number of specific line of the comment (as test item comment is multy-line text).

Include disabled items
This option tells HostMonitor to include or exclude currently disabled items into the report

Consider items as bad when

HostMonitor may mark report items (tests, folders and summary items) as "bad item" using color specified for "bad" items by selected color palette. With this option enabled you may specify when item should be considered as "bad" item. You may select one of the following parameters to be checked and compared with the number (e.g. "max reply > than 1000" or "average reply < 20").

- "dead" ratio
- "alive" ratio
- min reply
- max reply
- average reply

Display statistics for

Each SLA report (each file) may include set of "sub-reports" – information regarding specific period of time:

- Prediction: next 7 days
- Today
- Yesterday
- Last 24 hours
- Last 48 hours
- This week
- Last week
- Last 7 days
- Last 14 days
- This month
- Last month
- Last 30 days
- Last 60 days
- This year
- Last year
- Last 12 months
- Last 24 months

"Prediction: next 7 days" mode tells HostMonitor to calculate and show statistical counters for future 7 days. HostMonitor analyzes previous 30 days of test results trying to predict future test results. HostMonitor shows counters (textual information) for next 7 days while charts show data for last 7 days and next 7 days (using different color for past and the future). Of course software cannot tell you what really happens in the future, its just assumption based on historical data.

Important note: If you have a lot of test items, we would recommend to generate HTML SLA reports with charts using built-in Scheduler (e.g. start "Generate reports" action once a day). We do not recommend using "Generate reports" action (for reports with charts) in action profile assigned to some frequently performed test items. That's because generation of thousand charts can take significant time.

Macros

"Regular" macro variables
Below there is a list of the macro variables those can be used in an external header/footer for the HTML, Compact HTML, and Custom HTML reports:

Variable	Description
%Date%	current date
%Time%	current time
%DateTime%	current date & time
%TimeZone%	time zone information (note: you may specify different regional settings on per-folder basis)
%BGColor%	background color
%TextColor%	text color
%LinkColor%	hypertext link color
%VLinkColor%	visited link color
%ALinkColor%	active link color
%TotalTests%	number of tests in the report
%GoodTests%	number of tests with "Good" status
%BadTests%	number of tests with "Bad" status
%UnknownTests%	number of tests with "Unknown" status
%WarningTests%	number of tests with "Warning" status
%AckBadTests%	number of "Bad" acknowledged test items
%AckUnknTests%	number of "Unknown" acknowledged test items
%AckWarningTests%	number of "Warning" acknowledged test items
%DisabledTests%	number of disabled tests
%WaitForMasterTests%	number of tests with "Wait for master" status
%OutOfScheduleTests%	number of tests with "Out of schedule" status

"Folder specific" macro variables
Below is a list of the macro variables those can be used in "Folder title" and "Folder summary" sections of the Custom HTML report:

Variable	Description
%Folder%	Represents the name of the folder
%FullPath%	Displays full path to the folder (like Root\Main Office\Web server)
%FolderAverage_AliveTime%	The average value of the AliveTime counter over all test items within the folder. AliveTime counter represents overall time the test has had a "Good" status
%FolderAverage_DeadTime%	The average value of the DeadTime counter over all test items within the folder. DeadTime counter represents overall time the test has had

	a "Bad" status
%FolderAverage_UnknownTime%	The average value of the UnknownTime counter over all test items within the folder. UnknownTime counter represents overall time the test has had a "Unknown" status
%FolderAverage_AliveRatio%	The average ratio AliveTime to TotalTime, in percent (over all test items within the folder)
%FolderAverage_DeadRatio%	The average ratio DeadTime to TotalTime, in percent (over all test items within the folder)
%FolderAverage_UnknownRatio%	The average ratio UnknownTime to TotalTime, in percent (over all test items within the folder)
%FolderAverage_PassedTests%	The average number of passed probes over all test items within the folder (for all test items in the folder)
%FolderAverage_FailedTests%	The average number of failed probes over all test items within the folder (for all test items in the folder)
%FolderAverage_UnknownTests%	The average number of probes finished with “Unknown” status, over all test items within the folder (for all test items in the folder)
%FolderMin_MinReply%	The minimum value of the results obtained (over all test items within the folder)
%FolderMax_MaxReply%	The maximum value of the results obtained (over all test items within the folder)
%FolderAverage_AverageReply%	The average value of the results obtained (over all test items within the folder)
%FolderAverage_MinReply%	The average value of the MinReply counter over all test items within the folder. MinReply counter represents the minimum value of the results obtained by test item.
%FolderAverage_MaxReply%	The average value of the MaxReply counter over all test items within the folder. MaxReply counter represents the maximum value of the results obtained by test item.
%FolderTotal_PassedTests%	Total number of passed probes for all test items in the folder
%FolderTotal_FailedTests%	Total number of failed probes for all test items in the folder
%FolderTotal_UnknownTests%	Total number of probes finished with “Unknown” status, for all test items in the folder
%FolderCurrent_TotalTests%	Number of the test items in the folder (not

	counting tests you have decided not to include into the report, e.g. disabled tests)
%FolderCurrent_GoodTests%	Number of the test items (in the folder) those have “Good” status at the report generation time
%FolderCurrent_BadTests%	Number of the test items (in the folder) those have “Bad” status at the report generation time
%FolderCurrent_UnknownTests%	Number of the test items (in the folder) those have “Unknown” status at the report generation time
%FolderCurrent_WarningTests%	Number of the test items (in the folder) those have “Warning” status at the report generation time
%FolderCurrent_AcknowledgedBad%	Number of "Bad" acknowledged test items in the folder
%FolderCurrent_AcknowledgedUnknown%	Number of "Unknown" acknowledged test items in the folder
%FolderCurrent_AcknowledgedWarning%	Number of "Warning" acknowledged test items in the folder

Also in any section (header, footer, test items, etc) of the Custom HTML report you can use 2 contents specific macro variables:

- %ItemColor% - text color
- %Background% - background color

These varaibales are "contents specific" because value of the varaible depends on the item that uses variables. E.g. if you use these variables in "Folder title" section, they will represent colors which were specified for the folder item (see Color Schemes dialog). If you use these variables for "Good" tests, they will represent colors which were specified for tests with "Good" status. And so on...

Actions & Action profiles

HostMonitor provides different ways (30 methods!) to respond to failed services. Audio and visual notifications can alert people near the machine. E-mail and pager notifications can be used to inform a wider range of remote operators. Some of the actions HostMonitor can take will try to recover from a failure automatically without human intervention.

Each test can be set up with an individual action profile, and each action profile may contain a number of alert actions that can be launched in a predefined order depending on the test results. Action can be launched by HostMonitor or RMA.
Here is a list of available actions to kick off in response to a problem:

- Show message
- Play sound
- Hangouts chat
- Microsoft Teams
- Telegram message
- Slack message
- Viber message
- Jabber message
- ICQ message

- Send e-mail
- Send message to alphanumeric pager (TAP protocol)
- Send message to alphanumeric pager (SNPP protocol)
- Send message to numeric pager
- Send SMS (GSM)
- Send SMS (SMPP/IP)

- Stop service
- Start service
- Restart service
- Remote reboot
- Local reboot
- Execute external program
- Start program remotely
- Kill process

- Record HM log
- Generate reports
- Log Event
- SQL Query
- HTTP request

- Send data to TCP/UDP port

- Syslog
- SNMP Set
- SNMP Trap

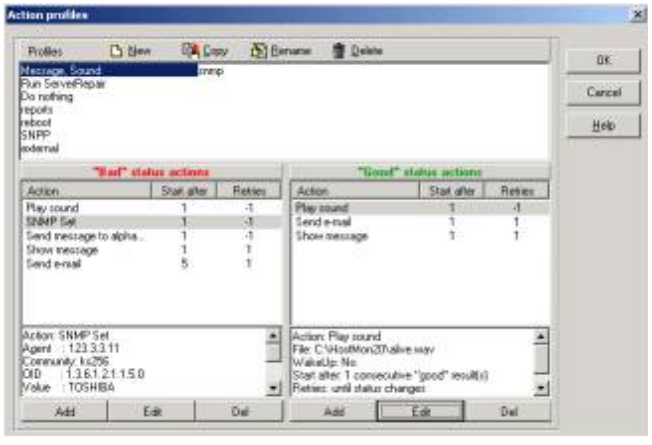
- Dial-up to network
- Disconnect dial-up connection

- Repeat test
- Change test interval
- Execute HMS script

Note: in most cases single alert profile is enough for test item because each alert profile may contain several actions with different starting conditions, different time restriction options; also you may use “advanced mode” actions.
However in some cases you may reduce number of necessary alert profiles by using 2 alert profiles per test item. If you enable "Allow 2nd alert profile for test items" option (located on Preferences page in HostMonitor Options dialog), you will be able to assign 1 or 2 alert profiles for each test item.

Action Profiles

To work with action profiles you can use the Action Profiles dialog. To bring up this dialog use menu Profiles->Action profiles in HostMonitor's main window or appropriate buttons in the Test Properties dialogs.



In the upper part of the dialog you can see a list of Action Profiles and buttons (New, Copy, Rename, Delete) that allow you to modify this list. Each of the Action Profile has 2 sets of actions: «Bad» actions and «Good» actions. The sets of actions and buttons for modifying these actions (Add/Edit/Del) you can find in the lower part of the dialog.

You have to understand difference between actions profile and actions: each test has link to one (only one) of the action profiles, and each of the action profiles may contain a number of actions that can be launched in a predefined order depending on the test results.

Assume action profile has been assigned to the test. In this case every time after test is done and log file was updated HostMonitor performs actions that are assigned in the related list: it uses list of "Good" actions if test has "Good" status, and uses list of "Bad" actions if test has "Bad" status. To determine which actions from the list should be executed and which should not, HostMonitor uses 3 properties that each "standard" action has:

- Start when [N] consecutive Bad/Good results occur - this parameter determines when to execute the action
- Repeat - defines the number of repeats of the action if the status of the test was not changed
- Time restriction - defines time restriction for an action execution

Also "Good" actions have one more property: Action depends on "bad" one. It allows starting "Good" action only if corresponding "Bad" action was executed.

For example you want to monitor some important service. In case the service does not respond you want to send an e-mail message to the network administrator and restart the service. If that does not help, "Reboot remote system" action must be executed. If the functionality of the services is restored, you want to send a message about this happy event to the administrator. To implement this behavior, create an action profile with four actions (3 "Bad" actions and 1 "Good" action):

1. "Bad" action: send e-mail
   Condition to start action: standard mode
   Start when: 1 consecutive "bad" result occur
   Retries: 1

2. "Bad" action: restart service
   Condition to start action: standard mode
   Start when: 1 consecutive "bad" result occur
   Retries: 1
3. "Bad" action: remote reboot
   Condition to start action: standard mode
   Start when: 2 consecutive "bad" results occur
   Retries: 1
4. "Good" action: send e-mail
   Condition to start action: standard mode
   Start when: 1 consecutive "good" result occur
   Retries: 1

In addition to "standard" actions HostMonitor 4+ supports "advanced" actions that allow you to use logical expression as a condition that triggers the alert.

If you do not specify an action profile for a test, HostMonitor will simply perform check and write down a record to the log file (if the logging is enabled). Also you can disable action profiles execution for all tests, to do so mark "Disable alert reactions" option on Behavior page in the Options dialog.

Note: In this terminology, "Bad" status means one of the following:
- "No answer";
- "Bad";
- "Bad contents".

"Warning" test items considered as "bad" if "Treat Warning as Bad" option is enabled
Also for a test with the option "Treat Unknown status as Bad" the following statuses considered as bad:
- "Unknown host"
- "Unknown"

Similarly, "Good" status means either:
- "Host is alive"
- "Ok"

You can modify existing demo profiles or create any number of your own profiles.

To manipulate with the list of profiles use 4 buttons above listbox with profiles list:

New
Create new profile

Copy
Copy selected profile. This command is convenient if you want to use an existing profile and just slightly change it.

Rename
Change profile's name. You can rename profiles without having to worry that the program will lose

the link to an action profile; HostMonitor uses internal IDs that are unique and non-changeable throughout the lifetime of an object.

Delete
Remove selected profile

Popup menu items provide access to additional options:

Sort by	Option allows you to sort profiles by name or creation time.
Columns	Use this option to change the number of columns (1,2 or 3) for the list of profiles.
Usage report	This option shows usage report for selected profile. It tells you where profile is used (test items, HostMonitor scheduler, folders, logging alerts, etc).
Mark unused	If you enable this option, profiles that are not currently in use will be displayed in grey color.

To modify each action profile use buttons located on bottom line of the dialog:
Add
Allow you to add new action into profile
Edit
Bring up Action Properties dialog for editing parameters of the selected action
Delete
Remove selected action

Move up / Move down
When several actions have the same start condition (e.g. start after 2nd consecutive bad result) these popup menu items allow moving actions up and down in the list within the same action profile.
Note: for most actions with the same starting condition changing starting order does not make any difference because HostMonitor executes such actions simultaneously. However for the following actions this makes sense because HostMonitor does not start other actions until one of these actions completed:
- Generate reports
- SQL Query
- Run HM Script

For example, you may setup alert profile that will generate report files and send reports using "Send E-Mail" action.

Copy as good/bad action
This popup menu item allows you to copy actions from "bad" to "good" and from "good" to "bad" sections of the same action profile.

Find & Replace

When you need to change action parameters on regular basis, you may use user defined variables. However in some cases you cannot predict necessary changes, e.g. you need to change path to

some external application because you moved HostMonitor to different system. In this case Find&Replace option can save your time.

Click “Find&Replace” button to open “Find&Replace” dialog window. Then provide search string and the replacement string. To replace the text with nothing, leave 2nd input box blank. Optionally you may mark “Check passwords” field.
Note: HostMonitor checks for possible result strings and does not allow you to make replacement for an item if entire action parameter will be empty after replacement (there are some exceptions: password fields; final packet of “Send data to TCP/UDP port” actions and SNMP Set Value).

When you click “Find” button, HostMonitor will scan action profiles checking for the search string within the following fields:

Action	Parameters
Any “advanced mode” action	Condition to start
Play sound	Path to the file
Hangouts chat	Webhook URL Message text
Microsoft Teams	Webhook URL Message text
Telegram message	Token Chat ID Text
Slack message	Webhook URL Title Message text
Viber message	Token Receiver Text
ICQ message	ICQ # (UIN)
Jabber message	Jabber account
Send message to pager (TAP)	Access number Pager ID Password*
Send message to pager (SNPP)	Pager ID Target server Login Password*
Send message to beeper	Beeper number Message

	Termination string
Send SMS (GSM)	Destination phone number
Send SMS (SMPP/IP)	Destination phone number
Send e-mail (SMTP)	Sender Recipient Subject Path to attachment
Record HM Log	Destination file name
Stop/Start/Restart service	Computer name Service name User name Password*
Remote reboot	Computer name Message to display
Execute external program	Command line Working directory
Start program remotely	Target host Command line Working directory Username Password*
Kill process	Target host Process name Process ID Username Password*
Dial-up to the network	Connection name Username Password*
Disconnect dial-up connection	Connection name
Log Event	Computer name Event log Event source Event description Login Password*
SQL Query	ODBC data source name Login

	Password* SQL Query
HTTP request	Host name HTTP request
Send data to TCP/UDP port	Target server Init packet Final packet
Syslog	Target server Message
SNMP Set	Agent address Community string OID Value
SNMP Trap	Destination address Agent address Community string Enterprise MIB OID
Execute HMS script	Path to HMS script file

Search is case insensitive. E.g. if you search for “admin” then actions with strings “ADMIN@domain.com”, “Admin555”, “333adminhost” will pass thru filter.

*Note: HostMonitor may check and replace passwords used in some action profiles when “Check passwords” option is enabled. But “password search” algorithm is different:
- search for passwords is case SENSITIVE;
- password specified for the action must EXACTLY match the search string (e.g. if you specify “SaTF” search string, password “SaTF5” will not be replaced.

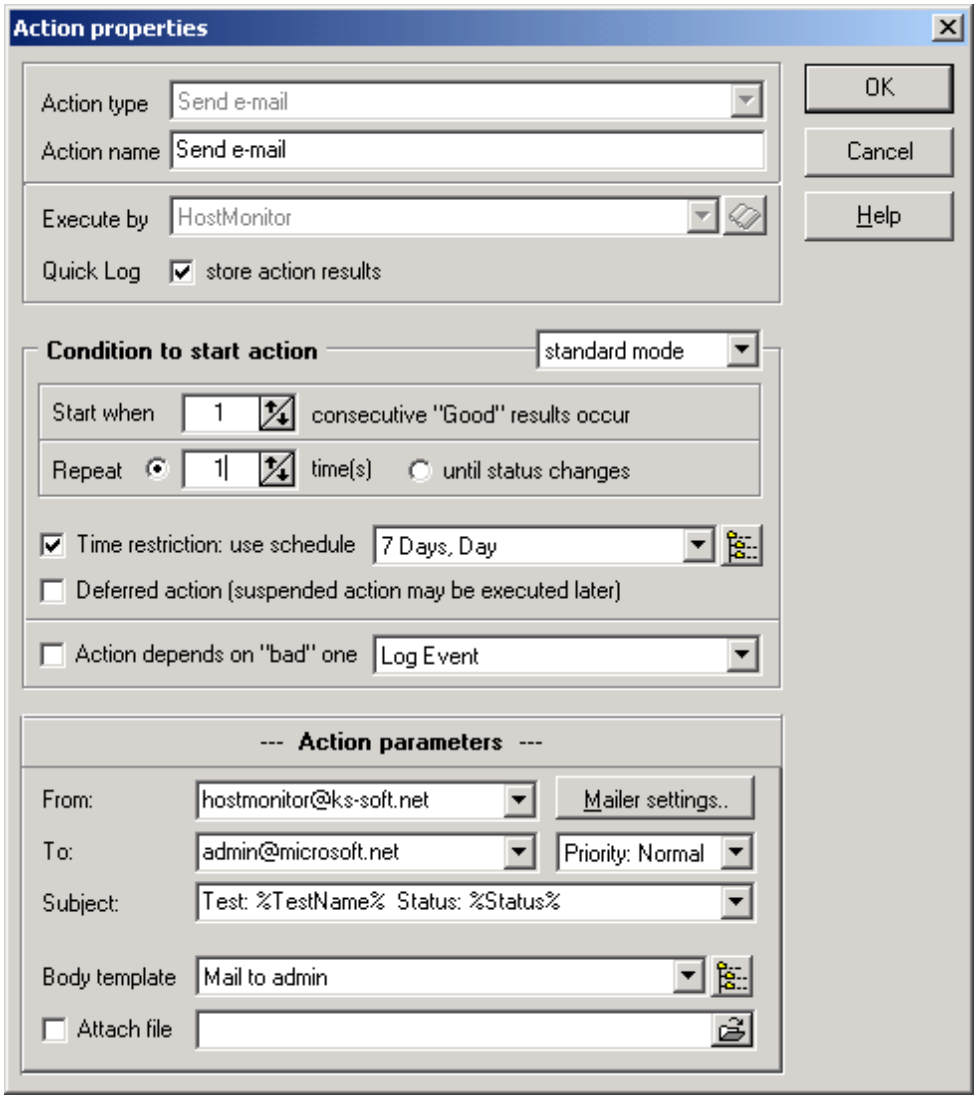
Find&Replace window will display list of action profiles, actions and parameters that contain the search string. Also you will see current value of the field and proposed new value (for each item). If the search string detected within several parameters of the action, or several actions within profile contain the search string, you will see several items in the list.

You may sort items by action profile name, action name, field name, current field value or proposed field value. You may mark all or some items and then use “Replace” button to perform replacement operation. This allows you to make replacement for some specific actions or specific fields. E.g. you may replace “admin@” with “manager@” in “recipient” field but keep “admin@domain.com” in “sender” field.

If you made mistake and wish to cancel all changes, close “Find&Replace” dialog and click “Cancel” button in “Action Profiles” dialog.

Action Properties

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

Execute by
Actions can be performed by HostMonitor or by Remote Monitoring Agent (RMA). "Execute by" option allows you to specify how and where action should be performed. You may select from the list one of the items:

- Test Performer — action will be executed by the same application that had performed the test (test that triggered alert reaction).
  What this means? As you know test can be performed by HostMonitor or RMA. It is a usual situation when some tests performed by HostMonitor, while other tests performed by various agents. Single action profile is assigned to many different tests is usual as well. If some test fails and triggers alert reaction, action with "Test Performer" option specified will be executed by the same module (HostMonitor or RMA) that was specified for test execution. So, if HostMonitor has performed the test, alert action will be executed by HostMonitor as well. If agent has performed the test, action will be executed by the same agent.

- HostMonitor — action will be executed by HostMonitor

- Specific RMA — action will be executed by specific agent. You may select an agent from drop down list or click on a button (to the right of the field) to manage agent list.
  Note: if specified RMA was linked with backup RMA and test was performed by that backup agent then action will be executed by the same backup agent.

Please note: not every action can be performed by agent. E.g. RMA does not support "Send e-mail", "Send message to pager" and some other actions. For more information regarding agent's configuration and functionality, please, refer to RMA section of the manual.

Quick Log: store action results
This option allows you to disable "Quick Log" recording for non-important actions, like "Play sound" action.
Note: this option does not effect "system log" processing; HostMonitor will record action results into system log file depending on options specified on System Log page in the Options dialog

Condition to start action
There are 3 different types of starting condition:

1) **standard mode**
   Standard actions are those actions that are performed by HostMonitor after a test has returned specified result for specified number of times. Following 3 parameters define when action should be executed:

   Start when N consecutive Bad/Good results occur
   This parameter determines when to execute an action. For example you want to send a message to a network administrator's pager after three unsuccessful tests of the web server consecutively, set this parameter to 3. If you want to start action right after the test status was changed, set parameter to 1.

Repeat: N times; or until status changes
Defines the number of repeats of the action if the status of the test was not changed. For example if you want to send an e-mail to a network administrator only once when test status changes, set this parameter to 1. If you need to execute action every time when test failed, set this option to "until status changes".

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 test fails 3 times consecutively (start when 3 consecutive "Bad" results occur), also you defined «Good» action to send a notification when the test status changes to "Good". What will happen if test fails 1 or 2 times and after this it restores "Good" status? HostMonitor will not send a notification about failure (because test did not fail 3 times) 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 HostMonitor will start "Good" action only if corresponding "Bad" action was executed.

Several examples:

Example 1: You want a fresh network stats report to be posted on your intranet web server every time the test finds the server to be up and running. This can be done simply by adding the following "Good" action to the action profile:
Action: Generate reports
Start when: 1 consecutive "good" result occur
Retries: until status changes

Example 2: When some critical service dies, you want the server to automatically reboot. If that does not help, an e-mail should be sent to the on-call technician. If, however, the server remains silent during the next three tests, the network administrator is to be paged until the server is brought back up. To implement this behavior, create an action profile with three "Bad" actions defined like these:
1. Action: remote reboot
   Start when: 1 consecutive "bad" result occur
   Retries: 1
2. Action: send e-mail
   Start when: 2 consecutive "bad" results occur
   Retries: 1
3. Action: send message to pager
   Start when: 5 consecutive "bad" results occur
   Retries: until status changes

2) **advanced mode**
Advanced mode allows you to use logical expression as a condition that triggers the alert action. An alert action is performed when a logical expression of a condition is true. In these expressions you can use:

- numbers and strings (in quotes). Strings that contain a number plus one of the following unit specificators [ms, Kb, Mb, Gb, %] are compared as numbers, so that '900 Kb' is less than '9 Mb'
- macro variables related to the current test or to any other test;
- global macro variables;

- logical operators [and, or, xor, not, <, >, >=, <=, ==, <>];

- arithmetic operators [div, mod, +, -]
  div (integer division)
  mod (remainder)
  + (addition)
  - (subtraction)
  Note: The value of (x div y) is the value of x divided by y and then rounded in the direction of zero to the nearest integer; 'mod' operator returns the remainder obtained by dividing its operands (in other words, (x mod y) == x - (x div y) * y);

- string operators:
  in - expression 'Substr' in 'Str' searches for a sub string "Substr" in a string "Str". Operator returns True when "Str" contains "Substr"; otherwise operator returns False
  getword - expression like ("string" getword N) returns Nth word from text string counting from beginning;
  endword - expression like ("string" endword N) returns Nth word from text string counting from end of the string
  Example:
  ('40 10 50' getword 3) returns 50 (third word)
  ('40 10 50' endword 3) returns 40 (3rd word counting from the end of the string)

- parentheses. In complex expressions, common rules of precedence determine the order in which operations are performed:

Operators	Precedence
not	first (highest)
div, mod	second
+, -, in	third
<, >, >=, <=, ==, <>	fourth
and, or, xor	fifth (lowest)

  An operator with higher precedence is evaluated before an operator with lower precedence, while operators of equal precedence associate to the left. You can use parentheses to override precedence rules. An expression within parentheses is evaluated first and then its result is treated as a single operand.

Advanced mode is more complicated than standard but is very very flexible. Just several simple examples:

- '%SimpleStatus%'<>'UP' - action will be executed every time the test is performed and status of the test is not "good";

- '%Status%'<>'%LastStatus%' - action will be executed every time the test status changes;
- ('%Status%'=='No answer') and ('%LastStatus%'=='Host is alive') - action will be executed when the test status changes from "Host is alive" to "No answer"
- ('%SimpleStatus%'=='DOWN') and (%Recurrences%==5) - action will be executed if the fifth attempt of a test in a row fails
- ('%SimpleStatus%'=='DOWN') and (%Recurrences% mod 3==1) - action will be executed after 1st, 4th, 7th, 10th,, 13th, … consecutive failed test
- ((%Reply%>200) and (%Reply%<800)) or ('::Main Router::%SimpleStatus%'=='DOWN') - action will be executed when "Reply" value of the test is between 200 and 800 or status of the "Main Router" test is "No answer" or "Bad".

Note: When you setup "advanced mode" actions, you may click on button located beside "expression" field. HostMonitor will bring up "Expression editor" dialog that simplifies modification of complicated expressions.

3) on the schedule

Unlike standard and advanced actions that are triggered by events related only to the tests, "scheduled" actions are conformable to the schedule. They also may be triggered by some "global" events (e.g. HostMonitor can start "scheduled" actions when user stops monitoring). There are several places where you can use scheduled actions:

- The Scheduler itself - a tab in the Options dialog allows you to execute up to 5 alert profiles by a schedule. E.g. HostMonitor may execute one profile every 1 hour and execute another profile every Monday at 21:00;
- Reports page in the Options dialog: now HostMonitor can execute alert profile after reports were generated;
- Reports page in the Folder Properties dialog;
- Statistics page in the Folder Properties dialog: HostMonitor can execute alert profile before resetting the statistics;
- Pause dialog: HostMonitor can execute alert profiles every time user starts or stops monitoring or when the user enables/disables alerts.

It is a good idea to create separate action profiles for standard/advanced actions and for scheduled actions.

Time restriction

Schedules can be applied to actions the same way they were used for tests. With schedules, actions can be customized per time of the day. For instance, an action profile can be set up to page both the IT manager and the network administrator during regular office hours, and to page the administrator alone the rest of the time, while doing nothing else but writing to the log on weekends. To make this possible, simply check the "Time restriction" option and select an appropriate schedule.

Deferred action

"Time restriction" option allows you to suppress action execution depending on time of the day and/or day of the week. Additional "Deferred action" option tells HostMonitor to delay action execution if specified schedule does not allow immediate execution of the action. HostMonitor will

execute action at the beginning of “allowed” time frame on condition that status of the test is identical to status that triggered alert (see Note #3).
Note1: If the same test triggers the same action several times within “restricted” time frame, HostMonitor will execute action just once at the beginning of “allowed” time frame.
Note2: When HostMonitor starts deferred (delayed) action, macro variables will be resolved with using of current (up to date) test status, current date and time, current status of HostMonitor, etc.
Note3: HostMonitor considers the following statuses as identical

- Bad, Bad contents, No answer
- Ok, Host is alive, Normal
- Unknown, Unknown host

Also “Warning” status can be considered as identical to “Bad” when “Treat Warning status as Bad” option of the test item is enabled. The same is true for “Unknown” and “Unknown host” statuses when “Treat Unknown status as Bad” option is enabled.

Macros: You may use special macro variables in a command line to execute an external program, in e-mail subject line, in the mail templates, etc. For more information, please, refer to Macros section of this document.

Action methods

Listed below is information about various action types supported by HostMonitor:

Show popup message

Executing this action, HostMonitor will display a popup window with information about state of the test. All settings for this window (position, time to display, etc) may be setup on the "Msg Window" page in the Options dialog.

See also common action parameters

Play sound

This action designed to play a sound file (WAV, MID, etc). In addition to the common action parameters, the «Play sound» 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 repeatedly
With this option enabled HostMonitor will display a popup window with information about the event and will play a sound repeatedly until you click "Stop" button.

Hangouts chat

This action allows to send messages into Google Hangouts Chat.
In addition to common action parameters, the «Hangouts chat» action has the following options:

Webhook URL
This parameter tells HostMonitor where it should to send data. How to create webhook URL: from the chat room menu (Google Hangouts Chat) select [Configure Webhooks]. A dialog appears that lists any incoming webhooks already defined for the room. Click on [Add Webhook], then fill in the name field and optionally the avatar URL field, click [Save], then copy the system-generated URL into HostMonitor action properties window.

Text
Provide text for the message. Macro variable such as %TestName%, %Status%, %Reply%, %RelatedURL% are supported in this field (to be substituted with their actual values at the message generation time).
Also Hangouts Chat lets you add basic formatting to the message text, including bold, italic, and strikethrough. To format text, wrap it with the following symbols:

* **bold**
_ _italic_
~ ~Strikethrough~
` `Monospace`
``` ```Monospace block``` (three backquotes)
If you include a plain link URL in your message text, such as https://google.com/, then google.com will be used as the link text and automatically hyperlinked to https://google.com. To provide alternate link text for your link, use the following syntax:
<https://www.ks-soft.net/hostmon.eng/index.htm|**link text**>

Microsoft Teams

Sends a message to Microsoft Teams channel.
In addition to common action parameters, the «Microsoft Teams» action has the following options:

Webhook URL
HostMonitor 14.70+ supports "office" and "workflows" webhooks (older versions support only "office" webhooks). Microsoft plans to disable "office" webhooks on August 15, 2024. While "workflows" mode requires interactive integration user account within Microsoft Teams with a premium Power Automate license.

How to create "office" Webhook URL:
in your Microsoft Teams app, choose More options (next to the channel name) and then choose Connectors. Scroll through the list of Connectors to Incoming Webhook, and click Add. Enter a name for the webhook, upload an image to associate with data from HostMonitor, and choose Create. Copy the webhook to the clipboard and paste into HostMonitor action properties window.

How to create "workflows" Webhook URL:
in your Microsoft Teams app, choose channel, select Workflows option, then select the workflow you want to setup (Template: Post to a channel when a webhook request is received) and click Add workflow. You will get webhook URL, copy it to the clipboard and paste into HostMonitor action properties window.

Text
Provide text for the message. Macro variable such as %TestName%, %Status%, %Reply%, %RelatedURL% are supported in this field (to be substituted with their actual values at the message generation time).

Markdown formatting (for "office" webhooks only)
Microsoft Teams supports a subset of Markdown formatting tags. Mark this option to enable markdown formatting.
** **bold**
* *italic*
~~ ~~Strikethrough~~
` `Monospace`
> >Block quote
[HyperLink text](https://www.bing.com/)
```

```
![Image link](https://www.www.ks-soft.net/images/hmbox3.jpg)
```
Please note: support for text formatting varies by platform, e.g. Android application does not support strike-through style; unordered and unordered lists supported only by Windows version of Microsoft Teams application.

Telegram message

This action method sends a message to Telegram messenger chat or channel.
In addition to common action parameters, the «Telegram message» action has the following options:

Token
The token is required to authorize the bot (HostMonitor) and send requests to the Bot API, token may look like `110201543:AAHdqTcvCH1vGWJxfSeofSAs0K5PALD`
You may use BotFather to create new bot (using /newbot command) and generate an authorization token. Note: bot's username must end in 'bot', e.g. 'hostmon_bot'.
See also BotFather commands

Chat ID
Provide unique identifier for the target chat or username of the target channel (in the format @channelusername). Macro variable are supported in this field (to be substituted with their actual values at the message generation time).

Note1: In order to send messages to channel bot should be added into admins of the channel.

Note2: How to get Group Chat ID
1) Add the bot to the group: go to the group, click on group name, click on Add members, search for bot (e.g. @hostmon_bot), select the bot and click Add.
2) Send a dummy message to the bot, e.g. /my_id @hostmon_bot
3) Make HTTPS request using the following url:
https://api.telegram.org/botXXX:YYYY/getUpdates (replace XXX:YYYY with bot token)
4) Check responce, look for "chat":{"id":-zzzzzzzzzz,
Done: -zzzzzzzzzz is your chat id (with the negative sign).

Text
Provide text for the message. Macro variable such as %TestName%, %Status%, %Reply%, %RelatedURL% are supported in this field (to be substituted with their actual values at the message generation time).

Parse as (Text / Markdown / HTML)
Telegram Bot API supports basic formatting for messages. You can use bold and italic text, as well as inline links and pre-formatted code in your messages. Telegram clients will render them accordingly. You can use either markdown-style or HTML-style formatting.

Markdown formatting
* ***bold***
_ *_italic_*

~ ~~Strikethrough~~
` `inline fixed-width code`
``` ```pre-formatted fixed-width code block``` (three backquotes)
[inline URL](http://www.example.com/)
[inline mention of a user](tg://user?id=123456789)
Links like tg://user?id=<user_id> can be used to mention a user by their id without using an username. Please note: these mentions are only guaranteed to work if the user has contacted the bot in the past, has sent a callback query to the bot via inline button or is a member in the group where he was mentioned.

HTML formatting
bold
<i>*italic*</i>
inline URL
inline mention of a user
<code>inline fixed-width code</code>
<pre>pre-formatted fixed-width code block</pre>
Please note:
- Only the tags mentioned above are currently supported by Telegram.
- Tags must not be nested.
- All numerical HTML entities are supported.
- The API currently supports only the following named HTML entities: <, >, &amp; and &quot;

Silent
Mark this option to send the message silently - users will receive a notification with no sound.

Slack message

Sends a message to Slack messenger channel.
In addition to common action parameters, the «Slack message» action has the following options:

Webhook URL
You can create Slack app at https://api.slack.com/apps/new, activate Incoming Webhooks, add New Webhook, pick a channel and authorize your Slack app. Than you can find Webhook URL in Slack app settings, it should look like
https://hooks.slack.com/services/T00000000/B00000000/XXXXXXXXXXXXXXXXXXXXXXXX

Title
Title of the message. Macro variable such as %TestName%, %Status%, %Reply% are supported in this field (to be substituted with their actual values at the message generation time).

Text
Provide text for the message. Macro variable such as %TestName%, %Status%, %Reply%, %TaskComment%, %RelatedURL% are supported in this field (to be substituted with their actual values at the message generation time).

Markdown formatting
```

With this option enabled you may use markdown formatting in your message:
* ***bold***
_ *_italic_*
~ ~~~Strikethrough~~~
` `Monospace`
``` ```Monospace block``` (three backquotes)
The Slack supports several binary emoji formats, the list of emoji supported are taken from https://github.com/iamcal/emoji-data

Viber message

This action allows to reach Viber messenger users using Viber Public Account.
In addition to common action parameters, the «Viber message» action has the following options:

Auth token
The authentication token (also known as application key) is a unique and secret account identifier. It is used to authenticate request in the Viber API and to prevent unauthorized persons from sending requests.
The authentication token is generated upon account creation and can be viewed by the account's admins in the "edit info" screen of their Public Account/bot or on the Viber Admin Panel. It may look like `445da6az1s345z78-dazcczb2542zv51a-e0vc5fva17480im9`

Receiver
Unique Viber user ID. Macro variable are supported in this field (to be substituted with their actual values at the message generation time).

Note: Viber API allows accounts to send messages to Viber users who subscribe to the account. Sending a message to a user will be possible only after the user has subscribed to the Public Account by pressing the subscribe button or by sending a message, or by sending a message to a bot.
User may find its userID using POST {} request to https://chatapi.viber.com/pa/get_account_info with header X-Viber-Auth-Token: authtoken

Text
Provide text for the message. Macro variable such as %TestName%, %Status%, %Reply%, %RelatedURL% are supported in this field (to be substituted with their actual values at the message generation time).

Jabber message

This action sends a message through a Jabber server to the specified Jabber client. You should specify parameters of your primary and backup (optional) Jabber accounts on the Jabber page in the Options dialog.
In addition to the common action parameters, the «Send message to Jabber» action has the following options:
```

Jabber account
Specify the Jabber user (client) to whom the message will be sent. More than one destination addresses separating with a semicolon (;). Macro variables are supported in this field.

Message template
Select one of the existing mail templates (that will be used for the message generation) from drop down list or click button to bring up the Mail Templates dialog and create template for your preferences. Macro variables are supported in message templates to be substituted with their actual values at the message generation time.

ICQ message (obsolete)

Sends a message through an ICQ server to the specified ICQ user. You should specify parameters of your primary and backup (optional) ICQ accounts on the ICQ page in the Options dialog.
In addition to the common action parameters, the «Send message to ICQ» action has the following options:

ICQ # (UIN)
Specify the ICQ user to whom the message will be sent. More than one destination address should be separated with a semicolon (;). Macro variables are supported in this field.

Message template
Select one of the existing mail templates (that will be used for the message generation) from drop down list or click button to bring up the Mail Templates dialog and create template for your preferences. Macro variables are supported in message templates to be substituted with their actual values at the message generation time.

Please note: HostMonitor utilizes message queue, supports primary and backup ICQ accounts and uses some other tricks to make message delivery as reliable as possible. However ICQ servers use anti-spam technologies and may block your account or do not accept your messages (temporarily). That's why you should not consider "Send message to ICQ" action as reliable way to notify network administrators about critical network problems.

Record HM Log

“Record HM log” action method allows you to store records in the log under some very specific circumstances. It also provides you with ability to manage flexibly which information should or should not be added into the logs.
E.g. you may add info about passed probes into one log (using “good” action) and save info about failed probes into another log file (using “bad” action). Or you may record results of some test item only when the "reply" is over 1500 ms (using “advanced” action with triggering expression '%Reply%'>'1500 ms').
Please use caution and do not create too many logs. Although Log Analyzer is capable of processing multiple log files together, it takes more time to analyze many small files rather than one big file.

In addition to common action parameters, the «Record HM log» action has the following options:

Add record into common log
Tells HostMonitor to record information about test result into common log file.

Add record into private log
Tells HostMonitor to record information about test result into private log file (log file that is assigned specifically for the test item that has triggered action execution). Even if “Use private log” test property is not activated for this test item, record will be added when action is executed. However if there is no private log specified (file name is empty) for the test item, no record will be added.

Add record into specific log
Tells HostMonitor to record information about test result into some specific log file. You may provide path to html, text or dbf file, HostMontor will record data in appropriate format according to file extension.

Generate reports

HostMonitor can generate reports in HTML, DBF, WML, and Text formats. If you want to generate reports when some test changes status, add "Generate reports" action into action profile. In addition to common action parameters select one of the options:

Generate reports for the containing folder
With this option selected HostMonitor will create reports for the Folder in which the test causing actions are contained. This option useful when you want to assign one action profile to many different tests that are located in different Folders. Each test will create reports for its own Folder.

"Generate reports for .."
Choose this option and select the Folder from drop-down list if you need to create reports for some specific Folder.

Recursive mode
This parameter defines whether HostMonitor includes subfolders to the report or not. Choose one of the following options:

- Single folder	Include specified folder only (no subfolders)
- Folder & all subfolders	Include specified folder and all descendant subfolders
- Folder & subfolders with inherited settings	Incude specified folder and subfolder which inherit report settings from the parent.folder

Use report pool
This option tells HostMonitor that report generation can be deferred for 1-2 seconds. In some cases this option noticeably reduces resource usage, e.g. if you use "Generate reports" action for many test items that can change status at the same time.
However you should not use this option if report must be processed immediately; e.g. you are using 2nd action to send reports by e-mail or you are using some script to publish report on your web site.

As you see you do not specify report to generate directly. That is because each Folder contains list of up to 6 reports or Folder can inherit this list from the Parent Folder. For more information about Folders, refer to "TestList & Windows" section of this documentation.
Also you can use "Execute HMS script" action to generate some specific reports. For more information about Reports, refer to "Log&Reports" section of this documentation.

Send e-mail

HostMonitor can send e-mail notification (that includes the problem data) to a mailbox, a pager or a mobile phone using any SMTP server. On the Mailer settings page in the Options dialog setup the parameters of your Primary and Backup SMTP servers (address of the server, port, authentication method, login, password, etc).
In addition to the common action parameters, the «Send e-mail» action has the following parameters:

From
Specify the email address of the sender.

To (recipients)
Specify a list of recipients for the mail message. A copy of the message is sent to each of them and a "To" SMTP header is created containing the destination addresses. More than one destination address should be separated with a semicolon (;).
Also you can specify optional [cc:] and [bcc:] lists in this field. e.g.
admin@company1.com **[bcc:]** manager@company1.com
admin1@dom1.com; admin2@dom1.com **[cc:]** manager@dom1.com **[bcc:]** hr2@dom1.com; hr5@dom1.com
Macro variables may be used in this field. If you use several variables for list of recipients and some of these variables represent empty string or not specified at all, HostMonitor removes such empty entries from the list. This way mail server will not generate error when your setup allows using of empty variables. Note: HostMonitor does not remove variables from action settings, it removes blank addresses from data transmitted between HostMonitor and mail server.

Priority
Priority option allows you to assign the message a priority so the recipient knows to either look at it right away (High Priority) or read it when time permits (Low Priority).

Subject
The subject of the mail message. Macro variables may be used in the subject line.

Mail template
Select one of the existing mail templates that will be used as a body of the mail (text) from drop down list or click button to bring up the Mail Templates dialog and create mail template for your preferences. Macro variables are supported in message templates to be substituted with their actual values at the message generation time. Also you can specify a particular character set for your mail templates.

Attach file
You can mark this option and select file that will be attached to the message. Enter the path manually or press button to select a file from the Open File dialog.
In addition to standard macro variables, the following variables can be used when you specify path to attachment file:
- %NewestFile% - newest file in specified folder
- %OldestFile% - oldest file in specified folder

- %NewestFolder% - newest sub-folder
- %OldestFolder% - oldest sub-folder

Send message to pager (TAP)

HostMonitor can send message to your alpha-numeric pager(s) using the TAP protocol. For this you need a modem and a phone line connected to the computer. On the Pagers page in Options dialog you can setup general modem settings.
In addition to the common action parameters, you will need to fill out some information about the paging company and pager of the person you wish to send a message to. These parameters can be different for each action.

What do you need to know about the paging company of the pager?

Access Number
You need to know the paging terminals alphanumeric paging access telephone number. This is the phone number of the modem at the paging company that will receive the message using the TAP protocol. This number is the same for everybody that has a pager from that company. Many carriers will offer 800 numbers - especially the nationwide guys like SkyPage or Mobilcomm. THIS IS DIFFERENT FROM THE PAGER TELEPHONE NUMBER. You may include dashes and commas like any other modem phone number (a comma usually pauses 2 seconds - i.e. 9,444-4444).
By putting "DIRECT" in this string, the program assumes a direct connection. No dialing takes place and DTR is NEVER dropped. If the phone number is in the format +1 (303) 799-0055 that is called canonical form, the access phone number will be TAPI converted to a dialable number. In this manner you can always send the area code and it will know if it is a local or long distance call. It will also dial the prefix digit (such as 9) to get outside line - etc.

Password
Does your paging carrier require a password? Most US companies DO NOT. In this case, the program sends six zeros as the password. This is the standard way of doing it. If you require a special password, define it in this field.

Max characters per block
This is the number of characters the paging company allows per message block. This number varies widely from company to company. Some are as small as 60 characters and some are as big as 1000 characters. The norms seem to be 80 and 230 characters per block. You will need to find out this information or learn this through trial and error. If the message you pass is bigger than the character per block limitation, the program automatically splits your message up into multiple blocks, so the recipient gets the entire message. However, he/she does get a different page for each block.

Parity
Specifies the parity, data bits, stop bits that the paging company's alpha access port communicates at. In very rare cases the paging terminal require N,8,1 rather than E,7,1.

What do you need to know about the Pager?

Pager ID
The only thing you need to know about the pager is the pager phone number or the Pager ID (Alpha PIN). DO NOT INCLUDE ANY DASHES in this number.
Macro variables may be used in this field.

Mail template
Select one of the existing mail templates (that will be used for the message generation) from drop down list or click button to bring up the Mail Templates dialog and to create the template for your preferences. Macro variables are supported in message templates to be substituted with their actual values at the message generation time.

Send message to pager (SNPP)

This action sends a message to a pager using the SNPP protocol; unlike TAP protocol, which employs the modem, SNPP is built on top of TCP/IP to send messages via an Internet connection.
In addition to the common action parameters, «Send message to pager (SNPP)» action has the following options:

PagerID
Specify the Pager ID (PID) number. Macro variables may be used in this field.

Mail template
Select one of the existing mail templates (that will be used for the message generation) from drop down list or click button to bring up the Mail Templates dialog and to create the template for your preferences. Macro variables are supported in message templates to be substituted with their actual values at the message generation time.

Server
Specify the name or IP address of the SNPP server.

Port
The default SNPP port is 444, but you can specify a non-standard port.

Login as
This parameter allows for a session login ID to be specified. It is used to validate the person attempting to access the paging terminal. If this option is disabled, "anonymous" user status is assumed.

Send message to beeper

HostMonitor can send messages to "numeric only" pagers (beepers). TAP protocol is not used in these cases. The program simply takes the phone line off-hook, dials the pager phone number, waits specified number of seconds, touch tones the digits to be displayed on the pager and hangs

up. This method does not guarantee delivery to the paging company. It just dials and hopes it works.
In addition to the common action parameters, the «Send message to beeper» action has the following options:

Beeper #
Enter the telephone number for the beeper. This is the number on the beeper that people call to touch tone in digits. You may use a comma in the number, the comma tells the modem to wait 2 seconds.
Macro variables may be used in this field.

Delay
Specify how many seconds to delay from the time the beeper number dialed and the display digits are dialed.

Send message
This parameter defines the digits that will appear on the pager. You may use macro variables (e.g. "%StatusID%", "%HostID%", "%CommentID%") and comma (for 2 seconds delay).

Termination string
Define the modem command used to terminate a call. Normally, this parameter is empty and HostMonitor uses a "**#,H;**" to finish the call. The # is normally used when you have finished touch-toning in the digits to send to the pager. The comma tells the modem to wait 2 seconds before hanging up. The "H" tells the modem to hang up when it is done. The semi-colon puts the modem in command mode and sends an OK to the computer when it has finished dialing.

Setup general paging settings on the Pagers page in Options dialog.

Send SMS (GSM)

"Send SMS (GSM)" action sends SMS messages through a GSM modem (cell phone) connected to the system where HostMonitor is running. You should specify parameters of your primary and backup (optional) GSM modems on the GSM page in the Options dialog.
In addition to thecommon action parameters, the “Send SMS (GSM)” action has the following parameters:

Destination phone
Provide phone number to which the message should be sent. More than one recipient separating with a semicolon (;). For example "+12063979723;+1555204090". Macro variables are supported in this field.

Message class
Choose class of the message:
- 0..Display immediately
- 1..ME (mobile equipment)
- 2..SIM
- 3..TE (terminal equipment)

The most of mobile phones support message class 0 and 2.

Message template
Select one of the existing mail templates that will be used as a body of the mail (text) from drop down list or click button to bring up the Mail Templates dialog and create mail template for your preferences. Macro variables are supported in message templates to be substituted with their actual values at the message generation time.
If a message is longer than 160 characters, HostMonitor will split the message and send several SMS to the recipient. If this is not really necessary, we recommend using compact mail templates for "Send SMS" actions.

Send SMS (SMPP/IP)

"Send SMS (SMPP/IP)" action sends SMS messages through a SMPP network service providers (SMSC) using TCP/IP connection. You should specify parameters of your primary and backup (optional) SMPP accounts on the "SMS: SMPP" page in the Options dialog.
In addition to the common action parameters, the “Send SMS (SMPP)” action has the following parameters:

Destination phone
Provide phone number to which the message should be sent. More than one recipients separating with a semicolon (;). For example "+12063979723;+1555204090". Macro variables are supported in this field.

Destination TON
Choose the Type of Number (TON) for the "Destination phone":
- Unknown
- International
- National
- Network Specific
- Subscriber Number
- Alphanumeric
- Abbreviated

We recommend using "International" format of the phone (with leading "+" character followed by a country code). E.g. +17057969345, +491710765342, etc.

Destination NPI
Choose the NPI for the "Destination phone".
- Unknown
- ISDN (E163/E164)
- Data (X.121)
- Land Mobile (E.212)
- National
- Private
- ERMES
- Internet (IP)

Message template
Select one of the existing mail templates that will be used as a body of the mail (text) from drop down list or click button to bring up the Mail Templates dialog and create mail template for your preferences. Macro variables are supported in message templates to be substituted with their actual values at the message generation time.
If a message is longer than 160 characters, HostMonitor will split the message and send several SMS to the recipient. If this is not really necessary, we recommend using compact mail templates for "Send SMS" actions.

Stop service

Microsoft Windows NT* supports an application type known as a service. HostMonitor can stop these applications on local or remote computers (if you have an account with privileges for starting/stopping services).
* Here "Windows NT" means Windows system based on NT technology, including Microsoft Windows NT 4.0, Windows 2000/XP/2003, Windows 7/8/10, Windows Server 2008-2019.

In addition to the common action parameters, the «Stop service» action has the following options:

Computer name
Provide the name of the target system (the target computer name must be prefixed by "\\") or select the "<local computer>" item to stop the service on a local machine. You may use the "Browse network" button to select a computer from the list. Also you can use macro variables (e.g. %ServiceComp%, %ServiceName%) in this field.

Service name
Name of the service to stop. You may select the service from the drop-down list. You can use macro variables in this field as well.
Comma separated lists are supported, HostMonitor can stop several services one by one. E.g. you may use %Reply% variable for action triggered by Service test that checks ALL “Auto” services.

Parameters
Parameters string passed to the service.

Connect as
To stop a service on remote Windows system you may mark this option and provide a username and a password for a connection to the target computer. Also Connection Manager can be used (when ConnectAs option is not marked)

Start service

Microsoft Windows NT* supports an application type known as a service. HostMonitor can start these applications on local or remote computers (if you have an account with privileges for starting/stopping services).
* Here "Windows NT" means Windows system based on NT technology, including Microsoft Windows NT 4.0, Windows 2000/XP/2003, Windows 7/8/10, Windows Server 2008-2019.

In addition to the common action parameters, the «Start service» action has the following options:

Computer name
Provide the name of the target system (the target computer name must be prefixed by "\\") or select the "<local computer>" item to start the service on a local machine. You may use the "Browse network" button to select a computer from the list. Also you can use macro variables (e.g. %ServiceComp%, %ServiceName%) in this field.

Service name
Name of the service to start. You may select the service from the drop-down list. You can use macro variables in this field as well.
Comma separated lists are supported, HostMonitor can start several services one by one. E.g. you may use %Reply% variable for action triggered by Service test that checks ALL “Auto” services.

Parameters
Parameters string passed to the service.

Connect as
To start a service on remote Windows system you may mark this option and provide a username and a password for a connection to the target computer. Also Connection Manager can be used (when ConnectAs option is not marked)

Restart service

Microsoft Windows NT* supports an application type known as a service. HostMonitor can restart these applications on local or remote computers (if you have an account with privileges for starting/stopping services)
* Here "Windows NT" means Windows system based on NT technology, including Microsoft Windows NT 4.0, Windows 2000/XP/2003, Windows 7/8/10, Windows Server 2008-2019.

In addition to the common action parameters, the «Restart service» action has the following options:

Computer name
Provide the name of the target system (the target computer name must be prefixed by "\\") or select the "<local computer>" item to restart the service on a local machine. You may use the "Browse network" button to select a computer from the list. Also you can use macro variables (e.g. %ServiceComp%, %ServiceName%) in this field.

Service name
Name of the service to restart. You may select the service from the drop-down list. You can use macro variables in this field as well.
Comma separated lists are supported, HostMonitor can restart several services one by one. E.g. you may use %Reply% variable for action triggered by Service test that checks ALL “Auto” services.

Do not start service if it was stopped prior to execution of the action
This option is useful when you want to stop service (e.g. for maintenance purpose) without disabling the test.

Connect as
To restart a service on remote Windows system you may mark this option and provide a username and a password for a connection to the target computer. Also Connection Manager can be used (when ConnectAs option is not marked)

Reboot remote system

HostMonitor can reboot or shut down remote Windows NT* system. To shut down a remote computer, the calling process must have the SE_REMOTE_SHUTDOWN_NAME privilege on the target system. By default Administrators have this privilege.
* Here "Windows NT" means Windows system based on NT technology, including Microsoft Windows NT 4.0, Windows 2000/XP/2003, Windows Windows 7/8/10, Windows Server 2008-2019.

In addition to the common action parameters, define the following options:

Computer name
Provide the name of the target system (the target computer name must be prefixed by "\\"). You may use the "Browse network" button to select a computer from the list. Also you can use macro variables (e.g. %HostAddr%) in this field.

Message to display
Provide a message to display on the remote system before shutdown.

Time to display
If time is not zero, system displays a dialog box on the specified computer. The dialog box displays the name of the user who called the function, displays the message, and prompts the user to log off. The dialog box beeps when it is created and remains on top of other windows in the system. The dialog box can be moved but not closed. A timer counts down the remaining time before a forced shutdown. If the user logs off, the system shuts down immediately. Otherwise, the computer is shut down when the timer expires.
If you set time to zero, the computer shuts down without displaying the dialog box.

Method
Select one of the 2 options:
- Reboot - shuts down the system and then reboots.
- Shutdown - shuts down the system to a point at which it is safe to turn off the power.

Force processes to terminate
During a shutdown or reboot operation, applications that are shut down are allowed a specific amount of time to respond to the shutdown request. If the time expires, the system displays a dialog box that allows the user to forcibly shut down the application, to retry the shutdown, or to cancel the shutdown request. If the "Forces processes to terminate" option is enabled, the program sets flag EWX_FORCE and the system always forces applications to close and does not display the dialog box. When this flag is set, the system does not send the WM_QUERYENDSESSION and WM_ENDSESSION messages. This can cause the applications to lose data. Therefore, you should only use this flag in an emergency.

Reboot local machine

HostMonitor can reboot local Windows system. In addition to the common action parameters, choose 1 of 4 reboot **Methods**:

- **Logout** - Shuts down all processes running in the current security context, logs the user off.
- **Reboot** - Shuts down the system and then reboots.
- **Shutdown** - Shuts down the system to a point at which it is safe to turn off the power.
- **Poweroff** - Shuts down the system and turns off the power. The system must support the power-off feature.

Force processes to terminate
During a shutdown or log-off operation, applications that are shut down are allowed a specific amount of time to respond to the shutdown request. If the time expires, the system displays a dialog box that allows the user to forcibly shut down the application, to retry the shutdown, or to cancel the shutdown request. If the "Forces processes to terminate" option is enabled, the program sets flag EWX_FORCE and the system always forces applications to close and does not display the dialog box. When this flag is set, the system does not send the WM_QUERYENDSESSION and WM_ENDSESSION messages. This can cause the applications to lose data. Therefore, you should only use this flag in an emergency.
When you reboot a local **Windows 2000/XP system** HostMonitor uses another flag: EWX_FORCEIFHUNG. This flag forces processes to terminate only if they do not respond to the WM_QUERYENDSESSION or WM_ENDSESSION message.

Execute external program

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

Command line
Specify command line to launch external application. Macro variables may be used in the command line.

Window mode
This parameter 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.

Known problems:
If you are using Windows Vista or newer version of the system, UAC is enabled and HostMonitor running as Win32 service cannot start external applications, you may need to assign "Replace a process level token" right to the account (user account used for HostMonitor service). Local Computer Policy -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> Replace a process level token -> Properties -> Add User or Group, then restart system.

Start program remotely

HostMonitor may start specified process on remote Windows systems. If the newly created process attempts to interact with objects on the target system without the appropriate access privileges, it will be terminated without notification. Also for security reasons this method cannot be used to start an interactive process remotely. If you cannot use administrator account or you need to start interactive process on remote system, you may use Remote Monitoring Agent running on target system and <Execute external program> action.
In addition to the common action parameters, the «Start program remotely» action has the following parameters:

Start process on
Provide the name or IP address of the target system . You may use the "Browse network" button to select a computer from the list. Also you may use macro variables (e.g. %HostAddr%) in this field.

Command line
Specify command line to launch external application. Macro variables may be used in the command line.

Working directory
You may specify current drive and directory for the process (full path is recommended). If you do not specify this path, %SystemRoot%\system32\ directory will be used.

User/password
Provide account that will be used for authentication on remote system (administrator account required). If you keep user field empty, then HostMonitor will use account specified in Connection Manager (account for WMI test related to target system).

Kill process

HostMonitor may kill specific process on local or remote Windows system. You may setup Dominant Process test to check for processes that use too much of CPU resources, handles or memory and use "Kill process", "Start program remotely" actions to restart "bad" processes (NOTE: some processes may lose data when you kill them).
In addition to the common action parameters, the «Kill process» action has the following parameters:

Kill process on
Provide the name or IP address of the target system . You may use the "Browse network" button to select a computer from the list. Also you may use macro variables (e.g. %HostAddr%) in this field.

Kill by name
Use this option when you need to kill process using its name, e.g. chrome.exe. HostMonitor will kill all instances of the process. Macro variables may be used, e.g. if action triggered by Dominant Process test method, you may use %ProcessName% variable.

Kill by proc ID
Use this option when you know process ID. HostMonitor will kill single instances of the process. Macro variables may be used, e.g. if action triggered by Dominant Process test method, you may use %ProcessID% variable.

User/password
Provide account that will be used for authentication on remote system. If you keep user field empty, then HostMonitor will use account specified in Connection Manager (account for WMI test related to target system).

Log Event

Event logging in Microsoft Windows NT* provides a standard, centralized way for applications (and the operating system) to record important software and hardware events. The event-logging service stores events from various sources in a single collection called an event log.
The Log Event action form allows you to add or edit an action that will log a record to the Event Log. Entries in the event log can be viewed with the Event Viewer or used by the other software utilities that perform centralized alerting from the event log.
* Here "Windows NT" means Windows system based on NT technology, including Microsoft Windows NT 4.0, Windows 2000/XP/2003, Windows Vista, Windows 7-11, Windows Server 2008-2022.

In addition to the common action parameters, the «Log Event» action has the following parameters:

Computer
The UNC (Universal Naming Convention) name of the server on which the event should be recorded (the target computer name must be prefixed by "\\"). Type the UNC or select the "<local computer>" item. You can use macro variables (e.g. %HostAddr%) in this field.

Log
Provide name of the log file. This can be the Application, Security, System log file, or a custom registered log file.

Event source
Select source of the events from drop down list. You can use macro variables (e.g. %CommentLine2%) in this field.

Event type
Choose type of the event to be logged. This parameter can have one of the following values
- Error
- Warning
- Information

Event ID
Specify event identifier. If you use “HostMonService” as Event Source, use ID within range 2001..2099. This range is reserved for users’ messages. HostMonitor does not and will not use IDs from this range.

Description
Provide description of the event (this field is optional). You can use macro variables (e.g. %TestName%, %Status%, %Reply%, etc) in this field.

Connect as
To log event on the remote system you can mark this option and provide username and password for the connection to the target computer.

SQL Query

Executes an SQL query against the specified ODBC data source. In addition to the common action parameters, the «SQL Query» action has the following parameters:

ODBC data source
Choose one of ODBC data sources available on your system (if action should be performed by RMA, HostMonitor will show ODBC sources list retrieved by the agent on remote host).
Macro variables are supported, e.g. you may use folder-related variable %fvar_datasource%, this way single action profile assigned to different test items may send requests to different databases

Login
Specify user identifier, if necessary.
Note: some ODBC drivers (e.g. MS SQL ODBC Driver version 13.1+) support Integrated Windows authentication and Active Directory Integrated authentication. In this case you may type `WindowsAuth` instead of login name (for Integrated Windows authentication) or set `ADAuth` as login name (for Active Directory Integrated authentication). Password field is not used in such case.

Password
Specify password, if necessary.

SQL Query
Specify SQL query to execute. Macro variables are supported in the query to be substituted with their actual values at the action execution time.

Timeout
Specify the number of seconds to wait for a login request to complete.

Reliability / Known problems

If you are using SQL Query action, you must be sure that ODBC driver (provided by 3rd party) works reliable and will not cause HostMonitor to crash. E.g.
- Microsoft dBase Driver v 4.00 causes resource leakage;
- Oracle drivers v8 and v10 have many "bugs" and may crash application;
- Old MySQL ODBC drivers v3 cause handles leakage in multithreaded environment;
- MySQL ODBC drivers version 8.00.11 – 8.00.15 may lead to various problems as well, including memory access violations. If you need to use MySQL ODBC driver version 8.x, please set two options in hostmon.ini file, [Misc] section:

```
[Misc]
ODBC_UseSharedEnvHandle=1
ODBC_KeepSharedEnvHandle=1
```

HTTP request

Sends HTTP request to the specified Web server. In addition to the common action parameters, the "HTTP request" action has the following options:

Host
This is the domain name or the IP address of the target web server.
HostMonitor can perform HTTPS requests as well - if you need HTTPS request, specify target host using https:// prefix (e.g. https://www.google.com). For HTTP requests you may use http:// prefix or specify host name without any prefix (e.g. www.google.com).
Note: HostMonitor will perform request even for hosts with invalid certificates (expired or certificate with wrong hostname).

Port
A valid TCP port number (a value between 1 and 65535). Usually port 80 used for HTTP requests, port 443 for HTTPS

Request
Provide data to send to the host. Macro variables are supported.
"HTTP request" action applies URL encoding rules to macro variables. E.g. if test status is "Host is alive", %Status% variable will be translated to Host%20is%20alive.
Some exceptions:
- if Content-Type: application/json specified, then HostMonitor will use JSON encoding rules;
- if hmvars: text HTTP header specified, HostMonitor will not encode variable values (will not apply JSON or HTML encoding rules)

You may send GET, HEAD, DELETE, PUT or POST requests. POST/PUT data should be provided in Request field, separated from header with 1 empty line. If you do not specify content-type for POST request, HostMonitor will use default type (Content-Type: application/x-www-form-urlencoded).
Also, HostMonitor adds <cr><lf><cr><lf> (empty line) after each request (according to HTTP protocol).

For example you may send messages to SLACK messenger using HTTP request like the following

-- SLACK action parameters –

```
Host: https://hooks.slack.com
Port: 443
Request:
POST https://hooks.slack.com/services/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 HTTP/1.1
Host: hooks.slack.com
Content-Type: application/json

{"channel": "#hmonitor", "username": "tom", "text": "TestName:%TestName%
Status: %Status%
Reply: %Reply%
Recurrences: %Recurrences%", "icon_emoji": ":ghost:"}
```

Send data to TCP/UDP port

Sends data to the specified host using TCP or UDP protocol. In addition to the common action parameters, the «Send data to TCP/UDP port» action has the following options:

Server
This is the domain name or the IP address of the target host.

Port
A valid port number (a value between 1 and 65535) is required for the connection to take place.

Protocol
Select the protocol to use: TCP or UDP.

Init packet (string) to send
Provide data to send to the host. In this field you can use regular text; macro variables; and sequences formatted **%XX** where XX is a hexadecimal code of a character (byte). E.g. define this parameter like: «**%TestName% %0D%0A %Status% %0D%0A %DateTime%**» to send 3 text lines with the information about the test, its status, and current time.

Wait for answer
Specify how many seconds HostMonitor should wait for an answer before sending Final packet.

Final packet (string) to send
Provide this parameter if you need to send two information packets with the pause between them to the host. The same as for the Init Packet parameter, in this field you can use regular text; macro variables; and sequences formatted **%XX** where XX is a hexadecimal code of a character (byte).

Syslog

This action sends data using the Syslog protocol. Syslog is the standard event logging subsystem for Unix, also you can find Syslog Daemon for Windows (e.g. Kiwi Syslog Daemon). 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 SNPP port is 514, but you can specify a non-standard port.

Message
Provide text message to send. Macro variables are 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 Set

Sets data on the local or remote system using the SNMP protocol. The 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). Using this protocol HostMonitor can change settings of your network devices.
In addition to the common action parameters, the «SNMP Set» action has the following parameters:

Agent address
Provide address of the target system. Specify either a dotted-decimal IP address or a host name that can be resolved to an IP address, an IPX address (in 8.12 notation), or an Ethernet address. You can use macro variables (e.g. %HostAddrB%) in this field.

Community
Specify the SNMP community name used when communicating with the device specified in the Agent Address parameter. By default on SNMP systems this is "PUBLIC" but it can be different on your systems.

Timeout
This is the amount of time in seconds the program will wait for a response from the server before the request fails.

Retries
Specify the communications retries count.

OID
The name that uniquely identifies the object, the value of which you have to change. For example OID "1.3.6.1.2.1.2.1" represents the number of network interfaces on which system can send/receive IP datagrams; OID "1.3.6.1.2.1.6.9" represents the number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT; etc. To get a list of valid OIDs for your SNMP enabled devices you should contact the vendor of the device. They should be able to give you a MIB file that contains all the OIDs for the device.

Set value
Define a new value for the object that HostMonitor has to set (please note some object can be read-only). Use "Get current value" button to retrieve current value of the object.
You can use macro variables (e.g. %HostAddr%) in this field.

SNMP Trap

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 (e.g. %HostAddr%) in this field.
Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) and specify hostname with suffixes ::ipv4 or ::ipv6 (e.g. www.google.com::ipv4 or www.6bone.net::ipv6). If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.
Note: on Windows NT 4.0, Windows 2000 and Windows XP SP1 IPv6 protocol is not supported. You may use menu Tools -> Local Info to check is your system IPv6 ready.
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**). You cannot specify port number when target host specified with ipv4/ipv6 suffix.

Agent address
Provide IP address of the agent that generated the SNMP Trap. If you keep default value "localhost", HostMonitor will use IP address of the system where it is running. You can use macro variables (e.g. %HostAddr%) in this field.

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
Identifies the type of the object causing the trap. You can use macro variables (e.g. %CommentLine1%) in this field.

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).
You can use macro variables (e.g. %CommentLine2%) in this field.

MIB Value
Define an object's value. You can use macro variables (e.g. %CommentLine2%) 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

Dial-up to the network

This action allows establishing dial-up connection to a network. E.g. HostMonitor can establish backup connection in case of primary channel malfunction. In addition to the common action parameters, the «Dial-up to the network» action has the following options:

Dial-up connection
Select from drop down list the remote access entry to establish the connection.

User name
Specify the user's name. This parameter is used to authenticate the user's access to the remote access server. If the user name is empty string (""), HostMonitor uses the user name of the current logon context for authentication. For a user-mode application, RAS uses the credentials of the currently logged-on interactive user. For a Win32 service process, RAS uses the credentials associated with the service.

Password
Specify the user's password. This parameter is used to authenticate the user's access to the remote access server. If the password is empty string (""), HostMonitor uses the password of the current logon context for authentication. For a user-mode application, RAS uses the credentials of the currently logged-on interactive user. For a Win32 service process, RAS uses the credentials associated with the service.

Save password
This option has sense only if Password parameter is not an empty string. Specifies whether to save the password (in the phone-book entry) for the user indicated by User Name parameter or not. If "Save password" option is disabled, the password will be removed. Disabling option is equivalent to checking the "Unsave Password" checkbox in Dial-Up Networking dialog.

Show dial-up dialog
With this option enabled HostMonitor will display a popup window when establishing the connection, and will display dial-up process information in it.

Retries
Set the number of times the dial-up connection is automatically redialed if the first attempt to connect fails.

Disconnect dial-up connection

Purpose of this action is to drop the specified dial-up connection (e.g. in case if the main channel will restore its functioning). In addition to the common action parameters, the «Disconnect from network» action has only one parameter:

Dial-up connection
Select from drop down list the remote access connection to terminate.

Repeat test

This action simply forces the program to perform the test one more time (not waiting until time of the test interval is elapsed). In addition to the common action parameters, you may select one of the following options: “Repeat test itself” or “Recheck dependant test items”

Repeat test itself
This action can be helpful in situations when the condition being checked is not stable. If, for some reason, the accuracy of the test is questionable, you can add this action into alert profile, and take the necessary measures based on the results of the follow-up test.

Recheck dependant test items
This option tells HostMonitor to recheck dependant test items (items that depend on Master test which triggered this action).
You may want to use this action is some special cases when “Recheck dependant test items when master test status has been changed” option located on Behavior page in Options dialog is disabled.

Change test interval

This action allows changing the test time interval. In addition to the common action parameters choose one of the options:

- **Restore original value** - restores the original test time interval that was defined by user using Test Propetries dialog
- **Set to HH:MM:SS** - set interval to the specific value
- **Set to N% of the current value** - increases or decreases the current test time interval by the specified amount of times.

Note: "Change test interval” action may set new interval for tests with irregular schedule as well. Action changes type of the schedule to “regular”, keeps old type in memory so it can be restored by “Change test interval” action with “Restore original interval” option. However “Set to N% of the current value” option cannot be applied for tests with “irregular” schedule.

Execute HMS script

This is very flexible action because script file may contain various commands for the program and tests control. In addition to the common action parameters, the «Execute HMS script» action has only one parameter:
Script file - specify full path to the script file or click small button on right side and select file from the Open File dialog.

HostMonitor Script file (file extension .HMS) is a text file that contains commands for HostMonitor. You can create and edit script file using any text editor (e.g. notepad). Some examples when this action method can be useful:

1. Assuming that you have dynamically (real-time) database with list of servers to monitor. When database is changing HostMonitor can reload the list of tests or import new tests automatically. To implement this behavior add test to monitor changes in the database (e.g. "File Integrity" test or "ODBC Query" test), and add "Execute HMS script" action to the action profile that assigned to the test to run a script like:
   ExecuteProgram 10000 c:\database\generator.exe c:\database\database.dbf c:\HostMon\import1.txt
   NewTestList
   ImportFromFile c:\HostMon\import1.txt
   SaveTestList c:\HostMon\temp1.hml

2. Assuming that you need to monitor 200 web servers in the Internet, but your LAN uses just one router to access to the Internet. Of course if your router goes down, HostMonitor will start hundreds alerts. To avoid unnecessary alerts make next steps:
   - add ping test to check the router;
   - set interval for this test less than intervals for Internet tests (e.g. 30 sec for router and 5 min for each web server);
   - create 2 scripts: one for "Bad" action that will be executed when router will die, another for "Good" action that will be executed when router will restore operability.
   "Bad" script:
   DisableTest _AllTCP
   DisableTest _AllURL
   "Good" script:
   EnableAllTests

   If you use HostMonitor version 3.0 or higher, this is not a topical example. You do not need to disable/enable tests, you can just assign router ping test as a Master test for all web tests.

HMScript
HostMonitor Script file (file extension .HMS) is a text file that contains commands for HostMonitor. You can create and edit script file using any text editor (e.g. notepad). Some common rules:

- You can put only one command in each line
- Comments: The program ignores all strings with a semicolon (;) as the 1st character

- Commands: commands are case insensitive (e.g. "LoadTestList" and "LOADTESTLIST" means the same)
- Parameters: parameters are case sensitive
- HostMonitor version 3.0 or higher supports macro variables (%HostName%, %Comment %, %Folder%, etc.). Please note:
  - if script is launched as a result of a test performance, the test parameters are used for macros;
  - if script is launched manually (using menu File->Execute Script), parameters of the selected test are used for the macros (if no test is selected, macros are not translated)
- HostMonitor version 9+ supports multi-line variables

List of commands:

Command	Parameter(s)	Description
- TestList operational commands		
NewTestList	[DiscardChanges]	Creates new empty TestList. Use optional DiscardChanges parameter to create new test list without saving current list of tests.
LoadTestList	<FileName.HML>	Loads an existing TestList
AppendTestList	<FileName.HML>	Appends data to the current TestList from a specified HML file
ImportFromFile	<FileName> [SkipDuplicates] [WriteLog]	Imports tests from special Text file. SkipDuplicates - optional parameter, HostMonitor will skip test when test with the same name already present in the TestList. WriteLog - optional parameter, HostMonitor will record to the system log file information about all errors and warnings during the import process.
SaveTestList	[<FileName>]	Saves the current list using its current or new file name. Parameter is optional when current list was loaded from the file (in this case HostMonitor knows the name of the file). You must specify a name of the file when you have created a new list.
ExportHmlIntoText	<FileName> [-SF] [-SL]	This command tells HostMonitor to export test settings into specified text file. Optional parameters: -SF - comment destination folders; -SL - comment test links
Note: HostMonitor doesn't save changes when executes script. If you need to save list of tests, use SaveTestList command. Examples: NewTestList LoadTestList c:\list1.hml AppendTestList c:\list2.hml ImportFromFile c:\import1.txt SkipDuplicates WriteLog SaveTestList c:\list3.hml		
- Folder selection		
ResolveMacros	yes|no	Normally HostMonitor resolves macro variables specified in the script. However you may turn this option off at any time (and later turn it on again if you need). Command has effect for the following commands within the script (commands located below ResolveMacros line). For example this can be useful when you need to assign some macros for comment pattern.

SetCurrentFolder	<name of folder> | <full path>	Set current folder, all following commands from this section (manipulation with tests) will work within specified folder. By default, HostMonitor uses the top folder including all subfolders (in other words, works with whole TestList).
IncludeSubfolders	yes|no	Define either to perform operations for the current folder only or to use the folder and all descendant subfolders. By default, HostMonitor works with the specified folder and all descendant subfolders.
UseLinks	yes|no	Tells HostMonitor to perform (or does not perform) operations with test items that represented in the folder as links
- folder modifications		
CreateFolder	<full path to the folder>	Creates new folder(s). The value of this parameter should specify the full path to the folder that you want to create. E.g. CreateFolder Root\USABranch\Support\part2\ will successively create 3 folders - "USABranch" folder in the "Root" folder, - "Support" folder in "USABranch" subfolder, - "part2" folder in "Support" subfolder. If some (or all) of specified folders already exist, HostMonitor will not create second copy of them.
SetFolderVariable	<variable_name> <variable_value> [-inheritpartly]	Sets or modifies folder variable for current folder. If currently folder settings set to "inherit all variables from parent folder", this command will set "Use folder variables only" mode. Unless you specify optional -inheritpartly parameter; in such case HostMonitor will set "Use inherited variables; folder variables may override inherited variables" option. Note: if you are using folder-level variables as parameters of some test items, this command will modify test settings automatically.
SetFolderAgent	<fullpath>| <folderID> <agentname> [UnlessInherited]	Sets Remote Monitoring Agent for specific folder. You may specify folder using full path or using folder ID; specify agent using its name. Optional "UnlessInherited" parameter tells HostMonitor to check agent used by parent folder and set (when possible) "Inherit agent from parent" option instead of changing folder-specific agent. If "UnlessInherited" is not specified then HostMonitor will set specified agent regardless of parent agent.

Examples:

```
CreateFolder Root\BackupOffice\WWW

SetCurrentFolder  Root\BackupOffice\WWW
SetFolderVariable fvar_host   "10.10.5.1"  -inheritpartly
SetFolderVariable fvar_e-mail  admin_mike@gmail.com

SetCurrentFolder  Root\MainOffice\WWW
SetFolderVariable fvar_host   "10.10.1.1"
SetFolderVariable fvar_e-mail  admin_greg@gmail.com
```

CopyFolder	[-r] <srcname>|<id>|<fullpath> <newname>|<newfullpath>	Optional parameter "-r" tells HostMonitor to copy folder with its subfolders. Source folder can be specified by name (if this folder located within current parent folder – folder selected by SetCurrentFolder command); folder ID or full path to the folder. Target folder can be specified by name or full path.
CopyTest	<testname>|<groupname> <destfullpath>|<folderid>	Copy specific test or group of tests (e.g. all Ping tests) into specified folder. Destination folder can be specified by full path or folder ID.

CopyTestByID	<testid> <destfullpath>| <folderid>	Copy single test specified by ID into target folder specified by full path or folder ID.
CopyAllTests	[-r] [-skipduplicates] [–adjustMasters] <destfullpath>|<folderid>	Copy all test items from current folder (and optionally subfolders) into target folder. “adjustmasters” option: if dependant tests copied with master(s) then HostMonitor adjust master-dependant relations for newly created tests. E.g. if you copy 6 tests (5 NetApp tests that depends on 1 Ping test) then new NetApp tests will depend on new Ping test (if you are using folder-related variables for target IP address, then new tests will start to monitor new device without any manual adjustments).
CopyIntoSelected Folders	<testname>|<TestID> Below <fullpath>| <TopFolderID> When <expression> [-skipduplicates]	This command allows you to copy specified test item into set of folders. You may select destination folders using logical expressions based on folder name or folder-level variables. First parameter (<test name> or <testID>) specifies what exactly test item should be copied. "Below <fullpath>" or "Below <TopFolderID>" parameter specifies target folders branch that should be used for operation. Then HostMonitor checks each folder and subfolder within specified branch, resolves folder-related macro variables, evaluates specified logical expression (When <expression> parameter) and copies the test item into folder when <expression> is true. For example, if you use "%folder %"=="Memory tests" expression, HostMonitor will copy test into each folder that named "Memory tests". If you use expression like "Important" in "%FolderComment%", HostMonitor will copy test into each folder that has word "Important" within folder comments. If you use expression "%fvar_testtype%" == "memory", HostMonitor will copy test into each folder that has %fvar_testtype% variable set to "memory" string Last optional parameter (-skipduplicates) tells HostMonitor to skip operation for the folder when target folder already has test with the same name. Note: as usually HostMonitor will resolve folder-related variables that can be used as test parameters. This way single command can create set of tests for various servers.

These commands allow you to create tests for new servers automatically in response to some event or copy tests using e-mail message sent to HostMonitor. E.g. you may setup template items then use CopyFolder, SetFolderVariable, SetFolderAgent and CopyAllTests commands to create complete set of tests for new server.
Example:

```
CopyFolder -r Root\ServerTemplate Root\SQLServer2
SetCurrentFolder Root\SQLServer2
SetFolderVariable host 10.10.0.11 -inheritpartly
SetFolderAgent Root\SQLServer2 “active 2“
SetCurrentFolder Root\ServerTemplate
CopyTests –r _AllPing Root\SQLServer2
CopyTests –r _AllODBC Root\SQLServer2
CopyTests –r _AllCPU Root\SQLServer2
SetCurrentFolder Root\SQLServer2
IncludeSubfolders yes
EnableAllTests

SetCurrentFolder Root\Templates
CopyIntoSelectedFolders 555 Below "Root\" When "Disk" in "%folder%" -skipduplicates
CopyIntoSelectedFolders "Top memory consumer" Below "Root\" When "%fvar_testtype%" == "memory"
```

- manipulation with tests

RefreshAll		Checks the status of all tests in the folder (except disabled hosts) immediately, do not wait for the elapse test interval for each test
ResetAll		Resets statistics for all tests within the folder
DisableAllTests		Disables all tests in the folder
EnableAllTests		Enables all tests in the folder
DisableTest	<TestName>	Disables the specified test
EnableTest	<TestName>	Enables the specified test
RefreshTest	<TestName>	Check the status of the specified test immediately
ResetTest	<TestName>	Resets statistics for specified test or group of tests
PauseTest	<TestName> <time_minutes> [<Comment>]	Pauses specified test or group of tests (up to 1440 min)
ResumeTest	<TestName>	Resumes paused test or group of tests

Note: instead specific TestName you can use the following group names (remember, parameters are case sensitive):

```
_AllGood
_AllBad
_AllUnknown
_AllWarning

_AllPing            _AllSMTP           _AllCPU
_AllTrace           _AllPOP3           _AllMemory
_AllTCP             _AllIMAP           _AllService
_AllUDP             _AllEMail          _AllProcess
_AllRAS             _AllMailRelay      _AllNTLog
_AllNTP                                _AllPerfCounter
_AllDNS             _AllURL            _AllDominantProcess
_AllDHCP            _AllHTTP           _AllRegistry
_AllLDAP            _AllSOAP           _AllWMI
_AllRadius          _AllOPC            _AllHddSMART
_AllDICOM           _AllCertificate    _AllFreeSpace
_AllTraffic         _AllDomain         _AllAVStatus
_AllNIS             _AllWebDavSpace    _AllLastUpdate
_AllSIP             _AllDHCPPool       _AllFirewallStatus

                                       _AllVMHostStatus
_AllODBC            _AllUNC            _AllVMHostCPU
_AllPostgre         _AllFolderSize     _AllVMHostMemory
_AllSybase          _AllFileExists     _AllVMHostDisk
_AllInterbase       _AllFileContents   _AllVMStatus
_AllMsSQL           _AllCountFiles     _AllVMCPU
_AllMySQL           _AllTextLog        _AllVMDisk
_AllOracle                             _AllVMMemory

_AllSNMP            _AllExternalPrg    _AllHPHealth
_AllSNMPTrap        _AllScript         _AllHPTemp
_AllSNMPTable       _AllShell          _AllHPFans
_AllTemp            _AllSSH            _AllHPPower
_AllHMMonitor                          _AllHPDisks

_AllCiscoHealth     _AllNetAppHealth   _AllJuniperHealth
_AllCiscoTemp       _AllNetAppTemp     _AllJuniperTemp
_AllCiscoFans       _AllNetAppDisks    _AllJuniperFans
_AllCiscoPower
```

```
  _AllBigIPHealth     _AllNScalerTemp
  _AllBigIPTemp       _AllNScalerStats
  _AllBigIPStats

  _AllQnapHealth      _AllSynHealth
  _AllQnapTemp        _AllSynTemp
  _AllQnapFans        _AllSynDiskLoad

  _AllUPSHealth       _AllApache
  _AllUPSLoad         _AllNginx
  _AllUPSCharge       _AllTomcat
  _AllUPSVoltageIn    _AllIIS
  _AllUPSVoltageOut
  _AllUPSTemp
  _AllUPSTime

  _AllPrinterStatus
  _AllPrinterLevels

  _AllRedfishHealth    _AllRMCPPing
  _AllRedfishTemp      _AllIPMIHealth
  _AllRedfishFans      _AllIPMITemp
  _AllRedfishVoltage   _AllIPMIFans
  _AllRedfishCurrent   _AllIPMIVoltage
  _AllRedfishPower     _AllIPMICurrent
  _AllRedfishSensor    _AllIPMIDiscrete


Examples:
 SetCurrentFolder  Root
 IncludeSubfolders yes

 DisableTest  _AllTCP
 EnableTest   _AllPing
 RefreshTest  _AllUnknown

 RefreshTest  my router
 EnableTest   server1
 PauseTest    mailserver  10

 ResolveMacros no
 SetTestParam  "Ping: www.nasa.gov" commentline01 %udv_admin_mail%
```

AckTestStatus	<TestName> [For <minutes> | Till ddMMyyyyHHmm [StopAlerts] [<Comment>]	Acknowledges failed test item(s)
ResetAcknowledgements	<TestName>	This command tells HostMonitor to clear "acknowledged" flag for specified test item(s)
SetTestParam	<TestName> <ParameterName> <Value>	Set parameters for the specified test or group of tests. ParameterName can be one of the following: timeout <number> changes communication timeout retries <number> changes number of retries username <name> changes account used for "Connect as" option password <pswd> changes password used for

				"Connect as" option
		comment	<text>	changes entire comment assigned to the item
		commentlineNN	<text>	changes specified line of the comment assigned to the item (NN is number from 1 till 99)
		testinterval	<min> | <HH:MM:SS>	changes execution interval for specified test items. Time interval can be specified in hh:mm:ss format or just as integer number that represents minutes (i.e. 5 is equivalent to 00:05:00, 60 is equivalent to 01:00:00)
		AlertProfile	<profile name>	changes alert profile
		AlertProfile2	<profile name>	changes second alert profile (when this feature enabled)
		Schedule	<profile name>	sets schedule assigned to the test
		TestBy	<name>	sets "Test by" parameter; you may provide agent name, hostmonitor or folder-specific string
		Threshold	<limit>	sets limits specified for the test (alert threshold). E.g. minimum free space for Drive Free Space test, minimum amount of free memory for Memory test, loss packet ratio limit for Ping test, limit for CPU load, upper limit for Process test, etc Also it sets CRC32 for HTTP test; hash for URL test
		ThresholdUp	<limit>	same as Threshold (e.g. upper limit for Process test, upper limit for UPS input voltage and so on)
		Threshold2	<limit>	sets 2nd limit for some tests, e.g. Jitter limit for Ping test, messages size limit for POP3 test, lower limit for Process test,
		ThresholdDown	<limit>	same as Threshold2 (e.g. lower limit for Process test, lower limit for UPS input voltage or lower limit for UPS battery temperature)
		Note: the following parameters used with ReplaceTestParam or ReplaceTestParamByID command changes test settings regardless of current parameter value:		
		usecommonlog	yes|no	turns on or off common logging
		reversealert	yes|no	turns on or off "reverse alert" option
		unknownasbad	yes|no	sets "Treat Unknown status as Bad" option
		warningasbad	yes|no	sets "Treat Warning status as Bad" option
		syncmastercounters	yes|no	turns on/off "Synchronize counters" property
		syncmasterstatus	yes|no	turns on/off "Synchronize status & alerts" test property

ReplaceTestParam	<TestName> <ParameterName> <Current. value> <New value>	Replaces a value of a given parameter for the specified test or group of tests. Unlike "SetTestParam" command, this one has a selective approach. It changes the value of a parameter only for the tests that have a current value equal to the <Current value> argument of the command. List of parameters equivalent to parameters of SetTestParam command

* Threshold (ThresholdUp) parameter can be used for the following tests:
  Ping, TCP, UDP, DNS, NTP, LDAP, POP3, IMAP, URL, HTTP, Certificate Expiration, Domain Expiration, SOAP, OPC, UNC, Drive Free Space (Windows, UNIX, NetApp, QNAP, Synology), Folder/File Size, Folder/File Availability, File Integrity, Compare Files, Count Files, Text Log, CPU, Memory, Process, Dominant Process, Performance Counter, WMI, Registry, Shell Script, External, SSH, ODBC Query, VM host CPU usage, VM host free memory, VM host free datastore space, VM guest CPU usage, VM guest free memory, VM guest free disk space, SNMP Get, SNMP Table, Network Traffic, Interfaces Status, Juniper Temperature, NetApp RAID Status, Synology Temperature, Synology Disk Load, Qnap Temperature, Qnap Fans, UPS Health, UPS Load, UPS Charge Level, UPS Input Voltage, UPS Output Voltage, UPS Temperature, UPS Remaining Time Apache, Nginx, Tomcat, IIS, Printer supply levels

* Threshold2 (ThresholdDown) parameter can be used for the following tests:
  POP3, Folder/File Availability, Process, Certificate Expiration, NetApp RAID Status, Qnap Fans, UPS Load, UPS Input Voltage, UPS Output Voltage, UPS Temperature, Apache, Nginx, Tomcat, IIS

* When you setup threshold for Traffic Monitor test using ReplaceTestParam command you should use the same unit as current one. E.g. If you set 8 Kbit/sec limit to the test, then the following command will not change threshold

```
ReplaceTestParam  TrafficTestSample Threshold "1 KB/sec" "2 KB/sec"
```

1 KB == 8Kbit but command will not set new limit because current threshold uses Kbit/sec units.
This command will change threshold

```
ReplaceTestParam TrafficTestSample Threshold "8 Kbit/sec" "2 KB/sec"
```

* When you setup threshold for Big-IP Temperature or Netscaler Temperature tests, HostMonitor will set all enable limits: internal, chassis, CPU, auxiliary temperarure limits.

Examples:

```
SetCurrentFolder   Root\Asia\Ping tests
IncludeSubFolders  no
SetTestParam       _AllPing  Timeout  2000

SetCurrentFolder   Europe
IncludeSubFolders  yes
SetTestParam       _AllCPU   UserName  test1
SetTestParam       _AllCPU   Password   pswd1
ReplaceTestParam   _AllTCP   timeout      2000   5000

SetTestParam       _AllPing  testinterval  5
SetTestParam       _AllPing  testinterval  00:02:30
ReplaceTestParam   _AllCPU   testinterval  5  00:15:00

SetTestParam       "M. router" AlertProfile  "E-mail to admin"
SetTestParam       _AllMemory  usecommonlog  yes
SetTestParam       _AllMemory  unknownasbad  no
ReplaceTestParam   _AllPing    TestBy  "hostmonitor"  "folder-specific"
ReplaceTestParam   _AllCPU     TestBy  "hostmonitor"  "agent - SouthWest domain"

SetTestParam       "main router"  Threshold     "50 %"
SetTestParam       "main router"  Threshold2    "50 ms"
SetTestParam       _AllMemory     Threshold     "20 %"
SetTestParam       _AllTraffic    Threshold     "55 KB/sec"
SetTestParam       _AllTraffic    Threshold     "33 pkt/min"
SetTestParam       _AllTraffic    Threshold     "22 pkt"
ReplaceTestParam   _AllTraffic    Threshold     "2 GB/sec"  "5 GB/sec"
ReplaceTestParam   _AllUPSTemp    ThresholdUp   65  55
ReplaceTestParam   _AllUPSTemp    ThresholdDown 15  10
```

```
ReplaceTestParam  _AllFreeSpace  Threshold     "20 %"  "17 %"
ReplaceTestParam  _AllFreeSpace  Threshold     "5 GB"  "8 GB"
ReplaceTestParam  _AllFreeSpace  Threshold     "6 GB"  "15 %"
SetTestParamByID   11054         Threshold     "10 MB"
```

ResetRecurrencesTest	<TestName>	Resets Recurrences counter to 0 for specified test. Note: after Recurrences counter is set to 0, HostMonitor will interpret ANY status assigned to the test by the next check as "new" status. E.g. if 1st check after you have used ResetRecurrencesTest command returns "Ok" status, HostMonitor will consider that previous status of the test was not "Ok" (either "Bad" or "Unknown"). This allows you to forcibly start actions that already were executed (e.g. for testing purpose).
ResetRecurrencesAll		Sets Recurrences counter to 0 for all tests in the folder.
ResetEventLogRefPoint	<TestName>	This command resets internal counters of the NT Event Log test so that the next time when the test is performed HostMonitor ignores all events that have happened before execution of this command. Please note: clocks on local and remote systems must be synchronized if you check event log on the latter, in order for this command to work correctly.
- note: the following commands work with specific test item(s) regardless of "setcurrentfolder" settings		
DisableTestByID	<TestID>	Disables test item specified by unique ID
EnableTestByID	<TestID>	Enables test item specified by unique ID
RefreshTestByID	<TestID> [forcelog]	Checks the status of the specified test immediately. Optional parameter "forcelog" tells HostMonitor to record test result into log file(s) regardless of logging mode and test result (effects just 1 test probe caused by "Refresh" command). In other words test result will be recorded even if you are using Brief logging mode and test status did not change.
RefreshIrregularTestByID	<TestID> [forcelog]	Command works similar to RefreshTestByID command - it tells HostMonitor to perform test probe immediately. In contrast to RefreshTestByID command, it can force execution even for test items that were configured with Irregular schedule
ResetTestByID	<TestID>	Resets statistics test item specified by unique ID
PauseTestByID	<TestID> <interval> [<Comment>]	Pauses test item specified by unique ID. Time interval should be specified in minutes (up to 1440 min)
ResumeTestByID	<TestID>	Resumes paused test item
AckTestStatusByID	<TestID> [For <minutes> | Till ddMMyyyyHHmm [StopAlerts] [<Comment>]	Acknowledges failed test item
ResetAcknowledgements ByID	<TestID>	This command tells HostMonitor to clear "acknowledged" flag for specified test item
SetTestParamByID	<TestID> <ParameterName> <Value>	Similar to SetTestParam command, you just need to specify unique ID of the test instead of test name
ReplaceTestParam ByID	<TestID> <ParameterName> <Current. value> <New value>	Similar to ReplaceTestParam command, you just need to specify unique ID of the test instead of test name

Examples:

```
EnableTestByID     412
RefreshTestByID    514
```

```
PauseTestByID          616   10    "pause for 10 min"

AckTestStatusByID   715   StopAlerts   maintenance
AckTestStatusByID   842   "comment"
AckTestStatusByID   842   StopAlerts  "comment 2"
AckTestStatusByID   842   FOR 25  "comment 3"
AckTestStatusByID   842   TILL 031220250544  "comment 4"

SetTestParamByID     178      Comment       my long ^M multulines ^M comment
SetTestParamByID     279      CommentLine02  address: 465 Whitefox Ave
SetTestParamByID     234      Schedule        "Weekdays, 24 hours"
ReplaceTestParamByID  1082  timeout          2000   5000
```

- global variable commands		
SetUserVariable	<VariableName> <VariableValue>	Sets the value of a variable (if such variable does not exist, creates a new variable)
SaveUserVariables		Saves changes
LoadUserVariables		Loads previously saved variables
- other		
FlushCommonLog		Tells HostMonitor to record into common log current test statuses of all test items except items that do not use common log and items that already have recorded (today!) their status into common log
FlushPrivateLogs		Similar to FlushCommonLog but performs the same operation for all test items that uses private log(s) These 2 commands can be useful for Log Analyzer in case when you are using Brief logging mode and for some reasons you do not want to use Midnight logging mode (e.g. you want to "flush" log records at noon instead of midnight or you want to "flush" log records for some specific private logs or you want to “flush” log records twice a day)
CreateReport	"report profile name" <target file name>	Generate the report to the specified file using specified report profile
StartProgram	<CommandLine>	Starts external program and continue to execute the script (do not wait until external program will terminate)
ExecuteProgram	<TimeToWait> <CommandLine>	Executes external program, waits until external program is terminated, and continues to execute the script. If parameter <TimeToWait> is not equal to 0, HostMonitor will "kill" the external application when the application is not finished within the given timeout (time defined in milliseconds). Be careful with this command, HostMonitor stops monitoring when executes external program by this command.
EnableAlerts		Enable alerts.
DisableAlerts		Disable all alerts (except “scheduled” actions). Note: if alerts are disabled then script can be launched manually (menu File->Execute script). Also you may setup built-in Scheduler to execute actions even when alerts are disabled. However if monitoring is stopped, Scheduler will be deactivated.
PauseAlerts	<interval>	Pause alerts for interval specified in minutes. In other words, all action profiles that usually were triggered by the change of test(s) status will not be executed within N minutes. All scheduled actions (those that are executed by built-in Scheduler) will continue to execute anyway.

PauseMonitor	<interval>	Pause monitoring for specified time (time should be specified in minutes)
StopMonitor		Stop monitoring
StartMonitor		Start monitoring
QuitMonitor		Quit HostMonitor

You can find an example of HMS script in HostMonitor's directory 'Examples\', file script1.hms.

Multiline variables

Starting from HostMonitor version 9.00 multiline variables supported. E.g. you may use %MailBody% or %HttpPage% variables as body of the script. This way you may setup HostMonitor to receive HM Script commands from mail server (see E-Mail test) or from some page on your web server and execute these commands. In other words, you may send e-mail with HM Script commands to HostMonitor and it will execute your e-mail.
E.g. you may setup HostMonitor to inform you about problems by e-mail and you may respond to HostMonitor by e-mail as well (e.g. pause or acknowledge failed items). Even more, HostMonitor may send confirmation back to you (e.g. you may assign to E-Mail test 2 actions: "Execute HM script" action and "Send e-mail" action using %MailFrom% variable as recipient's address).

If there is some invalid command within such multiline variable, HostMonitor will record information into system log file (as usually). Error description will tell you what exactly command within multiline variable is invalid and display 2 numbers (e.g. line #1:2) where 1st number represents line within HM script file where variable specified; 2nd number represents line within variable where invalid command specified.

Note: for security reasons commands StartProgram and ExecuteProgram restricted for HM Scripts when such commands specified within mail body, mail subject, HTTP page or HTTP header.
You may define parameters of StartProgram and ExecuteProgram commands using variables (e.g. StartProgram %MailSubj%), in such case HostMonitor will start external application specified in your e-mail but we do NOT RECOMMEND using such scripts for security reasons.
Also, please make sure you are using mail servers with secure connection!

Macros

When defining some of the alert action's parameters you can use special macro variables. There are 6 groups of macro variables:

1. variables that represent parameters of the test that had triggered an action;
   additional statistics;
   test method specific variables;
   variables specific to TCP and UDP tests ;
   variables specific to Service test;
   variables specific to Trace test;
   variables specific to URL, HTTP, SOAP and SIP tests;
   variables specific to DNS test;
   variables specific to Certificate Expiration test;
   variables specific to Domain Expiration test;
   variables specific to E-Mail test;
   variables specific to Drive Free Space test;
   variables specific to HDD SMART test;
   variables specific to file related test methods;
   variables specific to NT Event Log test;
   variables specific to Dominant Process test;
   variables specific to Firewall Status tests;
   variables specific to VM systems tests
   variables specific to SNMP Trap test;
   variables specific to Interfaces Status test;
   variables specific to NetApp Health test;
   variables spacific to NetApp RAID test;
   variables specific to HP iLO tests;
   variables specific to Redfish tests;
   variables specific to Printer Status, Printer Levels tests;
   variables specific to HM Monitor test;
   variables specific to SNMP Table test method;
2. variables that represent parameters of some explicitly specified test
3. variables that represent tests related to the same host
4. folder-related variables
5. HostMonitor status related macro variables
6. user defined variables also known as global macro variables
7. date & time variables

1. variables that represent parameters of the same test that had triggered an action

Macro variable	Description
Test properties	
%TestName%	The name of the test. Has the same value as %HostName%, which has been retained for backward compatibility
%HostName%	Represents the name of the test (obsolete, retained for backward compatibility. Please, use %TestName% macro instead)

%HostID%	Represents all numbers in the name of the test. HostMonitor removes all characters from the test name except decimal numbers and substitutes instead this macro. This macro can be useful when you need to send messages to numeric only pagers (beepers).
%TestID%	Represents unique ID of the test. TestID is always unique within an HML file
%Agent%	Represents a name of the remote agent that performs the test, this variable returns the string "*HostMonitor*" when the test is performed by HostMonitor
%AgentAddr%	This variable returns: - "localhost" when test performed directly by HostMonitor; - hostname or IP address specified for Passive RMA when test is performed by Passive agent; - address of Active RMA system when Active agent is connected to HostMonitor; - "0.0.0.0" when test should be performed by Active RMA but agent is not connected to HostMonitor.
%TestMethod%	Represents short description of a testing method
%MethodID%	Returns integer number that represents test method (test that has triggered action execution)

Ping	0	SNMP Get	18	HTTP	36
TCP	1	NT Event Log	19	Text Log	37
URL	2	CPU Usage	20	Shell Script	38
Disk free space	3	File Compare	21	Temperature Monitor	39
Folder size	4	ODBC	22	Network Traffic	40
File Availability	5	SMTP	23	SNMP Trap	41
External	6	POP3	24	WMI	42
SSH	7	IMAP	25	Mail relay	43
File Integrity	8	DNS	26	DICOM	44
Oracle	9	LDAP	27	Dominant Process	45
UNC	10	Trace	28	DHCP	46
Interbase	11	Count Files	29	HM Monitor	47
MS SQL	12	RAS	30	SOAP/XML	48
MySQ	13	Performance C.	31	E-Mail	49
PGSQL	14	Active Script	32	Certificate expiration	50
Sybase	15	UDP	33	Domain expiration	51
Process	16	NTP	34	Registry	52
Service	17	Radius	35	SNMP Table	53
Memory	54	Cisco Health	74	Synology Load	94
VM Host Status	55	Cisco Temp	75	Qnap Health	95
VM Host CPU	56	Cisco Fans	76	Qnap Temp	96
VM Host Mem	57	Cisco Power	77	Qnap Fans	97
VM Host Disk	58	Junip Health	78	BIG_IP Health	98
VM Guest Status	59	Junip Temp	79	BIG_IP Temp	99
VM Guest CPU	60	Junip Fans	80	BIG_IP Stats	100
VM Guest Mem	61	UPS Health	81	Netscaler Temp	101
VM Guest Disk	62	UPS Load	82	Netscaler Stats	102
OPC	63	UPS Charged	83	WebDav	103
SMART	64	UPS Volts In	84	SIP	104
Interface Status	65	UPS Volts Out	85	Antivirus Status	105
ILO Health	66	UPS Temp	86	Last OS Update	106
ILO Temp	67	UPS Time	87	RCMP Ping	107
ILO Fans	68	Apache	88	IPMI Health	108
ILO Power	69	Nginx	89	IPMI Temperature	109
ILO Disks	70	Tomcat	90	IPMI Fans	110
Netapp Health	71	IIS	91	IPMI Voltage	111
Netapp Temp	72	Synology Health	92	IPMI Current	112
Netapp Disks	73	Synology Temp	93	IPMI Discrete	113
DHCP Pool	114			Redfish Fans	120
Printer Status	115			Redfish Voltage	121
Printer Level	116			Redfish Current	122
Firewall	117			Redfish Power	123
Redfish Health	118			Redfish Sensor	124
Redfish Temp	119				

%TestedObjectInfo%	Provides information about tested object, variable returns string value like 'MS SQL database "MainLog" on 192.168.10.15' or 'Win32 service "FAX" on 192.100.10.5'. This variable offers more information than %TestMethod% variable
%AccountSet%	Returns username set for the test item (including URL, HTTP, OPC, SOAP, Mail Relay, Apache, NGINX, Tomcat, POP3, IMAP and many other tests)
%Interval%	The time between two consecutive checks defined for the test
%ScheduleName%	Name of a schedule assigned to the test

%AlertProfile%	Name of the action profile
%AlertThreshold%	Represents condition to set “Bad” status. E.g. for Drive Free Space test this macro will represent minimum limit of free space defined for the test; for TCP test it will display timeout; for CPU Usage test it will show maximum limit for CPU usage value. %AlertThreshold% variable for Ping test may return values like: 50% lost; Timeout: 1000 ms - this format used when "jitter" option is not enabled 50% lost; Jitter: 100 ms - when both "lost" and "jitter" alert options used Jitter: 100 ms - when only "jitter" alert option enabled
%AlertThresholdValue%	This variable works similar to %AlertThreshold% variable but it returns numeric value only (without any correspondent text comment). E.g. %AlertThreshold% variable may return text like “Absent, MaxAge: 60” when it is used in action triggered by “File/Folder Availability” test method. In the same case %AlertThresholdValue% would return “60”. For Traffic Monitor test method it converts any units specified for test item threshold to Kbit/sec or pkt/sec units. If %AlertThreshold% returns "500 MB/sec" then %AlertThresholdValue% will return 4096000 For Ping test this variable returns timeout value or jitter threshold (if "Jitter" option enabled for the test)
%MasterTest%	Master test name (provides information about 1st master test only)
%MasterTests%	Returns list of master tests (items separated by CRLF characters). If test item depends on single master test or does not depend on any test, %MasterTests% and %MasterTest% variables are equivalent
%DependantTestsName%	If Master test triggers some actions, this variable provides short list of dependant items (shows test names)
%DependantTestsPath%	Similar to %DependantTestsName%, shows full path to dependant test items (including folder name). Note: there is option that allows you to specify how many items should be displayed. This option is not accessible thru GUI however you may add line like MaxDependantItemsInMacro=10 into [Misc] section hostmon.ini file and restart HostMonitor (number of items should be in range 1..15; default value 5)
%PrivateLog%	The specified private log file name
%RelatedURL%	Related URL (without a hint)
%RelatedURLHint%	If you set the Related URL field of a test item with an additional optional hint string (e.g. [title=GOOGLE]https://www.google.com), %RelatedURLHint% variable will return only a hint (GOOGLE in this case)
%TaskComment%	Test's comment (whole comment, all lines separated by CRLF)
%CommentLine1%	Represents 1st line of test's comment
%CommentLine2%	Represents 2ndt line of test's comment
...	...
%CommentLine99%	Represents 99th line of test's comment
%CommentID%	This macro is similar to %HostID%, but uses a test's comment instead the test's name.
%CreatedTime%	The time when the test was created
%ModifiedTime%	The time when the test was last modified
Current test state	
%DateTime%	Current date and time

%DATE%	Current date
%TIME%	Current time
%LastTestTime%	Time when the test was last performed
%TestProbeTime%	Test execution time in milliseconds
%Reply%	Represents reply value (depends on the test type, it can be reply time, disk's free space, message from NT Event Log, etc). HostMonitor may encode special characters in %Reply% variable. E.g. it replaces CRLF chars with \r\n when you are using variable for SQL Query; or replaces CRLF with when you are using %Reply% variable for e-mail in HTML format (Send E-mail action)
%Reply_DQuotes%	Represents Reply field where single quotation marks replaced with double quotation marks
%Reply_SQuotes%	Represents Reply field where double quotation marks replaced with single quotation marks
%Reply_CStyle%	Represents "Reply" field with some characters replaced by special sequences conforming to C language standards: - characters ASCII 13 (line feed) and ASCII 10 (new line) replaced with **\r** and **\n** correspondingly; - characters ASCII 9 (tab) replaced with **\t** - characters ASCII 39 (quotation mark) replaced with **\'** - character ASCII 92 (back slash) replaced with \\ - and so on this variable could be useful for writing Java scripts (e.g. for Custom HTML report) or SQL Query for ODBC log.
%Reply_AsIS%	HostMonitor may encode special characters in %Reply% variable. E.g. it replaces CRLF chars with \r\n when you are using variable for SQL Query; or replaces CRLF with when you are using %Reply% variable for e-mail in HTML format (Send E-mail action). For %Reply_AsIS% variable HostMonitor does not perform any special encoding.
%Reply_Number%	Represents actual numeric value of Reply field as a real number. E.g. for the Reply field containing '12.01 Kb', %Reply_Number% will return '12298.24'. It returns zero when the content of the field is a string that cannot be converted into a number.
%Reply_Integer%	Represents actual numeric value of reply field as an integer number. E.g. for the Reply field containing '12.01 Kb', %Reply_Integer% will return '12298'. It returns zero when the content of the field is a string that cannot be converted into a number.
%Status%	Status of the test (text)
%StatusID%	A 2 digits number that represents status of the test 00- Not Tested 01- Host is Alive 02- No Answer 03- Unknown 04- Unknown host 05- Checking 06- Resolving 07- Ok 08- Bad 09- Disabled 10- Bad Contents 11- WaitForMaster 12- OutOfSchedule

	13- Paused 14- Normal 15- Warning
%SimpleStatus%	This macro may return one of the following text values: - "UP" for good statuses (Host is Alive, Ok); - "DOWN" for any bad status (No answer, Bad, Bad Contents); for Warning status when "Treat Warning as Bad" option is enabled; for Unknown status when "Treat Unknown as Bad" option is enabled - "UNKNOWN" if status of the test is "Unknown" or "Unknown host" and "Treat Unknown as Bad" option is disabled; variable also returns "UNKNOWN" for statuses like WaitForMaster, OutOfSchedule, Paused. - "WARNING" when status of the test is "Warning" and "Treat Warning as Bad" option is disabled
%CurrentStatusIteration%	The number of consecutive test probes resulting in the same status as the current one
%Recurrences%	Similar to %CurrentStatusIteration% but this counter is resetted by HostMonitor when test status changes from "bad" to "good", from "good" to unknown or warning and vice versa. While changes between "Ok", "Host is alive" and "Normal" statuses do not reset the counter, changes between "Bad" and "No answer" do not reset the counter either. "Threat Unknown status as Bad" and "Treat Warning status as Bad" options determine behaviour of the counter for Unknown and Warning statuses. In other words: %CurrentStatusIteration% relates to %Status% while %Recurrences% relates to %SimpleStatus%. This is important counter, you probably will use this counter for "advanced" actions.
%CurrentStatusDuration%	Represents the duration of current (simple) status of the test, shows time interval in "[N days] HH:MM:SS" format
%CurrentStatusDuration_sec%	Represents the duration of current (simple) status of the test, shows time in seconds
%FailureID%	This variable allows you to use unique failure ID as parameter of the actions. HostMonitor assigns unique failure ID for each failed test and keeps the same ID when test fails several times in a row (note: "failure" conditions may depend on "Treat Unknown as Bad" or "Treat Warning as Bad" test properties). HostMonitor assigns different IDs for different test items; it assigns new unique ID when test restores "good" status and then fails again. HostMonitor sets %FailureID% variable to 0 when test has "good" status.
%LastFailureID%	While %FailureID% variable represents unique failure ID for each current problem, %LastFailureID% returns ID of previous failure of the test
%PauseComment%	Represents comment specified for test item when operator paused test execution
The following variables may be used in the expressions that define Normal and Warning statuses (see Optional status processing section of the manual). These variables may be used as parameters of some actions as well, but usually this does not have sense.	
%SuggestedStatus%	Status that will be used for the test item, unless "normal" or "warning" options modify the status. Variable may return one of the following values: Host is alive, Ok, No answer, Bad, Bad contents, Unknown or Unknown host
%SuggestedSimpleStatus%	Similar to %SimpleStatus% but provides information about "suggested" status (test probe already responded with some result but %Status%, %Reply% and other regular counters not modified yet)
%SuggestedReply%	Represents "suggested" reply value ("Tune up reply" option allows you to change Reply value after test execution)

%SuggestedReply_DQuotes%	Represents "suggested" Reply value where single quotation marks replaced with double quotation marks
%SuggestedReply_SQuotes%	Represents "suggested" Reply value where double quotation marks replaced with single quotation marks
%SuggestedReply_AsIS%	HostMonitor may encode special characters in %SuggestedReply% variable. E.g. it replaces CRLF chars with \r\n when you are using variable for SQL Query; or replaces CRLF with when you are using %Reply% variable for e-mail in HTML format (Send E-mail action). For %SuggestedReply_AsIS% variable HostMonitor does not perform any special encoding.
%SuggestedReply_Integer%	Works similar to %Reply_Integer% variable but provides information about "suggested" reply value. E.g. if %SuggestedReply% shows '12.01 Kb', %SuggestedReply_Integer% will return '12298'. This variable returns zero when SuggestedReply is a string that can not be converted into a number
%SuggestedLastReply%	"Suggested" reply value returned by previous check
%SuggestedRecurrences%	Similar to %Recurrences% counter. Difference is HostMonitor sets this variable before Normal and Warning expressions processing. If you do not use optional status processing or both logical expressions return False, then %Recurrences% will be equivalent to %SuggestedRecurrences%
%FailureIteration%	The number of consecutive failed test probes. Shows 0 when test returns "good" result. In contrast to other counters (like %Recurrences%, %CurrentStatusIteration%, %FailedCnt%, etc) that depend on result of optional status processing (Normal and Warning expressions), this counter always tells you about REAL result of test probe. E.g. when test returns "bad" status, HostMonitor increments this variable even if "Use normal status…" option tells HostMonitor to change test status to Normal. See processing sequence for details
If test status was acknowledged	
%AcknowledgedAt%	Represents the date and time when test status was acknowledged
%AcknowledgedDate%	Represents the date when test status was acknowledged
%AcknowledgedTime%	Represents the time when test status was acknowledged
%AcknowledgedBy%	Shows the name of the operator who have acknowledged the test status
%AckComment%	Shows the comment which was provided for "acknowledge" operation
These 5 variables return empty string for non-acnowledged test items.	
%AckResponseTime%	Shows time elapsed sinse test failure till status acknowledgement by operator. This variable returns time in hh:mm:ss format; it may return empty string when test has Ok status; variable returns "not acknowledged" string when test has Bad or Unknown not acknowledged status
%AckRecurrences%	Represents the number of test probes which have returned similar (bad or unknown) result after it was already acknowledged. Returns 0 for non-acknowledged test items. For example if the test returned "bad" status during five consecutive probes, then %Recurrences% variable will be equal 5. If the user has acknowledged the bad status after the second probe then %AckRecurrences% will be equal 3 (5-2=3). This variable is useful when you want to configure alert profile to launch different actions for "non-acknowledged" and "acknowledged" test items. E.g. if condition

	to trigger action execution looks like ('%SimpleStatus%'=='DOWN') and (%AckRecurrences%==1), HostMonitor will start action when user confirmed status and test failed once again (after acknowledgement).
%AcknowledgedJustNow%	Advanced mode action and variables like %AckRecurrences%, %AckComment% allow starting special actions when Bad test status was acknowledged by the operator. Such actions could be started after the following test probes while sometimes you may need to start action right after acknowledgment. If you set advanced mode action using **%AcknowledgedJustNow%** variable, then HostMonitor may trigger action when operator acknowledges test status without waiting for the next test probe. This way you may pause or disable test (if you need) right after acknowledgement and still trigger special action(s). For example, you may use expressions like %AcknowledgedJustNow% and ("%Reply%" > "90 %") %AcknowledgedJustNow% and (("%AckComment%" getword 1)=="Attention") Note: HostMonitor may trigger such action even if operator chooses "acknowledge and STOP alerts" option; "New ack comment" operation may trigger such alerts as well.
Previous state	
To explain following variables we need to explain difference between terms “PreviousStatus” and “LastStatus”. “PreviousStatus” is status which test had before current status. “LastStatus” is status which test had after previous check. For example for the last 5 probes test had following statuses: #1-Bad, #2-Unknown, #3-Ok, #4-Ok, #5-Ok (current status is #5-Ok). In this case “PreviousStatus” is #2-Unknown but “LastStatus” is #4-Ok.	
%LastStatus%	Status of the test after previous check (LastStatus)
%LastSimpleStatus%	Similar to %SimpleStatus% but provides information about last test status
%LastReply%	Reply value returned by previous check
%LastReply_CStyle%	Represents “Reply” value returned by previous check with some characters replaced by special sequences conforming to C language standards: - characters ASCII 13 (line feed) and ASCII 10 (new line) replaced with **\r** and **\n** correspondingly; - characters ASCII 9 (tab) replaced with **\t** - characters ASCII 39 (quotation mark) replaced with **\’** - character ASCII 92 (back slash) replaced with \\ - and so on this variable could be useful for writing Java scripts (e.g. for Custom HTML report) or SQL Query for ODBC log.
%LastReply_AsIS%	HostMonitor may encode special characters in %LastReply% variable. E.g. it replaces CRLF chars with \r\n when you are using variable for SQL Query; or replaces CRLF with when you are using %Reply% variable for e-mail in HTML format (Send E-mail action). For %LastReply_AsIS% variable HostMonitor does not perform any special encoding.
%PreviousStatus%	The status, which the test had before last status change
%PreviousStatusTime%	Represents time when “PreviousStatus” was assigned to the test
%PreviousStatusDuration%	Represents the duration of the "PreviousStatus”. Shows time interval in “[X days] HH:MM:SS” format.
%PreviousStatusDuration_Sec%	Represents the duration of the “PreviousStatus” in seconds.
Statistical information	
%StatusChangedTime%	The time when the status last changed

%StatusChangesCnt%	The number of times the status has changed
%TotalTests%	Overall tests performed
%TotalTime%	The time the test has been in monitoring
%FailedCnt%	The number of "Bad" test results
%PassedCnt%	The number of "Good" test results
%UnknownCnt%	The number of "Unknown" test results
%AliveTime%	The overall time the test has had a "Good" status
%DeadTime%	The overall time the test has had a "Bad" status
%UnknownTime%	The overall time the test has had an "Unknown" status
%AliveRatio%	"Good" to overall tests ratio, in percent
%DeadRatio%	"Bad" to overall tests ratio, in percent
%UnknownRatio%	"Unknown" to overall tests ratio, in percent
%AverageReply%	The average value of the results obtained
%MinReply%	The minimum value of the results obtained
%MaxReply%	The maximum value of the results obtained

Note: If you are using %AverageReply%, %MinReply% or %MaxReply% variables for Custom HTML Report or HTML e-mail template, HostMonitor will use “human readable” format. E.g. if variable value is ‘10485760’, HostMonitor will show ’10 GB’ instead.

Another 72 new variables provide access to additional test statistics when “Store historical data in the file” option is enabled. You may get min/max/average reply and alive/dead/unknown ratio for several time intervals.

Today’s test results	Yesterday's results
%StatTODAY_MinReply%	%StatYESTERDAY_MinReply%
%StatTODAY_MaxReply%	%StatYESTERDAY_MaxReply%
%StatTODAY_AverageReply%	%StatYESTERDAY_AverageReply%
%StatTODAY_AliveRatio%	%StatYESTERDAY_AliveRatio%
%StatTODAY_DeadRatio%	%StatYESTERDAY_DeadRatio%
%StatTODAY_UnknownRatio%	%StatYESTERDAY_UnknownRatio%
Results for last 24 hours	Results for last 48 hours
%Stat24Hours_MinReply%	%Stat48Hours_MinReply%
%Stat24Hours_MaxReply%	%Stat48Hours_MaxReply%
%Stat24Hours_AverageReply%	%Stat48Hours_AverageReply%
%Stat24Hours_AliveRatio%	%Stat48Hours_AliveRatio%
%Stat24Hours_DeadRatio%	%Stat48Hours_DeadRatio%
%Stat24Hours_UnknownRatio%	%Stat48Hours_UnknownRatio%
Results for current week	Results for last week
%StatThisWeek_MinReply%	%StatLASTWeek_MinReply%
%StatThisWeek_MaxReply%	%StatLASTWeek_MaxReply%
%StatThisWeek_AverageReply%	%StatLASTWeek_AverageReply%
%StatThisWeek_AliveRatio%	%StatLASTWeek_AliveRatio%
%StatThisWeek_DeadRatio%	%StatLASTWeek_DeadRatio%
%StatThisWeek_UnknownRatio%	%StatLASTWeek_UnknownRatio%
Results for last 7 days	Results for last 14 days
%Stat7Days_MinReply%	%Stat14Days_MinReply%

%Stat7Days_MaxReply%	%Stat14Days_MaxReply%
%Stat7Days_AverageReply%	%Stat14Days_AverageReply%
%Stat7Days_AliveRatio%	%Stat14Days_AliveRatio%
%Stat7Days_DeadRatio%	%Stat14Days_DeadRatio%
%Stat7Days_UnknownRatio%	%Stat14Days_UnknownRatio%
Results for last 30 days	Results for last 60 days
%Stat30Days_MinReply%	%Stat60Days_MinReply%
%Stat30Days_MaxReply%	%Stat60Days_MaxReply%
%Stat30Days_AverageReply%	%Stat60Days_AverageReply%
%Stat30Days_AliveRatio%	%Stat60Days_AliveRatio%
%Stat30Days_DeadRatio%	%Stat60Days_DeadRatio%
%Stat30Days_UnknownRatio%	%Stat60Days_UnknownRatio%
Results for current month	Results for last month
%StatThisMonth_MinReply%	%StatLASTMonth_MinReply%
%StatThisMonth_MaxReply%	%StatLASTMonth_MaxReply%
%StatThisMonth_AverageReply%	%StatLASTMonth_AverageReply%
%StatThisMonth_AliveRatio%	%StatLASTMonth_AliveRatio%
%StatThisMonth_DeadRatio%	%StatLASTMonth_DeadRatio%
%StatThisMonth_UnknownRatio%	%StatLASTMonth_UnknownRatio%

For example, you may use these variables for Custom HTML Report templates; also you may create View and use these Views for any kind of reports. For example you may create SLA report with test items that show degradation in performance (this week is worse than previous week) using “Select items using expression” option with simple expression:

%StatThisWeek_AliveRatio% < %StatLASTWeek_AliveRatio%

Test specific macro variables	
%HostAddr%	Represents the host name (or IP address) of the target system for the following tests: Ping, TCP, URL, HTTP Oracle, Interbase, MS SQL, MySQL, Sybase, Postgre, Process, Service, NT Log, CPU Usage, SNMP, SMTP, POP3, IMAP, DNS, DHCP, LDAP, UDP, NTP, RADIUS, DICOM, UNC, Drive Free Space, Temperature Monitor, Traffic Monitor, Dominant Process, Performance Counter, WMI and Mail Relay. Also it can be used in actions triggered by file related test methods: Count Files, Text Log, Compare Files, File Integrity, Folder/File size, File/Folder Availability and Disk Free Space. When you are using this variable for action assigned to file related test method, HostMonitor analyzes path to target file and returns name of target server or "localhost" when test item checks local file. Note: if you setup test using path to mapped network drive (instead of using UNC path), this variable will return "localhost".
%HostAddrB%	Variable works similar to %HostAddr% variable, it returns host name without back slashes. E.g. if path to the file specified as \\sqlserver5\shareddisk1\file5 then %HostAddr% will return \\sqlserver5 while %HostAddrB% will return sqlserver5
%IP4%	IP address of the host checked by the test item (also %ip% variable can be used). "Normally" IP address is not applicable for some test methods: RAS, SNMP Trap, ODBC, External, Active Script and Shell Script. However when you add new test item using Network Map window,

	HostMonitor sets fixed IP address (address of the selected host) to such tests. This allows to link External/Script/ODBC tests to specific host on the map. Also Network Map offers 2 menu items for such tests: - Set fixed IP - Clear fixed IP For other tests IP address can be discovered by HostMonitor or Remote Monitoring Agent (even if you provide hostname as target host)
%TestTimeout%	Represents timeout specified for test item, in milliseconds. If timeout is not specified or not applicable, variable returns 0
the following variables have sense for Ping test items	
%Jitter%	Amount of variation in response time, in milliseconds Note: when you setup Ping test with "Alert if Jitter.." option disabled and "Lost ratio" option set to 100% and you are not using Lost, Received or Jitter display option then HostMonitor (or RMA) will wait for SINGLE received ICMP packet and %Jitter% variable will be set to -1 (unused)
%LostRatio%	Ratio of lost packets to total transmitted packets
the following variable has sense for TCP and UDP test items, for other tests this macro returns an empty string	
%ServerReply%	Represents data received from tested server (limited to first 512 bytes). Non-printable characters represented by sequences formatted **%XX** where XX is a hexadecimal code of a character (byte). If TCP test was not configured to check reply from the server (check TCP connection only), variable will return empty string.
the following variables have sense for "Service" test only, for other tests these macros return an empty string	
%ServiceComp%	The name of the target computer
%ServiceName%	The name of the service
the following variables have sense for "Trace" test only, for other tests these macros return an empty string	
%TraceBrief%	Route to the host. Contains IP addresses only
%TraceFull%	Route to the host. Contains hop number, IP address, and reply time for each hop
%TraceSlowestNode%	Position of the slowest node in the route
%TraceSlowestHost%	IP address of the slowest host in the route
%TraceSlowestTime%	Responce time of the slowest host in the route
%TraceLastNode%	Position of the last responsive host in the route
%TraceLastHost%	IP address of the last responsive host in the route
%TraceLastTime%	Responce time of the last responsive host in the route
the following variables have sense for "URL", "HTTP", "SOAP" and "SIP" tests only, for other tests these macros return an empty string	
%HostURL%	Represents URL used for the test
%HttpCode%	HTTP status code received from the server. Also this variable may return winsock error codes in case web server is not accessible (e.g. you have specified incorrect server name)
%HttpHeader%	Complete HTTP header received from the server
%HttpPage%	Represents contents of the monitored web page (first 32768 (32K) characters of the web page if test was performed by HostMonitor; first 2048 (2K) characters of the page if test was performed by RMA). Variable may be empty if you setup URL test item to check HTTP response only, without checking content or CRC of the page. HTTP test returns an

	empty string if a HEADER request is used. It also returns an empty string when a monitored web server does not respond.
the following variables provide information about the results of DNS tests	
%DnsResult%	Provides information about all entities received from DNS server (items separated by CRLF characters)
%DnsResults%	Provides information about 1st entity only
variables for Certificate Expiration test method	
%CertIssuer%	Shows information about the certificate issuer
%CertSubject%	Shows information about the certificate subject
%CertIssuerShort%	Short information about the certificate issuer
%CertSubjectShort%	Short information about the certificate subject
%CertValidFrom%	Shows the date that the certificate issuer specified as the start date for the certificate.
%CertValidTill%	Shows expiration date for the certificate
variables for Domain Expiration test method	
%DomainName%	Domain name specified for the test
%DomainExpirationDate%	Expiration date for specified domain
variables for E-Mail test method	
%MailFROM%	Represents address of the sender
%MailTO%	Represents recipient address
%MailSUBJ%	Shows e-mail subject
%MailBODY%	Returns e-mail body (up to 16KB)
%MailBodyNoQuotes%	Content of the mail (up to 16KB) without the following characters: ' “ [ ]
%MailLine1%	Represents 1st line of e-mail body
%MailLine2%	Represents 2nd line of e-mail body
%MailLine99%	Represents 99th line of e-mail body
variables for ODBC Query tests	
%ODBCField1%	Value of 1st specified field
%ODBCField2%	Value of 2nd specified field
the following variables have sense for "Drive Free Space" test only, providing information about drive with smallest amount of free space (or drive with minimal percentage of free space when "%" alert options is selected):	
%DiskID%	Drive ID (e.g. C:)
%DiskLabel%	Drive label
%DiskSize%	Capacity of the disk
%DiskFreeSize%	Amount of free space
%DiskFreePercent%	Percentage of free space
the following variables have sense for "HDD SMART" test only, providing information retrieved from the selected hard disk	
%Disk_Name%	Name of the selected disk
%Disk_Temp%	Current hard disk temperature (Celsius)
%Disk_Hours%	Count of hours in power-on state. On some disks manufactured before 2005 this value may advance erratically and/or reset to zero periodically
%Disk_Relocated%	Count of reallocated sectors represents a count of the bad sectors that have

	been found and remapped
%Disk_Pending%	Count of "unstable" sectors waiting to be remapped
%Disk_Uncorrectable%	The total count of uncorrectable errors when reading/writing a sector. A rise in the value of this attribute indicates defects of the disk surface and/or problems in the mechanical subsystem
%Disk_SpinupTime%	Average time of spindle spin up from 0 RPM to fully operational speed (milliseconds)
%Disk_SpinupRetries%	Count of retry of spin start attempts. This attribute stores a total count of the spin start attempts to reach the fully operational speed (under the condition that the first attempt was unsuccessful). An increase of this attribute value is a sign of problems in the hard disk mechanical subsystem
%Disk_ErrorRate%	The rate of hardware read errors that occurred when reading data from a disk surface. The value has different structure for different vendors
%Disk_Timeouts%	The count of aborted operations due to hard disk timeout
%Disk_AlertReason%	ID of the counter that triggered “bad” status for the disk, e.g. 194 for critical temperature; 198 for uncorrectable errors out of range (0 when all disks are healthy)
%Disk_AlertValue%	Current value of the counter that triggered “bad” status for the disk
the following variables provide information about the file detected by Folder/File Availability test method or the file processed by other file-related test methods (Text Log, Folder/File Size and Compare Files) Note: These variables provide information about file when tests performed by HostMonitor directly or tests performed by Passive or Active RMA for Windows. Variables return empty string when tests performed by RMA for UNIX	
%FileName%	Name of the file. Useful when you setup the test using wildcards or variables in “filename” field. This variable can be used for File/Folder Availability, Text Log, Folder/File Size and Compare Files test methods.
%FilePath%	Full path without filemask (Count Files and Folder/File Size tests only). Folder/File Size test - if test checks folder specified without trailing slash, variable will return parent folder path
%FileSize%	Size of the file (Folder/File Availability test method only)
%FileTime%	Modification time (Folder/File Availability test method only)
%FileAge_Min%	File age in minutes (Folder/File Availability test method only)
%FileAge_Hour%	File age in hours (Folder/File Availability test method only)
%FileAge_Day%	File age in days (Folder/File Availability test method only)
%FileName2%	Shows name of the 2nd file (if specified) for Compare Files test method. Useful when you are using variables or wildcards in filename (instead of static name).
the following variables have sense for "NT Event Log" test only, they represent parameters of the last "Bad" event detected:	
%NTEventSource%	Event source. Identifies the software that logged the event
%NTEventComp%	Name of the computer where the event occurred
%NTEventTime%	Time of the event
%NTEventType%	Type of the event
%NTEventTypeName%	Type of the event (string, like 'Error', 'Warning', 'Success audit', etc)
%NTEventID%	Event identifier

%NTEventUser%	Represents the user name if an event is attributed to a specific user
%NTEventText%	Event description
%NTEventTextNoQuotes%	Event description, text string without the following characters: ' " [ ] CR LF (useful for optional status processing and advanced mode actions)
the following variables provide information about previous detected event:	
%PrevNTEventSource%	Event source. Identifies the software that logged the event
%PrevNTEventComp%	Name of the computer where the event occurred
%PrevNTEventTime%	Time of the event
%PrevNTEventType%	Type of the event
%PrevNTEventID%	Event identifier
%PrevNTEventUser%	Provides user name if the event is attributed to a specific user
%PrevNTEventText%	Event description
%PrevNTEventTextNoQuotes%	Event description, text string without the following characters: ' " [ ] CR LF (useful for optional status processing and advanced mode actions)
the following variables provide number of new events when test set with “Report about last event but count ALL” option	
%NTEvents_BadCnt%	Number of new “bad” events
%NTEvents_GoodCnt%	Number of new “good” events
the following variables provide information about the process detected by Dominant Process test method	
%ProcessName%	Name of the process
%ProcessID%	PID (process ID or process identifier)
%ProcessOwner%	Owner of the process (account name)
the following variables provide information about firewall settings detected by Firewall Status test method	
%Firewall_StatusStr%	Firewall status string like "dom=111uuuuu pub=11101110 std=11uuuuuu"
%Firewall_ReasonStr%	Reason for "Bad" test status, like "LogDroppedPackets disabled (domain profile)"
the following variables provide information about detected host or guest system (e.g. guest OS with lowest amount of free memory or system with highest CPU usage). VM system group of tests	
%VMName%	guest name
%VMCPUusage%	CPU usage (%)
%VMFreeMem%	free memory (%)
%VMVolume%	disk volume name (applicable for VM Ware systems only)
%VMFreeDisk%	disk free space (%) (applicable for VM Ware systems only)
the following variables provide information about network interfaces checked by Interfaces Status test method	
%InterfacesDOWN_Index%	List of interfaces indexes which status not UP (separated by commas)
%InterfacesDOWN_Name%	List of interfaces descriptions which status not UP, separated by CRLF
%InterfacesChanged_Index%	List of interfaces indexes which status has been changed (separated by commas)
%InterfacesChanged_Name%c	List of interfaces descriptions which status has been changed (separated by CRLF)
the following variables supported by NetApp Health test method	
%DS_MaxUsedPercent%	The percentage of space currently in use or reserved by the fullest file system
%DS_MaxUsedINodesPercecnt%	The percentage of inodes currently in use by the fullest file system

the following variables supported by NetApp RAID test method	
%DS_ActiveCount%	The number of disks which are currently active, including parity disks
%DS_ReconstructingCount%	The number of disks which are currently being reconstructed
%DS_ReconstrparityCount%	The number of parity disks which are currently being reconstructed
%DS_VerifyingparityCount	The number of parity disks which are currently being verified
%DS_ScrubbingCount%	The number of parity disks which are currently being scrubbed
%DS_FailedCount%	The number of disks which are currently broken
%DS_SpareCount%	The number of available spare disks
%DS_AddingSpareCount%	The number of spare disks which are currently being added into a RAID group
%DS_PrefailedCount%	The number of prefailed disks marked for rapid raid recovery
%DS_OutdatedCount%	The number of outdated disks
the following variables supported by HP iLO tests (Health, Temp, Fans, Power, Disks)	
%HealthData%	If some problem detected, shows problem description like "STORAGE STATUS: Degraded"; otherwise reports status of all checked components, e.g. BIOS HARDWARE: OK POWER SUPPLIES: OK PROCESSOR: OK FANS: OKc
the following variables supported by Redfish Health tests	
%RF_SysInfo%	- detailed information about system
%RF_SysModel%	- system model
%RF_SysName%	- system name
%RF_HostName%	- host name
%RF_Description%	- description
%RF_Manufacturer%	- manufacturer
%RF_BIOS%	- BIOS version
%RF_SystemID%	- system ID
%RF_PowerState%	- power state
%RF_LastResetTime%	- last reset time
%RF_LastBoot%	- last boot
%RF_SysStatus%	- system status
%RF_CPUModel%	- CPU model
%RF_CPUCores%	- CPU cores
%RF_CPUStatus%	- CPU status
%RF_MemMirroring%	- memory mirroring
%RF_MemTotal%	- total amount of memory
%RF_MemStatus%	- memory status
%RF_TPMType%	- TPM type
%RF_TPMStatus%	- TPM status
%RF_Devices%	- information about storage devices
the following variables supported by Redfish Temperature, Fans, Redfish Voltage, Current, Power and Sesnor tests	
%RF_CHASSI%	- name of the chassi where the sensor is located

%RF_CONTEXT%	- context (location) of the sensor
the following variables applicable for Printer Status and Printer Supply Levels tests	
%PrinterDetails%	Printer Status test: name of the printer, description, location and information about the problem(s).
%PrinterDetails%	Printer Supply Levels test: name of the printer, description, location and information about all avilable supplies.
the following variable applicable for SSH tests	
%NewHostKeyWarning%	Variable returns 0 or 1. If "*autosave new key, but set Warning test status when key changed*" option is used but you want to avoid this Warning status for some specific test items or some specific test results, you may use this variable for optional status processing expressions. In this case (when public host key changed for some reason and optional status processing triggered status change) HostMonitor will not set "new pubic key" Warning status, it will set just one status defined by optional status processing (e.g. Normal status). Otherwise (if optional status processing did not trigger status change) HostMonitor may set "new pubic key" Warning status and then "regular" Ok/Bad/Unknown status depending on test result.
The following variables applicable for "SNMP Trap" test only, they represent parameters of the last filtered message (filtered message is the one that have passed all conditions of the test item filter). When HostMonitor launches action in response to received trap message, it substitutes macro variable with its value pertinent to the trap message being received.	
%TrapHost%	Represents IP address of the host that have sent the message
%TrapHostInfo%	If you have specified host name or description in HOSTINFO.LST file, HostMonitor will get information from the file and replace IP address with appropriate description. See HOSTINFO.LST file for details (it's a text file)
%TrapCommunity%	Community string
%TrapType%	Represents type of the trap. It provides information about generic type and enterprise specific number. Generic type could be one of the following: Cold Start, Warm Start, Link Down, Link Up, Auth Failure, EGP Loss and Specific. Enterprise specific number is only applicable when generic trap type is Enterprise Specific, otherwise enterprise specific number is 0
%TimeTicks%	Represents time ticks. "Time ticks" is the time interval (measured in hundredth of seconds) since the initialization (boot, start-up) of the entity that has sent the trap.
%Enterprise%	Enterprise field contains an OBJECT IDENTIFIER which names the device that sends the trap
%EnterpriseName%	Using the database of compiled MIB files HostMonitor may translate Enterprise OID from its numeric form to a MIB name. If you need to extend the database, include information about MIBs supported by some specific SNMP enabled device, use MIB Browser.
%EnterpriseNameShort%	Similar to %EnterpriseName% but shows the name without names of parent nodes. E.g. - %Enterprise% = 1.3.6.1.4.1.3955.5 - %EnterpriseName% = iso.org.dod.internet.private.enterprises.linksys.etherHub - %EnterpriseNameShort% = etherHub
%EnterpriseDescription%	Object description (defined within MIB file)
Each trap message may contain one or several variables that provide information about the event. Following macro variables allow you to access that information:	

%MibOid%	Represents OID (object identifier) of the variable
%MibName%	Using the database of compiled MIB files HostMonitor may translate %MibOID% from its numeric form to a MIB name. If you need to extend the database by including information about MIBs supported by some specific SNMP enabled device, use MIB Browser.
%MibNameShort%	Similar to %MibName% but shows the name of the variable (plus possible index) without names of parent nodes. E.g. - %MibOID% = .1.3.6.1.2.1.2.2.1.8.1 - %MibName% = iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOperStatus.1 - %MibNameShort% = ifOperStatus.1
%MibDescription%	Description of the variable (defined within MIB file)
%MibType%	Type of the variable
%MibValue%	Variable value
%MibRelative%	Relative value of the variable. This macro is applicable when you check incoming trap messages for some specific variable and compare current value of the variable with its previous value (see "Message contains OID…" option in the Trap Filter dialog). %MibRelative% may represent: - simple difference between current and previous value (if you use "increases by", "decreases by" or "changes by" compare option) - relative difference as a percentage of previous value (if you use "increases by (%)", "decreases by (%)" or "changes by (%)" compare option) - average increase/decrease of the counter per second since previous message (if you use "increases /sec", "decreases /sec" or "changes /sec" compare option)
%OidVal.1.2.3.5.204.0%	Such macro returns value of the specified variable (OID 1.2.3.5.204.0) received within SNMP Trap message. Use any valid OID instead of 1.2.3.5.204.0
%TrapAllValues%	This macro returns information about ALL variables received within Trap message (%TrapAllValues% returns "oid=value" line(s); if there is more than 1 variable in SNMP Trap message, lines will be separated by #13#10 characters). Note: %MibOid%, %MibName%, %MibType%, %MibValue% variables provide the information about specific OID variable (if you have set "Message contains OID" option of the test filter) or the information about 1st variable within SNMP Trap packet.
%TrapAllValues_Name%	Using the database of compiled MIB files HostMonitor may translate Object Identifiers (OIDs) provided by %MibAllValues% variable from its numeric form to a MIB name. If you need to extend the database by including information about MIBs supported by some specific SNMP enabled device, use MIB Browser.
%TrapAllValues_NameShort%	Similar to %TrapAllValues_Name% but shows the name of the variable (plus possible index) without names of parent nodes. E.g. if %TrapAllValues% returns 1.3.6.1.2.1.2.2.1.7.1 = 1 1.3.6.1.2.1.2.2.1.8.1 = 1 then %TrapAllValues_Name% will show iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifAdminStatus.1 = 1

	iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOperStatus.1 = 1 and %TrapAllValues_NameShort% will return ifEntry.ifAdminStatus.1 = 1 ifEntry.ifOperStatus.1 = 1
%TrapAllValues_NameValue%	Similar to %TrapAllValues_Name%, translates every OID **and** its value (if value represents some OID) from its numeric form to a MIB name.
%TrapAllValues_NameValueShort%	Similar to %TrapAllValues_NameShort%, translates every OID **and** its value (if value represents some OID) from its numeric form to a MIB name.

There is option that allows you to specify how many words (not including trailing numbers that could not be resolved to name) should be displayed by the following macro variables:
%EnterpriseNameShort%, %MibNameShort%,
%TrapAllValues_NameShort%, %TrapAllValues_NameValueShort%.
This option is not accessible thru GUI however you may add line like snmpShortMibNameLen=3 into [Misc] section hostmon.ini file and restart HostMonitor.

The following variables applicable for "HM Monitor" test only, they provide information related to HostMonitor requested by the test item	
%HMVersionText%	Version of HostMonitor, like HostMonitor v. 8.12
%HMVersionBin%	Binary version, like 0812
%HMSystemName%	Name of the system where HostMonitor is running
%HMStartedTime%	Date and time when HostMonitor was started
%HMTestItemsCnt%	How many test items are in use (including disabled and paused items)
%HMTestsDone%	Number of tests performed by tested HostMonitor (since previous test execution). Returns 0 if request failed
%HMTestsFailed%	Number of "failed' test probes performed by HostMonitor (since previous test execution). Returns 0 if request failed
%HMActionsDone%	Number of actions executed by HostMonitor (since previous test execution). Returns 0 if request failed
%HMLogsDone%	Number of log records added by tested HostMonitor (since previous test execution). Returns 0 if request failed
%HMTestsPerSec%	Average "tests per second" rate for tested HostMonitor since previous test execution
%HMActionsPerSec%	Average "actions per second" rate for tested HostMonitor since previous test execution
%HMLogsPerSec%	Average "log records per second" rate for tested HostMonitor since previous test execution
%HMActionsATC%	Actions ATC (Average Time Consumption). Time used by tested HostMonitor for actions (milliseconds per action). This time does not include time used by auxiliary threads, its not so important
%HMLogsATC%	Logging ATC (Average Time Consumption). Time used by tested HostMonitor for logging (milliseconds per record). This time does not include time used by auxiliary threads, its not so important. This option can be useful for investigation of some 3rd party software related problems (e.g. if ODBC driver specified for ODBC logging consumes too much time)
%HMLoggingPoolUsage%	Current logging pool usage (percentage). High value of this counter means logging performance is too low for your testlist
%HMStatusString%	String that represent status of target HostMonitor, like the following - monitoring started, alerts enabled, modifications stored - monitoring stopped, alerts disabled, modifications not stored If test failed (e.g. HostMonitor does not respond), this variable returns 'request failed' string

Macro variables that allow you to use remote site time as parameters of the actions
Note 1: We do not recommend using %*_RemoteSite% variables as parameters of SQL query used for ODBC logging unless you are using separate database tables for each folder with unique time settings.
Note 2: You may use %Date%, %Time%, %DateTime%, %LastTestTime% and other variables that utilizes local system time settings and the following variables that represent remote site time in the same action profile. This allows you to setup different actions for local administrators and for staff that works at remote site.

%GMTOffset_Local%	GMT offset (time zone) specified on local system
%GMTOffset_RemoteSite%	GMT offset (time zone) on remote site
%Date_RemoteSite%	Current date on remote site (shows the date using the format given by the ShortDateFormat Windows variable)

%Time_RemoteSite%	Current time on remote site (displays the time using the format given by the LongTimeFormat Windows variable)
%DateTime_RemoteSite%	Current date and time on remote site
%LastTestTime_RemoteSite%	Time when the test was last performed
%StatusChangedTime_RemoteSite%	The time when the status was last changed
%PreviousStatusTime_RemoteSite%	Represents time when "PreviousStatus" was assigned to the test
%AcknowledgedAt_RemoteSite%	Represents the date and time when test status was acknowledged
%AcknowledgedDate_RemoteSite%	Represents the date when test status was acknowledged
%AcknowledgedTime_RemoteSite%	Represents the time when test status was acknowledged
%CreatedTime_RemoteSite%	The time when the test was created
%ModifiedTime_RemoteSite%	The time when the test was last modified

Variables for SNMP Table test method (these variables can be used as parameters of actions assigned to SNMP Table test items)

%SNMPTable%	Shows entire table retrieved from SNMP agent, each row displays <oid> = <value> pair. E.g. 1.3.6.1.2.1.2.2.1.2.1 = MS TCP Loopback interface 1.3.6.1.2.1.2.2.1.2.2 = Broadcom NetLink Gigabit Ethernet
%SNMPTable_**Name**%	Shows table retrieved from SNMP agent, MIB name is displayed instead of OID. E.g. iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifDescr.1 = MS TCP Loopback interface iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifDescr.2 = Broadcom NetLink Gigabit Ethernet Using the database of compiled MIB files HostMonitor may translate Object Identifiers (OIDs) from its numeric form to a MIB name. If you need to extend the database by including information about MIBs supported by some specific SNMP enabled device, use MIB Browser.
%SNMPTable_**NameShort**%	Similar to %SNMPTable_Name% but HostMonitor shows the name of SNMP counter (plus index) without names of all parent nodes. E.g. ifTable.ifEntry.ifDescr.1 = MS TCP Loopback interface ifTable.ifEntry.ifDescr.2 = Broadcom NetLink Gigabit Ethernet
%SNMPTable_**VALUES**%	Values without OID E.g. MS TCP Loopback interface Broadcom NetLink Gigabit Ethernet
%**Last**SNMPTable%	Shows SNMP table retrieved by previous test probe, each row displays <oid> = <value> pair.
%**Last**SNMPTable_**Name**%	Shows table retrieved by previous test probe, MIB name is displayed instead of OID.
%**Last**SNMPTable_**NameShort**%	Similar to %LastSNMPTable_Name% but HostMonitor shows the name of SNMP counter (plus index) without names of all parent nodes.
%**Last**SNMPTable_**VALUES**%	Values without OID

If "Apply filter" test property is enabled, HostMonitor may skip some items from the table (e.g. you may skip all network interfaces with zero incoming traffic). The following variables allow you to retrieve SNMP table without showing these items	
%SNMP**Filtered**Table%	Shows table retrieved from SNMP agent (only items that passed filter), each row displays <oid> = <value> pair.
%SNMP**Filtered**Table_**Name**%	Shows table retrieved by test probe (items that passed filter), MIB name is displayed instead of OID
%SNMP**Filtered**Table_**NameShort**%	Similar to %SNMPFilteredTable_Name% but HostMonitor shows the name of SNMP counter (plus index) without names of all parent nodes.
%SNMP**Filtered**Table_**Values**%	Values without OID
%**Last**SNMP**Filtered**Table%	Shows table retrieved by previous test probe (only items that passed filter)
%**Last**SNMP**Filtered** Table_Name%	Shows table retrieved by previous test probe (items that passed filter), MIB name is displayed instead of OID
%**Last**SNMP**Filtered** Table_NameShort%	Similar to %LastSNMPFilteredTable_Name% but HostMonitor shows the name of SNMP counter (plus index) without names of all parent nodes.
%**Last**SNMP**Filtered**Table_**Values**%	Values without OID
%SNMP**FilteredPattern**%	Shows string like 11010011 where 1 means row of the table passed filter; 0 means row was skipped (such rows are not displayed by %SNMPFiltered*% variables).
%**Last**SNMP**FilteredPattern**%	Similar to %SNMPFilteredPattern% variable, shows information about passed and skipped values retrieved by previous test probe.
%SNMPTable**Diff**%	This variable shows only counters that were changed since previous test probe. E.g. 1.3.6.1.2.1.2.2.1.10.1 = 2316972916 (previously 2316956889) 1.3.6.1.2.1.2.2.1.10.5 = 2252070440 (previously 2252065336) If no counters were changed, variable will return "no items were changed" string.
%SNMPTable**Diff_Name**%	Similar to %SNMPTableDiff% but MIB name is displayed instead of OID. Using the database of compiled MIB files HostMonitor may translate Object Identifiers (OIDs) from its numeric form to a MIB name. If you need to extend the database by including information about MIBs supported by some specific SNMP enabled device, use MIB Browser.
%SNMPTable**Diff_NameShort**%	Similar to %SNMPTableDiff_Name% but HostMonitor shows the name of SNMP counter (plus index) without names of all parent nodes.
Note: There is option that allows you to specify how many words (not including trailing indexes that could not be resolved to name) should be displayed by %SNMPTable_NameShort%, %LastSNMPFilteredTable_NameShort % and %SNMPTableDiff_NameShort% variables. This option is not accessible thru GUI however you may add line like snmpShortMibNameLen=3 into [Misc] section hostmon.ini file and restart HostMonitor.	
The following variables provide HTML code that can be used in your HTML reports or HTML e-mails.	
%SNMPFilteredTable_HTML%	Shows table with filtered counters (or table with all counters when "Apply filter" option is disabled). For each counter HostMonitor

	provides the following information: - OID and short name - Value - Previous value - Difference - Difference percentage wise
%SNMPTableDiff_HTML%	Similar to %SNMPFilteredTable_HTML% but this variable does not include items that were not changed since previous test probe.

When you are using %SNMPFilteredTable_HTML% or %SNMPTableDiff_HTML% variables in your HTML code, you may define your own styles for the table. You may define 4 classes:

.snmptable	Style for the table
.snmpheader	Style for table header
.snmprow	Style for rows, rows with counters that were not changed since previous test probe
.snmpchangedrow	Style for changed rows, rows with counters that were changed since previous test probe

Sample:

```
<STYLE TYPE="text/css"> <!--
.snmptable { padding: 5px; border-top: dotted thin silver; border-bottom: solid
medium silver; border-left: dotted thin silver; border-right: solid medium silver }
.snmpheader { text-align: center; background: #FFFFCC; color: #000000; border-style:
inset; border-width: 0 2 2 0; border-color: #333333; }
.snmprow { font-size: smaller; text-align: center; background: #E9E9E9; color:
#000000; border-style: inset; border-width: 0 2 2 0; border-color: #333333; }
.snmpchangedrow { font-size: smaller; text-align: center; background: #FF0000; color:
#FFFFFF; border-style: inset; border-width: 0 2 2 0; border-color: #333333; }
</STYLE>
```

If you are using “Alert if **any item** …” mode for SNMP Table test, HostMonitor checks entire table and finds not just a value that fits specified alert threshold but finds the counter that maximally satisfies specified condition.
For example:

- if you setup “Alert if any item is < than 1000” condition and SNMP agent returns numbers 2222, 100, 50, 5000 then HostMonitor will report 50 as test result (1st number that fits condition is 100 but HostMonitor will continue scanning and find minimal number 50).
- If you setup “Alert if any item is > than 1000” condition and SNMP agent returns numbers 2222, 100, 50, 5000 then HostMonitor will report 5000 as test result (not 2222)

The same rule works when you use “increases by”, “decreases by”, “changes by %” and other comparative modes - HostMonitor will find counter that increased or decreased maximally (or increased/decreased maximally percentage wise)

Then you may get additional information about such detected counter using the following variables:

%MibOid%	Represents OID (object identifier) of the variable
%MibName%	Using the database of compiled MIB files HostMonitor may translate %MibOID% from its numeric form to a MIB name. If you need to extend the database by including information about MIBs supported by some specific SNMP enabled device, use MIB Browser.
%MibNameShort%	Similar to %MibName% but shows the name of the variable (plus index) without names of all parent nodes. E.g. - %MibOID% = .1.3.6.1.2.1.2.2.1.8.1 - %MibName% = iso.org.dod.internet.mgmt.mib2.interfaces.ifTable.ifEntry.ifOperStatus.1 - %MibNameShort% = ifOperStatus.1
%MibType%	Type of the variable

%MibValue%	Variable value
%MibRelative%	Relative value of the variable. If you setup SNMP Table test to check how counters change comparatively to the values received by previous test probes, %MibRelative% may represent: - simple difference between current and previous value (if you use "increases by", "decreases by" or "changes by" compare option) - relative difference as a percentage of previous value (if you use "increases by (%)", "decreases by (%)" or "changes by (%)" compare option) - average increase/decrease of the counter per second since previous test probe (if you use "increases /sec", "decreases /sec" or "changes /sec" compare option)

2. variables that represent parameters of some explicitly specified test

If you want to access the parameters of some specific test (not just the one that had triggered an action), specify the name of a test or id of the test confined by a double colon (**::**) in front of the name of the macro variable (%::<testname>::<macrovariable>% or %::<testid>::<macrovariable>%). E.g. if you want to access "Reply" and "Status" fields of the "Ping Yahoo" test, use the following syntax for the variables: %**::**Ping Yahoo**::**Reply%, %**::**Ping Yahoo**::**Status%
To find out ID of the test items, you may use Custom HTML report with %TestID% macro variable

3. host related variables

You can setup actions using variables that refer not to some specific test (like "CPU test for MainWebServer") but rather to test items that check the same host - HostMonitor will search for test items related to the host that triggered this action execution. E.g. if you setup CPU Usage, Memory and Dominant Process tests for Host01, Host02 .. Host99, then you may setup single alert profile with "Send e-mail" action using HTML template like:

ver A

```
E-mail triggered by
%TestName% %Status% %Reply%<br>
<br>
Related tests:<br>
<br>
%::RelatedCPU::short_table%<br>
%::RelatedMemory::short_table%<br>
%::RelatedProcess::short_table%
```

ver B

```
%TestName%<br>%Status%<br>%Reply%<br>
<table border=0>
<tr><td colspan=4>CPU load:</td></tr>
%::RelatedCPU::short%
<tr><td colspan=4>Memory</td></tr>
%::RelatedMemory::short%
<tr><td colspan=4>Top Processes</td></tr>
%::RelatedProcess::short%
<table>
```

ver C

```
%TestName%<br>%Status%<br>%Reply%
<br><br>
%::RelatedTests::short_table%
```

Then if any CPU Usage test (e.g. "CPU Usage for Host05" test) will change status from Ok to Bad and trigger assigned actions, HostMonitor will find Memory and Dominant Process tests related to the same Host05 and you will get e-mail with information about CPU load, memory usage and information about process(es) that use the most of system resources (CPU, memory, Handles, etc)

Note: disabled test items ignored

You should specify variable using two parts: prefix like RelatedProcess and suffix like short or short_table. E.g.

```
%::RelatedTests::short%
%::RelatedSpace::stat%
%::RelatedProcess::short_table%
%::RelatedProcess::stat_table%
```

Prefix tells HostMonitor what kind of tests should be selected:

RelatedTests	All tests related to the host. E.g. If "Cisco CPU Usage" test triggers alert, such variable provides information about ALL test items related to this Cisco device
RelatedLan	Ping, Trace, TCP, UDP, DNS, DHCP, NTP, SIP, RAS, Radius and DICOM tests related to the host
RelatedMemory	Memory tests (physical, virtual, swap memory tests)
RelatedCPU	CPU Usage tests
RelatedProcess	Process and Dominant Process tests
RelatedSpace	Drive Free Space tests
RelatedWMI	WMI tests
RelatedPerf	Performance Counter tests
RelatedTraffic	Traffic Monitor tests items related to the host
RelatedSNMP	SNMP Get and SNMP Table tests
RelatedTemperature	Various Temperature checks, like Cisco temperature, Juniper temperature, Sensatronics temperature, HDD SMART tests when temperature mode used, etc

Suffix tells what data should be displayed:

short	Shows test name, status, status age, reply E.g. result of %::RelatedMemory::stat% variable may look like SwapTest1 Ok (3 min ago) 70% MemTest2 Ok (30 sec ago) 50%
stat	Shows test name, status, status age, reply, average reply, min reply, max reply. E.g. result of %::RelatedMemory::stat% variable may look like SwapTest1 Ok (3 min ago) 70% (51 / 15 / 89) MemTest2 Ok (30 sec ago) 50% (33 / 10 / 90)
short_table	Similar to "short" suffix (shows test name, status, status age, reply) but adds <table> and </table> tags. Such suffix can be used when variable specified for some HTML related action, e.g. "Send e-mail" action with template in HTML format or HTTP request action. E.g. result of %::RelatedMemory::short_table% may look like <table border=0> <tr><td>SwapTest1</td><td>Ok</td><td>(3 min ago)</td><td>70%</td></tr> <tr><td>MemTest2</td><td>Ok</td><td>(30 sec ago)</td><td>50%</td></tr> </table>
stat_table	Similar to "stat" suffix but adds <table> and </table> tags. Such suffix can be used when variable specified for some HTML related action, e.g. "Send e-mail" action with template in HTML format or HTTP request action.

Exact result depends on where a variable is declared. HostMonitor may use Text, HTML, JSON, URL encoding rules. E.g. if you are using such variable for e-mail template, HostMonitor will use text or HTML format depending on [E-mail body: Text/HTML] switch. The same variable %::RelatedMemory::stat_table % can be resolved to text

```
SwapTest1    Ok  (3 min ago)   70%
MemTest2     Ok  (30 sec ago)  50%
```

or it can be resolved to HTML

```
<table border=0>
<tr><td>SwapTest1</td><td>Ok</td><td> (3 min ago) </td><td>70%</td></tr>
<tr><td>MemTest2</td><td>Ok</td><td> (30 sec ago) </td><td>50%</td></tr>
</table>
```

If you are using several variables, then it may be better to use single table for all variables – use short/stat suffixes and specify <table> tags manually. E.g.

```
<table border=0>
<tr><td colspan=4>CPU usage</td></tr>%::RelatedCPU::short%
<tr><td colspan=4>Memory</td></tr>%::RelatedMemory::short%
<table>
```

4. Folder-related macro variables

The following variables provide information about the folder (folder that contains the test which has triggered action execution)

%Folder%	The name of the folder containing the test
%FolderID%	Represents unique ID of the folder (integer number)
%FullPath%	The full folder path name
%FullPathSlash%	The full folder path name, uses slash instead of back slash character
%FolderComment%	Folder's comment (entire comment, lines separated by CRLF)
%FCommentLineNN%	Returns a line #NN of a folder`s comment
Statistical variables	
%FolderCurrent_TotalTests%	Total number of the test items in the folder
%FolderCurrent_GoodTests%	Number of the test items (in the folder) those have "Good" status
%FolderCurrent_BadTests%	Number of the test items (in the folder) those have "Bad" status
%FolderCurrent_UnknownTests%	Number of the test items (in the folder) those have "Unknown" status
%FolderCurrent_WarningTests%	Number of the test items (in the folder) those have "Warning" status
%FolderCurrent_AcknowledgedBad%	Number of "Bad" acknowledged test items in the folder
%FolderCurrent_AcknowledgedUnknown%	Number of "Unknown" acknowledged test items in the folder
%FolderCurrent_AcknowledgedWarning%	Number of "Warning" acknowledged test items in the folder
%FolderCurrent_DisabledTests%	Number of disabled test items in the folder
%FolderCurrent_PausedTests%	Number of paused and OutOfSchedule test items
%FolderCurrent_WaitMasterTests%	Number of test items with WaitForMaster status
%FolderCurrent_TotalProbes%	Number of test probes executed since last statistics reset
%FolderCurrent_SessionProbes%	Number of test probes executed since HostMonitor restart
The following variables work similar to statistical macros listed above with 1 distinction – they count test items within folder AND all descendant subfolders (not applicable to Custom HTML reports)	
%FolderRecursive_TotalTests%	Total number of the test items in the folder and its subfolders
%FolderRecursive_GoodTests%	Number of the test items those have "Good" status
%FolderRecursive_BadTests%	Number of the test items those have "Bad" status
%FolderRecursive_UnknownTests%	Number of the test items those have "Unknown" status

%FolderRecursive_WarningTests%	Number of the test items those have "Warning" status
%FolderRecursive_AcknowledgedBad%	Number of "Bad" acknowledged test items
%FolderRecursive_AcknowledgedUnknown%	Number of "Unknown" acknowledged test items
%FolderRecursive_AcknowledgedWarning%	Number of "Warning" acknowledged test items
%FolderRecursive_DisabledTests%	Number of disabled test items
%FolderRecursive_PausedTests%	Number of paused and OutOfSchedule test items
%FolderRecursive_WaitMasterTests%	Number of test items with WaitForMaster status
%FolderRecursive_TotalProbes%	Number of test probes executed since last statistics reset
%FolderRecursive_SessionProbes%	Number of test probes executed since HostMonitor restart

Also you may retrieve summary information for specific folder using expressions like %::<fullpath>::<folder_macro>% or %::<folderID>::<folder_macro>%.
E.g. %::Root\Asia::FolderCurrent_BadTests% or %::12:: FolderCurrent_GoodTests%
You may find out FolderID using Folder Properties dialog (ID is displayed at the right bottom corner of the window)

5. HostMonitor status related macro variables:

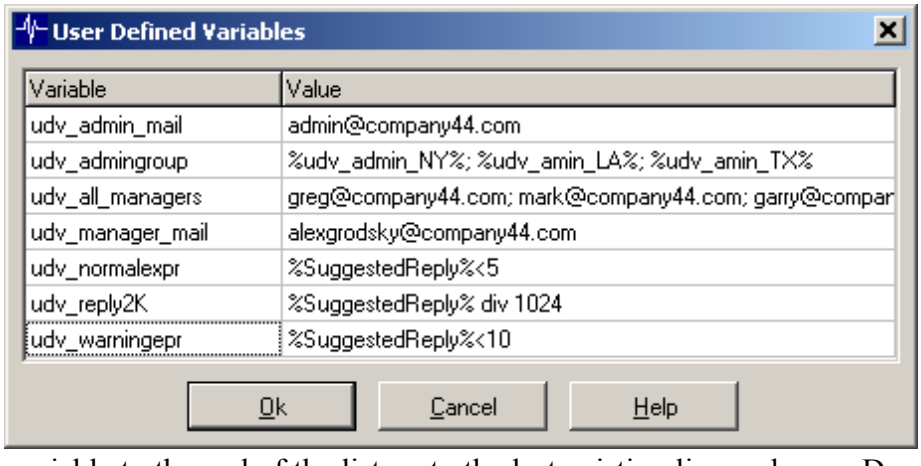
These variables represent the status of HostMonitor:

%MonitorState%	this variable may have 2 values: "Monitoring Started" or "Monitoring Stopped"
%AlertsState%	this variable may have 2 values: "Alerts Enabled" or "Alerts Disabled"
%HM_LastLoggingError%	represents description of last logging error (if any); can be useful for actions triggered by HostMonitor when it cannot save data into the log
%HM_RccSessions%	represents number of active RCC sessions
%HM_TestListFile%	name of the TestList file being used
%HM_TestsPerformed%	number of tests performed since startup
%HM_TotalTestItems%	total number of test items (in loaded file)
%HM_GoodItems%	number of tests with "Good" status
%HM_BadItems%	number of tests with "Bad" status
%HM_UnknownItems%	number of tests with "Unknown" status
%HM_WarningItems%	number of tests with "Warning" status
%HM_AckBadItems%	number of "Bad" acknowledged test items
%HM_AckUnknItems%	number of "Unknown" acknowledged test items
%HM_AckWarnItems%	number of "Warning" acknowledged test items
%HM_DisabledItems%	number of disabled test items
%HM_PausedItems%	number of paused and OutOfSchedule test items
%HM_WaitMasterItems%	number of test items with WaitForMaster status

6. user defined variables (UDV, also known as global macro variables)

Specifics of user defined variables vs. simple macro variables: macro variables that were described above represent different properties of the tests and you cannot change their values directly. On the contrary, there are user defined (global) macro variables that can be used in any of the action profiles. This type of variables may be of great use. For example if you have lots of alerts that send e-mails to different mailing lists (one action sends the mail to administrators, another to managers, 3rd action sends notifications to managers and administrators, etc). When some of the e-mail addresses have been changed you will then need to correct these addresses in all profiles that are using them. To avoid this you may define global variables. Define several variables such as "udv_admingroup = rick@mycompany.com; brand@mycompany.com", "udv_managmentgroup = bob@mycompany.com; john@mycompany.com; kim@mycompany.com", etc and use them as a destination address for the actions: "%udv_admingroup%". Now if any of the e-mail addresses will change, you will have to track this change only in the definition of the variable. This is far more efficient than checking all action profiles that may use the address being changed.

Global variables are defined in the “User Defined Variables” dialog. This dialog is accessible from the menu “Profiles”->”Global macro variables”.



To add a new variable to the end of the list go to the last existing line and press Down Arrow key. Press INSERT button to insert a new line. Press CTRL+DEL to remove variable or several selected vaiables. Press F2 when you want to change variable value or name.
You may use popup menu items to sort items alphabetically by name or by value. Also you may use popup menu items to copy set of variables (or copy entire list) into Windows clipboard and paste variables from Windows clipboard. HostMonitor offers "Copy as CSV" and "Copy as Expression" options for copying while “paste” function detects format of such list automatically.

You can also create an HMScript that will modify variables automatically (for example in respond to some event). Moreover, you may change the value(s) of variables remotely through Telnet Service and any telnet client.

Any name of user defined variable always starts with the prefix “udv_”. Even if you will forget to add this prefix to the name HostMonitor will add it automatically. When specifying the name of the variable in action parameter you have to enclose the name in `%`. When HostMonitor performs an action it will substitute the name of the variable by its` current value.
In the string that represents a value of a UDV you may use the name of another macro variable(s): e.g. date-time variables or test related variables.

7. date & time variables

To represent a date or time you may use the following variables:

%d% - Current day as a number without a leading zero (1-31).

%dd% - Current day as a number with a leading zero (01-31).

%ddd% - Current day as an abbreviation (Sun-Sat). HostMonitor uses system's regional settings for abbreviation format.

%jjj% - The day of the year as a three digit decimal number in the range of 001 to 366

%ww% - Current week as two-digit number (01-54).

%www% - Current week number according to ISO 8601 specification (1st week of the year is the week with the year's first Thursday in it)

%m% - Current month as a number without a leading zero (1-12).

%mm% - Current month as a number with a leading zero (01-12).

%mmm% - Current month as an abbreviation (Jan-Dec) using system's regional settings.

%yy% - Current year as a two-digit number (00-99).

%yyyy% - Current year as a four-digit number (0000-9999).

%uuu% - Current local time as UnixTimeStamp (seconds since 1970)

%uuu[-0u]% - Current UTC time as UnixTimeStamp (seconds since 1970)

%h% - Current hour without a leading zero (0-23).

%hh% - Current hour with a leading zero (00-23).

%h12% - Current hour of the day using 12-hour clock (0-12,1-11)

%hh12% - Current hour of the day using 12-hour clock with a leading zero

%n% - Current minute without a leading zero (0,1…59).

%nn% - Current minute with a leading zero (00,01…59).

%am/pm% - Returns 'am' for any hour before noon, and 'pm' for any hour after noon

%AM/PM% - Returns 'AM' for any hour before noon, and 'PM' for any hour after noon

%a/p% - Returns 'a' for any hour before noon, and 'p' for any hour after noon

%A/P% - Returns 'A' for any hour before noon, and 'P' for any hour after noon

The following table illustrates where you can use macro variables:

Action	Macros applicable	Action parameters where macros are applicable
Show message	No	
Play sound	Yes	Path to the file
Hangouts chat	Yes	Webhook URL Message text
Microsoft Teams	Yes	Webhook URL Message text
Telegram message	Yes	Token Chat ID Text
Slack message	Yes	Webhook URL Title Message text
Viber message	Yes	Token Receiver Text
Send message to ICQ	Yes	ICQ # (UIN) Message template
Send message to Jabber	Yes	Jabber account Message template
Send message to pager (TAP)	Yes	Pager ID Message template
Send message to pager (SNPP)	Yes	Pager ID Message template
Send message to beeper	Yes	Beeper # Message line
Send SMS (GSM)	Yes	Destination phone Message template
Send SMS (SMPP/IP)	Yes	Destination phone Message template
Send e-mail (SMTP)	Yes	Address of the sender Destination address Subject Message template Attachment
Record HM Log	Yes	Destination file name
Generate reports	No	
Stop/Start/Restart service	Yes	Computer name Service name
Remote reboot	Yes	Computer name
Local reboot	No	
Execute external program	Yes	Command line

Start program remotely	Yes	Target host Command line Working directory
Kill process	Yes	Target host Process name Process ID
Dial-up to the network	No	
Disconnect dial-up connection	No	
Log Event	Yes	Computer name Event source Event description
SQL Query	Yes	ODBC data source SQL Query
HTTP request	Yes	Host name HTTP request
Send data to TCP/UDP port	Yes	Init packet Final packet
Syslog	Yes	Message
SNMP Set	Yes	Agent address Value
SNMP Trap	Yes	Destination address Agent address Enterprise MIB OID MIB Value
Repeat test	No	
Change test interval	No	
Execute HMS script	Yes	In the HMS script file

E.g. message template for pager notification can look like: "Host %TestName% changed status to %status% at %datetime%."

Please note: HostMonitor resolves test specific variables depending on the type of module where variables are used:

- if variable is used in HTML mail or HTML report, HostMonitor resolves it according to HTML encoding rules. E.g. if test name is "**<local comp>**", %TestName% variable will be translated into "**<local comp>**;"
- if variable is used in ODBC Query (ODBC logging or SQL Query action) then HostMonitor resolves this variable and replaces single quotation marks (‘) with 2 single quotation marks (‘’); replaces CR LF (#13 #10) symbols with "\r" and "\n" correspondingly
- in all other cases variables are substituted as is (variables are replaced by appropriate test parameters)

User defined variables and folder related variables are substituted as is. This allows you to use folder comments and user defined macro variables to store certain elements of HTML code (can be used as styles).

Logs & Reports

Logs

HostMonitor can log application events to a log file(s) or database. Different log detail levels and log file formats can be configured to suit your needs. You may setup the following logs:
Common log
Private log
Custom log
System log
User operations log
See also: Log processing

Common Log

Common log is a file or database that is shared by all test items defined in the working test list. All events that are subject to logging (according to test's configuration) get recorded in the common log.

You may specify Primary and Backup common logs. For each log you may choose defferent log type (ODBC or File), file format (HTML, Text or DBF) and logging mode (Full, Brief, Midnight or Reply). E.g. you may use Full logging mode for primary ODBC log managed by your SQL server and use Brief logging mode for backup HTML log stored on local hard drive.
HostMonitor can switch from primary to backup log when necessary or use both logs at the same time. Also HostMonitor may execute specified alert profiles when primary or backup logs are not accessible.

All aspects of the common log's behavior are controlled through Options dialog:
- Log settings
- Log processing

Private Log

Additionally, for each test you can define its own, "private" log file. The type of a private log is determined based on the file extension: HTML for .htm*, DBF for .dbf, plain text for any other extension.
Private logs can be configured to work in one of the following modes:
- Default - the common settings defined in the Options dialog are used;
- Brief - record information whenever status of the test changes;
- Full - record all test results, regardless of whether their status had changed or not;
- Reply - record information into log every time the status or reply value of the test changes.

If a private log is specified, the popup menu for that test will contain the item, "View private log".

Custom logs

In some cases you may need very specific logging option, like “if temperature in server room between 70 and 75 degrees F, record every test probe; othewise log nothing”. In such case you may disable common and private logs for the test item and use “Record HM log” or “SQL Query” actions to save information.

System Log

System log is yet another log type. HostMonitor uses the system log to record events like start/stop monitoring, as well as information on started and/or failed alert actions. You may setup log parameters on the System log page in the Options dialog.

User operations log

Also HostMonitor may record operations performed by local or remote operators, operations performed by HM Script or HostMonitor itself. It records information about enabled and disabled test items, paused and refreshed items, removed folders and tests, modified folders, views and tests, started scripts, import operations and so on. Each type of operation has its own ID. List of such operations listed in Appendix #2.

For each operation HostMonitor records:

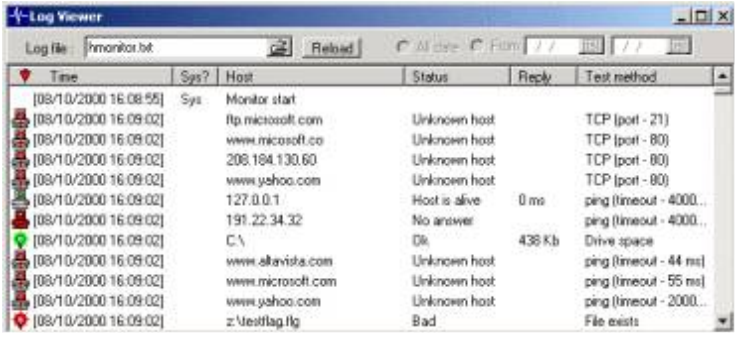
- Event time
- Operator type (HostMonitor, local operator, remote operator, HM Script, import procedure)
- Unique ID of the operator and operator’s name (for local and remote operators)
- Operation ID and operation name (XML log file contains operation ID only)
- Item ID (usually this is test ID or folder ID, e.g. if you move test item, this field will show test ID)
- Result (Done, Rejected or Failed)
- Description (may contain test name, folder name, some comments)

Log setting located on System log page in HostMonitor Options dialog

Log processing

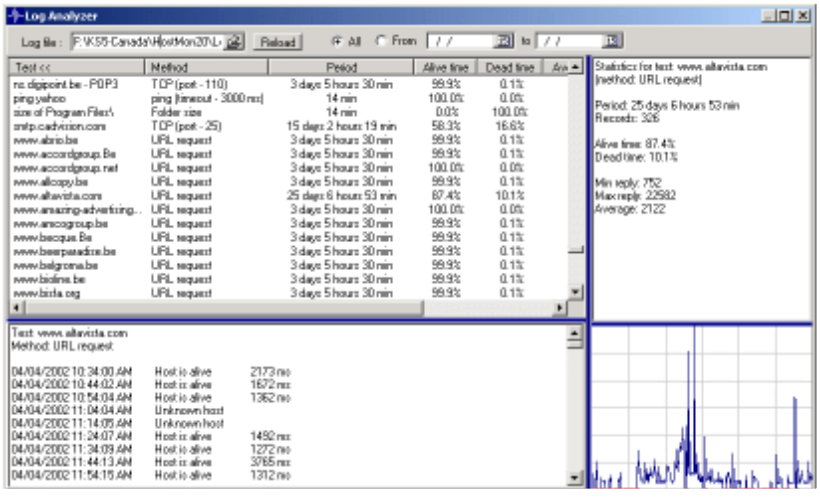
Log processing options allow you to manage log files: e.g. you may setup HostMonitor to remove files older than 3 months, or you may configure HostMonitor to keep just 2 log files - for previous and current month.

Log Viewer



To view log files, you can use the built-in viewer, associated programs or an external program. You can setup different viewers to view different log types. For example, to view an HTML log file you can use the associated program (your default web browser); to view a text log file you can use the build-in log viewer, etc.
See Options -> Log Viewers.
With the built-in log viewer, you can view any of the supported log types (HTML, Text, DBF). The viewer supports sorting, which allows you to order log records by any field (time, test name, status, reply value, etc).

Log Analyzer



Advanced Host Monitor package includes Log Analyzer. Log Analyzer is a graphical tool that visualizes the log data. It parses the contents of a log file and presents the data as a variety of charts representing different test statistics. Log Analyzer may analyze all types of log files: HTML, Text, and DBF log files. In a second, administrator can get a snap shot of the host performance over a period of days or even months.
Several examples of the reports that were generated by Log analyzer:
Example #1
Example #2
Example #3

Reports

HostMonitor can generate reports at regular intervals and/or when some tests change their status. Reports can be in either HTML, DBF, WML, or Text formats. The highly flexible Report Manager allows you to create and customize reports to your liking in a variety of ways. Also note that each folder may contain its own list of reports, and each of the reports can be set up with a launching schedule specific to that folder. With reports, you can easily check the status of your network from anywhere using a Web browser or your WAP cell phone. Example.
DBF report is useful for analyzing (after generating reports HostMonitor can launch an external program for analyzing or other purposes).

A list of up to 6 global reports (reports that apply to all tests in the working HML file) can be defined on the Reports page in the Options dialog. Additionally, each folder may have its own list of reports; only the tests contained in the folder will be used in generating these folder-specific reports. There are two more parameters that can be specified for both global and folder-specific reports:

- time interval - tells HostMonitor how often reports should be generated
- external program to execute - if specified, HostMonitor will launch the external program after reports have been generated.

It is also possible to have HostMonitor generate a report every time a test changes its status. This can be done by adding "Generate reports" action to the Action Profile. The other way to implement the same behavior would be to add a "Run HMS Script" action, and include a CreateReport command in the script to execute.

Also note that reports can be generated at user request at any time through the Reports menu in HostMonitor's main window.

Macros

When you provide the name of the common, private or system log file or setup target files for the reports you can use special macro variables in the file name:

%d% - Current day as a number without a leading zero (1-31).
%dd% - Current day as a number with a leading zero (01-31).
%ddd% - Current day as an abbreviation (Sun-Sat) using system's regional settings.
%dddd% - Current day as a full name (Sunday-Saturday) using system's regional settings.
%ddddd% - Current date using the short date format (see Windows Regional Options).
%dddddd% - Current date using the long date format.
%ww% - Current week as a number with a leading zero (01-54).
%m% - Current month as a number without a leading zero (1-12).
%mm% - Current month as a number with a leading zero (01-12).
%mmm% - Current month as an abbreviation (Jan-Dec) using system's regional settings.
%mmmm% - Current month as a full name (January-December) using system's regional settings.
%yy% - Current year as a two-digit number (00-99).

%yyyy% - Current year as a four-digit number (0000-9999).
%/% - Displays the date separator character given by the DateSeparator global variable.

Macro variables may be written in upper case as well as in lower case letters - both produce the same result.
Examples:
c:\HostMonitor\Logs**%DDMMYYYY%**.DBF
c:\ HostMonitor\Reports**%dd%-%mm%-%yy%**.html
c:\HostMonitor**%YYYY%**log**%mm%**.html

Remote Control Interface & Operators

Advanced Host Monitor 4+ has components that allow users (with different access rights) to control it from a remote locations via web interface or telnet client. HostMonitor supports multiple user profiles both for local and remote operators.

RCI (Remote Control Interface)

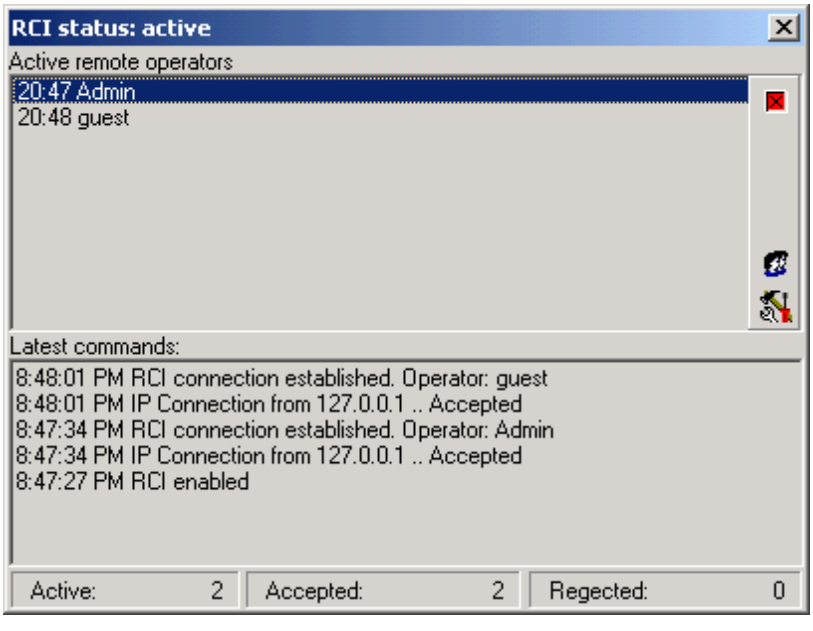
RCI is a feature of the monitor that allows you to check and control HostMonitor remotely (using web browser or telnet client). RCI uses TCP/IP protocol and needs just one TCP port (by default this is a port #1054). You can setup different parameters of the interface (like port number, timeout, limit for the number of simultaneous connections, etc) on RCI page in the Options dialog. For each user account you can specify a list of IP addresses from which a connection can be accepted and a list of operations (such as start/stop of monitoring, enable/disable tests, etc) that are allowed for the user.

To control HostMonitor through RCI you have to install either Web Service and/or Telnet Service. These applications can be installed on the same system where HostMonitor is already installed or on any other (remote) system that can communicate with HostMonitor's system via TCP/IP protocol.
Web Service application will allow you to use web browser (such as Internet Explorer) to control HostMonitor. Telnet Service application allows you to use any telnet client to check HostMonitor.

Also you may use Remote Control Console (RCC). RCC allows you to work with HostMonitor which is running on a remote system just like you work with HostMonitor when it is started on your local system. RCC has exactly same interface as the one of the HostMonitor.

RCI Status window

To bring up this window use menu "View"->"RCI Status". There you may check the status of Remote Control Interface. The list of remote operators that are currently connected to the HostMonitor and the recent list of commands being send to HostMonitor are also available in this window. With the buttons in the right panel of the window you may change the RCI settings, manage user's accounts, etc.



Active remote operators
In the upper part of the window there is a list of remote operators that are currently connected to the HostMonitor. Using the button "Disconnect" (in the right panel) you may disconnect selected remote operator(s). The button "User profiles" brings up the User Profiles dialog, where you may manage the access permissions for each of the remote operators (users). You may add new user accounts, disable or enable existing accounts, etc.
Also RCI Status window allows you to send text messages to remote RCC operators.

Latest commands
In the lower part of the window there is a list of the latest connections and commands that were executed by remote operators.

Status bar
The status line shows statistical information: the number of active remote connections, the number of connections that were accepted and rejected since the HostMonitor was last started.

Notes:
When RCC client receives text message from another operator, it shows "green" popup window. Operator may close this window or keep window on screen and continue working with test items and profiles as usually.

When admin selects some RCC client and clicks "Disconnect" button for the first time, RCC client will not be disconnected immediately. HostMonitor will mark this client as "disconnecting" while RCC operator will see "red" popup window with countdown timer and "I need more time" button. Operator may click (once or several times) on "I need more time" button and reset timer to 60 sec. Otherwise client will be disconnected in 15 seconds.

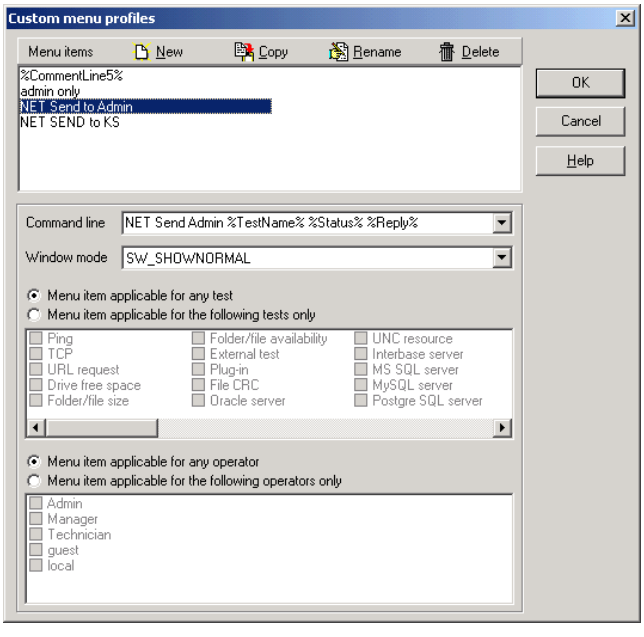
When admin clicks "Disconnect" button 2nd time (for the same RCC client), RCC will be disconnected immediately.

User

This menu of HostMonitor's main window accommodates the set of tools related to user profiles and accounts management in HostMonitor

- Custom menu profiles - allows you to create custom menu items.
- Operators - user profiles manager. Allows you to create new users accounts, delete existing user's accounts and manage their rights and permissions.
- Login as - here you may log in as another user without interrupting the HostMonitor. For example when you have to perform an operation that requires Administrators privileges
- Change password - if "change its own RCC password" permission granted, RCC allows operator to change its own password

Custom menu profiles



This dialog is accessible from the menu "User"->"Custom menu profiles". This feature allows you to create custom menu items. These menus will appear after right clicking on the test in the Test Details area of HostMonitor window. For each menu item you have to provide a name, a command line and a window mode parameter (Hide, Normal, Maximized, etc). You may specify a list of users that will be able to execute this menu item and a list of test methods that will inherit this menu.
Note: "Sort by" popup menu allows you to sort profiles by name, command line or creation time.

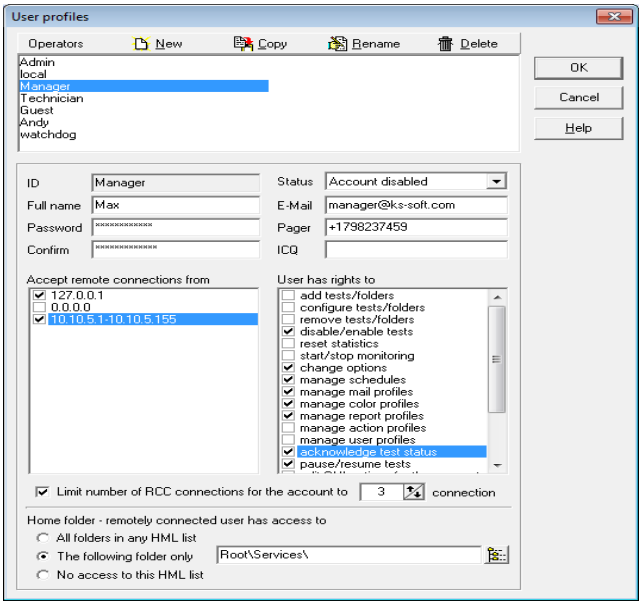
In the name and in the command line of custom menu item you may use macro variables. Depending on the test which you will right click, HostMonitor will use current values of variables. E.g. you can define the command line to send a message to administrator such as "NET SEND admin %TestName% %Status% %Reply%". Another example - you may define a name of the menu item as "%CommentLine7%", HostMonitor will use 7th comment line of the selected test as a name of the menu. If the 7th comment line is empty, then this menu item will not appear. This feature is useful when it is necessary to apply a custom menu command only for some specific tests. If you want to limit the use of a menu item by tests from some specific folders, then you should use folder related macro variables (%FolderComment% or %FCommentLineX%) as a name of the item (or in a command line).
Also you may use %OperatorName% variable – name of the logged in operator.

If command starts with [copy] keyword then HostMonitor does not execute command, instead it resolves variables and copies data into clipboard. E.g. if you set menu item using the following

command line [Copy] Test: %TestName%<cr>Reply: %Reply% select the test and click on menu, then HostMonitor will copy into clipboard buffer string with test name and reply value (note: <cr> resolves to CRLF characters).

Operators

HostMonitor supports different permissions for each user. Each user (operator) has an account with a name, full name and a password. According to the set of permissions users may perform some (or all) of the following operations:



- add tests/folders
- configure tests/folders
- remove tests/folders
- disable/enable tests
- reset statistics
- start/stop monitoring
- change options
- manage schedules
- manage mail profiles
- manage color profiles
- manage report profiles
- manage action profiles
- manage user profiles
- acknowledge test status
- pause/resume test items
- edit GUI options for the account
- edit GUI options for ALL accounts
- view test setting (read-only)
- manage shell scripts
- use Connection Manager
- change its own RCC password
- backup/restore operations

For example "Admin" has permissions to perform any operation; "Technician" has permissions to disable/enable tests, change options and manage mail profiles; "Manager" has permissions to reset statistics and manage report profiles.

Also you can specify a list of IP addresses authorized for remote connections for each of the accounts.
Please note:

- to insert new address press INSERT button; to remove item press CTRL+DEL;

- you may specify ranges of IP addresses from which a connection may be accepted. E.g. 192.168.1.1 - 192.168.1.100;
- you may use '0.0.0.0' IP address. If you specify 0.0.0.0 address, HostMonitor will accept incoming connections from ANY address.

Status
Here you can temporarily disable account or set authentication options by choosing one of the following options:
- account disabled
- HM authentication
- HM or Windown authentication

HM authentication can be used by any application (Web Service, Telnet Service, WatchDog, Remote Control Console) started on any system – workgroup or domain member, Windows or Linux. E.g. HostMonitor authentication mode used when you login to HostMonitor thru Web Service using web browser started on Linux system.
Windows authentication can be used when you connect to HostMonitor using RCC (Remote Control Console) and both Windows systems (HostMonitor system and RCC system) are domain members. In such case remote RCC operator may choose “Windows authentication” option and connect to HostMonitor without providing username/password.
Windows account on HostMonitor side can be specified as domain\username or just username (in case of single domain). E.g. if operator logged in to Windows system and started RCC under “DOMAIN1\manager123” name, then either “DOMAIN1\manager123” or “manager123” operator account should be created on HostMonitor side.

Limit number of RCC connections for the account to N connection(s)
This option allows you to limit number of simultaneous RCC connections on per-user basis. E.g. you may allow “admin” to use 1 connection only and allow “guest” account to use up to 5 RCC connections. If you set limit to 0, user will be able to use Web Service and Telnet service but will not be able to use RCC

Home folder
Since the version 6 HostMonitor provides a "home folder" option that can be specified for each operator. If you do so, the operator(s) will see test items within their own specified folder (and its subfolders) only. In this way, you may easily separate work/permissions between departments of a company.
For each account (operator) you may choose one of the following options
- Access to: All folders in any HML list
- Access to: The following folder only <folder name>
- Access to: No access to this HML list

If you are using several test lists, you may assign different home folders for each operator. For example: operator "US_Manager" may have access to all folders (Root\) within "USA.HML" file and access to single folder "Root\Public\" within "Canada.HML" file.

Note 1: "Home folder" option has effect for any operator that works with monitor remotely using Remote Control Console, Web Service or Telnet Service. An operator that works with HostMonitor's GUI on a local system will have access to the entire test list as in previous versions.

Note 2: Using Remote Control Console to edit test properties (list of master tests), it is possible to see 'ID <number>' instead of the name of the master test (Test Properties dialog). This means that the master test is located in a folder to which the operator does not have access. If you need information about this master test, it can be provided by an operator with a higher level of rights.

Note 3: HostMonitor uses GUID to identify HML files and a unique FolderID to identify a user's home folder. This means if you copy or rename the file, rename or move the home folder, HostMonitor still knows what home folder is assigned for each user. However, if you use menu "File"->"Save as", HostMonitor will assign new GUID to new HML file. In this case, it may be necessary to reassign the home folder for the operators except when they have access to all/root folder.

Special accounts

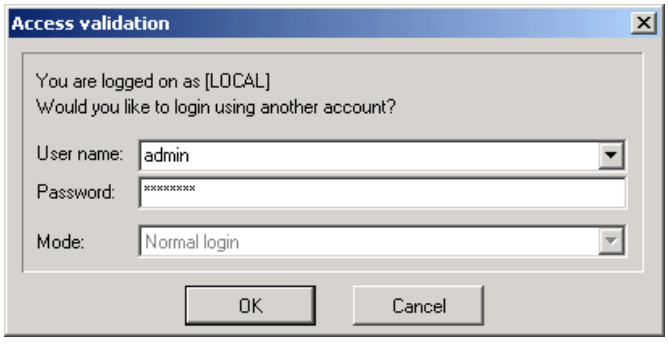
There are 3 special accounts: "Admin", "Local" and "Watchdog"

- "Admin" and "Local" accounts cannot be deleted or disabled (however you can change the list of allowed operations for these accounts). An "Admin" account always has permission to manage other user's accounts. The "Local" account has no password and no permissions for remote connections. The "Local" account may be used only by a staff that has direct access to the system on which HostMonitor is installed. It is also used by HostMonitor at startup. To log in as another user go to the menu "User"->"Login as".
- "Watchdog" account can be used for remote connections established by WatchDog application. This account does not have any rights to manage test list or profiles. You cannot remove this account however you can disable it. Also you may specify a list of IP addresses authorized for remote connections.

To setup and configure users accounts use the menu "User"->"Operators".

Login As

When HostMonitor starts it always uses the special built in user account - "Local". If you want to perform operation(s) that are not permitted for the "Local" user go to this menu item where you may log in as another user at any time. The dialog will ask you to provide a username and a password.



The same dialog appears every time when the user tries to perform an operation that is not permitted for him. In this case within the Login dialog you will have three options:

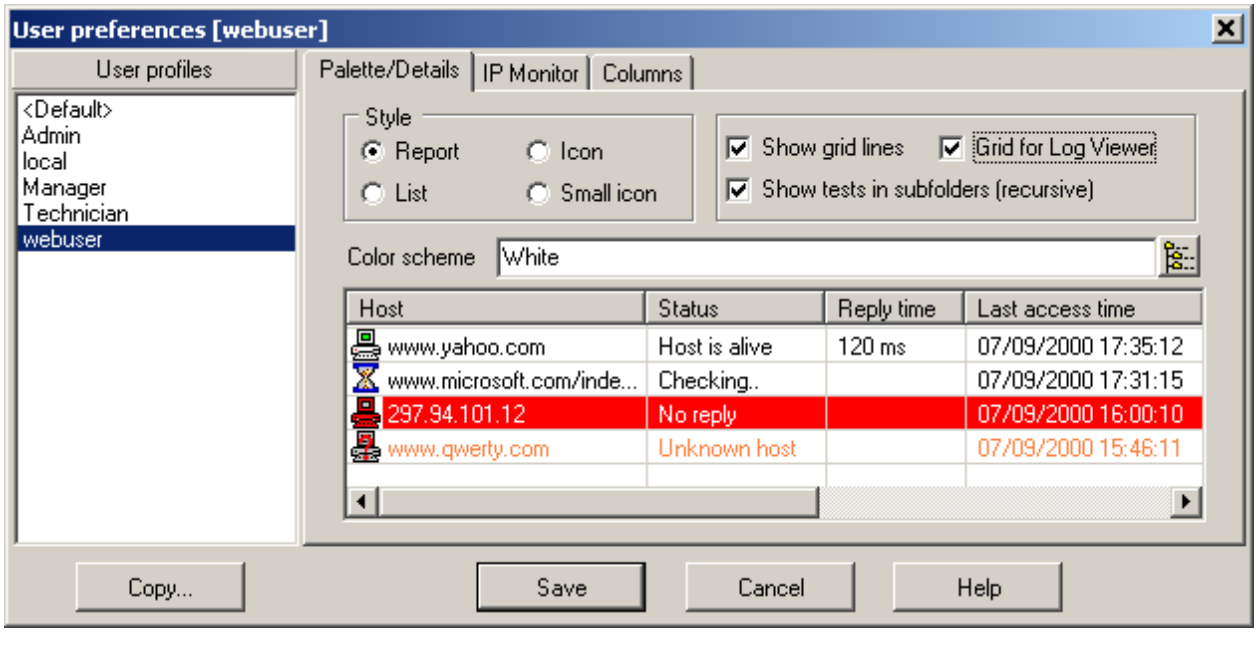
- If you do not have the rights and permission to perform the desired operation then your only choice is the "Cancel" button. Contact your system administrator to acquire the rights for that operation later.

- Log in as another user. Select an account and enter the password if you know it. If you chose «normal login» mode then you will stay logged under the selected account until you or another user will select another account or until the HostMonitor will be restarted.
- In "Temporary" login mode you will gain the rights and permissions of the selected user only for the single operation. As soon as you finish the desired operation, (for example if you wanted to change a test property then "finish" means the test properties dialog is closed) HostMonitor will roll back to the previous user account.

User Preferences dialog

User Preferences dialog allows you to setup various GUI options on per-user basis.
Yes, HostMonitor allows you to setup different color profiles, list of test properties to display, sorting mode, etc for some specific folder(s) of the test list. “Per-folder” level settings may be useful when each operator has its own home folder or you want to distinguish some folder among rest of tests.
While User Preferences dialog allows you to use different GUI settings even if several users have access to the same folder (e.g. “admin”, “manager 1”, “manager 2” and “boss” accounts may have access to Root’ folder (entire test list) but they want to use different color scheme and display different list of test properties).
In other words, you may setup unique color palette and other GUI related options for each operator plus you may set specific color palette for some folder(s) as well. These folder-level settings will be used for all user account.

User Preferences dialog allows you to copy settings between accounts and setup <Default> account. Settings of <Default> account will be applied for each new user account, then admin or user may change its own settings. Note: you may change name of fields using <Default> account only; new name will be applied for all account.
Use menu “User“ -> “GUI preferences” to open this dialog.



There are 2 permissions can be specified for each operator:

- edit GUI options for the account
  With this option enabled operator may change GUI options for its own account only. If operator works with HostMonitor remotely using RCC, settings specified in User Preferences dialog will be stored in the profile on HostMonitor system. This allows operator to move between different remote systems, login to HostMonitor and use the same settings on any

remote system. When user changes column sizes, RCC sends this information to HostMonitor as well.

- edit GUI options for ALL accounts
  If operator with such permission opens User Preferences dialog, he will see list of user profiles and he will be able to change settings for any profile (including <Default> profile), copy settings from one profile to another and so on.
- if operator does not have any of these rights, he cannot change GUI options using HostMonitor. He can change settings using RCC, however these changes will not be stored. Next RCC session will use settings specified for this account by admin (or another operator with necessary rights). This is useful when you want to use the same account for many operators (e.g. guest account).

Note: These GUI settings are applicable to HostMonitor and Remote Control Console (RCC) while Web Service application uses its own profiles.

Interface

Grouped on the Interface page are the general look and feel options that apply to the program, its main window and built-in utilities.

Style
Define how tests are displayed in the Test Detail Area:

- Report - table view, one test per line as a small icon followed by detailed test information
- List - top-down view, a small icon with a test name;
- Icon - tests arranged left to right, a large icon with a test name;
- Small icon - tests arranged left to right, a small icon with a test name.

Color scheme
Choose a color scheme to be used for the main window, log viewer, log analyzer and utilities. Select one of the pre-defined or create a new scheme by pressing the button to the right of the Scheme Name box.
See Color profiles for more information on colors.

Show grid lines
If the option is enabled, HostMonitor will display gridlines to separate task items in the main window.

Show tests in subfolders (recursive)
If the option is disabled, displayed in the Test Detail Area will be tests contained directly in the currently selected folder. If the option is enabled, all tests contained in the current folder and in all of its descending subfolders will appear in the Test Detail Area.

IP-Monitor

Options for the IP-Monitor utility: refresh time, chart colors, number of grid lines.

Columns

Use the Columns page to select columns (test parameters) to display in the Test Detail Area. To select/deselect a column, toggle the check mark next to it. To change a column's display order, highlight the column and then use the Up and Down arrow buttons to the right of the list of columns to display.

The **Sort by** list defines the order in which tests will be arranged. To add a column to the sort order, highlight a column in the left-hand list and then click the Right arrow button. The column will show up in the **Sort by** list. To remove a column from the search order, select a column in the **Sort by** list and then click the Left arrow button.

To change the display name of a column, highlight the column and click the little button to the right of the list box.

Here is a list of test parameters supported by HostMonitor with a brief description of each parameter.

Column name	Field description
Test name	The name of the test
Test method	The type of the test
Test by	Name of the remote agent that performs the test. Field displays "HostMonitor" when the test is performed by HostMonitor
Comment	Any arbitrary comments
Related URL	Test-related URL
Master test	The name of the Master test (for more information on test dependencies see Common test properties)
Interval	The time between two consecutive runs defined for the test
Schedule	The name of the associated schedule
Alert profile	Alert profile name
Private log	The specified private log file name
Created at	The time when the test was created
Modified at	The time when the test was last modified
Status	The current status of the test
Recurrences	The number of consecutive tests resulting in the same status as the current one
Reply	The value last returned by the test (the meaning of the Reply parameter is test specific)
Last test time	The time when the test was last performed
Last status	The status of the previous test
Last reply	The value returned by the previous test (test-specific)
Acknowledged at	The date and time when test status was acknowledged
Acknowledged by	Name of the operator who has acknowledged the test status
ACK comment	Shows the comment which was provided for "acknowledge" operation

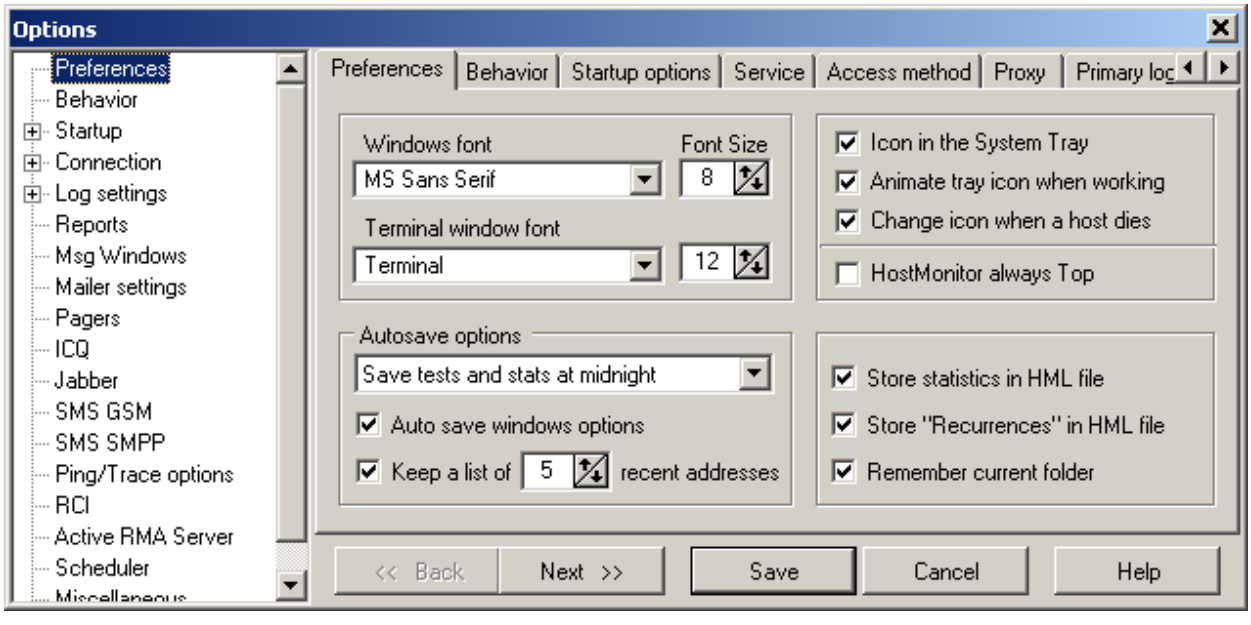
In addition to the static test parameters (test name, interval, status, etc.), and current status related (status, reply, etc.) a number of dynamic statistics data fields are maintained and can be viewed (and reset) in real time.

Column name	Field description
Alive %	"Good" to overall tests ratio, in percent
Dead %	"Bad" to overall tests ratio, in percent
Unknown %	"Unknown" to overall tests ratio, in percent
Total time	The time the test has been in monitoring
Alive time	The overall time the test has had a "Good" status
Dead time	The overall time the test has had a "Bad" status
Unknown time	The overall time the test has had an "Unknown" status
Total tests	Overall tests performed
Passed tests	The number of "Good" tests
Failed tests	The number of "Bad" tests
Unknown resul	The number of "Unknown" tests
Average reply	The average value of the results obtained
Min reply	The minimum value of the results obtained
Max reply	The maximum value of the results obtained
Status changed at	The time when the status last changed
Status changes count	The number of times the status has changed

Also you may add up to 8 custom fields for each account. You can use most of test related variables to define field value and any static text to describe the field (note: you cannot use "historical" variables like %Stat24Hours_MinReply%, %Stat30Days_AliveRatio% and SNMP related variables). You may use one or several variables in each field and static text but you cannot use expressions like %TestID% + %FailureID% (here + will be considered as static text, not mathematical operator, in other words HostMonitor will display value of these two variables, not sum of the values).
For example you may create FolderA for file related test items and tell HostMonitor to display filename, file size and modification time for each test item; another FolderB may contain URL test items and display HTTP response code as additional field.
Note: you may add custom fields for Folders and Views as well.

Options dialog

You can define “global” HostMonitor's settings in the Options dialog window. Customize the color palette for HTML logs & reports, mailer parameters, proxy settings, log file formats, options for utilities, etc. Options are categorized on different pages and navigation is made through a convenient tree structure.
Note: some additional parameters can be specified on startup in the command line.



Preferences

On this page define the following options:

Font options

Windows Font
Choose the font/size for the main window, log viewer, log analyzer and the utilities.

Terminal window font
Choose the font/size for the Telnet utility.

Tray icon options

Icon in system Tray
Hide to tray HostMonitor when it is minimized.

Animate tray icon when working
The program can animate the tray icon when it is in working mode.

Change icon when a host dies

HostMonitor will change icon from blue to red when any host changes status to "bad", or change color to yellow if a test goes to "Unknown" status.

HostMonitor always Top
HostMonitor will remain in front of all other windows (unless minimized).

Autosave options

Do not save test list automatically
If this option is selected, HostMonitor does not save test list modifications automatically. Saving changes is up to the user (use the "Save" and "Save as" menu items in the File menu). If changes have been made, the program will remind you to save them before exiting, loading another TestList, etc.
BTW: HostMonitor will save modification automatically if Windows is shutting down.

Save tests and stats at midnight
With this option selected HostMonitor will save test settings (if test list was modified) and statistical information (Alive%, Dead%, Total time and other counters) every midnight. Of course you may save modifications and statistics manually using menu File -> Save. Also HostMonitor will save modification automatically if Windows is shutting down.

Auto save TestList after any changes
If this option is selected, HostMonitor will automatically save changes every time you add or import new test items, remove a test, modify, enable or disable items, etc. Also HostMonitor will save test statistics every 30 minutes (HostMonitor does not save statistical information constantly for better performance).

Auto save windows options
When this options is enabled the program will save and restore window parameters (column widths, the size of the panels, etc).

Keep a list of N recent addresses
Instructs HostMonitor to keep a history of recently used addresses.

Other

Store statistics in HML file
This option tells HostMonitor to write all statistical information into a file, so that the statistics build up across multiple program sessions. If the option is turned off, when an HML file closes down, the statistics pertaining to its tests get reset. Please note that statistics for any or all of the tests can be nullified at any time using the "Reset ..." menu command

Store "Recurrences" in HML file
This is an important option, because it is the "Recurrences" field that the program looks at to determine what actions and when to fire off. Therefore, if the option is deselected, upon closing an HML file or shutting down HostMonitor, the counter will be reset, so that when the program is restarted, actions will be triggered as tests are first performed. With the option turned on,

recurrence counters will be saved on shutdown, and at the next startup the program will pick up where it left off, as if the program execution was not interrupted.

Remember current folder
If this option is turned on, HostMonitor will remember current folder and display it on the next load of the file with tests.

Allow 2 alert profiles for test items
In most cases single alert profile is enough for test item because each alert profile may contain several actions with different starting conditions, different time restriction options; also you may use "advanced mode" actions.
However in some cases you may reduce number of necessary alert profiles by using 2 alert profiles per test item. If you enable this option, you will be able to assign 1 or 2 alert profiles for each test item.

Behavior

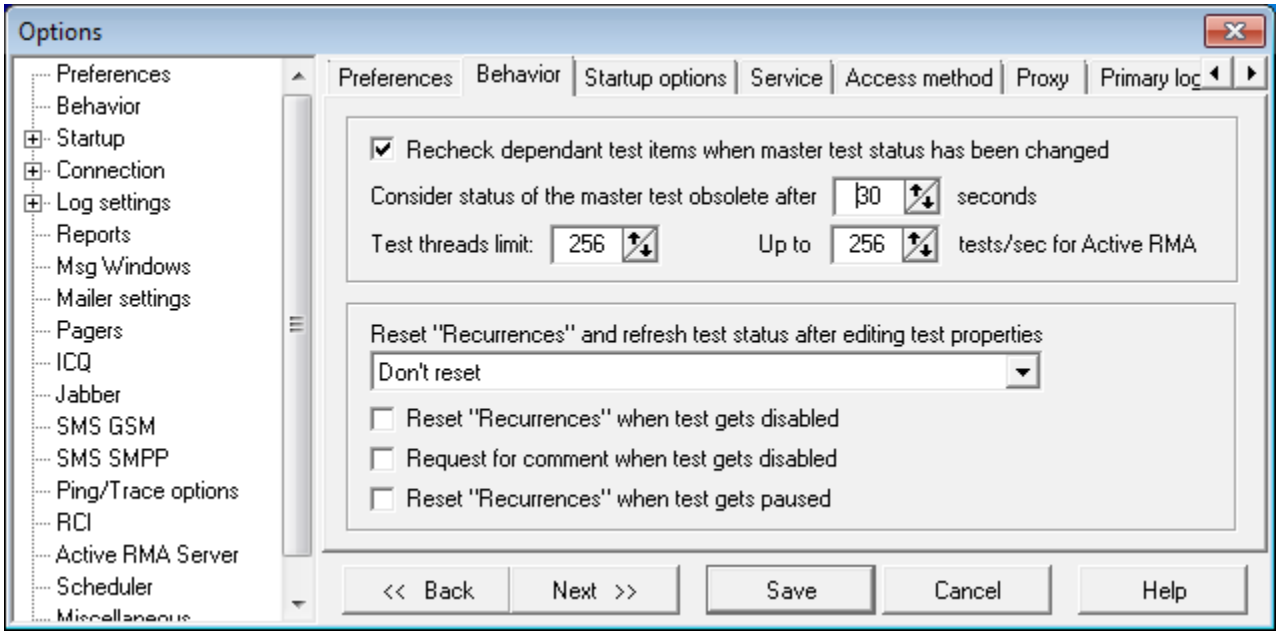
On this page you may set the following options:

Recheck dependent test items when master test status has been changed
This option tells HostMonitor to recheck all dependent test items immediately after their master test failure or recovery (otherwise tests will be executed on regular schedule). This helps to maintain more accurate statistic information.
However HostMonitor does not "touch" dependant items when the master test changes its status to any of the "inactive" statuses (OutOfSchedule, WaitForMaster, Disabled, Paused)
Count inactive master test statuses as well
This option tells HostMonitor to change the statuses of all dependant tests when the Master test becomes inactive (OutOfSchedule, WaitForMaster, Disabled, Paused)

Consider status of the master test obsolete after N seconds
This parameter is used by the program to determine whether the Master test status is up-to-date. Before starting a dependent test HostMonitor checks the status values of the Master tests defined on it. The parameter mandates for how long a Master test status is considered to be current - if Master test was performed more than N seconds ago, HostMonitor will recheck the Master test item before checking dependant items.
Please note: HostMonitor makes an exception for SNMP Trap test methods. If such test is used as Master test, its status never considered as obsolete. In other words status of Master SNMP Trap test will always be considered as up-to-date, regardless of the time when last trap message was received.

Test threads limit [N]
This option replaced old "Do not start more than [N] tests per second" option. Here you set limit for total number of threads used for test execution while HostMonitor will decide how many tests can be started at any given moment. Actually its not firm limit, in some cases HostMonitor may start additional threads (e.g. some tests need a lot of time to provide results).

Up to [N] tests/sec for Active RMA
Sets limit for requests from HostMonitor to ActiveRMA agents



In some cases 20 threads is enough to perform 300 tests per second; in other cases you need 100 threads just for 50 tests/sec (depends on test methods, test settings, speed of your LAN or internet connection and so on).
After significant changes in test list we recommend to let HostMonitor run for some time (at least 10 minutes) and then use Auditing Tool to check for possible problems and recommendations (e.g. it may recommend increasing thread limit or limit related to Active RMA agents).

Reset "Recurrences" and refresh test status after editing test properties
This option will determine the behavior of the program when the user changes the test parameters (using Test Properties dialog). You can choose one of the 3 options:

- Always reset "Recurrences" - after modifying test, program will work as the test was just created, the program will perform test and starts alert actions if needed
- Ask confirmation - the program will ask user about action
- Don't reset - the program will not reset any counters

Reset "Recurrences" when test gets disabled
With this option enabled HostMonitor will reset "Recurrences" counter for a test every time when this test becomes disabled. "Recurrences" field determines what actions to undertake and when to fire off. It means that with this option enabled when test will be disabled and enabled again, actions will be triggered as tests are first performed.

Request for comment when test gets disabled
With this option enabled HostMonitor will prompt for comment every time operator disables test item(s). However operator may continue operation without entering any information (keep comment field empty).

Reset "Recurrences" when test gets pause

With this option enabled HostMonitor will reset "Recurrences" counter for a test when operator (or HMS script) pauses test execution. Note: after Recurrences counter is set to 0, HostMonitor will interpret ANY status assigned to the test by the next check as "new" status and start actions assigned to the test item.

Startup

On this page you can define different options to determine HostMonitor's behavior at startup.

File load mode
This parameter set HML file (file with list of tests) that HostMonitor should use for monitoring

- empty list after load - do not load an HML file
- load file [xxx] - load specified file
- restore last status - reload last used file

Start/Stop mode
Define if program should starts monitoring upon loading or not. There are 3 options:

- start after loading
- stop after loading
- restore last status

Window status
Choose state of HostMonitor's main window:

- minimize after loading - minimize main window after startup.
- maximize after loadng - maximize main window after startup.
- normal size - display window in its normal size after startup.
- restore last status - restore window position, size and state that were set at the last closing of the program

Error handler
This parameter defines program behavior in case error occurs at startup. Choose 1 of 3 options:

- Normal start - show error message (if one occurs) and continue after user confirmation.
- Ignore errors during starting - don't stop and display message.
- Quit if an error occurs - HostMonitor displays message, waits 20 seconds and quits if the user does not press any key to continue.

Also you can override these parameters using command line. See "Command line parameters" section.

Place program in Startup menu
Mark this option to add HostMonitor into Startup group. Windows Workstation NT/2000, Windows XP, Windows Server 2000/2003 will start HostMonitor upon user logon.
On Windows Vista, Windows Server 2008 and newer systems we recommend to use Windows Task Scheduler instead. Please use "Run with highest privileges" option for HostMonitor task.

Also you can install HostMonitor as a service on any system, please refer to "How to install HostMonitor as Win32 Interactive service" section for more information.

Service

HostMonitor uses settings located on this page only when starts as Win32 interactive service (how to install HostMonitor as a service you can read here).

Log on as

Specify user account (login and password) to impersonate the security context of the user.
When HostMonitor starts as a service, it uses the system account (as all interactive services). But this account may not have all the necessary permissions, so some tests will not work correctly (UNC test, "disk free space" test for shared drives, "CPU Usage" test for remote machines, etc). If you need these tests, you will need to assign a special user account. In this case HostMonitor will impersonate the security context of the user.
Note: Do not change the account using the system utility "Services". If you do so, HostMonitor will not be able to interact with the desktop.

Startup delay

In some cases, initialization of dependent applications and services on the HostMonitor machine may consume a substantial amount of time. If HostMonitor's tests depend on these applications, false alerts may be generated while they are initialized.
This setting will cause HostMonitor to wait at least (n) minutes before executing the first monitoring cycle thus allowing applications and services to start and initialize properly. A setting of "1" (one minute) should be adequate for most systems.

When service is being stopped

Define HostMonitor's behavior when service is being stopped, choose 1 of 2 options:

- save changes in HML file
- discard all changes

Access method

On this page define the method to access the net to retrieve URLs.

Type of access to retrieve pages:

- USE REGISTRY CONFIGURATION
  Retrieves the proxy or direct configuration from the registry.
- DIRECT TO NET
  Resolves all host names locally.
- VIA NAMED PROXY
  Passes requests to the proxy unless a proxy bypass list is supplied and the name to be resolved bypasses the proxy.
- PRECONFIG, PREVENT USING JAVA/SCRIPT/INS
  Retrieves the proxy or direct configuration from the registry and prevents the use of a startup JScript or Internet Setup (INS) file.

Proxy

Define the following settings if the access method is set to "VIA NAMED PROXY"

Proxy server - address of your proxy server
Proxy port - port number of the proxy server
Use proxy authentication - if your proxy server require authentication you may specify the username and password in these fields.

Proxy bypass list - list of addresses that don't need to be accessed through your proxy server. This list may include IP addresses, host names, or names of computers from your intranet. Also, wildcards may be used as well to match domains, host names or addresses. For example: www.*.com; 128.*; *man*; and so on. For local addresses use the "<local>" macro. Use semicolons ";" to separate entries.

Log settings: Primary log / Backup log

You may specify Primay and Backup common logs, so there are 2 identical sets of parameters located on 2 pages in the Options dialog:

- [Primary log]
- [Backup log]

For each log you may choose defferent log type (ODBC or File), file format (HTML, Text or DBF) and logging mode (Full, Brief, Midnight or Reply). E.g. you may use Full logging mode for primary ODBC log managed by your SQL server and use Brief logging mode for backup HTML log stored on local hard drive.
HostMonitor can switch from primary to backup log when necessary or use both logs at the same time. Also HostMonitor may execute specified alert profiles when primary or backup logs are not accessible.

First you should decide what type of the log you need: File or ODBC and choose logging mode that will be used for all test items.

Log type

- **None**
  Choose this option if you are really sure you don't need a log
- **File**
  Record test results into a file stored on local hard driver is a fast and most reliable solution. HostMonitor supports three different data formats: plain text, HTML and DBF.
- **ODBC**
  Starting with version 3.0, HostMonitor can write log information into database using any ODBC driver installed on your system (e.g Oracle, MS SQL or MySQL database). It's a very flexible solution - you may define table structure and choose type of the fields to fit your needs. However you must be sure that ODBC driver (provided by 3rd party) works reliable and will not cause HostMonitor to crash.
  E.g. Microsoft dBase Driver v 4.00 causes resource leakage; Oracle driver v8 may crash application.

Default logging mode

This option tells HostMonitor when information should be written. Choose one of the following options:

- Full: Save information about every performed test
  The "Save information about every performed test" option tells HostMonitor to add a record every time a test is performed.
- Brief: Write a record when test status changes
  With this option selected no logging happens as consecutive tests return same status value, until the status changes, at which point a new log record is added.
- Midnight: Write a record when test status changes + midnight logging
  With this option selected HostMonitor records information about current status of all test items at midnight (every night), then no logging happens as consecutive test probes return same status value, until the status changes, at which point a new log record is added.
- Reply: Write a record when test status or reply value changes

While the second option (Brief) is obviously most space-efficient, the first one (Full) allows you to build up statistics on helpful test parameters like response time, reply value, etc. This statistical information can be then parsed and visualized by the Log Analyzer.
3rd option is useful if you are using Log Analyzer to generate reports for different time intervals but you do not want to keep large log files.

Please note: you may change logging mode for particular test items in the Test Properties dialog by choosing one of the options:

- Default - the common settings defined in the Options dialog are used;
- Brief - record information whenever status of the test changes;
- Full - record all test results, regardless of whether their status has changed or not;
- Reply - record information into log every time the status or reply value of the test changes.

File log

If you have chosen "File" as type of the log, then you should define location and name of the common log file. Select one of the following options:

- Log to specific file
- Automatically change the log every month (MMYYYY-Log.ext)
- Automatically change the log every week (WWYYYY-Log.ext)
- Automatically change the log every day (DDMMYYYY-Log.ext)

If you select option to automatically change the log file date macro variables may be specified in the log file name. HostMonitor interprets text between the '**%**' of the log name as a macro, where '**DD**' represents the day of the month, '**WW**' - current week number, '**MM**' - the month, '**YY**' - the year in two digit format, '**YYYY**' - the year.

Log format

- HTML file
- Text file
- DBF file

"File" logs support three different data formats: plain text, HTML and DBF. Each file format has its own strengths and weaknesses.

Plain text:

- Text log is the most compact of the three formats (about 80 bytes per record)
- All fields in a text log are delimited with Tab (09), so you can easiliy import the data from a text log into a spreadsheet or a database

HTML:

- HTML logs are more visual;
- HTML logs can be made automatically available over the Web;
- on the flip side, HTML logs take up a lot more disk space (about 800 bytes per record) than text or DBF logs.

DBF:

- DBF logs are relatively compact (173 bytes per record).

- DBF log data is easy to analyze and manipulate, or import into another DBMS

Please note: The date and time formats used internally in DBF and HTML files do not depend on the system's regional setings. Therefore, changing the system date/time formats has no effect on Log Analyzer's ability to interpret those log elements, which is not the case with the text format. If you choose to keep your log in a text file, and then change the system date/time format, Log Analyzer may have difficulties calculating test parameters of the date/type type, like the alive/dead time. To avoid this problem, turn on the "Use fixed date&time formats" option located on the Miscellaneous page in the Options dialog. In this case, HostMonitor will use the date&time formats specified, regardless of the system settings.

Also, If you are running several instances of HostMonitor using different test lists (HML files), please use separate log files as well.

ODBC Log

If you have chosen “ODBC” log type, then you should specify data source and SQL query for the logging.

ODBC data source
Choose one of ODBC data sources available on your system.

Note #1: Windows provides system data source names and user data source names (System DSN and User DSN). User data sources are local to a user and accessible only by the specified user.
If you start HostMonitor as service, it will not be able to use User DSN. So, if you are planning to start HostMonitor as service and as regular application, select “System DSN” option (that is located on Misc page in the Options dialog) and choose system ODBC data source for the logging. In this case HostMonitor will work equally in both modes.

Note #2: you must be sure that ODBC driver (provided by 3rd party) works reliable and will not cause HostMonitor to crash. E.g.
- Microsoft dBase Driver v 4.00 causes resource leakage;
- Oracle drivers version 8 and especially version 10 have a lot of bugs, these drivers may lead to high CPU usage, handles and memory leakage and may crash application.
- MySQL ODBC drivers version 8.00.11 – 8.00.15 may lead to various problems as well, including memory access violations. If you need to use MySQL ODBC driver version 8.x, please set two options in hostmon.ini file, [Misc] section:

```
[Misc]
ODBC_UseSharedEnvHandle=1
ODBC_KeepSharedEnvHandle=1
```

Login
Specify user identifier, if necessary.
Note: some ODBC drivers (e.g. MS SQL ODBC Driver version 13.1+) support Integrated Windows authentication and Active Directory Integrated authentication. In this case you may type `WindowsAuth` instead of login name (for Integrated Windows authentication) or set `ADAuth` as

login name (for Active Directory Integrated authentication). Password field is not used in such case.

Password
Specify password, if necessary

Timeout
Specify the number of seconds to wait for a login request to complete. If value is 0, the timeout is disabled and a connection attempt will wait indefinitely.

SQL Query
Here you should specify SQL query to logging test data. Format of the query is up to you; you may use the macro variables to put in as much detail as you want. For instance SQL command might look like this:
INSERT INTO HMLOG (EVENTTIME, TESTNAME, STATUS, REPLY, TESTID, TESTMETHOD, Recurrences) VALUES ('%DateTime%', '%TestName%', '%Status%', '%Reply_Number%', %TestID%, '%TestMethod%', %Recurrences%)
Of course an appropriate database table has to be created before you start using the ODBC logging. However some parameters are obligatory, especially when you plan to use Log Analyzer. Database logging table should store the following information:

Macro variable	Field type	Alternative variable(s)	Alternative type	Meaning
%DateTime%	datetime or timestamp			time of the event
%TestName%	char or varchar			name of the test item
%TestID%	int			unique test ID*
%TestMethod%	char or varchar			test method**
%Status%	char(16) or varchar	%StatusID%	int or tinyint	status of the test
%Reply%	char or varchar	%Reply_CStyle% %Reply_Number% %Reply_Integer% %SuggestedReply%	char or varchar decimal or float int char or varchar	reply value***

* ID is unique within test list (HML file). If you are running several instances of HostMonitor, test item from listA may have the same TestID as different item from listB. In such case you may use separate tables for each instance of HostMonitor or add additional field and use %HM_FILEGUID% variable.
** If you are using descriptive names for your test items, you may skip this field. However it's better to use TestMethod field, unless you need to keep your database as compact as possible
*** If you don't need very accurate statistics for Traffic Monitor and/or Performance Counter test items, you may use %Reply_Integer% variable and int data type.

Note 1: Maximum length of the query: 4096 symbols.

Note 2: If you click button, HostMonitor opens "Expression editor" window for convenient SQL Query editing.

Note #3: If you are using Log Analyzer and you have chosen "ODBC" as primary log, you should describe database parameters using "ODBC logs Manager" dialog (that is available thru Log Analyzer menu File -> Setup ODBC logs) and mark "Use this source as default" option. This allows you to use ODBC logs for "Statistics" feature (HostMonitor: menu Test -> Show statistics).

Alerts

Execute alert profile when log inaccessible
If you mark this option and choose alert profile, HostMonitor will execute specified actions when it's impossible to record data into the log (e.g. disk is full or SQL server does not respond).
Note: only "scheduled" actions will be executed, i.e. a condition to start action should be set to "on the schedule" (in Action Properties dialog).

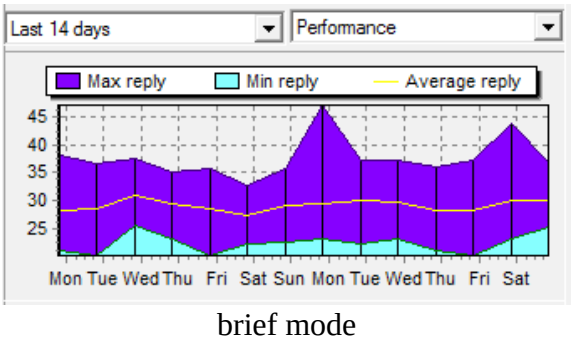
Execute alert profile when log comes to life
This option tells HostMonitor to execute specified actions when log becomes accessible (e.g. link to SQL server was restored).
Note: only "scheduled" actions will be executed, i.e. a condition to start action should be set to "on the schedule" (in Action Properties dialog).

Compact Logs

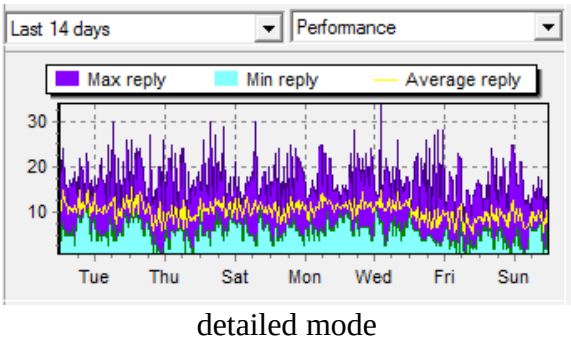
History-related windows may display performance charts using 2 modes:

- brief (works without log files)
- detailed (requires compact logs)

HostMonitor automatically chooses detailed or brief mode for charts. If you just installed HostMonitor version 13, there are no data yet so Brief mode will be used. After 5-10 minutes HostMonitor may switch to Detailed mode for some time intervals (Today; Last 24 hours). In couple days HostMonitor may enable Detailed mode for [Yesterday], [Last 48 Hours], [Last 7 days], [Last 14 days] time intervals. And finally Detailed mode will be enabled for [This month], [Last 30 days], [Last moth], [Last 60 days] intervals.
Note #1: [This year], [Last year], [Last 12 months], [Last 24 months] - only brief mode supported for such time intervals.
Note #2: If you disable **compact logs** , only brief mode will be used.



brief mode



detailed mode

If you are using Brief or Midnight mode for Primary/Backup log files while you need detailed historical charts (Test History, SysInfo, SuperMatrix, NetMap windows), you may enable Compact logs. HostMonitor will store extra data in specified folder, keep results related to last 2 months and remove older data.

If you are using Full logging mode for Primary log file, you still may like detailed charts because HostMonitor charts can be displayed within 1 second while Log Analyzer may need a minute in order to parse large log files.

Disk space requirements
If you set 100,000 test items and HostMonitor performs over 1,000 tests per second, such data files may consume about 10GB of disk space.
If you set just 5,000 test items and perform 50 tests/sec, then data files will consume about 500MB of disk space.

See also Auditing Tool → Log files

System Log

HostMonitor uses the system log to record events like start/stop monitoring, as well as information on started and/or failed alert actions. You can either specify a particular file name for the log, or use date macro variables to have HostMonitor switch to a different file every day, week, month or year.

There are two more options available:
- Record info about successful actions
- Record info about failed actions

You can select one, both, or none of these options.

To get more information about different logging options available in HostMonitor, please, refer to "Log & Reports" section.

User operations log

HostMonitor may record operations performed by local or remote operators, operations performed by HM Script or HostMonitor itself. It records information about enabled and disabled test items, paused and refreshed items, removed folders and tests, modified folders, views and tests, started scripts, import operations and so on. Each type of operation has its own ID. List of such operations listed in Appendix #2.

For each operation HostMonitor records:
- Event time
- Operator type (HostMonitor, local operator, remote operator, HM Script, import procedure)
- Unique ID of the operator and operator's name (for local and remote operators)
- Operation ID and operation name (XML log file contains operation ID only)
- Item ID (usually this is test ID or folder ID, e.g. if you move test item, this field will show test ID)
- Result (Done, Rejected or Failed)
- Description (may contain test name, folder name, some comments)

File name

If you enable this log, you should specify file name for the log using .html, .txt, .dbf or .xml file extension. HostMontor will choose file format accordingly to specified file extension:

- TXT	simple TSV (tab separated values) text file
- DBF	dBase file that can be opened by various database applications including Excel and Access
- HTML	Hypertext Markup Language, can be viewed by any modern web browser
- XML	the most versatile file format. It can be used for data import and processing; also data from XML file can be displayed directly by web browsers. There is userlogstyle1.xsl file – sample XSLT file (styles for XML file) that can be used with XML log. You may easily modify these styles or create your own styles and filters. Also for group operations (e.g. you pause or disable set of selected test items) this format provides most compact records.

Also, you may set the following filters:

Results filter
You may choose what operations should be recorded (filter by operation result)
- Successful
- Rejected
- Failed

Operators filter
You may choose "operation source" that should be recorded:
- HostMonitor (e.g. HostMonitor itself may load specified test list on startup)
- Local operators (operators that work directly with HostMonitor console)
- Remote operators (users connected thru RCC, Web Service or Telnet Service)
- HM Script
- Import procedure

Include list of tests
Also you may enable "Include list of tests" option for group (bulk) operations such as:
- Tests imported from text file
- Folder refreshed
- Folder resetted
- Folder enabled
- Folder disabled
- Folder removed
- Folder copied

E.g. if you enable "Folder disabled" item in this filter, HostMonitor will record list of disabled tests when you perform "Disable this folder" operation. Otherwise HostMonitor will write just 1 record with information about disabled folder.

External syslog

HostMonitor may send test results, action results, diagnostic messages, RCI and Active RMA related messages to external Syslog server.
"External Syslog" page in Options dialog offers the following option:

Send logs to host
If you want to send data to external Syslog server, mark this option and provide hostname or IP address of the server
Port
Specify port on which Syslog server is listening for incoming UDP packets (UDP protocol is suitable for fast, efficient transmission however there is no guarantee that all messages sent would reach the server)

Test results
Mark this option if you want to send test results to Syslog server. Note: if you want to send results of some specific test item, you may use Syslog action instead
Message template
Here you should specify syslog message template. Format of the message is up to you; you may use the macro variables to put in as much details as you want. For instance template might look like this: [%TestID%] %TestName% status: %Status% %Reply%

Brief mode	send data to the server when test status changes
Reply mode	send data to the server when test status or reply value changes

Facility – specify facility number for messages related to test results

Action results
Mark this option if you want to send action results to Syslog server.

Send errors	send data to the server when action failed for some reason
Send all results	send information about failed and executed actions

Facility – specify facility number for messages related to action results

Monitor messages
With this option enabled HostMonitor will send diagnostic messages to the server

Send errors	send to the server error diagnostic messages (e.g. HostMonitor cannot open RCI port for listening, cannot create report or ODBC logging pool is full)
Send all results	send to the server all diagnostic messages

Facility – specify facility number for diagnostic messages

Active RMA log
Information about connection requests from Active Remote Monitoring Agents will be sent to the server when this option enabled:

Rejected requests	with this option selected HostMonitor will send information about rejected connection requests from Active RMA
All connections	HostMonitor will send information about rejected and successful connections from the agents

Facility – specify facility number for messages related to Active RMA

RCI log

Information about connection requests from remote operators will be sent to the server when this option enabled:

Rejected requests	with this option selected HostMonitor will send information about rejected connection requests from the remote users. E.g. RCC, Web or Telnet operator tried to connect from non-allowed IP address or used invalid password
All connections	HostMonitor will send information about rejected and successful connections from the remote users (RCC, Web Service and Telnet). Options located on RCI page tell HostMonitor to exclude or include WatchDog account (account used for WatchDog application).

Facility – specify facility number for Remote Control Interface messages

Facility

The logging facility parameters allow administrators to logically separate messages. Messages with different facilities may be handled differently, e.g. write records to separate files, forward them to different destinations, etc.

That's why HostMonitor allows specifying facility number for each kind of logging data.

Severity

Severity level of the message set automatically by HostMonitor:

Critical	- reserved for cluster mode, not used yet (e.g. cluster node disconnected)
Error	- tests status changed to "Bad", "No answer" or "Bad contents"; - action failed; - error diagnostic message (e.g. HostMonitor cannot create report or ODBC logging pool is full)
Warning	- test status changed to unknown or warning; - rejected RMA and RCI connections (e.g. IP address not allowed or invalid password used)
Notice	- other test statuses (e.g. test status changed to "Ok" or test was disabled); - operator acknowledged "bad" test status; - acknowledged test fails again with different reply
Informational	- executed actions; - accepted RMA and RCI connections; - informational system messages (e.g. monitoring started)

Log processing

HostMonitor can switch from primary to backup log when necessary or use both logs at the same time. Choose one of the following options:

Use backup log when primary is not accessible
If both logs are specified, HostMonitor uses primary log until 1st failure. When logging operation fails, HostMonitor switches to backup log right away. However it will try to use primary log for the following test probes and switch back to primary log in case of success. If logging operation fails 8 times in a row, HostMonitor will not check primary log for the next 5 min.

- **Use primary and backup logs all the time**
  This option tells HostMonitor to use both logs at the same time. It has sense when you are using different logging options for primary and backup log. E.g. you may use Full logging mode for primary ODBC log managed by your SQL server and use Brief logging mode for backup HTML log stored on local hard drive.

Special file processing

The following options allow you to manage log files: e.g. you may set HostMonitor to remove files older than 3 months, or you may configure HostMonitor to keep just 2 log files - for previous and current month.

There are 2 similar sets of options: one for common log files, another - for private log files.

You may define command line for execution and choose one of 3 available options to specify when HostMonitor should execute external command for processing common log file(s):

- **If common log(s) was created <N> days/weeks/months/years ago**
  with this option selected HostMonitor will apply specified external command for each log file that was created specified number of days/weeks/months or years ago. HostMonitor checks age of log files once a day (normally at midnight).
- **If common log(s) is bigger than <N> KB**
  with this option selected HostMonitor will apply specified external command for current log file only when its size reaches specified limit. ("current" means this option does not affect old log files into which no records are added anymore).
- **If common log(s) is switching**
  with this option selected HostMonitor will apply specified external command for current log file when HostMonitor switches to another (new) log. E.g. if you use "Automatically change the log every month" option, HostMonitor will execute specified command before creating new log at midnight every 1st day of every month).

Please read notes below. Some important restrictions apply to external programs.

You may choose one of 2 options to specify when HostMonitor should execute external command for processing private log file(s). They could be same as for common log (above) or different:

- **If private log(s) was created <N> days/weeks/months/years ago**

with this option selected HostMonitor will apply specified external command for each log file that was created specified number of days/weeks/months or years ago. HostMonitor checks age of log files once a day (normally at midnight).

- **If private log(s) is bigger than <N> KB**
  with this option selected HostMonitor will apply specified external command for current log file only when its size reaches specified limit. ("current" means this option does not affect old log files into which no records are added anymore).

Please read notes below. Some important restrictions apply to external programs.

Execute command:
You may specify 2 commands for execution: one for common log files, another for private logs. You may use special variables in the command line:

%log%	represents full name (including path) of the log file (e.g. C:\Program Files\HostMonitor\Logs\04-2004.htm)
%logpath%	represents path to the log file (including trailing back slash. E.g. C:\Program Files\HostMonitor\Logs\)
%logname%	represents name of the log file (e.g. 04-2002.htm)
%logext%	represents extension of the log file (e.g. ".htm")

(!) Please note:
When you design external command/application for log processing you should consider following: external application MUST NOT lock CURRENT log file for more than 60 seconds. If it does, HostMonitor will terminate external application to unlock the log.
So, if you want to perform some operation that can take more than 60 sec (e.g. pack log file or move it to slow backup device), move it to another folder or rename log file first and then start slow process. See example #4
On the other hand, this limitation is not applicable for processes that work with old log files. If you change log file dynamically and want to pack old log files, you may do this without any restrictions. See example #2 and #3

Examples:

1) If you want to keep 2 log files at any moment: one log for current month and another for previous month, you may use following settings:
   - If common log(s) `[was created 1 month ago]` execute command `[cmd /c move /y "%log%" "%logpath%oldlog%logext%"]`
   - Name of the log file could be static, you don't need to use "Automatically change the log every month" option (but you may use this option if you want)

   Please note: 1 month ago doesn't mean exactly 1 month (30 or 31 days) ago. It means "previous" month. E.g. if log file was created in October (any day of the October), HostMonitor will execute specified command on November 1st.

2) If you want to keep log files for last 3 months, you may use following settings:
   - If common log(s) `[was created 3 months ago]` execute command `[cmd /c del "%log%"]`
   - Name of the log file should be dynamic. Use "Automatically change the log every month (week or day)" option

3) If you want to zip old log files once a year,
   - Use "Automatically change the log every month (week or day)" option
   - Set If common log(s) `[was created 1 year ago]` execute command `[pkzip c:\logs\archive.zip "%log%"]` option

   Here you may start archive program to pack log file. It will lock the file but it's not a problem in this case - HostMonitor switches to a new log (because of "Automatically change the log" option)

4) If you want to zip current log file when it reaches 1,000,000 Kb simultaneously starting new log, this is more complicated because archiver is not allowed to lock log file for more that 1 minute.
   One of possible solutions:
   - You may create simple BAT file with the following commands

     ```
     cd %~p1
     mkdir tmp
     move /y %1 tmp\%~n1%~x1
     pkzip c:\logs\archive.zip tmp\%~n1%~x1
     ```

     Comments:
     3rd command moves log file, it allows HostMonitor to create new log. If you move file within the same drive, Windows moves it fast;
     4th command starts archiver that may pack new (moved) file as long as it needs, HostMonitor will work with another file
   - Use If common log(s) `[is bigger than 1000000 Kb]` execute command `[cmd /c NameOfTheBATfile.BAT %log%]` option to start that BAT file

If you set Private logs for 10,000 test items and tell HostMonitor to set new log files on daily basis, then you will have 300,000 log files just in one month; 3,650,000 log files per year. HostMonitor v12.42+ uses low priority thread usually started after midnight to process log files. You may set specific time for log processing using DailyTime parameter in [Logging_PrivProcessing] section of HostMon.INI file (e.g. DailyTime=0222 tells to start log processing at 2:22 AM).

The following options (when set) can trigger log processing commands during daytime:
- if common log is switching
- if private logs is bigger than N KB

usually this is not a problem, these commands will process just 1 log file, not 300,000 files

HTML Colors

Customize color scheme for HTML log files. You can use Color Profiles dialog to select scheme or create new one (use button to the right of the Scheme Name box to bring up Color Profiles dialog).

Log Viewers

For each type of log file (HTML, Text, DBF) select one of the options:

- Internal - use the build-in viewer
- Associate program - use the default Windows viewer for file
- External - use an external viewer. Define a command line to start the program that will be used as the viewer. The name of the log file to view can be passed to this program as a parameter using macro variable **%LOG%**. E.g. "notepad.exe %Log%"

Reports

HostMonitor can generate HTML, DBF, WLM, and Text reports with the information about tested hosts (e.g. for publishing on your WEB or WAP site, for sending with E-Mail notification, or for analyzing). On this page you can define a list of up to 6 global reports (reports that apply to all tests in the working HML file). Just select report profile from drop-down list and specify name of a target file (you can use a naming pattern to have HostMonitor switch to a different file every day, month, year, etc., as prescribed by the date macro variables appearing in the pattern).
Also you can bring up Report Manager dialog to configure an existing report or create a new one.

There are two more parameters that can be specified on this page:
Generate reports every N min
Tells HostMonitor how often reports should be generated

Execute action profile when complete
With this option enabled HostMonitor will launch the specified alert profile after reports were generated (for example you may use this option to send reports by e-mail). Note: only "scheduled" actions will be executed, i.e. a condition to start action should be set to "on the schedule" (in Action Properties dialog).

Use "Generate reports now" button to immediately create reports (for testing purposes).

Note #1: Additionally, each folder may have its own report list; only the tests contained in the folder will be used to generate these folder-specific reports. For more information about folder, please, refer to "Folders" section of this documentation.
Note #2: To exclude some tests from reports use test property "Exclude from reports".
Note #3: If you need to create reports every time a test changes its status add the "Generate reports" action to the Actions Profile. The other way to implement the same behavior would be to add a "Run HMS Script" action, and include a CreateReport command in the script to execute.
Note #4: Also reports can be generated at user request at any time through the Reports menu in HostMonitor's main window.

Message window settings

HostMonitor can display a popup window when a test changes its status (as long as you specify the "Show message" option in the alert profile for the test). On this page of the Options dialog window you can define the parameters for this popup window.

Position

You can choose "Predefined position" option and define the coordinates for the top left corner of the window. Or choose "Show in the last remembered position" option and HostMonitor will remember the window position on the screen and will display the popup window in the same location.

Time live

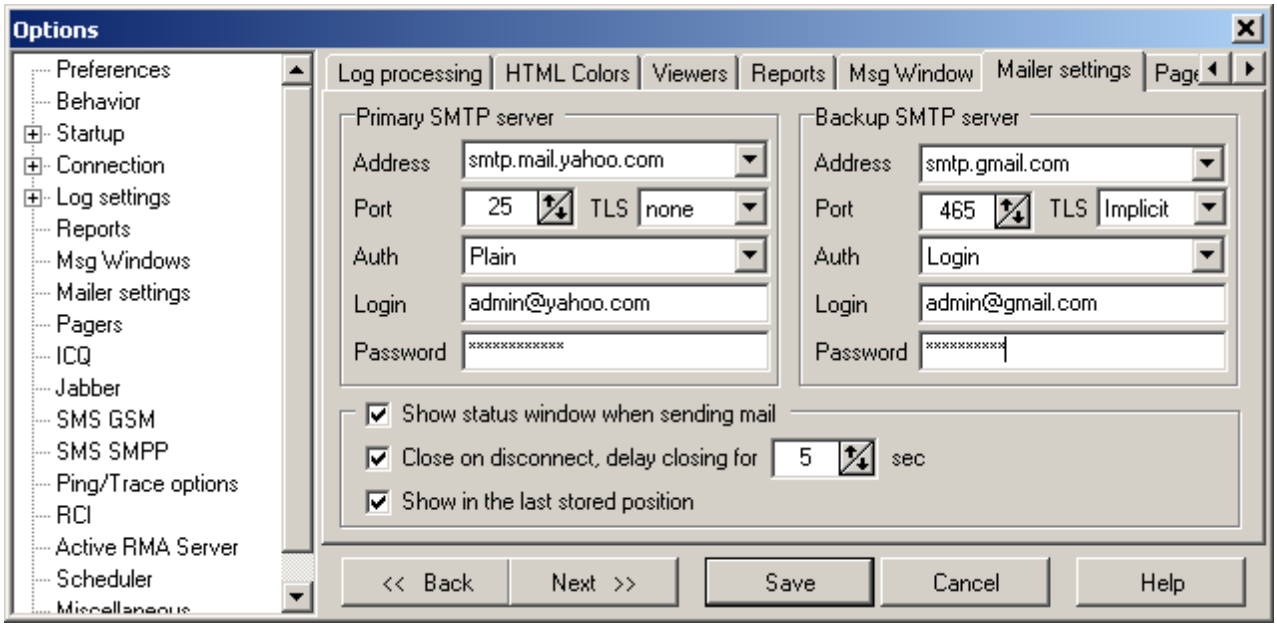
- "Close after N sec" - Select this option and specify the amount of time a window will stay open before automatically closing, unless the [Close] button is selected or the [Stop] button is used to stop the countdown.
- "Close manually" - Window will stay open on screen until the [Close] button is used.

Stay on top" style

Popup window will appear in front of all other windows

Mailer

On this page define the settings for the build-in mail client.



Primary SMTP Server

Address
IP address or hostname of your SMTP server.

Port
TCP port number used by the mail server for incoming connections (normally SMTP servers use port #25 unless server requires secured connection).

TLS
This option allows you to use secured and encrypted connection (SSL). You may set "None" option to use unencrypted connection, select "Implicit" or "Explicit" to use encrypted connection.
*Note 1: not every mail server supports such options; normally mail servers that use "Implicit" security mechanism accept connections on TCP port 465; "Explicit" security mechanism usually use TCP port 587

Authentication method
Select one of authentication methods: None, Plain, Login, Cram-MD5, CRAM-SHA1, NTLM or POP before SMTP
* POP before SNMP option notes: HostMonitor chooses the TCP port for POP3 connection based on TLS mode (None-110, Implicit-995, Explicit-995). You can also set a specific port for POP3 connection when "POP before SMTP" authentication mode is used: add 1 or 2 lines in hostmon.ini file, [SMTP] section. E.g. if you want to set TCP port 2095 for the primary mail server and port 110 for the backup mail server, add the following 2 lines to the [SMTP] section and restart HostMonitor
Pop3Port1=2095
Pop3Port2=110

Login
Specify login (if authentication method is not None)

Password
Define password (if authentication method is not None)

The same parameters you can define for the **Backup SMTP server**. When HostMonitor tries to send e-mail, at first it uses Primary SMTP server. If in consequence of some error this is impossible, HostMonitor tries to send e-mail using Backup SMTP server.

Show status window when sending mail
With this option enabled, HostMonitor will display a window when sending e-mail and show all requests to and answers from the mail server.

Close on disconnect, delay closing for [N] sec
If you enable this option, HostMonitor will close the window after a specified time interval after disconnection. Or, press the [Close] button to close the window immediately or the [Stop] button to continue displaying the window on the screen.

Show in the last stored position
The status window will save its coordinates and restore back to those coordinates when displayed again.

Pagers

Use this page to setup general settings for the subsystem which sends messages to pagers and beepers. Information related to specific pagers may be defined in each Send message to pager action.

Device
Specifies your TAPI device (modem) which will be used by the program. Select a modem from the drop-down list or select the "**Auto select free TAPI device item**". In this case HostMonitor will search through all the compatible devices on the system and attempt to send the message. If one port is busy, it will try the next port until it has exhausted all the compatible TAPI ports.

Baud rate
Specifies the baud rate that will be used to communicate with your modem. This can be any of the following: "300", "1200", "2400", "4800", "9600", "19200".

Modem init string
This is the initialization string for your modem. The modem must then respond with an "OK". You can leave the default value as "**AUTO**" in this parameter. HostMonitor will search your Modem's INF file from Windows and prepare a string that will work with most paging carriers. If the default string does not work, you will need to search the modem's manual and figure a string that will work. Any time you need to replace the string use the tilde character (~) (i.e. AT&F~). If you need to pause, the hat character (^) will give you a one second pause. (i.e. AT&F~^^AT~). The maximum length of the modem initialization string is 80 characters.
Specify a termination string by placing a vertical bar (|) after the modem init string. By specifying AUTO, it will use the strings specified in the modems INF settings. Examples: (AT~|ATZ~) (AUTO|AUTO)

Modem dial string
This is the string the program will send to the modem when it is ready to dial. The default value is "ATDT". If only a pulse dialtone is available, "ATDP" must be passed to this parameter. To control how long HostMonitor will wait for a connection before giving up, pass "TO=20" where 20 is the number of seconds desired. For example, the string to use here is: "TO=20,ATDT".

Show status window when dialing
HostMonitor can display a window when sending messages to a pager, displaying how it sends the message and the results of the operation (also, the program writes the result of sending the message into a log file).

Close window on disconnect, delay before close [NN] sec
After a specified time interval, HostMonitor will close the message window after sending the current message. Press the [Close] button to close the window immediately or the [Stop] button to keep the window onscreen indefinitely.

If device(s) busy wait up to [xx] min
Specify how long the program will attempt to resend messages.

ICQ

If you want to use “Send message to ICQ” action method, specify parameters of your primary and backup (optional) ICQ accounts here. For each account you should provide UIN and password.

Why do you need backup account?
HostMonitor utilizes message queue, uses deferred logout algorithm and some other tricks to make message delivery as reliable as possible. However ICQ servers use anti-spam technologies and may temporarily lock your account or do not accept messages for a while. When this happens HostMonitor switches to backup account.
If you do not specify backup account, HostMonitor will utilize flow control options provided by ICQ protocol.
Please note: we do not consider "Send message to ICQ" action as reliable way to notify network administrators about critical network problems.

Jabber

If you want to use “Send message to Jabber” action method, specify parameters of your primary and backup (optional) Jabber accounts here. For each account you should provide the following parameters:

Login server
Host name or IP address of the server

Jabber ID (JID)
Every user on the network has a unique Jabber ID (usually abbreviated as JID). To avoid the need for a central server with a list of IDs, the JID is structured like an e-mail address with a username and a DNS address for the server where that user resides separated by an at sign (@), such as username@domain.com

Password
Password

SSL/TLS
This option allows you to use secured and encrypted connection. You may set “None” option to use unencrypted connection, select “Implicit” or “Explicit” to use encrypted connection.
*Note 1: normally Jabber servers that use “Implicit” security mechanism accept connections on TCP port 5223; “Explicit” security mechanism usually use TCP port 5222

Port
TCP port used by the server. Normally Jabber server listens on port 5222

Note: when you specify login server you should provide the host name (e. g. www.jabber.org) or IP address (e. g. 204.71.200.68). Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) and specify hostname with suffixes ::ipv4 or ::ipv6 (e.g. www.jabber.org::ipv4 or www.6bone.net::ipv6).

If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.
Note: on Windows NT 4.0, Windows 2000 and Windows XP SP1 IPv6 protocol is not supported. You may use menu Tools -> Local Info to check is your system IPv6 ready.

SMS: GSM

If you have GSM modem (cell phone) connected to the system where HostMonitor is running and you want to use "Send SMS" action to send SMS messages to your support staff or some devices, specify parameters of your primary and optional backup GSM modems here.
If you have 2 modems connected to the system and HostMonitor cannot send SMS through the primary modem, it will try to send messages using backup cell phone.

For each GSM modem you should specify the following parameters:

COM port
Specify COM port to which GSM modem is connected.

Baud rate
Specify the baud rate that will be used to communicate with your modem.

Modem type
Choose type of the cell phone that you have connected to the system. HostMonitor supports the following devices:

- Ericsson GM12
- Ericsson K750i
- Ericsson W660i
- Huawei E220
- Huawei Mobile Connect 3G
- Maestro 20 GSM
- Motorola G20
- Motorola T260
- Multi-Tech MTCBA-E
- Multi-Tech MTCBA-G-F1-EU
- Nokia 6210
- Nokia 6310i
- Nokia 6650
- Nokia 9110
- Nokia N30
- Siemens A1
- Siemens M1
- Siemens M20
- Siemens M35

- Siemens ES75
- Siemens TC35
- Siemens S25
- WaveCom
- Wavecom Fasttrack
- Z-text Fixed Line SMS modem

If you do not see your phone in the list, you may try to choose similar model. For example Seimens C45 and Siemens S45 both work like Siemens M35.
Also you may choose Custom mode.

Mode
Choose the type of SMS format that should be used by your GSM modem. When the modem supports both formats (Text and PDU), the PDU mode is recommended

PIN
Provide PIN of the SIM card installed in your modem (cell phone)

Service center
The SMS center number, e.g. +17044100000 (Sprint, USA), +17057969300 (Rogers, Canada) or +491710760000 (D1, Germany)

Logging options
SMS module has its own logging options. Why? HostMonitor puts messages into query and does not spend its resources to manage GSM modems. Separate module, called SMS spooler, manages messages and works with the modems.

SMS log
Choose one of the following logging options:

- No log
- Failed events only
- Failed and successful events
- Detailed tech info

Log file
Provide the path to the log file. If you use .HTM or .HTML extension for the file, SMS spooler will create log file in HTML format, otherwise TEXT format will be used

Custom AT commands
When you choose "Modem type: custom" HostMonitor creates simplified script for your modem considering PDU/Text mode, PIN number, service center number. E.g. commands may look like

```
AT+CMGF=0
AT+CMGS=%PDULen1%>%Message0PDU%^Z
```

another example

```
AT+CPIN="1111"
AT+CSCA="+12065415500"
AT+CMGF=1
AT+CMGS="%DestPhone%">%MessageText%^Z
```

Also, this mode tells HostMonitor to ignore most of errors, often SMS can be delivered even if some commands were rejected by modem.

You may modify commands manually, using different commands for primary and backup modem. Use the following variables and special symbols:

^Z	as EOF symbol
^J	as LF (line feed) symbol
>	tells HostMonitor to wait for '>' prompt from modem
%DestPhone%	destination phone number specified for the action
%MessageText%	text message created by "Send SMS (GSM)" action according to specified template and test results
%MessagePDU%	message encoded as Packet Data Unit (includes destination number, does not include service center number)
%Message0PDU%	message encoded as Packet Data Unit with leading 00 characters (includes destination number, does not include service center number)
%MessageSCAPDU%	encoded packet with service center number, destination number and the message
%PDULen%	size of the PDU message
%PDULen1%	size of the PDU message (%PDULen1%==%PDULen%+1) – for some modems you need %PDULen%, for other %PDULen1%

Test

"Test" button allows you to check your settings and modems right away.

Please note:

1) HostMonitor will not send testing SMS when SMS spooler is busy sending messages that were initiated by "Send SMS" alert actions.
2) SMS Test window will display technical information about your testing SMS; then it may display information about SMS messages that were initiated by "Send SMS" action started at the test execution time (if any).

SMS: SMPP

In order to use "Send SMS (SMPP)" action you should specify parameters of your primary and optional backup SMPP accounts. If you provide 2 SMPP accounts and HostMonitor cannot send SMS through the primary account, it will try to send messages using backup account.
For each account you should specify the following parameters:

Host
Provide host name or IP address of the Short Message Service Centre (SMSC).

Port
Provide the port that SMSC is listening on for connections from SMPP clients.

System ID
Provide the account that should be used to login to the SMSC.

Password
Provide the password that should be used to login to the SMSC.

Source Address
Specify source address

Source TON
Type of the Number (TON) used for "Source Address". Choose one of the following options:

- Unknown
- International
- National
- Network Specific
- Subscriber Number
- Alphanumeric
- Abbreviated

We recommend using "International" format of the adresses (number starts with the country code followed by the national destination code and the subscriber number, e.g. +17057969345).

Source NPI
Source Numbering Plan Indicator (NPI) - type of numbering scheme used in telecommunications. Choose one of the following options:

- Unknown
- ISDN (E163/E164)
- Data (X.121)
- Land Mobile (E.212)
- National
- Private
- ERMES
- Internet (IP)

Please consult with your SMPP service provider for the list of supported options.

Ping/Trace

On this page specify parameters for the Trace utility and for Ping tests.

Packets to Send
Specify the number of ECHO packets.

Packet Size
Specify the size of ECHO packets.

Timeout
Specify a timeout interval in milliseconds.

Time to Live
Specify a TTL value. TTL (Time To Live) - a technique used in best-effort delivery systems to avoid endlessly looping packets. For example, each IP datagram is assigned an integer time to live when it is created. IP gateways decrement the time to live field when they process a datagram and discard the datagram if the time to live counter reaches zero.

Number of Hops
Specify the maximum number of hops to reach the target. This is a measure of the distance between two points on the Internet. A hop count of n means that n gateways separate the source and destination.

Clean old info at start
If selected, Trace utility will clear the output window before perform new test.

Show Host's Description
If option is enabled, the program will display a description of the host beside host name in the Trace utility. Example:

```
... www.microsoft.com (Microsoft Corporation)
... mainboss.xaxa.BD (Bangladesh)
... www.gazprom.ru (Join-stock company GAZPROM, Moscow, Russia)
```

Stop tracing when a non-responding device is encountered
By default Trace utility stop tracing when some device does not respond. When you disable this option HostMonitor will continue trace until reach destination host.

RCI

RCI is a feature of the monitor that allows you to check and control HostMonitor remotely (using web browser or telnet client). RCI uses TCP/IP protocol and needs just one TCP port. On this page you may setup different parameters of the interface:

Enable Remote Control Interface
HostMonitor will accept remote control requests and commands only when this option is enabled. This is the main "switch" of all remote control functions of HostMonitor.

Listen for incoming connections on port
Here you may specify the TCP port number which HostMonitor will use to listen for incoming requests and commands from Web Service or Telnet Service. Note that both Web Service and Telnet Service should be configured to use the same TCP port number as the HostMonitor itself.

Timeout
This is the maximum amount of user inactivity time which HostMonitor will hold an established connection with the remote user. If the remote user after establishing the connection with HostMonitor does nothing (i.e. does not sends any control commands) HostMonitor will drop this connection after the specified amount of time expires.

Maximum simultaneous connections
This option specifies the maximum number of simultaneous remote connections that HostMonitor may accept from the remote users.
It is important to note here that even just one user that connects to HostMonitor via web browser may generate several simultaneous connections. When an internet browser acquires the document from the internet it may fetch several parts of the document at once to increase performance. Thus "Maximum simultaneous connections" option of the HostMonitor's RCI interface should be set to 4 (minimum) if you plan to use web browser to control HostMonitor (even if just one user at a time will be connected to HostMonitor). Otherwise the web browser may not be able to display a web page with an interface of the HostMonitor correctly.

User profiles button
This button brings up a User Profiles dialog. There you can specify (for each user account separately) a list of authorized IP addresses from which a connection to HostMonitor can be accepted and a list of authorized operations (such as start/stop of monitoring, enable/disable tests, etc) that are allowed for each user. Only "Admin" and users that already have permissions to modify accounts of other users may access the User Profile dialog.

The following group of check boxes specifies the types of events (associated with Remote Control Interface) that HostMonitor will or will not add to system log:
Record info about accepted connections / including WatchDog account
You may enable or disable recording the information about successful connections from the remote users. You may apply this option for all accounts or you may exclude account used for WatchDog application.
Record info about rejected connections / including WatchDog account

Disable or enable recording the information about rejected (by a HostMonitor) connections from the remote users. You may apply this option for all accounts or you may exclude account used for WatchDog application.

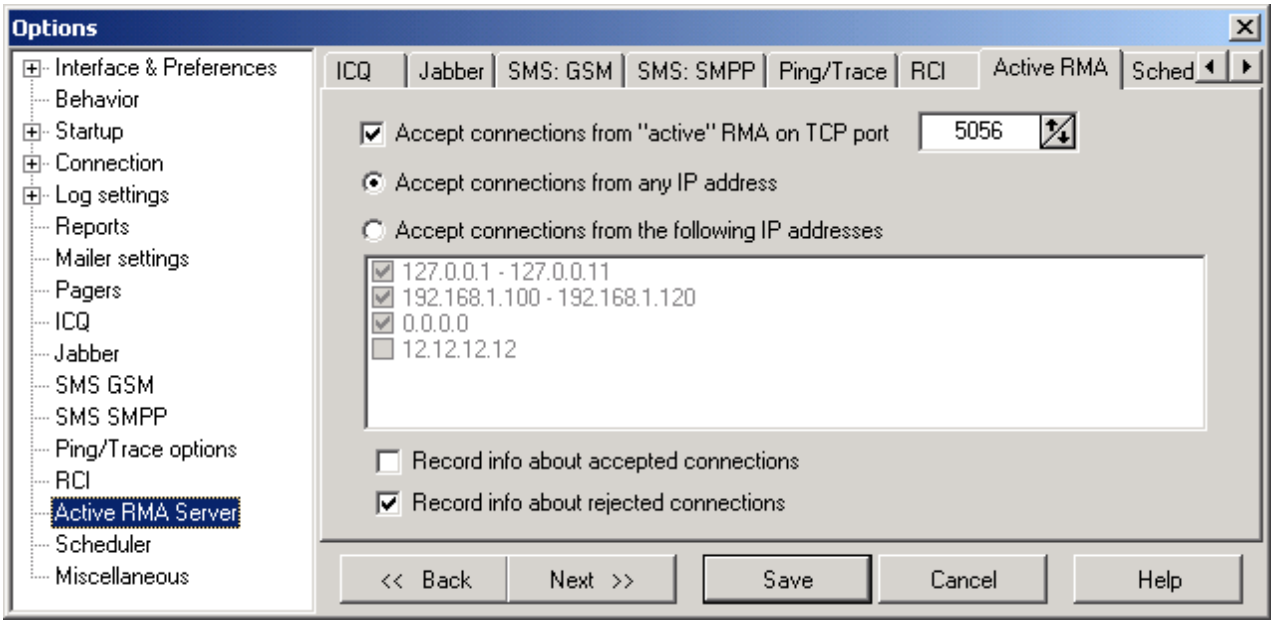
Record info about accepted/executed commands

Disable or enable logging of accepted commands.

Record info about rejected/failed commands

Disable or enable logging of rejected commands.

Active RMA Server



Options located on this page allow you to specify TCP port that will be utilized by HostMonitor to listen for incoming connections from Active RMA agents.

Also it allows you to setup filter for IP addresses

- **Accept connections from any IP address**

Enabling this option will allow HostMonitor to accept connections from any IP address (as long as the incoming RMA request provides correct name and password)

- **Accept connections from the following IP addresses**

This option allows you to specify the list of IP addresses. After enabling this option HostMonitor will accept remote connections only from the addresses within this list (password is required as always).

Please note:

- to insert new address press INSERT button; to remove item press CTRL+DEL; to edit item press Enter or double-click it
- you may specify ranges of IP addresses from which a connection may be accepted. E.g. 192.168.1.1 - 192.168.1.100

The following options specify the types of events that HostMonitor will or will not add to system log:

Record info about accepted connections

You may enable or disable recording the information about successful connections from Active RMA agents.

Record info about rejected connections

Disable or enable recording the information about rejected (by a HostMonitor) connections from the agents.

Scheduler

HostMonitors` built in scheduler. Here you may specify which action profiles HostMonitor will execute on schedule. You have five separate entries in the list. Each of the entries has the following schedule options:

- "**None**" - no action (alert) will be performed.
- "**Regular**" - specify the time interval (e.g. every 60 minutes) to perform action profile.
- "**Daily**" - an action profile will be executed every day at a specified time of the day. Note: the time of the day is specified in 24h format.
- "**Weekly**" - an action profile will be launched once a week on specified day of the week at a specified time of the day (e.g.: weekly, every Tuesday at 22:00).
- "**Monthly**" - once a month, on a specified day of the month, at a specified time of that day (e.g.: every 5-th day of the month at 7:00). Use "Last day" option to start action profile on the last day of the month (you don't have to worry how many days it is in the current month).
- "**Quarterly**" - an action profile is performed once in a quarter on a specified day of the FIRST month of each quarter (1,4,7,10 month) at the specified time. Please note: if you are using "Quarterly" schedule with "Last day" option, action will be performed on the last day of the LAST month of each quarter (3,6,9,12 month).

You may set maximum five schedules of a/m types. In each schedule you may select an action profile that will be executed accordingly. Use the drop down list to select action profiles. By clicking the button next to a drop down list you will access the Action Profiles dialog window where you may add new action profiles and actions or edit the properties of existing actions.
Note: only "scheduled" actions will be executed by Scheduler, i.e. a condition to start action should be set to "on the schedule" (in Action Properties dialog).

Miscellaneous

Use fixed date & time formats
By default HostMonitor gets current Windows regional settings at startup and uses these parameters until you change Windows settings and restart monitor. You can mark this option and define date & time formats. In this case, HostMonitor will use the specified formats, regardless of the system settings.

Reports and Statistics

Reports:

- **Show folder names**
  With this option enabled HostMonitor inserts into reports additional line with the name of folder preceding the list of tests in this folder. Compact HTML and Dashboard reports always display folder name, regardless of this option.
- **Skip empty folders**
  With this option enabled folders that do not contain any tests will not be included into reports. Otherwise report will display single line (row or cell - it depends on report type) with the folder name.

Statistics:

- **Display Alive/Dead ratio of passed/failed tests**
- **Display Alive/Dead ratio of alive/dead time**
  This switch defines how Alive/Dead/Unknown ratio should be calculated: it is either based on quantity of passed/failed probes (HostMonitor version 3 and 4 supported this mode only) or based on alive/dead time (new mode). New mode is useful when you setup HostMonitor to change test intervals for failed tests.
- **Precision: display [N] digit(s) after decimal**
  Sets precision of the Alive%, Dead%, Unknown% fields

RMA / Logging

If backup agent is specified and connection to primary RMA failed

- Set "Unknown" status, log the error, then repeat test using backup agent
- Request backup agent without reporting error

If you setup primary and backup agents, HostMonitor will be able to balance load between agents and use the backup agent when primary one does not respond.
This option defines behaviour of the tests in case primary agent does not respond.

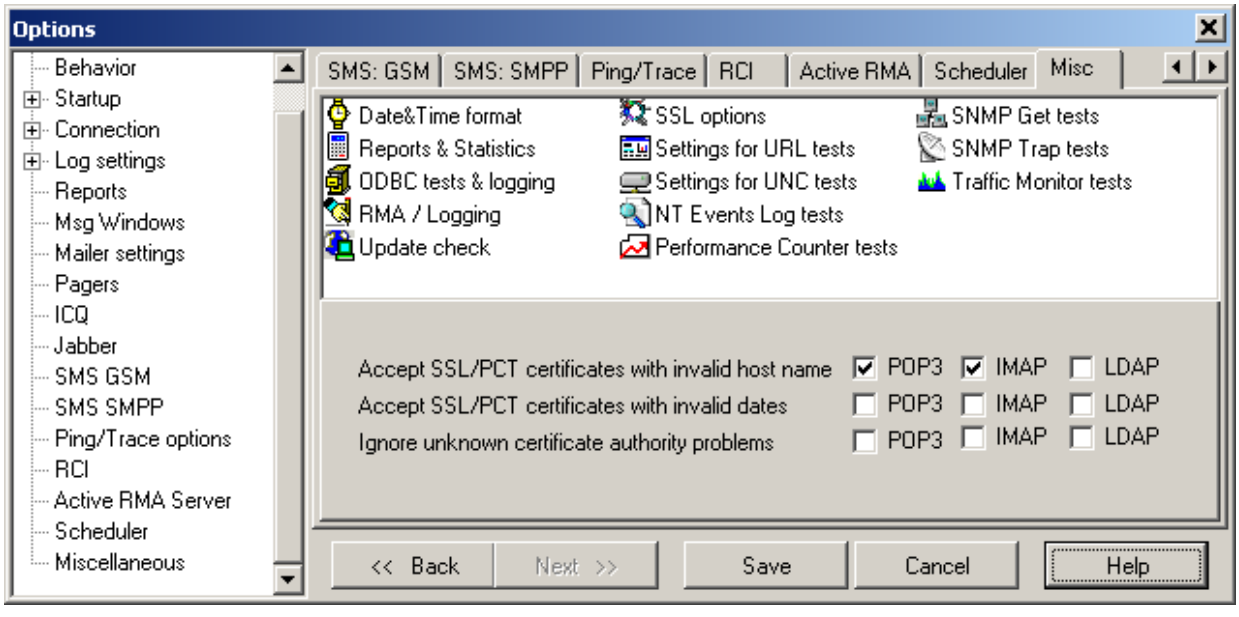
Log: record info about inactive statuses (Disabled, Wait for Master, Paused)
Normally HostMonitor records information about every status change. If you disable this option, HostMonitor will not record information about "inactive" test statuses.

Update check

This option tells HostMonitor to check for software updates at http://www.ks-soft.net/ every 3rd night. If new version detected, HostMonitor will inform logged in operator (next morning). HostMonitor also checks your license and informs operator about validity of the registration code for this new version.

Also you may use menu item "Help" -> "Update check" to check for software updates at any time convenient for you.

SSL options



The following set of options allows you to configure SSL parameters for POP3, IMAP, Mail Relay and LDAP test methods. There are similar set of options for each network protocol: POP3, IMAP and LDAP

Accept SSL/PCT certificates with invalid host name
This option tells HostMonitor to accept SSL certificate when certificate CN does not match target server name.

Accept SSL/PCT certificates with invalid dates
Disables function checking of SSL/PCT-based certificates for proper validity dates. In other words: this option tells HostMonitor to accept expired certificates.

Ignore unknown certificate authority problems
With this option enabled, HostMonitor will accept security certificates issued by any company. When this option disabled, certificate should belongs to trusted company

URL test related options

Do not check Internet connection
Normally HostMonitor checks if computer connected to Internet before "URL request" test (to avoid appearance Dial-Up dialog). With this option enabled HostMonitor will not perform this check.

Agent name
Some server-based scripts can check agent name and returns different information for different HTTP agents (e.g. generate different HTML pages for IE or Netscape). You can change this parameter to get correct results.

Accept SSL/PCT certificates with invalid host name
Disables function checking of SSL/PCT-based certificates that are returned from the server against the host name given in the request.

Accept SSL/PCT certificates with invalid dates
Disables function checking of SSL/PCT-based certificates for proper validity dates. In other words: this option tells HostMonitor to accept expired certificates.

UNC test related options

UNC test mode
This parameter defines behavior of UNC tests. Select 1 of 3 options:

- Normal - HostMonitor can start many tests simultaneously.
- OnePerServer - HostMonitor will start only 1 test per server at one time, but can start several tests for different servers at the same time.
- OneByOne - only 1 attempt at one time (one attempt means - if "UNC test retries" value greater than 1, HostMonitor tries to get information from 1st server; if this try failed, HostMonitor will pause test for this server and will try to check another servers, after 900ms HostMonitor returns to 1st server and performs 2nd attempt).

UNC test retries
Define how many times HostMonitor will try to get information from server (in one test)

Show errors description in "Reply" field when cannot access resource
If you check this option, HostMonitor will put error description in "Reply" field in case "UNC" test cannot access to resource.

NT Event Log test related options

Show events description in "Reply" field for "check NT Event Log" test
HostMonitor can show events description in field "Reply". You can use %Reply% macro in e-mail body, in message for pager, etc. Also this description will appear in reports, log file.

Performance Counter test related options

Test mode
Windows implementation of performance counters has bugs. E.g., Windows 2000 (Professional, Server, and Advanced Server editions) can produce memory leak in PDH.DLL when user (application) querying performance counter that does not exist. This bug fixed in SP2. Also PDH.DLL does not work correctly with multithread applications.
That's why in HostMonitor we have implemented several different methods to work with PDH.DLL:

- MultiThread mode: HostMonitor works almost according to Microsoft documentation with some workaround to avoid most likely problems. HM loads pdh.dll at once and uses it all the time. This method fast because HM can start several tests simultaneously. If everything will work correctly on your system, use this method.
- OneByOne mode: Using this method HM will start Performance Counter tests one by one. This method is slow (when you setup Performance Counter test using Test Properties dialog program even can hung for 1-2 min) but using this method you may avoid problems due to a buggy pdh.dll
- Smart mode: With this method HM will try to detect when pdh.dll has to be reloaded...
- External – HostMonitor uses external (perfobj.exe) utility to perform the tests. This is fast and most reliable method.

PerfObj utility is included into package. Remote Monitoring Agent (RMA) can use this utility as well (utility should be located in the same directory where RMA is installed).
If you want to change test method used by the agent, add line "PerfWorkMode=N" into [Misc] section of the rma.ini file and restart agent. N is a code of the mode:

0 – MultiThread mode,
1 – OneByOne mode,
2 – Smart mode,
3 – External mode

"SNMP Get" test related options

Automatically append the single instance sub-identifier (".0").
Since the "SNMP test" is typically applied to single instance MIB objects that HostMonitor automatically appends the single instance sub-identifier (".0"). Though this has an unfortunate side effect for table instance retrieval, to retrieve correct values for the table instances disable this option.

"SNMP Trap" test related options

Here you may specify general settings of the SNMP Trap test method and provide special processing instructions to warn you about high SNMP traffic from network devices.

Receive traps on UDP port #
This option specifies the UDP port number, which HostMonitor utilizes to listen for incoming messages. Default setting is 162.

v1 / v2c / v3 / Priv
These options allow you to disable certain types of Trap messages: you can disable v1, v2 trap messages, separately disable v3 without encryption and v3 with encryption (Priv option). Similar options can be set for each RMA agent separately.
Please note:
- If Traps v3 with encryption (Priv option) disabled on the RMA side, then only this agent will skip all encrypted messages and will not forward them to HostMonitor;
- If Traps v3 with encryption (Priv) disabled on HostMonitor side, then encrypted messages will not be processed at all
- Other options work independently on HostMonitor/RMA side. You can disable Trap v1 protocol for HostMonitor (v1 trap messages will be rejected when received directly by HostMonitor), but keep v1 enabled on some remote RMA agent, so v1 trap messages will be forwarded from that agent to HostMonitor and processed by the test items.

Unlike other test methods that are performed by specified time interval, SNMP Trap test method reacts on each incoming message from remote network devices. Thus HostMonitor cannot predict how many messages will be received and how often tests/actions will be performed, as a result HostMonitor cannot balance system load.
To prevent overload of the system (which may delay execution of other tests) we have implemented several options:

High traffic alert if more than NN incoming messages per NN sec
This option allows performing special actions when HostMonitor receives more than specified number of messages within specified time. The purpose is to prevent system overload caused by improper configuration of some network device or hacker's attack.
Note: this option has effect to HostMonitor and every Active RMA that is listening for SNMP Trap messages.

Following options define what HostMonitor should do when high traffic is detected:

Suspend receiving messages for NN sec
With this option enabled HostMonitor ignores all incoming SNMP messages for next NN seconds. It reduces system load and allows performing of other (non SNMP Trap) tests.
Note: this option has effect to HostMonitor and every Active RMA that is listening for SNMP Trap messages.

Execute action profile

Here you may select action profile that will be executed when high traffic detected. E.g. it can inform network administrator by e-mail or cell phone.

Note: only "scheduled" actions will be executed, i.e. a condition to start action should be set to "on the schedule" (in Action Properties dialog).

Note: This option affects HostMonitor only. Active RMA that is listening for SNMP Trap messages does not execute specified action profile; instead it sends information about high traffic to HostMonitor. HostMonitor in turn sets unknown status (and shows “RMA: Too many traps received” error in Reply field) to all SNMP Trap test items managed by the agent.

Settings for Traffic Monitor tests

This parameter allows you to specify units that should be used to report amount of network traffic. Choose one of the following options:

- Display traffic using KB / MB units
- Display traffic using Kbit / Mbit units
- Select units considering test settings (threshold value)

ODBC related options

(the following options have effect for ODBC tests, ODBC logging, and "SQL Query" action)

User DSN/System DSN

As you know Windows has system data source names (System DSN) and user data source names (User DSN). System data sources are local to a computer but not user-dedicated; any user with privileges can access a system DSN. User data sources are local to a user and accessible only by the specified user. Using "User DSN/System DSN" option you can choose which data sources list will be used by HostMonitor.

Please note if you start HostMonitor as service, it will not be able to use User DSN. Only System DSN will be used. So, if you are planning to start HostMonitor as service and as regular application, use "System DSN" option. In this case HostMonitor will work equally in both modes.

Do not use SQLFetchAbsolute command

Not every ODBC driver supports SQL_FETCH_ABSOLUTE command. HostMonitor tries to use this command and if driver returns error, HostMonitor use cycle with SQL_FETCH_NEXT command.

It works fine with most ODBC drivers. However ODBC driver which comes with Oracle client v.8 (and may be some other drivers) has bug in error handler. This bug can cause ODBC driver to crash.

That's why this option was implemented. Use it if you experience problem with ODBC driver.

Enable connection pooling

This option enables an ODBC driver to reuse a connection from a pool of connections. Once a connection has been created and placed in the pool, driver can reuse the same connection without performing the complete connection process. This can increase performance of HostMonitor.

PS.: ODBC driver manager controls the number of connections in the pool, HostMonitor cannot change it.

Command line parameters

You can start HostMonitor using command line parameters (these parameters have priority before settings defined in the Options dialog) such as:

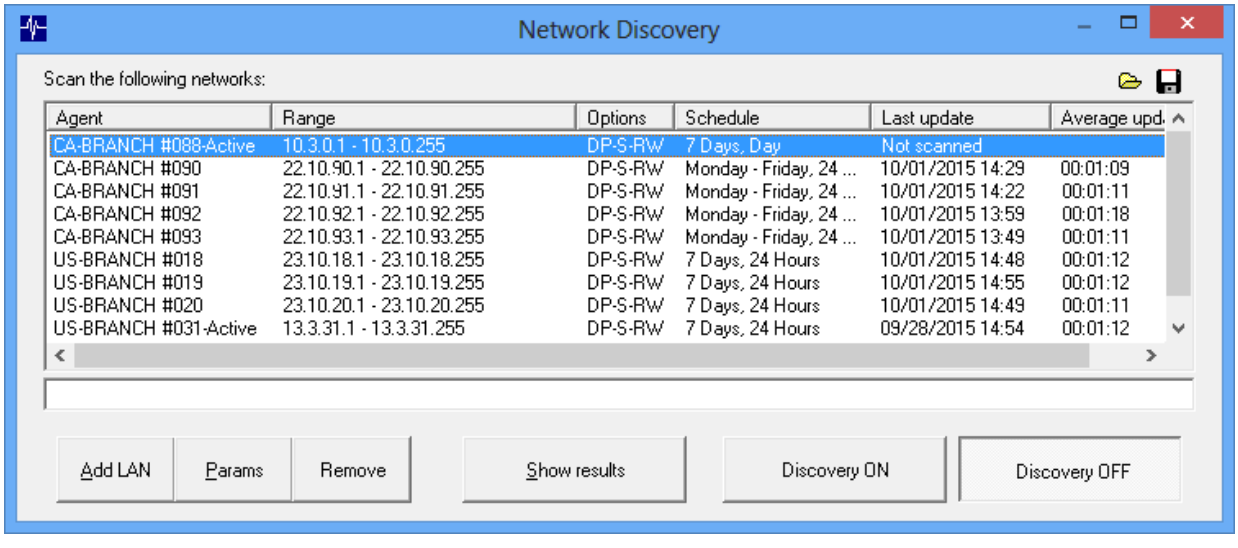
/Ini=*IniFileName*	Read options from specified ini file, by default from "hostmon.ini".
/List=*HostsFileName*	After startup load specified TestList file (HML file with tests).
/ErrorHandler=Default	Normal startup (show error message (if one occurs) and continue).
/ErrorHandler=Ignore	Ignore all errors during startup (do not stop and display message).
/ErrorHandler=Quit	Quit if error (HostMonitor will display the message, wait 20 seconds and quit if operator does not press a key on the keyboard).
/start	Start monitoring after loading.
/stop	Do not start monitoring after loading.
/minimized	Minimize main window after startup.
/maximized	Maximize main window after startup.
/normal	Display window in it normal size after startup.
/InstallService	Install HostMonitor as Win32 interactive service.
/UninstallService	Uninstall service

If you install HostMonitor as a service, the program will be started by the service control manager automatically during system startup. For more information see "How to install HostMonitor as Win32 Interactive service" section.

Network discovery, map and replicator

Network discovery

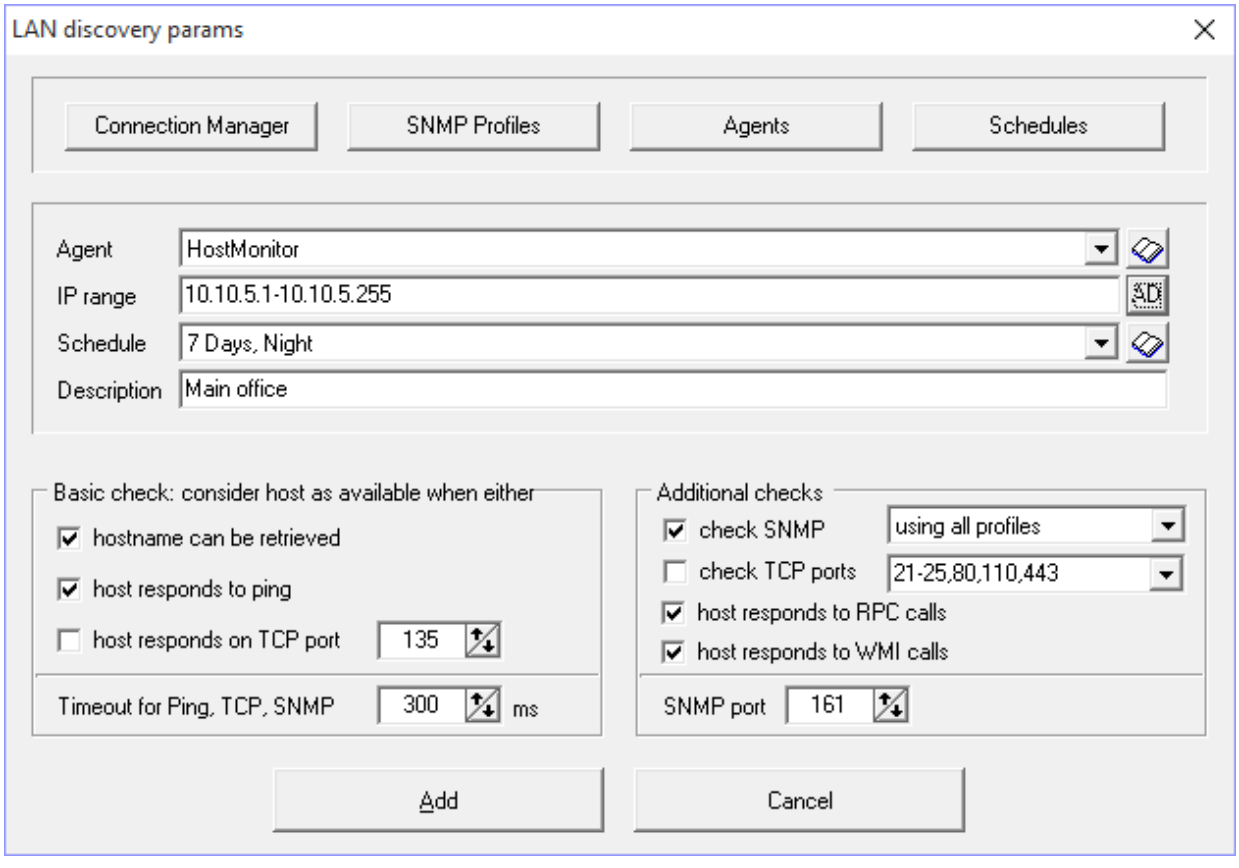
Menu LANs provides access to new function - now you may setup network records for scanning and HostMonitor or RMA will find all systems in the LANs (well, at least systems that can be discovered by ICMP, TCP, SNMP, DNS, MAC requests).



Networks can be scanned by HostMonitor itself, Active RMA or Passive RMA for Windows. You may set agent, IP range, schedule, short description and scanning options:

- consider host as available when either:
  - hostname can be retrieved;
  - host responds to ping;
  - host responds on specific TCP port, e.g.
    - Web servers listen on port 80 and 443
    - Mail servers listen on ports 25, 110, 143, 465, 993, 995
    - WinRM service usually uses port 5985 and/or 5986
- timeout for Ping, TCP connects and SNMP requests
- SNMP port
- check if there is SNMP agent running (using one or list of SNMP credentials)
- check additional TCP ports
- check if host responds to RPC calls
- check if host responds to WMI calls

IP range can be set like 192.168.1.0/24 or 192.168.1.1-192.168.1.255. Also HostMonitor may show LAN information retrieved from domain controller.

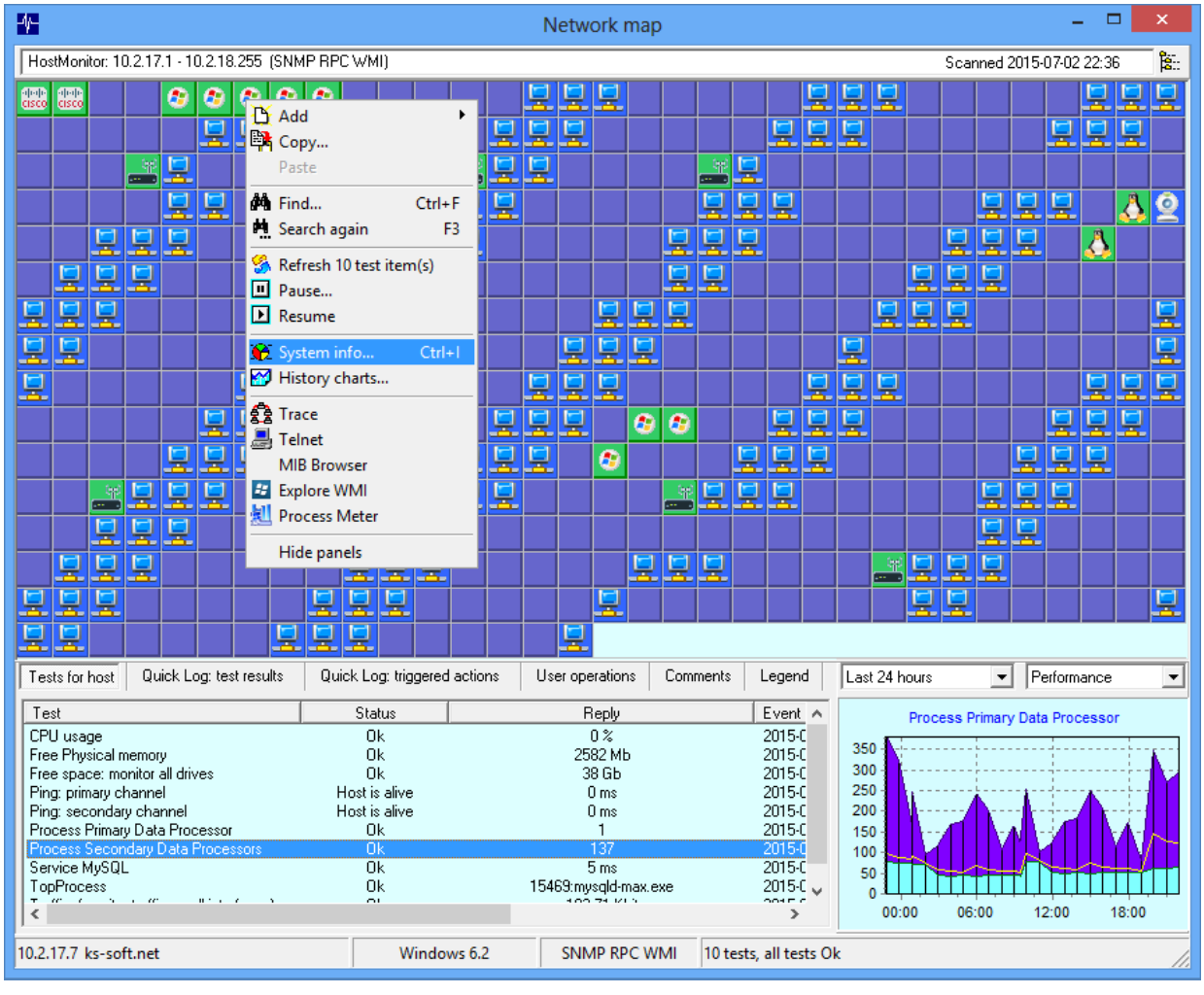


If you decide to use SNMP check (very useful option that allows to detect type of various network devices), please make sure you setup SNMP credentials used in your network (click SNMP Profile button and setup credentials).

If network discovery started, HostMonitor and Remote Monitoring Agents will scan selected networks in background and update database when any changes detected. At any time you may open "Network map" window and see up to date map of your network. Note: HostMonitor and RMA agents do not use a lot of system resources for such scan (even for large networks) so changes in network can be detected with some delay (e.g. new system in network will be detected 5 min after system turned on - exact time depends on number of LANs, number of hosts in the LAN and other parameters).

Network map

Network map window shows all hosts within selected LAN, HostMonitor paints cells in different colors depending on host properties and displays icons when possible (when size of the window is big enough for selected network), so you can easily identify Windows and Unix systems, CISCO routers, Apple devices, Printers, etc.



If there are some test items related to selected host, HostMonitor will group all test items related to this device and display tests in "Tests for host" list. HostMonitor will paint hosts in yellow or red when any test related to the host has "unknown" or "bad" status accordingly.

Lower pane displays consolidated information related to selected host. There are several pages in this pane

- Tests for host - all test items related to the host
- Quick Log: test results - latest test results for all test items related to the host
- Quick Log: actions - latest actions triggered by all test items related to the host
- User operations - list of latest operations such as paused, disabled tests...
- Comments - user comments

- Chart for selected test item

Performance chart shows graph using information about minimum, maximum and average reply values of the test item over selected time interval. Availability chart - shows graph using information about alive/dead/unknown test results ratio over selected time interval
You may choose any of the following time periods to display:
- Today
- Yesterday
- Last 24 hours
- Last 48 hours
- This week
- Last week
- Last 7 days
- Last 14 days
- This month
- Last month
- Last 30 days
- Last 60 days
- This year
- Last year
- Last 12 months
- Last 24 months

Double click on chart opens Test History window

Status bar shows information related to selected host: IP address, hostname, OS version, protocols supported by target host, number of test items related to the host.

There are popup menus in upper and lower panes.

Upper pane menu relates to host and group of tests. E.g. you may add new test item related to the host, refresh or pause all items related to this host, display various information collected from target host. Also you may create your own menu items with associated commands. For more information, refer to Custom menu profiles section of this manual.

Most commands work similar to same commands available in main HostMonitor window however there are some distinctions:

Add test: when you add new test using Network Map window, HostMonitor automatically sets agent and target host fields, SNMP Profile for SNMP related tests, etc. Also HostMonitor highlights menu items if target host supports protocols necessary for such test (e.g. "Add"->"SNMP Get" item will be highlighted when target host supports SNMP protocol). HostMonitor gray out menu items when target host does not support protocols necessary for the test or such test for target host already created (e.g. "Add"->"Service test" item will be displayed in gray color when target host does not support RPC protocol or protocol blocked by firewall); however it does not disable such items so you may create test if you need.

Find operation allows you to find specific host using simple search for IP address or hostname.

Also you may use advanced search with expressions like ("Windows 5" in "%OS%") and ("%WMI %"=="ON")
The following variables can be used for search or clone (copy) operations %hostname% host name

%ip%	IP address of the host (IPv4)
%os%	OS running on target host
%mac_addr%	MAC address (available for systems located within LAN where HostMonitor or RMA installed)
%nc_vendor%	network card vendor
%snmp%	"on" when host responds to SNMP requests (otherwise "off")
%rpc%	"on" when RPC service detected
%wmi%	"on" when host responds to WMI requests
%winrm%	"on" when host supports WinRM requests
%type%	when HostMonitor can detect host type this variable returns one of the following values: router, printer, video, windows, unix, vmware, apple, cisco, juniper, bigip, netscaler, qnap, netapp, synology

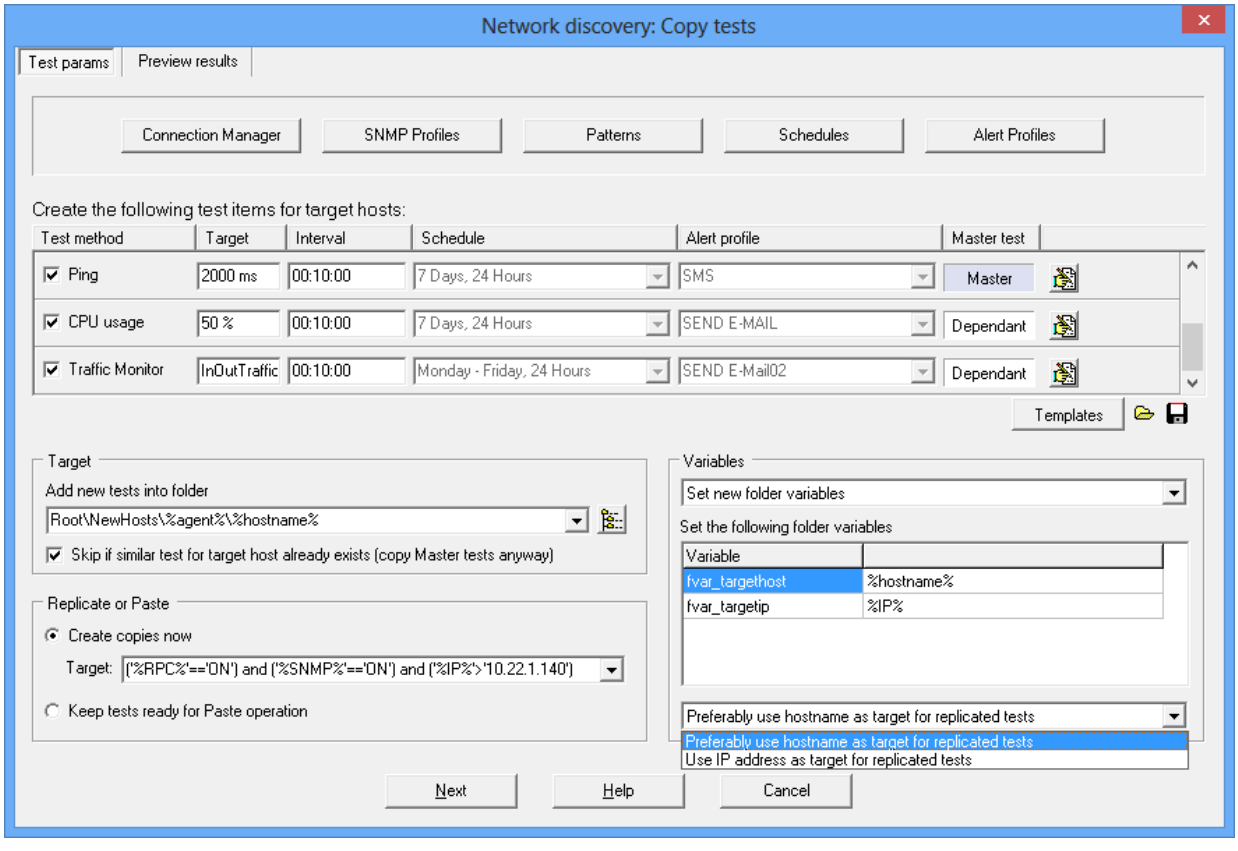
Lower pane menu allows you to operate with specific test items related to the host, e.g. Acknowledge test status, Edit test properties, Enable, Disable, Refresh or Pause test item, etc. Also you may create your own menu items with associated commands. For more information, refer to Custom menu profiles section of this manual.

Note: when you add new test using Network Map window, HostMonitor sets fixed IP address (address of the selected host) to tests that "normally" do not have such property - External test, RAS, Active Script, Shell Script and ODBC test. This allows to link such test to specific host on the map. "Tests for host" pane offers 2 menu items for such tests:

- Set fixed IP
- Clear fixed IP

Replicator

HostMonitor comes with new built-in Replicator. You may select some host using Network map and choose "Copy" item from popup menu. "Copy test" window will show all test items related to selected host



Then you can unmark some items, change test parameters and set options for replication process.

Add new tests into folder
This option tells HostMonitor where new tests should be located. Here you can specify static folder name (e.g. Root\MainOffice\) or you may specify folder using variables like Root\NewTests\ %Agent%\%IP% - in this case HostMonitor will create new folder for each new target host (%IP% variable represents IP address of the host)

Skip if similar test for target host already exists
With this option enabled HostMonitor will check if similar test, related to target host, already exists and will not create another copy. E.g. if there is TCP test that checks port 80 on hostA, HostMonitor will not add another TCP test for this port on hostA but it may add TCP test that checks port 81 (when such test exist in "source" list). Also it will not duplicate tests that check some specific file, ping tests with the same display and packet size options, and so on.
Note: Master tests (test items that have some dependant items) will be copied anyway.

Adjust test settings automatically
This option tells HostMonitor to adjust some settings according to target host OS and detected protocols. E.g. if you copy CPU Usage test from Windows to Linux host, HostMonitor may change OS property from “Windows (RPC)” to “UNIX (SNMP)”; also HostMonitor may change SNMP profile specified for the tests; change OS property for Memory tests; adjust Drive Free Space tests for Windows, UNIX or NetApp devices and so on.

If Master tests not copied, try to find new masters using existing tests as examples
This option can be very useful when you already have set of test items related to target hosts but you want to replicate some new test methods. If you copy just dependent items, this option tells HostMonitor to check test items located in target folder, find tests with similar “master-pattern” and set the same masters for new test items.
Example: if you replicate Memory_A test that depends on 1 external Ping test and 1 internal TCP_A test (TCP_A and Memory_A tests check the same host_A), then HostMonitor will try to find test related to target host_B that depends on 1 external Ping test and 1 internal TCP_B test (related to target host_B). This way new Memory_B test (related to host_B) will depend on Ping and TCP_B masters.
If you replicate set of master and dependent items, then HostMonitor adjusts master-dependent relations regardless of this option.

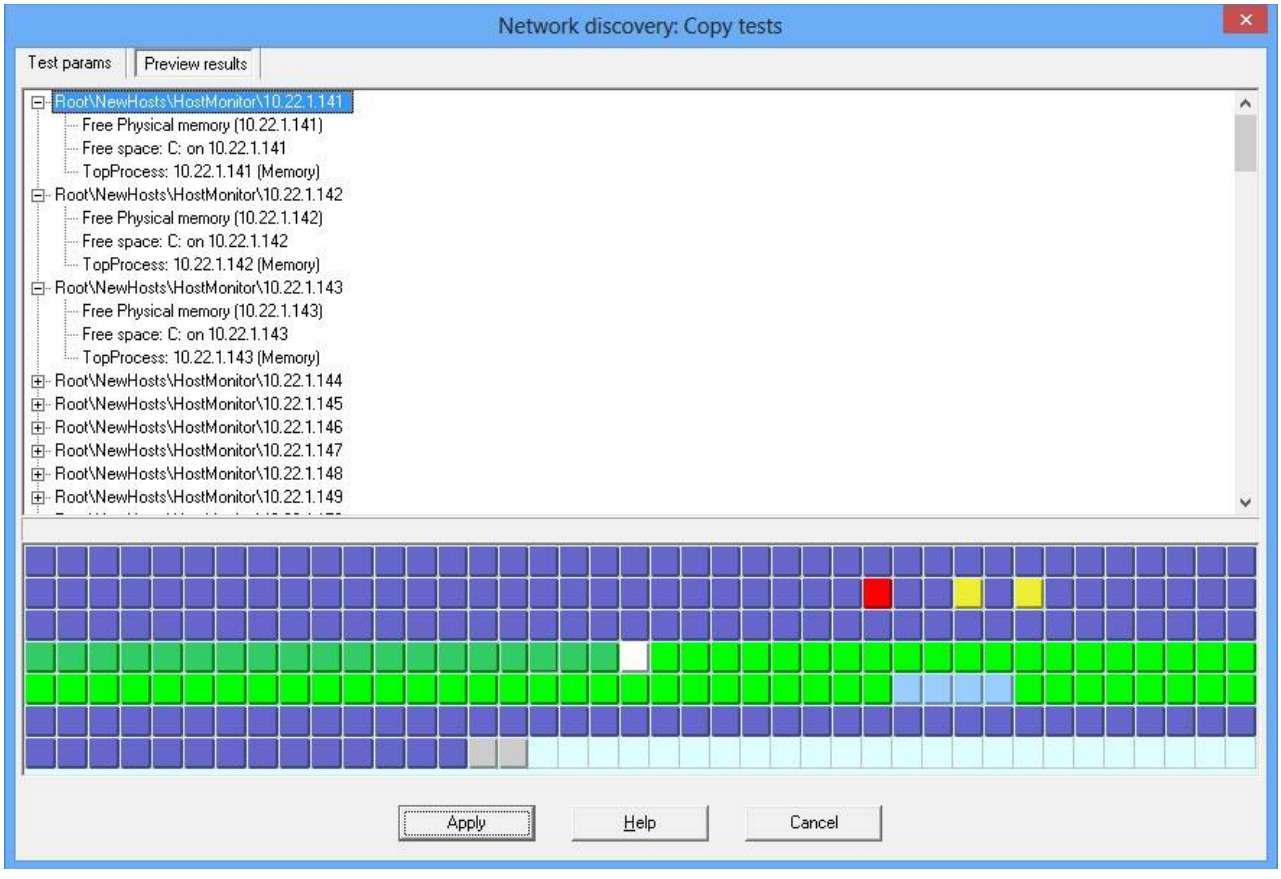
There are 2 modes for replication:
- Create copy now
- Keep tests ready for Paste operations

Create copy now
Using this mode you should specify target hosts before you close "Copy tests" window. You may type target host name or IP address or use complex expressions. For example you may tell HostMonitor to replicate selected tests for Windows systems with enabled WMI service within 10.22.1.50 - 10.22.1.250 IP range using expression like
("%WMI%"=="ON") and ("%IP%">="10.22.1.50") and ("%IP%"<="10.22.1.250")

The following variables can be used in expression

%hostname%	host name
%ip%	IP address of the host (IPv4)
%os%	OS running on target host
%mac_addr%	MAC address (available for systems located within LAN where HostMonitor or RMA installed)
%nc_vendor%	network card vendor
%snmp%	"on" when host responds to SNMP requests (otherwise "off")
%rpc%	"on" when RPC service detected
%wmi%	"on" when host responds to WMI requests
%winrm%	"on" when host supports WinRM requests
%type%	when HostMonitor can detect host type this variable returns one of the following values: router, printer, video, windows, unix, vmware, apple, cisco, juniper, bigip, netscaler, qnap, netapp, synology

Then you may preview results, HostMonitor will show network map with highlighted target hosts. You may switch back to "Test params" page if you want to change something, you may start cloning procedure or you may cancel entire operation.



Keep tests ready for Paste operations

This mode works in different way - when you close "Copy tests" window HostMonitor will keep source tests in internal clipboard. At any time you may select some hosts using Network Map and select Paste item from popup menu. You may select hosts using current LAN or you may switch to another LAN and "paste" the same test items, this allows you to copy tests from one LAN to another (e.g. from LAN monitored by HostMonitor to LAN monitored by Remote Monitoring Agent).

Variables

You may use folder-related variables as parameters of test items (target host, path to the file, etc) and parameters of actions assigned to these test items. For example you may define %fvar_IP% variable and use this variable for various test items - specify %fvar_IP% as target address for Ping and Trace tests, use string like http://%fvar_IP%/database/index.cgi as URL specified for HTTP test, check drive free space using \\%fvar_IP%\driveC path for UNC tests, etc. For details please check Templates section of the manual.

The following options define how Replicator should setup new folders:

- Set new variables

- Inherit all variables from parent folder(s)
- Inherit from parent, new folder variables may override inherited variables

When 1st or 3rd option is selected you may specify folder-level variables. You may use static values and you may use macro variables.
For example: if you set the following settings:
- Add new tests into folder: Root\NewTests\%IP%
- Create copies now, target ('%IP%'>='192.168.1.100') and ('%IP%'<='192.168.1.200')
- Set new variables:
- fvar_targetIP %IP%

then Replicator will create 100 folders:

Folder path	Variables
Root\NewTests\192.168.1.100	fvar_targetIP = 192.168.1.100
Root\NewTests\192.168.1.101	fvar_targetIP = 192.168.1.101
...	...
Root\NewTests\192.168.1.200	fvar_targetIP = 192.168.1.200

Note 1: To add a new variable to the end of the list go to the last existing line and press Down Arrow key. Press INSERT button to insert a new line. Press CTRL+DEL to remove variable. Press F2 to edit variable.
Note 2: if target folders already exist, Replicator will not change folders settings so existing test items will not be affected.

Preferably use hostname as target for replicated tests
This option tells Replicator to use target host name for new tests related to the host. If hostname unknown, IP address will be used
Use IP address as target for replicated tests
With this option selected Replicator will use IP addresses for all new tests created by this copy operation.

Cloning process

What exactly happens when Replicator clones test items? This depends on test methods - there are 5 groups of tests:

RAS, SNMP Trap, ODBC, Active Script tests	HostMonitor does not clone such tests
External test Shell Script	HostMonitor will create copy of the tests for each target host; If there is IP or host name of the source (host) used in command line or used as parameters of shell script, HostMonitor will replace this IP/hostname with target host IP address (or hostname) - patterns not used for target copies
Mail Relay, E-mail, SOAP, OPC, HM Monitor	HostMonitor will create copy of the tests for each target host; set target host IP or host name for each item - patterns not used

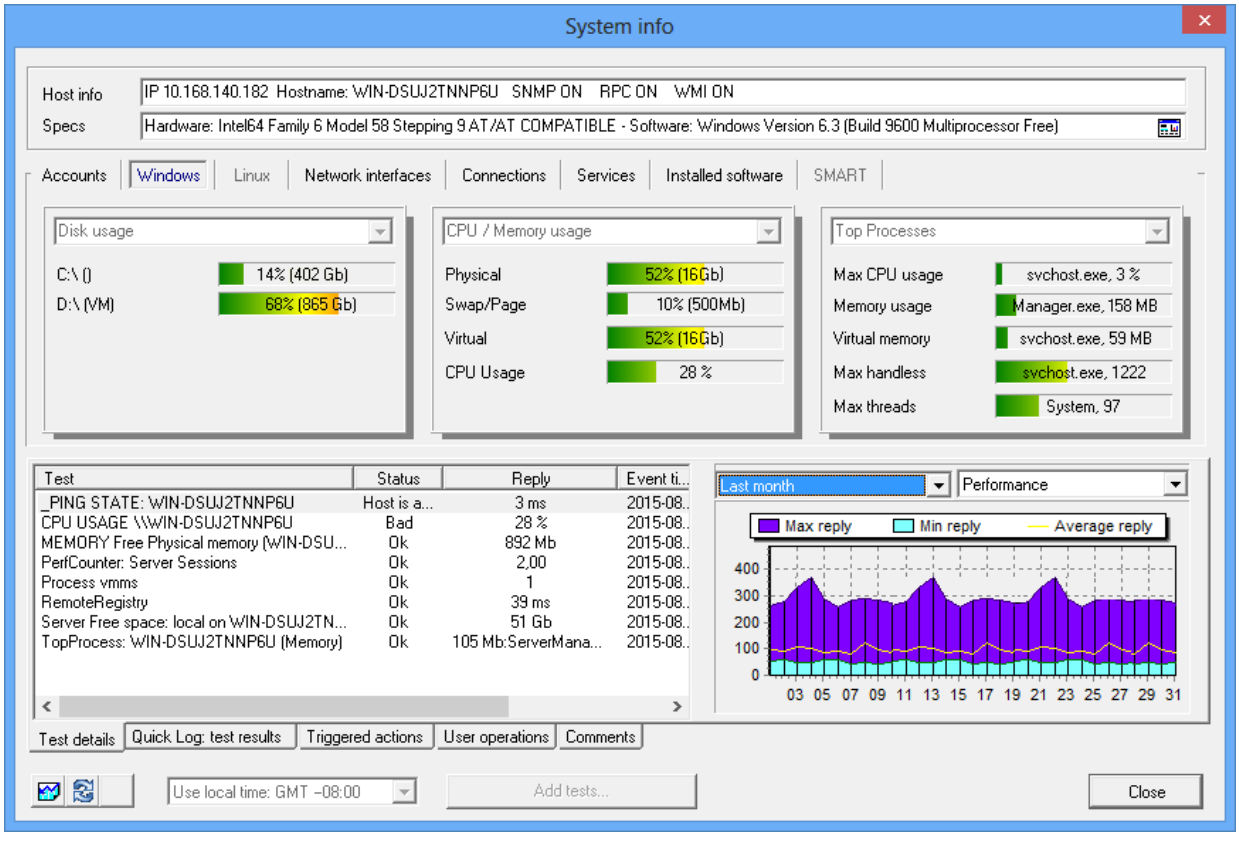
URL, HTTP, File related test methods, Performance Counter, Memory, SNMP Get, VM systems	HostMonitor will create copy of the tests for each target host; set target host IP or host name for each item using patterns when source test uses patterns and destination folder created with correct variables;
5) other test methods	HostMonitor will create copy of the tests for each target host; set target host IP or host name for each item using patterns when destination folder created with correct variables (patterns will be used even if source test did not use patterns)*;

*For example you want to clone "Ping" test with static IP 10.10.1.5 in address field and you are using fvar_IP %IP% variable for target folders. Then HostMonitor will create new folders and new Ping tests using %fvar_IP% string in address field. Unless some folder already exist and such variable does not hold correct IP address (or variable is not specified for this folder) - in such case static IP will be used for new test item.

Network Discovery and Replication great combination - it's pretty easy to create thousand new test items for entire LAN or find couple systems that were not monitored by HostMonitor yet.

System info

System info function uses various protocols to collect data and shows information related to selected host. It can be called from main HostMonitor window or from Network Map window using System Info popup menu item.



System Info window may show

- disk, CPU and memory usage on Windows systems;
- disk, memory usage and system load on Unix systems;
- memory usage and system load on some Cisco routers;
- network interfaces on various network devices (including Windows and Unix systems, routers, etc);
- opened TCP ports and established TCP connections;
- Windows services;
- installed software on Windows and Linux systems;
- hard drive status (SMART data) on Windows systems;
- processes that use most of CPU, memory or handles on Windows system

Data can be collected by HostMonitor, Passive or Active RMA for Windows.

Since version 15.80 System Info tool can retrieve various data using WinRM protocol (in addition to RPC, WMI, SNMP)

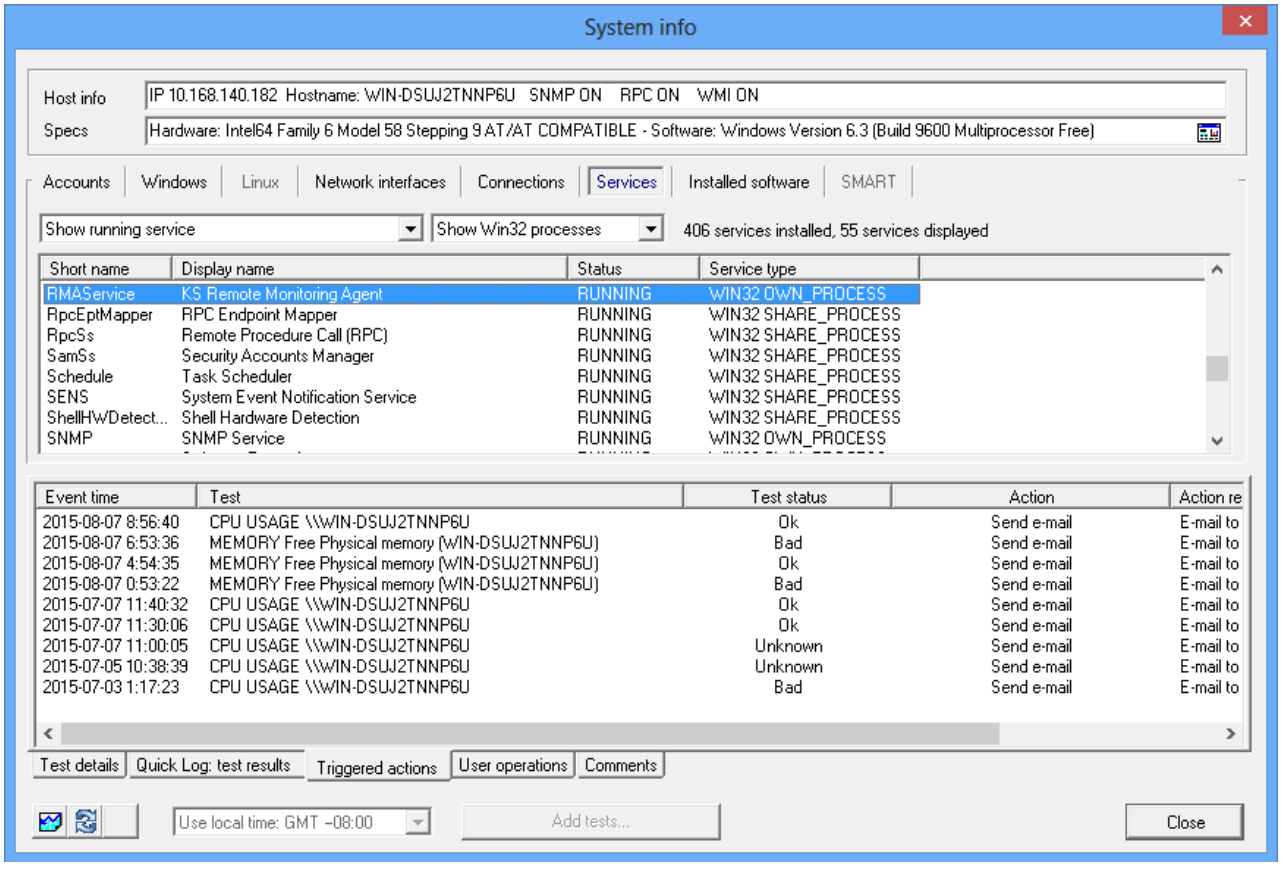
- CPU load, memory usage, disk space usage
- list of Windows services and list of installed software
- hard drive status (SMART data)
- processes that are using the most CPU, memory or handles

Note: WinRM does NOT list 'driver' type of services

Also you may see all test items related to the host regardless where these items located within HostMonitor folders tree. Quick Log pages show test results and actions related to selected host and so on.
Chart shows performance and/or status related history; double click on chart opens Test History window.

You can perform operations with test items without leaving System Info panel:

- Acknowledge status
- Edit
- Refresh (perform test)
- Pause and Resume
- Disable and Enable
- Check historical charts
- Check private logs (for HostMonitor and RCC connected to local HostMonitor)
-



Also you may check target host using built-in and external tools, e.g. start the following utilities:
- Trace
- Telnet
- MIB Browser
- WMI Explorer
- Process Meter

Custom menu items can be added as well.

Accounts

When HostMonitor cannot find account related information (used for connection to target system) you can provide SNMP profile and 2 user accounts manually. When you set new or change user accounts you may store these new accounts using the following options:

Set accounts to network database
HostMonitor stores SNMP profile and user accounts in database managed by Network discovery utility. Existing test items are not affected in any way.

Apply to database and ALL related tests
This option stores user accounts in database managed by Network Discovery as well. Also it changes account for test items related to this host when "Connect as" test property is enabled. Plus this option changes or creates new records for Connection Manager. It may create up to 6 new records (this may happen when you need to use different accounts for WMI and RPC related tests and you are using test items with different format of "target" field - host name, IP address and FQDN) but normally just 1 or 2 records will be modified.

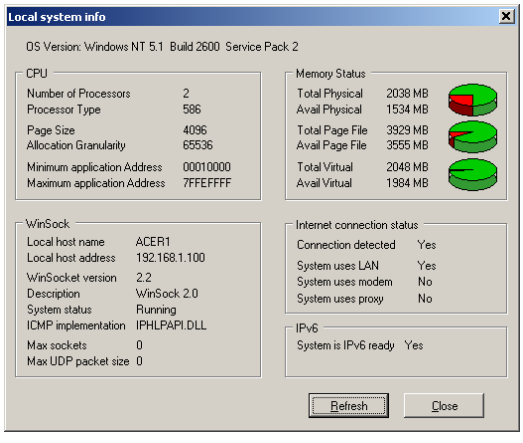
Tools

HostMonitor includes 4 built-in utilities available through the Tools menu:

Local Info

Examines the local host and displays information about the local computer: processor, memory, Winsock data, etc

Some comments regarding counters that show memory status:



Total Physical
The amount of actual physical memory installed on the system.

Avail Physical
The amount of physical memory currently available. This is the amount of physical memory that can be immediately reused without having to write its contents to disk first.

Total Page File
The current size of the committed memory limit. This is physical memory plus the size of the page file, minus a small overhead.

Avail Page File
The maximum amount of memory the HostMonitor can commit.

Total Virtual
The size of the user-mode portion of the virtual address space of the HostMonitor process.

Avail Virtual
The amount of unreserved and uncommitted memory currently in the user-mode portion of the virtual address space of the HostMonitor process.

Trace

Traces the route to a remote host over the network. This utility allows you to see the route all packets take to go from your machine to a specific host on the Internet (Intranel, LAN). It also displays the time each hop (or each machine packets go through) takes to answer. You can specify the parameters to trace (such as the packet size, timeout, packets to send, TTL, and the maximum number of hops) on the Ping/Trace page in the Options dialog.

When you specify trace target you should provide the domain name (e. g. www.yahoo.com) or IP address (e. g. 204.71.200.68) of the host. Also you may provide IPv6 addresses (e.g. fe80::370:ff56:fed5:22) and specify hostname with suffixes ::ipv4 or ::ipv6 (e.g. www.google.com::ipv4 or www.6bone.net::ipv6).
If you specify hostname without any suffix, HostMonitor will try to resolve name into IP address using IPv4 protocol. If name cannot be resolved by IPv4 protocol, HostMonitor will try to use IPv6 protocol. If you specify hostname with ::ipv4 (or ::ipv6) suffix, HostMonitor will use IPv4 (or IPv6) protocol only.
Note: on Windows NT 4.0, Windows 2000 and Windows XP SP1 IPv6 protocol is not supported. You may use menu Tools -> Local Info to check is your system IPv6 ready.

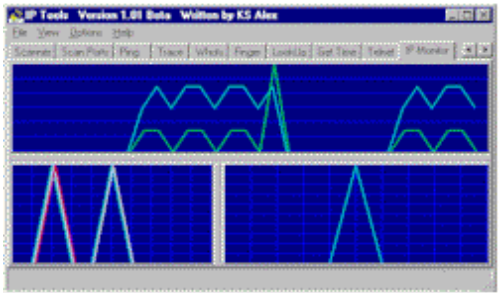
How Trace works?
The program determines the route taken to a destination by sending Internet Control Message Protocol (ICMP) echo packets with varying TTL (Time-To-Live) values to the destination. Each router along the path is required to decrement the TTL on a packet by at least 1 before forwarding it, so the TTL is effectively a hop count. When the TTL on a packet reaches 0, the router is supposed to send back an ICMP Time Exceeded message to the source system. Trace determines the route by sending the first echo packet with a TTL of 1 and incrementing the TTL by 1 on each subsequent transmission until the target responds or the maximum TTL is reached. The route is determined by examining the ICMP Time Exceeded messages sent back by intermediate routers. Notice that some routers silently drop packets with expired time-to-live (TTL) and are invisible to trace.

Telnet

Telnet client is a terminal emulation program for TCP/IP networks such as the Internet, which allows you to logon to the computer from a remote location. You can then enter commands through the Telnet program and the commands will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network.

This utility has two windows. The lower window doesn't translate ESC sequences but stores all received data and works similar to the log file. The upper window uses the telnet client's virtual terminal that translates ESC sequences.

IP Monitor



The IP-Monitor displays, in real time, graphics for counting In, Out and Error packets for TCP, UDP, and ICMP protocols.

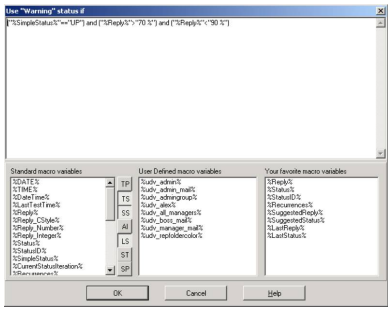
TCP In
The total number of segments received, including those received in error. This count includes segments received on currently established connections.
TCP Out
The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.

UDP In
The total number of UDP datagrams delivered to UDP users.
UDP Out
The total number of UDP datagrams sent from this entity.
UDP Error
The total number of received UDP datagrams for which there was no application at the destination port. + The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.

ICMP In
The total number of ICMP messages which the entity received (this counter includes all those counted by icmpInErrors).
ICMP Out
The total number of ICMP messages which this entity attempted to send (this counter includes all those counted by icmpOutErrors).
ICMP Error
The number of ICMP messages which the entity received but determined as having errors (bad ICMP checksums, bad length, etc.). + The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error, which contribute to this counter's value.

In addition to these built-in uilities, KS-Soft offers IP-Tools, a feature-rich suite integrating 19 helpful TCP/IP utilities. Please check out how IP-Tools can help you in diagnosing network problems on a LAN or WAN, detecting trojan programs on your computer, gathering information from network devices, and a lot more.

Expression editor



Expression editor shows list of standard and user defined macro variables, also it allows each operator to create his own "favorite" list of variables. There are buttons that allow you to filter standard macro variables by category.
Several menu items help to work with variables (popup menu appears when you click right mouse button on macro variable in the list):

- Insert into expression (equivalent to double click on the variable)
- Add variable to favorites (Ctrl+C)

Favorite variables can be moved up (Ctrl+Up) and down (Ctrl+Down) or sorted alphabetically.

Also Expression Editor checks expressions for quotation marks and parenthesis, marks such elements in red when error detected, shows warning label with hint.

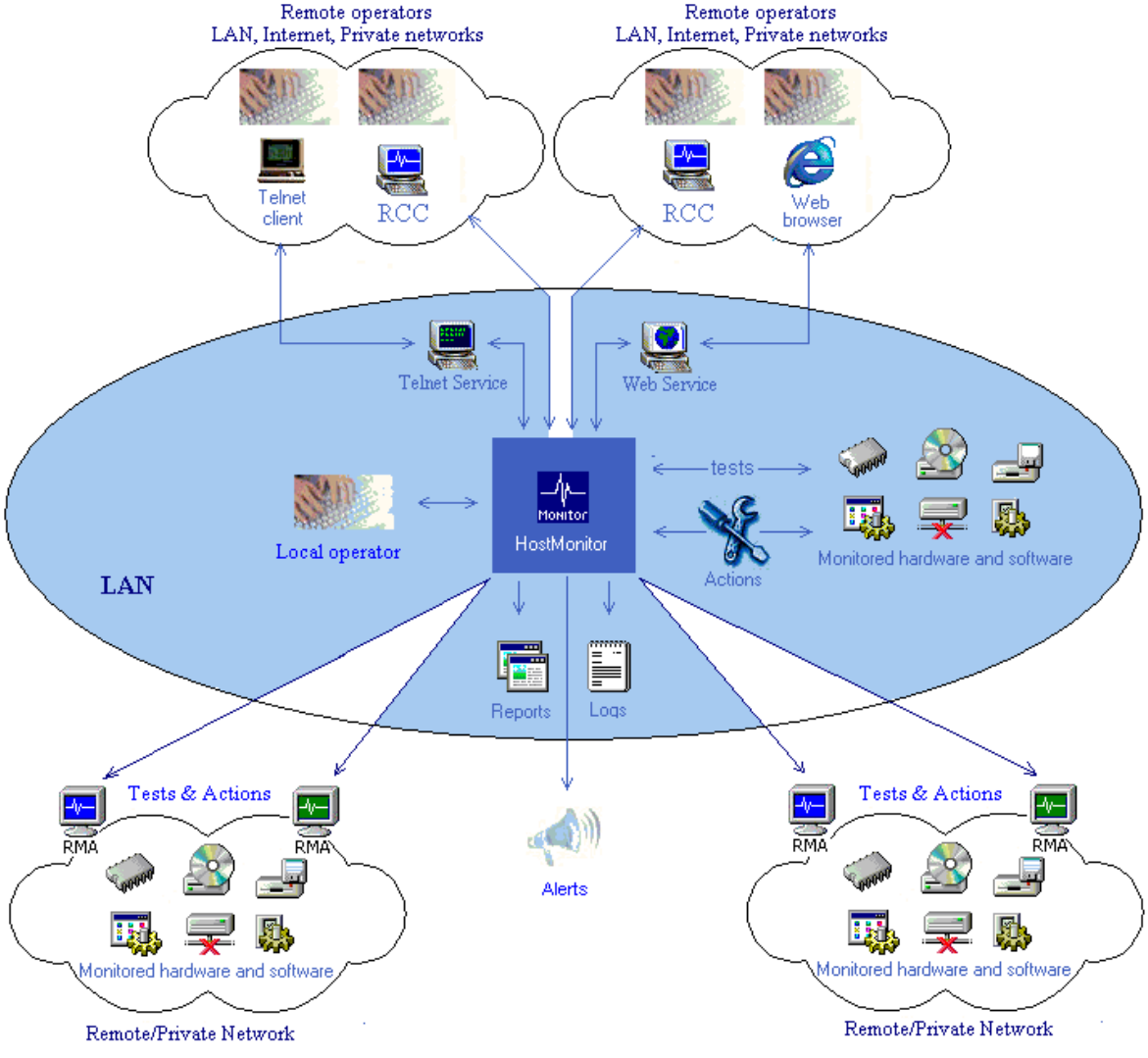
There are special buttons in Test Properties dialog that allow you to bring up “Expression editor” window for “Warning”, “Normal”, “Tune up Reply” and “Master-Dependent” expressions editing.
Also “Expression editor” can be used when you setup expressions for “advanced mode” actions and specific properties for the following actions:

- Send e-mail
- Log Event
- SQL Query
- Send data to TCP/UDP port
- Syslog

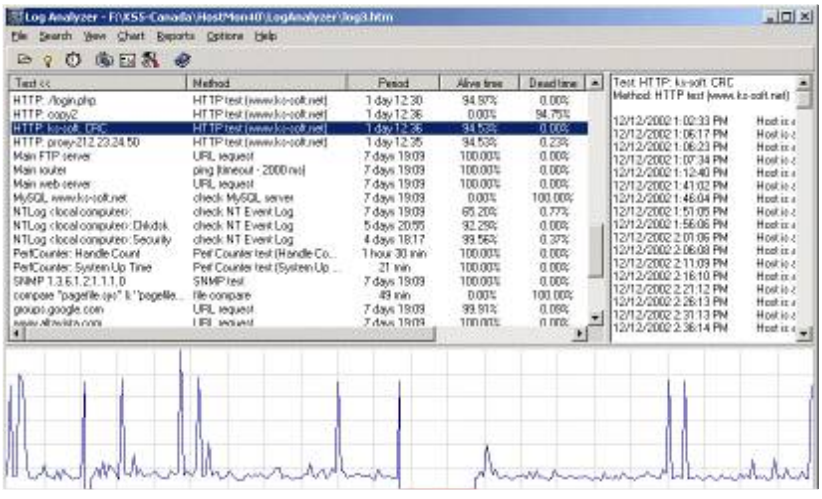
Auxiliary applications

In addition to HostMonitor (the core of a whole package) an Advanced Host Monitor package has the following auxiliary components:

- Log Analyzer
- Log Visualizer
- Disk Meter
- MIB Browser
- WMI Explorer
- Process Meter
- RMA for Windows
- RMA for UNIX
- RMA Manager
- Telnet Service
- Web Service
- RCC, WatchDog



Log Analyzer



As you know HostMonitor is able to log test results into a log file. Log Analyzer is a graphical tool that visualizes the log data. It parses the contents of a log file and presents the data as a variety of charts representing different test statistics. Log Analyzer may analyze all types of log files: HTML, Text, and DBF log files. In a second, administrator can get a snap shot of the host performance over a period of days or even months.
Several examples of the reports:
Example #1
Example #2
Example #3

Features:

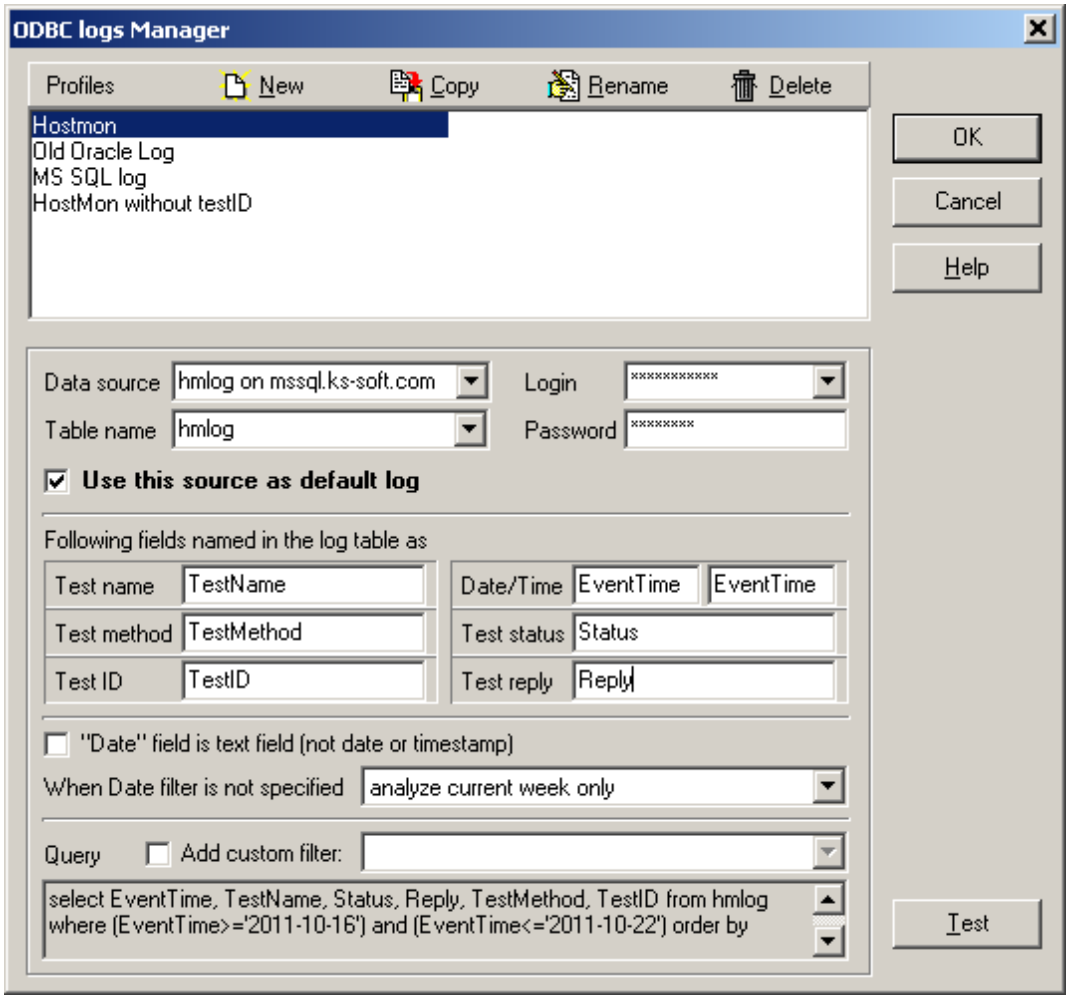
- Log Analyzer allows you to check information individually for each test;
- It allows to analyze several log files at once;
- For each test you can view a graphical chart;
- The highly flexible Report Manager allows you to create and customize reports to your taste in a variety of ways;
- Scripting support allows you to create reports automatically.

See also: Log Visualizer

Main menu is pretty straightforward, it allows you to load one or several log files including text, html, dbf files and load logs from ODBC data source. Search menu allow you to find some specific test item and setup date/time filter (this filter allows you to analyze log file(s) for specified period of time) and so on…
Also, each pane provides popup menu that allows you to open full screen chart, copy image to clipboard or print image on your printer.
“Test log” pane on right side of the window provides “Erase line” and “Erase top value” menu items. "Erase top value" popup menu item allows you to remove (temporarily) log record with top (maximum) reply value for selected test item. This option is useful when you want to remove one or several records with outstanding results from the chart. Log Analyzer does not remove records from the file or database, just skips the record from analyzing process.
Similar “Erase line” popup menu item allows you to remove (skip) specific log record (it removes current line).

Log Analyzer: ODBC logs Manager

Log Analyzer version 5+ may analyze log records which are stored in various databases. Before using such logs you should describe database parameters. “ODBC logs Manager” dialog (that is available thru menu File -> Setup ODBC logs) allows you to create special profiles where each profile describes one log.



For each log you should specify following parameters:

Name
Name of the profile - log will be available for loading under this name. E.g. if you named profile as “HMLog-Oracle”, you will be able to load such log using script command “LoadTable HMLog-Oracle”. You may use any name but it should be unique.

Data source
Select the data source from drop-down list that displays list of all ODBC data sources installed on your system.
*Note: To install or configure Data Source, click Windows **[Start]** button, point to **Settings**, and then click **Control Panel**. Double-click **Administrative Tools**, and then double-click **Data Sources (ODBC).***

Table name
Provide the name of a table that contains log records

Login/Password
Provide login and password (if required) for database access

Use this source as default
This option allows you to use ODBC log for "Statistics" feature (HostMonitor: menu [Test] -> [Show statistics]).

Following fields named in the log table as
This option defines actual fields in the table which contain the information about the test (HostMonitor's ODBC logging could be configured in different ways).

Test name
Specify the name of a field that stores the name of the test.

Test method
Provide the name of a field which stores information about the test method.

TestID
Specify name of a field that stores test ID.
Normally Log Analyzer collects information considering TestID as test property with high priority (test name can be changed by operator while test ID never changes).
In particular this means you will see single item in the report even if you renamed the test item several times. Log Analyzer will show latest used test name but collect test statistics using all recorded names. Also, if you have 2 test items with the same name, Log Analyzer will show 2 items separating statistics using TestID.

Log Analyzer displays warning when you "forget" to specify TestID field however it allows you to save and use such profile. If you setup ODBC log profile without using TestID field, Log Analyzer will process data provided by such log in different way. It will collect statistics using test name and test method. E.g. report will display several items for single TCP test when port specified for the test was changed or test name was changed.

Date / Time
Provide the name of field(s) that stores information about event date and time. If a single field of the table contains information about date and time, type the same name for both options. Type of the field could be Date, DateTime, TimeStamp or it can be a text field (which is not recommended).

Status
Provide the name of a field whith status information. It could be text field that stores status as a text, e.g. "Host is alive", "No answer", etc. Or it can be numeric field, where number represents certain status:

00- Not Tested	05- Checking	11- WaitForMaster
01- Host is Alive	06- Resolving	12- OutOfSchedule
02- No Answer	07- Ok	13- Paused
03- Unknown	08- Bad	14- Warning
04- Unknown host	09- Disabled	15- Normal
	10- Bad Contents	

Reply
Specify the name of a field that stores Reply value of the test. It could be text or numeric field.

Date field is text field
Mark this option if the field which stores date and time of the event is of text type (not datetime or timestamp).

When Date filter is not specified
This option allows you to specify "default" time interval which should be analyzed when Date filter is not specified. You may choose one of three options:

- analyze all data
- analyze current week
- analyze current month

Please note: this option is available when date&time field(s) of the table is of timestamp or datetime type (not text field). If the field is of the text type, then an entire table will be analyzed.

Add custom filter
Here you may provide additional filter that will be used in "where" part of the SQL statement. For example you may use this filter to select information about some specific test item (testname='main router')

Test button executes SQL query and checks the result, showing warning/error messages in case of some problem. This is useful for validation of your settings.

To manipulate with profiles use 4 buttons located on the upper portion of the dialog window:

New	Create new profile
Copy	Copy selected profile. This is useful if you want to make small modifications for the existing log profile
Rename	Change name of the profile
Delete	Remove selected profile

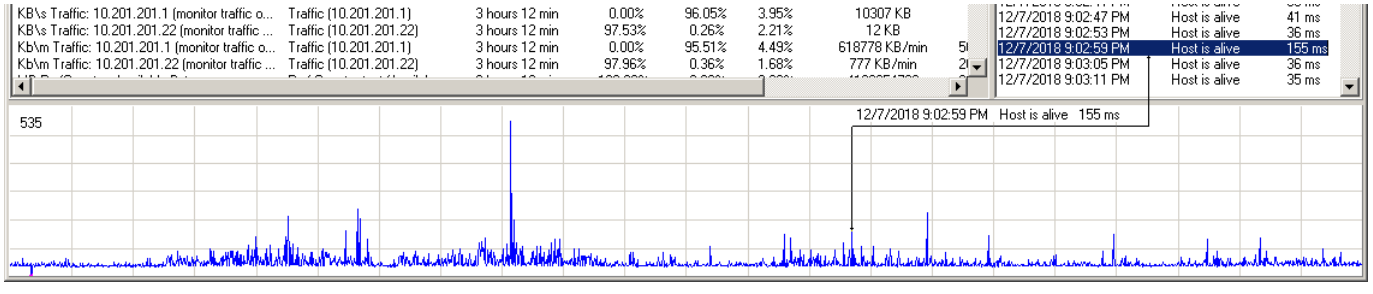
Once log profile is set, you may analyze data using "Load ODBC log" or "Append ODBC log" items of the File menu. Also data could be loaded in automatic mode (for details refer to Script section of this manual)

Log Analyzer: Quick chart

This chart quickly visualizes thousands of log records for selected test item. You may switch on/off several options:

- Logarithmic mode: this mode can be useful when test results are very close in values; or on the contrary, when results cover a large range of values (you may set this mode using popup menu)
- Average mode: if there are thousands of records in the log for the test, then each point on the chart may represent several log records. Average mode tells application to calculate and display average test result for each time interval (point). Otherwise chart will show minimum and maximum value for each time interval. You may set Average chart mode using popup menu

On left mouse click Quick Chart may show log record related to the selected point. If you click on displayed label, Log Analyzer will scroll test related log to this record.



When chart shows thousands of records application helps you to find “points of interest”:

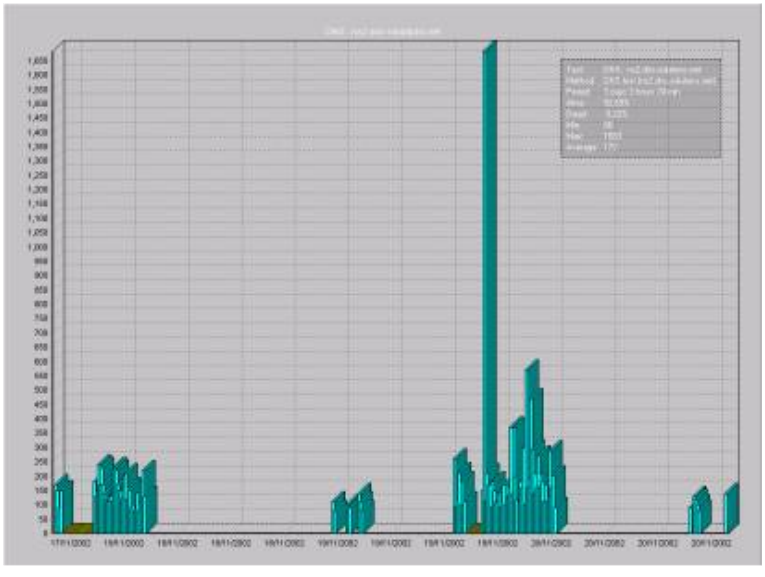
- When you just click left mouse button, Quick Chart will try to find nearest point with minimum or maximum test result. Behavior depends on test method, for example:
  - Memory tests, Drive Free Space, UNC, VM host free space, VM guest free space, VM host memory, VM guest memory, UPS Charged, UPS Time Remaining tests - Quick Chart will look for local minimum;
  - CPU Usage, Temperature tests, Dominant Process, Ping, TCP, URL, HTTP and for many other tests application will look for local maximum;
  - for some tests (like Performance Counter, SNMP Get, SNMP Table) Quick Chart will look for nearest local minimum or local maximum

- When you move mouse with button pressed, Quick Chart will show log record related to new selected point, exact point.
  However if there are thousands of records in the log for the test, then each point on screen may represent several log records (one point on chart represents some time interval). In this case application selects log record with minimum or maximum value (depending on test method) related to the point.
  If you set “Average” chart mode, then you may see difference between logged test result and the chart – chart will show average value for some time interval while text label will show minimum or maximum result for the same time interval

Log Analyzer: Full screen chart

To display a chart in a full screen window, choose the item "Full screen chart" from the popup menu (this menu appears when you right-click in the Log Analyzer window).

Starting from version 3.50 Log Analyzer allows zooming in and out over the selected area of a chart. To zoom in on a chart area, hold the left mouse button and drag mouse down and right. You will see a rectangle around the selected area. Release the left mouse button to zoom in. You may continue zooming again and again.
To restore (undo) the zoom, drag a rectangle in the opposite direction (up and left).



After you right click the chart you may change upper and lower limits of the vertical and horizontal axis using "Set bounds" popup menu item. In the Chart Bounds dialog use an "Interval to display" parameter to set what time period needs to be displayed on the graph (horizontal axis). Use "Bounds to display" parameter to set the limits for "Reply" value mapping onto a graph (vertical axis).

Chart may display graphs in several modes:

• display all data	every test probe will be displayed as separate item
• display average on hourly basis	one bar/point with average reply value will be displayed for each hour when tests were performed
• display average on daily basis	one bar/point with average reply value will be displayed for each day when tests were performed
• display average on weekly basis	one bar/point with average reply value will be displayed for each week when tests were performed
• display average on monthly basis	one bar/point with average reply value will be displayed for each month when tests were performed

You may choose the display mode from popup menu while you work with GUI. This option is also available in each report profile in the Report Manager dialog.
Note: when a lot of records selected for the test (over 7,000) then chart may automatically switch to "Display average on daily basis" or "Display average on hourly basis" mode depending on selected time interval and number of records.
See also: Threshold for charts in average modes option

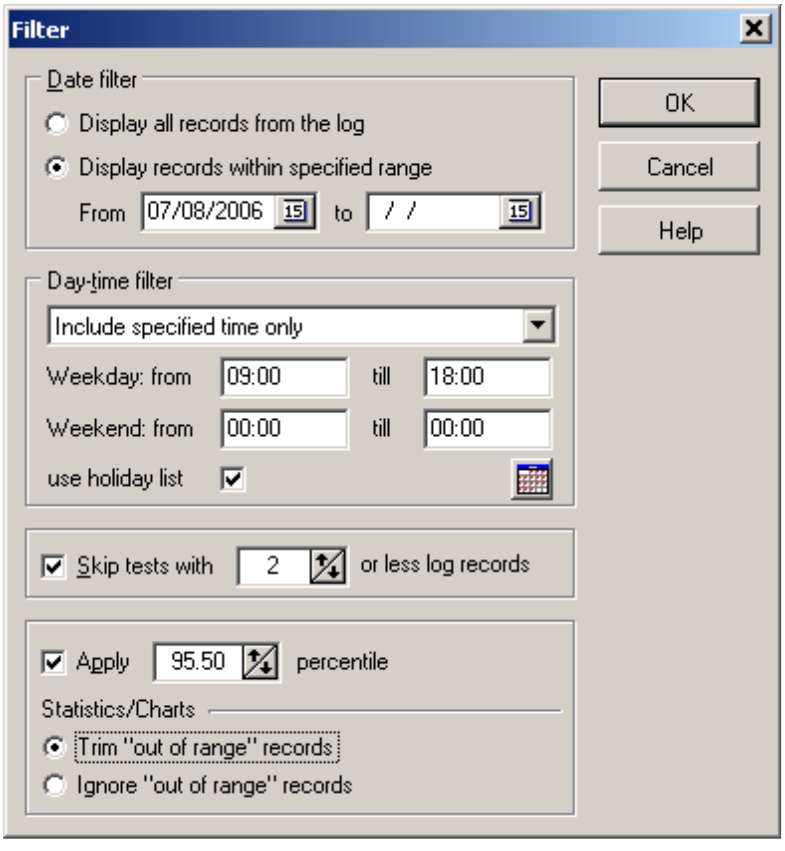
There are following commands available in the chart's popup menu:

Menu item	Description
- Bar	display points (Reply values of the test) as vertical bars
- Line	output all points (Reply values of the test) by drawing a line between them
- Points	displays points (Reply values of the test) as small triangles
- Line & Points	displays points as small triangles and draws a line between them
- 3D	enable/disable 3D effects
- Statistics	show/hide semi-transparent panel with statistical information about test
- Logarithmic mode	this mode can be useful when test results are very close in values; or on the contrary, when results cover a large range of values
- Options	bring up Options dialog
- Set bounds	bring up Chart Bounds dialog (allows you to set bounds for vertical and/or horizontal axis)
- Adjust	sets the lower and upper limit of a vertical axis so that the "Reply" values of the selected time interval are fit on the screen
- Copy image to Clipboard	copy a chart image into the clipboard
- Save to file	save image as bitmap (BMP), Windows Meta File (WMF) or Enhanced Meta File (EMF) file
- Print	bring up Print Preview dialog
- Close	close full screen chart

To close the full screen chart and return to Log Analyzer main window, press [ESC] or [Enter] or select "Close" menu item after the right click on the chart.

Log Analyzer: Filter

The following options allow you to analyze test results for certain time period. E.g. Log Analyzer may calculate statistics (alive/dead ratio, average reply, etc) for 2 months period during business hours.



Date filter
This option allows you to specify the date 'window'. Statistics will be calculated for specified days only.

- **Display all records from the log**
  Date filter is disabled; all records from the log file(s) will be displayed and accounted for in the statistical information
- **Display records within specified range**
  Only log records which fall within specified date range will be displayed and considered for statistics. You may provide start date and/or end date.

Day-time filter
In addition to date filter Log Analyzer provides "Day-time" filter. You may choose one of 3 options:

- **Display all records (24/7)**
  Day-time filter is disabled, all records will be displayed and accounted for in the statistical information
- **Include specified time only**
  Only log records which fall within specified time will be displayed and considered for statistics. You may specify separate time intervals for weekdays and for weekends. If you specify 00:00-23:59 interval, all records will be calculated. If you specify 00:00-00:00 interval, all records for the day will be ignored.
- **Exclude specified time**
  Exclude log records within specified interval - do not display these records and do not include them in statistics. You may specify separate time intervals for weekdays and for weekends. If you specify 00:00-23:59 interval, all records for the day will be ignored. If you specify 00:00-00:00 interval, all records will be calculated.

Use holiday list

This option tells Log Analyzer to process holidays in the same way it processes weekends (including or excluding some time intervals).
Note: Log Analyzer allows you to check list of holidays however Log Analyzer does not allow you to change this list. Use HostMonitor or RCC GUI to modify the list (menu Profiles -> Schedules -> Holidays). If Log Analyzer is installed on different system then you need to copy holidays.lst file from system where HostMonitor is installed.

Skip tests with <N> or less log records
This filter option tells Log Analyzer to exclude from statistics test items with <N> or less records in the log. These skipped test items will not be included into the reports either.

Percentile
"Apply N percentile" option tells application to ignore or trim out-of-range records. When enabled, this option has effect on "quick" and "full screen" charts, statistics and reports. For example, if you set "Apply 90 percentile", Log Analyzer will trim (or skip) 10% of records with highest reply numbers. Application will perform this operation for each test item so highest reply values of "Traffic on hostA" test item will not be mixed with highest reply numbers of "CPU usage on host B" test.
Trim out of range records
Use this option when you want to trim out-of-range values to maximum allowed value. E.g. if test results are 1, 2, **10**, 2, **7**, 2, 5, 3, 1, 3 then Log Anlayzer will calculate 90% percentile using the following numbers: 1, 2, 7, 2, **7,** 2, 2, 5, 3, 1, 3
Ignore out of range records
Use Ignore parameter when you want to skip all out-of-range records. This option may have effect on alive/dead statistic results as well because some records just ignored.
E.g. if test results are 1, 2, **10**, 2, 7, 2, 5, 3, 1, 3 then Log Anlayzer will calculate 90% percentile using the following numbers: 1, 2, 2, 7**,** 2, 2, 5, 3, 1, 3

Log Analyzer: Report Manager

The highly flexible Report Manager allows you to create and customize reports in a variety of ways. Within each profile you may set the following parameters:

Table settings

Display following fields
The listbox on the left in the Report Manager dialog window contains the list of fields that you may include into the report (e. g., test name, test method, average reply, downtime, etc.). Click on the check box next to a field name to mark/unmark the item. Use "Mark all" button to select all available fields, use "Unmark all" button to deselect all items, use "Invert selection" to invert selection for the list.

Include following tests
The list in middle selects the test types to include into the report (e. g., all tests except Ping and CPU Usage tests). Click on the check box next to a field name to mark/unmark the item. Use "Mark all" button to select all available fields or use "Clear all" button to deselect all items. "Invert selection" option is also available.

Skip following tests
Use the listbox on the right to exclude some specific tests from the report.

Chart settings:

Log Analyzer can create chart image for each test that is included in the report. Charts are stored as images in GIF file format.

Choose one of the following options to set chart generating mode:
- Do not create charts
- Create charts, show links in the report
- Create charts, insert images into the report
- Create charts, interactive mode

Display mode
What data should be displayed:

• display all data	every test probe will be displayed as separate item
• display average on hourly basis	one bar/point with average reply value will be displayed for each hour when tests were performed
• display average on daily basis	one bar/point with average reply value will be displayed for each day when tests were performed
• display average on weekly basis	one bar/point with average reply value will be displayed for each week when tests were performed
• display average on monthly	one bar/point with average reply value will be displayed for

basis	each month when tests were performed

See also: Threshold for charts in average modes option

Chart type
Choose type of the chart:

• Bar	display points (Reply values of the test) as vertical bars
• Line	output all points (Reply values of the test) by drawing a line between them
• Points	displays points (Reply values of the test) as small triangles
• Line & Points	displays points as small triangles and draws a line between them

3D
Mark this option if you want to enable 3D effects

Chart width
This parameter specifies width of the chart image (maximum possible width is 6000 pixels).

Chart height
This parameter specifies height of the chart image (maximum possible height is 5000 pixels).

Vertical bounds
The option allows you to specify the lower and upper limits of the vertical axis. You may keep default value (Auto) or set bounds to display the "Reply" values within specified range. For example you may specify range 0-100 for report that shows CPU Usage test methods.

Interactive mode
This mode allows you to create reports like these sample1, sample2
(click on test item to open/close chart)

There are several advantages over "static" reports with charts:
- much smaller report size (3-10 times smaller, depending on data and chart size)
- much faster generation time
- entire report created as single HTML file, its easy to attach report to e-mail (no hundreds JPG files necessary)
- interactivity - you may open and close charts for specific test items at any time

There are some drawbacks as well:
- run-time interactive chart generation is slow, if you want to check charts for many test items, this will take some time (speed depends on your web browser, e.g. Chrome and Opera works pretty well, while Edge and especially IE is much slower)
- in order to work with interactive charts you need access to internet. If your system does not have internet access, you may download the following file https://www.ks-soft.net/download/libs/json/set1.zip, unzip 3 files (**jquery.min.js, raphael.min.js, morris.min.js**) and make them available using your corporate web server; then you need to modify logsman.ini file – add single line like
  ExternalScripts=<script src="http://path_to_the_file_on_your_server/jquery.min.js"></script><script

src="http://path_to_the_file_on_your_server/raphael.min.js"></script><script
src="http://path_to_the_file_on_your_server/morris.min.js"></script>
into [Reports] section and restart Log Analyzer

File / Header / Footer

File
By default Log Analyzer saves all reports into one directory (you can specify that directory in the Options dialog), and uses the name of the profile as a file name (with HTM extension). But you can specify another file name by choosing the "**Put report into particular file**" option and providing a path and name of the file.

Overwrite prompt
With this option enabled Log Analyzer will ask for confirmation if the report file that is going to be created already exists.

Resolve macros
If you enable this option a date macro variables may be specified in the destination file name. Log Analyzer will interpret text between the '**%**' in the file name as a macro variable, where '**DD**' represents the day of the month, '**MM**' - the month, '**YY**' - the year (2 last digits), '**YYYY**' - the year.
This allows creating file names by a template such as one of these:
C:\HostMonitor4\Reports**%DDMMYY%**-rep.htm
C:\HostMonitor4\Reports**%YYYY\DD-MM%**.htm

Templates

Use external header
Use external footer
Using these options you can provide an HTML files that will be used as a header and/or footer for the report. Mark this option only if you want to change the standard header or footer of the report. In HostMonitor's directory "Examples\LAReports\" you can find an example of the header and footer (the files: footer1.htm, header1.htm, header2.htm).
In the header/footer file you can use macro variables to show the current date and time, name of the log file, information about date/time filter, etc. You may select different colors and so on. Below is a list of the macro variables that may be used in an external header/footer:

Variable	Description
%Date%	Current date
%Time%	Current time
%DateTime%	Current date & time
%BGColor%	Background color
%TextColor%	Text color
%LinkColor%	Hypertext link color
%VLinkColor%	Visited link color

%ALinkColor%	Active link color
%LogFilePath%	Full path with name of the log file(s) that is analyzed
%LogFileName%	Name of the log file(s) that is being analyzed
%DateInterval%	Information about date interval that was analyzed. E.g. “01/01/04 – 01/15/04” or “May 2005” (when the date interval covers one full month from the first to last day thereof, the variable will contain only the name of the month and year).
%TimeFilter%	Information about time filter in use. E.g. “Included: Weekday [09:00-18:00]”, “Excluded: Weekend [00:00-23:59]”. When no time filter was applied the value of this variable is “24/7”.

Use template for the table

By using this option you may provide a file with HTML code that will be used to represent each test within the report. Of course each test has unique parameters so you have to use macro variables (which represent different test parameters) in the template. For example: if you want to create the report that will display a table with an average reply value for each test, use simple template with 2 variables:

"<tr><td>**%TestName%**</td><td>**%AverageReply%**</td></tr>" (an HTML code for the header of a table should be contained in the header file). In HostMonitor's directory "Examples\LAReports\" you will find an example of such template (file templ1.htm).

Below is a list of the macro variables that can be used in a template:

Variable	Description
%TestName%	Name of the test
%TestMethod%	Test method
%TestID%	Unique ID of the test
%Period%	Represents the whole time interval of the test log
%AverageReply%	The average value of the results obtained
%MinReply%	The minimum value of the results obtained
%MaxReply%	The maximum value of the results obtained
%AliveRatio%	Percentage of "Good" test results
%DeadRatio%	Percentage of "Bad" test results
%UnknownRatio%	Percentage of "Unknown" test results
%DetailedLogFile%	When this variable occurs in the table template, Log Analyzer creates HTML file that contains all check results for the test. It substitutes this variable with a corresponding file name. So, if you want to provide detailed log file for each test, use HTML code such as <a href="%DetailedLogFile%">
%ImageFile%	When this variable occurs in a template Log Analyzer creates GIF image that represents the test results and inserts the file name of this image file instead of the variable. So, if you want to insert images into the report, use HTML code like <img src="%ImageFile%">

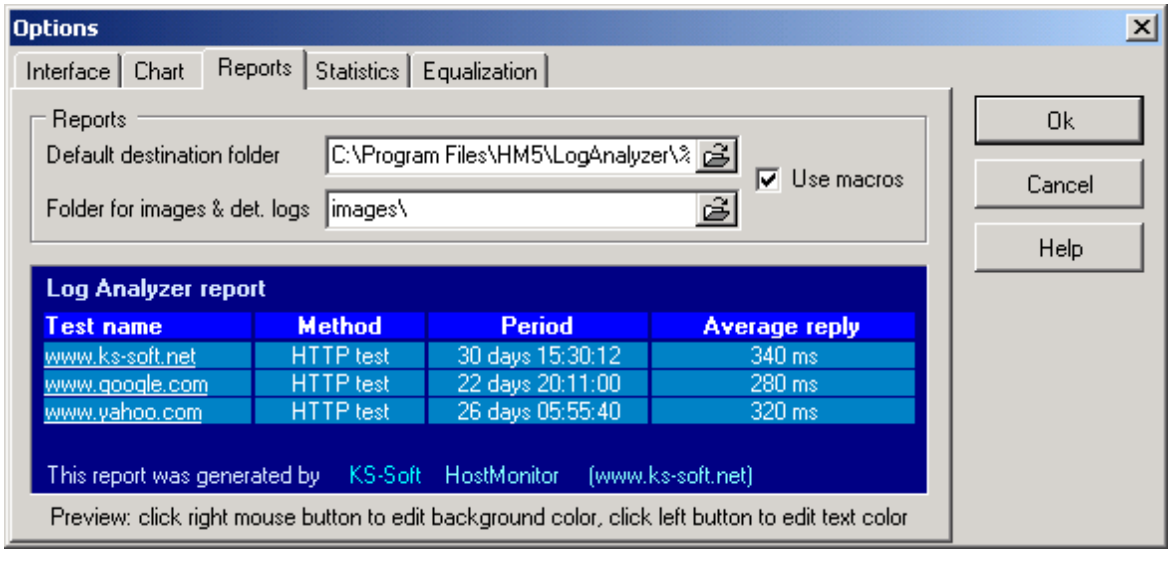
	If you want to insert links to images into the report, use code like <a href="%ImageFile%">

Several examples of the reports:
Example #1
Example #2
Example #3

Create reports
Report Manager dialog contains several buttons that allow you to generate reports right away:

- **Current profile**: creates report using current profile (the one you are currently editing)
- **Selected profiles**: creates reports for marked profiles
- **All profiles**: creates reports for all profiles

Log Analyzer: Options



Interface options

Colors
Offers a choice of colors for the text, background and a chart pane.

Show Toolbar
Shows/hides the toolbar
Show Log pane
Shows/hides the log pane
Show Chart
Shows/hides the chart pane

Grid
By using this option you may specify a number of vertical and horizontal lines of the grid in a chart pane. You may also enable or disable grid in the log pane.

Use fixed date&time format
By default Log Analyzer gets current Windows regional settings at startup and uses these parameters until you change Windows settings and restart application. You may use this option to define the date & time formats (e.g. DD/MM/YYYY h:mm:ss AMPM). In this case, Log Analyzer will use the specified formats overriding the system settings.
BTW: Changing the date format does not affects analyzing of the DBF and HTML log files. Log Analyzer is able to analyze these log files correctly regardless of the date & time settings. However this option can be useful to analyze text log files or html log files that were created by older versions of HostMonitor.

Chart options
You may chose the color scheme for the full screen chart on this page.

Reports page

Default destination folder
Provide a path to the default destination folder for the reports. If this parameter is empty, Log Analyzer will use the directory where it was started from. In Report Manager you may specify different destination directory for some of the reports.

Folder for images & detailed logs
Here you may specify a path to a separate folder where auxiliary images and detailed log files will be stored. If you specify the relative path, Log Analyzer will use "Default destination folder"+"Folder for images" as a destination path. E.g. if you have defined "C:\HostMonitor4\Reports\" as a default folder and "Images\" as folder for images, then images and detailed logs will be stored in "C:\HostMonitor4\Reports\Images\" directory.

Use macros
If you enable this option a date macro variables may be specified in the path. Log Analyzer will interpret the text between the '**%**' of the path string as a macro, where '**DD**' represents the day of the month, '**MM**' - the month, '**YY**' - the year (2 last digits), '**YYYY**' - the year.
For example the use of such a template will create a separate folder every day:
C:\HostMonitor4\Reports**%DD-MM-YY%**\
C:\HostMonitor4\Reports**%YYYY\DD-MM%**\

Color palette
You may customize color scheme for the HTML reports. The following elements have customizable colors (you may change both fore- and background colors):

- underlaying layer;
- table header;
- test items;
- system messages;
- HTML links;
- Visited HTML links;
- Active HTML links;

To change the color of an element, click on an element that you want to change. Use right-click to change its background color, and left-click to change the text color.
The colors of the chart (GIF images) may be changed on Chart page of the Options dialog.

Statistics options

Alive/Dead ratio
This option specifies how “alive time” versus “dead time” percentage should be calculated:

- **100% time = alive + dead + unknown**
  Defines the total monitored time (for each test) as the sum of time intervals when the test had “good”, “bad” or “unknown” status. Time intervals during which the test was disabled or was waiting for master test are ignored. So, “alive” ratio = (alive time) / (alive + dead + unknown time)
- **100% time = alive + dead + unknown + WaitForMaster**

Defines the total monitored time (for each test) as the sum of time intervals when the test had “good”, “bad”, “unknown” or “WaitForMaster” status. Time intervals during which test was disabled are ignored. So “alive” ratio = (alive time) / (alive + dead + unknown + WaitForMaster time)

- **100% time = alive + dead + unknown + disabled**
  Defines the total monitored time (for each test) as the sum of time intervals when the test had “good”, “bad”, “unknown” or “disabled” status. Time intervals during which test was waiting for master test are ignored. So, “alive” ratio = (alive time) / (alive + dead + unknown + disabled time)
- **100% time = alive + dead + unknown + disabled + WaitForMaster**
  Defines the total monitored time (for each test) as the sum of time intervals when test had “good”, “bad”, “unknown”, “disabled” or “WaitForMaster” status. So “alive” ratio = (alive time) / (alive + dead + unknown + disabled + WaitForMaster time)

Threshold for charts in average modes

When “display all data” chart mode is selected, color of each point depends on status of the test at this specific time (e.g. green for passed probes, red for failed).
Behavior of the chart in “average” modes is more complicated – test items may change their status several times during the time interval (day, month…) but the chart displays just the single item. What color should be used for such points? 2 new options (located on Statistics page in the Options dialog) allow you to specify “bad” and “unknown” thresholds for such items:

- **Display "Bad" status when (Bad time)/(Total time) ratio exceeds <N>%**
  specifies threshold for “bad” statuses in % of time interval. If the accrued time during which the test had bad status equals or exceeds specified percentage then the item on the chart will be displayed with “bad” color (red by default). E.g. if you are using “display average on hourly basis” mode and 10% threshold, then if some host did not respond for ping test for 6 or more minutes within an hour, you will see red bar on the chart.
- **Display "Unknown" status when Unknown/Total time ratio exceeds <N>%**
  specifies threshold for “unknown” statuses in % of time interval. If the accrued time during which the test had unknown status equals or exceeds specified percentage then the item on the chart will be displayed with “unknown” color (yellow by default). E.g. if you are using “display average on daily basis” mode and 25% threshould, then if some test had “unknown” status for 6 or more hours within a day, you will see yellow bar on the chart.

Please note: “bad” status has higher priority than “unknown” status. It means if “bad” time reached specified threshold, the point will be displayed in red color regardless of how long this test had “unknown” or “good” status.

Equalization

This parameter allows you to equalize Traffic Monitor test results to the same units. Choose one of the following options:

- Reduction: use Kbit units for all tests
- Reduction: use KB units for all tests
- Reduction: use Mbit units for all tests
- Reduction: use MB units for all tests
- Display values as is

Log Analyzer: Scripts

Log Analyzer 4.0+ supports scripts. Scripts allow you to generate reports automatically by schedule (e.g. using standard NT scheduler). Log Analyzer Script file (default extension .LAS) is a simple text file that contains commands for the application. You can create and edit script file using any text editor (e.g. notepad).

Some common rules:

- You can put only one command in each line
- Comments: The program ignores all strings with a semicolon (;) as the 1st character
- Commands: commands are case insensitive (e.g. "Load" and "LOAD" means the same)
- When you provide a log file name or a date filter you can use date macro variables. Log Analyzer will interpret the text between '**%**' in the parameter as a date macro variable, where '**DD**' represents the day of the month, '**MM**' - the month, '**YY**' - the year (2 last digits), '**YYYY**' - the year. Also you may use special date expressions.

List of the commands:

Command	**Parameter(s)**	**Description**
LoadFile	<log file name>	Loads and analyzes specified log file
AppendFile	<log file name>	Appends information from specified log file into current data set
LoadTable	<ODBC log source name>	Loads and analyzes log records from database (see ODBC logs Manager dialog for details)
AppendTable	<ODBC log source name>	Appends information from specified database (see ODBC logs Manager dialog for details)
DateFilter	<start date> <end date>	Applies filter that determines what time period Log Analyzer should include into the reports. Format of the <start date> & <end date> is: DDMMYYYY
TimeFilter Include	<time interval (weekdays)> <time interval (weekends)> [UseHolidayList]	Only log records within specified time will be considered for statistics. You should specify separate time intervals for weekdays and for weekends. If you specify 00:00 23:59 interval, all records will be accounted. If you specify 00:00 00:00 interval, all records for the day will be ignored. Format of each time interval is HH:MM hh:mm, where HH:MM – hour and min of the beginning of the inteval, hh:mm – hour and min of the end of the interval. E.g. TimeFilter Include 09:00 18:00 00:00 00:00 Please note: the most resent TimeFilter

		command overrides any and all previous TimeFilter commands.
TimeFilter Exclude	<time interval (weekdays)> <time interval (weekends)> [UseHolidayList]	Exclude log records within specified interval – Log Analyzer will not display these records; will not include them into statistics for specified time. You should specify separate time intervals for weekdays and for weekends. If you specify 00:00-23:59 interval, all records for the day will be ignored. If you specify 00:00-00:00 interval, all records will be calculated. Format of each time interval is HH:MM hh:mm, where HH:MM – hour and min of the beginning of the inteval, hh:mm – hour and min of the end of the interval. E.g. TimeFilter Exclude 09:00 18:00 00:00 23:59 Please note: the most resent TimeFilter Exclude command overrides any and all previous TimeFilter Exclude commands.
TimeFilter 24/7		Disables "Day-time" filter. All log records will be displayed and calculated for statistical information
SkipMode On		Tells Log Analyzer not to display test items with <N> or less records in the log. By default <N> is set to 0, unless you specify different number using SkipLevel command.
SkipMode Off		Display all test items. Even for tests that after "day-time" filtering have less records then is specified by SkipLevel command.
SkipLevel	<min number of records>	Do not display statistics for test items with <N> or less records in the log.
Percentile	Trim|Ignore <percentile_number>	Sets percentile options and value. Use Trim parameter when you want to trim out-of-range values to maximum allowed value. Use Ignore parameter when you want to skip all out-of-range records (this option may have effect on alive/dead statistic results as well). Set percentile to 100 when you want to calculate test results as is, without "percentile" processing (this is default mode for Log Analyzer) Examples:

		Percentile Trim 90 Percentile Ignore 89.9 Percentile Trim 100
CreateReport	"<report profile name>"	Creates report using specified report profile
CreateSelectedReports		Creates reports for marked profiles (those that are marked in the Report Manager dialog)
CreateAllReports		Creates reports for all profiles

Date expressions:
What if you need to use yesterday's date? Or date that specifies last month? In this case you may use expressions.
For example if you need to create report for a week, use command "DateFilter %ddmmyyyy[-7d]% %ddmmyyyy[-1d]%"

Rules	Examples
1. to subtract a number of days from current date, use expression like [-NNd]	%dd[-1d]%
2. to add a number of days to current date, use expression like [+NNd]	%ddd[+22d]%
3. to subtract a number of months from current date, use expression like [-NNm]	%dm[-24m]%
4. to add a number of month to current date, use expression like [+NNm]	%ddmm[+1m]%
5. to subtract a number of years from current date, use expression like [-NNy]	%dmyy[-2y]%
6. to add a number of years to current date, use expression like [+NNy]	%ddmmyyyy[+10y]%
7. expression must be concluded in the same percent signs (%) that concludes date variables	%ddmm[-1d]% - correct expression %ddmm%[-1d] - invalid expression
8. expression must be specified after regular date variables	%dd[-1d]% - correct expression %[-1d]dd% - invalid expression
9. you may use only one expression in each macro variable.	%ddmm[-1m]% - correct expression (one variable and one expression) %dd[-1d]%%mm[-1m]% - correct expression (2 variables, 1 expression in each variable) %ddmm[-1d][-1m]% - incorrect expression (2 expressions in one variable)

Example of the script:

```
;load log files, set date filter
LoadFile    C:\HostMonitor4\logs\%YYYY%\log.htm
AppendFile C:\HostMonitor4\logs\privatelog1.htm
AppendFile C:\HostMonitor4\logs\privatelog2.htm
DateFilter %01MMYYYY% %30MMYYYY%
;only log records that were created between 9am and 6pm
```

```
;on weekday will be used for the report
TimeFilter Include 09:00 18:00 00:00 00:00  UseHolidayList
SkipMode On
SkipLevel 2
CreateReport "HTTP tests (no charts)"
;now skip log records that were created between 6pm and 9pm on weekday
;and skip records that were added at any time on weekend.
;change skiplevel and generate another report
DateFilter %DDMMYYYY[-7d]% %DDMMYYYY[-1d]%
TimeFilter Exclude 18:00 21:00 00:00 23:59
SkipLevel 4
CreateReport "HTTP tests (charts)"
;disable "day-time" filter
TimeFilter 24/7
SkipMode Off
Percentile Trim 95.5
Createreport "Template1"
```

To execute a script, you should start Log Analyzer with the following command line parameter "**-script:<name of script file>**". There is also an optional parameter "**-log:<name of the log file>**". With this optional parameter Log Analyzer will record information about script execution and about errors in the script (if any) into the specified file.
Example: LogsMan.exe -script**:**reports.las -log**:**scriptlog.txt

Log Analyzer: optional command line parameters

2GB file analyzing can take several minutes (time depends on file format, number of test items, system performance, etc). There are some options that may save your time:

- onetest command line parameter tells Log Analyzer to find and analyze one or several tests and ignore other test items. You may specify test ID, list of test IDs, full name of the test or text with wildcard (wildcard should be located at the beginning or at the end). Examples

Logsman -logfile:log.txt -onetest:105	Analyze records related to test with ID 105
Logsman -logfile:log.txt -onetest:105,106,107	Analyze tests with ID 105, 106 and 107
Logsman -logfile:log.txt '-onetest:ping10.10.1.5'	Analyze test named ping10.10.1.5
Logsman -logfile:log.txt "-onetest:Cisco*"	Analyze test items with "Cisco" string in test name or test method
Logsman -logfile:log.txt "-onetest:*temperature"	Analyze test items with "temperature" string in test name or test method

  When you are using HostMonitor or RCC GUI to analyze log file for specific test, HostMonitor (RCC) checks log file size and applies "onetest" switch for large files, this way Log Analyzer will load log file much faster.
  You may adjust limit for such "large" files using MinLogSizeForSingleTest parameter in [Misc] section of hostmon.ini (or rcc.ini) file. For example
  [Misc]
  MinLogSizeForSingleTest=100
  sets 100 MB limit. If you set 0, then "onetest" switch will not be used.

- When Log Analyzer started without "onetest" switch and its not started in scripting mode then application checks number of records in the file. If there are over 2,000,000 records, it asks "would you like to load last 500,000 records?" so you may choose: load and analyze recent log records or read entire log file. You may adjust these limits using logsman.ini file. For example
  [LogAnalizer]
  MaxRecordsWarn=8880000
  LastRecordsCnt=444000

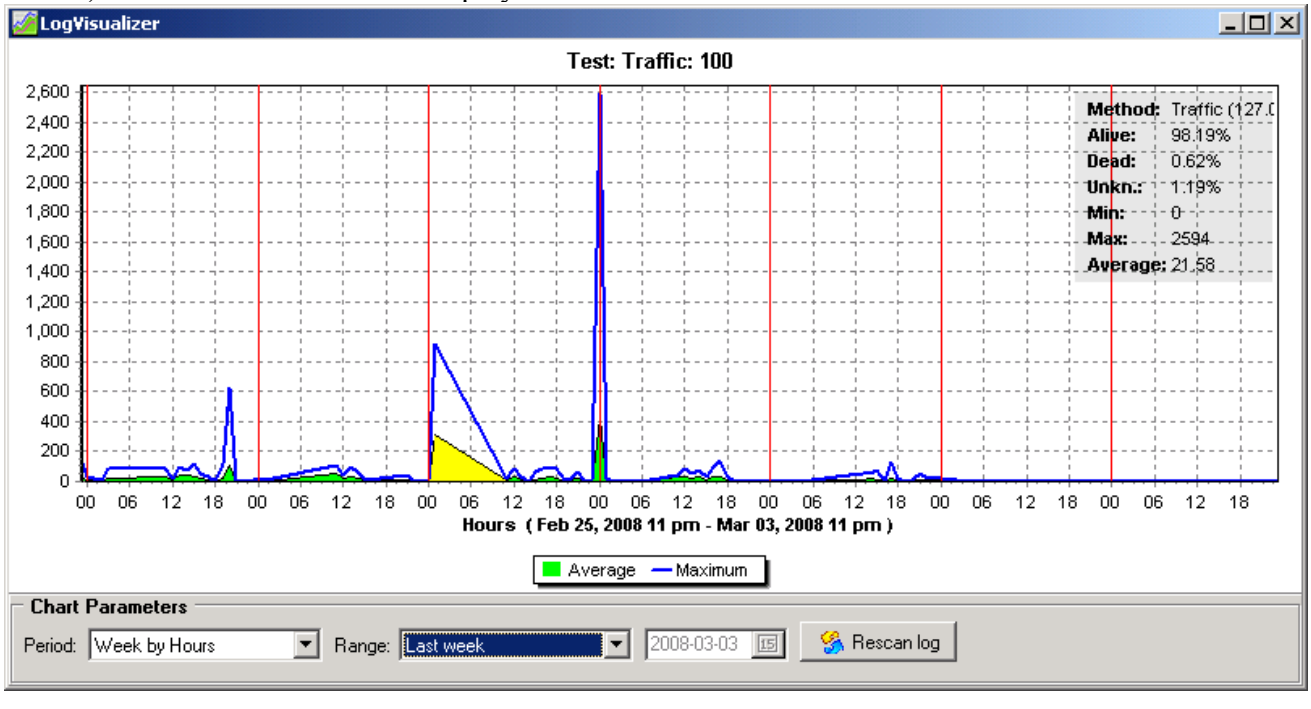
Log Visualizer

Log Visualizer is a command line utility that is designed as auxiliary application for HostMonitor. HostMonitor may store tests results in log files (DBF, HTML, Text), also it may use user-specified database to keep history of test results. The purpose of Log Visualizer is to visualize test results for certain test item on demand. The application parses content of a log file and presents test results over period of time as a variety of charts.

What is the difference between Log Visualizer and Log Analyzer?

1. Log Analyzer provides information about all test items that are listed in the log; it creates reports for set of tests. Log Visualizer creates chart for specific test item.
2. Log Analyzer can be used as GUI application and as command line utility while Log Visualizer is command line utility; it is designed to be started by HostMonitor or your own homemade script (nevertheless it provides some simple GUI as well).
3. When you need a chart for single test, it's much better to use Log Visualizer because it is optimized for such tasks. Log Visualizer uses specially formatted files (repository) to store intermediate data grouped by test items on hourly, daily, weekly and monthly basis. That trick helps application to increase productivity and execution speed significantly. When you need report with charts for a large amount of test items, Log Analyzer might be preferable.

Log Visualizer creates chart that shows test results over specified period of time (day, week, month, etc). Depending on command line parameters chart can be stored in specified file (GIF format) or the same chart can be displayed on screen.



Using Log Visualizer you may:

- compose your own documents with the charts created by Log Visualizer on regular basis; e.g. you may create HTML template with links to images and use scheduler to launch Log Visualizer to update the images on regular basis (e.g. every midnight)
- create shortcuts on your desktop for specific test items; then you may bring up chart for the test with easy point-and-click operation;
- also, if you have Log Visualizer installed, HostMonitor will provide additional option thru Test Info dialog window. HostMonitor will display button that allows you to bring up chart for the test item

Log Visualizer may utilize all types of log files: HTML, Text, and DBF log files. It is also able to utilize the log records, stored in various databases using ODBC interface.

Usage and input parameters

When you use HostMonitor to start Log Visualizer, HostMonitor checks logvisualizer.ini file, adjusts parameters (e.g. ODBC data source parameters) and utilizes necessary command line switches to start utility in maintenance-free mode. So you just should click a button to see the chart for specified test item.

When you start Log Visualizer manually or you need to create your own script to launch the utility, use the following command line syntax:

```
logvisualizer.exe -testid:<TestID> -logprofile:<profile_name> [-inputfile:<log_filename>]
  [-outputimage:<image_filename>] [-period:<chart_period>]
  [-daysback:<number_of_days> | -starttime:<mm/dd/yyyy>] [-setmax:<upper_limit>]
  [-setunits:<unit_name>]
```

First 2 parameters are obligatory:

-testid	TestID - ID of the test that should be analyzed and visualized. You may use HostMonitor's Test Info dialog to find out ID of some specific test item. If you need to know ID for all test items, you may use Custom HTML report with %TestID% macro variable in the template.
-logprofile	profile_name - name of the file that contains application settings. See Setup profiles section for details. You may specify filename without path when profile is located in current directory (e.g. –logprofile:logvisualizer.ini), otherwise you should provide path to the file (e.g. "–logprofile:c:\program files\hostmon\lv2.ini")

Other parameters are optional:

-inputfile	log_filename - HostMonitor's log file (HTML, TXT or DBF). When inputfile is not specified, Log Visualizer will check ODBC log setting. If ODBC log is specified, it will be used for analyzing.
-outputimage	image_filename - name of the GIF file. If this parameter is specified, Log Visualizer will create GIF file with image of the chart. Application will not display anything on screen.
-period	chart_period parameter specifies length of time frame that should be displayed and precision of the chart. There are several visualization levels

available:

1. DayByHours – a chart on hourly basis based on last 48 hours
2. WeekByHours – a chart on hourly basis based on 1 week of data
3. WeekbyDays – a chart on daily basis based on 1 week of data
4. MonthByDays – a chart on daily basis based on 1 month of data
5. MonthByWeeks – a chart on weekly basis based on 1 month of data
6. YearByWeeks – a chart on weekly basis based on 1 year of data
7. YearByMonths – a chart on monthly basis based on 1 year of data

-daysback — This parameter allows you to shift time interval used for the chart by certain number of days. By default, daysback is set to 0. This means chart bounds are calculated relatively to current date. If you set daysback to 1, charts bounds will be calculated from yesterday, and so on.
Note: you also may specify negative values for daysback parameter. Unlike positive values, that just shift chart bounds back in time, negative values have predefined meanings that depend on chart period parameter. There is a list of special values:

If chart period is set to WeekByHours or WeekByDays, you may use the following numbers for daysback parameter
-3 the beginning of the chart will be aligned to the first day of the current week
-4 the beginning of the chart will be aligned to the first day of the previous week
-10 two weeks shift, aligned to the first day of the week
-11 three weeks shift, aligned to the first day of the week

If chart period is set to MonthByDays or MonthsByWeeks, you may set daysback parameter to using the following values:
-5 the initial chart bound will be aligned to the first day of this month
-6 the initial chart bound will be aligned to the first day of the previous month
-9 two months shift, aligned to the first day of the month

If chart period is set to YearByWeeks or YearByMonths, you may use the following numbers for daysback parameter
-7 the left chart bound will be aligned to the first day of this year
-8 the left chart bound will be aligned to the first day of the last year

-starttime — Sometimes you may need to visualize logging data for specific period of time instead of showing test results for the last day/week/month. In such case you may use -starttime:mm/dd/yyyy command line parameter instead of -daysback parameter.

-setmax — <upper_limit> specifies the upper limit of the vertical axis. You may use this parameter to display the "Reply" values of the test with a different scale. E.g. for CPU Usage tests you may use –setmax:100 option to set axis of ordinates to 100(%).
<upper_limit> can be specified as an integer number or a number and special suffix: Kbit, Mbit, Gbit, KB, MB, GB. Please conclude parameter in quotes when you are using suffix E.g. “-setmax:50 MB”.

Note: if some test results are greater than specified limit, Log Visualizer will adjust limit so all tests results will be visible.

-setunits — You may use one of the following units for "setunits" parameter:
- KB
- MB
- GB
- TB
- Kbit
- Mbit
- GBit

Several examples of command line that starts Log Visualizer:

```
logvisualizer -testid:1520 -logprofile:C:\HM\lv_profile.ini "-setmax:500 Gb" –setunits:MB
logvisualizer -testid:1520 -logprofile:C:\HM\lv_profile.ini -inputfile:C:\HM\Logs\log.htm
logvisualizer -testid:1520 -logprofile:C:\HM\lv_profile.ini -period:MonthByDays -outputimage:C:\HM\Images\daily_11564.gif
logvisualizer -testid:1520 -logprofile:C:\HM\lv_profile.ini -daysback:30 -outputimage:C:\HM\Images\daily_115645.gif
logvisualizer -testid:1520 -logprofile:C:\HM\lv_profile.ini -starttime:01/15/2009
```

Batch mode

If you setup HostMonitor to change log file on regular basis (weekly, monthly, etc) and you have not used Log Visualizer on regular basis, you may need to start application in batch mode using the following command line:

```
logvisualizer.exe -batch_mode -logprofile:<profile_name> -inputfile:<log_filename> [-clear_repository]
```

-batch_mode — This parameter tells application to analyze specified log file (see -inputfile parameter) and update repository without displaying GUI and without creating GIF image for a test item

-logprofile — profile_name - name of the file that contains application settings. See Setup profiles section for details. You may specify filename without path when profile is located in current directory (e.g. –logprofile:logvisualizer.ini), otherwise you should provide path to the file (e.g. "–logprofile:c:\program files\hostmon\lv2.ini")

-inputfile — log_filename - HostMonitor's log file (HTML, TXT or DBF)

-clear_repository — When this optional parameter specified, Log Visualizer removes all records from repository before processing log file

Batch mode allows you to analyze several log files one by one and create up-to-date repository without spending time for manual setup. For example, if you setup HostMonitor using "Automatically change the log every month" option, HostMonitor creates 12 files during each year: 012007-log.htm, 022007-log.htm, 032007-log.htm, …, 122007-log.htm. Then you may create simple BAT file to analyze all log files for 2007:

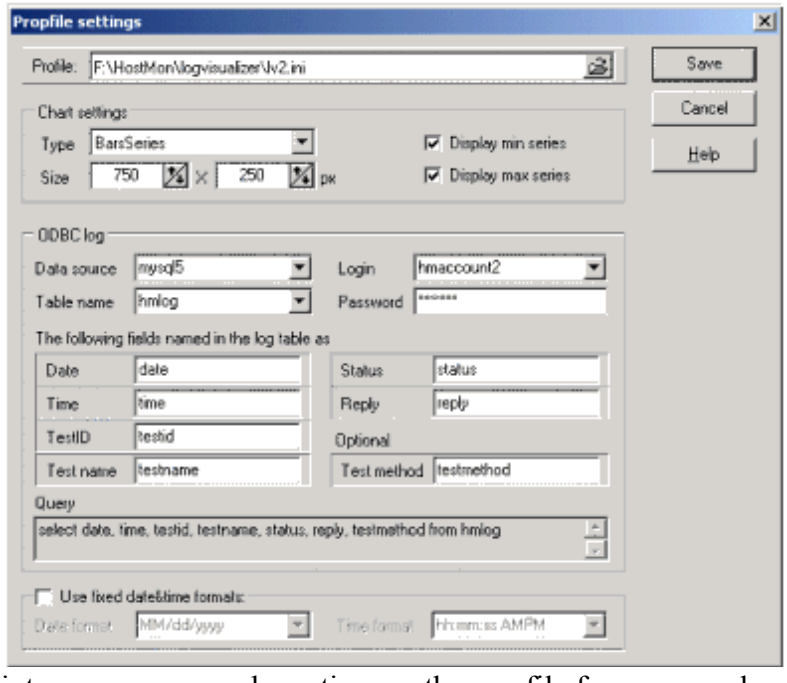
```
for /L %i in (1,1,9) do logvisualizer.exe -batch_mode -logprofile:logvisualizer.ini "-inputfile:c:\hostmon7\logs\0%i2007-log.htm"
for /L %i in (10,1,12) do logvisualizer.exe –batch_mode –logprofile:logvisualizer.ini "-inputfile:c:\hostmon7\logs\%i2007-log.htm"
```

Note: you should analyze log files in proper order, i.e. April log file should be analyzer before May log file.

Setup profiles

To setup profile use the following command line

```
logvisualizer.exe –setupprofile:<profile_name>
```



-setupprofile parameter tells application to load specified profile (specially formatted text file) and bring-up "Profile setting" dialog window. You may specify filename without path when profile is located in current directory (e.g. –setupprofile:logvisualizer.ini), otherwise you should provide path to the file (e.g. "–setupprofile:c:\hostmon\lv2.ini").

Note #1: if you specify non-existing file, application may create new file after user's confirmation.
Note #2: HostMonitor may modify logvisualizer.ini file. If you plan to use Log Visualizer with your own scripts, we recommend creating another profile for your needs.

You may use "Profile settings" dialog window to setup several profiles. Different profiles may describe different ODBC logs and various chart setting. This way you may easily generate various kinds of charts.

Chart settings

Type
This option allows you to select type of the chart. There are four chart types available: Area series, Bar series, Line series, Point series

Size
This parameter specifies width and height of the chart image

Display min series
Display max series

Chart always shows average results (reply of the test item) for each time interval (hour, day, week…). In addition to average reply Log Visualizer may display minimum and maximum values. These 2 options allow you to enable such series.

ODBC log

Log Visualizer may analyze log records that are stored in various databases. Before using such logs you should describe database parameters using "ODBC logs" section of the profile.
For each log you should specify the following parameters:

Data source

Select the data source from drop-down list that displays list of all ODBC data sources installed on your system.
Note: To install or configure Data Source, click Windows Start button, point to Settings, and then click Control Panel. Double-click Administrative Tools, and then double-click Data Sources (ODBC)

Table name

Provide the name of a table that contains log records

Login/Password

Provide login and password (if required) for database access

Following fields named in the log table as

This option defines actual fields in the table that stores tests results (HostMonitor's ODBC logging could be configured in different ways).

Date / Time

Provide the name of field(s) that stores information about event date and time. If a single field of the table contains information about date and time, type the same name for both options. Type of the field could be Date, DateTime, TimeStamp or it can be a text field (which is not recommended).

TestID

Name of the field that stores unique ID of the test. TestID is always unique within an HML file.

Test name

Specify the name of a field that stores the name of the test.

Status

Provide the name of a field with status information. It could be text field that stores status as a text, e.g. "Host is alive", "No answer", etc. Or it can be numeric field, where number represents certain status:

00- Not tested
01- Host is alive
02- No answer
03- Unknown
04- Unknown host
05- Checking
06- Resolving
07- Ok
08- Bad
09- Disabled
10- Bad contents
11- Wait for Master
12- Out of schedule
13- Paused
14- Warning
15- Normal

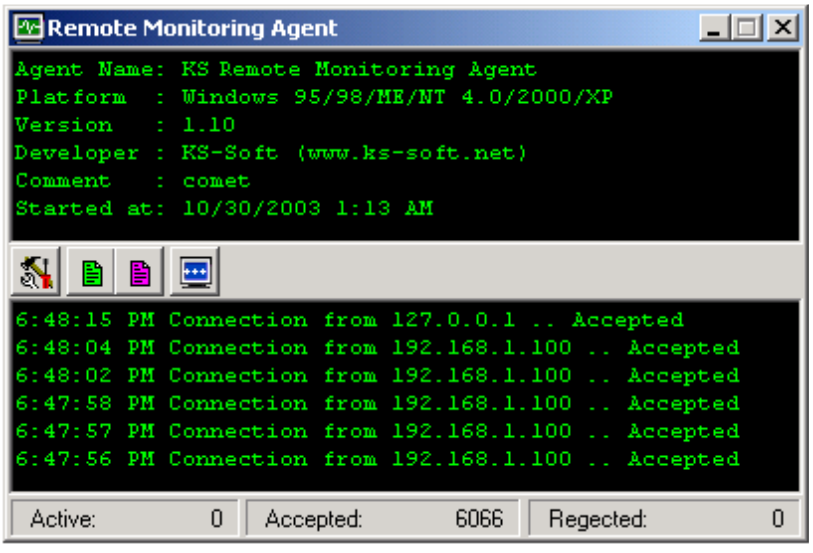
Reply
Specify the name of a field that stores Reply value of the test. It could be text or numeric field.

Test method
Optionally you may (and we recommend doing this) provide the name of a field that stores information about the test method.

Use fixed date&time format
By default Log Visualizer gets current Windows regional settings at startup and uses these parameters to process data/time variables. You may use this option to define the date & time formats (e.g. DD/MM/YYYY h:mm:ss AMPM). In this case, Log Visualizer will use the specified formats overriding the system settings.
BTW: Changing the date format does not affect analyzing of the DBF and HTML log files. Log Visualizer is able to analyze these log files correctly regardless of the date & time settings. However this option can be useful to analyze text log files or html log files that were created by older versions of HostMonitor.

RMA for Windows

HostMonitor can monitor remote networks using Remote Monitoring Agents (RMA). RMA is small application that accepts requests from HostMonitor, performs test (or action) and provides information about test result back to HostMonitor.



Why you may need RMA? Here are just several reasons:

1. RMA increases security of the network. When you have to run the tests such as CPU Usage test or Performance Counters tests on a remote system, HostMonitor must be able to log in to that system with administrators privileges. Instead you may now use an agent installed on that remote system. In this case HostMonitor will not have to log on to that system at all. HostMonitor needs just one TCP port to communicate with the RMA agent (by default Passive RMA utilizes TCP port 1055, Active RMA uses port 5056; however you may set an agent to use any other port).

2. Remote Monitoring Agent is also a very useful tool when you have to monitor two (or many) separated networks (connected through Internet). In this case installing just one instance of RMA behind the firewall in network "A" will allow to monitor entire network "A" using the HostMonitor located in the network "B" with just one open TCP port.

3. RMA decreases the network traffic. E.g. frequent use of "File Integrity" or "Compare Files" tests in an array of remote systems may apply significant load on the network. The more and the bigger files you test the more traffic increase you get. RMA runs locally and sends only the test results to the HostMonitor thus decreasing the amount of network traffic.

4. RMA simplifies network administration. You no longer need to share drives to perform tests like Folder/File Size, File Availability, Count Files, etc

5. RMA for Window allows you to execute actions on remote systems. E.g. agent can launch some application or restart service on a system behind firewall.

6. RMA for AIX / Linux / BSD / Solaris allows you to perform tests that HostMonitor cannot perform. For example HostMonitor cannot monitor processes that are running on Linux systems. RMA can do that.

Features:

- All traffic between RMA and HostMonitor is encrypted.
- It is possible to customize the list of enabled tests for each of the agents (e.g. living only Count Files and Drive Free Space tests only).
- You can restrict incoming TCP connections with the list of acceptable addresses.
- With RMA Manager you may configure, restart and even upgrade agent(s) remotely.

Backup Agent

Since the version 6.00 HostMonitor allows you to setup primary and backup agents. Using this feature, HostMonitor is able to balance load between agents and use the backup agent when primary one does not respond. Yes, RMA is pretty stable software however system may not respond due to some hardware or network error.
See "Agent Connection Parameters" for details.

Passive RMA versus Active RMA

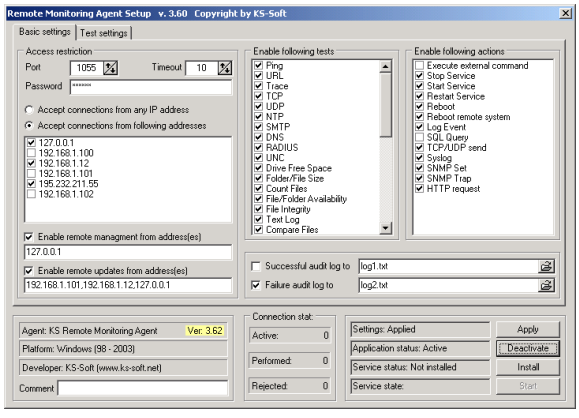
Passive RMA opens specified TCP port for listening and waits for connection requests from HostMonitor and RMA Manager, then RMA performs test (or action) and provides information about test result back to HostMonitor.

Active RMA – Remote Monitoring Agent that is not waiting for TCP connection from HostMonitor like regular RMA (now it's called as Passive RMA). Active RMA itself establishes connection with HostMonitor and RMA Manager. This allows you to install RMA inside private network protected by firewall without necessity to open any TCP port (Passive RMA requires 1 open TCP port). Also Active RMA allows you to monitor system that does not have fixed IP address, e.g. system that is connecting to the network using temporary dial-up connection.
Several procedures help to monitor networks over unreliable connections:

- Active RMA may store test results when network connection unexpectedly brakes off, it will try to reconnect to HostMonitor and send test results upon connection;
- HostMonitor uses more flexible schedule for the tests that should be performed by Active RMA, e.g. if test has to be performed immediately but Active RMA is not connected while it was connected several minutes ago, HostMonitor may wait for another connection up to 4 min before assigning Unknown status to the tests. Note: if you select the test item and click Refresh button, HostMonitor will not wait for connection, it will set Unknown status right away;
- For each active agent you may setup Backup Active RMA. Using this feature, HostMonitor is able to balance load between agents and use the backup agent when the primary one cannot establish communication channel.

Active RMA for Windows can be started as a regular application or as a Win32 service and perform the same set of tests and actions supported by Passive RMA.
Active RMA for UNIX is not available yet.

How to install RMA



To install RMA run installation program for Advanced Host Monitor package (host-mon.exe). At the stage when installation wizard offers you to choose an installation package, you should select "Custom Install". Then in the list of available components check the box in front of the "RMA for Windows". If you want to install only "RMA for Windows" then uncheck everything except "RMA for Windows".

If you need to install RMA on an array of systems, then the easiest way is to:

- Install it on one system using installation program (see the instructions in previous paragraph)
- Configure an agent (setup timeout, password, list of enabled tests, enable or disable remote management, etc)
- Then simply copy preconfigured agent to all systems. You need to copy just 3 files: rma_cfg.exe, rma.ini, rma.exe (if you need Passive RMA) or rma_active.exe (when you need Active RMA).
- Note: you should assign unique name for each Active RMA. If you assign the same name for several agents, HostMonitor will accept connection from 1st started agent and reject connections from other agents with the same name

Note 1: It is also possible (however you may never need it) to run several instances of RMA on the same system. To do this you have to install several copies of RMA into different folders on the hard drive. Each copy of Passive RMA should then be set to use different TCP port. You should assign unique name for each Active agent.

Note 2: RmaInstaller utility allows you to install Remote Monitoring Agent as Win32 service on remote systems. The utility included into Advanced Host Monitor package; after installation you may find this utility in “Utils\RmaInstaller“ sub-directory.

How to configure RMA

To configure an agent you may use rma_cfg.exe program (after installation it will be located in the same directory where an agent is installed) or you may start an agent and click on "Settings" button on the tool bar. This button launches the same configuration utility which pops up as a new window.

The lower part of the configuration window mostly contains information about an agent. Those fields are joined into three groups: Agent information, Statistics and Agent status.

Agent information:
You are not able to change information shown in grey fields. They show data that was predefined by a software developer.

- Agent: an internal name of an agent
- Version: the version number of the agent.
- Platform: OS platform that this agent is designed for.
- Developer: the company that created RMA software.
- Comment: this is the only field available for editing in this section. Here you may specify a comment (actually you may type any text here, it could be a simple recognizable name or an identifier for this agent). This helps to identify agents easier.

HostMonitor and RMA Manager will display the content of these fields when they work with remote agents.

Connection statistics

- Active: this is the number of requests that this agent is currently processing
- Performed: the number of requests processed since last time the agent was started.
- Rejected: the number of requests that have been rejected by the agent since it was started. A rejection may be a result of a connection with invalid password or from an IP address that is not allowed.

Agent status

These three fields show the status of an agent as an application or Win32 service (you may start an agent in either of these two modes). Also this section shows you the state of currently edited agent configuration i.e.: are the changes for the current configuration already saved or not. Each field is followed by a corresponding control button:

- **Settings**: initially, or after you just have started configuration utility, this field says "Applied". This means that the current settings of RMA were not changed yet. As soon as you start typing in any of the fields available for the user, caption changes to "Modifications are not saved" as a reminder that the current changes for the configuration are not saved and thus are not in effect. Only after you click the button "Apply" the changes will be saved. Note that after you have applied changes the caption returns to "Applied".

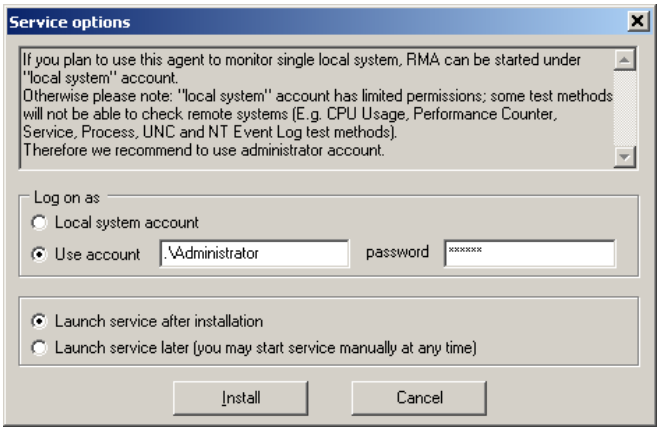
- **Application status**: says either "Active" when RMA is running as a regular application or "Not Active" when RMA is not running. The button beside this field is correspondingly captioned saying "Activate" when RMA is not running, so it will start RMA if you press it. Caption "Deactivate" on the button means that RMA is currently running as a regular application and if you press the button it will be terminated.
  Note that the configuration utility is a separate application and it may run independently, even when RMA is not running.

- **Service status**: On Windows agent can be installed as a Win32 service (except Windows 9x and Windows ME). This field and the button display and control the status of RMA as a Win32 service. "Not installed" means RMA is not installed as a Win32 service. "Installed" means that RMA is already installed as a Win32 service. The button beside the field changes its` caption correspondingly - "Uninstall" when RMA is installed as a Win32 service or "Install" when its not. RMA in a Win32 service mode is loaded automatically at a system startup.

- **Service state**: this field is empty when Win32 service is not installed. After the servise was installed the following captions will tell you its status: "STOPPED" means the service is

installed but not started. "STARTED" is displayed when the service is running. The button "Start/Stop" allows you to start or stop the service.

- When you install RMA as a service, configuration utility displays “Service options” dialog. “Service options” dialog allows you to specify user account for the service and then lauch the service. If you do not plan to start service right away, select “Launch service later” option and click Ok. In such case service will be started at system startup. Also you may start service at any time using standard Windows “Services” applet or RMA_CFG utility.



  Note: If you plan to use agent to monitor single local system, RMA can be started under "local system" account. Otherwise please note: "local system" account has limited permissions; some test methods will not be able to check remote systems (E.g. CPU Usage, Performance Counter, Service, Process, UNC and NT Event Log test methods). Therefore we recommend using administrator account.

Passive RMA settings

Connection parameters

- **Port**
  specifies the TCP port number which RMA utilizes to listen for incoming connections. Default setting is #1055.

- **Timeout**
  the maximum amount of time (in seconds) that agent will keep waiting for the complete request packet from HostMonitor (after initial TCP connection established) before dropping the connection.

- **Password**
  minimum six character length password. Using of an empty password is not permitted. The password is required for every communication session between RMA and HostMonitor or RMA and RMA Manager. All traffic between RMA and HostMonitor or RMA and RMA Manager is encrypted and the password itself is never transmitted through the network without encryption.

Security settings

- **Accept connections from any IP address**
  enabling this option will allow RMA to accept control commands from any IP address (as long as the incoming connection provides correct password)
- **Accept connections from following addresses**

specifies the list of IP addresses. After enabling this option RMA will accept remote connections only from the addresses in this list (password is required as always). Usually you have to add just one address to this list, namely the one for the system where HostMonitor is running.
To add an address to the list press Insert key, to remove an address from the list press Ctrl+Del, to edit item press Enter or double-click it.

- **Enable remote management from address**
  this option sets the IP address from which it is allowed to control and manage RMA. Using RMA Manager installed on the system with that IP address you will be able to change agent's settings remotely, also you will be able to restart and terminate an agent.

- **Enable remote updates from address**
  this option allows remote updates of the RMA code (e.g. when a new version is available) from the IP address being provided. To upgrade an array of remote agents you may use RMA Manager. Of course all operations with agents are encrypted and password protected but this option increases security even more.

- **Enable following tests**
  specifies the list of tests methods allowed for execution by this RMA. To enable a test mark the corresponding check box, to disable a test unmark the box near it.

- **Enable following actions**
  specifies the list of actions allowed for execution by the agent. To enable a action mark the corresponding check box, to disable a action unmark the box near it.

Logging

Successful audit log to
here you may specify a log file where agent will store information about successfully accepted connections. This log has no use when everything works well (it then just takes space on the hard drive), but you may found it really helpful when a sophisticated network problem has to be fixed. If you specify just the name of the file (without a full path), an agent will store a log in the same directory where it was started from.

Failure audit log to
you may specify another log file where an agent will store information about rejected requests. E.g.: connections from an IP addresses that are not allowed or connections with invalid password, etc. Log file is a simple text file that contains date of the event, remote IP address from which an attempt of connection has occurred and information about the error. If you specify just the file name (without path), an agent will store it in the directory where it was started from.

Active RMA settings

Agent identification

- Name
  Unique name that identifies an agent. You should not assign the same name for several agents. If you do so, HostMonitor will accept connection from 1st started agent and reject connection from other agents with the same name
- Password
  Minimum six-character length password. An empty password using is not permitted. Several RMA agents may use the same password. The password is required for every communication session between RMA and HostMonitor or RMA and RMA Manager. All traffic between RMA and HostMonitor or RMA and RMA Manager is encrypted and the password itself is never transmitted through the network without encryption.

Note: when you setup agent record using HostMonitor or RMA Manager GUI, you should use exactly the same name and password that were used when you setup Active RMA on remote system using rma_cfg utility

HostMonitor connection parameters

- Host
- Port

These parameters specify where HostMonitor is running and what TCP port should be used for connection. You can configure the agent to work with a primary and a backup HostMonitor and RMA Manager.

If you specify the HostMonitor address using 2 hostnames (or IP addresses) separated by comma (for example 10.10.1.5,10.10.2.100) then the agent will try to connect to the first address; if the connection cannot be established, the agent will try to use the second address.

This option can help when HostMonitor system experience some problems with Internet connection and need to switch to a backup Internet service provider.

Allow remote management

- Host
- Port

If you enable remote management, you should specify IP address or hostname of the system where RMA Manager is running. RMA Manager and HostMonitor can be started on the same system and we recommend to do this. In this case you should use different TCP ports for connection. Default settings: HostMonitor listens for incoming connections from RMA on TCP port 5056, while RMA Manager utilizes port 5057.

Note1: It is not necessary to have RMA Manager running all the time. If RMA cannot connect to RMA Manager it will try to establish communication every 30 sec.

Note2: If you start RMA Manager on the same system where HostMonitor is running, HostMonitor tells all connected RMA to establish connection with RMA Manager immediately (if "Full management" option is enabled for the agent).

Note3: You can configure the agent to work with a primary and a backup RMA Manager. If you specify the host using 2 hostnames (or IP addresses) separated by comma (for example 10.10.1.5,17.10.16.100) then the agent will try to connect to the first address; if the connection cannot be established, the agent will try to use the second address.

This option is useful if you need to manage RMA agents from 2 locations, and it can also help when you experience some problems with Internet connection and need to switch to a backup Internet service provider.

Security

- **Enable following tests**
  Here you may specify the list of tests methods allowed for execution by this RMA. To enable a test mark the corresponding check box, to disable a test unmark the box near it.

- **Enable following actions**
  Here you may define the list of actions allowed for execution by the agent. To enable an action mark the corresponding check box, to disable an action unmark the box near it.

Logging

Successful audit log to
here you may specify a log file where agent will store information about successfully accepted connections. This log has no use when everything works well (it then just takes space on the hard drive), but you may found it really helpful when a sophisticated network problem has to be fixed. If you specify just the name of the file (without a full path), an agent will store a log in the same directory where it was started from.

Failure audit log to
you may specify another log file where an agent will store information about rejected requests. E.g.: connections from an IP addresses that are not allowed or connections with invalid password, etc. Log file is a simple text file that contains date of the event, remote IP address from which an attempt of connection has occurred and information about the error. If you specify just the file name (without path), an agent will store it in the directory where it was started from.

The following settings have absolutely identical meaning for Passive and Active agents, however you may setup agents independently even if both RMA installed in the same folder.

Test settings:

Following options define how agent should access the net in order to perform "URL" tests.

- **USE REGISTRY CONFIGURATION**
  Agent retrieves the proxy or direct configuration from the registry.
- **DIRECT TO NET**
  Agent resolves all host names locally.
- **VIA NAMED PROXY**
  Agent passes requests to the proxy unless a proxy bypass list is supplied and the name to be resolved bypasses the proxy.
- **PRECONFIG, PREVENT USING JAVA/SCRIPT/INS**
  Agent retrieves the proxy or direct configuration from the registry and prevents the use of a startup JScript or Internet Setup (INS) file.

Do not check Internet connection

Normally RMA checks if computer is connected to Internet before performing "URL" test (to avoid appearance of Dial-Up dialog). With this option enabled RMA will not perform such check.

Following settings are used when access method is set to "VIA NAMED PROXY"

- **Proxy server** - address of your proxy server
- **Proxy port** - port number of the proxy server
- **Use proxy authentication** - if your proxy server requires authentication you may specify the username and password in these fields.
- **Proxy bypass list** - list of addresses that don't need to be accessed through your proxy server. This list may include IP addresses, host names, or names of computers from your intranet. Also, wildcards may be used as well to match domains, host names or addresses. For example: www.*.com; 128.*; *man*; and so on. For local addresses use the "<local>" macro. Use semicolons ";" to separate entries.

Performance Counter test related options

Windows implementation of performance counters has bugs. E.g., Windows 2000 (Professional, Server, and Advanced Server editions) can produce memory leak in PDH.DLL when user (application) querying performance counter that does not exist. This bug fixed in SP2. Also PDH.DLL does not work correctly with multithread applications.
That's why in RMA we have implemented several different methods to work with PDH.DLL:

- **MultiThread** mode: RMA works almost according to Microsoft documentation with some workaround to avoid most likely problems. Agent loads pdh.dll at once and uses it all the time. This method fast because RMA can start several tests simultaneously. If everything will work correctly on your system, use this method.
- **OneByOne** mode: Using this method agent will start Performance Counter tests one by one. This method is slow but using this method you may avoid problems due to a buggy pdh.dll
- **Smart** mode: With this method RMA will try to detect when pdh.dll has to be reloaded...
- **External**: Use external (perfobj.exe) utility to perform the tests. This is fast and most reliable method.

Alerts

If for some reason Active RMA cannot connect to HostMonitor and RMA Manager, or Passive RMA does not receive any TCP connections from HostMonitor and RMA Manager, then agents can execute the specified commands. There are new options that can be set using RMA Manager or rma_cfg utility

Execute 1st command if there is no connection to/from HostMonitor for N minutes
Ping the following host and execute different commands depending on the results

<Host> | <Timeout> | <Retries>
Exec command if accessible <command line>
Otherwise execute command <command line>

Execute 2nd command if there is no connection to/from HostMonitor for N minutes
Ping the following host and execute different commands depending on the results
<Host> | <Timeout> | <Retries>
Exec command if accessible <command line>
Otherwise execute command <command line>

Execute command if connection was restored after "bad" alert command was triggered
<command line>

For example, you can setup an Active RMA agent to start a dial-up program when the agent cannot connect to HostMonitor and RMA Manager for 5 minutes and ping to your web site fails.

Please note: Active RMA agents always trying to connect to HostMonitor as soon as possible. While HostMonitor connects to Passive RMA only when it needs to perform some test. If only a few tests with long intervals are set for some passive RMA agents, then the lack of connection requests from HostMonitor may be perfectly normal. For example, if there are only a few tests that the Passive RMA agent needs to perform once an hour, then HostMonitor will only connect to that agent once an hour and then disconnect.

RMA Manager

To configure huge arrays of remote agents installed in different networks you may use RMA Manager. It allows you to change settings for hundreds of agents installed on remote systems at one time and from one comfortable location.

How to use

O.k., now when you have your agents installed in different networks, how to use them?
HostMonitor since version 4.0 supports a list of remote agents and can perform tests not only by itself but also may send a request to the agent which will then execute the test. Every test in HostMonitor has now an additional property: "Test by". By default it has the value "HostMonitor"; it means that the test will be executed by HostMonitor. Alternatively you may choose an agent from drop down list and the test will be performed by that agent.

How to check status of the agent

When you use single agent to perform various tests, you may want to setup Master test to check agent status. In such case HostMonitor may send single alert informing you about disconnected agent and hold dependant test items (so you will receive single alert instead of hundred warnings for all tests performed by this agent).
What test can you use as Master test?

- Passive RMA: It's pretty easy to check Passive RMA status when you do not use Backup RMA. You may use TCP test to check if RMA receives connections on specified TCP port or use Ping

test performed by the agent to check localhost (127.0.0.1). Such Ping test will always return "Host is alive" status when successfully authenticated connection to the agent can be established. If there is backup agent in use, you may setup Ping test performed by Passive RMA using **rma itself** string as target host name. In such case HostMonitor will check agent status without using backup agent even if such backup agent was specified for selected RMA

- Active RMA: Things a little more tricky when you need to check Active RMA status. Yes, you may setup the same "Ping localhost" test to check agent status. However this may lead to some delay in reaction - HostMonitor will not perform test if agent was connected but lost connection just a moment ago. HostMonitor may wait up to several minutes for new connection before changing test status to "Unknown". Dependant test items will be delayed as well so such delay is not a big problem, you will not receive a lot of alerts. However if for some reason you need to receive alert immediately, there is solution: setup Ping test using Active RMA and type **rma itself** string instead of localhost or target host name. In such case HostMonitor will display agent status immediately. HostMonitor will not use backup agent (if any) when specified agent is not connected; also HostMonitor will not wait for agent re-connection.

Known problems:

Windows NT Workstation, Windows 2000 Workstation and XP Professional has a serious limitation: maximum length of the queue for pending TCP connections is limited to 5 items.
This limitation creates problems when you want to perform lots of tests by a single Passive remote agent (e.g. monitoring many systems by a single agent that is installed on the system in the remote network).

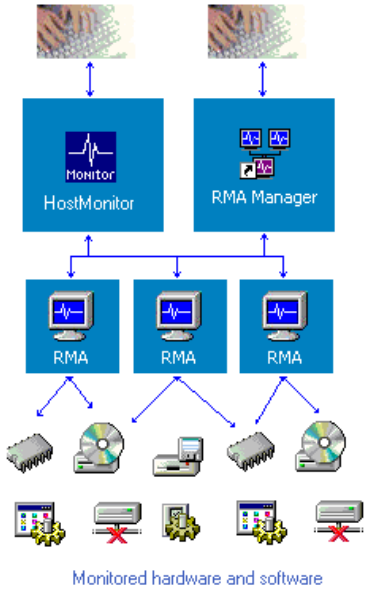
Suggested solution:
To avoid possible rejections of requests caused by the queue overflow you should:

- Install an agent on the system with Windows Server edition.
- Use Active RMA agent

RMA for Linux, FreeBSD, NetBSD, OpenBSD and Solaris

HostMonitor can monitor remote networks using Remote Monitoring Agents (RMA). RMA is small application that accepts requests from HostMonitor, performs test and provides information about test result back to HostMonitor.

Why you may need RMA? Here are just several reasons:



1. RMA increases security of the network. When you have to run the tests such as CPU Usage test or Performance Counters tests on a remote Windows system, HostMonitor must be able to log in to that system with administrator's privileges. Instead you may now use an agent installed on that remote system. In this case HostMonitor will not have to log on to that system at all. HostMonitor needs just one TCP port to communicate with the RMA agent (by default it uses #1055 port, however you may set an agent to use any other port).

2. Remote Monitoring Agent is also a very useful tool when you have to monitor two (or many) separated networks (connected through Internet). In this case installing just one instance of RMA behind the firewall in network "A" will allow to monitor entire network "A" using the HostMonitor located in the network "B" with just one open TCP port.

3. RMA decreases the network traffic. E.g. frequent use of "File Integrity" or "Compare Files" tests in an array of remote systems may apply significant load on the network. The more and the bigger files you test the more traffic increase you get. RMA runs locally and sends only the test results to the HostMonitor thus decreasing the amount of network traffic.

4. RMA simplifies network administration. You no longer need to share local drives/folders to perform tests such as File Integrity, Folder/File Size, File Availability, Count Files, etc

5. RMA for BSD/Linux/Solaris allows you to perform tests that HostMonitor cannot perform itself. For example HostMonitor cannot check number of user sessions on Linux systems. RMA can do that.

Features:

- All traffic between RMA and HostMonitor is encrypted.
- It is possible to customize the list of enabled tests for each of the agents (e.g. living only Count Files and UNC tests only).
- You can restrict incoming TCP connections with the list of acceptable addresses.
- With RMA Manager you may configure, restart and even upgrade agent(s) remotely.

Backup Agent
Since the version 6.00 HostMonitor allows you to setup primary and backup agents. Using this feature, HostMonitor is able to balance load between agents and use the backup agent when primary one does not respond. Yes, RMA is pretty stable software however system may not respond due to some hardware or network error.
See "Agent Connection Parameters" for details.

Remote Monitoring Agent for Windows platform is included into Advanced Host Monitor package. For more information, please, refer to RMA for Windows section of this document.

How to install and configure RMA

To install an agent on BSD/Linux/Solaris system download appropriate package from www.ks-soft.net/hostmon.eng/downpage.htm, unzip and untar the files (e.g. using command "tar –xzf rma_lin.tgz"). Check, and modify if necessary, settings in the rma.ini file using any text editor.

RMA Settings

In the rma.ini file you will find comments that describe each parameter, so configuration should be easy

Basic settings

- **RmaPath**
  Obligatory parameter - full path to the agent. UNIX-like systems do not have common method that allows the program to retrieve its module name and path. Without this parameter agent will not be able to upgrade and restart itself.
  Example: **RmaPath** = /usr/sbin/rma

- **TmpDir**
  This parameter is optional. For some tests (CPU, Process and Shell Script) agent creates temporary files. RMA searches for temporary directory in the following order:
  - directory that specified by this option (TMPDIR)
  - directory that specified by "TMPDIR" environment variable
  - directory that specified by "TMP" environment variable
  - if non of these parameters are specified or specified directories do not exist, RMA uses current directory

  Example: **TmpDir** = /usr/tmp/rma

- **Comment**
  Comment is optional parameter, here you may specify a comment (actually you may type any text here, it could be a simple recognizable name or an identifier for this agent). This helps to identify agents easier.
  Example: **Comment**=RMA on Primary Web Server (FreeBSD)

- **Host**
  Optional parameter that defines host name or IP address of the local network interface (RMA should listen on). Useful when system has several network interfaces.

- **Port**
  Obligatory parameter - specifies the TCP port number, which RMA utilizes to listen for incoming connections. Default setting is #1055.

- **Timeout**
  The maximum amount of time (in miliseconds) that agent will keep waiting for the complete request packet from HostMonitor (after initial TCP connection established) before dropping the connection.

- **Password**
  Minimum six characters length password. Using of an empty password is not permitted. The password is required for every communication session between RMA and HostMonitor or RMA and RMA Manager. All traffic between RMA and HostMonitor or RMA and RMA Manager is encrypted and the password itself is never transmitted through the network without encryption.

Logging settings

- **LogSuccess**
- **OkLogFile**

  "Successful" log. Here you may specify a log file where agent will store information about successfully accepted connections. This log has no use when everything works well (it then just takes space on the hard drive), but you may found it helpful when a sophisticated network problem has to be fixed.
  First option enables or disables the logging (LogSuccess=0 – logging is disabled; LogSuccess=1 – logging is enabled), second parameter specifies path to the log file. If you specify just the name of the file (without a full path), an agent will store a log in the same directory where configuration file is located.
  Example:
  LogSuccess=0
  OkLogFile=log_ok.txt

- **LogFails**
- **BadLogFile**
  "Failure" log. Here you may specify another log file where an agent will store information about rejected requests and errors. Log file is a simple text file that contains date of the event, remote IP address from which an attempt of connection has occurred and information about the error.
  First option enables or disables the logging (LogFails=0 – logging is disabled; LogFails=1 – logging is enabled), second parameter specifies path to the log file. If you specify just the file name (without path), an agent will store it in the directory where configuration file is located.
  Example:
  LogFails=1
  BadLogFile=log_err.txt

- **VerboseLogFile**
  Use this parameter to provide the path to a "Verbose" log file. Unlike Successful and Failure logs this log file can be enabled by command line parameter only. You should start RMA with '-v' command line parameter (e.g. "./rma –i –v rma.ini") . In this case RMA will store various information about each incoming connection in the log file specified.
  Example: VerboseLogFile=log_verbose.txt

Security settings

- **FilterActive**
  Enables or disables IP filtering "FilterActive=0" will allow RMA to accept control commands from any IP address (as long as the incoming connection provides correct password). Set "FilterActive=1" and RMA will accept connections only from the addresses that are specified in by FilterList parameter (password is required as always).
- **FilterList**
  Provides list of IP addresses. After enabling IP filtering (FilterActive=1) RMA will accept remote connections only from the addresses in this list (password is required as always). Usually you have to add just one address to this list, namely the one for the system where HostMonitor is running. If you want to specify several IP addresses, separate them by spaces.
- **FilterMarks**
  This additional option works as switch for the addresses that are specified by "FilterList" parameter. E.g. if you have 4 addresses in the list, and you want to turn on (enable) 1st, 2nd, and 4th address and turn off (disable) 3rd address in the list, type "1101" in this field.
  Example:
  FilterActive=1
  FilterList=127.0.0.1 194.168.1.10 194.168.1.12
  FilterMarks=101

- **AllowManage**
- **ManageAddr**
  These options control remote management function. AllowManage=0 – disables remote management feature, AllowManage=1 – enables remote management. ManageAddr option sets

the IP address(es) from which it is allowed to control and manage RMA. Using RMA Manager installed on the system with that IP address you will be able to change agent's settings remotely, also you will be able to restart and terminate an agent.
Note: Instead of single IP address you may specify a list and/or a range of IP addresses. IP addresses in the list should be separated by comma. Dash is used to define a range of addresses.
Example:
AllowManage=1
ManageAddr=192.168.1.100-192.168.1.105, 192.168.1.12, 127.0.0.1

- **AllowUpdates**
- **UpdateAddr**

  AllowUpdates option allows or restricts remote updates of the RMA (e.g. when a new version is available). AllowUpdates=0 – restricts updating, AllowUpdates=1 – allows updating. UpdateAddr option sets the IP address(s) from which it is allowed to perform upgrade. To upgrade a single agent or an array of remote agents, you may use RMA Manager.
  Note: Instead of single IP address you may specify a list and/or a range of IP addresses. IP addresses in the list should be separated by comma. Dash is used to define a range of addresses.
  Example:
  AllowUpdates=1
  UpdateAddr=192.168.1.100-192.168.1.105, 192.168.1.12, 127.0.0.1

Test settings

- **[EnabledTests]**

  Specifies the list of tests methods allowed for execution by the agent. To enable the test, assign '1' to the parameter. To disable the test, assign '0' to the parameter.
  Example:
  TCP=1
  UDP=0
  UNC=1
  FolderSize=0

- **[Tests]**

  Following parameters provide the path to specialized scripts that RMA needs to perform some tests (such as CPU Usage and Process tests). These tests were implemented as external scripts to simplify customization for various systems. You may easily modify scripts using any text editor.
  If you specify just the name of the file (without a full path), an agent will assume that script shares the same directory with the agent.

  CPUUsageScript
  Provides the path to a script that returns current CPU Usage

  ProcCntScript

Provides the path to a script that returns current number of running instances of the specified process

ProcListScript
Provides the path to a script that returns list of started processes.

RMA Manager

To configure single agent or huge array of remote agents installed in different networks you may use RMA Manager. It allows you to change settings for hundreds of agents installed on remote systems at one time and from one comfortable location.

Starting an agent

You can start agent as daemon or as regular console utility.

Usage: rma [-d|-i] [-v] [-p <port>] <cfg_file>
-d - daemon mode (default)
-i - interactive mode
-v - verbose mode
-p <port> - overrides TCP port number specified in cfg_file
cfg_file - obligatory parameter, path to configuration file
Examples:
./rma -i -v -p 1055 /etc/rma/rma.ini
./rma -d /home/ks/rma/rma.ini

Note: SIGHUP signal
You can use SIGHUP to signal the agent that it should reread configuration file E.g. "kill -HUP <agent_pid>" (to retrieve agent pid you can use command "ps -A|grep rma" (on Linux systems) or "ps –x|grep rma" on FreeBSD systems).
PS: of course you can use RMA Manager for the same purpose.

How to use

O.k., now when you have agents installed, how to use them?
HostMonitor since version 4.0 supports a list of remote agents and can perform tests not only by itself but also may send a request to the agent, which will then execute the test. Every test in HostMonitor has now an additional property: "Test by". By default it has the value "HostMonitor"; it means that the test will be executed by HostMonitor. Alternatively you may choose an agent from drop down list and the test will be performed by that agent.

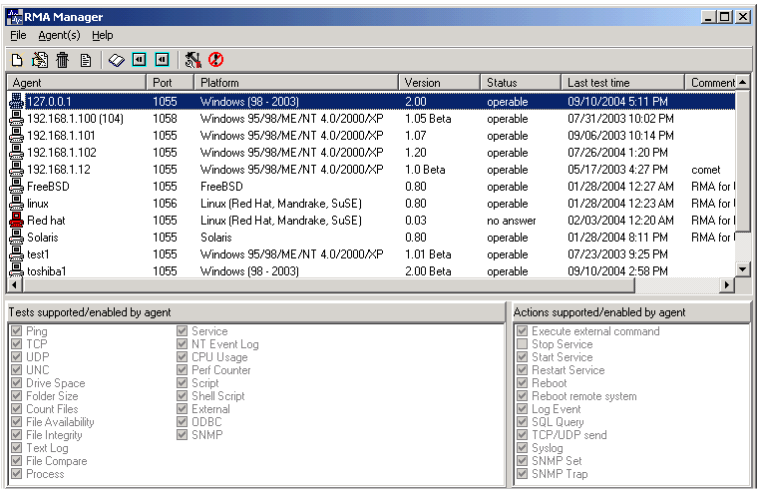
Peculiarities of tests' settings for UNIX-like systems

When you setup file-related tests (UNC, Folder/File Size, Count Files, File Integrity, etc) using an agent installed on UNIX-like system you should have in mind:

- on Windows system file masks '*' and '*.*' represent any file. On UNIX-like system only '*' represents any file; '*.*' can be used for any file that has dot (.) in the name;
- use slash (/) in the path (instead of backslash (\) that you are using on Windows systems);
- on UNIX-like systems name of the file is case sensitive (so "/etc/RMA" and "/etc/rma" are different files);
- “Drive Free Space” test does not have sense for UNIX-like system because there are no drives, use UNC test instead (e.g. you can check free space for file system “/home”)

RMA Manager

To manage an array of Remote Monitoring Agents (RMA) you may use RMA Manager utility. It allows you to change settings for hundreds of agents installed on remote systems at one time and from one location. Both RMA Manager and HostMonitor are using the same list of Remote Monitor Agents. Working with this list you may select group(s) of agents and then perform the following actions over the whole group:



- obtain information about an agent: version, platform, list of tests supported by the agent, list of allowed tests, etc;
- change agent configuration: change TCP port, timeout, password; enable/disable tests, change different management parameters, etc;
- reload agent (restart application);
- force agent to reread settings from its ini file;
- terminate agent
- and even upgrade agent's code remotely.

RMA Manager splits Passive RMA and Active RMA between 2 lists on the screen. However information about all agents stored in the same file (agents.lst).

How to do:

- How to add new agent to the list
- How to edit network connection parameters for an agent
- How to obtain information about agent(s)
- How to reload/terminate agent(s)
- How to upgrade agent(s)
- How to change agents settings (Passive RMA)
- How to change agents settings (Active RMA)

How to add new agent to the list

To add a record for a (new) agent you should choose appropriate list: Passive RMA list or Active RMA list. Then you may click on "New agent" button or press Insert key in the list of agents or select "New" item from "Agent(s)" menu. When the dialog "Agent Connection Parameters" appears set the following parameters for the agent:

Passive RMA

Passive RMA is small application that accepts requests from HostMonitor, performs test (or action) and provides information about test result back to HostMonitor.

- Agent address:
  provide the host name or an IP address of the system where RMA is installed
- Item name:
  name of the agent (this name will be displayed in agent's list, and will be used by HostMonitor for agent identification). By default RMA Manager uses agent's addresses as names but you may specify any other name that you like
- Port:
  TCP port that will be used for communication between RMA Manager (or HostMonitor) and the agent. Here you should specify the same port that you have already specified when that agent was installed and configured on a remote system (by default agent uses port #1055)
- Timeout:
  communication timeout in seconds. A maximum amount of time that RMA Manager or HostMonitor will wait for an answer from the agent. Please note: this timeout should be big enough to allow an agent to perform a test before sending an answer to HostMonitor. When, for example, you are launching an external test and an external program needs 15 seconds to perform this test then the timeout should be set to 15 seconds plus an amount of time that is necessary for data exchange between HostMonitor and an agent.
- Password:
  here you should provide the same password that you have specified when an agent was installed and configured on a remote system.

After you have finished entering the above information click "Test/Get info" button to check the settings of an agent or click "Ok" button to check the settings and close dialog. RMA Manager will try to establish connection with an agent and get information about agent: platform, version, comment, etc. Also RMA returns information regarding system where it is running on: hostname, Windows version, Service Pack, etc.
If connection with an agent was established, RMA Manager updates all agent information and sets status of the agent to "operable". If RMA Manager was not able to get proper information from an agent, it sets its` status to "no answer" (if no answer from agent received) or "bad answer" (if some error code was received from an agent, e.g. wrong password).

Active RMA

Active RMA – Remote Monitoring Agent that is not waiting for TCP connection from HostMonitor like Passive RMA. Active RMA itself establishes connection with HostMonitor and RMA Manager. This allows you to install RMA inside private network protected by firewall without necessity to open any TCP port

(Passive RMA requires 1 open TCP port). Also Active RMA allows you to monitor system that does not have fixed IP address, e.g. system that is connecting to the network using temporary dial-up connection.

There are just 2 obligatory parameters

- Name
  unique name of the agent. You should not assign the same name for several agents. If you do so, HostMonitor will accept connection from 1st started agent and reject connection from other agents with the same name
- Password
  minimum six character length password. An empty password using is not permitted.

The password is required for every communication session between RMA and HostMonitor or RMA and RMA Manager. All traffic between RMA and HostMonitor or RMA and RMA Manager is encrypted and the password itself is never transmitted through the network without encryption.
Note: you should use exactly the same name and password that were used when you setup Active RMA on remote system using rma_cfg utility.

Note #1 (RMA Manager): The manager cannot connect to Active RMA due to nature of the agent. If "Accept Active RMA on TCP port #5057" option is enabled, RMA Manager waits for incoming connection from the agent. This option located beside Active RMA list; you may easily change TCP port utilized by the manager but you should remember that RMA should be reconfigured as well.

Note #2 (Active RMA): If "Allow remote management" option is enabled, RMA tries to connect to RMA Manager every 30 sec. If appropriate RMA Manager's record for the agent is not created yet, RMA Manager will reject such connections; once connection is established it will be kept until you close it forcedly. If "Allow remote management" option is disabled, RMA will not work with RMA Manager at all.
See also: additional comments

If connection with an Active RMA was established, RMA Manager updates agent information and sets status of the agent to "connected". If RMA Manager was not able to get any information from an agent, it sets its' status to "no answer". If TCP connection request was received but some error occurred (e.g. wrong password), RMA Manager sets "bad answer" status. If communication session was established and then RMA disconnected, the manager sets status to "operable".

Backup agent
Since the version 6.00 HostMonitor allows you to setup primary and backup agents. Using this feature, HostMonitor is able to balance load between agents and use the backup agent when primary one does not respond. Yes, RMA is pretty stable software however system may not respond due to some hardware or network error.
When you have installed second agent you may choose the following "Load balancing" options:

- **Backup only**
  In this case, HostMonitor will request the main agent to perform the tests and will switch to backup agent only in the case of the primary agent not responding.
- **50/50**
  With this option selected, HostMonitor will balance requests for service between the agents. Even if you specify a single primary agent for all your tests, some tests will be performed by

primary agent and other by backup RMA. If the primary or the backup agent does not respond, tests will be performed by another (paired) RMA.

- **Redundant check**
  This option available for Passive RMA only. When “Redundant check” mode is selected for 2nd (backup) agent, HostMonitor uses specified agent as “backup” agent as well (this means HostMonitor sends request to backup RMA when cannot establish connection with primary agent). Also HostMonitor sends request to 2nd RMA every time primary RMA returns “bad” test result (e.g. “No answer”, “Unknown host”, “Bad”). This means test can be performed from 2 different locations and “Bad” status will be used when both checks performed by both agents fail. Yes, you can use “master-dependant” test relations for such checks and for other much more complicated schemes. However this option allows you to simplify setup, you need just 1 test item instead of 2 items.
  The following table illustrates how HostMonitor performs test using 2 agents in “Redundant check” mode:

1st RMA result	2nd RMA result	Test status
“Good” status	Not used	“Good” status
“Unknown” status	“Good” status	“Good” status
“Unknown” status	“Unknown” status	“Unknown” status
“Unknown” status	“Bad” status	“Bad” status
“Bad” status	“Bad” status	“Bad” status
“Bad” status	“Unknown” status	“Bad” status
“Bad” status	“Good” status	“Good” status

Note 1: "Primary agent" - the agent that is specified for the test execution. As you may specify different agents for different test items, the same agent can be a "primary" and "backup", depending on the situation. For example, you may use AgentA to perform set of WMI tests and use AgentB to perform SNMP tests. In case of an emergency AgentB may execute WMI tests as well (AgentB is backup agent for AgentA). AgentA may perform SNMP tests in the case of AgentB failing (AgentA is backup agent for AgentB).

Note 2: Options located on Misc page in the Options dialog (HostMonitor application) specify the behaviour of the tests when primary agent does not respond to be specified. "If backup agent is specified and connection to primary RMA failed" parameter allows you to choose one of the two options:

- Set "Unknown" status, log the error, then repeat test using backup agent
- Request backup agent without reporting error

How to edit connection parameters for the agent

To change connection parameters for an agent, select it from the list and press Enter (or choose "Edit connection parameters" item in "Agents" menu). An "Agent Connection Parameters" dialog will pop up, there you may setup connection parameters (agent address, port, timeout, password, etc) like it was already described in previous abstract ("How to add new agent to the list").

How to obtain information about agent(s)

When you create a new agent record in the list, RMA Manager tries to connect to a specified agent and gets information from it. However you can refresh/reload this information at any time. Just select a set of agents (or select just one record), and choose "Refresh info" item from the menu "Agent(s)" or press CTRL + I.
RMA Manager will then try to connect to each agent being selected and gets the following information:

- Agent: an internal name of an agent;
- Platform: OS platform that this agent is designed for;
- Version: the version number of the agent;
- Developer: the company that created RMA software;
- Comment: the content of a comment field that you or system administrator had provided when a remote agent was installed and configured.
- Host: information regarding system where the agent is running on: hostname, Windows version, Service Pack, etc.

If a connection with agent was established, RMA Manager updates all information and sets the status of an agent to "operable". If RMA Manager was not able to get information from an agent, it sets the status to "no answer" (if no answer from an agent was received) or "bad answer" (if some error code was received from an agent, e.g. wrong password).
Active RMA notes:

- "Connected" status is used for Active RMA only. It inticates that agent is connected to RMA Manager.
- See also: Note #1 and Note #2.

How to reload/terminate agent(s)

You may reload or terminate an agent on a remote system. It is obvious, that to be able to perform either of these operations an agent should be running and an option "Enable remote management from address" should be enabled. An IP address specified in "Enable remote management from address" of that agent should match the address of the system where you are currently working with RMA Manager.
To reload/terminate agent(s), select a group of agents (or just one agent) in the list and click "Reload agent"/"Terminate agent" button on the tool bar (or use similar item from the menu "Agents").

How to upgrade agent

First: to upgrade an agent you need at least to have a newer version of agents` software. Second: an agent of older version should be already running on the remote system. Third (a): If you want to update passive agent, "Enable remote updates from address" parameter of the agent configuration must be enabled and an IP address specified by this option should point to the machine where you are currently working with RMA Manager. Of course all operations with agent(s) are encrypted and password protected but this option provides additional security (an extra security is never superfluous :-) Third (b): If you want to update Active RMA, "Allow remote management"

parameter of the agent configuration must be enabled and agent should be connected to the manager (this process may take some time, see Note #2).

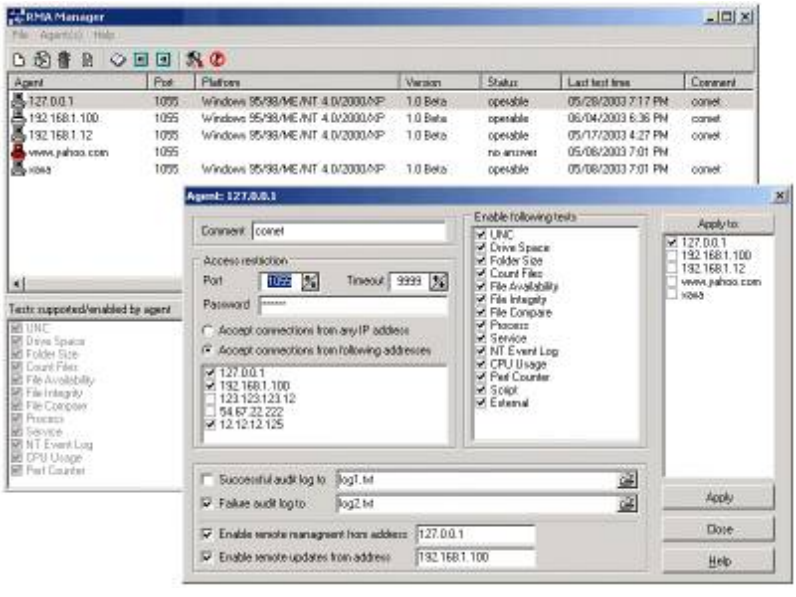
So, to upgrade agent(s), select a group of agent items in the list and click "Upgrade agent" button on the tool bar (or use similar item from menu "Agents"). The dialog will prompt you to select the file with newer version of agents` software code. After this RMA Manager will send this file to all selected agents. Agents then will write that file to the hard drives of their remote systems and restart themselves. After the completion of this operation an agent with a new code will run on each of the remote systems.
Note: agents have been compiled into standalone executable modules: **rma.exe** (passive agent) and **rma_active.exe** (active agent)

Similarly you may upgrade the configuration utility (rma_cfg.exe) on the set of remote systems*. The only difference is in using the menu item “Upgrade configuration utility” instead of “Upgrade agent” and selecting new version of “rma_cfg” utility for upgrade.

How to change agents' settings (Passive RMA)

You may change settings of many agents at one time. Obviously those agents should be running. An agents` setting "Enable remote management from an address" should be enabled and an IP address specified there should point to the machine where you are currently working with RMA Manager. This is an additional measure that together with password protection and encryption of all communications between RMA Manager and an agent provides extra security.

To view/modify agent(s) configuration, select group of agents in the list and click "Agent configuration" button on the tool bar (or use similar item from menu "Agents"). RMA Manager will then connect to a first agent from the group and after getting its` configuration settings will display them in the dialog window. The following individual settings and groups of settings are available:



Comment:
here you may specify a comment (actually you may type any text here, it could be a simple recognizable name or an identifier for this agent). This helps to identify agents easier.

Connection parameters

- **Port**
  specifies the TCP port number which RMA utilizes to listen for incoming connections. Default setting is #1055.

- **Timeout**
  the maximum amount of time (in seconds) that agent will keep waiting for the complete request packet from HostMonitor (after initial TCP connection established) before dropping the connection.

- **Password**
  minimum six character length password. Using of an empty password is not permitted. The password is required for every communication session between RMA and HostMonitor or RMA and RMA Manager. All traffic between RMA and HostMonitor or RMA and RMA Manager is encrypted and the password itself is never transmitted through the network without encryption.

Security settings

- **Accept connections from any IP address**
  enabling this option will allow RMA to accept control commands from any IP address (as long as the incoming connection provides correct password)

- **Accept connections from following addresses**
  specifies the list of IP addresses. After enabling this option RMA will accept remote connections only from the addresses in this list (password is required as always). Usually you have to add just one address to this list, namely the one for the system where HostMonitor is running.
  To add an address to the list press Insert key, to remove an address from the list press Ctrl+Del, to edit item press Enter or double-click it.

- **Enable remote management from address**
  this option sets the IP address from which it is allowed to control and manage RMA. Using RMA Manager installed on the system with that IP address you will be able to change agent's settings remotely, also you will be able to restart and terminate an agent.

- **Enable remote updates from address**
  this option allows remote updates of the RMA code (e.g. when a new version is available) from the IP address being provided. To upgrade an array of remote agents you may use RMA Manager. Of course all operations with agents are encrypted and password protected but this option increases security even more.

- **Enable following tests**
  specifies the list of tests methods allowed for execution by this RMA. To enable a test mark the corresponding check box, to disable a test unmark the box near it.

- **Enable following actions**
  specifies the list of actions allowed for execution by the agent. To enable an action mark the corresponding check box, to disable an action unmark the box near it.

Logging

Successful audit log to
here you may specify a log file where agent will store information about successfully accepted connections. This log has no use when everything works well (it then just takes space on the hard drive), but you may found it really helpful when a sophisticated network problem has to be fixed. If you specify just the name of the file (without a full path), an agent will store a log in the same directory where it was started from.

Failure audit log to
you may specify another log file where an agent will store information about rejected requests. E.g.: connections from an IP addresses that are not allowed or connections with invalid password, etc. Log file is a simple text file that contains date of the event, remote IP address from which an attempt of connection has occurred and information about the error. If you specify just the file name (without path), an agent will store it in the directory where it was started from.

Alerts

If Passive RMA agent does not receive any TCP connections from HostMonitor and RMA Manager, then agents can execute the specified commands. There are settings related to such actions:

Execute 1st command if there is no connection from HostMonitor for N minutes
Ping the following host and execute different commands depending on the results
<Host> | <Timeout> | <Retries>
Exec command if accessible <command line>
Otherwise execute command <command line>

Execute 2nd command if there is no connection from HostMonitor for N minutes
Ping the following host and execute different commands depending on the results
<Host> | <Timeout> | <Retries>
Exec command if accessible <command line>
Otherwise execute command <command line>

Execute command if connection was restored after "bad" alert command was triggered
<command line>

For example, you can setup an RMA agent to start a dial-up program when agent does not receive connection requests from HostMonitor and RMA Manager for 15 minutes and ping to your web site fails.

Please note: Active RMA agents always trying to connect to HostMonitor as soon as possible. While HostMonitor connects to Passive RMA only when it needs to perform some test. If only a few tests with long intervals are set for some passive RMA agents, then the lack of connection requests from HostMonitor may be perfectly normal. For example, if there are only a few tests that the Passive RMA agent needs to perform once an hour, then HostMonitor will only connect to that agent once an hour and then disconnect.

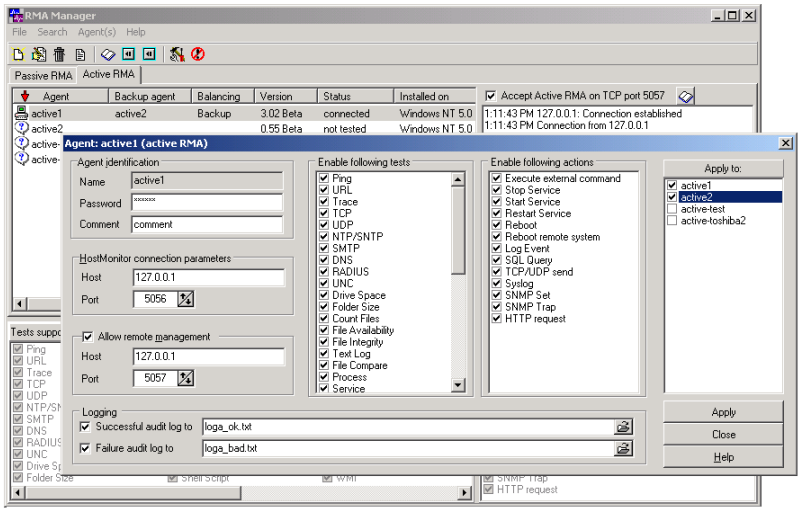
After you have made changes to the settings above, you may refine the list of agents that will accept these settings (an "Apply to" list). By default this list contains all those agents that were selected before you have pressed the "Agent configuration" button. You may remove or add new agents from/to the list.
After you click "Apply" button the new settings will be sent to the agents. You may click "Cancel" button if you have changed your mind.

How to change agents' settings (Active RMA)

You may change settings of many agents at one time. Obviously those agents should be running, "Allow remote management" parameter of the agent configuration must be enabled and agent should be connected to the manager (this process may take some time, see Note #2).

To view/modify agent(s) configuration, select group of agents in the list and click "Agent configuration" button on the tool bar (or use similar item from menu "Agents"). RMA Manager will then request first agent from the group and after getting its` configuration settings will display them in the dialog window. The following individual settings and groups of settings are available:

Agent identification



- Name
  Unique name that identifies an agent. You should not assign the same name for several agents. If you do so, HostMonitor will accept connection from 1st started agent and reject connection from other agents with the same name
- Password
  Minimum six-character length password. An empty password using is not permitted. Several RMA agents may use the same password. The password is required for every communication session between RMA and HostMonitor or RMA and RMA Manager. All traffic between RMA and HostMonitor or RMA and RMA Manager is encrypted and the password itself is never transmitted through the network without encryption.
- Comment:
  here you may specify a comment (actually you may type any text here, it could be a simple recognizable name or an identifier for this agent). This helps to identify agents easier. HostMonitor and RMA Manager will display the content of these fields when they work with remote agents.

Note: when you setup agent record using HostMonitor or RMA Manager GUI, you should use exactly the same name and password that were used when you setup Active RMA on remote system using rma_cfg utility

HostMonitor connection parameters

- Host
- Port

These parameters specify where HostMonitor is running and what TCP port should be used for connection

Allow remote management

- Host

- Port

If you enable remote management, you should specify IP address or hostname of the system where RMA Manager is running. RMA Manager and HostMonitor can be started on the same system and we recommend to do this. In this case you should use different TCP ports for connection. Default settings: HostMonitor listens for incoming connections from RMA on TCP port 5056, while RMA Manager utilizes port 5057.
Note1: It is not necessary to have RMA Manager running all the time. If RMA cannot connect to RMA Manager it will try to establish communication every 30 sec.
Note2: If you start RMA Manager on the same system where HostMonitor is running, HostMonitor tells all connected RMA to establish connection with RMA Manager immediately (if "Full management" option is enabled for the agent).

Enable the following tests

Here you may specify the list of tests methods allowed for execution by this RMA. To enable a test mark the corresponding check box, to disable a test unmark the box near it.

Enable the following actions

Here you may define the list of actions allowed for execution by the agent. To enable an action mark the corresponding check box, to disable an action unmark the box near it.

Logging

Successful audit log to

Here you may specify a log file where agent will store information about successfully accepted connections. This log has no use when everything works well (it then just takes space on the hard drive), but you may found it really helpful when a sophisticated network problem has to be fixed. If you specify just the name of the file (without a full path), an agent will store a log in the same directory where it was started from.

Failure audit log to

You may specify another log file where an agent will store information about rejected requests. E.g.: connections from an IP addresses that are not allowed or connections with invalid password, etc. Log file is a simple text file that contains date of the event, remote IP address from which an attempt of connection has occurred and information about the error. If you specify just the file name (without path), an agent will store it in the directory where it was started from.

Also HostMonitor's system log should be useful when you face some connection problems.

Alerts

If for some reason Active RMA cannot connect to HostMonitor and RMA Manager, then the agent can execute the specified commands. There are settings related to such actions:

Execute 1st command if there is no connection to/from HostMonitor for N minutes
Ping the following host and execute different commands depending on the results (*)
<Host> | <Timeout> | <Retries>
Exec command if accessible <command line>
Otherwise execute command <command line>

Execute 2nd command if there is no connection to/from HostMonitor for N minutes
Ping the following host and execute different commands depending on the results (*)
<Host> | <Timeout> | <Retries>
Exec command if accessible <command line>
Otherwise execute command <command line>

Execute command if connection was restored after "bad" alert command was triggered
<command line>

* Linux note: in order to send and receive ICMP packets Linux applications require CAP_NET_RAW capability. Setcap allows to set capabilities, so you don't need to start RMA agent under root account.
sudo setcap cap_net_raw+ep rma_active
sudo setcap cap_net_raw+ep rma_active_x

For example, you can setup an Active RMA agent to start a dial-up program when the agent cannot connect to HostMonitor and RMA Manager for 5 minutes and ping to your web site fails.

Please note: Active RMA agents always trying to connect to HostMonitor as soon as possible. While HostMonitor connects to Passive RMA only when it needs to perform some test. If only a few tests with long intervals are set for some passive RMA agents, then the lack of connection requests from HostMonitor may be perfectly normal. For example, if there are only a few tests that the Passive RMA agent needs to perform once an hour, then HostMonitor will only connect to that agent once an hour and then disconnect.

After you have made changes to the settings above, you may refine the list of agents that will accept these settings (an "Apply to" list). By default this list contains all those agents that were selected before you have pressed the "Agent configuration" button. You may remove or add new agents from/to the list.
After you click "Apply" button the new settings will be sent to the agents. You may click "Cancel" button if you have changed your mind.

Additional comments:

Note: We recommend you to start RMA Manager on the same system where HostMonitor is running. In this case RMA Manager sends message to HostMonitor that, in turn, tells all connected RMA to establish connection with RMA Manager (if "Full management" option is enabled for the agent). Otherwise RMA will connect to RMA Manager within 30 sec time frame.
Also, if you start RMA Manager on system where Advanced Host Monitor package is not installed, you will need to synchronize agents.lst files manually (copy modified file into the folder where HostMonitor is installed).

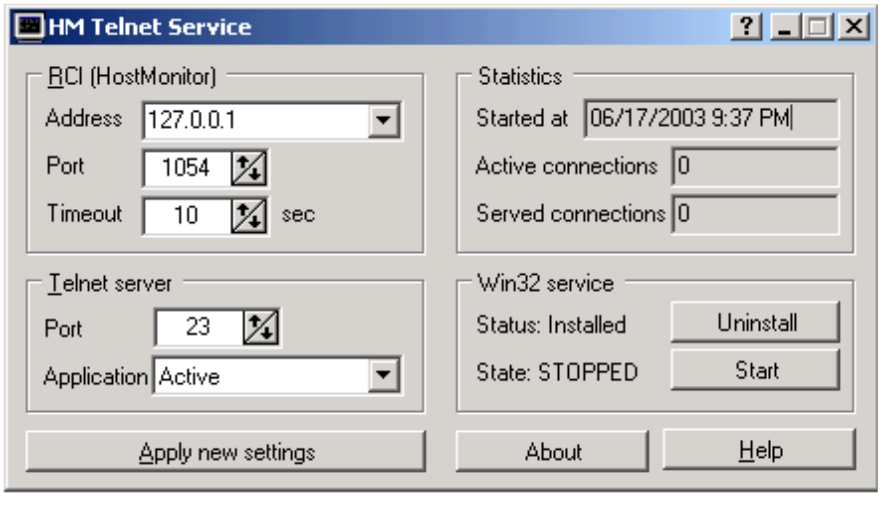
Export/Import:

The list of agents may be exported into CSV file (menu "File" -> "Export..."). After some modifications that file may be then imported back again into RMA Manager (menu "File" -> "Import...").

Import Passive RMA list from CSV (comma-separated value) file.
The file should begin with header line
Address,Name,Port,Timeout,Password,BackupAgent,BalanceMode
the following lines contain information about the agents (1 agent per line).
E.g.
Address,Name,Port,Timeout,Password,BackupAgent,BalanceMode
292.168.1.101,"RMA in UK office",1055,12000,"pppp"
292.168.1.101,"RMA in UK backup",1055,12000,"pppp","RMA in UK office"50/50
252.188.1.102,"RMA in USA office",1055,12000,"www"

Import Active RMA list from CSV (comma-separated value) file.
The file should begin with header line
Name,Password,Timeout,KeepConnection,BackupAgent,BalanceMode
the following lines contain information about the agents (1 agent per line). Note: Timeout and KeepConnection parameters are not used in current version however we recommend you to set these fields to "10000" and "yes" accordingly.
E.g.
Name,Password,Timeout,KeepConnection,BackupAgent,BalanceMode
"active1-mainftp","pswdpswd",10000,yes,"active2-backup",Backup
"active2-backup","pswdpswd",10000,yes

Telnet Service



This application works like Telnet server and allows you to control HostMonitor remotely using any telnet client. Telnet Service allows you to check brief or detailed status of any test and folder. Also you can disable and enable tests, reset statistics, force tests to execution and even change some parameters of the tests. HM Telnet Service allows you to start or stop monitoring process, enable or disable alerts, change global macro variables, etc.

Features:

- All data transmission between HostMonitor and Telnet Service is encrypted and password protected;
- HostMonitor & Telnet Service allow you to setup different user accounts with different sets of permissions;
- Application can be installed on the HostMonitor's system or can be located on any another system that is accessible by TCP/IP protocol;
- Telnet Service can be started as a regular application or as a Win32 service.

Settings

RCI (Remote Control Interface) settings

- **Address**: here you should provide an address of the system where HostMonitor is installed (keep the default '127.0.0.1' if HostMonitor and Telnet Service are installed on the same system)
- **Port**: please provide TCP port that is used by HostMonitor's Remote Control Interface (1054 by default)
- **Timeout**: the maximum amount of time (in seconds) that Telnet Service will keep waiting for the reply from HostMonitor before returning an error response to the client.

Telnet server settings

- **Port**: TCP port which Telnet Service utilizes to listen for incoming connections from the telnet client (default TCP port for telnet protocol is 23. You may need to change it in case you already have a regular telnet server running on the same system).

- **Application** status: set "Active" to activate Telnet service (it will then start listening for incoming connections and will respond to requests from any telnet client). If you start the software as a Win32 service then telnet server will be activated regardless of this option at the system startup.

Win32 service mode:
This group of controls allows you to check the status of the Windows service, install/uninstall, start or stop the service:
- **Install / Uninstall**: this button allows you to install/uninstall software as a Win32 service
- **Start / Stop**: this button allows you to start/stop the service

How to do (Quick start)

To allow remote management of HostMonitor via telnet client follow these simple steps:
- start HostMonitor
- configure HostMonitor's Remote Control Interface on RCI page in the Options dialog
- setup user accounts: use HostMonitor's menu "User"->"Operators"
- start the Telnet Service. You can start it on the same system where HostMonitor is running or on any system that has TCP/IP connection with HostMonitor's system. E.g. HostMonitor can be installed on the server inside of a corporate network but Telnet Service can be running on your home computer.
- configure Telnet Service: provide an address of the HostMonitor's system and TCP port that you had specified for RCI

That's it. Now you can start telnet client (e.g. standard client included in Windows) and connect to HostMonitor using an address of the system where Telnet Service is running (e.g. 209.173.80.15 or www.mycompany.com).
If you are running regular telnet server and our Telnet Service is installed on the same system, change the TCP port of our Telnet Service from 23 (default) to any other. In this case you will need to specify this port number for telnet client as well.

Commands

When you start telnet client and establish a connection with Telnet Service, you will be asked for your user name and password. You will then get the rights and permissions that are specified in your user account. E.g. "Admin" can perform any operations, "Guest" can only view test statuses, etc.

After logging in you may type commands that Telnet Service will execute. You will then see responses from HostMonitor.
Here are some common rules for the commands:
- commands are not case sensitive (e.g. "stop monitoring" and "STOP Monitoring" mean the same);
- parameters of the commands (e.g. <test name> or <group name>) are indeed case sensitive;
- parameters shown in [..] are optional, you may use them or not;

- symbol '|' means either one or another (e.g. <test name> | <group name> means that you may provide the name of the test or the name of the special group);
- if some parameter (e.g. <test name>) includes spaces, conclude parameter into double or single quotation marks (e.g. TestInfo 'Main Router').

List of available commands:

Command	Parameter(s)	Description
- management commands:		
Getstatus		Retrieves information about HostMonitor (version, status of the application, parameters).
Start monitoring		Starts monitoring. Accomplishes the same action as clicking the Start button on the Main window of HostMonitor.
Stop monitoring		Stops monitoring. HostMonitor will still remain running as an application (or as Win32 service) but will not perform any tests.
Enable alerts		Enables alert actions of HostMonitor.
Disable alerts		Disables alert actions of HostMonitor.
PauseMonitoring	<interval>	Pauses monitoring for specified time (time should be specified in minutes).
PauseAlerts	<interval>	Pause alerts for interval specified in minutes. In other words, all action profiles that usually were triggered by the change of test(s) status will not be executed within N minutes. All scheduled actions (those that are executed by built-in Scheduler) will continue to execute anyway.
ExecuteScript	<pathtoscript>	Executes specified HM Script. Example: ExecuteScript "C:\HostMon\pause3backuptests.hms"
ImportFromFile	<filename> [SkipDuplicates] [WriteLog]	Imports test items from special Text file. SkipDuplicates - optional parameter, HostMonitor will skip item when test item with the same name already present in the TestList. WriteLog - optional parameter, HostMonitor will record to the system log file information about all errors and warnings during the import process.
SaveTestList		Saves the current test settings using current file name.
Reload app		Reloads HostMonitor (as a service if it was started in Win32 service mode or as an application if it was started as a regular application).
Reload cfg		Forces the HostMonitor to re-read its` settings from INI file (hostmon.ini by default).
Terminate		Terminates HostMonitor.
- folder/test lists:		

CD | ChangeFolder	<folder name>|<path>	Sets the current folder. All commands listed in this and next sections affect tests only from the current folder. You may specify the name of the folder without the full path if it is a subfolder of the current folder. You may specify the full path to the folder which you want to make current. You may use "**..**" instead of a folder name when you want to step up one level. This command actually uses similar syntax as MS-DOS or UNIX command interpreter. Examples: CD "Main office" CD Root\USA\Office CD **..** ChangeFolder **..****..**\pingtests\
FL | ShowFolders	[-r]	Displays the list of subfolders within the current folder. The numbers of Good/Bad/Unknown tests are displayed for each folder. If an optional parameter "-r" was provided then all descendant subfolders would be displayed as well.
TL | ShowTests	[-r] [-s:<sort mode>]	Displays the list of all tests (ID, name, status, reply) within the current folder. If an optional parameter "-r" was provided then the tests from all descendant subfolders would be displayed. Another optional parameter "-s:<sort mode>" defines the sorting order. <sort mode> could be one of the following: name, status, testtime, reply, method. Examples: ShowTests TL -r TL -r -s**:**name
TI | TestInfo	<test name>	Displays detailed information about specified test. It tries to find specified test in a current folder, if the test was not found there, HostMonitor continues to check all available folders until it finds the test with the specified name.
TID | TestInfoByID	<testID>	Displays detailed information about specified test item. Similar to TestInfo command but you should provide test item ID instead of test name.
tcmt or GetTestComments	<test name>	Show complete comment specified for test item and comments that were provided when operators acknowledged, disabled, paused test or scheduled test to be paused (different kinds of comments separated by '----' line)
tcmtid or	<testID>	Similar to GetTestComments command but you

GetTestCommentsByID		should provide test item ID instead of test name.
tdid or TestDependentsByID	<testID>	Shows list of IDs of all test items that depend on Master test specified by TestID
- the following commands allow you to create new folders and copy test items; if you are using templates, HostMonitor will modify new test items using destination folder variables.		
CreateFolder	<full path to the folder>	Creates new folder(s). The value of this parameter should specify the full path to the folder that you want to create. E.g. CreateFolder Root\USABranch\Support\part2\ will successively create 3 folders - "USABranch" folder in the "Root" folder, - "Support" folder in "USABranch" subfolder, - "part2" folder in "Support" subfolder. If some (or all) of specified folders already exist, HostMonitor will not create second copy of them.
CopyFolder	<srcname>|<id>|<fullpath> <newname>|<newfullpath> [-r]	Creates new folder using all properties of the source folder (such as Reports list, Variables, Color scheme, etc). Source folder can be specified by its name (if this folder located within current parent folder – folder selected by ChangeFolder command); folder ID or full path to the folder. Target folder can be specified by name or full path. Optional parameter "-r" tells HostMonitor to copy folder with its subfolders. Example: CopyFolder Root\Template Root\SQLServer2 CopyFolder 10 Root\Windows5 -r
SetFolderVariable	<variable_name> <variable_value> [-inheritpartly]	Sets or modifies folder variable for current folder. If currently folder settings set to "inherit all variables from parent folder", this command will set "Use folder variables only" mode. Unless you specify optional -inheritpartly parameter; in such case HostMonitor will set "Use inherited variables; folder variables may override inherited variables" option. Note: if you are using folder-level variables as parameters of some test items, this command will modify test settings automatically. Example: SetFolderVariable fvar_host "10.10.5.1"

CopyTestByName	<testname>|<groupname> <destfullpath>|<folderid>	Copies specific test or group of tests (e.g. all Ping tests) into specified folder. Destination folder can be specified by full path or folder ID. Example: CopyTestsByName _AllPing Root\Server2 CopyTestsByName "router 2" Root\Newsetup CopyTestsByName _AllGood 105
CopyTestByID	<testid> <destfullpath>|<folderid>	Copies single test specified by ID into target folder specified by full path or folder ID.
CopyAllTests	<destfullpath>|<folderid> [-skipduplicates] [-adjustmasters] [-r]	Copies all test items from current folder (and optionally subfolders) into target folder. "adjustmasters" option: if dependent tests copied with master(s) then HostMonitor adjust master-dependent relations for newly created tests. E.g. if you copy 6 tests (5 Cisco tests that depends on 1 Ping test) then new Cisco tests will depend on new Ping test (if you are using folder-related variables for target IP address, then new tests will start to monitor new device without any manual adjustments).
- test manipulation (1) note: the following commands work with test items within Current Folder (initially when session just started the root folder is current)		
DisableTest	<test name> | <group> [-r]	Disables specified test or group of tests. If an optional parameter "-r" is provided then this operation will be applied to the current folder and all descendant subfolders within it.
EnableTest	<test name> | <group> [-r]	Enables specified test or group of tests. If an optional parameter "-r" is provided then this operation will be applied to current folder and all descendant subfolders.
RefreshTest	<test name> | <group> [-r]	Forces specified test or group of tests to execution. If an optional parameter "-r" is specified then operation will be applied to current folder and all descendant subfolders.
ResetTest	<test name> | <group> [-r]	Resets statistics for specified test or group of tests. If an optional parameter "-r" is specified then operation will be applied to current folder and all its` subfolders.
PauseTest	<test name> | <group> <interval>	Pauses specified test or group of tests (time interval should be specified in minutes).

<table>
<tr><td></td><td>[<comment>]
[-r]</td><td>If an optional parameter "-r" is specified then operation will be applied to current folder and all its` subfolders.
Examples:
PauseTest "www.nasa.gov" 5 "paused for 5 min"
PauseTest _AllBad 3 -r</td></tr>
<tr><td>ResumeTest</td><td><test name> | <group>
[-r]</td><td>Resumes paused test or group of tests. If an optional parameter "-r" is specified then operation will be applied to current folder and all its` subfolders.</td></tr>
<tr><td>DisableAll</td><td>[-r]</td><td>Disables all tests within the current folder. If an optional parameter "-r" is specified then all tests within the current folder including all subfolders will be disabled.</td></tr>
<tr><td>EnableAll</td><td>[-r]</td><td>Enables all tests within the current folder. If an optional parameter "-r" is provided then all tests within the current folder and all its` subfolders will be enabled.</td></tr>
<tr><td>RefreshAll</td><td>[-r]</td><td>Forces all tests within the current folder to execution. If an optional parameter "-r" is specified then the command affects subfolders as well.</td></tr>
<tr><td>ResetAll</td><td>[-r]</td><td>Resets statistics for all tests within current folder. If an optional parameter "-r" is specified then the subfolders are included as well.</td></tr>
<tr><td>SetTestParam</td><td><test name> | <group>
<ParamName>
<new value>
[-r]</td><td>Sets a value of a given parameter for the specified test or group of tests. <ParamName> could be one of the following:
timeout <number> changes communication timeout
retries <number> changes number of retries
username <name> changes account used for "Connect as" option
password <pswd> changes password used for "Connect as" option
comment <text> changes entire comment assigned to the item
commentlineNN <text> changes specified line of the comment assigned to the item (NN is number from 1 till 99)
testinterval <min> | <hh:mm:ss> changes execution interval for specified test items. Time interval can be specified in hh:mm:ss format or just as integer number that represents minutes (i.e. 5 is equivalent to 00:05:00, 60 is equivalent to 01:00:00)
AlertProfile <name> changes alert profile
AlertProfile2 <name> changes second alert profile (when this feature enabled)</td></tr>
</table>

		Schedule	<name>	sets schedule assigned to the test
		TestBy	<name>	sets "Test by" parameter; you may provide agent name, hostmonitor or folder-specific string
		sqlquery	<query>	Sets query, for ODBC tests only)
		Threshold	<limit>	sets limits specified for the test (alert threshold). E.g. minimum free space for Drive Free Space test, minimum amount of free memory for Memory test, loss packet ratio limit for Ping test, limit for CPU load, upper limit for Process test, etc Also it sets CRC32 for HTTP test; hash for URL test
		ThresholdUp	<limit>	same as Threshold (e.g. upper limit for Process test, upper limit for UPS input voltage and so on)
		Threshold2	<limit>	sets 2nd limit for some tests, e.g. Jitter limit for Ping test, messages size limit for POP3 test, lower limit for Process test,
		ThresholdDown	<limit>	same as Threshold2 (e.g. lower limit for Process test, lower limit for UPS input voltage or lower limit for UPS battery temperature)
		Note: the following parameters used with ReplaceTestParam command changes test settings regardless of current parameter value:		
		usecommonlog	yes|no	turns on or off common logging
		reversealert	yes|no	turns on or off "reverse alert" option
		unknownasbad	yes|no	sets "Treat Unknown status as Bad" option
		warningasbad	yes|no	sets "Treat Warning status as Bad" option
		syncmastercounters	yes|no	turns on/off "Synchronize counters" property
		syncmasterstatus	yes|no	turns on/off "Synchronize status & alerts" test property
ReplaceTestParam	<test name> | <group> <ParameterName> <current value> <new value>	Replaces a value of a given parameter for the specified test or group of tests. Unlike "SetTestParam" command, this one works selectively. It changes the value of a parameter only		

	[-r]	for the tests that already have a current value of this parameter equal to the <current value> argument of the command. List of parameters equivalent to parameters of SetTestParam command Example: ReplaceTestParam _AllTCP timeout 2000 5000

* Threshold (ThresholdUp) parameter can be used for the following tests:
Ping, TCP, UDP, DNS, NTP, LDAP, POP3, IMAP, URL, HTTP, Certificate Expiration, Domain Expiration, SOAP, OPC, UNC, Drive Free Space (Windows, UNIX, NetApp, QNAP, Synology), Folder/File Size, Folder/File Availability, File Integrity, Compare Files, Count Files, Text Log, CPU, Memory, Process, Dominant Process, Performance Counter, WMI, Registry, Shell Script, External, SSH, ODBC Query, VM host CPU usage, VM host free memory, VM host free datastore space, VM guest CPU usage, VM guest free memory, VM guest free disk space, SNMP Get, SNMP Table, Network Traffic, Interfaces Status, Juniper Temperature, NetApp RAID Status, Synology Temperature, Synology Disk Load, Qnap Temperature, Qnap Fans, UPS Health, UPS Load, UPS Charge Level, UPS Input Voltage, UPS Output Voltage, UPS Temperature, UPS Remaining Time Apache, Nginx, Tomcat, IIS, Printer supply levels

* Threshold2 (ThresholdDown) parameter can be used for the following tests:
POP3, Folder/File Availability, Process, Certificate Expiration, NetApp RAID Status, Qnap Fans, UPS Load, UPS Input Voltage, UPS Output Voltage, UPS Temperature, Apache, Nginx, Tomcat, IIS

* When you setup threshold for Traffic Monitor test using ReplaceTestParam command you should use the same unit as current one. E.g. If you set 8 Kbit/sec limit to the test, then the following command will not change threshold

```
ReplaceTestParam  TrafficTestSample Threshold "1 KB/sec" "2 KB/sec"
```

1 KB == 8Kbit but command will not set new limit because current threshold uses Kbit/sec units.
This command will change threshold

```
ReplaceTestParam TrafficTestSample Threshold "8 Kbit/sec" "2 KB/sec"
```

* When you setup threshold for Big-IP Temperature or Netscaler Temperature tests, HostMonitor will set all enable limits: internal, chassis, CPU, auxiliary temperarure limits.

Examples:

```
SetTestParam      _AllCPU   UserName  test1
SetTestParam      _AllCPU   Password  pswd1
ReplaceTestParam  _AllTCP   timeout   2000   5000

SetTestParam      _AllPing  testinterval  5
SetTestParam      _AllPing  testinterval  00:02:30
ReplaceTestParam  _AllCPU   testinterval  5  00:15:00

SetTestParam      "M. router" AlertProfile  "E-mail to admin"
SetTestParam      _AllMemory  usecommonlog  yes
SetTestParam      _AllMemory  unknownasbad  no
ReplaceTestParam  _AllPing    TestBy  "hostmonitor"  "folder-specific"
ReplaceTestParam  _AllCPU     TestBy  "hostmonitor"  "agent - SouthWest domain"

SetTestParam      "main router"  Threshold     "50 %"
SetTestParam      "main router"  Threshold2    "50 ms"
SetTestParam      _AllMemory     Threshold     "20 %"
SetTestParam      _AllTraffic    Threshold     "55 KB/sec"
SetTestParam      _AllTraffic    Threshold     "33 pkt/min"
SetTestParam      _AllTraffic    Threshold     "22 pkt"
ReplaceTestParam  _AllTraffic    Threshold     "2 GB/sec"  "5 GB/sec"
ReplaceTestParam  _AllUPSTemp    ThresholdUp   65  55
ReplaceTestParam  _AllUPSTemp    ThresholdDown 15  10
ReplaceTestParam  _AllFreeSpace  Threshold     "20 %"  "17 %"
ReplaceTestParam  _AllFreeSpace  Threshold     "5 GB"  "8 GB"
```

ReplaceTestParam _AllFreeSpace Threshold "6 GB" "15 %" SetTestParamByID 11054 Threshold "10 MB"		
ResumeTestByID	<testID1> [<testID2> [...]]	Resumes paused test item(s).
AckTestByID	[StopAlerts] <comment> <testID> [testID2 [testID3 [...]]]	Acknowledges failed test item(s)
SetTestParamByID	<testID> <param> <new value>	Sets a value of a given parameter for the specified test or group of tests. <Param> could be one of the following: - timeout - username - password - sqlquery (for ODBC tests only) - retries - testinterval - comment - commentlineNN (where NN is a number between 1 and 99) Example: SetTestParam 55 timeout 2000
ReplaceTestParamByID	<testID> <param> <current value> <new value>	Replaces a value of a given parameter for the specified test or group of tests. Unlike "SetTestParamByID" command, this one works selectively. It changes the value of a parameter only for the tests that already have a current value of this parameter equal to the <current value> argument of the command. Example: ReplaceTestParam 55 timeout 2000 5000
- global variable commands:		
ShowUserVariables	[<variable>]	Shows the list of global macro variables and their current values. If an optional parameter <variable> is specified then only the value of this variable will be displayed
SetUserVariable	<variable> <value>	Sets the value of a variable (if such variable does not exist, creates a new variable). Note: Variable names are not case sensitive.
SaveUserVariables		Saves changes
LoadUserVariables		Loads previously saved variables
- other:		
Help		Displays list of available commands (and parameters)

Disconnect		Disconnects client from HostMonitor

Most of commands that work with tests allow you to use special group name instead of name of the test. In this case a command will be applied to all tests of specific type (within the current folder).
Available group names:

Group name	Test type (method)
_AllGood	Test items with “Ok”, “Host is alive”’or “Normal” status
_AllBad	Test items with “Bad”, “NoAnswer” or “Bad content” status
_AllUnknown	Test items with “Unknown” or “Unknown host” status
_AllWarning	Test items with “Warning” status
_AllPing	Ping tests
_AllTrace	Trace tests
_AllSIP	SIP tests
_AllRAS	RAS tests
_AllTCP	TCP tests
_AllUDP	UDP tests
_AllDNS	DNS tests
_AllLDAP	LDAP tests
_AllNTP	NTP tests
_AllRadius	Radius tests
_AllDICOM	DICOM tests
_AllDHCP	DHCP test items
_AllTraffic	Traffic Monitor test items
_AllNIS	Network Interfaces Status
_AllSMTP	SMTP tests
_AllPOP3	POP3 tests
_AllIMAP	IMAP tests
_AllEMail	E-Mail test items
_AllMailRelay	Mail Relay test items
_AllApache	Apache tests
_AllNginx	NGINX tests
_AllTomcat	Tomcat tests

_AllIIS	IIS tests
_AllURL	URL tests
_AllHTTP	HTTP tests
_AllSOAP	SOAP tests
_AllOPC	OPC tests
_AllCertificate	Certificate Expiration test items
_AllDomain	Domain Expiration test items
_AllWebDavSpace	WebDAV Free space test items
_AllFolderSize	Folder/File Size tests
_AllFileExists	File/Folder Availability tests
_AllCountFiles	Count Files tests
_AllFileContents	File Integrity tests
_AllFileComp	Compare Files tests
_AllTextLog	Text Log test items
_AllUNC	UNC tests
_AllFreeSpace	Drive Free Space tests
_AllHddSMART	HDD SMART test items
_AllCPU	CPU Usage tests
_AllMemory	Memory tests
_AllService	Service tests
_AllProcess	Process tests
_AllDominantProcess	Dominant Process tests
_AllNTLog	NT Event Log tests
_AllPerfCounter	Performance Counter tests
_AllRegistry	Registry test items
_AllWMI	WMI tests
_AllDHCPPool	DHCP Pool tests
_AllAVStatus	Antivirus Status tests
_AllLastUpdate	Last OS Update tests
_AllFirewallStatus	Firewall Status tests
_AllODBC	ODBC tests
_AllInterbase	Interbase tests
_AllMsSQL	MS SQL tests

_AllMySQL	MySQL tests
_AllOracle	Oracle tests
_AllPostgre	Postgre tests
_AllSybase	Sybase tests
_AllVMHostStatus	VM host status
_AllVMHostCPU	VM host CPU usage
_AllVMHostMemory	VM host free memory
_AllVMHostDisk	VM host datastore space
_AllVMStatus	VM guest status
_AllVMCPU	VM guest CPU usage
_AllVMDisk	VM guest free disk space
_AllVMMemory	VM guest free memory
_AllRMCPPing	RCMP Ping tests
_AllIPMIHealth	IPMI Healths tests
_AllIPMITemp	IPMI Temperature tests
_AllIPMIFans	IPMI Fans tests
_AllIPMIVoltage	IPMI Voltage tests
_AllIPMICurrent	IPMI Current tests
_AllIPMIDiscrete	IPMI tests
_AllHPHealth	HP iLO Health tests
_AllHPTemp	HP iLO Temperature tests
_AllHPFans	HP iLO Fans tests
_AllHPPower	HP iLO Power tests
_AllHPDisks	HP iLO Disks tests
_AllRedfishHealth	Redfish Health tests
_AllRedfishTemp	Redfish Temperature tests
_AllRedfishFans	Redfish Fans tests
_AllRedfishVoltage	Redfish Voltage tests
_AllRedfishCurrent	Redfish Current tests
_AllRedfishPower	Redfish Power tests
_AllRedfishSensor	Redfish Sensor tests

_AllCiscoHealth	Cisco Health tests
_AllCiscoTemp	Cisco Temperature tests
_AllCiscoFans	Cisco Fans tests
_AllCiscoPower	Cisco Power tests
_AllJuniperHealth	Juniper Health tests
_AllJuniperTemp	Juniper Temperature tests
_AllJuniperFans	Juniper Fans tests
_AllBigIPHealth	Big-IP Health tests
_AllBigIPTemp	Big-IP Temperature tests
_AllBigIPStats	Big-IP Statistics tests
_AllNScalerTemp	Citrix Netscaler Temperature tests
_AllNScalerStats	Citrix Netscaler Statistics tests
_AllNetAppHealth	Juniper Health tests
_AllNetAppTemp	Juniper Temperature tests
_AllNetAppDisks	Juniper RAID/Disks tests
_AllQnapHealth	QNAP Health tests
_AllQnapTemp	QNAP Temperature tests
_AllQnapFans	QNAP Fans tests
_AllSynHealth	Synology Health tests
_AllSynTemp	Synology Temperature tests
_AllSynDiskLoad	SynologyDisk Load tests
_AllUPSHealth	UPS Health tests
_AllUPSLoad	UPS Load tests
_AllUPSCharge	UPS Charge level tests
_AllUPSVoltageIn	UPS Voltage In tests
_AllUPSVoltageOut	UPS Voltage Out tests
_AllUPSTemp	UPS Temperature tests
_AllUPSTime	UPS Remaining time tests
_AllPrinterStatus	Printer status

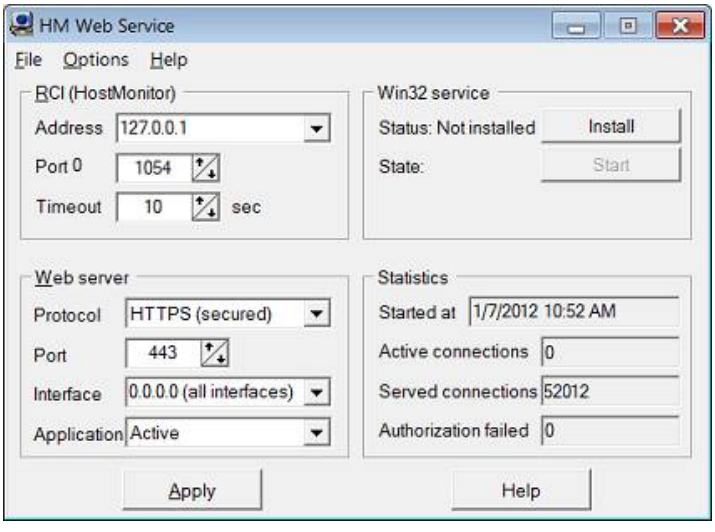
_AllPrinterLevels	Printer supply levels
_AllSNMP	SNMP Get tests
_AllSNMPTable	SNMP Table test items
_AllSNMPTrap	SNMP Trap tests
_AllScript	Active script tests
_AllShell	Shell script tests
_AllExternalPrg	External tests
_AllSSH	SSH tests
_AllTemp	Temperature Monitor tests
_AllHMMonitor	HM Monitor test items

Examples:

```
DisableTest  _AllTCP -r
EnableTest   _AllPing
RefreshTest  _AllURL
RefreshTest  "my router"
EnableAll
AckTestByID StopAlerts “Server scheduled upgrade” 1152 1153 1154
```

Web Service

This application works like an HTTP server and provides web interface for HostMonitor. You can install Web Service on a local or remote system and check (and control) HostMonitor in real time using a web browser on any computer that is connected to the Internet. Web Service allows you to check brief or detailed status of any test and folder. Also you may disable or enable tests, reset statistics and force tests to execution. You will be able to start and stop monitoring, enable and disable alerting, etc.



Features:

- All data transmission between HostMonitor and Web Service is encrypted and password protected;
- HostMonitor & Web Service allow you to setup different user accounts with different sets of permissions;
- Controlling the HostMonitor is not the only function of HM Web Service. It can be used as a simple web server providing access to files on a system where the Web Service is running. You may view HTML reports, logs and settings from anywhere.
- Web service can be started as regular application or as Win32 service.

How to do (Quick start)

To allow remote management of HostMonitor via web browser follow these simple steps:

- start HostMonitor
- configure HostMonitor's Remote Control Interface on RCI page in the Options dialog. **Please note:** when an internet browser acquires the document from the internet it may fetch several parts of the document at once to increase performance. Thus "Maximum simultaneous connections" option of the HostMonitor's RCI interface should be set to 4 (minimum) even if just one user at a time will be connected to HostMonitor. Otherwise the web browser may not be able to display a web page correctly.
- setup user accounts: use HostMonitor's menu "User"→"Operators"
- start the Web Service. You can start it on the same system where HostMonitor is running or on any system that has TCP/IP connection with HostMonitor's system. E.g. HostMonitor can be installed on the server inside of a corporate network but Web Service can be running on your home computer.
- configure Web Service: provide an address of the HostMonitor's system and TCP port that you had specified for RCI
- optionally set authentication methods and install certificates for secure connection

Settings

RCI (Remote Control Interface) settings

- **Address**: here you should provide an address of the system where HostMonitor is installed (keep the default '127.0.0.1' if HostMonitor and Web Service are installed on the same system)
- **Port**: please provide TCP port that is used by HostMonitor's Remote Control Interface (1054 by default)
- **Timeout**: the maximum amount of time (in seconds) that Web Service will keep waiting for the reply from HostMonitor before returning an error response to the browser.

Web server settings

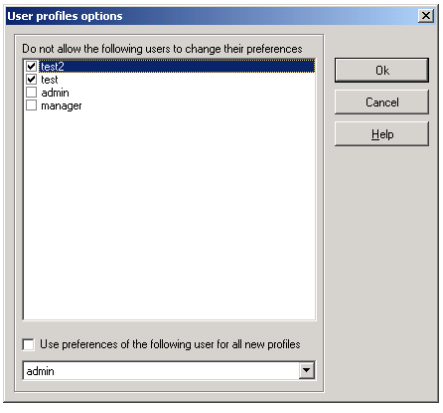
- **Protocol**: You may choose protocol that should be used for communication between Web Service and web browser: HTTP or HTTPS. If you choose secured HTTPS protocol, you should install SSL certificates. For more information please check SSL section of the manual.
- **Port**: TCP port on which Web Service will listen for incoming connections from the web browser (default TCP port for HTTP protocol is 80; default TCP port for HTTPS protocol is 443. You may need to change the port in case you already have another web server running on the same system, e.g. IIS).
- **Interface**: this option allows you to select specific network interface on which Web Service will listen for incoming connections from the clients (web browser). Default value for this parameter "0.0.0.0" - all network interfaces installed on the system.
- **Application** status: set "Active" to activate Web service (it will then start listening for incoming connections and will respond to HTTP requests from any web browser). If you start the software as a Win32 service then web server will be activated regardless of this option at the system startup.

Win32 service mode:

This group of controls allows you to check the status of the Windows service, install/uninstall, start or stop the service:

- **Install / Uninstall**: this button allows you to install/uninstall software as a Win32 service
- **Start / Stop**: this button allows you to start/stop the service

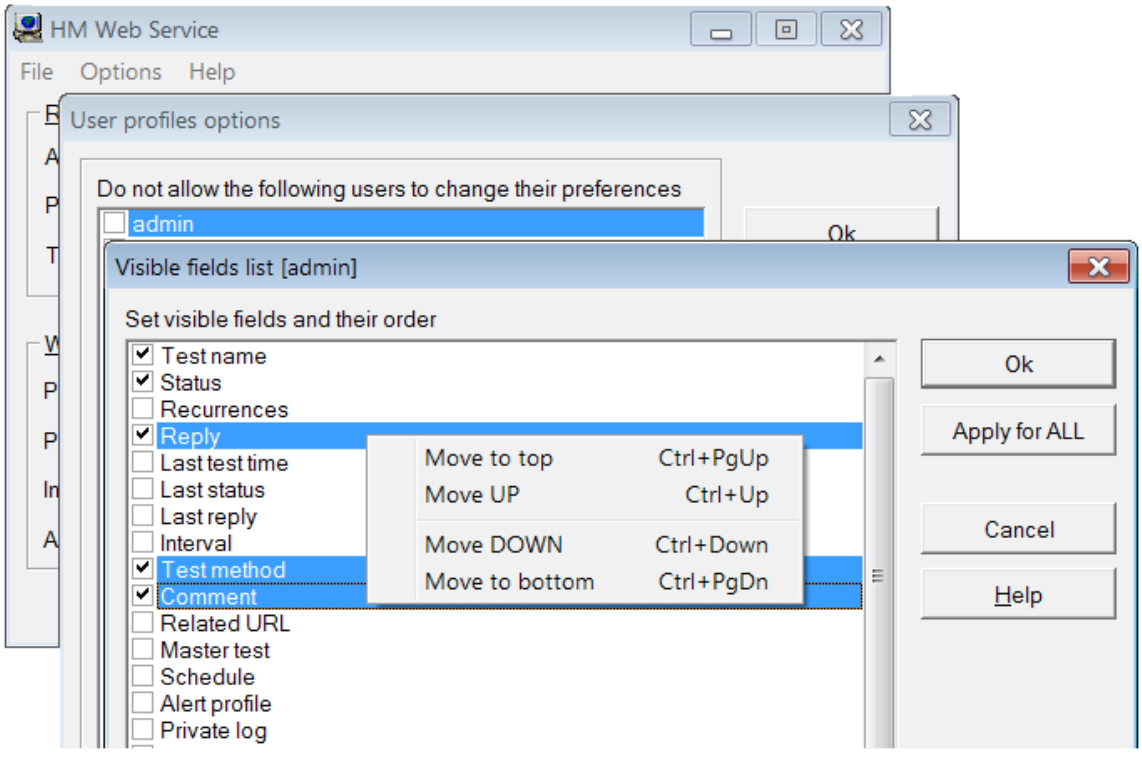
User profiles



User Profiles manager allows you to choose specific user profile as a default profile. Settings from this profile will be used (copied) for each new account. Note: Web Service creates new account on 1st successful login of the user; later profiles for each account can be modified independently. “User Profiles” dialog is available through menu Options -> User profiles.

Also User Profiles manager allows you to set "Do not allow the following users to change their preferences” option for set of user accounts. This option can be useful for “guest” accounts when the same account may be used for several/many persons. If you set this option for the account, operator will not be able to change web interface preferences, such as:
- color palette
- folders tree mode
- folder pane width
- list of visible test properties
- sorting mode
- etc

You may open "Visible fields list" window using menu Options->User Profiles->Set fields. Then reorder list of fields - select one or several items (using Shift and Ctrl) and move selected items using Ctrl+UP/Down, Ctrl+PgUp/PgDn keys.

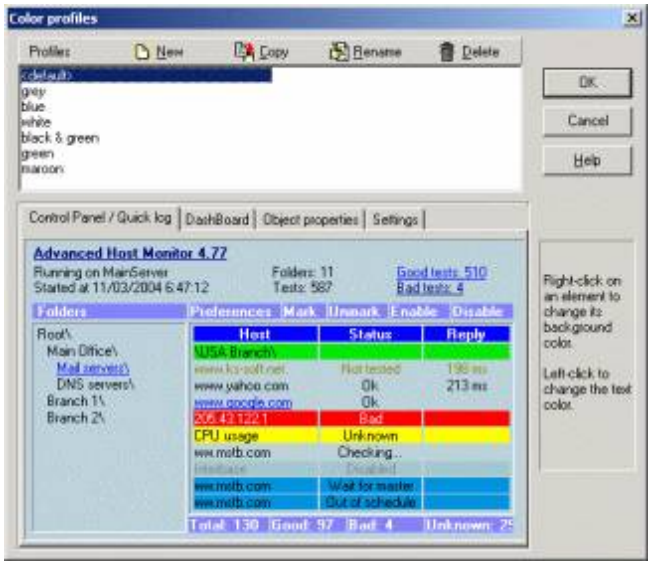


Colors

Each user may select a color palette for web interface according to his/her liking. Only users who have access to the system where Web Service is running may control (create, delete and modify) color profiles. Use menu Options->Color to bring up Color Profiles dialog window.
You can fully customize color schemes for the Control Panel, DashBoard, Quich Log and other panels.

To manipulate with color schemes use 4 buttons:

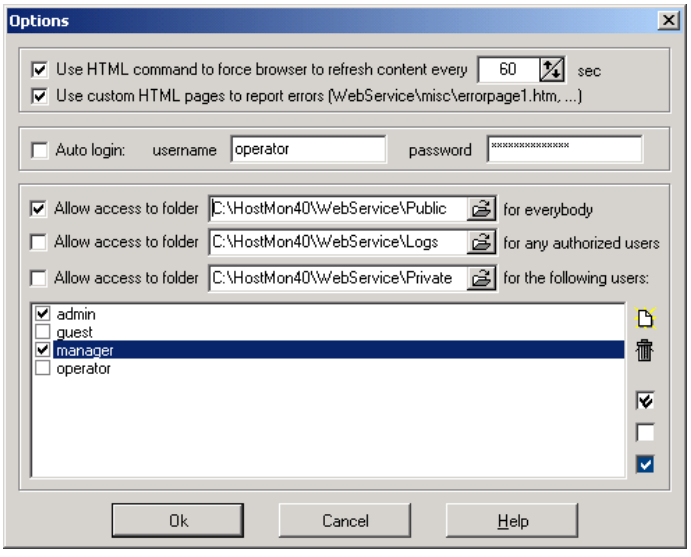
New	Create new palette.
Copy	Copy selected palette. This is useful if you want to make small modifications for the existing color palette.
Rename	Change palette's name.
Delete	Remove selected palette; you can remove all but one (the one named <Default>) color schemes.



In order to modify colors of the selected palette, click on the element which you want to change color for. Use right-click on an element to change its background color, and left-click to change the text color.

Advanced options

Use menu Options->Advanced to access dialog with some optional (non obligatory) settings.



- **Regular Web Interface: force browser to refresh content every NN sec**
- **Compact Web Interface: force browser to refresh content every NN sec**

  Normally the content of a web browser window is refreshed only after the user had pressed the refresh button or after he had performed some operations (e.g. disabled or enabled a test). With these options enabled Web Service will force browser to refresh the content every NN seconds.

- **Use custom HTML pages to report errors**

  This option allows you to use custom configurable HTML pages to report errors. With this option enabled in case of some problems Web Service will search 'misc' subdirectory for the following files:

Errorpage1.htm	this page is used when Web Service cannot retrieve information from HostMonitor. E.g. RCI Interface is disabled or HostMonitor was not started at all.
Errorpage2.htm	this page is used when wrong (invalid) information is requested. For example this error may occur when another user have removed the test that you just want to check (retrieving detailed information about non existent test).
Errorpage3.htm	this page is used to report the error which indicates usage of incompatible HostMonitor and WebService versions.

  Please note: you may (and probably you should) use %WSResponse% variable in your custom HTML error pages. This variable represents actual error message (the response from Web Service).

  Examples of error pages are found in 'misc' subdirectory. Feel free to change them according to your liking.

  If an error page file does not exist, Web Service will use standard predefined error pages.

- **Auto login**

  This option allows you to specify username and password that will be used when browser connects to Web Service. This way user (who had started web browser to connect to HostMonitor) will not be prompted for a name/password at all (unless you provide invalid name or password). We highly recommend to refrain from specifying accounts that have rights to change HostMonitor's settings (e.g. stop monitoring or disable test items).

Controlling the HostMonitor is not the only function of HM Web Service. It can be used as a simple web server providing an access to the files on a system where the Web Service is running. You may view HTML reports, logs and settings from anywhere.
Use the following settings for enabling multilevel access to files and folders of a system where Web Service is running:

- **Allow access to folder <path to folder> for everybody**
  You may enable an access to a specified folder (and all subfolders) for anybody who uses web browser and is connected to Internet/Intranet. Anybody on the Internet/Intranet will be able to access this folder without authorization.
  Regardless of the real name of the shared folder on your computer it will be visible under the name "**public**". For example if Web Service is running on the machine hostmonitor.mycompany.com then to access the shared folder you should use this URL: "http://hostmonitor.mycompany.com/public/" (if the name of the of the target file or folder is not specified then the closing "/" should always be present in url string).

- **Allow access to folder <path to folder> for any authorized user**
  You may enable an access to a specified folder (and all subfolders) for authorized users only. The user account with remote access permissions should be present in HostMonitor. When the user will try to access this folder via internet he will be asked to provide his user name and a password.
  Regardless of the real name of the shared folder in the computer it will be visible under the name "**authorized**". For example if Web Service is running on the machine hostmonitor.mycompany.com then to access the shared folder you should use this URL: "http://hostmonitor.mycompany.com/authorized/" (if the name of the target file or folder is not specified then the closing "/" should always be present in url string).

- **Allow access to folder <path to folder> for the following users**
  You may enable an access to a specified folder (and all subfolders) for specified user(s) only, (e.g. you may allow an access only for "Admin" and "Manager"). The user account with remote access permissions should be present in HostMonitor. When the user will try to access this folder via internet he will be asked to provide his user name and a password.
  Regardless of the real name of the shared folder in the computer it will be visible under the name "**private**". For example if Web Service is running on the machine hostmonitor.mycompany.com then to access the shared folder you should use this URL: "http://hostmonitor.mycompany.com/private/" (if the name of the of the target file or folder is not specified then the closing "/" should always be present in url string).

  If you will allow an access to public or authorized folders where HostMonitor stores private logs (for some tests) then the links to these private logs will be visible and users will be able to check the logs. Note that the "private log" field must be included in the list of displayed fields.

Web Interface

When you start a new instance of the browser and request information from the HostMonitor using URL like http://webservicehostname/, the browser first will ask for your name and password. You will get the rights and permissions that are specified in your user account. E.g. admin can perform any operations, guests can only view test statuses, etc.

Recommended web browsers: Google Chrome 32+, Opera 12+, FireFox 24+, Internet Explorer 11+ (some other browsers can be used as well, e.g. Safari for iOS)

Simplified web interface

If you have to use old web browser (not HTML5 compatible), you may switch to simplified interface (WS1) using URL like http://webservicehostname/**ws1**/index.htm
This way you may use Internet Explorer 5.50+, Opera 8.0+, Firefox 2.0+.

Compact web interface

Also, there is version of the interface designed for mobile devices with small screens.
To access this service use the following links:
http://webservicehostname/**compact.htm**
http://webservicehostname/**tiny.htm**
http://webservicehostname/**links.htm**
You may use compact interface on PC as well, it may look better if you add optional parameter "?mobile=0", e.g.
http://webservicehostname/compact.htm**?mobile=0**
http://webservicehostname/tiny.htm**?mobile=0**
Also you may use "?mobile=1" parameter if your mobile device misrecognized as PC, e.g.
http://webservicehostname/compact.htm**?mobile=1**
http://webservicehostname/links.htm**?mobile=1**

Toolbar

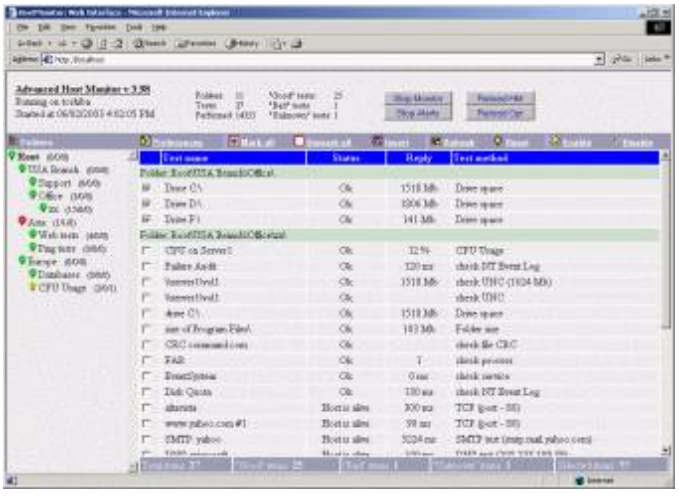
This pane shows brief statistics, also you may start and stop monitoring, disable and enable actions using sliding panel located near "Logout" button

- "Start/Stop Monitor"
  starts or stops monitoring. The caption of the button changes to reflect the current state of the HostMonitor on the remote (local) system
- "Enable/Disable Alerts"
  enables or disables actions. The caption of the button changes to reflect the current state of the Alerts on HostMonitor.

Additional “warning” icons displayed when monitoring is stopped or actions disabled. If you hide toolbar using “Toolbar off” button, warning icons can be moved to any convenient place (use mouse to drag icon).

Toolbar pane allows you to switch between 4 main workplaces: Management panel, DashBoard, Quick Log and Top Hosts.

1) Management panel



Management panel provides the interface which resembles HostMonitor's own GUI. Left part of the pane is a Folder section that displays Folders and Views. The right part - Test section, it shows test items from within the selected folder or view.

Folder section
Here you see the list of all folders and subfolders available in HostMonitor. If you click on the folder name, you will see the list of test items from that folder in test section.

If you are using simplified version of the interface (WS1), Web Service does not change color of each folder item depending on number of bad/warning test items within the folder; instead it shows an indicator to the left of the folder name. When an indicator is green it means all the tests in this folder have "good" status, yellow means that one or more tests have "unknown" status, red is an indication that at least one test has a "bad" status. You may click on indicator to check folder properties or to see corresponding lists displaying good, bad or unknown test items. There are also numbers to the right of the folder name - the number of "good" / "bad"+"warning" / "unknown" tests in the folder.

Test section
It displays the list of all tests from within the selected folder (or view). You may set the Web Service to show you any available property of the test in this list, sort them, filter by the status and perform the following operations with selected set of test items:

- Enable — enables selected test(s)
- Disable — disables selected test(s)
- Refresh — forces test probe for selected item(s) regardless of schedule
- Reset — resets the statistics for the selected test(s)
- Pause — allows you to pause monitoring for selected test item(s) for a specific interval, e.g. next 20 min
- Resume — resumes paused test item(s)
- Ack — use this link to acknowledge test(s) status
- Ack/Stop — acknowledges status and stop alerts
- Test info — opens Test Info window (applicable for single selected item)

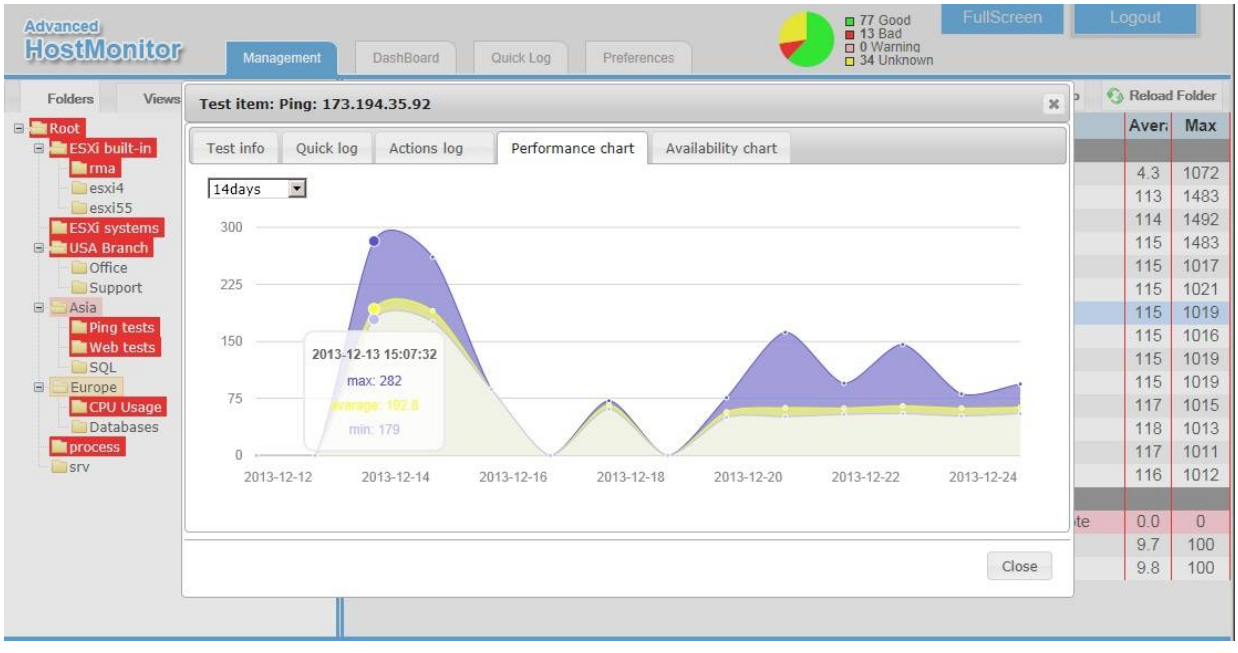
Also you may use popup menu functions: click right mouse button on test item and choose operation - it allows you to Refresh, Pause or Disable test items, Acknowledge "bad" status, open Test Info window, etc. You may use Ctrl+H and Ctrl+L hot keys to check performance history and quick log accordingly.

Note: If you are using simplified version of the interface (WS1), popup menu functions are not available; instead you may click on first field (usually it displays test name). This link will take you to a new window with detailed information about the test.

You may select set of test items using Shift key or Ctrl key and left mouse click (this option is not available if you are using WS1 simplified interface); also you may select the test using checkbox in front of each test name - mark it to select the test or unmark it to deselect it.
Plus there are 3 commands (in order to access these commands click on checkbox image located in header line):

- [Select all] - selects all tests in the list;
- [Unselect all] - use this command to unmark (clear) all checkboxes at once;
- [Inverse selection] - inverts the selection

Test Info



Test Info window can be used in any workplace, it offers the following pages:

Test info page provides information about selected test item, such as current and previous state, statistics, modification date, comments, related URL, etc.

Quick log page displays last 10 events for selected test item. The term "event" means a log record that was added with every test status change. If logging mode for the test is set to "Reply" or "Full", HostMonitor will add a new record when test status changes or the value of "Reply" field changes.

Actions log page shows the following information:

- Event time (the time when action has been executed);
- Status of the test (when action was triggered);
- Action method (type of the action);
- Result of the action execution

Note: you may tell HostMonitor to ignore some actions, i.e. do not store information about action results in Quick Log. The option "Quick Log: store action results" is located in Action Properties dialog. You may disable the option for non-important actions, like "Play sound" action.

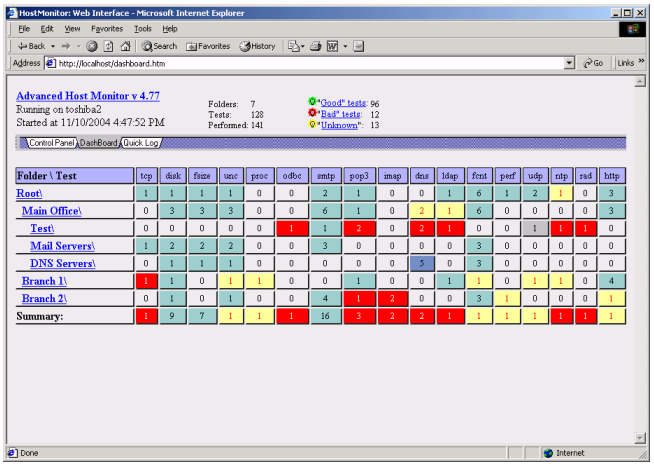
Performance chart shows graph using information about minimum, maximum and average reply values of the test item over selected time interval

Availability chart shows graph using information about alive/dead/unknown test results ratio over selected time interval
You may choose any of the following time periods to display:

- Today
- Yesterday
- Last 24 hours
- Last 48 hours
- This week
- Last week
- Last 7 days
- Last 14 days
- This month
- Last month
- Last 30 days
- Last 60 days
- This year
- Last year
- Last 12 months
- Last 24 months

SNMP Data page: when you select SNMP Table test item, you may check the table with data retrieved from SNMP agent. For each retrieved counter, it shows OID, current value, previous value and difference.

2) Dashboard



Dashboard is an indicator panel. One glance at the dashboard will give you comprehensive overview of all tests in all folders.

Every folder is represented by a row on the dashboard. Each cell of the row represents tests of a certain type from within that folder (e.g. Ping, CPU Load, Service, Drive Free Space).

Number inside cell and their color depend on the tests results:

Color*	Meaning of the color of the cell	Meaning of the number in the cell
N	Some test(s) have “bad” status (non-acknowledged)	Number of “bad” test items
N	No “bad” tests but some test(s) have “warning” status (non-acknowledged)	Number of “warning” tests
N	No “bad” or “warning” test items but some test(s) have “unknown” status (non-acknowledged)	Number of “unknown” tests
N	There are some "bad", “warning” or "unknown" items, all of them acknowledged	Number of acknowledged tests
N	No bad/unknown tests but there are WaitForMaster test(s)	Number of tests with “Wait for master” status
N	ALL tests are disabled	Number of disabled tests
N	All tests have “OutOfSchedule” status	Number of “OutOfSchedule” tests
N	No “bad”/”unknown”/”wait” items, some (all) tests are “good”	Number of “good” test items
0	No tests of this type in the folder	0 – no tests

* colors used for the report depend on color palette you have chosen.

When you click on cell, popup window will show list of tests which have determined current status (color and value) of the cell. For example if you click on "red" cell that represents Ping tests for "USA Office" folder, you will see all "bad" ping test items within this folder. Then you may use popup menu items to check test statistics, quick log, actions log, charts, enable or disable test items, acknowledge test status, etc.

When you click on folder item, interface will switch to Management mode and open selected folder.

Note: If you are using simplified version of the interface (WS1), popup menu functions are not available; instead you may click on folder name link to check folder properties or to see

corresponding lists displaying good, bad and unknown test items as well as complete list of tests in the folder.

3) Quick Log

Quick Log workplace displays most recent events. The term "event" means a log record that was added with every test status change. If logging mode for some test is set to "Reply" or "Full", HostMonitor adds a new record when either the test status or "Reply" field value of the test changes.

Quick Log pane offers popup menu: you may click right mouse button on test item and choose operation - it allows you to Refresh, Pause or Disable test items, Acknowledge "bad" status, open Test Info window, check log records for the test item, actions log, availability and performance charts for various periods (7, 14 days, 30 or 60 days, week or 2 weeks, last or current month, etc.)

Quick Log mode can be used for audio alerts, interface will start alert when new “bad” event detected. There are 3 modes available:

- Sound off
- Sound once
- Sound continuously

Note 1: in order to switch mode use right mouse click on "Quick Log" tab
Note 2: when "Sound continuously" option is selected you may stop audio alert using "Stop alerts" button located in "Alert" window or "Stop alerts" popup menu item located in "Quick log" tab context menu

If you are using simplified version of the interface (WS1), audio alerts option is not available; also there is no popup menu. Quick Log pane provides links to test properties. Click on the name of the test and the Web Service will display the Test Properties window.

4) Top Hosts

Top Hosts pane shows "top" test items from the following categories

Highest ratio of lost packets (%)	Ping tests
Slowest echo reply (ms)	Ping tests
Slowest web site (ms)	URL and HTTP tests
Highest CPU usage (%)	CPU Usage tests
Hottest system/CPU	QNAP, Synology, NetApp, Cisco, Juniper and HP iLO Temperature tests
Lowest free memory (%)	Memory tests
Lowest disk space (%)	Disk Free Space and UNC tests
Lowest disk space	Disk Free Space and UNC tests
HDD: Highest disk load	Synology Disk Load and Windows Performance Counter ('% Disk Time') tests
HDD: Hottest disk	includes QNAP Temperature, Synonoly Temperature and HDD Smart tests
HDD: Most bad sectors	SMART tests
HDD: Oldest disks	SMART tests
Highest CPU usage (%)	Dominant Process tests
Highest handles usage	Dominant Process tests

Highest threads number	Dominant Process tests
Highest memory usage	Dominant Process tests
Highest VM usage	Dominant Process tests
UPS Load tests	UPS: Highest load
UPS: Highest temperature	UPS Temperature tests
UPS: Lowest charge level	UPS Charge tests

You may click right mouse button on displayed test item and choose operation, popup menu allows you to Refresh, Pause or Disable test items, Acknowledge "bad" status, open Test Info window, check log records for the test item, actions log, availability and performance charts for various periods (7, 14 days, 30 or 60 days, week or 2 weeks, last or current month, etc.)

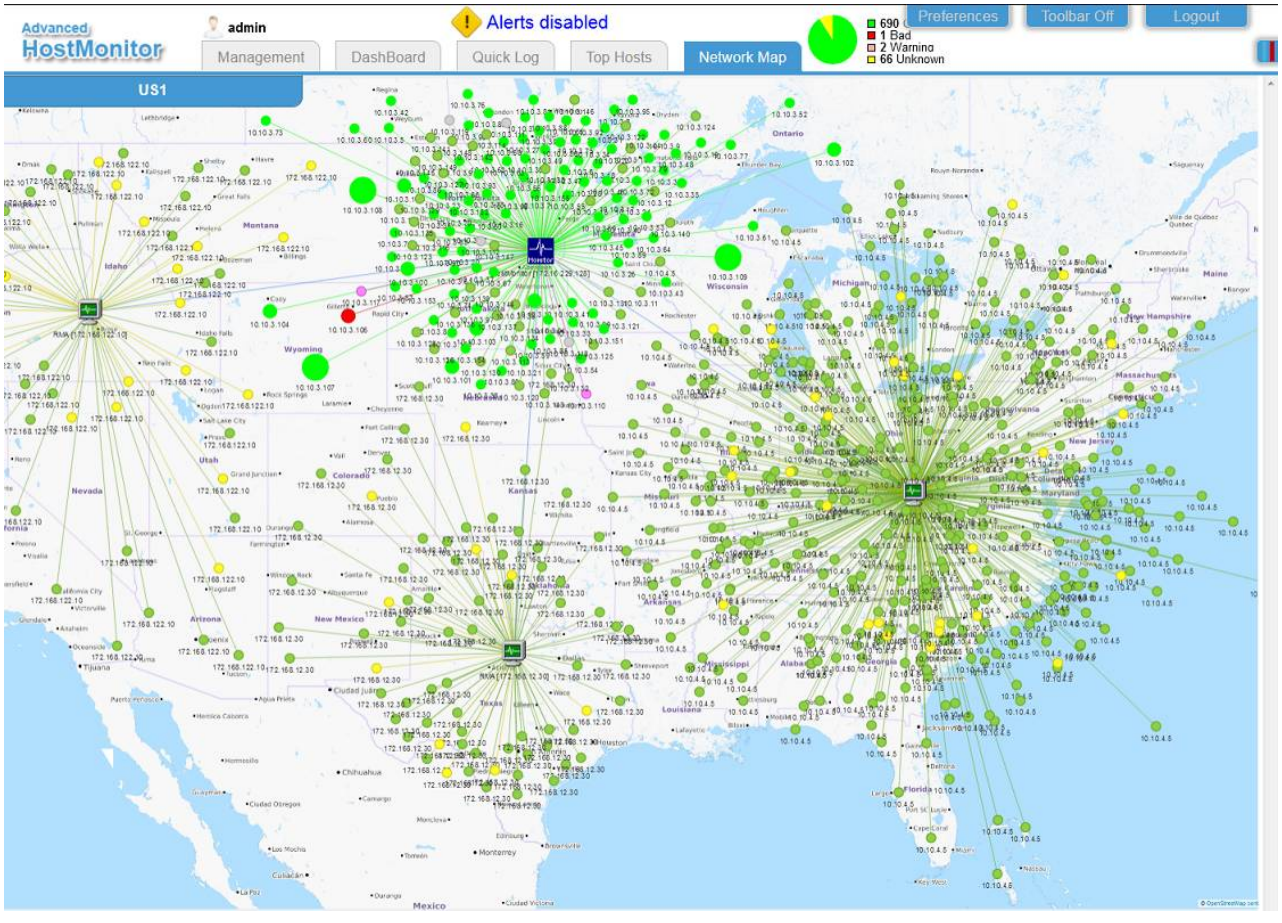
- **Show** collapsed / **Hide** collapsed
- **Automatically** open&close panels / **Manually** open&close panels

Using these options and drag&drop operations, you may organize panels to your liking. For example you may set Show Collapsed + Manually open&close panels options, move Web related groups to the top, move UPS related groups to the bottom, minimize(close) HDD related groups, then switch from Show Collapsed to Hide Collapsed.
While "Automatically open&close panels" option tells Web Service to open groups with data (tests) and minimize or hide groups without available tests.

Note: Top Hosts pane not available in simplified version of the interface (WS1).

5) Network map

Web Service may group all tests related to the same host, set links between different hosts depending on HostMonitor-RMA and Master-Dependants relations and display HostMonitor, RMA agents and all hosts on interactive map.



Gravity and Spiral. Web Service may set initial positions for the elements using "Gravity" and "Spiral" algorithms. Spiral works much faster so we recommend this method when you are monitoring thousands of hosts. Actually you may use both methods - init entire WAN map using Spiral algorithm, then select some part of the map (e.g. click on RMA agent to select agent and all hosts monitored by this agent) and apply Gravity algorithm for this LAN. **Note:** Spiral algorithm will reset entire map, while Gravity algorithm may work with entire map or selected subset (e.g. RMA agent with hosts or Master test with dependent items). When you click on Gravity button, button caption changes to "Stabilize/Stop" and you may click it again when map looks "good enough" without waiting for algorithm to complete.

Then you may manually adjust position of any element (standard drag&drop). If you drag master item and hold the button depressed, interface will rearrange dependant items using Gravity algorithm; release mouse button to stop this process at any time.

Rotate left / Rotate right – these buttons may work with entire map or with selected segments (just like Gravity button).

Undo and Redo buttons help to fix mistakes.

Zoom – use mouse wheel to zoom in / zoom out.

Background images

You may set comment, load background image (select image from drop-down list and click "Set map background" button), then save map settings using Save or SaveAs buttons. Some background samples located in WebService\mapsbg\ folder, images based on data provided by OpenStreetMap (http://www.openstreetmap.org/copyright). You can create your own images to fit your company standards and copy files into this folder.

Items

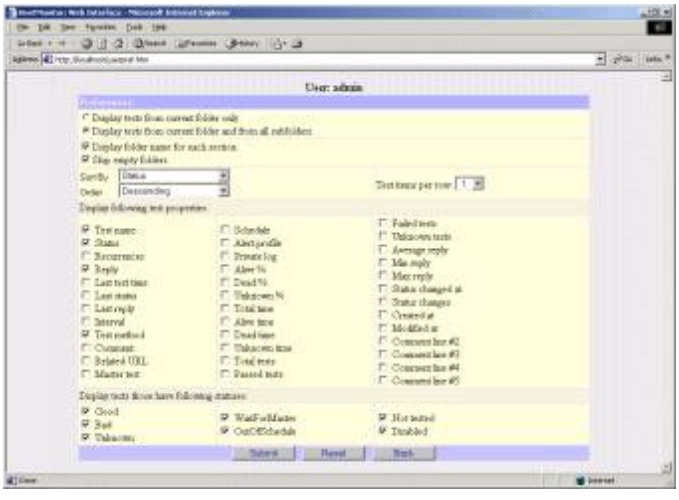
Item color depends on status of all tests related to the host. E.g. green means all tests have "good" status (and may be some disabled tests); yellow means there are some tests with "unknown" status; pink – warning tests; red – there are some "bad" tests; orange - there are some "bad", "warning" or "unknown" items, all of them acknowledged; grey – all tests disabled.

Size of the item depends on number of tests related to the host.

Click on the host (right mouse button) and you will see test items related to the host: test name, last reply and average reply value. Then you may select test and use popup menu (right mouse click again) to enable, pause, resume test, acknowledge test status, check quick log, check performance history and so on.

Preferences

This link brings up the options/settings window. The settings and options that you define through this window are individual for each user and they are stored with Web Server so that when you will log in to HostMonitor next time (even from some another computer) your settings from the previous session will be saved for you.
The following options are available:



- **Palette**
  Here you may choose a color palette for Web Interface. Please note: only persons that have access to system where Web Service is running can modify predefined palettes or create new palettes.

- **Display all (sub) folders at once**
  With this option selected Web Service will always display expanded view of all folders and descendant subfolders in the Folder section.
- **Use interactive folder tree (cookies must be enabled)**
  With this option selected you will be able to expand or collapse any folder(s).
  (these options make sense for simplified version of the interface WS1)

- **Folder section width**
  This parameter allows you to set the default width (in pixels) for the Folder section.

- **Display tests from current folder only**
  When this option is enabled the right pane will show you only the tests from the current folder (the one that is selected through the left pane; the name of this folder is shown in bold) not including the tests from the subfolders.
- **Display tests from current folder and all subfolders**
  This option allows you to see all tests from the current folder and all of subfolders.

- **Display folder name for each section**
  This option lets you to see the name(s) of folder(s) in the right pane of the window. The folder name appears at the beginning of the list of tests from within that folder. You may found this option useful especially when the current folder has lots of subfolders.
- **Skip empty folders**
  After enabling this feature folders that have no tests in them will disappear from the right pane.

- **Sort by**, here you may specify the field to sort the tests by.
- **Sort order**, you may set the ascending or descending sort direction.

- **Test items per row**
  This option allows you to place more then one tests in each row of the tests list, so that tests will be arranged in columns
  (this option make sense for simplified version of the interface WS1)

- **Display the following test properties**
  This is an array of checkboxes, by marking/unmarking them you may specify the list of fields (test properties) to display.

- **Display only tests that have following statuses**
  Here you may filter the list of tests forcing the Web Service to show you only the tests with certain statuses.
  Please note: if "Checking" switch is marked, Web Service will display "Checking.." for test items which HostMonitor is checking right now). Otherwise you will see status that said test items had just before check was started.

Notes related to simplified interface (WS1): after you had changed any of the options do not forget to hit "Submit" button. Only after this the changes will take effect. Hitting the "Back" button in the settings window as well as the browsers back button will discard all your changes. The button "Reset" sets all settings to their default values. Note, after you have changed the settings in web interface you may need to click browsers "refresh" button to see immediate results of the changes (especially if you are using Internet Explorer, sometimes you need to use Refresh function several times).

Web Service: Authentication modes

You may set allowed authentication mode using Web Service menu Options -> Authentication

- HostMonitor authentication
  Web browser will prompt for user name and password, operator should type user name and password set on HostMonitor side (menu User → Operators).
  Traffic between browser and Web Service is not secured (unless HTTPS is used). Traffic between Web Service and HostMonitor are secured (just like HostMonitor↔RCC or HostMonitor↔RMA traffic).

- Windows or HostMonitor authentication (priority: Windows authentication)
  If remote operator logged on to the domain, web browser will try to get access to Web Service using Windows authentication mechanism (Kerberos). HostMonitor user account with the same name should be set with "HM or Windows authentication" option and both HostMonitor and WebService processes should be started on the same system (domain member).
  Otherwise browser will prompt for user name and password and HostMonitor authentication will be used.

- HostMonitor or Windows authentication (priority: HostMonitor authentication)
  Web browser will prompt for user name and password. However If remote operator logged on to the domain and HostMonitor user account with the same name set with "HM or Windows authentication" option and both HostMonitor and WebService processes are running on the same system (domain member) then you can type **WindowsAuth** instead of user name and web browser will be able to connect to HostMonitor using Windows authentication mechanism (Kerberos).

Kerberos notes

When web browser and web service begin communications, they pass encrypted tickets through a trusted third-party system (Key Distribution Center). The KDC passes a secret ticket with a decryption key to both nodes. The nodes then pass encrypted time stamps to each other and use the key to decrypt them. If they do so successfully, they authenticate their counterparts and can trust each other.
The KDC is integrated with Windows Server security services that run on the domain controller (DC) and uses the Active Directory Domain Services database as its security account database. However you should set remote user permissions on HostMonitor side (password in not used in this case, provide password if you plan to use Windows AND HostMonitor authentication modes).

Requiements

- approximate clock synchronization between the machines on the network (HostMonitor, WebService system, Domain Controller, remote operator system). If the time difference between the server and client is greater than five minutes, authentication will fail
- DNS entries and hosts on the network are all properly configured
- HostMonitor and Web Service should be started on the same system (domain member)

- Web Service cannot use local system account in this case, it should be started under domain user (e.g. domain1\webuser)
- set Service Principal Names (SPN) directory property for an Active Directory service account used by Web Service. E.g.
  setspn /s HTTP/wshostname.domain1.com domain1\webuser
  setspn /s HTTP/wshostname domain1\webuser
  You may need to use both commands, this helps to avoid some Internet Explorer problems (e.g authorization will work for 30 minutes).
  More information available at docs.microsoft.com

Browser settings

FireFox:

- in the URL text box of the Firefox browser, enter **about:config** to access the advanced settings; click Accept the Risk and Continue;
- find and double-click on **network.negotiate-auth.trusted-uris** in the Preference Name column; enter web service URL in the text box (If you are using multiple connectors for Kerberos authentication, add a comma separated list of connectors);
- HTTPS protocol should be set on Web Service and must be used for FireFox

Internet Explorer / Microsoft Edge:

- in the Internet Options window select the Security tab; click on the Trusted Sites icon and then click the Sites button; add Web Service URL to the Web sites list;
- in the Internet Options → Security tab click the Custom Level button; make sure
  - User Authentication → Logon is set to Automatic logon with current username and password
  - Miscellaneous → Web sites in less privileged Web content zones can navigate into this zone is set to Enable.
- in the Internet Options window click the Advanced tab; ensure that Security → Enable Integrated Windows Authentication option is set

Chrome:

- Chrome uses the Internet Explorer configuration to enable Kerberos authentication so you should configure Internet Explorer

Web Service: SSL

You may secure Web Service by using HTTPS protocol and SSL certificates. An SSL (Secure Sockets Layer) certificate is a digital certificate that authenticates the identity of the web site, SSL technology allows to encrypt all data transfer between web server and the client (web browser). Each SSL Certificate consists of a public key and a private key. When a web browser connects to a secured web server, a Secure Sockets Layer handshake authenticates the server and the client (web browser). An encryption method is established with a unique session key and secure transmission can begin.

If you want to setup Web Service to work over HTTPS protocol, you should have two files in PEM format: server certificate and private key. There are several file formats, certificate can be stored in: DER, PEM, P7B, P7C, etc. Web Service requires certificate and private key in PEM format (Privacy Enhanced Mail) Its Base64 encoded DER certificate, enclosed between "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" text.

Certificate and private key files must be named as **ServerCert.pem** and **ServerKey.pem** accordingly. These files should be located in the same folder where Web Service is installed. If you have certificate and private key, stored in PEM files with other names, just rename the files.

- ServerKey.pem – Private key used to encrypt data. It must correspond to the public key stored in the certificate (ServerCert.pem file)
- ServerCert.pem – Public key (certificate) to be sent to the remote site for authetification. This key can be protected by password. In such case Web Service will ask you for password on startup (just 1 time, unless you change the file).

Where can you get these files?
There are several possible ways:

1. Use SSL certificate that already installed on your IIS web server
2. Use SSL certificate that already installed on your Apache web server
3. Create CSR (Certificate Signing Request) and request certificate from external certification authority like VeriSign, Thawte, etc.
4. Create self-signed SSL certificate

Please note: OpenSSL package has to be installed in order to perform all necessary steps.

1. IIS -> Web Service

If you have SSL certificate installed on your IIS web server, you may use this certificate for Web Service as well. You just should follow the steps provided below in order to export certificate from IIS and convert it into PEM format.

α) Export your IIS certificate into a PFX file

8. Run mmc.exe
9. Click the 'Console' menu and then click 'Add/Remove Snap-in'.
10. Click the 'Add' button and then choose the 'certificates' snap-in and click on 'Add'.
11. Select 'Computer Account' then click 'Next' button.

12. Select 'Local Computer' and then click 'OK'.
13. Click 'Close' and then click 'OK'.
14. Expand the menu for 'Certificates' and click on the 'Personal' folder.
15. Right click on the certificate that you want to export and select 'All tasks' -> 'Export'.
16. A wizard will appear. Make sure you check the box to include the private key, enable "Include all certificates in the certification path if possible" and continue through with this wizard until you have a .PFX file.

β) Use OpenSSL to extract the private key and the cert file into PEM files

- Export the private key file from the pfx file

```
openssl pkcs12 -in filename.pfx -nocerts -out ServerKey.pem
```

- Export the certificate file from the pfx file

```
openssl pkcs12 -in filename.pfx -clcerts -nokeys -out ServerCert.pem
```

- Export intermediate certificate (if necessary)

```
openssl pkcs12 -in filename.pfx -cacerts -nokeys -out ServerCAcert.pem
```

If there are some intermediate certificate(s) then you may add content of ServerCAcert.pem file into ServerCert.pem file.

You may use simple BAT file like the following

```
set OPENSSL_BIN=c:\openssl\bin
set WebService_BIN=c:\Program Files\HostMonitor\WebService
%OPENSSL_BIN%\openssl pkcs12 -in %1 -nocerts -out "%WebService_BIN%\ServerKey.pem"
%OPENSSL_BIN%\openssl pkcs12 -in %1 -clcerts -nokeys -out "%WebService_BIN%\ServerCert.pem"
rem Export intermediate certificate (if necessary) and append to ServerCert.pem file
%OPENSSL_BIN%\openssl pkcs12 -in %1 -cacerts -nokeys -out ServerCAcert.pem
type ServerCAcert.pem >>"%WebService_BIN%\ServerCert.pem"
del ServerCAcert.pem
```

Just make sure you have specified correct path for OPENSSL_BIN and WebService_BIN variables.

2. Apache -> Web Service

Apache web server uses OpenSSL libraries just like our Web Service does, so it uses the same PEM files to store certificates. You may find path to certificate files using httpd.conf file. Then you may copy files into Web Service directory and rename files according to Web Service specification:

httpd.conf should contain the following parameters:

SSLCertificateFile - certificate,
SSLCertificateKeyFile – private key
SSLCertificateChainFile – intermediate (chain) certificate(s)

For example, if you see the following lines

SSLCertificateFile /etc/ssl/crt/primary.crt
SSLCertificateKeyFile /etc/ssl/crt/private.key
SSLCertificateChainFile /etc/ssl/crt/intermediate.crt

you may copy private.key file as ServerKey.pem, copy primary.crt file as ServerCert.pem and append intermediate.crt into ServerCert.pem

SSLCertificateFile /etc/ssl/crt/primary.crt -> WebService\ServerCert.pem
SSLCertificateKeyFile /etc/ssl/crt/private.key -> WebService\ServerKey.pem
SSLCertificateChainFile /etc/ssl/crt/intermediate.crt -> WebService\ServerCert.pem

```
set WebService_BIN=c:\Program Files\HostMonitor\WebService
copy private.key "%WebService_BIN%\ServerKey.pem"
copy primary.crt+intermediate.crt "%WebService_BIN%\ServerCert.pem"
```

3. How to create a CSR to request certificate from external certification authority like VeriSign, Thawte etc.

The CSR is a string of text generated by your server software. You provide this text to certification authority during the enrollment process. You may use the following command to create private key and CSR.

```
openssl req -newkey rsa:1024 -sha1 -keyout ServerKey.pem -out ServerReq.csr -text
```

Foregoing command creates two files:

- ServerKey.pem – private key you should use for WebService
- ServerReq.csr – certificate signing request (CSR) which you should provide to external certification authority

You will be asked for several pieces of information like the following:

- Country Name (2 letter code)
- State or Province Name (full name)
- Locality Name (e.g., city)
- Organization Name (e.g., company)
- Organizational Unit Name (e.g., section)
- Common Name (e.g., your name or your server hostname)
- Email Address
- A challenge password
- An optional company name

Answer them truthfully. Specify the domain name of your server as the Common Name (e.g. microsoft.com). After ServerReq.csr is generated, you should submit ServerReq.csr to certification authority. They will use information, stored in CSR file to create certificate for you. Certificate will be sent to you in text format, so you just should save it into ServerCert.pem file and copy it along with ServerKey.pem into Web Service folder.

Please note: certificates signed by recognized (trusted) certification authority are automatically accepted by web browsers. Otherwise web browser will ask you to accept or reject the certificate. To avoid this situation, you may download and install certification authority root CA certificate. For instance, if you decide to use VeriSign Test certificates, you should download and install the Test Root CA Certificate. Use the link listed below and follow the steps to install the Root certificate for your internet browser:

https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=SO10670

4. How to create self signed certificate

We can suggest you two possible solutions. First one is pretty simple, just two commands to execute:

```
openssl req -newkey rsa:1024 -sha1 -keyout ServerKey.pem -out ServerReq.csr -text
```

```
openssl x509 -req -days 365 -in ServerReq.csr -signkey ServerKey.pem -out ServerCert.pem
```

As you may see, first command creates CSR and private key. Second one creates certificate according to CSR and sign it using private key. That's all. You may copy ServerCert.pem and ServerKey.pem into Web Service folder and start Web Service. What's the catch? This certificate will not be recognized by web browsers as "trusted" certificate; it will be displayed as "untrustworthy" cert. You will need to accept this certificate every time web browser opens session and connects to Web Service.

Second solution is more complicated however it allows you to create server certificate authority certificate that can be imported into browser in order to avoid "untrustworthy certificate" warning.
First of all, you should use OpenSSL to create root CA. If you already have root CA, you may skip this step.

```
openssl req -newkey rsa:1024 -sha1 -keyout RootKey.pem -out RootReq.pem -text
```

```
openssl x509 -req -in RootReq.pem -sha1 -extensions v3_ca -signkey RootKey.pem -out Root.pem -days 730
```

```
type Root.pem >RootCert.pem
```

```
type RootKey.pem >>RootCert.pem
```

Result of foregoing commands provides two files: RootCert.pem and RootKey.pem

After that, you may export RootCert.pem into format, accepted by web browser

```
openssl pkcs12 -export -inkey RootKey.pem -in RootCert.pem -out Root.p12
```

You will get Root.p12 certificate that can be imported into your browser. For instance, using Internet Explorer you may open menu Tools → Internet Options → Content → Certificates →
Import and then import this certificate into "Trusted Root certification authorities" group.

Now we have to create server CA and sign it with root CA:

```
openssl req -newkey rsa:1024 -sha1 -keyout ServerCAkey.pem -out ServerCAreq.pem -text
openssl x509 -req -in ServerCAreq.pem -sha1 -extensions v3_ca -CA RootCert.pem -CAkey RootCert.pem -CAcreateserial -out ServerCA.pem -days 730
type ServerCA.pem >ServerCACert.pem
type ServerCAkey.pem >>ServerCACert.pem
```

Result of the foregoing commands provides two files: ServerCACert.pem and ServerCAkey.pem

The following command converts ServerCACert.pem into format accepted by the browser:

```
openssl pkcs12 -export -inkey ServerCAKey.pem -in ServerCACert.pem -out ServerCA.p12
```

Please, import ServerCA.p12 into your web browser and place it into “Intermediate certification authorities” section.

Eventually, we can create certificate for Web Service.

```
openssl req -newkey rsa:1024 -sha1 -keyout ServerKey.pem -out ServerReq.pem
openssl x509 -req -in ServerReq.pem -sha1 -extensions usr_cert -CA ServerCA.pem -CAkey ServerCA.pem -CAcreateserial -out Server.pem -days 730
type Server.pem > ServerCert.pem
type ServerKey.pem >> ServerCert.pem
```

Now you may copy ServerCert.pem and ServerKey.pem into Web Service folder and start Web Service using HTTPS protocol. When you import root CA and server CA into your browser, browser will accept certificate automatically, without annoying warnings and requests.

Please note: on each stage (creating root CA, server CA and server certificate) you will be asked for several pieces of information as described in topic devoted to Apache. Answer them truthfully.

You may create a .BAT file like the following to process all certificates at once:

```
@echo off
set OPENSSL_BIN=c:\openssl\bin
set WebService_BIN=c:\Program Files\HostMonitor\WebService


echo Create the root CA
%OPENSSL_BIN%\OpenSSL req -newkey rsa:1024 -sha1 -keyout RootKey.pem -out RootReq.pem  -text
%OPENSSL_BIN%\OpenSSL x509 -req -in RootReq.pem -sha1  -extensions v3_ca -signkey RootKey.pem -out Root.pem  -days 730
type Root.pem >RootCert.pem
```

```
type RootKey.pem >>RootCert.pem

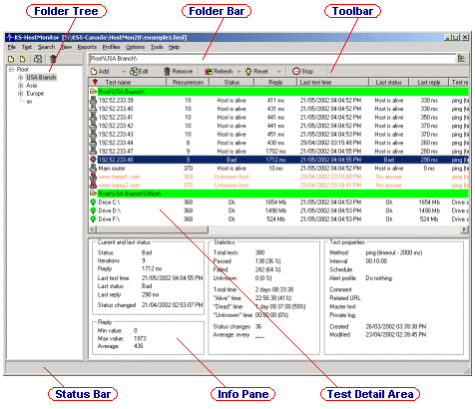

echo Export the root CA in a format suitable for IE
%OPENSSL_BIN%\openssl pkcs12 -export -inkey RootKey.pem -in RootCert.pem -out Root.p12


echo Create the server CA and sign it with the root CA
%OPENSSL_BIN%\OpenSSL req -newkey rsa:1024 -sha1 -keyout ServerCAkey.pem -out
ServerCAreq.pem -text
%OPENSSL_BIN%\OpenSSL x509 -req -in ServerCAreq.pem -sha1 -extensions v3_ca -CA
RootCert.pem -CAkey RootCert.pem -CAcreateserial -out ServerCA.pem -days 730
type ServerCA.pem >ServerCACert.pem
type ServerCAkey.pem >>ServerCACert.pem


echo Export the server CA in a format suitable for IE
%OPENSSL_BIN%\openssl pkcs12 -export -inkey ServerCAKey.pem -in ServerCACert.pem -out
ServerCA.p12


echo Create the server's certificate and sign it with the server CA
%OPENSSL_BIN%\OpenSSL req -newkey rsa:1024 -sha1 -keyout ServerKey.pem -out
ServerReq.pem
%OPENSSL_BIN%\OpenSSL x509 -req -in ServerReq.pem -sha1 -extensions usr_cert -CA
ServerCA.pem -CAkey ServerCA.pem -CAcreateserial -out Server.pem -days 730
type Server.pem > "%WebService_BIN%\ServerCert.pem”
type ServerKey.pem >> "%WebService_BIN%\ServerCert.pem”
type ServerKey.pem >  "%WebService_BIN%\ServerKey.pem”
```

RCC



RCC allows you to work with HostMonitor that is running on a remote system just like you work with HostMonitor when it is started on your local system. RCC has exactly same interface as the one of the HostMonitor. Via RCC you will be able to modify alert profiles, reports, change any option, edit mail templates, create new or modify existing test items, etc.

Features:

- All data transmission between HostMonitor and RCC is encrypted and password protected;
- HostMonitor & RCC allow you to setup different user accounts with different sets of permissions;
- RCC does not require installation;
- Several operators may connect to the same instance of HostMonitor at the same time.

What is important - several operators may start RCC on different systems and work with the same instance of HostMonitor at the same time (please note: in such case you will need to buy more than 1 RCC license). There is one restriction: if one operator is editing certain sort of profiles (e.g. alert profiles), other operators will not be able to edit profiles of the same sort at the same time. However they will be able to view these profiles and edit other HostMonitor's settings, e.g. modify report profiles, schedules or mail templates. Several operators may add new test items at the same time; also they are able to edit different test items at the same time. But several operators cannot edit the same test item simultaneously. Only one operator who is the first to open the Test Properties dialog for certain test is able to change its settings, other operators may only view properties of this test but are still able to modify other test items.
When an operator cannot modify some settings, profiles, etc, because of another operator activity, RCC displays this image in the dialog. You may contact the operator who had locked you out or try to open the dialog later.

RCC and RMA
RCC works with Active RMA using HostMonitor as gateway. RCC ↔ HostMonitor ↔ Active RMA. In other words, there is no direct TCP connection between RCC and Active RMA at all. At the same time RCC uses direct TCP connection when it works with Passive RMA (RCC ↔ Passive RMA).

Import

RCC allows you to import test settings from a text file offering 2 options (both options accessible thru main menu File):
- Import from text file on HM system
- Import from text file on RCC system

“Import from text file on HM system” allows you to import test settings using text file located on system where HostMonitor is running. You may select any import file and tell application to keep or skip duplicates. Import statistics will be displayed on screen right away; errors and warnings can be checked by using Auditing Tool or system log file.

“Import from text file on RCC system” allows you to import test settings using text file located on system where RCC is running. This function works like HostMonitor analogue with one disadvantage: you cannot use CreateFolder commands in import file, yet

Limitations:
You cannot create new HML file (test list) and load another HML file;

RCC Installation

Remote Control Console does not require any installation. When you install HostMonitor using "Enterprise" or "Custom" installation mode**, rcc.exe** module will be located in HostMonitor's directory. You may simply copy this file to any system where you want to start RCC. Or you may upload rcc.exe to your web site and start Remote Console on any system connected to the Internet/Intranet.

Optionally you may copy the **hostmon.chm** file together with rcc.exe, it will serve as a local help system and RCC will not need to request on-line help. This will increase performance and make the work with RCC more convenient.

Quick start

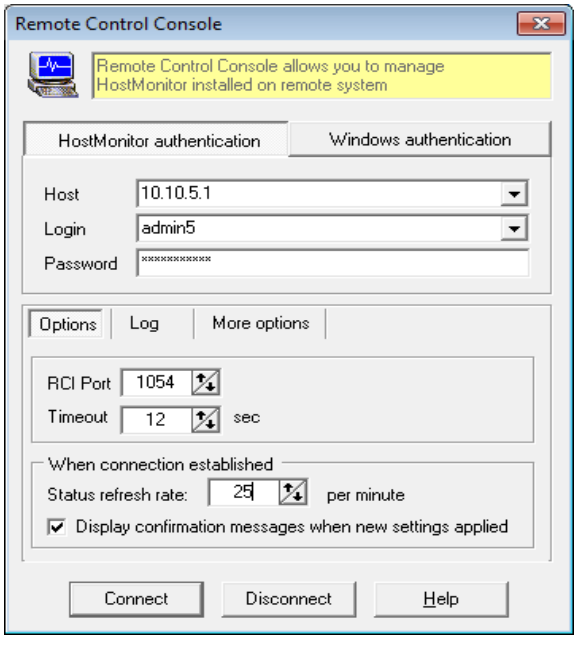
To allow remote management of HostMonitor please follow these simple steps:

- start HostMonitor
- configure HostMonitor's Remote Control Interface on RCI page in the Options dialog (menu Options)
- setup user accounts: use HostMonitor's menu "User"->"Operators"

Now you may start RCC, type address of the system where HostMonitor is running (**Host**), enter your login name (**Login**) and password (**Password**) and click "Connect" button. That's it.
When TCP connection established and authentication passed, RCC will display information about test items, folders, profiles. GUI is identical to HostMonitor's GUI, so you don't need to learn how to use new application.

Windows authentication
If user account set with "HM or Windows authentication" option and both HostMonitor and RCC systems are domain members then you can switch from "HostMonitor authentication" option to "Windows authentication" mode and connect to HostMonitor without providing username/password.

There are some optional parameters:



- **RCI Port**:
  if you setup HostMonitor to use other then the default TCP port (default port is 1054), please specify the same port to be used by RCC;
- **Timeout**
  the maximum amount of time (in seconds) that RCC will keep waiting for the reply from HostMonitor before returning an error response to the operator;
- **Status refresh rate**
  RCC requests HostMonitor in regular intervals of time and retrieves information about new, modified and removed test items or folders. Also RCC retrieves information about HostMonitor's status and the list of recently checked test items. So, you are able to see what HostMonitor is doing in real time. Refresh rate option specifies how often such requests should be made. Define this parameter depending on the network speed, HostMonitor's load and number of operators that may work with HostMonitor simultaneously.
- **Display confirmation messages when new settings applied**
  With this option enabled RCC will display confirmation messages received from HostMonitor. HostMonitor sends such messages when it accepts new test settings, new

options, profiles modifications, etc. If this option is disabled, RCC will display only error messages.

Additional options:

- **Try to reconnect automatically**
  If connection between HostMonitor and RCC was dropped due to some network error, this option tells RCC to establish new connection with HostMonitor without operator interaction. If such connection cannot be established, RCC will prompt for further action.

- **Play sound when connection to HostMonitor is lost**
  Name of this option speaks for itself. You just need to provide path to WAV or MIDI file.

- **Perform "play sound" actions**
  With this option enabled RCC replicates "Play sound" actions that were initiated by the HostMonitor and plays those sounds on the system where RCC runs.
  You should specify path to "bad" and "good" sound files (WAV, MID). These files must be located on drive that is accessible from RCC system (system where RCC is running).
  Notes:
  1) If several test items changed status simultaneously and HostMonitor played both ("good" and "bad") sound files, RCC will play "bad" sound only.
  2) Even if "Play sound" actions were configured with "Show Wakeup window" option, RCC will not show "WakeUp" window unless you enable "Perform 'show popup window' actions" option as well

- **Perform "show popup window" actions**
  This option allows to execute on remote system(s) (where RCC is running) the same "Show popup window" actions that where started by HostMonitor.
  RCC allows you to define the following parameters for this popup window:
  - **Position**
    You can choose "Predefined position" option and specify the coordinates for the top left corner of the window. Or switch to "Show in the last remembered position" option and RCC will remember the window position on the screen and display the popup window in the same location.
  - **Time live**
    "Close after N sec" - select this option and specify the amount of time a window will stay open before automatically closing, unless the [Close] button is selected or the [Stop] button is used to stop the countdown.
    "Close manually" - window will stay open on screen until the [Close] button is used.
  - **Style**
    If you mark "Stay on top" option, popup window will appear in front of all other windows and applications

Command line parameters:

There are 5 optional command line parameters:

-uniqueprofiles	Tells RCC to store options and connection parameters separately for each user (Windows user)
-storepassword	Tells RCC to save passwords used for connection with HostMonitor. Option can be used only if "-uniqueprofiles" option is used as well Please note: passwords are stored unencrypted in the system registry HKEY_CURRENT_USER. This means: the user with admin privileges on the system will be able to read such passwords. We do not recommend using this option unless it's really necessary.
-autoconnect	If you specify this parameter, RCC will try to establish connection with HostMonitor right after startup (without human interaction). The parameter can be used only if "-uniqueprofiles" and "-savepassword" options are specified as well
-defaultfolder	This parameter tells RCC to display specified folder after startup. You should provide full path to the folder, e.g. "-defaultfolder:Root\Main Office\CPU Usage\"
-defaultview	This parameter tells RCC to display specified view after startup. You should provide full path to the view, e.g. "-defaultview:Views\Bad and Unknown items"

Examples:

```
>rcc.exe  -uniqueprofiles
>rcc.exe  -uniqueprofiles  -storepassword
>rcc.exe  -uniqueprofiles  -storepassword  -autoconnect
>rcc.exe  -defaultview:Views\Bad_and_Unknown
>rcc.exe  "-defaultfolder:Root\Main Office\"
```

WatchDog

Lets say you have installed HostMonitor on reliable server and setup thousand test items to monitor entire network (or several networks). HostMonitor will inform you in case of any problem. Unless... unless something happens to system where HostMonitor is running. What if power supply dies, motherboard fries or Windows crashes due to some buggy driver? What if your main router stops responding?
There are various solutions. Lets start from less effective and go to the most effective.

1) You may setup HostMonitor to check connection to your router or ISP and use "network independent" alerts (such as "Send SMS using GSM modem") to inform you about this problem.
2) You may setup HostMonitor to start alerts when another operator stops monitoring or disables alerts (using "Pause monitoring/alerting" dialog window) or just allow to stop monitoring for single administrator account using User Profiles

Sure, this will not help when system where HostMonitor is running crashes. There is another option:

3) You may use HostMonitor's built-in Scheduler to start some action(s) on regular basis. E.g. you may setup HostMonitor to send e-mail to your smart phone every 30 min. If you do not receive e-mail then you know something is wrong.

You think this is annoying and not effective solution? We agree. There are much better solutions. There are other ways to monitor the monitor.

4) Manually: You may use RCC, Web Service or Telnet Service to check HostMonitor remotely. This way you may see what is going on, what test fails, what actions executed; you may acknowledge statuses and change test parameters. You can do anything but you should do everything by yourself. RCC will not be able to take any actions when HostMonitor stop responding (except call for help in case you set "play sound" action)

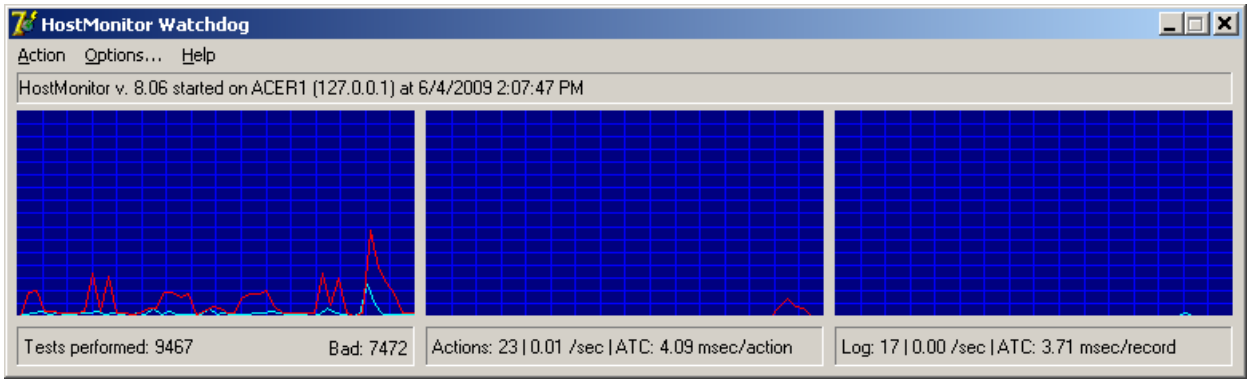
5) There is another way: install WatchDog (and optionally another instance of HostMonitor) on another system and use this system to monitor primary monitor automatically 24/7. Even better: you may setup 2nd system to start network monitoring when primary HostMonitor does not respond.

6) And finally you may monitor primary HostMonitor using another copy of HostMonitor! In such case all necessary action can be started automatically. Also there is another good feature: primary HostMonitor may monitor backup HostMonitor so each system will monitor colleague!
While WatchDog provides charts and alerts in one application at no additional cost (it is included into Enterprise package), 2nd instance of HostMonitor will provide great flexibility and reliability. See HM Montor test method.

Note: If you want to install HostMonitor on 2 systems, you need to order 2 licenses.

So, lets talk about WatchDog.

WatchDog can be used as interactive application that displays statistic information and charts in real-time. It does not allow you to manage test items like Remote Control Console. It provides just basic information about HostMonitor health: you will see is monitoring started and actions enabled, how many test probes HostMonitor performs, how many test probes failed, how many actions started, etc.



In case you have many thousands of test items, Remote Control Console may increase network load and put additional load on HostMonitor (HostMonitor needs to encrypt information about each performed test probe and send data to RCC).
In the same case WatchDog requests just general statistics information and does not increase resource usage.

On the other hand, you may start WatchDog as Win32 service, setup some actions and leave it unattended. Service will be started automatically on system boot, WatchDog will try to connect to HostMonitor and examine connection almost constantly. If connection drops, WatchDog will execute specified actions and try to reconnect. If connection recovered, service will start another set of actions.
For example you may use the following set of actions

- Visual/sound alert when connection drops and 1st reconnect attempt failed
- Send syslog message to some console if connection cannot be established for 1 minute
- Start external program (sendmail): send e-mail to admin if connection cannot be established for 1 minute
- Start external program: start backup HostMonitor if connection cannot be established for 2 minutes

---

- Visual/sound alert when connection restored
- Start external program (sendmail): send e-mail to admin if connection is stable for 1 minute
- Start external program: stop backup HostMonitor if connection is stable for 2 minutes

Regardless how you start WatchDog (using application or service mode), it will provide the same user interface. Also it shows icon in system tray and changes icon image depending on conditions: connection dropped; connection established while HostMonitor alerts disabled; connection

established but monitoring stopped; everything is Ok (connection established, monitoring started and alerts enabled).

WatchDog installation

WatchDog does not require any special installation. When you install HostMonitor using "Enterprise" or "Custom" installation mode, **watchdog.exe** module will be located in HostMonitor's directory. You may simply copy this file to any system where you want to start WatchDog. Optionally we recommend copying watchdog.ini and wdactions.lst files with default settings. When you want to move preconfigured WatchDog from one system to another, you should copy these 3 files.

How to install WatchDog as Win32 Interactive service

Start WatchDog with the command line parameter "/InstallService". E.g. "watchdog.exe /InstallService". Software will install itself as Win32 interactive service. Normally service will be started at system startup however you may start and stop service at any time using standard Windows "Services" applet or command line like "net start HMWatchDogService", "net stop HMWatchDogService"

Note 1: We do not recommend installing WatchDog as a service under Windows NT 4.0. At least not as an interactive service. In the case you really need to start WatchDog as a Win32 service on Windows NT 4.0, please disable the "Allow service to interact with desktop" option for the service (option provided by Windows Services applet). In this case you will not be able to see WatchDog icon in the system tray.
Note 2: If you are using Windows Vista or Windows Server 2008, you will not be able to use GUI in service mode. You need to start another instance in application mode when you want to change some settings.
Note 3: When you start WatchDog in application mode it checks for another instance and may stop service after confirmation (then it allows you to start service when you close application).

To uninstall service, start WatchDog with command line parameter "/UninstallService". E.g. "watchdog.exe /UninstallService".

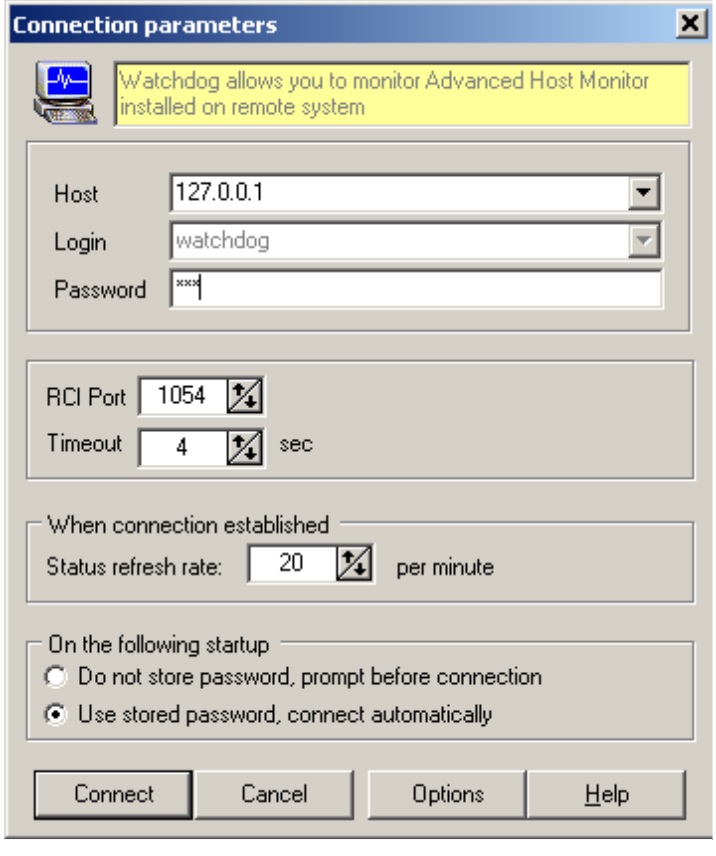
WatchDog configuration

To allow remote monitoring of HostMonitor please follow these simple steps:

- start HostMonitor
- configure HostMonitor's Remote Control Interface on RCI page in the Options dialog (menu Options)
- setup “watchdog” user account: specify password and list of acceptable IP addresses using HostMonitor's menu "User"->"Operators"

Now you may start WatchDog, type address of the system where HostMonitor is running (**Host**), enter password (**Password**) and click "Connect" button. That's it.
When TCP connection established and authentication passed, WatchDog will display information about HostMonitor, show real-time charts, etc.

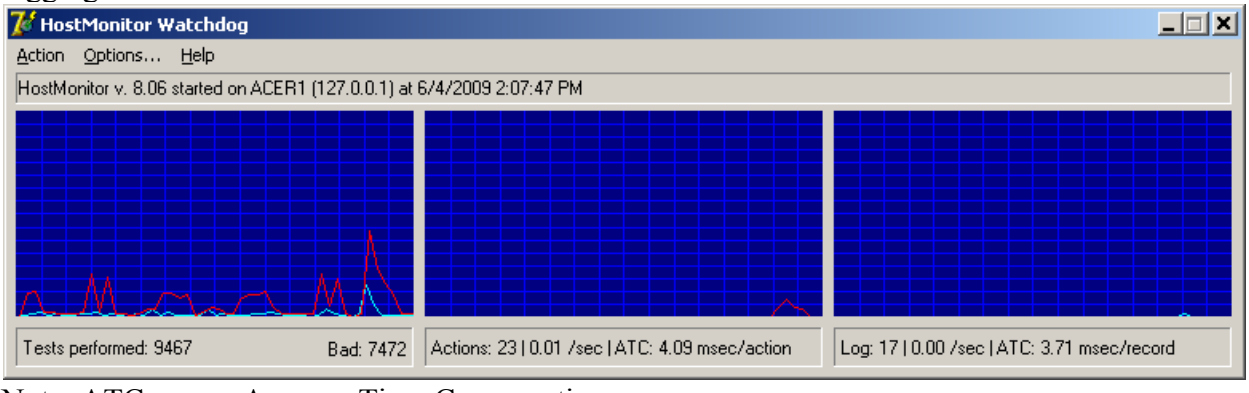
Optionally you may change TCP port used by HostMonitor, RCC, Web Service and WatchDog (RCI port); specify timeout and status refresh rate.



- **RCI Port**:
  if you setup HostMonitor to use other than the default TCP port (default port is 1054), please specify the same port to be used by WatchDog; If system where HostMonitor is running protected by firewall, make sure firewall does not reject TCP requests on RCI port
- **Timeout**:
  the maximum amount of time (in seconds) WatchDog will keep waiting for the reply from HostMonitor before returning an error response;
- **Status refresh rate**:
  WatchDog requests HostMonitor at regular intervals and retrieves statistical information. Refresh rate option specifies how often such requests should be made.
- **Do not store password, prompt before connection**
  if this option selected, WatchDog will show “Connection parameters” dialog and ask for password on every startup
- **Use stored password, connect automatically**
  use this option when you want to start WatchDog without human interaction. Application will store password and connect to HostMonitor automatically at startup. If you want to start WatchDog as service, you should use this option.

Note: you may change connection parameters at any time using menu “Action”->”Connect to HostMonitor”

If you just want to watch HostMonitor performance charts, your setup is done. WatchDog will request HostMonitor, retrieve statistics, display charts, information about performed tests, actions, logging



Note: ATC means Average Time Consumption.
E.g. “Actions: 230 | 0.01/sec | ATC: 4.09 msec/action” means the following:

- HostMonitor performed 230 actions
- HostMonitor started 0.01 action per second (in average)
- HostMonitor used 4.09 milliseconds for each action execution (in average). Note: HostMonitor calculates time used by main thread for logging and actions, it does not include time used by auxiliary threads because its not so important

This information can be useful for investigation of some 3rd party software related problems (e.g. if ODBC driver specified for ODBC logging consumes too much time).

Options/Actions

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

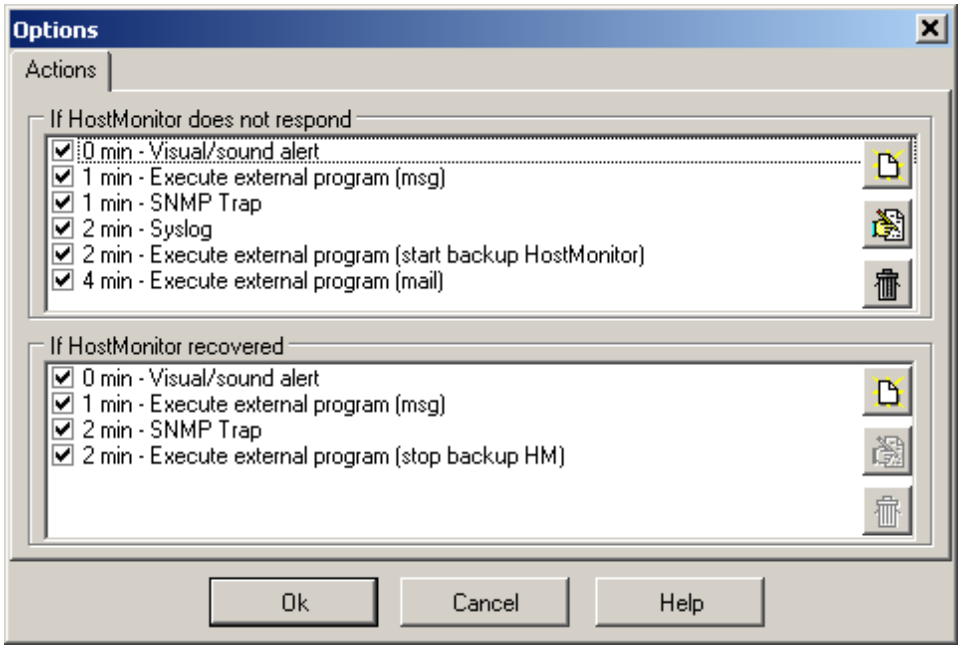
You may setup 2 lists of actions

- 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:

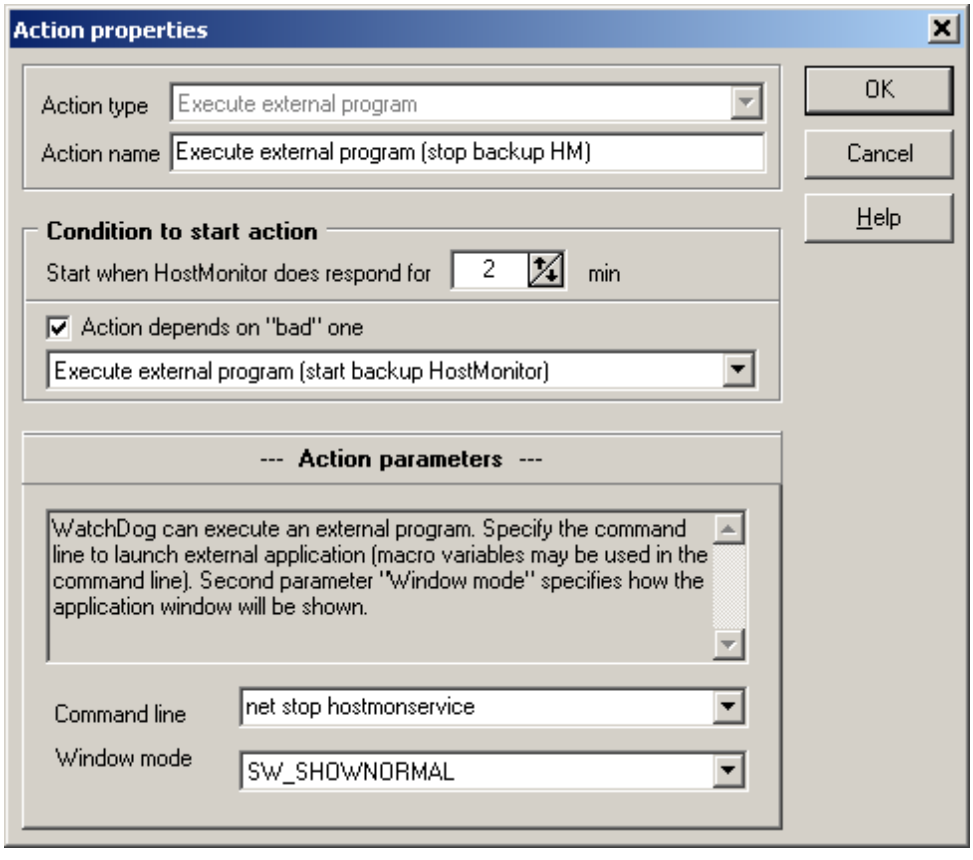
- **Add** Add new action into set
- **Edit** Bring up Action Properties dialog for editing parameters of the selected action
- **Delete** Remove selected action



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 repeatedly
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" 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.
For example 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.

Window mode
This parameter 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 find Syslog Daemon for Windows (e.g. Kiwi Syslog Daemon). 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. 8.12
%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

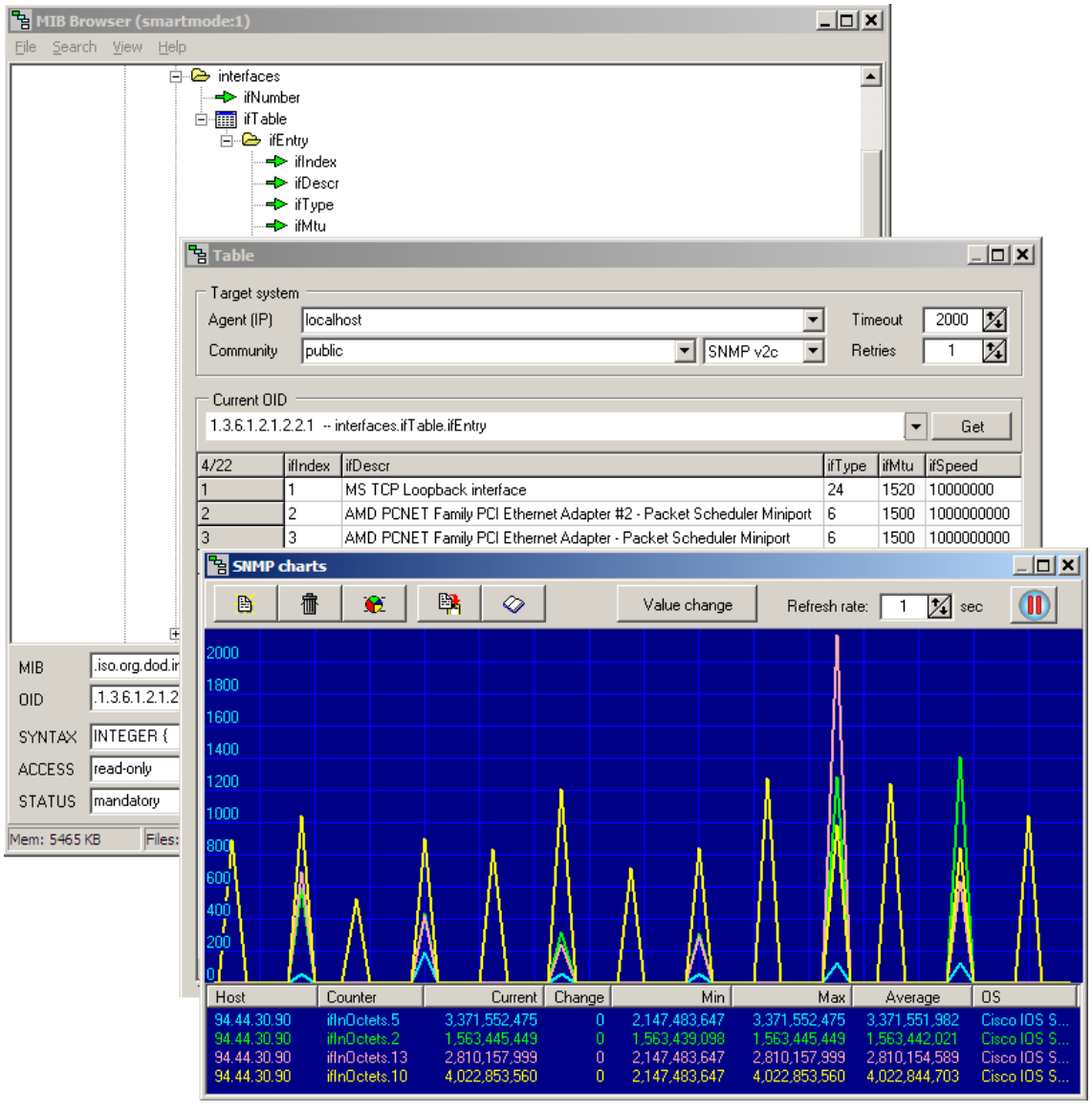
%WDSystemAddr%	IP address of the system where WatchDog is running
%WDSystemName%	Host name of the system where WatchDog is running
%ConnectedAt%	Date and time when connection to HostMonitor was established, can be used for “good” actions
%ConnectedTime%	Time when connection to HostMonitor was established, 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

MIB Browser

MIB Browser is an auxiliary application for HostMonitor. It allows you to view the hierarchy of SNMP MIB variables in the form of a tree and provides you with additional information about each node.



With MIB Browser you can easily load (compile) proprietary MIB files, view and manipulate data provided by local or remote SNMP agent - MIB Browser may retrieve counters value from specific SNMP agent, display tables, show system informaion and real-time charts.

MIB Browser and HostMonitor

When you are configuring SNMP Get, SNMP Table or SNMP Trap test methods with MIB Browser installed HostMonitor allows you to specify SNMP variables by a name (e.g. iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0) as well as by an OID in numeric format (e.g. 1.3.6.1.2.1.1.3.0). If you click on "Browse MIBs" button next to "OID" field, HostMonitor will launch MIB Browser displaying the hierarchy tree of SNMP variables. The specified variable (if any) is highlighted and additional information is displayed for it (such as status, access mode, description). Now you may browse variables, choose another variable if needed and click [Ok] button to use the selected variable by HostMonitor.
Also, by using a database of compiled MIB files HostMonitor may translate OID from its numeric form to the MIB name for received SNMP Trap messages. In such case MIB Browser is needed when you want to extend a database to include information about MIBs supported by some specific SNMP enabled device (e.g. your CISCO 1603 router).

Note: you may find IP-Tools' SNMP Scanner utility useful for your needs. SNMP Scanner allows you to scan a range or list of hosts performing Ping, DNS and SNMP queries. For each SNMP responding device the scanner displays additional information.
More information about SNMP Scanner is available at
http://www.ks-soft.net/ip-tools.eng/mframe.htm#info.htm#snmpscan

Interface of the browser is simple and straightforward so we note just few key points:

Main window

Main screen displays the hierarchy of SNMP MIB variables in the form of a tree and provides you with the following additional information about each node of the tree:
- Name
- OID
- SYNTAX
- Access
- Status
- Description

Hints:
- Press "+" or "*" to expand a tree node. If you press "+", immediate sub-nodes of the selected node will be displayed. If you press "*", all descendants of the immediate sub-nodes will be expanded as well. When the node is expanded the [-] button appears next to the node name.
- To collapse a tree node press "-". When a node is collapsed, all of its sub-nodes are hidden and the [+] button will be displayed near the node name.

Popup menu helps to retrieve value of the selected counter:
- Get value
- Get next
- Get row
- Get table
- Chart

Menu File

Allows you to perform operations with MIB files and MIB database (the database stores information about all compiled MIB files). This menu is disabled when MIB Browser is started while you were editing a HostMonitor's test item.

- Append MIB file — Brings up an "Open file" dialog, reads specified MIB file, analyzes the structure and adds branch(es) with SNMP variables into the database, displays updated tree with new items. You may use menu View->Statistics to get information about every analyzed MIB file that is included into database.
- Load database — Discards all changes and loads previously saved database
- Save database — Saves all changes into MIB database
- Clear — Removes all compiled MIBs from database
- Exit — Closes application

Note: MIB files are provided by vendors of SNMP enabled devices. If you cannot contact the vendor, try to find the file on the Internet. Numerous free resources offer wide lists of MIB files for various devices (e.g. http://www.mibdepot.com/index.shtml)

Menu Search

- Find name — Searches for specific name, and highlights the first occurrence. The search is case insensitive
- Search next — Searches for the next entry of the specified name
- Find OID — Searches for the specific OID (e.g. 1.3.6.1.2.1.1.3)

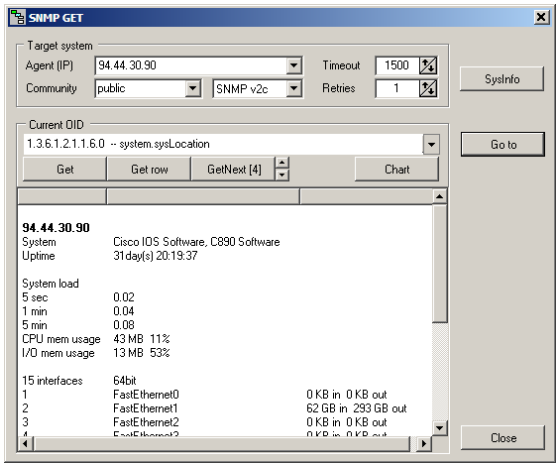
Menu View

- Chart — Loads selected SNMP chart profile and starts real-time monitoring
- System into — This utility connects to target SNMP agent and retrieves up to date system information such as OS description, uptime, disk free space, memory usage, network interfaces.
- Get counter — Brings up SNMP Get window that allows you to perform SNMP Get and Get_Next requests for SNMP agents. You may also use popup menu items "Get value" and "Get next".
- Table — Connects to target SNMP agent and retrieves current values of all counters that belong to specified table.
- Statistics — Displays information about every analyzed MIB file that is included into the database: MIB name, date when the file was analyzed, how many items are specified in the file and the number of errors (if any)

Menu Help

- Help — Displays Help
- Support — Allows you to send an e-mail request to our tech support staff
- About — Information about program

SNMP Get



This utility may request data from target SNMP agent: it may retrieve single counter, get all instances of the multi-instance counter, display up to date system info, etc

First you need to specify target system address, port, SNMP profile, then choose OID to request.

OID
The object identifier which uniquely identifies the object for requesting (e.g. 1.3.6.1.2.1.1.1.0). MIB Browser sets this field automatically using the selected MIB variable, however you may change the automatically assigned value.

After specifying above parameters you may perform the following actions:

GET
Retrieves value of the specified variable.
Please note: If you are requesting a single instance counter, add ".0" to the OID. Otherwise make sure that you have specified a valid index or use the Get Next request instead (if you don't know the index).

Get Row
This operation is useful when you need to retrieve variables from within a table. If you select multi-instance counter, this function will retrieve all instances of the counter. E.g. Get Row 1.3.6.1.2.1.2.2.1.10 will retrieve the total number of octets received on EACH network interface installed on target system.
For single-instance counters this function works similar to Get function.

Get Next
Retrieves one or several SNMP variables following the specified OID. With this operation, you don't need to know the exact variable index. The SNMP agent searches sequentially to find the needed variable within the database.

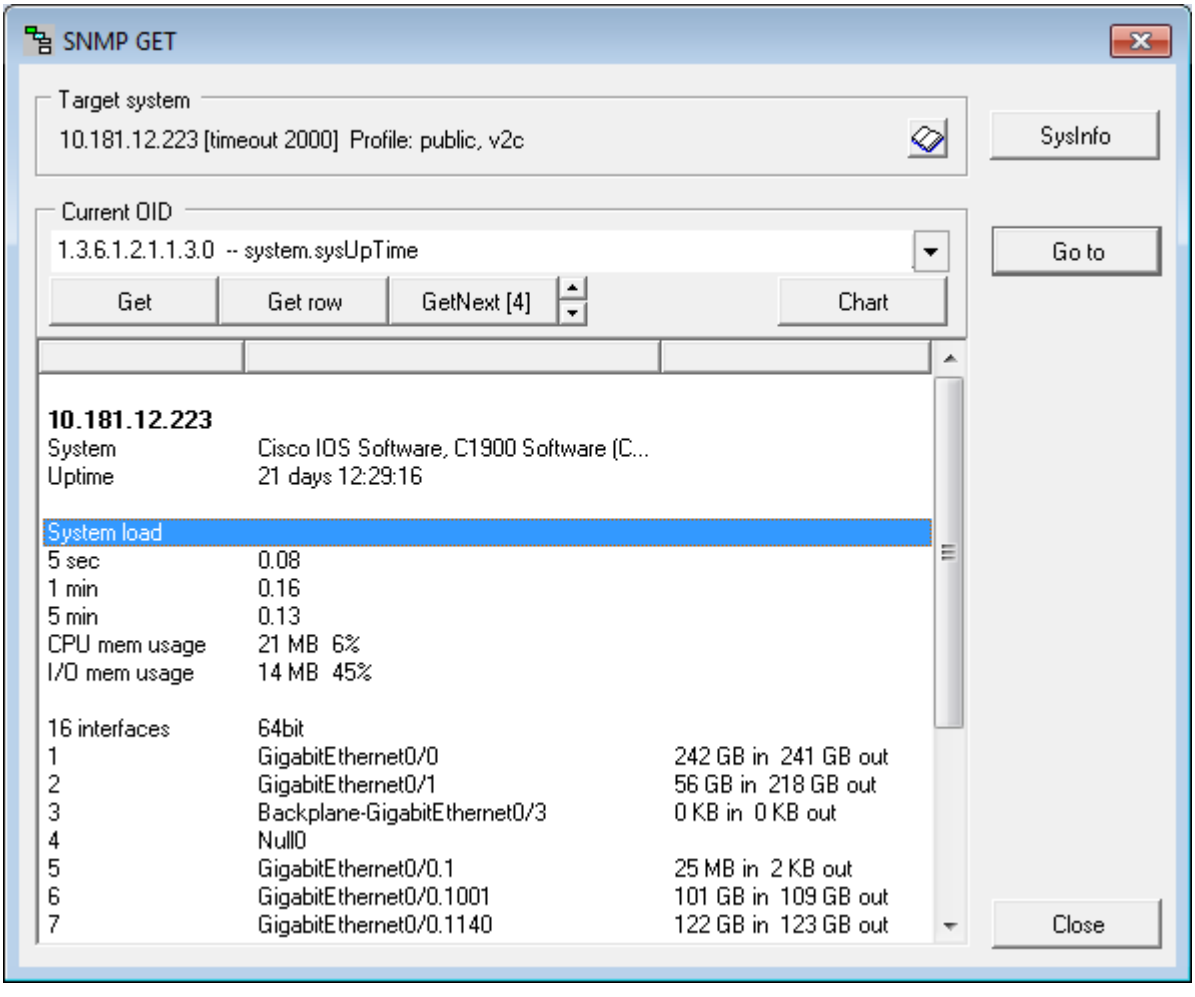
Chart
For a numeric counters you may use "Chart" function – display counter value as real-time charts.

Go to
Searches for last requested OID in the MIB tree, selects the counter and displays information about the variable.

Close
Simply closes "SNMP Get" window (returns focus to main window or chart window)

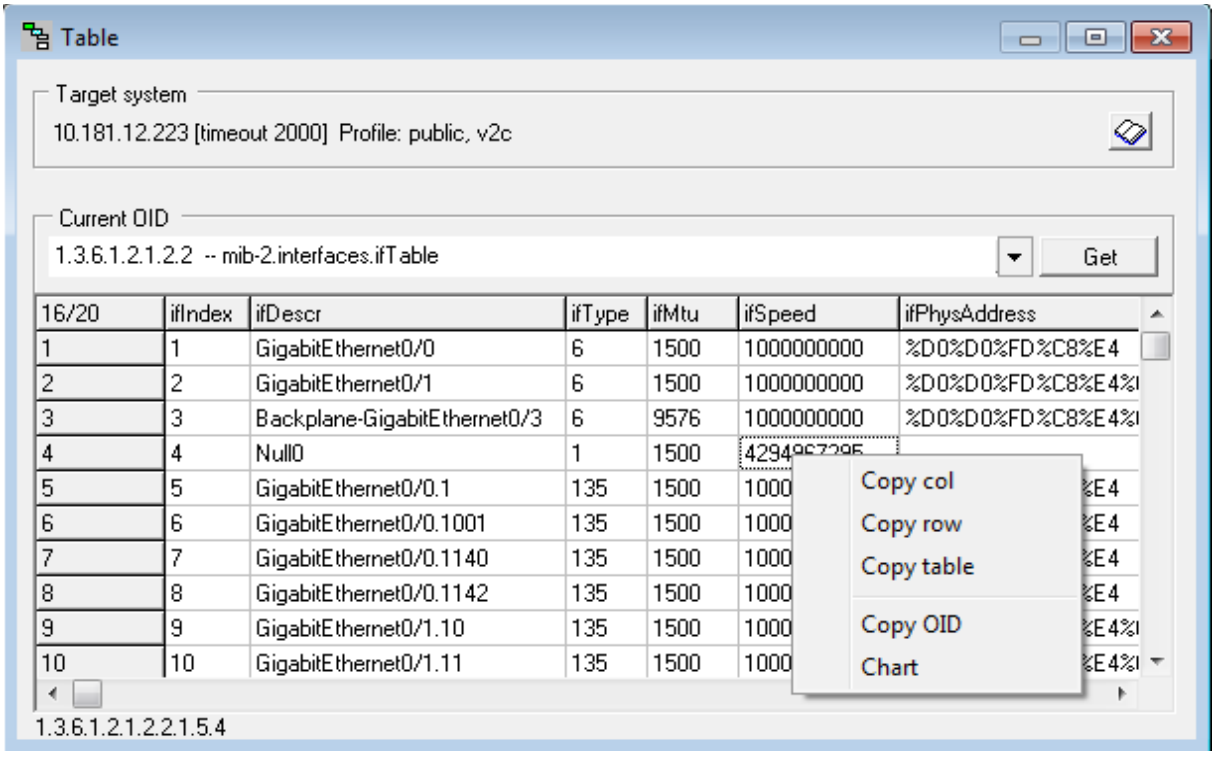
System info

This utility connects to target SNMP agent and retrieves up to date system information such us OS description, uptime, disk free space, memory usage, network interfaces.



Table

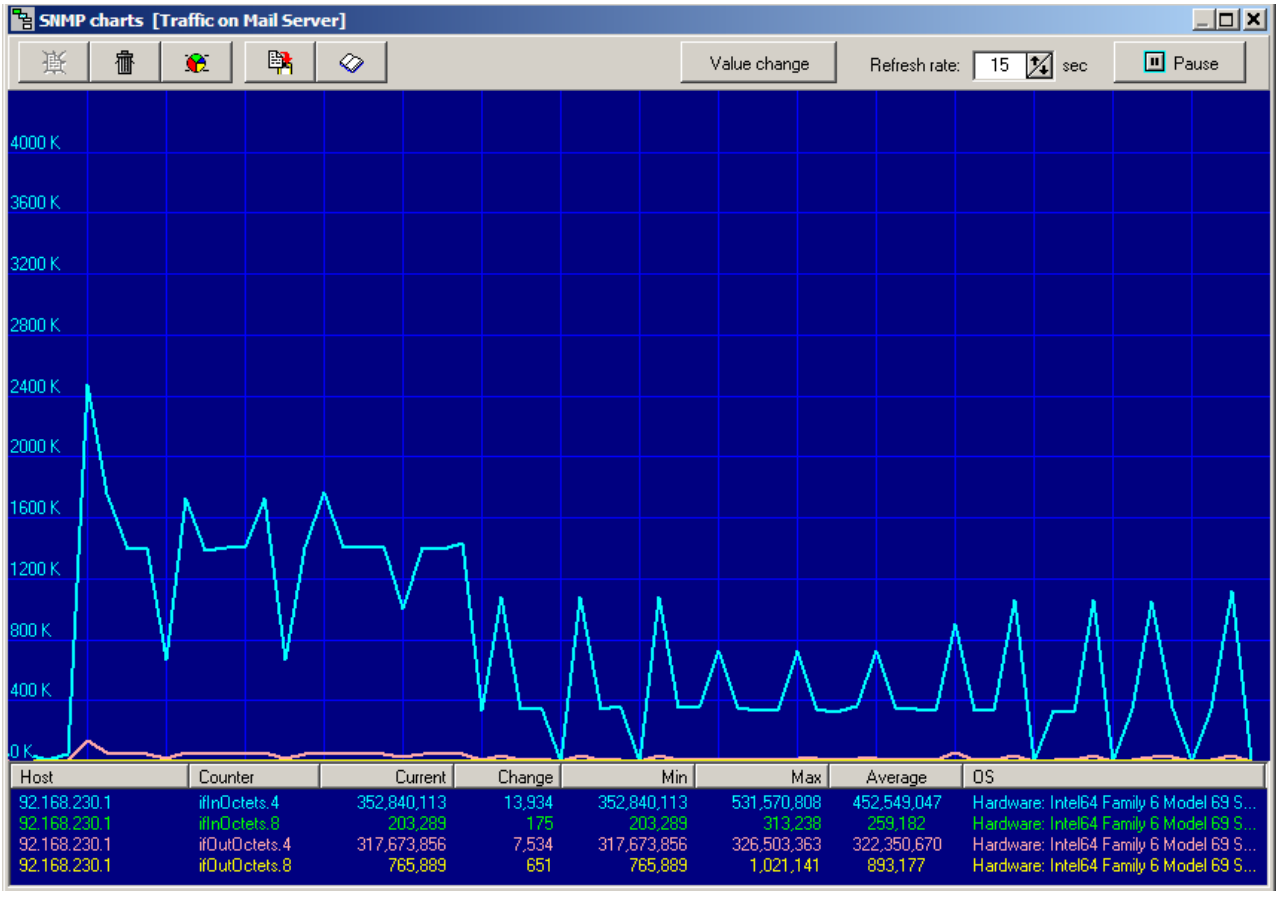
This MIB Browser utility connects to target SNMP agent and retrieves current values of all counters that belong to specified table. E.g. if you select ifTable element, MIB Browser will display detailed information about all network interfaces installed on target device, including interface description, physical address, speed, admin and operational status, total number of octets received on the interface, errors and so on.



Popup menu allows you to copy all fields within selected column or row into clipboard, copy entire table into clipboard, copy OID related to selected cell. For a numeric counters you may use “Chart” menu item – display counter value as real-time charts.

SNMP charts

This utility displays real-time charts for one or several counters (up to 4 counters). You can choose counters using main window, SNMP Get window or Table window. MIB Browser may monitor counters provided by one or several SNMP agents, e.g. you may see traffic on your server and your router at the same time.



You may set refresh rate, pause and resume monitoring, choose color palette, set one of the following visualization modes:

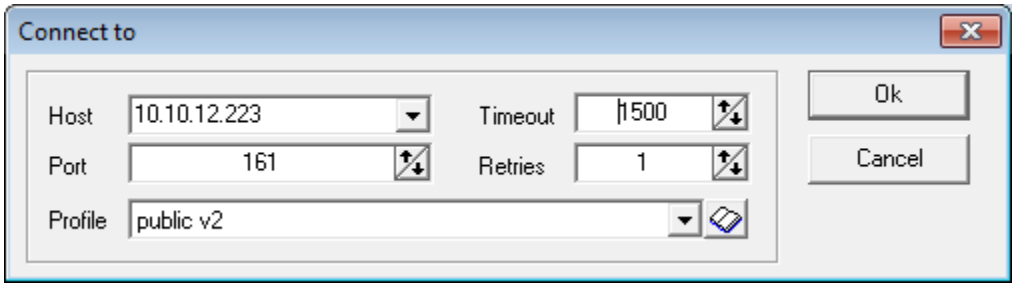
- Counter value
- Value change
- Value change /sec
- Percentage change

Also popup menu offers “Copy data” option – copies data into clipboard.

Save profiles / Load profiles

This option allows you to save current settings into file. MIB Browser stores list of counters, refresh rate, visualization mode. Then you may load stored profile at any time using “Load profiles” button or using main window menu View->Charts.

Target system



In order to connect to remote SNMP agent the following parameters should be specified:

Agent address
A string specifying either a dotted-decimal IP address or a host name that can be resolved to an IP address (e.g. 195.168.10.10).

Port
UDP port used by target SNMP agent (default port for SNMP requests 161)

Timeout
This is the amount of time in milliseconds the program will wait for a response from SNMP agent before the request fails.

Retries
Specifies the communications retry count.

SNMP Profile
Choose SNMP credentials profile

SNMP Credentials

SNMP Credentials dialog allows you to setup list of SNMP profiles (accounts). Profiles store login or community string and other information necessary for communication with SNMP agent.
For each profile you should specify name of the profile (your choice) and version of SNMP protocol used by SNMP agent. MIB Browser supports SNMP v1, v2c and v3.

Community
If SNMP agent uses SNMP v1 or v2c protocol, specify the SNMP community name (often SNMP agents use “public” as community string).

If SNMP agent is configured to use SNMP v3, you should specify the following parameters:

Username

Enter the username that is configured for the SNMP agent(s). An SNMP device, upon reception of a request, uses this username to look for configured authentication and encryption parameters and applies them to the received request message.

Context
Specify the context needed to identify specific SNMP instances. This parameter is optional.

Authorization
You may choose one of the following authorization methods: None (no authorization), MD5, SHA-1, SHA256, SHA384 or SHA512.
Only MD5 and SHA1 algorithms are defined in SNMP standards however many manufacturers use more strong "unofficial" SHA256/384/512 hashes.

Authorization password
If authorization is used, use this field to specify authorization password.

Privacy type
Specify encryption mode: None, DES, 3DES, AES128, AES192, AES256, AES192C, AES256C.
Note1: AES192, AES256, AES192C and AES256C are not defined in SNMP standards however many manufacturers use these algorithms.
Note2: AES192C and AES256C modes used by Cisco, they are equivalent to AES192/AES256 when SHA256, SHA384 or SHA512 authorization mode is used. We would not recommend to use MD5+AES192C/AES256C or SHA1+AES192C/AES256C.
Note3: we do not recommend DES or 3DES encryption mode. DES is not secure. 3DES slower and less secure than AES encryption.

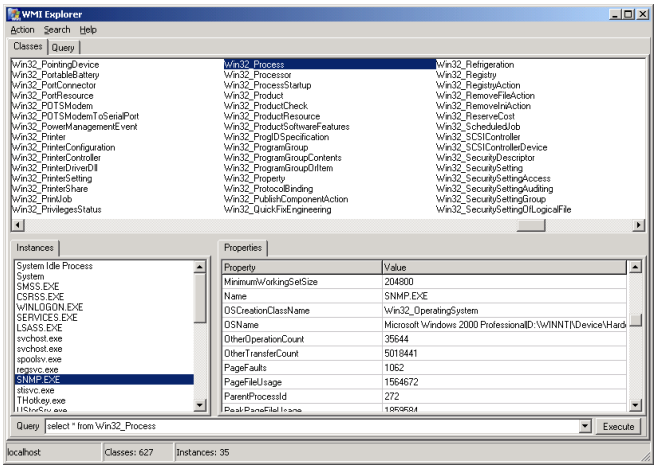
Privacy password
Specify key for encryption

Note:
When you install Advanced Host Monitor package, then all applications (MIB Browser, HostMonitor, DiskMeter, RCC) use the same set of SNMP Profiles stored in snmpacc.lst file. You may modify profiles using HostMonitor or RCC application. MIB Browser and DiskMeter does not allow modifications so operator without necessary rights cannot change profiles.

When MIB Browser (or DiskMeter) installed as standalone application, it allows SNMP credentials modification, profiles stored in snmpacc2.lst file.

WMI Explorer

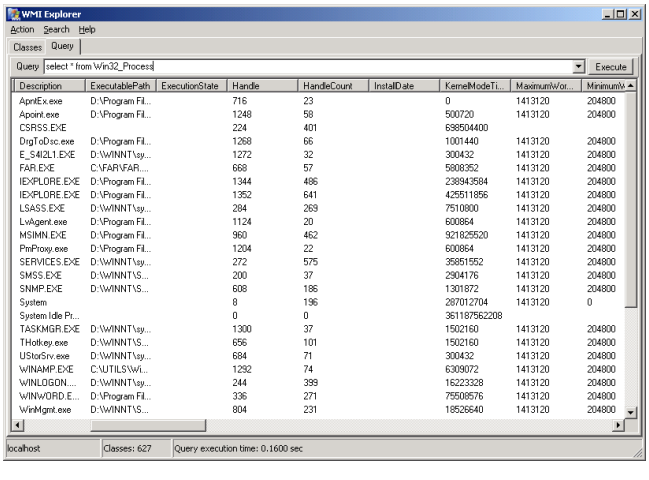
WMI Explorer is an auxiliary application for HostMonitor, however it can be used independently as well.



WMI is an acronym for **W**indows **M**anagement **I**nstrumentation. WMI is the Microsoft's implementation of Web-Based Enterprise Management (WBEM) - a new management technology that allows software to monitor and control managed resources throughout the network.
Such managed resources include hard drives, file systems, settings of operating system, processes, services, shares, registry settings, networking components, event logs, users, groups, etc.
WMI allows monitoring of performance counters as well. Microsoft applications such as Exchange and SQL Server have WMI built-in. Many non-Microsoft applications utilize WMI and thus they could be monitored using Advanced Host Monitor as well.
WMI is already built into Windows 2000 or above, and can be installed on any other 32-bit Windows system. See also:

- System requirements
- Known problems
- Microsoft WMI FAQ

WMI Explorer



Explorer allows you to

- Explore the full set of WMI management classes, objects and their properties
- Browse through objects and settings on remote machines
- Execute any WQL query and view the result set

WMI Explorer can be started as an independent application or it can be launched by HostMonitor to tune up a WMI test.
Once you have started WMI Explorer, you will be presented with two ways to explore a machine's objects:

The Classes (browser) view*

This view displays full set of classes within the specified namespace** (on local or remote machine), child objects and their properties.

Top portion of the main window shows all classes available on the system. In order to quickly find a class you may use “Search” menu. Menu item “Find” searches (using the name) for the specified class. Menu item “Search again” looks for the next suitable entry. If the search option “Match whole word only” is disabled, the search string might be found within longer words. E.g. consecutive searches for the string “_Process” will find CIM_*Process*, CIM_*Process*Executable, CIM_*Processs*or, CIM_*Process*Thread, Win32_*Process* and Win32_*Process*or items.

Instances

The Instances panel is located in the bottom-left portion of the main window. Every time you click on a class in Classes panel, WMI Explorer queries Windows and retrieves all instances (objects) of the selected class.

Please note: some classes have many instances, retrieving of information about them may require a lot of time and system resources. That is why WMI Explorer requests the target system in the background using dedicated thread. This allows the user to check properties or switch to another class while the request is still in progress. When request is completed, explorer shows the number of instances in the status line (if you see “Requesting instances...” in the status line, it means explorer have not yet finished retrieving the information).

Properties

The Properties panel is located in the bottom-right portion of the main window. Every time you click on a class in Classes panel, WMI Explorer queries Windows to retrieve the list of properties of the selected class. Even if there are no instances of the class, you will be able to see the list of its properties.

To view the property value for specific object, simply click the mouse on the object’s instance in Instances panel.

Note: If object property represents one-dimensional array with 4 or less elements, WMI Explorer will display array elements. If object property represents one-dimensional array with 5 or more elements, explorer will offer "Copy array values" popup menu item, it copies up to 512 elements of array into clipboard.

Methods

Here WMI Explorer can display methods of the selected class, also it shows parameters of each method. Popup menu allows you to copy method description into clipboard; sort methods alphabetically.

The Query view*

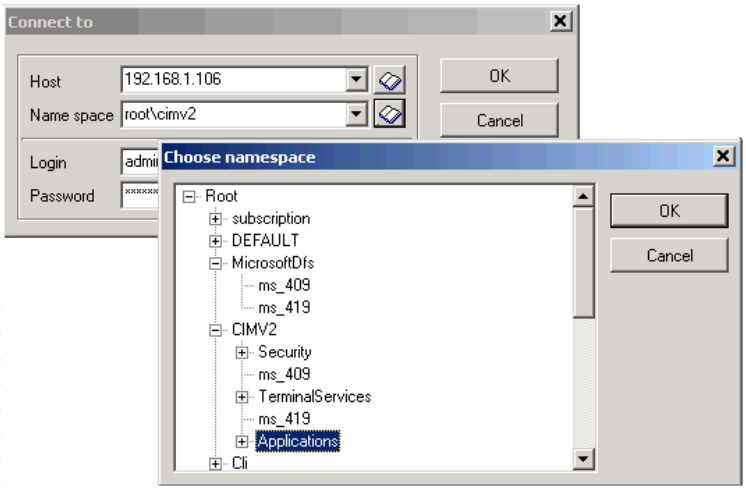
The Query View gives you the capability to run standard WMI Query Language (WQL) queries; each instance that's returned is listed in the Results window.

- E.g. if you want to monitor the number of handles used by all running instances of the Internet Explorer, use the query like this: `SELECT HandleCount FROM Win32_Process WHERE name='iexplore.exe'`
- If you need to monitor the number of processes which use more than 10 threads, use the following query: `SELECT ThreadCount FROM Win32_Process WHERE ThreadCount>10`
- The query: `SELECT * FROM Win32_Service WHERE Started=0 AND StartMode="Auto"` shows all services which have not started and have the start mode configured to “Automatic”.

Query window is an invaluable resource for those who know where to look for something but need to see what exactly is returned by Windows API to HostMonitor.
If you are running HostMonitor and you already have configured some "WMI" test items, you may click the right mouse button on the test item and choose "Explore WMI" item from the popup menu. When you do so, HostMonitor will start WMI Explorer in the Query mode, passing the query and information about the target host (such as the hostname, name space, login, etc) to the explorer. This allows you to check quickly hardware and software parameters on the target system and instantly see what is going on (e.g. why the test item has been failed).

*To switch between views, click on their respective tabs at the top of the main window. You can do it at anytime since views are absolutely independent.

Connecting to remote host



WMI Explorer allows you to request both local (the system where explorer is running) and remote systems. To connect to the remote system you may use GUI or command line parameters.

GUI:

If you already have started explorer and you need to connect to another system, use menu "Action" -> "Connect to remote host". In the connection dialog you should specify the hostname and WMI name space** (default is root\cimv2); optionally you may provide the login name and password.

Also you may set authentication level using one of the following options:

- Default
  Tells DCOM to choose the authentication level by using its normal security blanket negotiation (note: it will never choose an authentication level of None).
- None
  No authentication is performed during the communication between client and server. All security settings are ignored.
- Connect
  The normal authentication handshake occurs between the client and server, and a session key is established but that key is never used for communication between the client and server. All communication after the handshake is insecure.
- Call
  Only the headers of the beginning of each call are signed. The rest of the data exchanged between the client and server is neither signed nor encrypted. Most SSPs do not support this authentication level and silently promote it to Packet.

- Packet
  The header of each packet is signed but not encrypted. The packets themselves are not signed or encrypted.
- Packet Integrity

  Each packet of data is signed in its entirety but is not encrypted. Because all of the data is signed by the sender, the recipient can be certain that none of the data has been tampered with during transit.
- Packet Privacy

  Each data packet is signed and encrypted. This helps protect the entire communication between the client and server.

Command line:

You may specify connection parameters in command line so that WMI Explorer connects to specified system right after startup.

Format of the command line:

>wmiexplorer.exe [-host:<hostname>] [-namespace:<namespace>] [-authlevel:0..6]
[-user:<username>] [-pswd:<password>] [-query:<WQL query>]

Examples:

```
>wmiexplorer.exe "-host:primarywebserv" "-namespace:root\cimv2" "-user:admin" "-pswd:secret words"
>wmiexplorer.exe "-query: select * from Win32_Process"
```

**Note: WMI namespace is a container grouping child objects related to one another in some way. A namespace contains a hierarchy of classes and associations which define either a machine's object or the relationship between two or more objects. The most commonly used namespace is CIMV2 (Common Information Model Version 2.)

See also: "Known problems"

System requirements

The following versions of Windows **do** have the WMI pre-installed:

- Windows ME
- Windows 2000
- Windows XP
- Windows 2003
- Windows Vista
- Windows 7, 8, 10, 11
- Windows Server 2008
- Windows Server 2012
- Windows Server 2016

- Windows Server 2019
- Windows Server 2022

These systems **do not** have the WMI pre-installed:

- Windows 95
- Windows 98
- Windows NT

The WMI Core software package for Windows 95, 98, and Windows NT 4.0 available at Microsoft's web site.
Please note: WMI CORE for Windows 95/98/NT requires Microsoft Internet Explorer version 5 or later.

Known problems

OS: Windows XP SP2

Problem: built-in firewall may block WMI requests from remote systems

In order to remotely administer a Windows XP SP2 machine using WMI, you will need to configure the built-in firewall. If the Windows firewall is enabled and if it hasn't been configured to accept a WMI connection, WMI Explorer (and HostMonitor) will not be able to connect to the system. In such case, HostMonitor shows "The RPC Server is unavailable" error.

To configure Windows XP firewall to accept WMI connections, you need to enable the "Allow remote administration exception" group policy entry. This setting can either be configured on the local group policy of a machine or globally by configuring the global Group Policy settings of an Active Directory domain.

OS: Windows 95/98/NT

Problem: winmgmt.exe does not start automatically on such systems

If you want to monitor such Windows 95/98/NT using WMI, you should install WMI Core software package **AND** perform the following steps

- enable DICOM (set HKLM\SOFTWARE\Microsoft\OLE\EnableDCOM to "Y")
- enable remote connections (set HKLM\SOFTWARE\Microsoft\OLE\EnableRemoteConnect to "Y")
- set HKLM\SOFTWARE\Microsoft\WBEM\CIMOM\AutoStartWin9x to 2
- add link to the Winmgmt.exe file into the Startup directory

OS: Windows 2000-2019

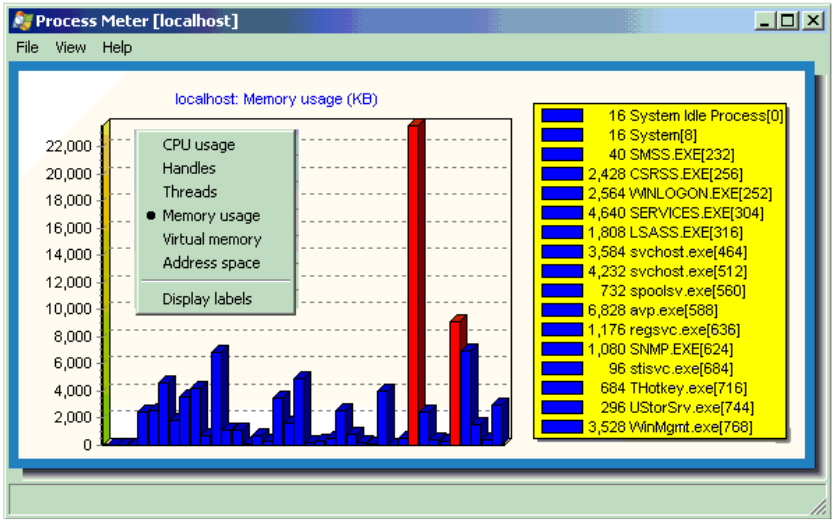
Problem: If application displays "Class ISWbemLocator is not registered" error, it is most likely that there is system registry problem. The following article shows how to fix a corrupted WMI repository and how to register the WMI components: Rebuilding the WMI Repository

Other useful links:

- WMI Troubleshooting Tips by Yvette O'Meally at techcommunity.microsoft.com
- How to troubleshoot "Access is denied" error at social.technet.microsoft.com
- WMI Troubleshooting Tips at docs.microsoft.com
- If you are receiving "This schema for this assembly has not been registered with WMI" error, there is hotfix available from Microsoft

Process Meter

Process Meter is an auxiliary application for HostMonitor, however it can be used independently as well.



Process Meter displays chart with information about all processes running on local or remote system. It may show the following information for each process:

- CPU usage
- Handles
- Threads
- Memory usage
- VM size
- Address space usage

Each process represented by a bar; red colored bar indicates process that uses resources over specified limit. You may specify limits using menu View → Set limits. When you are using HostMonitor to start Process Meter, HostMonitor sets resource usage limit using test properties (Dominant Process test).
You may click on the bar to see detailed process information.

menu **File**

Target host	-	this menu item allows you to specify target host connection parameters
Copy image to Clipboard	-	copies the chart as an image into the clipboard
Save to File	-	saves an image of the chart as a bitmap or WMF (Windows Meta File)
Print	-	brings up Print Preview dialog and allows you to print the chart
Exit	-	closes application

menu **View**

CPU usage	-	shows amount of CPU time (%) used by each process. If there are several CPUs installed on the system, CPU load can be over 100%.
Handles	-	this menu item tells the application to show the total number of handles currently open by the processes. Handles number is the sum of the handles currently open by each thread in the process.
Threads	-	tells ProcessMeter to show the number of threads currently active in each process. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. Every running process has at least one thread.
Memory usage	-	shows the current number of kilobytes (KB) in the Working Set of the processes. The Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the

	computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed they will then be soft-faulted back into the Working Set before they leave main memory.
VM size	- this menu item tells the application to show the current size in kilobytes (KB) of pages allocated that are only accessible to the process.
Address space	- shows current size of the virtual address space that processes are using, not the physical or virtual memory actually used by the process. Use of virtual address space does not necessarily imply corresponding use of either disk or main memory pages. Virtual space is finite, and by using too much, the process might not be able to load libraries.
Refresh	- tells Process Meter to collect up-to-date information from target system and update the chart.
Auto refresh ON	- using this menu item you may setup Process Meter to update the chart on regular basis, e.g. every 5 sec.
Auto refresh OFF	- use this menu to disable "auto refresh" option.
Display labels	- turns on/off chart labels. Label - a mark near a bar on the chart. A mark consist of a colored rectangle with a process name on it and a line that indicates which bar corresponds to which mark. Note: when you point mouse cursor on some bar, Process Meter will display corresponding process name in the status bar (regardless of "Display labels" option).
Set limits	- brings up "Set limits" dialog window. Using this dialog you may setup threshoulds separately for each "view" mode. Process Meter will show red colored bar when a process uses resources over specified limit. E.g. you may setup application to use red color when a process uses more than 30% CPU, more than 1100 handles or more than 90,000 KB of memory.

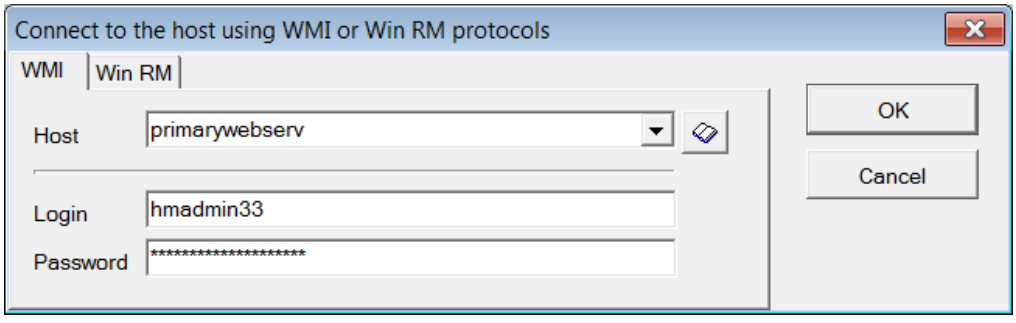
Process Meter can be started as an independent application or it can be launched by HostMonitor: Dominant Process and Process test methods offer "Process Meter" popup menu item that allows you to launch application to check specified system. In such case HostMonitor sends test parameters to Process Meter.

Connecting to remote host

Process Meter allows you to request local (the system where application is running) and remote systems. To connect to the remote system you may use GUI or command line parameters.

GUI:
If you have already started Process Meter and you need to connect to another system, use menu "File" → "Target host". Then choose protocol: WMI or WinRM

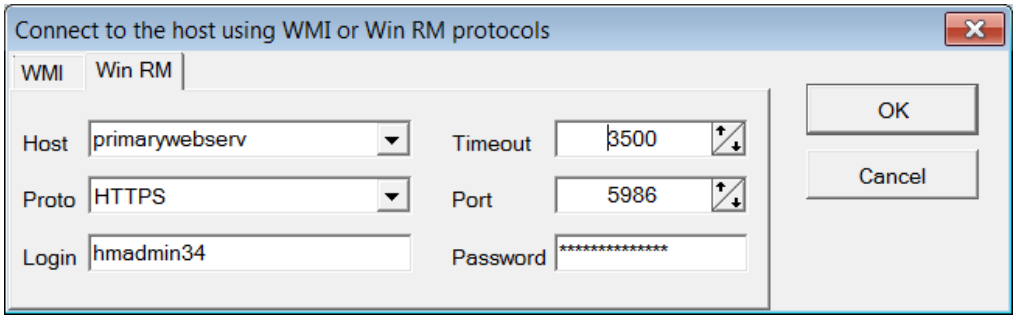
WMI: Windows Management Instrumentation is the Microsoft's implementation of Web-Based Enterprise Management.



Please set the following options:

Host	a string specifying either a dotted-decimal IP address or a host name
Login	this parameter allows you to specify account that should be used for connection with remote system
Password	provide password for specified account

WinRM
Windows Remote Management (WinRM) uses the WS-Management protocol, it transfers requests over the network using SOAP (Simple Object Access Protocol) messages sent over standard web protocols



Please set the following options:

Host	a string specifying either a dotted-decimal IP address or a host name
Timeout	the amount of time in milliseconds the program will wait for a response from target system before the request fails
Proto	select HTTP (unencrypted) or HTTPS transport protocol
Port	specify the TCP port number on which target system is listening for incoming WinRM requests
Login	this parameter allows you to specify account that should be used for connection with remote system
Password	provide password for specified account

Command line:
You may specify connection parameters in command line so that Process Meter connects to specified system right after startup.

Format of the command line for WMI connections:

```
>processmeter.exe  -host:<hostname>  [-user:<username>]  [-pswd:<password>]
[-mode:<mode>]  [-limit:<limit>]
```

Format of the command line for WinRM connections:

```
>processmeter.exe  -host:http[s]://<hostname>  [-port:<portnumber>]  [-timeout:<timeout>]
[-user:<username>]  [-pswd:<password>]  [-mode:<mode>]  [-limit:<limit>]
```

Where

<hostname> - host name or IP address of the destination host. If this parameter is not specified, application will check local system

<username> - this parameter allows you to specify account that should be used for connection with remote system

<password> - password for connection. If password contains space character(s), use quotation marks to wrap parameter

<mode> - one of the following strings:
cpu
handles
threads
memory
vmem
addrspace

<limit> - using this parameter you may setup threshould for specified "view" mode (see "-mode" parameter). Process Meter will show red colored bar when a process uses resources over specified limit. Note: when you are using "memory", "vmem" or "addspace" mode, limit is specified in KB (e.g. "-limit:5000" sets threshold to 5,000 KB)

<portnumber> - specify the TCP port number on which target system is listening for incoming WinRM requests

<timeout> - the amount of time in milliseconds the program will wait for a response from target system before the request fails

Examples:

```
processmeter.exe -host:primwebserv "-user:admin" "-pswd:secret 1" -mode:handles -limit:550
processmeter.exe -host:https://primwebserv "-user:adminw"  -port:5986  -timeout:3000
processmeter.exe -mode:vmem -limit:50000
processmeter.exe -mode:memory
```

Known problems

OS: Windows XP SP2

Problem: built-in firewall may block Process Meter requests from remote systems
In order to remotely monitor a Windows XP SP2 machine, you will need to configure the built-in firewall. If the Windows firewall is enabled and if it hasn't been configured to accept a WMI connection, Process Meter (and HostMonitor) will not be able to connect to the system. In such a case, HostMonitor shows "The RPC Server is unavailable" error.

To configure Windows XP firewall to accept WMI connections, you need to enable the "Allow remote administration exception" group policy entry. This setting can either be configured on the local group policy of a machine or globally by configuring the global Group Policy settings of an Active Directory domain.

OS: Windows 95/98/NT

Problem: winmgmt.exe does not start automatically on such systems. If you want to monitor Windows 95/98/NT systems, you should install WMI Core software package AND perform following steps:

- enable DICOM (set HKLM\SOFTWARE\Microsoft\OLE\EnableDCOM to "Y")
- enable remote connections (set HKLM\SOFTWARE\Microsoft\OLE\ EnableRemoteConnect to "Y")
- set HKLM\SOFTWARE\Microsoft\WBEM\CIMOM\AutoStartWin9x to 2
- add link to the Winmgmt.exe file into the Startup directory

OS: Windows 2000-2019

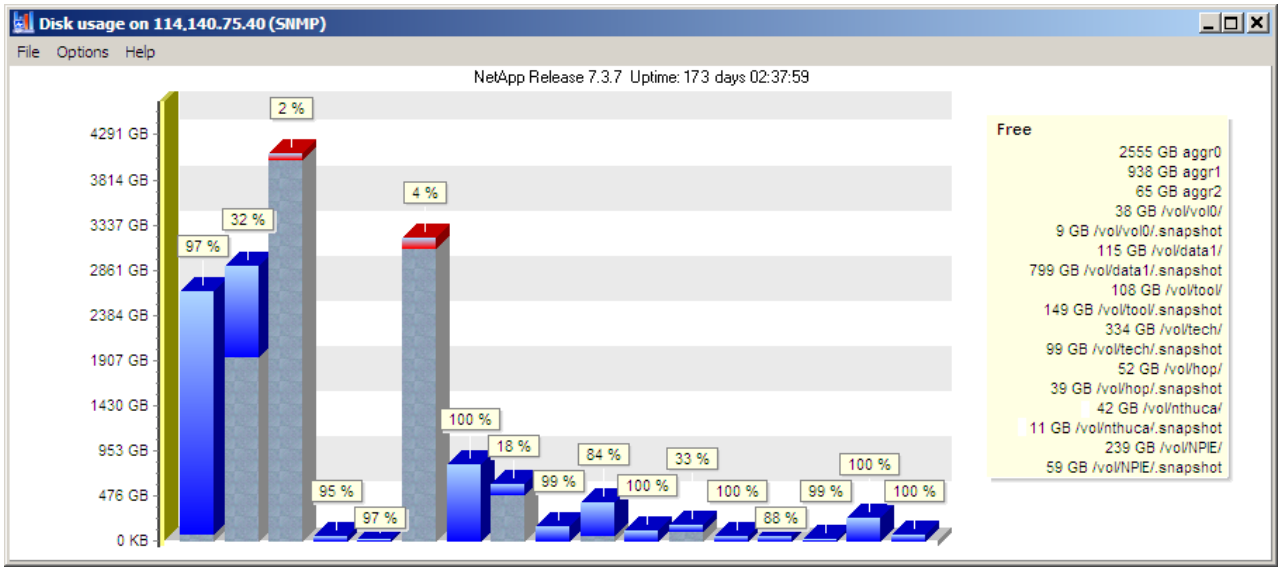
Problem: Process Meter shows "Class ISWbemLocator is not registered" error
If application returns such an error, it is most likely that there is system registry problem. The following article shows how to fix a corrupted WMI repository and how to register the WMI components: Rebuilding the WMI Repository

Other useful links:

- WMI Troubleshooting Tips by Yvette O'Meally at techcommunity.microsoft.com
- How to troubleshoot "Access is denied" error at social.technet.microsoft.com
- WMI Troubleshooting Tips at docs.microsoft.com
- If you are receiving "This schema for this assembly has not been registered with WMI" error, there is hotfix available from Microsoft

Disk Meter

Disk Meter is an auxiliary application for HostMonitor, however it can be used independently as well.



Disk Meter displays chart with information about all disk drives mounted on local or remote system. Each disk represented by a bar; red colored bar indicates disk with free space below 5% (unless you set custom free space limit).
When you are using HostMonitor to start Disk Meter, HostMonitor sets minimum free space limit using Drive Free Space test properties.

DiskMeter can connect to remote system using WMI, WinRM or SNMP protocol and retrieve data from various systems:

- Windows
- FreeBSD
- Linux
- AIX
- ESXi
- Solaris
- NetApp NAS

NetApp related notes:

DiskMeter may show negative free space for snapshots, when shapshot too big and uses active file system space. Snapshot copy reserve sets a specific percent of the disk space for storing Snapshot copies. If the Snapshot copies exceed the reserve space, they spill into the active file system and this process is called Snapshot spill.

NetApp recommends: The Snapshot copy reserve must have sufficient space allocated for the Snapshot copies. If the Snapshot copies exceeds the reserve space, you must delete the existing Snapshot copies from the active file system to recover the space, for the use of the file system. You can also modify the percent of disk space that is allotted to Snapshot copies.

Menu

menu **File**		
Target host	-	this menu item allows you to specify connection parameters for remote system monitoring
Copy image to Clipboard	-	copies the chart as an image into the clipboard
Save to File	-	saves an image of the chart as a bitmap or WMF (Windows Meta File)
Print	-	brings up Print Preview dialog and allows you to print the chart
Exit	-	closes application

menu **Options**		
Refresh	-	tells Disk Meter to collect up-to-date information from target system and update the chart.
Auto refresh ON	-	using this menu item you may setup Disk Meter to update the chart on regular basis, e.g. every 120 sec (2 min).
Auto refresh OFF	-	use this menu to disable "auto refresh" option.
Display labels	-	turns on/off chart labels

Help		
Help	-	displays Help
Home page	-	starts default web browser, opens home page of the Disk Meter on www.ks-soft.net
Support	-	allows you to send e-mail to our tech support staff
About	-	about Disk Meter

Disk Meter can be started as an independent application or it can be launched by HostMonitor: Drive Free Space test method offers "Disk Meter" popup menu item that allows you to launch application to check specified system.

HostMonitor/RCC GUI automatically sets the protocol and the settings depending on the corresponding test settings and Connection Manager entries.

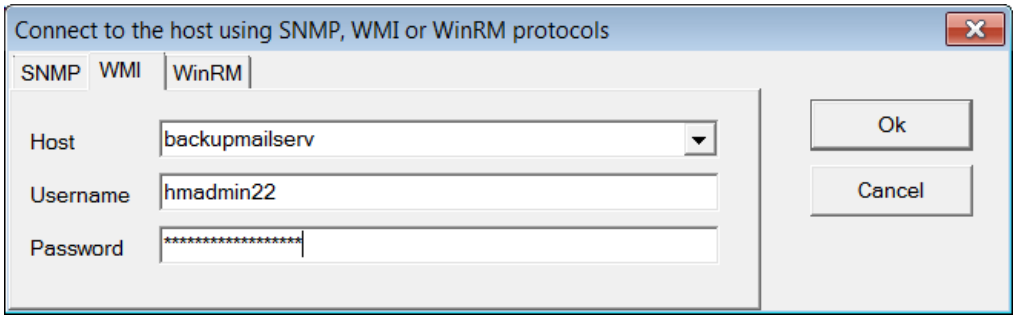
Target system

Disk Meter allows you to request local and remote systems. To connect to the remote system you may use GUI or command line parameters.

Connecting to remote host using GUI

If you have already started Disk Meter and you need to connect to another system, use menu "File" -> "Target host". Then choose protocol: SNMP, WMI or WinRM

WMI: Windows Management Instrumentation is the Microsoft's implementation of Web-Based Enterprise Management. DiskMeter can connect to remote Windows systems using WMI protocol.

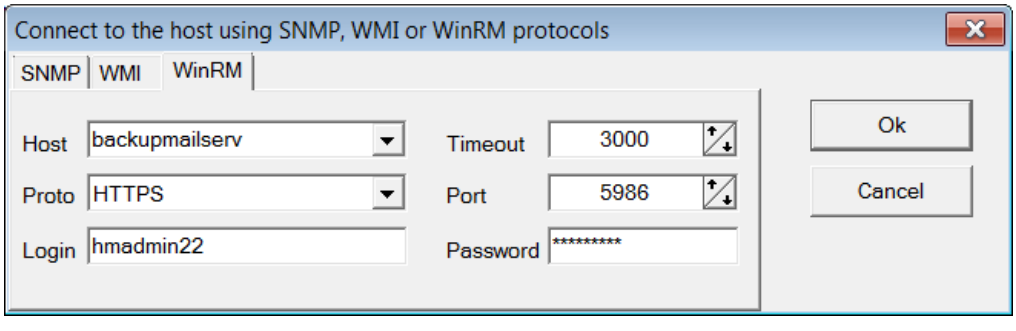


Please set the following options:

Host	a string specifying either a dotted-decimal IP address or a host name
Username	this parameter allows you to specify account that should be used for connection with remote system
Password	provide password for specified account

WinRM

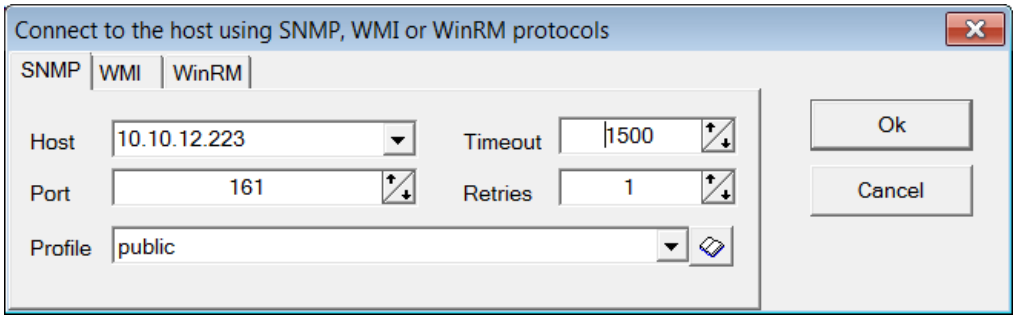
Windows Remote Management (WinRM) uses the WS-Management protocol, it transfers requests over the network using SOAP (Simple Object Access Protocol) messages sent over standard web protocols



Please set the following options:

Host	a string specifying either a dotted-decimal IP address or a host name
Timeout	the amount of time in milliseconds the program will wait for a response from target system before the request fails
Proto	select HTTP (unencrypted) or HTTPS transport protocol
Port	specify the TCP port number on which target system is listening for incoming WinRM requests
Login	this parameter allows you to specify account that should be used for connection with remote system
Password	provide password for specified account

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). Using SNMP protocol Disk Meter can retrieve data from various Windows and UNIX systems, also it can check NetApp NAS devices



Set the following options:

Host	a string specifying either a dotted-decimal IP address or a host name that can be resolved to an IP address (e.g. 195.168.10.10)
Port	specify the port number on which target SNMP agent is listening for incoming requests (by default SNMP agents use port 161)
Timeout	this is the amount of time in milliseconds the program will wait for a response from target system before the request fails
Retries	specifies the communications retry count
Profile	Choose SNMP credentials profile

SNMP Credentials

SNMP Credentials dialog allows you to setup list of SNMP profiles (accounts). Profiles store login or community string and other information necessary for communication with SNMP agent.
For each profile you should specify name of the profile (your choice) and version of SNMP protocol used by SNMP agent. Disk Meter supports SNMP v1, v2c and v3.

Community

If SNMP agent uses SNMP v1 or v2c protocol, specify the SNMP community name (often SNMP agents use “public” as community string).

If SNMP agent is configured to use SNMP v3, you should specify the following parameters:

Username
Enter the username that is configured for the SNMP agent(s). An SNMP device, upon reception of a request, uses this username to look for configured authentication and encryption parameters and applies them to the received request message.

Context
Specify the context needed to identify specific SNMP instances. This parameter is optional.

Authorization
You may choose one of the following authorization methods: None (no authorization), MD5, SHA-1, SHA256, SHA384 or SHA512.
Only MD5 and SHA1 algorithms are defined in SNMP standards however many manufacturers use more strong "unofficial" SHA256/384/512 hashes.

Authorization password
If authorization is used, use this field to specify authorization password.

Privacy type
Specify encryption mode: None, DES, 3DES, AES128, AES192, AES256, AES192C, AES256C.
Note1: AES192, AES256, AES192C and AES256C are not defined in SNMP standards however many manufacturers use these algorithms.
Note2: AES192C and AES256C modes used by Cisco, they are equivalent to AES192/AES256 when SHA256, SHA384 or SHA512 authorization mode is used. We would not recommend to use MD5+AES192C/AES256C or SHA1+AES192C/AES256C.
Note3: we do not recommend DES or 3DES encryption mode. DES is not secure. 3DES slower and less secure than AES encryption.

Privacy password
Specify key for encryption

Note:
When you install Advanced Host Monitor package, then all applications (MIB Browser, HostMonitor, DiskMeter, RCC) use the same set of SNMP Profiles stored in snmpacc.lst file. You may modify profiles using HostMonitor or RCC application. MIB Browser and DiskMeter does not allow modifications so operator without necessary rights cannot change profiles.

When DiskMeter (or MIB Browser) installed as standalone application, it allows SNMP credentials modification, profiles stored in snmpacc2.lst file.

Connecting to remote host using command line parameters

You may specify connection parameters in the command line, this way Disk Meter connects to specified system right after startup.
Format of the command line for local system:
diskmeter.exe [-limit:<limit>]

Format of the command line for WMI connections:
diskmeter.exe -host:<hostname> -user:<username> [-pswd:<password>] [-limit:<limit>]

Format of the command line for WinRM connections:
diskmeter.exe -host:http[s]://<hostname> [-port:<portnumber>] -user:<username> [-pswd:<password>] [-limit:<limit>]

Format of the command line for SNMP connections:
diskmeter.exe -host:<hostname> [-port:<portnumber>] [-timeout:<timeout>] [-retitries:<retries>] [-snmpver:<version>] [-community:<community>] [-limit:<limit>]

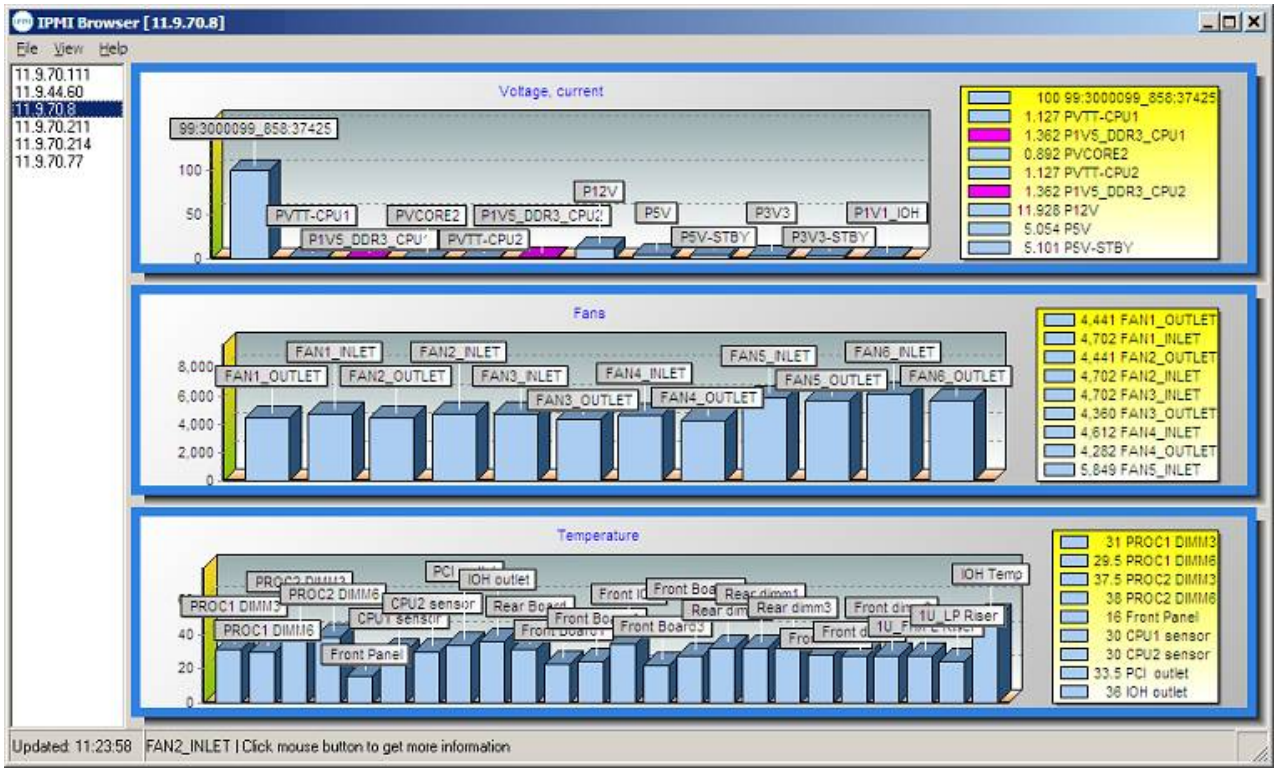
<hostname>	- host name or IP address of the destination host
<limit>	- using this parameter you may setup free space threshould. Disk Meter will show red colored bar when free space on some disk falls below specified limit. If you specify limit using number from 0 to 100, then Disk Meter will check free space percentage. if you specify limit using number plus suffux (K, M, G or T) then Disk Meter will check free space using KB, MB, GB or TB units. E.g. -limit:**5** (5% limit), -limit:**500M** (500 MB limit), -limit:**20G** (20 GB limit), -limit:**2T** (2 TB limit)
WMI/WinRM mode	
<username>	- this parameter allows you to specify account that should be used for connection with remote system
<password>	- provide password for specified account. If password contains space characters, use quotation marks to wrap parameter
SNMP mode	
<portnumber>	- specify the port number on which target SNMP agent is listening for incoming requests (default port 161)
<timeout>	- amount of time in milliseconds the program will wait for a response from target system before the request fails
<retries>	- specifies the communications retry count (default 1)
<version>	- choose SNMP protocol version supported by target system: 1 or 2 (default version 2c)
<community>	- specify the SNMP community name used for communication with the target device (default "public")

Examples:

```
diskmeter.exe  -host:112.20.1.55  "-user:admin" "-pswd:secretword"  -limit:8
diskmeter.exe  -host:https://112.20.1.55  "-user:admin" "-pswd:secretword"  -limit:8
diskmeter.exe  -host:10.10.1.90  -snmpver:2 -community:readonly  -limit:500M
diskmeter.exe  -host:10.10.1.90  -port:161 -timeout:2000 -community:readonly
```

IPMI Browser

IPMI (Intelligent Platform Management Interface) is a set of computer interface specifications for out-of-band management of computer systems. IPMI subsystem works independently of the host CPU, firmware and operating system. IPMI provides a way to manage a computer that may be powered off or otherwise unresponsive by using a network connection to the hardware rather than to an operating system.
A wide range of servers from leading manufacturers such as IBM, Lenovo, Dell, HPE, Supermicro support IPMI either through a dedicated management interface or through a shared LAN and provide the ability to remotely reboot a frozen server, monitor for hardware failures, access firmware sensors and logs.



Youtube demo

IPMI Browser retrieves data from remote servers using IPMI protocol, shows charts with temperature sensors, voltage, current and fans speed. Also you may check all available counters (e.g. disk status, memory errors) with details: value, lower and upper thresholds, critical and non-repairable thresholds; export data into text file and more.

Main menu

File		
Target host	-	this menu item allows you to specify connection parameters for remote system monitoring
Copy image to clipboard	-	copies the charts as an image into the clipboard
Copy data to clipboard	-	copies list of all counters with details (value, status, threshoulds, etc) into clipboard
Exit	-	closes application

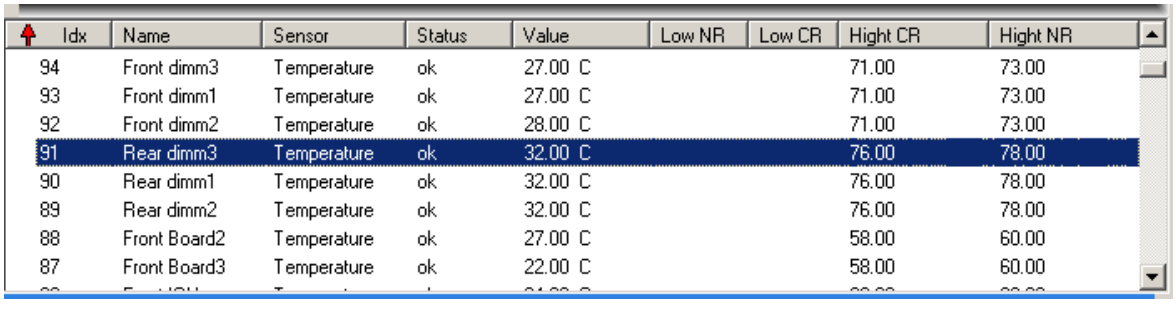
Options		
Show all counters	-	opens/closes Details panel
Refresh	-	tells IPMI Browser to collect up-to-date information from target system and update the chart
Auto refresh ON	-	using this menu item you may setup IPMI Browser to update the charts on regular basis, e.g. every 30 sec
Auto refresh OFF	-	use this menu to disable "auto refresh" option
Display labels	-	turns on/off chart labels

Help		
Help	-	displays Help
Home page	-	starts default web browser, opens home page of the IPMI Browser on www.ks-soft.net
Support	-	allows you to send e-mail to our tech support staff using your default mail client
About	-	about IPMI Browser

IPMI Browser can be started as an independent application or it can be launched by HostMonitor: IPMI related test methods (e.g IPMI Health) offer "IPMI Browser" pop up menu item that allows you to check target system.

Details

This pane shows all available counters (including counters not displayed on the charts, like Drive Slot counters, Firmware status and more). You may open it using F3 hot-key or by clicking on any item on the chart (in this case browser will scroll list to the selected item). Press ESC or F3 key again in order to close Details pane.



Idx	Name	Sensor	Status	Value	Low NR	Low CR	Hight CR	Hight NR
94	Front dimm3	Temperature	ok	27.00 C			71.00	73.00
93	Front dimm1	Temperature	ok	27.00 C			71.00	73.00
92	Front dimm2	Temperature	ok	28.00 C			71.00	73.00
91	Rear dimm3	Temperature	ok	32.00 C			76.00	78.00
90	Rear dimm1	Temperature	ok	32.00 C			76.00	78.00
89	Rear dimm2	Temperature	ok	32.00 C			76.00	78.00
88	Front Board2	Temperature	ok	27.00 C			58.00	60.00
87	Front Board3	Temperature	ok	22.00 C			58.00	60.00

Idx	Index of the sensor
Name	This item displays the sensor name
Sensor	Type of the sensor, e.g. Temperature, Voltage, Processor, Power supply, Memory, Fan, etc
Status	Status of the sensor item. IMPI Browser calculates status based on type of the sensor, value and thresholds
Value	This item displays the reading of the sensor
Low NR	Low Non-Recoverable threshold. Any item with a reading below this point will not be recovered
Low CT	Low Critical-Threshold. Any item with a reading below this threshold is in a critical state
High CT	High Critical-Threshold. Any item with a reading above this threshold is in a critical state
High NR	High Non-Recoverable threshold. Any item with a reading above this point will not be recovered

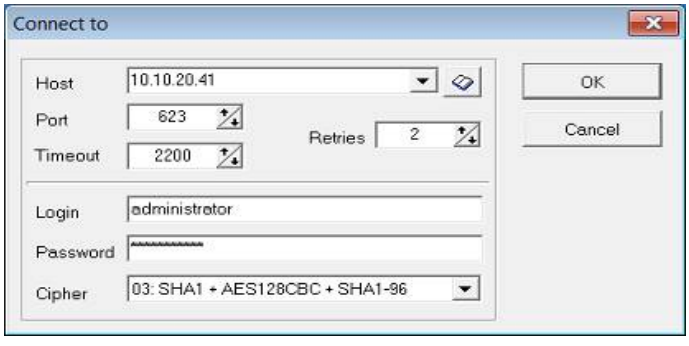
You may change the sorting order by clicking on a columns header. A second click on the column header switches between ascending and descending sorting modes.

You may copy entire list (Ctrl+C) into clipboard or select some items and use popup menu to copy selected rows.

In order to connect to the remote system you may use GUI or command line parameters.

Connecting to the remote host using GUI

You may connect to another system using menu "File" -> "Target host"



Please set the following parameters:

Host	a string specifying either a dotted-decimal IP address or a host name that can be resolved to an IP address (e.g. 195.168.10.10)
Port	set the port number on which target host is listening for incoming requests (default IPMI port: 623)
Retries	the communications retry count
Timeout	the amount of time in milliseconds the program will wait for a response from target system before the request fails
Username	provide account that should be used for connection with the remote system
Password	provide password for the specified account
Cipher	choose cipher mode (set of authentication, integrity and encryption algorithms)

The following cipher modes are supported
00: None
01: RAKP-HMAC-SHA1
02: RAKP-HMAC-SHA1 + HMAC-SHA1-96
03: RAKP-HMAC-SHA1 + AES128CBC + HMAC-SHA1-96
15: RAKP-HMAC-SHA256
16: RAKP-HMAC-SHA256 + HMAC-SHA256-128
17: RAKP-HMAC-SHA256 + AES128CBC + HMAC-SHA256-128

Also IPMI Browser displays list of previously visited servers, you may select such item and press Enter or double click on the item - IPMI Browser will ask password and connect to the server.

Connecting to the remote host using command line parameters

You may specify the connection parameters on the command line, this way IPMI Browser connects to the specified system right after start up.
Format of the command line:
ipmibrowser.exe -host:<hostname> [-port:<portnumber>] [-timeout:<timeout>] [-retr:<retries>] [-cipher:<ciphermode>] [-user:<username>] [-pswd:<password>]

host	-	host name or IP address of the destination server
port	-	port number on which the host is listening for incoming IPMI requests (default 623).
timeout	-	amount of time in milliseconds the program will wait for a response from target system before the request fails
retr	-	the communications retry count (default 3)
ciphermode	-	0,1,2,3,15,16 or 17 as described above (e.g. 3 = RAKP-HMAC-SHA1 + AES128CBC + HMAC-SHA1-96)
user	-	account name that should be used for connection with the remote system
pswd	-	provide password for the specified account

Examples:
ipmibrowser.exe -host:10.10.1.90 -port:623 -timeout:800 -retries:3 -cipher:3 -user:admin
ipmibrowser.exe -host:10.20.1.55 "-user:admin" "-pswd:secretword"

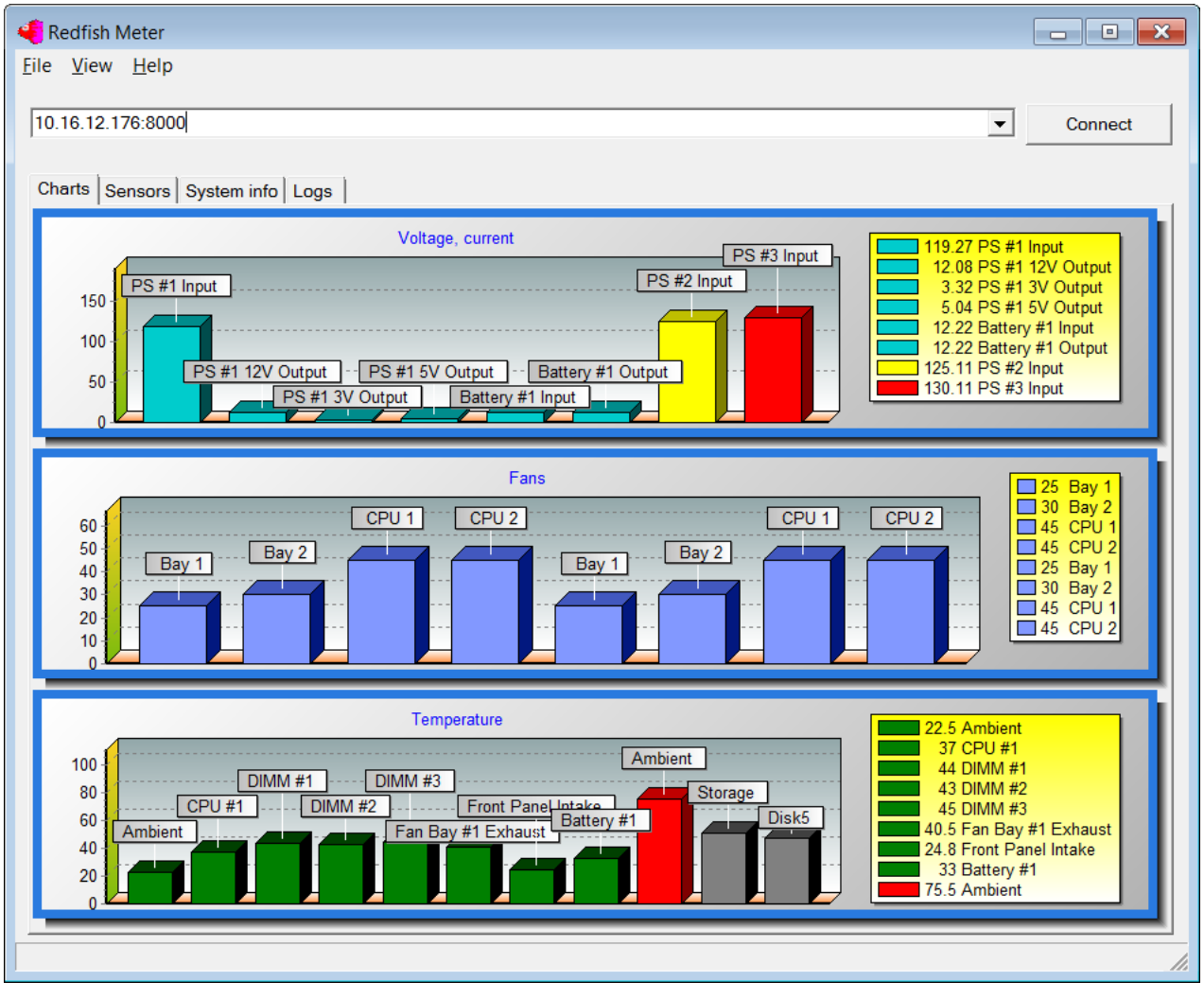
Known problems

Servers
Often, firmware running on servers cannot provide entire SDR record in one packet. Servers provide SDR data in small portions, e.g. 16 bytes per request. As a result, IPMI client software needs to make hundreds (sometimes over thousand) requests in order to retrieve information about available counters.
IPMI Browser caches some data, this helps to reduce number of requests when you are connecting to previously visited server.

OEM
IPMI Browser does not decode OEM specific counters yet. It will show sensor index, name and value but status field will be empty.

Redfish Meter

Redfish is a set of specifications for out-of-band management of computer systems. Redfish subsystem operates independently of the host CPU, firmware and operating system (similar to IPMI and HP iLO). Redfish allows you to manage a computer that may be powered off or otherwise unresponsive by using a network connection to the hardware rather than to an operating system.
A wide range of servers from leading manufacturers such as Cisco, Dell, HPE, IBM, Lenovo, Supermicro support Redfish either through a dedicated management interface or through a shared LAN and provide the ability to remotely reboot a frozen server, monitor for hardware failures, access firmware sensors and logs.



Redfish Meter retrieves data from remote servers using Redfish protocol, shows charts with temperature sensors, voltage and fans speed. Also you can check all available sensors with details: type, name, location, reading, status, etc.

Please note: marketing names such as "iDRAC" or "HP iLO" can be misleading as "HP iLO"-compatible servers can actually support at least 3 different protocols: IPMI, iLO and Redfish.

- HP iLO versions 1, 2 and 3 do not use the Redfish protocol, but the older HPE "iLO" protocol (IPMI is also usually supported).
- HP iLO version 4 and 5 - can use either the older HPE protocol or the Redfish protocol (IPMI is also usually supported). As we know, this depends on the firmware version, HPE switched to Redfish protocol in iLO 5 v2.30

Dell servers with iDRAC can also support several different protocols: IPMI and Redfish.

Also Redfish specifications change slightly every year. HostMonitor supports several versions and should be able to work with older and newer servers. If it does not work with your server, Redfish Meter may help to diagnose the problem.

Main menu

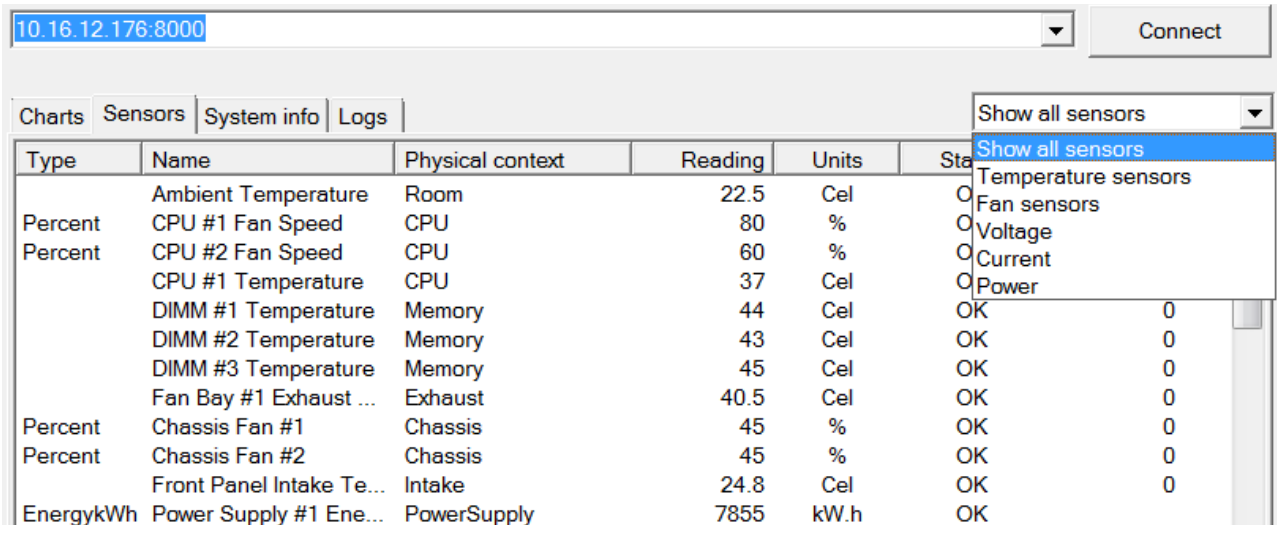
File		
Target host	-	this menu item allows you to specify connection parameters for remote system monitoring
Copy image to clipboard	-	copies the charts as an image into the clipboard
Copy data to clipboard	-	copies system information and list of all sensors with details into clipboard
Copy log to clipboard	-	copies logs into the clipboard
Exit	-	closes application
View		
Charts	-	opens Charts pane
Sensors	-	opens Sensors pane
System info	-	opens System info pane
Logs	-	opens Logs pane
Refresh	-	tells the application to collect up-to-date information from target system and update the charts and sensors
Auto refresh ON	-	using this menu item you may setup Redfish Meter to update data on regular basis, e.g. every 30 sec
Auto refresh OFF	-	use this menu to disable "auto refresh" option
Display labels	-	turns on/off chart labels
Help		
Help	-	displays Help
Home page	-	starts default web browser, opens home page of the Redfish Meter on www.ks-soft.net
Support	-	allows you to send e-mail to our tech support staff using your default mail client

About - about Redfish Meter

Redfish Meter can be started as an independent application or it can be launched by HostMonitor: Redfish related test methods (e.g Redfish Health) offer "Redfish Meter" pop up menu item that allows you to check target system.

Sensors

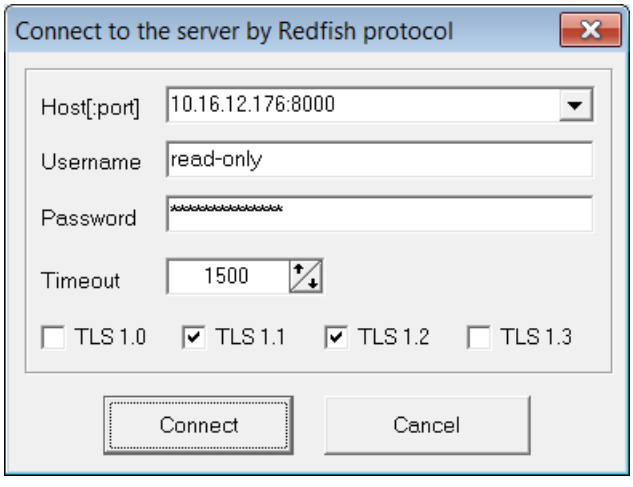
This pane shows all available sensors (including sensors not displayed on the charts).



You can tell Redfish Meter to display subset of the sensors, e.g. display just temperature sensors, display voltage sensors or sensors related to power consumption.

In order to connect to the remote system you may use GUI or command line parameters.

Connecting to the remote host using GUI
You may connect to another system using menu "File" -> "Target host"



Please set the following parameters:

Host	Here you should specify the domain name or IP address of the host you want to monitor. You can also specify the TCP port (default is 443), for example 10.10.10.1:8000. You can also set the prefix http://, in which case the regular HTTP protocol will be used without encryption, and the default TCP port will be changed to port 80. E.g. server55.msinternal.com 204.71.200.68 204.71.200.68:8000 http://10.10.10.1:8002
Username	provide account that should be used for connection with the remote system
Password	provide password for the specified account
Timeout	amount of time in milliseconds the program will wait for a response from target system before the request fails
TLS	enable one or several versions of TLS protocol (for TLS 1.3 you need to start application on Windows 11, Windows Server 2022 or Windows Server 2025)

Connecting to the remote host using command line parameters

You may specify the connection parameters on the command line, this way Redfish Meter connects to the specified system right after start up.
Format of the command line:
RfMeter.exe -host:[http://|https://]<hostname>[:<port>] [-timeout:<timeout>] [-user:<username>] [-pswd:<password>] [-mode:<sensorsdisplaymode>]

host	-	the host name or IP address of the host you want to monitor. You can also specify the TCP port (default is 443), for example 10.10.10.1:8000. You can also set the prefix http://, in which case the regular HTTP protocol will be used without encryption, and the default TCP port will be changed to port 80. E.g. server55.msinternal.com 204.71.200.68 204.71.200.68:8000 http://10.10.10.1:8002
timeout	-	amount of time in milliseconds the program will wait for a response from target system before the request fails
user	-	account name that should be used for connection with the remote system
pswd	-	provide password for the specified account
mode	-	by default Redfish Meter displays all available sensors however you can tell application to display subset of the sensors, e.g. display just temperature sensors, display voltage sesnors or sensors related to power consumption. Possible options: temp fans voltage current power

Examples:
RfMeter.exe -host:10.10.1.90:8000 -timeout:1500 -user:roadmin
RfMeter.exe -host:http://10.20.1.55 "-user:roadmin" "-pswd:secretword" -mode:voltage

---

Installation / Technical information / Other

How To Install / Upgrade / Uninstall Advanced Host Monitor

How To Install/Update/Repair Advanced Host Monitor

Run installation program, answer "Yes" on the prompt to install Advanced Host Monitor software. Setup wizard will then ask you to choose between the two available types of installation.

- "**Install**" – Use this option either for a fresh new installation or to completely replace an old version. With this option the newer installation will overwrite all files of previously installed (if any) version of Advanced Host Monitor unless you selected different disk folder for installation.

- "**Update/repair**" – Use this option to update previously installed Advanced Host Monitor to a newer version while keeping all user settings unchanged. Also you may use this option to repair installed software when some files were removed by mistake or after virus attack. Setup program will overwrite all executable modules of previously installed HostMonitor, help files, etc; all user settings will remain intact.

After choosing Install or Update mode click "Next" button and select one of the following options:

- **Install Advanced Host Monitor and utilities;**
- Install Remote Control Console only;
- Install Remote Monitoring Agent only

Last 2 options provide quick way to install or update RCC and RMA modules only; while 1st option allows you to choose various sets of applications.

If you continue with selected by default "Install/Update Advanced Host Monitor and utilities" option then Setup program allows you to choose 2 different folders for Advanced Host Monitor package:

- one folder for executable files (by default this is the folder where the Advanced Host Monitor was previously installed on your system or \Program Files\HostMonitor\ folder for first time installation);
- another folder for configuration files

E.g.

- *.EXE, *.DLL, *.DOC files can be stored in C:\Program Files\HostMonitor\
- *.INI, *.LST, *.HML files, reports, logs and HM script files can be located at C:\ProgramData\HostMonitor\

Note: if you want to use several different versions of the software

on the same system (for testing purpose) then you need to install configuration files using <same path> mode.
Also, please see notes regarding UAC and Virtualization

There is also a choice of 4 setup packages:

- "**Lite/Standard**" – only HostMonitor, Process Meter, Disk Meter, WMI Explorers, samples and help files will be installed.
- "**Professional**" – 7 components will be installed: HostMonitor, Disk Meter, MIB Browser, WMI Explorer, Process Meter, Log Analyzer and Log Visualizer.
- "**Enterprise**" – All components will be installed.
- "**Custom**" – use this option when you need to install some specific utilities, e.g. install RMA, RCC and Log Analyzer.

Beside each setup package there is a help button. Press this button to bring up the reminder about the components that will be installed.

After choosing the destination path and setup package, press the "next" button of the setup wizard. Now, if you have chosen "custom" setup package the next screen will ask you to select which components to install (selection step is skipped if you have chosen "Lite/Standard", "Professional" or "Enterprise" packages). The next screen will show you a summary of all options you have just chosen. If you change your mind then press "back" button to step back and adjust your settings.

Finally press "Install" button to start installation. When the final stage of installation will finish you will be prompted to put the HostMonitor icon on the desktop, create HostMonitor program group and to run HostMonitor right after the installation. Check these options according to your desire and press "Done" button.

How To Uninstall Advanced Host Monitor

Method 1:
Run **uninstall.exe** from the HostMonitor directory (or from the HostMonitor program group) and click the "Start" button.
Method 2:
Open the Windows Control Panel, double click the "Add/Remove Programs" icon, select "HostMonitor" from the list and click the "Add/Remove" button.

UAC and Virtualization

If you are using Windows Vista or newer Windows system, UAC is enabled and you setup software using separate application/data folders then most applications disable virtualization. In addition to HostMonitor and RMA Manager (these applications disable virtualization regardless of location), the following modules disable virtualization when data files located in separate folder:

- MIB Browser
- Log Analyzer
- Log Visualizer
- Web Service
- Telnet Service
- WatchDog
- Process Meter
- WMI Explorer

If you install software using single destination folder below Program Files\ then configuration files can be virtualized by UAC.

RMA for Windows modules work differently:

- if you install new copy of RMA using setup program, it will disable virtualization regardless of data files location (RMA agent always keep rma.ini file in the same folder);
- if you update existing old RMA installation using setup program or RMA Manager, it will keep current settings (in such case rma.ini file can be virtualized depending on UAC settings and installation folder location).

Note: you may enable/disable virtualization for RMA agent using the following registry key:

- on 32bit Windows: HKLM\Software\KS-Soft\HostMonitor\RMAVirtualizationOff
- on 64bit Windows: HKLM\ Software\Wow6432Node\KS-Soft\HostMonitor\RMAVirtualizationOff

There is another UAC-related problem: if software is running as Win32 service, it may not have "write" access to data folders (this depends on version of the system, location of the folder and UAC settings). HostMonitor may not be able to store settings even if you provide admin account for the service (admin - user that belongs to Administrators and Users groups).
There are several possible solutions:

- disable UAC;
- use BUILT-IN "administrator" account to start service;
- add "write" and "modify" permissions to Users group.

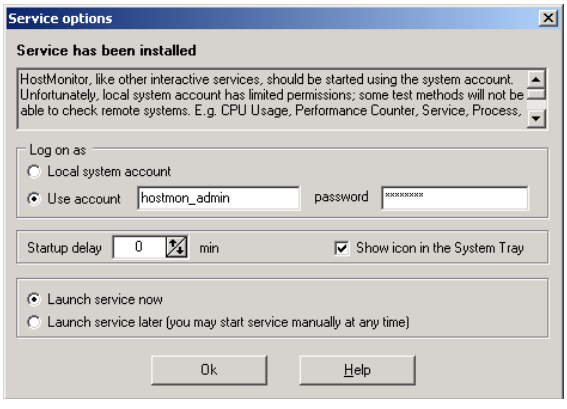
That's why Setup program assigns "write" and "modify" permissions to Authenticated Users group when you install (not update) software on Windows Vista+ using separate folder for data files.
If you are sure you will run HostMonitor as service under built-in administrator account or UAC always will be disabled or HostMonitor will be started as application only, then you may adjust folder permissions (for better security) after installation and initial configuration.

Useful links:
Why administrator gets access denied
Inside Windows Vista UAC
Inside Windows 7 UAC

How to install HostMonitor as Win32 service

1. Install Advanced Host Monitor package on your system. If you already have Advanced Host Monitor installed, skip this step.

2. Start HostMonitor (**hostmon.exe**, not host-mon.exe) with the command line parameter "/InstallService" (**hostmon.exe /InstallService**). HostMonitor will install itself as a service and display "Service options" dialog. "Service options" dialog allows you to specify some important parameters and then lauch the service. If you do not plan to start service right away, select "Launch service later" option and click Ok. In such case service will be started at system startup. Also you may start service at any time using standard Windows "Services" applet or command line like "net start hostmonservice".



Please read the following notes (#1..#4)

Note #1: "Local system" account does not allow to monitor remote systems using test methods like CPU Usage, Process, Service, NT Event Log, etc. If you need these tests, you will need to assign a special user account using "Service options" dialog. Also, you may change this account later using options located on the Service page in the Options dialog. In this case HostMonitor will impersonate the security context of the user.
Windows XP and Windows Server 2003 related note: do not change the account using Windows applet "Services". If you do so, HostMonitor service may be unable to interact with the desktop and you will need to use RCC as remote management application.
Windows Vista+ related note: Windows services cannot interact with desktop so you may provide user account for the service using HostMonitor options or using Windows "Services" applet.

Note #2: In some cases Win32 service is unable to interact with desktop. There are 3 most common reasons:
- You have disabled “Allow service to interact with desktop" option
- Service is running on remote system and you are using Terminal Service to login to the remote system
- You are using Windows Vista, Windows 7-11 or Windows Server 2008-2022

It’s pretty easy to enable “Allow service to interact with desktop" option but how to manage HostMonitor that is running as service on remote system / on Windows Server 2016? Use Remote Control Console (RCC) that allows you to manage HostMonitor started on local or remote system

in service or application mode. HostMonitor started on Windows Vista+ allows 1 additional LOCAL RCC connection.

Note #3: There is common mistake - install HostMonitor as service, start service, then start application. Please DO NOT start several instances of HostMonitor on the same system using the same installation folder and configuration files. If you do so, several instances will work simultaneously, monitor the same target systems, and launch the same actions. If you modify test settings or profiles using 2nd instance of the software (application), 1st instance (service) will not apply modifications until you restart service. Also, your log files and statistical information will not be accurate when you are running several instances of the monitor using the same log files.
That's why HostMonitor warns you when you are trying to start application while service is running as well, then it may stop service before launching application.

Note #4 (obsolette, we do not support Windows NT 4.0 anymore): we do not recommend installing HostMonitor as a service under Windows NT 4.0. At least not as an interactive service. In the case you really need to start HostMonitor as a service on Windows NT, please, disable the "allow service to interact with desktop" option for HostMonitor service (option provided by Windows Services applet). In this case you will not be able to see HostMonitor's icon in the system tray.

System Requirements:

HostMonitor (core of the package) has following system requirements:

Minimum system requirements

- Windows XP Professional SP3, Windows 7 Professional
- Windows 10, Windows 11
- Windows Server 2003 SP2, Server 2008 SP2/R2, Server 2012, Server 2012/R2,
- Windows Server 2016, Windows Server 2019, Windows Server 2022
- Internet Explorer 6
- Microsoft TCP/IP protocol
- Free disk space: 50 MB (if you install HostMonitor only)
- Screen resolution: 1024 x 768

Recommended:

- Windows Server 2016, 2019 or 2022
- Internet Explorer 11 or Microsoft Edge
- Free disk space: 150 MB (for all components) + some space for logging (depends on your settings)

Windows x64:

- HostMonitor is 32-bit application, however it can be used on Windows x64 Edition running on x86-64 (AMD64) systems (not on Itanium/IA-64). E.g. you can start HostMonitor on Windows XP Professional x64 Edition or Windows Server 2003 x64 Edition.
- If you are using Windows x64 Edition and you want to setup ODBC Logging or ODBC test method, you should setup ODBC datasources using 32-bit ODBC Data Source Administrator (e.g. C:\WINDOWS\SysWOW64\odbcad32.exe).
- Also we can offer x64 version of HostMonitor. Its not available to everyone and its not needed by everyone, for most of customers x86 (32bit) version works more efficiently and uses less memory. On the other hand, if you have over 100,000 test items plus a lot of remote RCC operators and 1000+ Active RMA agents connected to HostMonitor, then you may need x64 version. It may use over 2GB memory and in some cases works faster.

Windows 2012 / Windows 8:
HostMonitor can run on Windows 8 Pro and Windows Server 2012 however we do not recommend these systems due to some problems in Windows API related to Event Logs.

Database monitoring

To monitor Oracle servers HostMonitor uses the Oracle Call Interface (OCI.DLL). You should have the Oracle client software installed on the same computer. The same is true for other SQL servers, install the client software for testing your SQL server. HostMonitor uses the following DLLs:

- gds32.dll to monitor Interbase connections
- ntwdblib.dll to monitor MS SQL Server
- libmysql.dll to monitor MySQL
- libpq.dll to monitor PostgreSQL
- libsybdb.dll to monitor Sybase

Important note:

- some versions of libmysql.dll have a bug that can cause HostMonitor to crash. If you experience this problem, you may download stable version of MySQL library from http://www.ks-soft.net/download/LIBMYSQL.DLL
- If you are using ODBC Query test method or you have setup ODBC logging, you must be sure that ODBC driver (provided by 3rd party) works reliable and will not cause HostMonitor to crash. E.g. Microsoft dBase Driver v 4.00 causes resource leakage; Oracle driver v8 may crash application.

Process monitoring

To monitor processes on a remote Windows system, make sure you have RPC and Remote Registry services started on the remote system. On Windows 2000-2022 this service is installed by default, for Windows NT 4.0 you can find this service in the Resource Kit.

Technical Info:

If you wish to move the program from one computer to another you do not need to re-implement all the lists and settings again. Simply copy the program files from one computer or install the program on another computer and then copy only the files containing your settings.

File	Used by	Description
Hostmon.exe	HostMonitor	Main executable module
LogsMan.exe	Log Analyzer	Main executable module
Rma.exe	Passive RMA	Main executable module
Rma_active.exe	Active RMA	Main executable module
Rma_cfg.exe	RMA	Configuration utility
Rma_mgr.exe	RMA Manager	Main executable module
Telnetservice.exe	Telnet Service	Main executable module
Webservice.exe	Web Service	Main executable module
Rcc.exe	Remote Control Console	Main executable module
MibBrowser.exe	MIB Browser	Main executable module
Hostmon.chm	All applications	Help file
MibBrowser.chm	MIB Browser	Help file
Hostmon.ini	HostMonitor	Includes all global parameters (almost all of them represented in the Options dialog). You can create different ini files and specify the name of ini file in the command line when starting HostMonitor
Logsman.ini	Log Analyzer	Options and settings defined in Options dialog
Rma.ini	RMA	Options and settings
Rma_Mgr.ini	RMA Manager	Options and settings
Telnetservice.ini	Telnet Service	Options and settings
Webservice.ini	Web Service	Options and settings
MibBrowser.ini	MIB Browser	Options and settings
Actions.lst	HostMonitor	Contains the action profiles
Agents.lst	HostMonitor RMA Manager	List of Remote Monitoring Agents
Custmenu.lst	HostMonitor	Custom menu profiles
Deftemplates.lst	HostMonitor	Predefined template folders and tests
Holidays.lst	HostMonitor	List of holidays (for schedules)
Larep.lst	Log Analyzer	Report profiles
MailList.lst	HostMonitor	Mail templates
Palettes.lst	HostMonitor	Color schemes
Prbypass.lst	HostMonitor	Proxy bypass list
RepPList.lst	HostMonitor	Report profiles
Schedule.lst	HostMonitor	Contains the list of schedules
Services.lst	HostMonitor	List which includes TCP port descriptions
snmpacc.lst	HostMonitor	Profiles used for SNMP Get and Traffic Monitor test

		methods
Sscripts.lst	HostMonitor	Shell Script profiles (used by Shell Script test method)
Ttemplates.lst	HostMonitor	Patterns
Udvmacro.lst	HostMonitor	User defined macro variables
Users.lst	HostMonitor	User profiles (operators)
Wsuserprof.lst	Web Service	User profiles (preference settings for each user)
Wcolors.lst	Web Service	Color schemes for Web Interface
mibdata.lst	MIB Browser, HostMonitor, RCC	Stores information about compiled MIB files
mibtree.lst	MIB Browser, HostMonitor, RCC	Stores information about compiled MIB files

Examples	This directory contains different examples:
Example1.hml	A sample HML (test list) file. It is recommend that you save your test configurations in a diferent HML file rather than just modify the one shipped with the program, otherwise your changes will get lost during the upgrade process as the sample HML file will be overwriten with the newest version available.
Errorlev.exe	Example of program for external test
Import1.txt	The sample import file
Script1.hms	Example of HMS sript
AutoRefresh.html	This file can be used as an external header for HTML reports. It contains command to auto refresh HTML. Your browser will be refreshing the page's contents at regular intervals
Summary.html	Another external header, will display tests' statuses summary
StdHeader.html	Just an example of external header for HTML reports, can be used as a base for creating your own headers
CompactHeader.html	Sample of external header for Compact HTML report
StdFooter.html	Just an example of external footer for HTML reports, can be used as a base for creating your own footers
Summary2.html	Another external footer, will display tests' statuses summary
Examples\LAReports\	Directory contains samples of the external header, footer, template for Log Analyzer's Report Manager
Examples\Scripts\	Directory contains sample scripts for Script test

Troubleshooting:

If you are using HostMonitor with a license key that had been generated illegally or using a cracked version of HostMonitor, the program will become unstable causing frequent software problems and crashes.

If you are using ODBC logging or ODBC Query test items, you must be sure that ODBC driver (provided by 3rd party) works reliable and will not cause HostMonitor to crash. E.g. Microsoft dBase Driver v 4.00 causes resource leakage; Oracle drivers version 8 and especially version 10 have a lot of mistakes, these drivers may lead to high CPU usage, handles and memory leakage and may crash application.

If you have any questions, please visit the online forum at www.ks-soft.net. There you can find answers to a lot of questions. If not, please do not hesistate ask, we will be happy to help you.

Sales department: sales@ks-soft.net
Technical support: support@ks-soft.net

Appendix #1: Useful SQL queries for popular SQL servers

Using ODBC Query test method you may retrieve information about SQL server status. There are some useful SQL queries for most popular SQL servers.

MySQL
Interbase
Oracle

MySQL

SHOW GLOBAL STATUS LIKE 'Aborted_connects'
Query returns the number of failed attempts to connect to the MySQL server.

SHOW GLOBAL STATUS LIKE 'Aborted_clients'
The number of connections that were aborted because the client died without closing the connection properly

SHOW GLOBAL STATUS LIKE 'Aborted_connects'
The number of failed attempts to connect to the MySQL server.

SHOW GLOBAL STATUS LIKE 'Bytes_received'
Query returns the number of bytes received from all clients.

SHOW GLOBAL STATUS LIKE 'Bytes_sent'
The number of bytes sent to all clients.

SHOW GLOBAL STATUS LIKE 'Connections'
The number of connection attempts (successful or not) to the MySQL server.

SHOW GLOBAL STATUS LIKE 'Created_tmp_files'
How many temporary files mysqld has created.

SHOW GLOBAL STATUS LIKE 'Innodb_buffer_pool_pages_data'
The number of pages containing data (dirty or clean).

SHOW GLOBAL STATUS LIKE 'Innodb_buffer_pool_pages_dirty'
The number of pages currently dirty.

SHOW GLOBAL STATUS LIKE 'Innodb_data_pending_writes'
The current number of pending writes.

SHOW GLOBAL STATUS LIKE 'Innodb_row_lock_time_avg'
The average time to acquire a row lock, in milliseconds.

SHOW GLOBAL STATUS LIKE 'Innodb_row_lock_time_max'
The maximum time to acquire a row lock, in milliseconds.

SHOW GLOBAL STATUS LIKE 'Max_used_connections'
The maximum number of connections that have been in use simultaneously since the server started.

SHOW GLOBAL STATUS LIKE 'Open_files'
The number of files that are open. This count includes regular files opened by the server. It does not include other types of files such as sockets or pipes. Also, the count does not include files that storage engines open using their own internal functions rather than asking the server level to do so.

SHOW GLOBAL STATUS LIKE 'Open_tables'
The number of tables that are open.

SHOW GLOBAL STATUS LIKE 'Qcache_free_memory'
The amount of free memory for the query cache.

SHOW GLOBAL STATUS LIKE 'Slow_queries'
The number of queries that have taken more than long_query_time seconds.

SHOW GLOBAL STATUS LIKE 'Table_locks_waited'
The number of times that a request for a table lock could not be granted immediately and a wait was needed. If this is high and you have performance problems, you should first optimize your queries, and then either split your table or tables or use replication.

SHOW GLOBAL STATUS LIKE 'Threads_connected'
The number of currently open connections.

SHOW GLOBAL STATUS LIKE 'Threads_created'
The number of threads created to handle connections. If Threads_created is big, you may want to increase the thread_cache_size value. The cache miss rate can be calculated as Threads_created/Connections.

SHOW GLOBAL STATUS LIKE 'Threads_running'
The number of threads that are not sleeping.

Interbase

SELECT TMP$ATTACHMENTS FROM TMP$DATABASE
Number of active connections (SMALLINT)

SELECT TMP$STATEMENTS FROM TMP$DATABASE
Number of compiled statements (INTEGER)

SELECT TMP$ALLOCATED_PAGES FROM TMP$DATABASE
Pages allocated to all database files (INTEGER)

SELECT TMP$POOLS FROM TMP$DATABASE
Number of memory pools (INTEGER)

SELECT TMP$PROCEDURES FROM TMP$DATABASE
Number of procedures loaded (SMALLINT)

SELECT TMP$RELATIONS FROM TMP$DATABASE
Number of relations loaded (SMALLINT)

SELECT TMP$TRIGGERS FROM TMP$DATABASE
Number of triggers loaded (SMALLINT)

SELECT TMP$ACTIVE_THREADS FROM TMP$DATABASE
Active threads in database (SMALLINT)

SELECT TMP$SORT_MEMORY FROM TMP$DATABASE
Sort buffer allocated memory (INTEGER)

SELECT TMP$CURRENT_MEMORY FROM TMP$DATABASE
Current memory allocated database (INTEGER)

SELECT TMP$MAXIMUM_MEMORY FROM TMP$DATABASE
Maximum memory ever allocated (INTEGER)

SELECT TMP$PERMANENT_POOL_MEMORY FROM TMP$DATABASE
Permanent pool memory size (INTEGER)

SELECT TMP$CACHE_POOL_MEMORY FROM TMP$DATABASE
Buffer pool memory size (INTEGER)

SELECT TMP$TRANSACTIONS FROM TMP$DATABASE
Number of active transactions (SMALLINT)

SELECT TMP$TRANSACTION_COMMITS FROM TMP$DATABASE
Number of transaction commits (INTEGER)

SELECT TMP$TRANSACTION_ROLLBACKS FROM TMP$DATABASE
Number of transaction rollbacks (INTEGER)

SELECT TMP$TRANSACTION_PREPARES FROM TMP$DATABASE
Number of transaction prepares (INTEGER)

SELECT TMP$TRANSACTION_DEADLOCKS FROM TMP$DATABASE
Number of transaction deadlocks (INTEGER)

SELECT TMP$TRANSACTION_CONFLICTS FROM TMP$DATABASE
Number of transaction update conflicts (INTEGER)

SELECT TMP$TRANSACTION_WAITS FROM TMP$DATABASE
Number of transaction wait for (INTEGER)

SELECT TMP$CACHE_BUFFERS FROM TMP$DATABASE
Number of cache buffers (INTEGER)

SELECT TMP$CACHE_PRECEDENCE FROM TMP$DATABASE
Nodes in cache precedence graph (INTEGER)

SELECT TMP$CACHE_LATCH_WAITS FROM TMP$DATABASE
Buffer latch waits (INTEGER)

SELECT TMP$CACHE_FREE_WAITS FROM TMP$DATABASE
Number of waits for a free buffer (INTEGER)

SELECT TMP$CACHE_FREE_WRITES FROM TMP$DATABASE
Number of writes to free buffers (INTEGER)

SELECT TMP$SWEEP_INTERVAL FROM TMP$DATABASE
Sweep trigger interval (INTEGER)

SELECT TMP$SWEEP_ACTIVE FROM TMP$DATABASE
‘Y’ (active) or ‘N’ (not-active) (CHAR[1])

SELECT TMP$SWEEP_RELATION FROM TMP$DATABASE
Relation currently being swept (CHAR[67])

SELECT TMP$SWEEP_RECORDS FROM TMP$DATABASE
Records swept in above relation (INTEGER)

SELECT TMP$PAGE_READS FROM TMP$DATABASE
Page reads all database files (INTEGER)

SELECT TMP$PAGE_WRITES FROM TMP$DATABASE
Page writes all database files (INTEGER)

SELECT TMP$PAGE_FETCHES FROM TMP$DATABASE
Page fetches all database files (INTEGER)

SELECT TMP$PAGE_MARKS FROM TMP$DATABASE
Page marks all database files (INTEGER)

SELECT TMP$RECORD_SELECTS FROM TMP$DATABASE
Records selected from database (INTEGER)

SELECT TMP$RECORD_INSERTS FROM TMP$DATABASE
Records inserted into database (INTEGER)

SELECT TMP$RECORD_UPDATES FROM TMP$DATABASE
Records updated to database (INTEGER)

SELECT TMP$RECORD_DELETES FROM TMP$DATABASE
Records deleted from database (INTEGER)

SELECT TMP$RECORD_PURGES FROM TMP$DATABASE
Garbage collect record purges (INTEGER)

SELECT TMP$RECORD_EXPUNGES FROM TMP$DATABASE
Garbage collect record expunges (INTEGER)

SELECT TMP$RECORD_BACKOUTS FROM TMP$DATABASE
Garbage collect record backouts (INTEGER)

Oracle server

The following counters supported by Oracle version 10g or higher

Number of active connections:
SELECT COUNT(*) FROM V$SESSION
Returns the number of currently active sessions on Oracle server.

Buffer Cache Hit Ratio.
The Buffer Cache Hit Ratio Oracle metric monitors the rate at which Oracle finds the data blocks it needs in memory over the lifetime of an instance.
Measurement unit: % (LogRead - PhyRead)/LogRead
SELECT value FROM sys.v_$sysmetric where metric_name = 'Buffer Cache Hit Ratio' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

CPU Usage Per Sec.
The CPU Time Per Sec Oracle metric shows the amount of CPU usage per second for the specific task, SQL statement or session.
Measurement unit: CentiSeconds Per Second
SELECT value FROM sys.v_$sysmetric where metric_name = 'CPU Usage Per Sec'
Results:
Row 1: Long duration value (60-second)

CPU Usage Per Transaction.
The CPU Time Per Txn Oracle metric shows the amount of CPU usage per transaction for the specific task or session
Measurement unit: CentiSeconds Per Transaction
SELECT value FROM sys.v_$sysmetric where metric_name = 'CPU Usage Per Txn'
Results:
Row 1: Long duration value (60-second)

Current Logons Count.
The Current Logons Count Oracle metric is the total number of current logons.
Measurement unit: Logons
SELECT value FROM sys.v_$sysmetric where metric_name = 'Current Logons Count'
Results:
Row 1: Long duration value (60-second)

Current Open Cursors Count.
The Current Open Cursors Count Oracle metric refers to the current number of open cursors; whether they are being utilized or not.
Measurement unit: Cursors
SELECT value FROM sys.v_$sysmetric where metric_name = 'Current Open Cursors Count'
Results:
Row 1: Long duration value (60-second)

Current OS Load.
Measurement unit: Number Of Processes
SELECT value FROM sys.v_$sysmetric where metric_name = 'Current OS Load'
Results:
Row 1: Long duration value (60-second)

Cursor Cache Hit Ratio.
The Cursor Cache Hit Ratio Oracle metric is determined by the ratio of the number of times an open cursor was found divided by the number of times a cursor was sought.
Measurement unit: % CursorCacheHit/SoftParse
SELECT value FROM sys.v_$sysmetric where metric_name = 'Cursor Cache Hit Ratio'
Results:
Row 1: Long duration value (60-second)

Database CPU Time Ratio.
Measurement unit: % Cpu/DB_Time
SELECT value FROM sys.v_$sysmetric where metric_name = 'Database CPU Time Ratio' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

Host CPU Utilization (%).
Measurement unit: % Busy/(Idle+Busy)
SELECT value FROM sys.v_$sysmetric where metric_name = 'Host CPU Utilization (%)' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

Disk Sort Per Sec.
This metric represents the number of sorts going to disk per second for this sample period. For best performance, most sorts should occur in memory, because sorts to disks are expensive to perform. If the sort area is too small, extra sort runs will be required during the sort operation. This increases CPU and I/O resource consumption.
Measurement unit: Sorts Per Second
SELECT value FROM sys.v_$sysmetric where metric_name = 'Disk Sort Per Sec'
Results:
Row 1: Long duration value (60-second)

Disk Sort Per Transaction.
This metric represents the number of sorts going to disk per transactions for this sample period. For best performance, most sorts should occur in memory, because sorts to disks are expensive to perform. If the sort area is too small, extra sort runs will be required during the sort operation. This increases CPU and I/O resource consumption. The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" metric of the

same name will be a better indicator of current performance.
Measurement unit: Sorts Per Transaction
SELECT value FROM sys.v_$sysmetric where metric_name = 'Disk Sort Per Txn'
Results:
Row 1: Long duration value (60-second)

Global Cache Average CR Get Time.
This metric represents the average time, measured in hundredths of a second, that CR block was received.
Measurement unit: CentiSeconds Per Get
SELECT value FROM sys.v_$sysmetric where metric_name = 'Global Cache Average CR Get Time'
Results:
Row 1: Long duration value (60-second)

Global Cache Average Current Get Time.
This metric represents the average time, measured in hundredths of a second, to get a current block.
Measurement unit: CentiSeconds Per Get
SELECT value FROM sys.v_$sysmetric where metric_name = 'Global Cache Average Current Get Time'
Results:
Row 1: Long duration value (60-second)

Global Cache Blocks Corrupted.
This metric represents the number of blocks that encountered a corruption or checksum failure during interconnect over the last observation period.
Measurement unit: Blocks
SELECT value FROM sys.v_$sysmetric where metric_name = 'Global Cache Blocks Corrupted'
Results:
Row 1: Long duration value (60-second)

Global Cache Blocks Lost.
This metric represents the number of global cache blocks lost over the last observation period.
Measurement unit: Blocks
SELECT value FROM sys.v_$sysmetric where metric_name = 'Global Cache Blocks Lost'
Results:
Row 1: Long duration value (60-second)

Hard Parse Count Per Sec.
This metric represents the number of hard parses per second during this sample period. A hard parse occurs when a SQL statement has to be loaded into the shared pool. In this case, the Oracle Server has to allocate memory in the shared pool and parse the statement.
Each time a particular SQL cursor is parsed, this count will increase by one. There are certain operations that will cause a SQL cursor to be parsed. Parsing a SQL statement breaks it down into atomic steps, which the optimizer will evaluate when generating an execution plan for the cursor.
Measurement unit: Parses Per Second
SELECT value FROM sys.v_$sysmetric where metric_name = 'Hard Parse Count Per Sec'

Results:
Row 1: Long duration value (60-second)

Hard Parse Count Per Transaction.
This metric represents the number of hard parses per second during this sample period. A hard parse occurs when a SQL statement has to be loaded into the shared pool. In this case, the Oracle Server has to allocate memory in the shared pool and parse the statement.
Each time a particular SQL cursor is parsed, this count will increase by one. There are certain operations which will cause a SQL cursor to be parsed. Parsing a SQL statement breaks it down into atomic steps which the optimizer will evaluate when generating an execution plan for the cursor. The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" metric of the same name will be a better indicator of current performance.
Measurement unit: Parses Per Transaction
SELECT value FROM sys.v_$sysmetric where metric_name = 'Hard Parse Count Per Txn'
Results:
Row 1: Long duration value (60-second)

Logons Per Sec.
This metric represents the number of logons per second during the sample period
Measurement unit: Logons Per Second
SELECT value FROM sys.v_$sysmetric where metric_name = 'Logons Per Sec' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

Memory Sorts Ratio.
This metric represents the sort efficiency as measured by the percentage of times sorts were performed in memory as opposed to going to disk.
For best performance, most sorts should occur in memory because sorts to disks are less efficient. If the sort area is too small, extra sort runs will be required during the sort operation. This increases CPU and I/O resource consumption.
Measurement unit: % MemSort/(MemSort + DiskSort)
SELECT value FROM sys.v_$sysmetric where metric_name = 'Memory Sorts Ratio' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

Network Traffic Volume Per Sec.
This metric represents the total number of bytes sent and received through the SQL Net layer to and from the database.
Measurement unit: Bytes Per Second
SELECT value FROM sys.v_$sysmetric where metric_name = 'Network Traffic Volume Per Sec'
Results:
Row 1: Long duration value (60-second)

Open Cursors Per Sec.
This metric represents the total number of cursors opened per second.
Measurement unit: Cursors Per Second
SELECT value FROM sys.v_$sysmetric where metric_name = 'Open Cursors Per Sec'
Results:
Row 1: Long duration value (60-second)

Open Cursors Per Transaction.
This metric represents the total number of cursors opened per transaction.
Measurement unit: Cursors Per Transaction
SELECT value FROM sys.v_$sysmetric where metric_name = 'Open Cursors Per Txn'
Results:
Row 1: Long duration value (60-second)

Parse Failure Count Per Sec.
This metric represents the total number of parse failures per second.
Measurement unit: Parses Per Second
SELECT value FROM sys.v_$sysmetric where metric_name = 'Parse Failure Count Per Sec'
Results:
Row 1: Long duration value (60-second

Parse Failure Count Per Transaction.
This metric represents the total number of parse failures per transaction
Measurement unit: Parses Per Transaction
select value from sys.v_$sysmetric where metric_name = 'Parse Failure Count Per Txn'
Results:
Row 1: Long duration value (60-second

PGA Cache Hit %.
This metric represents the total number of bytes processed in the PGA versus the total number of bytes processed plus extra bytes read/written in extra passe
Measurement unit: % Bytes/TotalBytes
select value from sys.v_$sysmetric where metric_name = 'PGA Cache Hit %'
Results:
Row 1: Long duration value (60-second

Physical Read IO Requests Per Sec.
This metric represents the number of data blocks read from disk per second during this sample period. When a user performs a SQL query, Oracle tries to retrieve the data from the database buffer cache (memory) first, then searches the disk if it is not already in memory. Reading data blocks from disk is much more inefficient than reading the data blocks from memory. The goal with Oracle should always be to maximize memory utilization.
Measurement unit: Requests Per Second
select value from sys.v_$sysmetric where metric_name = 'Physical Read IO Requests Per Sec'
Results:
Row 1: Long duration value (60-second

Physical Reads Direct Per Sec.

This metric represents the number of direct physical reads per second.
Measurement unit: Reads Per Second
select value from sys.v_$sysmetric where metric_name = 'Physical Reads Direct Per Sec' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

Physical Write IO Requests Per Sec.
This metric represents the number of write IO requests per second.
Measurement unit: Requests Per Second
select value from sys.v_$sysmetric where metric_name = 'Physical Write IO Requests Per Sec'
Results:
Row 1: Long duration value (60-second)

Physical Write Total IO Requests Per Sec.
Measurement unit: Requests Per Second
select value from sys.v_$sysmetric where metric_name = 'Physical Write Total IO Requests Per Sec'
Results:
Row 1: Long duration value (60-second)

Physical Writes Direct Per Sec.
This metric represents the number of direct physical writes per second
Measurement unit: Writes Per Second
select value from sys.v_$sysmetric where metric_name = 'Physical Writes Direct Per Sec'
Results:
Row 1: Long duration value (60-second)

Physical Writes Per Sec.
This metric represents the number of disk writes per second during the sample period. This statistic represents the rate of database blocks written from the SGA buffer cached to disk by the DBWR background process, and from the PGA by processes performing direct writes.
Measurement unit: Writes Per Second
select value from sys.v_$sysmetric where metric_name = 'Physical Writes Per Sec' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

Process Limit %.
The PROCESSES initialization parameter specifies the maximum number of operating system user processes that can simultaneously connect to a database at the same time. This number also includes background processes utilized by the instance.
Measurement unit: % Processes/Limit
select value from sys.v_$sysmetric where metric_name = 'Process Limit %'
Results:
Row 1: Long duration value (60-second)

PX downgraded Parallel Operation Per Sec.
Measurement unit: Operations Per Second
select value from sys.v_$sysmetric where metric_name = 'PX downgraded Parallel Operation Per Sec'
Results:
Row 1: Long duration value (60-second)

PX downgraded to serial Per Sec.
Number of times per second parallel execution was requested but execution was serial because of insufficient parallel execution servers.
Measurement unit: PX Operations Per Second
select value from sys.v_$sysmetric where metric_name = 'PX downgraded to serial Per Sec'
Results:
Row 1: Long duration value (60-second)

PX downgraded 25% or more Per Sec.
Number of times per second parallel execution was requested and the degree of parallelism was reduced to 25% and more because of insufficient parallel execution servers.
Measurement unit: PX Operations Per Second
select value from sys.v_$sysmetric where metric_name = 'PX downgraded 25% or more Per Sec'
Results:
Row 1: Long duration value (60-second)

PX downgraded 50% or more Per Sec.
Number of times per second parallel execution was requested and the degree of parallelism was reduced to 50% and more because of insufficient parallel execution servers.
Measurement unit: PX Operations Per Second
select value from sys.v_$sysmetric where metric_name = 'PX downgraded 50% or more Per Sec'
Results:
Row 1: Long duration value (60-second)

PX downgraded 75% or more Per Sec.
Number of times per second parallel execution was requested and the degree of parallelism was reduced to 75% or more because of insufficient parallel execution servers.
Measurement unit: PX Operations Per Second
select value from sys.v_$sysmetric where metric_name = 'PX downgraded 75% or more Per Sec'
Results:
Row 1: Long duration value (60-second)

Recursive Calls Per Sec.
This metric represents the number of recursive calls, per second during the sample period.
Sometimes, to execute a SQL statement issued by a user, the Oracle Server must issue additional statements. Such statements are called recursive calls or recursive SQL statements. For example, if you insert a row into a table that does not have enough space to hold that row, the Oracle Server makes recursive calls to allocate the space dynamically if dictionary managed tablespaces are being used. Recursive calls are also generated:

- When data dictionary information is not available in the data dictionary cache and must be

retrieved from disk
- In the firing of database triggers
- In the execution of DDL statements
- In the execution of SQL statements within stored procedures, functions, packages and anonymous PL/SQL blocks
- In the enforcement of referential integrity constraints

Measurement unit: Calls Per Second
select value from sys.v_$sysmetric where metric_name = 'Recursive Calls Per Sec'
Results:
Row 1: Long duration value (60-second)

Recursive Calls Per Transaction.
This metric represents the number of recursive calls, per second during the sample period.
Sometimes, to execute a SQL statement issued by a user, the Oracle Server must issue additional statements. Such statements are called recursive calls or recursive SQL statements. For example, if you insert a row into a table that does not have enough space to hold that row, the Oracle Server makes recursive calls to allocate the space dynamically if dictionary managed tablespaces are being used. Recursive calls are also generated:
- When data dictionary information is not available in the data dictionary cache and must be retrieved from disk
- In the firing of database triggers
- In the execution of DDL statements
- In the execution of SQL statements within stored procedures, functions, packages and anonymous PL/SQL blocks
- In the enforcement of referential integrity constraints

The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" metric of the same name will be a better indicator of current performance.
Measurement unit: Calls Per Transaction
select value from sys.v_$sysmetric where metric_name = 'Recursive Calls Per Txn'

Redo Allocation Hit Ratio.
Redo log entries contain a record of changes that have been made to the database block buffers. The log writer (LGWR) process writes redo log entries from the log buffer to a redo log file. The log buffer should be sized so that space is available in the log buffer for new entries, even when access to the redo log is heavy. When the log buffer is undersized, user process will be delayed as they wait for the LGWR to free space in the redo log buffer.
The redo log buffer efficiency, as measured by the hit ratio, records the percentage of times users did not have to wait for the log writer to free space in the redo log buffer.
Measurement unit: % (#Redo - RedoSpaceReq)/#Redo
select value from sys.v_$sysmetric where metric_name = 'Redo Allocation Hit Ratio'
Results:
Row 1: Long duration value (60-second)

Session Limit %.
The SESSIONS initialization parameter specifies the maximum number of concurrent connections that the database will allow.

Measurement unit: % Sessions/Limit
select value from sys.v_$sysmetric where metric_name = 'Session Limit %'
Results:
Row 1: Long duration value (60-second)

Shared Pool Free %.
This metric represents the percentage of the Shared Pool that is currently marked as free.
Measurement unit: % Free/Total
select value from sys.v_$sysmetric where metric_name = 'Shared Pool Free %' order by roup_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

Soft Parse Ratio.
A soft parse is recorded when the Oracle Server checks the shared pool for a SQL statement and finds a version of the statement that it can reuse.
This metric represents the percentage of parse requests where the cursor was already in the cursor cache compared to the number of total parses. This ratio provides an indication as to how often the application is parsing statements that already reside in the cache as compared to hard parses of statements that are not in the cache.
Measurement unit: % SoftParses/TotalParses
select value from sys.v_$sysmetric where metric_name = 'Soft Parse Ratio' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

SQL Service Response Time.
This metric represents the average elapsed time, in centiseconds, for calls to a particular database service.
Measurement unit: CentiSeconds Per Call
select value from sys.v_$sysmetric where metric_name = 'SQL Service Response Time'
Results:
Row 1: Long duration value (60-second)

Transactions Per Logon.
Measurement unit: Transactions Per Logon
select value from sys.v_$sysmetric where metric_name = 'Txns Per Logon' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

User Calls Per Sec.
This metric represents the number of logins, parses, or execute calls per second during the sample period.
Measurement unit: Calls Per Second
select value from sys.v_$sysmetric where metric_name = 'User Calls Per Sec' order by group_id
Results:
Row 1: Long duration value (60-second)

Row 2: Short duration value (15-second)

User Calls Ratio.
This metric represents the percentage of user calls to recursive calls.
Occasionally, to execute a SQL statement issued by a user, the Oracle Server must issue additional statements. Such statements are called recursive calls or recursive SQL statements. For example, if you insert a row into a table that does not have enough space to hold that row, the Oracle Server makes recursive calls to allocate the space dynamically if dictionary managed tablespaces are being used. Recursive calls are also generated:
When data dictionary information is not available in the data dictionary cache and must be retrieved from disk.

- In the firing of database triggers
- In the execution of DDL statements
- In the execution of SQL statements within stored procedures, functions, packages and anonymous PL/SQL blocks
- In the enforcement of referential integrity constraints

Measurement unit: % UserCalls/AllCalls
select value from sys.v_$sysmetric where metric_name = 'User Calls Ratio'
Results:
Row 1: Long duration value (60-second)

User Commits Percentage.
Measurement unit: % (UserCommit/TotalUserTxn)
select value from sys.v_$sysmetric where metric_name = 'User Commits Percentage'
Results:
Row 1: Long duration value (60-second)

User Limit %.
The LICENSE_MAX_SESSIONS initialization parameter specifies the maximum number of concurrent user sessions allowed simultaneously.
This metric checks whether the number of users logged on is reaching the license limit. If the percentage of the number of concurrent user sessions to the limit set in the LICENSE_MAX_SESSIONS initialization parameter exceeds the values specified in the threshold arguments, then a warning or critical alert is generated. If LICENSE_MAX_SESSIONS is not explicitly set to a value, the test does not trigger.
Note: This metric is most useful when session licensing is enabled. Refer to the Oracle Server Reference Manual for more information on LICENSE_MAX_SESSIONS and LICENSE_MAX_USERS.
Note: Unlike most metrics, which accept thresholds as real numbers, this metric can only accept an integer as a threshold.
Measurement unit: % Sessions/License_Limit
select value from sys.v_$sysmetric where metric_name = 'User Limit %'
Results:
Row 1: Long duration value (60-second)

User Rollbacks Per Sec.
This metric represents the number of times, per second during the sample period, that users manually issue the ROLLBACK statement or an error occurred during a user's transactions.

Measurement unit: Rollbacks Per Second
select value from sys.v_$sysmetric where metric_name = 'User Rollbacks Per Sec'
Results:
Row 1: Long duration value (60-second)

User Rollbacks Percentage.
Measurement unit: % (UserRollback/TotalUserTxn)
select value from sys.v_$sysmetric where metric_name = 'User Rollbacks Percentage'
Results:
Row 1: Long duration value (60-second)

User Transaction Per Sec.
This metric represents the total number of commits and rollbacks performed during this sample period.
Measurement unit: Transactions Per Second
select value from sys.v_$sysmetric where metric_name = 'User Transaction Per Sec'
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

Background Checkpoints Per Sec.
This metric represents the BG checkpoints per second
Measurement unit: Check Points Per Second
select value from sys.v_$sysmetric where metric_name = 'Background Checkpoints Per Sec'
Results:
Row 1: Long duration value (60-second)

CR Blocks Created Per Sec.
This metric represents the number of current blocks per second cloned to create consistent read (CR) blocks.
Measurement unit: Blocks Per Second
select value from sys.v_$sysmetric where metric_name = 'CR Blocks Created Per Sec'
Results:
Row 1: Long duration value (60-second)

CR Blocks Created Per Transaction.
This metric represents the number of current blocks per transaction cloned to create consistent read (CR) blocks.
Measurement unit: Blocks Per Transaction
select value from sys.v_$sysmetric where metric_name = 'CR Blocks Created Per Txn'
Results:
Row 1: Long duration value (60-second)

Database Time Per Sec.
This metric represents the time spent in database operations per second
Measurement unit: CentiSeconds Per Second
select value from sys.v_$sysmetric where metric_name = 'Database Time Per Sec' order by oup_id
Results:

Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

Database Wait Time Ratio.
This metric represents the percentage of time that database calls spent waiting for an event. Although there is no correct value for this metric, it can be used to detect a change in the operation of a system, for example, an increase in Database Time Spent Waiting from 50% to 75%. ('No correct value' means that there is no single value that can be applied to any database. The value is a characteristic of the system and the applications running on the system.)
Measurement unit: % Wait/DB_Time
select value from sys.v_$sysmetric where metric_name = 'Database Wait Time Ratio'
Results:
Row 1: Long duration value (60-second)

DB Block Changes Per Sec.
This metric represents the total number of changes per second that were part of an update or delete operation that were made to all blocks in the SGA.
Measurement unit: Blocks Per Second
select value from sys.v_$sysmetric where metric_name = 'DB Block Changes Per Sec' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

DB Block Changes Per Transaction.
This metric represents the total number of changes per transaction that were part of an update or delete operation that were made to all blocks in the SGA.
Measurement unit: Blocks Per Transaction
select value from sys.v_$sysmetric where metric_name = 'DB Block Changes Per Txn' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

Branch Node Splits Per Sec.
Number of times per second an index branch block was split because of the insertion of an additional value.
Measurement unit: Splits Per Second
select value from sys.v_$sysmetric where metric_name = 'Branch Node Splits Per Sec'
Results:
Row 1: Long duration value (60-second)

Branch Node Splits Per Transaction.
Number of times per transaction an index branch block was split because of the insertion of an additional value.
Measurement unit: Splits Per Transaction
select value from sys.v_$sysmetric where metric_name = 'Branch Node Splits Per Txn'
Results:

Row 1: Long duration value (60-second)

Consistent Read Changes Per Sec.
This metric represents the number of times per second a user process has applied rollback entries to perform a consistent read on the block.
Measurement unit: Blocks Per Second
select value from sys.v_$sysmetric where metric_name = 'Consistent Read Changes Per Sec' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

Consistent Read Changes Per Transaction.
This metric represents the number of times per transaction a user process has applied rollback entries to perform a consistent read on the block.
Measurement unit: Blocks Per Transaction
select value from sys.v_$sysmetric where metric_name = 'Consistent Read Changes Per Txn' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

Consistent Read Gets Per Sec.
This metric represents the number of times per second a consistent read was requested for a block.
Measurement unit: Blocks Per Second
select value from sys.v_$sysmetric where metric_name = 'Consistent Read Gets Per Sec' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

Consistent Read Gets Per Transaction.
This metric represents the number of times per transaction a consistent read was requested for a block.
Measurement unit: Blocks Per Transaction
select value from sys.v_$sysmetric where metric_name = 'Consistent Read Gets Per Txn' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

CR Undo Records Applied Per Sec.
This metric represents the number of undo records applied for consistent read per second.
Measurement unit: Undo Records Per Second
select value from sys.v_$sysmetric where metric_name = 'CR Undo Records Applied Per Sec'
Results:
Row 1: Long duration value (60-second)

CR Undo Records Applied Per Transaction.
This metric represents the consistent read undo records applied per transaction.
Measurement unit: Records Per Transaction
select value from sys.v_$sysmetric where metric_name = 'CR Undo Records Applied Per Txn'
Results:
Row 1: Long duration value (60-second)

DB Block Changes Per User Call.
This metric represents the total number of changes per user call that were part of an update or delete operation that were made to all blocks in the SGA.
Measurement unit: Blocks Per Call
select value from sys.v_$sysmetric where metric_name = 'DB Block Changes Per User Call'
Results:
Row 1: Long duration value (60-second)

DB Block Gets Per Sec.
This metric represents the number of times per second a current block was requested.
Measurement unit: Blocks Per Second
select value from sys.v_$sysmetric where metric_name = 'DB Block Gets Per Sec' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

DB Block Gets Per Transaction.
This metric represents the number of times per transaction a current block was requested.
Measurement unit: Blocks Per Transaction
select value from sys.v_$sysmetric where metric_name = 'DB Block Gets Per Txn' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

DB Block Gets Per User Call.
This metric represents the number of times per user call a current block was requested.
Measurement unit: Blocks Per Call
select value from sys.v_$sysmetric where metric_name = 'DB Block Gets Per User Call'
Results:
Row 1: Long duration value (60-second)

DBWR Checkpoints Per Sec.
This metric represents the number of times, per second, during this sample period DBWn was asked to scan the cache and write all blocks marked for a checkpoint.
The database writer process (DBWn) writes the contents of buffers to datafiles. The DBWn processes are responsible for writing modified (dirty) buffers in the database buffer cache to disk.
When a buffer in the database buffer cache is modified, it is marked dirty. The primary job of the DBWn process is to keep the buffer cache clean by writing dirty buffers to disk. As user processes dirty buffers, the number of free buffers diminishes. If the number of free buffers drops too low,

user processes that must read blocks from disk into the cache are not able to find free buffers. DBWn manages the buffer cache so that user processes can always find free buffers.
When the Oracle Server process cannot find a clean reusable buffer after scanning a threshold of buffers, it signals DBWn to write. When this request to make free buffers is received, DBWn writes the least recently used (LRU) buffers to disk. By writing the least recently used dirty buffers to disk, DBWn improves the performance of finding free buffers while keeping recently used buffers resident in memory. For example, blocks that are part of frequently accessed small tables or indexes are kept in the cache so that they do not need to be read in again from disk. The LRU algorithm keeps more frequently accessed blocks in the buffer cache so that when a buffer is written to disk, it is unlikely to contain data that may be useful soon.
Additionally, DBWn periodically writes buffers to advance the checkpoint that is the position in the redo log from which crash or instance recovery would need to begin.
Measurement unit: Check Points Per Second
select value from sys.v_$sysmetric where metric_name = 'DBWR Checkpoints Per Sec'
Results:
Row 1: Long duration value (60-second)

Enqueue Deadlocks Per Sec.
This metric represents the number of times per second that a process detected a potential deadlock when exchanging two buffers and raised an internal, restartable error.
Measurement unit: Deadlocks Per Second
select value from sys.v_$sysmetric where metric_name = 'Enqueue Deadlocks Per Sec'
Results:
Row 1: Long duration value (60-second)

Enqueue Deadlocks Per Transaction.
This metric represents the number of times per transaction that a process detected a potential deadlock when exchanging two buffers and raised an internal, restartable error.
Measurement unit: Deadlocks Per Transaction
select value from sys.v_$sysmetric where metric_name = 'Enqueue Deadlocks Per Txn'
Results:
Row 1: Long duration value (60-second)

Enqueue Requests Per Sec.
This metric represents the total number of table or row locks acquired per second.
Measurement unit: Requests Per Second
select value from sys.v_$sysmetric where metric_name = 'Enqueue Requests Per Sec'
Results:
Row 1: Long duration value (60-second)

Enqueue Requests Per Transaction.
This metric represents the total number of table or row locks acquired per transaction.
Measurement unit: Requests Per Transaction
select value from sys.v_$sysmetric where metric_name = 'Enqueue Requests Per Txn'
Results:
Row 1: Long duration value (60-second)

Enqueue Timeouts Per Sec.

This metric represents the total number of table and row locks (acquired and converted) per second that time out before they could complete.
Measurement unit: Timeouts Per Second
select value from sys.v_$sysmetric where metric_name = 'Enqueue Timeouts Per Sec'
Results:
Row 1: Long duration value (60-second)

Enqueue Timeouts Per Transaction.
This metric represents the total number of table and row locks (acquired and converted) per transaction that timed out before they could complete.
Measurement unit: Timeouts Per Transaction
select value from sys.v_$sysmetric where metric_name = 'Enqueue Timeouts Per Txn'
Results:
Row 1: Long duration value (60-second)

Enqueue Waits Per Sec.
This metric represents the total number of waits per second that occurred during an enqueue convert or get because the enqueue get was deferred.
Measurement unit: Waits Per Second
select value from sys.v_$sysmetric where metric_name = 'Enqueue Waits Per Sec'
Results:
Row 1: Long duration value (60-second)

Enqueue Waits Per Transaction.
This metric represents the total number of waits per transaction that occurred during an enqueue convert or get because the enqueue get was deferred.
Measurement unit: Waits Per Transaction
select value from sys.v_$sysmetric where metric_name = 'Enqueue Waits Per Txn'
Results:
Row 1: Long duration value (60-second)

Execute Without Parse Ratio.
This metric represents the percentage of statement executions that do not require a corresponding parse. A perfect system would parse all statements once and then execute the parsed statement over and over without reparsing. This ratio provides an indication as to how often the application is parsing statements as compared to their overall execution rate. A higher number is better.
Measurement unit: % (ExecWOParse/TotalExec)
select value from sys.v_$sysmetric where metric_name = 'Execute Without Parse Ratio' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

Executions Per Sec.
This metric represents the rate of SQL command executions over the sampling interval.
Measurement unit: Executes Per Second
select value from sys.v_$sysmetric where metric_name = 'Executions Per Sec' order by group_id
Results:

Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

Executions Per Transaction.
This metric represents the rate of SQL command executions per transaction over the sampling interval.
Measurement unit: Executes Per Transaction
select value from sys.v_$sysmetric where metric_name = 'Executions Per Txn' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

Executions Per User Call.
This metric represents the rate of SQL command executions per user call over the sampling interval.
Measurement unit: Executes Per Call
select value from sys.v_$sysmetric where metric_name = 'Executions Per User Call'
Results:
Row 1: Long duration value (60-second)

Full Index Scans Per Sec.
This metric represents the number of fast full index scans per second.
Measurement unit: Scans Per Second
select value from sys.v_$sysmetric where metric_name = 'Full Index Scans Per Sec' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

Full Index Scans Per Transaction.
This metric represents the number of fast full index scans per transaction.
Measurement unit: Scans Per Transaction
select value from sys.v_$sysmetric where metric_name = 'Full Index Scans Per Txn' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

GC CR Block Received Per Second.
Global Cache Consistent Read Blocks received per second
Measurement unit: Blocks Per Second
select value from sys.v_$sysmetric where metric_name = 'GC CR Block Received Per Second'
Results:
Row 1: Long duration value (60-second)

GC CR Block Received Per Transaction.
Global Cache Consistent Read Blocks received per transaction
Measurement unit: Blocks Per Transaction

select value from sys.v_$sysmetric where metric_name = 'GC CR Block Received Per Txn'
Results:
Row 1: Long duration value (60-second)

GC Current Block Received Per Second.
Global Cache Current Blocks received per second
Measurement unit: Blocks Per Second
select value from sys.v_$sysmetric where metric_name = 'GC Current Block Received Per Second'
Results:
Row 1: Long duration value (60-second)

GC Current Block Received Per Transaction.
Global Cache Current Blocks received per transaction
Measurement unit: Blocks Per Transaction
select value from sys.v_$sysmetric where metric_name = 'GC Current Block Received Per Txn'
Results:
Row 1: Long duration value (60-second)

Leaf Node Splits Per Sec.
Number of times per second an index leaf node was split because of the insertion of an additional value.
Measurement unit: Splits Per Second
select value from sys.v_$sysmetric where metric_name = 'Leaf Node Splits Per Sec'
Results:
Row 1: Long duration value (60-second)

Leaf Node Splits Per Transaction.
Number of times per transaction an index leaf node was split because of the insertion of an additional value.
Measurement unit: Splits Per Transaction
select value from sys.v_$sysmetric where metric_name = 'Leaf Node Splits Per Txn'
Results:
Row 1: Long duration value (60-second)

Library Cache Hit Ratio.
This metric represents the library cache efficiency, as measured by the percentage of times the fully parsed or compiled representation of PL/SQL blocks and SQL statements are already in memory.
The shared pool is an area in the SGA that contains the library cache of shared SQL requests, the dictionary cache and the other cache structures that are specific to a particular instance configuration.
The shared pool mechanism can greatly reduce system resource consumption in at least three ways: Parse time is avoided if the SQL statement is already in the shared pool.
Application memory overhead is reduced, since all applications use the same pool of shared SQL statements and dictionary resources.
I/O resources are saved, since dictionary elements that are in the shared pool do not require access.
If the shared pool is too small, users will consume additional resources to complete a database operation. For library cache access, the overhead is primarily the additional CPU resources

required to re-parse the SQL statement.
Measurement unit: % Hits/Pins
select value from sys.v_$sysmetric where metric_name = 'Library Cache Hit Ratio' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

Library Cache Miss Ratio.
This metric represents the percentage of parse requests where the cursor is not in the cache.
Measurement unit: % Misses/Gets
select value from sys.v_$sysmetric where metric_name = 'Library Cache Miss Ratio'
Results:
Row 1: Long duration value (60-second)

Logical Reads Per Sec.
This metric represents the number of logical reads per second during the sample period. A logical read is a read request for a data block from the SGA. Logical reads may result in a physical read if the requested block does not reside with the buffer cache.
Measurement unit: Reads Per Second
select value from sys.v_$sysmetric where metric_name = 'Logical Reads Per Sec' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

Logical Reads Per Transaction.
This metric represents the number of logical reads per transaction during the sample period.
The value of this statistic is zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding per second metric of the same name will be a better indicator of current performance.
Measurement unit: Reads Per Transaction
select value from sys.v_$sysmetric where metric_name = 'Logical Reads Per Txn' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

Logical Reads Per User Call.
This metric represents the number of logical reads per user call during the sample period. A logical read is a read request for a data block from the SGA. Logical reads may result in a physical read if the requested block does not reside with the buffer cache.
Measurement unit: Reads Per Call
select value from sys.v_$sysmetric where metric_name = 'Logical Reads Per User Call'
Results:
Row 1: Long duration value (60-second)

Logons Per Transaction.
This metric represents the number of logons per transaction during the sample period.
The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" metric of the same name will be a better indicator of current performance.
Measurement unit: Logons Per Transaction
select value from sys.v_$sysmetric where metric_name = 'Logons Per Txn'
Results:
Row 1: Long duration value (60-second)

Long Table Scans Per Sec.
This metric represents the number of long table scans per second during sample period. A table is considered 'long' if the table is not cached and if its high-water mark is greater than 5 blocks.
Measurement unit: Scans Per Second
select value from sys.v_$sysmetric where metric_name = 'Long Table Scans Per Sec'
Results:
Row 1: Long duration value (60-second)

Long Table Scans Per Transaction.
This metric represents the number of long table scans per transaction during sample period. A table is considered 'long' if the table is not cached and if its high-water mark is greater than 5 blocks.
The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" metric of the same name will be a better indicator of current performance.
Measurement unit: Scans Per Transaction
select value from sys.v_$sysmetric where metric_name = 'Long Table Scans Per Txn'
Results:
Row 1: Long duration value (60-second)

Physical Reads Direct Lobs Per Sec.
This metric represents the number of direct large object (LOB) physical reads per second.
Measurement unit: Reads Per Second
select value from sys.v_$sysmetric where metric_name = 'Physical Reads Direct Lobs Per Sec'
Results:
Row 1: Long duration value (60-second)

Physical Reads Direct Lobs Per Transaction.
This metric represents the number of direct large object (LOB) physical reads per transaction.
Measurement unit: Reads Per Transaction
select value from sys.v_$sysmetric where metric_name = 'Physical Reads Direct Lobs Per Txn'
Results:
Row 1: Long duration value (60-second)

Physical Reads Direct Per Transaction.
This metric represents the number of direct physical reads per transaction.
Measurement unit: Reads Per Transaction

select value from sys.v_$sysmetric where metric_name = 'Physical Reads Direct Per Txn'
Results:
Row 1: Long duration value (60-second)

Physical Reads Per Sec.
This metric represents the number of data blocks read from disk per second during this sample period. When a user performs a SQL query, Oracle tries to retrieve the data from the database buffer cache (memory) first, then searches the disk if it is not already in memory. Reading data blocks from disk is much more inefficient than reading the data blocks from memory. The goal with Oracle should always be to maximize memory utilization.
This test checks the data blocks read from disk per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Measurement unit: Reads Per Second
select value from sys.v_$sysmetric where metric_name = 'Physical Reads Per Sec' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

Physical Reads Per Transaction.
This metric represents the number of disk reads per transaction during the sample period. When a user performs a SQL query, Oracle tries to retrieve the data from the database buffer cache (memory) first, then goes to disk if it is not in memory already. Reading data blocks from disk is much more expensive than reading the data blocks from memory. The goal with Oracle should always be to maximize memory utilization.
The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" metric of the same name will be a better indicator of current performance.
Measurement unit: Reads Per Transaction
select value from sys.v_$sysmetric where metric_name = 'Physical Reads Per Txn' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

Physical Writes Per Transaction.
This metric represents the number of disk writes per transaction during the sample period.
The value of this statistic is zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" metric of the same name is a better indicator of current performance.
Measurement unit: Writes Per Transaction
select value from sys.v_$sysmetric where metric_name = 'Physical Writes Per Txn'
Results:
Row 1: Long duration value (60-second)

Physical Writes Direct Per Transaction.
This metric represents the number of direct physical writes per transaction.
Measurement unit: Writes Per Transaction
select value from sys.v_$sysmetric where metric_name = 'Physical Writes Direct Per Txn'
Results:
Row 1: Long duration value (60-second)

Physical Writes Direct Lobs Per Transaction.
This metric represents the number of direct large object (LOB) physical writes per transaction.
Measurement unit: Writes Per Transaction
select value from sys.v_$sysmetric where metric_name = 'Physical Writes Direct Lobs Per Txn'
Results:
Row 1: Long duration value (60-second)

Physical Writes Direct Lobs Per Sec.
This metric represents the number of direct large object (LOB) physical writes per second.
Measurement unit: Writes Per Second
select value from sys.v_$sysmetric where metric_name = 'Physical Writes Direct Lobs Per Sec'
Results:
Row 1: Long duration value (60-second)

Redo Generated Per Sec.
This metric represents the amount of redo, in bytes, generated per second during this sample period.
The redo log buffer is a circular buffer in the SGA that holds information about changes made to the database. This information is stored in redo entries. Redo entries contain the information necessary to reconstruct, or redo, changes made to the database by INSERT, UPDATE, DELETE, CREATE, ALTER or DROP operations. Redo entries can be used for database recovery if necessary.
Measurement unit: Bytes Per Second
select value from sys.v_$sysmetric where metric_name = 'Redo Generated Per Sec' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

Redo Generated Per Transaction.
This metric represents the amount of redo, in bytes, generated per transaction during this sample period.
The redo log buffer is a circular buffer in the SGA that holds information about changes made to the database. This information is stored in redo entries. Redo entries contain the information necessary to reconstruct, or redo, changes made to the database by INSERT, UPDATE, DELETE, CREATE, ALTER or DROP operations. Redo entries are used for database recovery, if necessary.
The value of this statistic is zero if there have been no write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" metric of the same name will be a better indicator of current performance.

Measurement unit: Bytes Per Transaction
select value from sys.v_$sysmetric where metric_name = 'Redo Generated Per Txn' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

Redo Writes Per Sec.
This metric represents the number redo write operations per second during this sample period.
The redo log buffer is a circular buffer in the SGA that holds information about changes made to the database. This information is stored in redo entries. Redo entries contain the information necessary to reconstruct, or redo, changes made to the database by INSERT, UPDATE, DELETE, CREATE, ALTER or DROP operations. Redo entries can be used for database recovery if necessary.
The log writer processes (LGWR) is responsible for redo log buffer management; that is, writing the redo log buffer to a redo log file on disk.
Measurement unit: Writes Per Second
select value from sys.v_$sysmetric where metric_name = 'Redo Writes Per Sec' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

Redo Writes Per Transaction.
This metric represents the number of redo write operations per second during this sample period.
The redo log buffer is a circular buffer in the SGA that holds information about changes made to the database. This information is stored in redo entries. Redo entries contain the information necessary to reconstruct, or redo, changes made to the database by INSERT, UPDATE, DELETE, CREATE, ALTER or DROP operations. Redo entries are used for database recovery, if necessary.
The log writer process (LGWR) is responsible for redo log buffer management; that is, writing the redo log buffer to a redo log file on disk.
Measurement unit: Writes Per Transaction
select value from sys.v_$sysmetric where metric_name = 'Redo Writes Per Txn' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

Response Time Per Transaction.
This metric represents the time spent in database operations per transaction. It is derived from the total time that user calls spend in the database (DB time) and the number of commits and rollbacks performed. A change in this value indicates that either the workload has changed or that the database s ability to process the workload has changed because of either resource constraints or contention.
Measurement unit: CentiSeconds Per Transaction
select value from sys.v_$sysmetric where metric_name = 'Response Time Per Txn'
Results:
Row 1: Long duration value (60-second)

Row Cache Hit Ratio.

This metric represents the percentage of row cache hit ratio.
Measurement unit: % Hits/Gets
select value from sys.v_$sysmetric where metric_name = 'Row Cache Hit Ratio'
Results:
Row 1: Long duration value (60-second)

Row Cache Miss Ratio.
This metric represents the percentage of row cache miss ratio.
Measurement unit: % Misses/Gets
select value from sys.v_$sysmetric where metric_name = 'Row Cache Miss Ratio'
Results:
Row 1: Long duration value (60-second)

Rows Per Sort.
This metric represents the average number of rows per sort during this sample period.
Measurement unit: Rows Per Sort
select value from sys.v_$sysmetric where metric_name = 'Rows Per Sort'
Results:
Row 1: Long duration value (60-second)

Total Index Scans Per Sec.
This metric represents the total number of index scans per second.
Measurement unit: Scans Per Second
select value from sys.v_$sysmetric where metric_name = 'Total Index Scans Per Sec'
Results:
Row 1: Long duration value (60-second)

Total Index Scans Per Transaction.
This metric represents the total number of index scans per transaction.
Measurement unit: Scans Per Transaction
select value from sys.v_$sysmetric where metric_name = 'Total Index Scans Per Txn'
Results:
Row 1: Long duration value (60-second)

Total Parse Count Per Sec.
This number reflects the total number of parses per second, both hard and soft. A hard parse occurs when a SQL statement has to be loaded into the shared pool. In this case, the Oracle Server has to allocate memory in the shared pool and parse the statement. A soft parse is recorded when the Oracle Server checks the shared pool for a SQL statement and finds a version of the statement that it can reuse.
Each time a particular SQL cursor is parsed, this count will increase by one. There are certain operations which will cause a SQL cursor to be parsed. Parsing a SQL statement breaks it down into atomic steps which the optimizer will evaluate when generating an execution plan for the cursor
Measurement unit: Parses Per Second
select value from sys.v_$sysmetric where metric_name = 'Total Parse Count Per Sec'
Results:
Row 1: Long duration value (60-second)

Total Parse Count Per Transaction.
This number reflects the total number of parses per transaction, both hard and soft. A hard parse occurs when a SQL statement has to be loaded into the shared pool. In this case, the Oracle Server has to allocate memory in the shared pool and parse the statement. A soft parse is recorded when the Oracle Server checks the shared pool for a SQL statement and finds a version of the statement that it can reuse.
Each time a particular SQL cursor is parsed, this count will increase by one. There are certain operations which will cause a SQL cursor to be parsed. Parsing a SQL statement breaks it down into atomic steps which the optimizer will evaluate when generating an execution plan for the cursor.
Measurement unit: Parses Per Transaction
select value from sys.v_$sysmetric where metric_name = 'Total Parse Count Per Txn'
Results:
Row 1: Long duration value (60-second)

Total Table Scans Per Sec.
This metric represents the total number of table scans per second during sample period
Measurement unit: Scans Per Second
select value from sys.v_$sysmetric where metric_name = 'Total Table Scans Per Sec' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

Total Table Scans Per Transaction.
This metric represents the total number of table scans per transaction during sample period
Measurement unit: Scans Per Transaction
select value from sys.v_$sysmetric where metric_name = 'Total Table Scans Per Txn' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

User Calls Per Transaction.
This metric represents the number of logins, parses, or execute calls per transaction during the sample period.
The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" metric of the same name will be a better indicator of current performance.
Measurement unit: Calls Per Transaction
select value from sys.v_$sysmetric where metric_name = 'User Calls Per Txn' order by group_id
Results:
Row 1: Long duration value (60-second)
Row 2: Short duration value (15-second)

User Rollback Undo Records Applied Per Transaction.

This metric represents the number of undo records applied to user-requested rollback changes per transaction.
Measurement unit: Records Per Transaction
select value from sys.v_$sysmetric where metric_name = 'User Rollback Undo Records Applied Per Txn'
Results:
Row 1: Long duration value (60-second)

User Rollback Undo Rec Applied Per Sec.
This metric represents the number of undo records applied to user-requested rollback changes per second.
Measurement unit: Records Per Second
select value from sys.v_$sysmetric where metric_name = 'User Rollback UndoRec Applied Per Sec'
Results:
Row 1: Long duration value (60-second)

User Commits Per Sec.
This metric represents the number of user commits performed, per second during the sample period. When a user commits a transaction, the redo generated that reflects the changes made to database blocks must be written to disk. Commits often represent the closest thing to a user transaction rate.
Measurement unit: Commits Per Second
select value from sys.v_$sysmetric where metric_name = 'User Commits Per Sec'
Results:
Row 1: Long duration value (60-second)

Appendix #2: **User operations log: list of implemented operations**

User operations log: list of implemented operations

Operation ID	Operation description
0	HostMonitor started
1	Monitoring started
2	Monitoring stopped
3	Alerts enabled
4	Alerts disabled
6	HostMonitor will be terminated
7	HostMonitor will be reloaded
8	HostMonitor settings reloaded
9	New test list created
10	Test list loaded
11	New settings applied
12	Import from text file
13	Merged HML file
14	HM Script started
15	HM Script finished
16	Test list file properties changed
20	New test item
21	New test link
22	Test modified (single test modified)
23	Test modified (group of tests were modified)
24	Test parameter changed (parameter was changes by HM Script or Telnet)
25	Test moved (test moved from one folder to another)
26	Test deleted
27	Test link deleted
28	Test paused
29	Test resumed
30	Test scheduled to be paused
31	Test pause repealed
32	Test refreshed
33	Test statistics resetted
34	Test disabled
35	Test enabled
36	Test status acknowledged
37	Status acknowledged and alerts for this test stopped
38	Acknowledgement recalled
39	Test quick log cleaned

50	Entire folder refreshed
51	Entire folder resetted
52	Entire folder disabled
53	Entire folder enabled
60	Folder created
61	Folder edited
62	Folder renamed
63	Folder deleted
64	Folder moved
65	Folders resorted
66	Folder-specific agent changed
67	Folder variables changed
70	View created
71	View edited
72	View renamed
73	View deleted
74	View moved
75	Views resorted
80	Denomination